Addition laws on elliptic curves

D. J. Bernstein
University of Illinois at Chicago

Joint work with:
Tanja Lange
Technische Universiteit Eindhoven

2007.01.10, 09:00 (yikes!),
Leiden University, part of
"Mathematics: Algorithms and
Proofs" week at Lorentz Center:

Harold Edwards speaks on
"Addition on elliptic curves."

Edwards

on laws on elliptic curves

Bernstein

sity of Illinois at Chicago

work with:

Lange

sche Universiteit Eindhoven

2007.01.10, 09:00 (yikes!),
Leiden University, part of
"Mathematics: Algorithms and
Proofs" week at Lorentz Center:

Harold Edwards speaks on
"Addition on elliptic curves."

Edwards

What w
"additi

Additio

elliptic curves

ois at Chicago

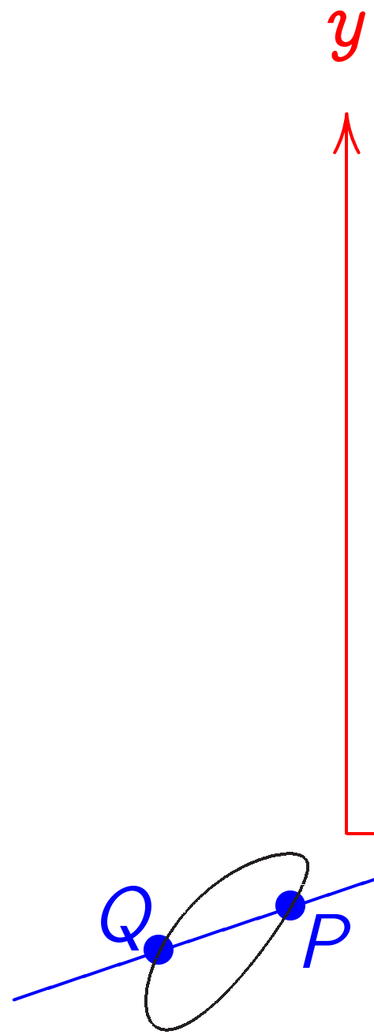
ersiteit Eindhoven

2007.01.10, 09:00 (yikes!),
Leiden University, part of
"Mathematics: Algorithms and
Proofs" week at Lorentz Center:

Harold Edwards speaks on
"Addition on elliptic curves."

Edwards

What we think w
"addition on ellip



Addition on y^2 –

urves

cago

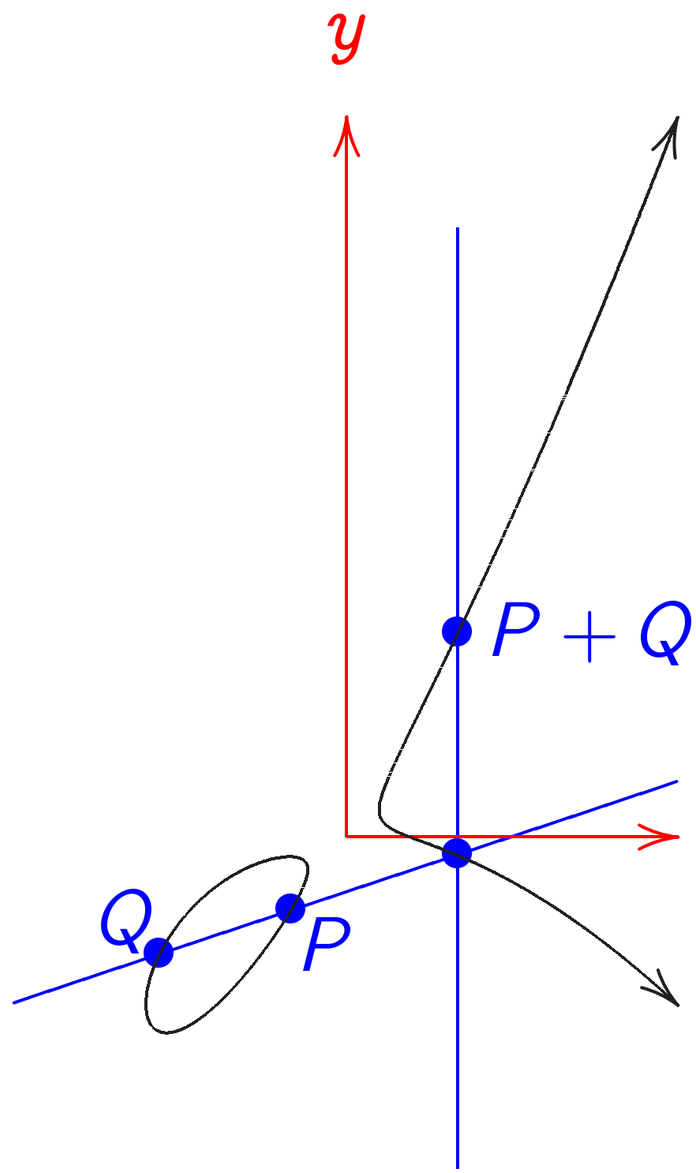
dhoven

2007.01.10, 09:00 (yikes!),
Leiden University, part of
"Mathematics: Algorithms and
Proofs" week at Lorentz Center:

Harold Edwards speaks on
"Addition on elliptic curves."

Edwards

What we think when we he
"addition on elliptic curves



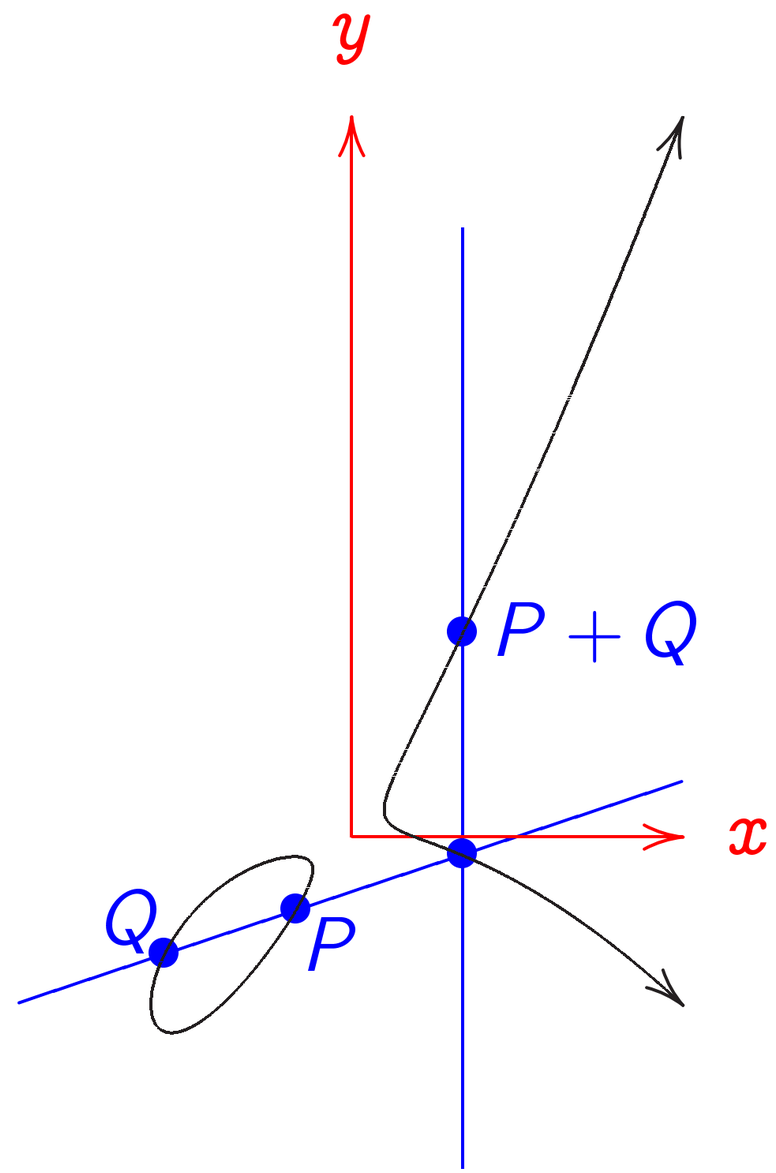
Addition on $y^2 - 5xy = x^3$

2007.01.10, 09:00 (yikes!), Leiden University, part of "Mathematics: Algorithms and Proofs" week at Lorentz Center:

Harold Edwards speaks on "Addition on elliptic curves."

Edwards

What we think when we hear "addition on elliptic curves":



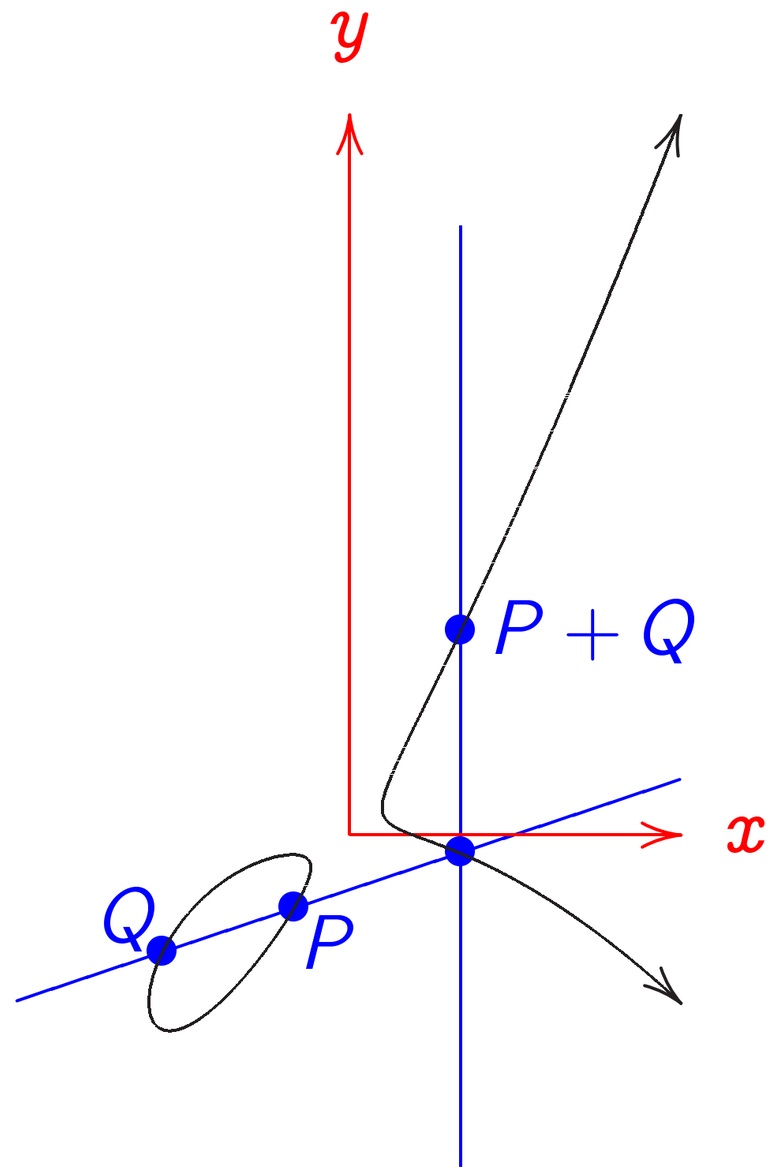
Addition on $y^2 - 5xy = x^3 - 7$.

1.10, 09:00 (yikes!),
University, part of
ematics: Algorithms and
' week at Lorentz Center:

Edwards speaks on
ion on elliptic curves."

Edwards

What we think when we hear
"addition on elliptic curves":

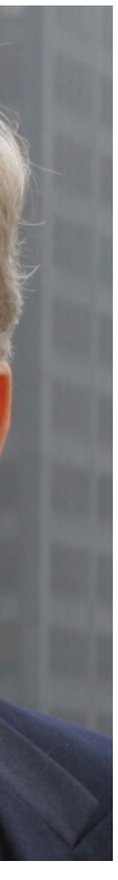


Addition on $y^2 - 5xy = x^3 - 7$.

$\lambda = (y$
$x_3 = \lambda$
$y_3 = 5$
$\Rightarrow (x_1$

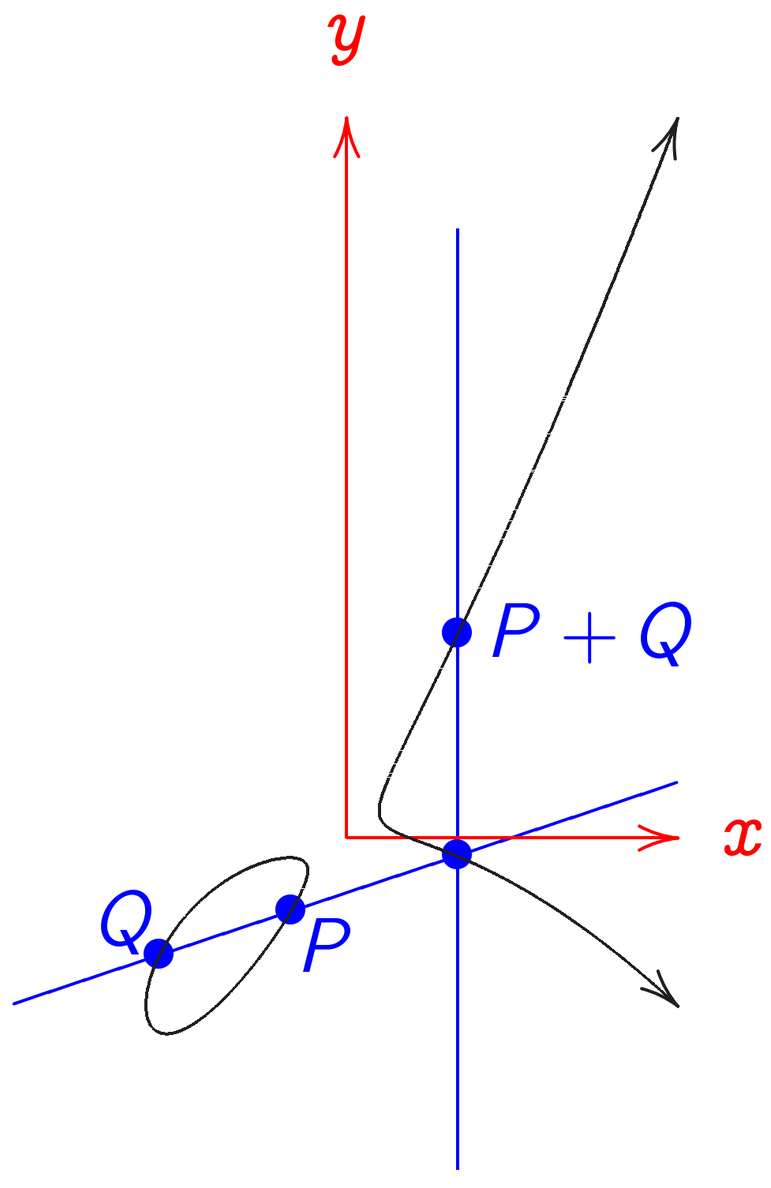
0 (yikes!),
, part of
Algorithms and
Lorentz Center:

speaks on
ptic curves."



Edwards

What we think when we hear
"addition on elliptic curves":



Addition on $y^2 - 5xy = x^3 - 7$.

$\lambda = (y_2 - y_1)/(x$
$x_3 = \lambda^2 - 5\lambda -$
$y_3 = 5x_3 - (y_1 +$
$\Rightarrow (x_1, y_1) + (x_2$

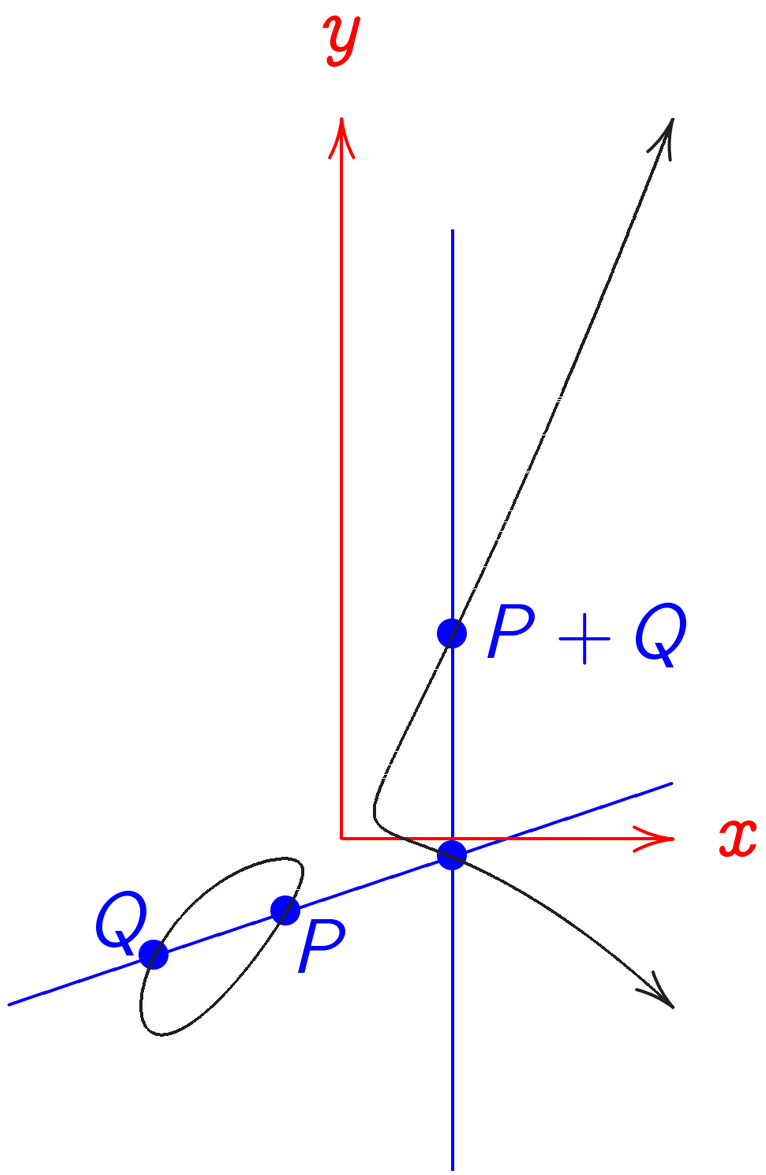
and

enter:

s."

ls

What we think when we hear "addition on elliptic curves":



Addition on $y^2 - 5xy = x^3 - 7$.

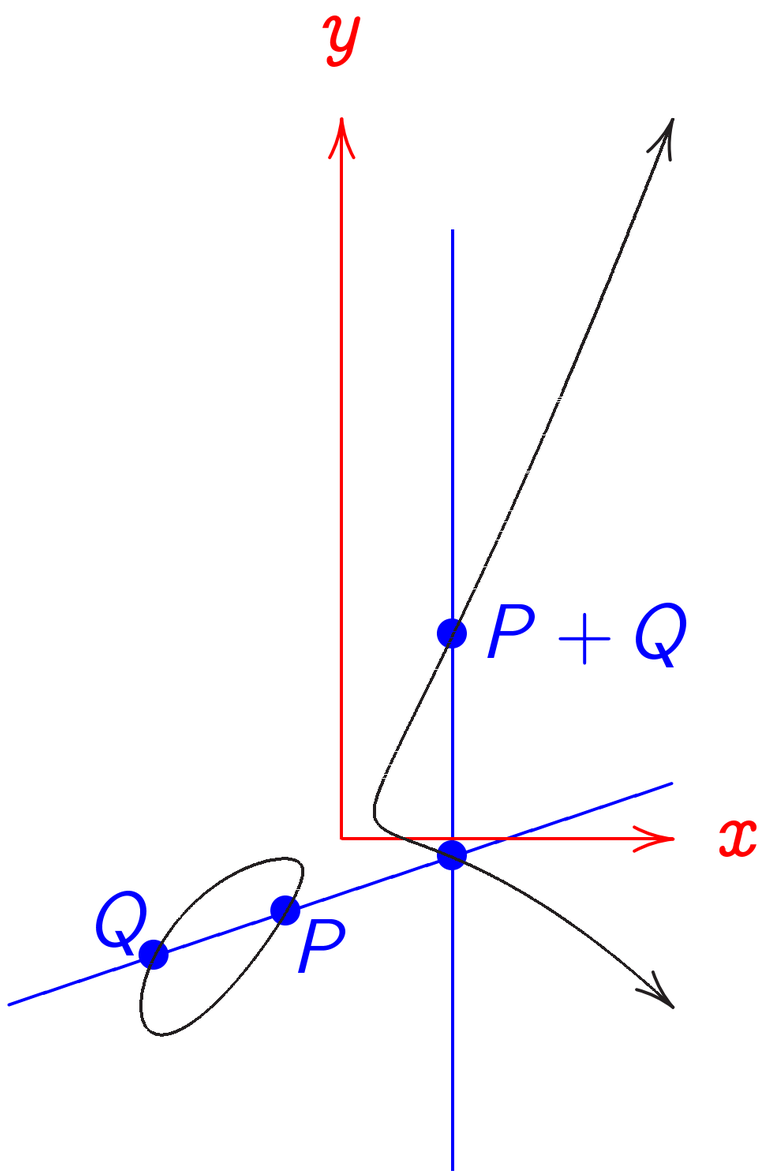
$\lambda = (y_2 - y_1)/(x_2 - x_1)$,

$x_3 = \lambda^2 - 5\lambda - x_1 - x_2$,

$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x$

$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x$

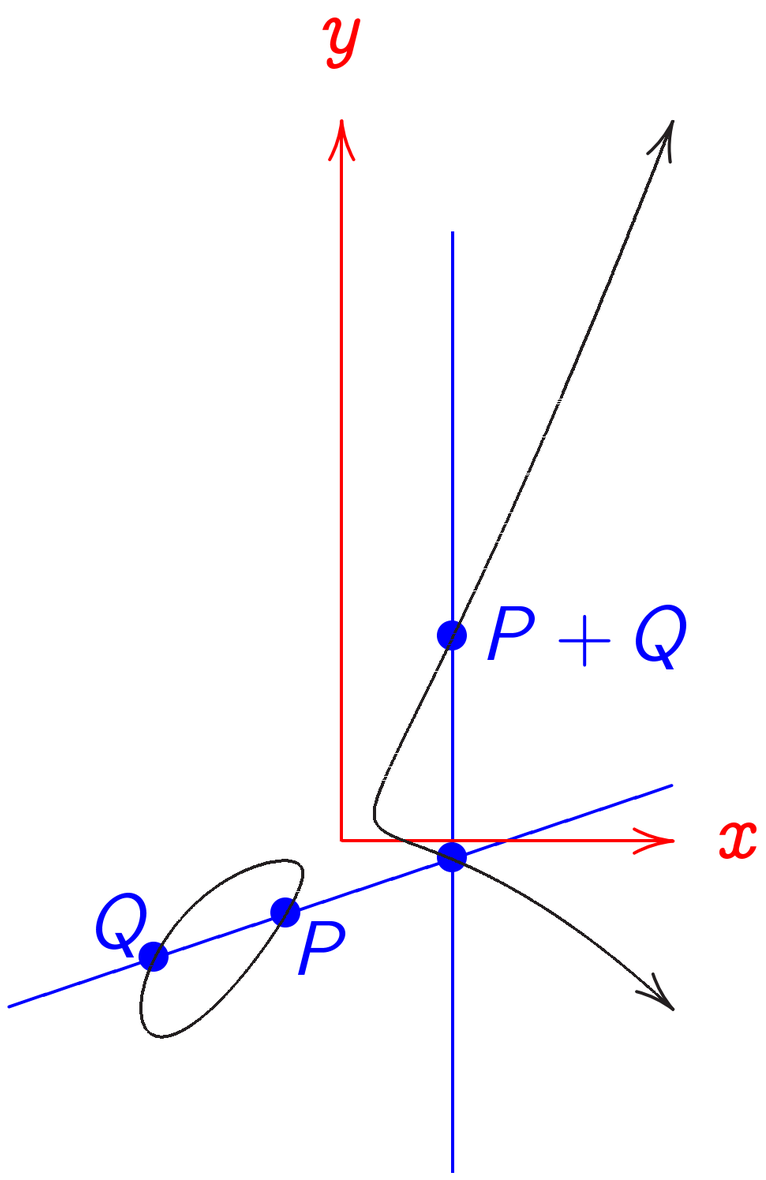
What we think when we hear "addition on elliptic curves":



Addition on $y^2 - 5xy = x^3 - 7$.

$$\lambda = (y_2 - y_1)/(x_2 - x_1),$$
$$x_3 = \lambda^2 - 5\lambda - x_1 - x_2,$$
$$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$$
$$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3).$$

What we think when we hear "addition on elliptic curves":



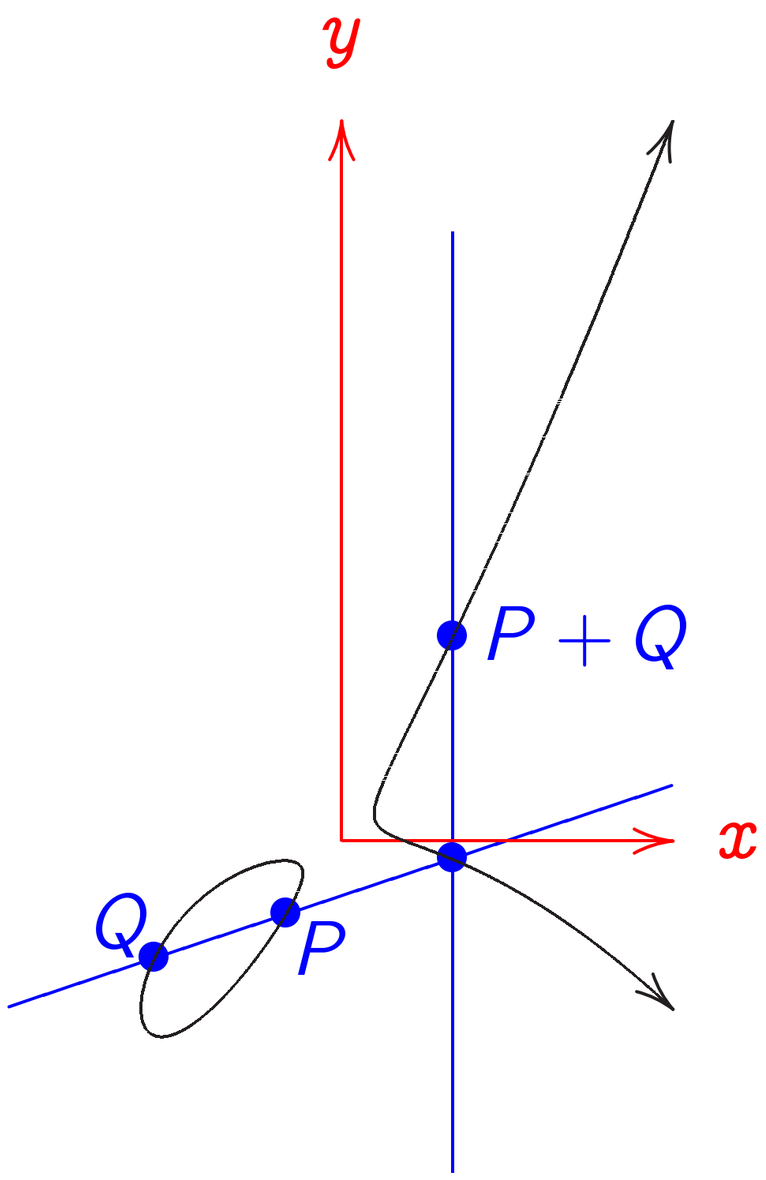
Addition on $y^2 - 5xy = x^3 - 7$.

$$\lambda = (y_2 - y_1)/(x_2 - x_1),$$
$$x_3 = \lambda^2 - 5\lambda - x_1 - x_2,$$
$$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$$
$$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3).$$

Oops, this requires $x_1 \neq x_2$.

$$\lambda = (5y_1 + 3x_1^2)/(2y_1 - 5x_1),$$
$$x_3 = \lambda^2 - 5\lambda - 2x_1,$$
$$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$$
$$\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3).$$

What we think when we hear "addition on elliptic curves":



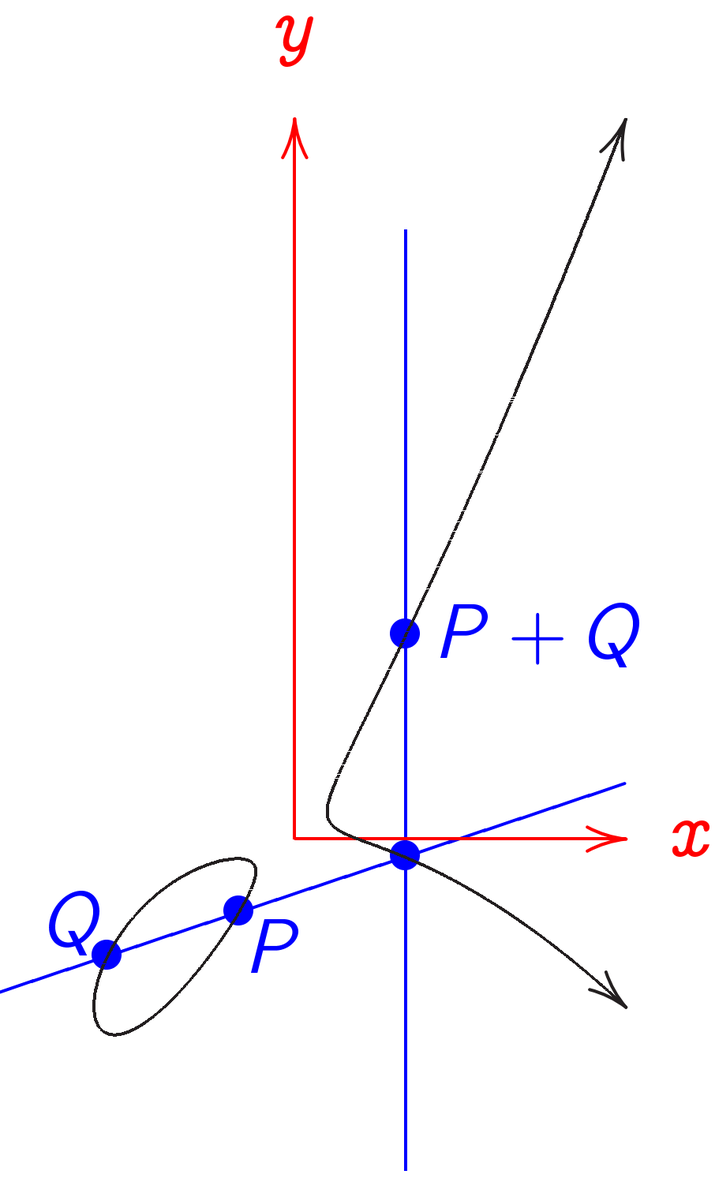
Addition on $y^2 - 5xy = x^3 - 7$.

$\lambda = (y_2 - y_1)/(x_2 - x_1)$,
$x_3 = \lambda^2 - 5\lambda - x_1 - x_2$,
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$.
Oops, this requires $x_1 \neq x_2$.

$\lambda = (5y_1 + 3x_1^2)/(2y_1 - 5x_1)$,
$x_3 = \lambda^2 - 5\lambda - 2x_1$,
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3)$.
Oops, this requires $2y_1 \neq 5x_1$.

$(x_1, y_1) + (x_1, 5x_1 - y_1) = \infty$.
$(x_1, y_1) + \infty = (x_1, y_1)$.
$\infty + (x_1, y_1) = (x_1, y_1)$.
$\infty + \infty = \infty$.

we think when we hear
on on elliptic curves":



on on $y^2 - 5xy = x^3 - 7$.

$\lambda = (y_2 - y_1)/(x_2 - x_1)$,
$x_3 = \lambda^2 - 5\lambda - x_1 - x_2$,
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$.
Oops, this requires $x_1 \neq x_2$.

$\lambda = (5y_1 + 3x_1^2)/(2y_1 - 5x_1)$,
$x_3 = \lambda^2 - 5\lambda - 2x_1$,
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3)$.
Oops, this requires $2y_1 \neq 5x_1$.

$(x_1, y_1) + (x_1, 5x_1 - y_1) = \infty$.
$(x_1, y_1) + \infty = (x_1, y_1)$.
$\infty + (x_1, y_1) = (x_1, y_1)$.
$\infty + \infty = \infty$.

Despite
despite
we atte

Edwarc

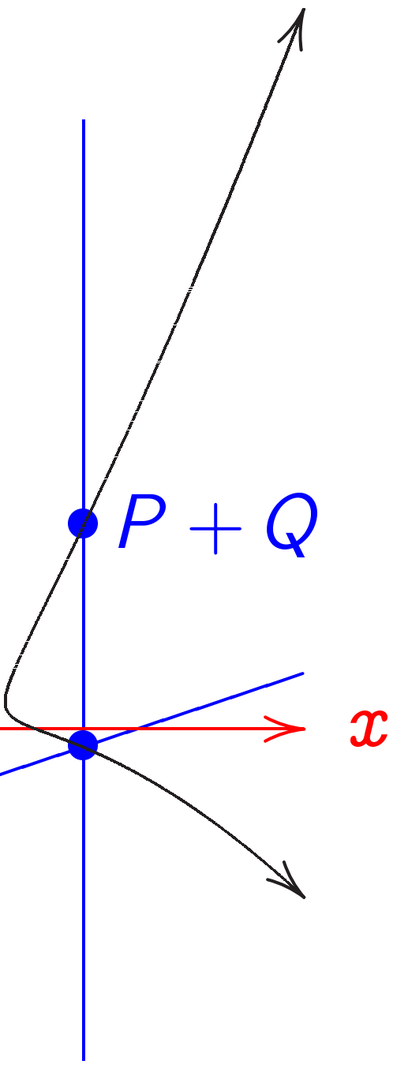
Euler–
on x^2 -
$(x_1, y_1$

$x_3 = \frac{}{1}$

$y_3 = \frac{}{1}$

hen we hear

tic curves":



$- 5xy = x^3 - 7.$

$\lambda = (y_2 - y_1)/(x_2 - x_1),$
$x_3 = \lambda^2 - 5\lambda - x_1 - x_2,$
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3).$
Oops, this requires $x_1 \neq x_2$.

$\lambda = (5y_1 + 3x_1^2)/(2y_1 - 5x_1),$
$x_3 = \lambda^2 - 5\lambda - 2x_1,$
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3).$
Oops, this requires $2y_1 \neq 5x_1$.

$(x_1, y_1) + (x_1, 5x_1 - y_1) = \infty.$
$(x_1, y_1) + \infty = (x_1, y_1).$
$\infty + (x_1, y_1) = (x_1, y_1).$
$\infty + \infty = \infty.$

Despite 09:00,
despite Dutch tra
we attend the ta

Edwards says:

Euler–Gauss addi
on $x^2 + y^2 = 1 -$
$(x_1, y_1) + (x_2, y_2$

$$x_3 = \frac{x_1y_2 + y_1}{1 - x_1x_2y_1}$$

$$y_3 = \frac{y_1y_2 - x_1}{1 + x_1x_2y_1}$$

Euler

ear
":

x

$^3 - 7.$

$\lambda = (y_2 - y_1)/(x_2 - x_1),$
$x_3 = \lambda^2 - 5\lambda - x_1 - x_2,$
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3).$
Oops, this requires $x_1 \neq x_2$.

$\lambda = (5y_1 + 3x_1^2)/(2y_1 - 5x_1),$
$x_3 = \lambda^2 - 5\lambda - 2x_1,$
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3).$
Oops, this requires $2y_1 \neq 5x_1$.

$(x_1, y_1) + (x_1, 5x_1 - y_1) = \infty.$
$(x_1, y_1) + \infty = (x_1, y_1).$
$\infty + (x_1, y_1) = (x_1, y_1).$
$\infty + \infty = \infty.$

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y$

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

G

$\lambda = (y_2 - y_1)/(x_2 - x_1)$,
$x_3 = \lambda^2 - 5\lambda - x_1 - x_2$,
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$.
Oops, this requires $x_1 \neq x_2$.

$\lambda = (5y_1 + 3x_1^2)/(2y_1 - 5x_1)$,
$x_3 = \lambda^2 - 5\lambda - 2x_1$,
$y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))$
$\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3)$.
Oops, this requires $2y_1 \neq 5x_1$.

$(x_1, y_1) + (x_1, 5x_1 - y_1) = \infty$.
$(x_1, y_1) + \infty = (x_1, y_1)$.
$\infty + (x_1, y_1) = (x_1, y_1)$.
$\infty + \infty = \infty$.

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

$_2 - y_1)/(x_2 - x_1)$,
$^2 - 5\lambda - x_1 - x_2$,
$x_3 - (y_1 + \lambda(x_3 - x_1))$
$, y_1) + (x_2, y_2) = (x_3, y_3)$.
this requires $x_1 \neq x_2$.

$y_1 + 3x_1^2)/(2y_1 - 5x_1)$,
$^2 - 5\lambda - 2x_1$,
$x_3 - (y_1 + \lambda(x_3 - x_1))$
$, y_1) + (x_1, y_1) = (x_3, y_3)$.
this requires $2y_1 \neq 5x_1$.

$) + (x_1, 5x_1 - y_1) = \infty$.
$) + \infty = (x_1, y_1)$.
$x_1, y_1) = (x_1, y_1)$.
$\circ = \infty$.

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

Edward

Every
is birat
$x^2 + y$
for som

(Euler–
"lemnis

$x_2 - x_1)$,
$x_1 - x_2$,
$+ \lambda(x_3 - x_1))$
$_2, y_2) = (x_3, y_3)$.
es $x_1 \neq x_2$.

$/(2y_1 - 5x_1)$,
$2x_1$,
$+ \lambda(x_3 - x_1))$
$_1, y_1) = (x_3, y_3)$.
es $2y_1 \neq 5x_1$.

$x_1 - y_1) = \infty$.
(x_1, y_1).
(x_1, y_1).

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

Edwards, continu

Every elliptic cur
is birationally equ
$x^2 + y^2 = a^2(1 -$
for some $a \in \overline{\mathbf{Q}}$ -

(Euler–Gauss cur
"lemniscatic ellip

$x_1))$

$x_3, y_3).$

$^2.$

$x_1),$

$x_1))$

$x_3, y_3).$

$\sqrt{5}x_1.$

$= \infty.$

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm$

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve."

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve.")

Despite 09:00,
despite Dutch trains,
we attend the talk.

Edwards says:

Euler–Gauss addition law
on $x^2 + y^2 = 1 - x^2y^2$ is
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve.")

$x^2 + y^2 = a^2(1 + x^2y^2)$ has
neutral element $(0, a)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

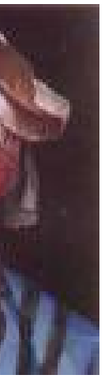
e 09:00,
e Dutch trains,
end the talk.

ds says:

Gauss addition law
$+ y^2 = 1 - x^2y^2$ is
$) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 - x_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 + x_1x_2y_1y_2}.$$


Euler

Gauss

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve.")

$x^2 + y^2 = a^2(1 + x^2y^2)$ has
neutral element $(0, a)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)},$$

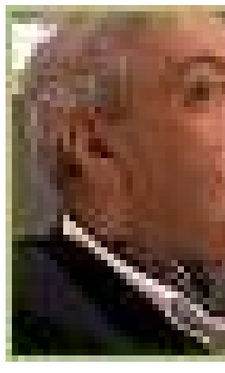
$$y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Additio
$(x_1, y_1$

$x_3 = \frac{}{a}$

$y_3 = \frac{}{a}$

Have s
e.g., 19
17**M** u
for $(S$
$S^2 + C$



ains,
lk.

ition law
$-x^2y^2$ is
$_2) = (x_3, y_3)$ with

$$\frac{x_2}{y_1 y_2},$$

$$\frac{x_2}{y_1 y_2}.$$


Gauss

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve.")

$x^2 + y^2 = a^2(1 + x^2y^2)$ has
neutral element $(0, a)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Addition law is "

$(x_1, y_1) + (x_1, y_1$

$$x_3 = \frac{x_1y_1 + y}{a(1 + x_1x_1}$$

$$y_3 = \frac{y_1y_1 - x}{a(1 - x_1x_1}$$

Have seen unifica
e.g., 1986 Chudn
17**M** unified add
for $(S : C : D : Z$
$S^2 + C^2 = Z^2$, k

$y_3)$ with

auss

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve.")

$x^2 + y^2 = a^2(1 + x^2y^2)$ has
neutral element $(0, a)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Addition law is "unified":

$(x_1, y_1) + (x_1, y_1) = (x_3, y$

$$x_3 = \frac{x_1y_1 + y_1x_1}{a(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{a(1 - x_1x_1y_1y_1)}.$$

Have seen unification befo
e.g., 1986 Chudnovsky[2]:
17**M** unified addition formu
for $(S : C : D : Z)$ on Jaco
$S^2 + C^2 = Z^2$, $k^2S^2 + D^2$

Edwards, continued:

Every elliptic curve over $\overline{\mathbf{Q}}$
is birationally equivalent to
$x^2 + y^2 = a^2(1 + x^2y^2)$
for some $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

(Euler–Gauss curve $\equiv$ the
"lemniscatic elliptic curve.")

$x^2 + y^2 = a^2(1 + x^2y^2)$ has
neutral element $(0, a)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Addition law is "unified":

$(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_1 + y_1x_1}{a(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{a(1 - x_1x_1y_1y_1)}.$$

Have seen unification before.
e.g., 1986 Chudnovsky[2]:
17**M** unified addition formulas
for $(S : C : D : Z)$ on Jacobi's
$S^2 + C^2 = Z^2$, $k^2S^2 + D^2 = Z^2$.

ds, continued:

elliptic curve over $\overline{\mathbf{Q}}$
ionally equivalent to
$^2 = a^2(1 + x^2y^2)$
ne $a \in \overline{\mathbf{Q}} - \{0, \pm 1, \pm i\}$.

-Gauss curve $\equiv$ the
scatic elliptic curve.")

$^2 = a^2(1 + x^2y^2)$ has
element $(0, a)$, addition
$) + (x_2, y_2) = (x_3, y_3)$ with

$$\frac{x_1y_2 + y_1x_2}{a(1 + x_1x_2y_1y_2)},$$

$$\frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)}.$$

Addition law is "unified":

$(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_1 + y_1x_1}{a(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{a(1 - x_1x_1y_1y_1)}.$$

Have seen unification before.
e.g., 1986 Chudnovsky[2]:
17**M** unified addition formulas
for $(S : C : D : Z)$ on Jacobi's
$S^2 + C^2 = Z^2$, $k^2S^2 + D^2 = Z^2$.

2007.0
Bernste

Edwar
standa
standa
commo
10**M** +
Faster

M: fie
S: fiel
A: mu

ued:

rve over $\overline{\mathbf{Q}}$

uivalent to

$+ x^2y^2)$

$- \{0, \pm 1, \pm i\}$.

rve $\equiv$ the

otic curve.")

$+ x^2y^2)$ has

$(0, a)$, addition

$_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_1 + y_1x_1}{a(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{a(1 - x_1x_1y_1y_1)}.$$

Addition law is "unified":

$(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_1 + y_1x_1}{a(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{a(1 - x_1x_1y_1y_1)}.$$

Have seen unification before.

e.g., 1986 Chudnovsky[2]:

17**M** unified addition formulas

for $(S : C : D : Z)$ on Jacobi's

$S^2 + C^2 = Z^2$, $k^2S^2 + D^2 = Z^2$.

2007.01.10, $\approx$ 09

Bernstein–Lange

Edwards addition

standard projecti

standard Karatsu

common-subexp

$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A}$.

Faster than anyt

M: field multipli

S: field squaring

A: multiplication

Karatsu

Addition law is "unified":

$(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ with

$$x_3 = \frac{x_1 y_1 + y_1 x_1}{a(1 + x_1 x_1 y_1 y_1)},$$

$$y_3 = \frac{y_1 y_1 - x_1 x_1}{a(1 - x_1 x_1 y_1 y_1)}.$$

Have seen unification before.

e.g., 1986 Chudnovsky[2]:

17**M** unified addition formulas for $(S : C : D : Z)$ on Jacobi's $S^2 + C^2 = Z^2$, $k^2 S^2 + D^2 = Z^2$.

2007.01.10, $\approx$ 09:30, Bernstein–Lange:

Edwards addition law with standard projective $(X : Y$ standard Karatsuba optimi common-subexp eliminatio $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A}$.

Faster than anything seen

M: field multiplication.

S: field squaring.

A: multiplication by a.

Karatsuba

Addition law is "unified":

$(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_1 + y_1x_1}{a(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{a(1 - x_1x_1y_1y_1)}.$$

Have seen unification before.

e.g., 1986 Chudnovsky[2]:

17**M** unified addition formulas

for $(S : C : D : Z)$ on Jacobi's

$S^2 + C^2 = Z^2$, $k^2S^2 + D^2 = Z^2$.

2007.01.10, $\approx$ 09:30,

Bernstein–Lange:

Edwards addition law with

standard projective $(X : Y : Z)$,

standard Karatsuba optimization,

common-subexp elimination:

10**M** + 1**S** + 1**A**.

Faster than anything seen before!

M: field multiplication.

S: field squaring.

A: multiplication by a.

Karatsuba

on law is "unified":

$) + (x_1, y_1) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_1 + y_1x_1}{c(1 + x_1x_1y_1y_1)},$$

$$y_3 = \frac{y_1y_1 - x_1x_1}{c(1 - x_1x_1y_1y_1)}.$$

een unification before.

986 Chudnovsky[2]:

nified addition formulas

$: C : D : Z)$ on Jacobi's

$^2 = Z^2$, $k^2S^2 + D^2 = Z^2$.

2007.01.10, $\approx$ 09:30,
Bernstein–Lange:

Edwards addition law with
standard projective $(X : Y : Z)$,
standard Karatsuba optimization,
common-subexp elimination:
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A}$.
Faster than anything seen before!

M: field multiplication.

S: field squaring.

A: multiplication by a.

Karatsuba

Edward
44 (20

Many p
have n
to set s
for crit
in ellip

Also ne
for EC
Lange's

Also ex
elliptic-

unified":

$_1) = (x_3, y_3)$ with

$$\frac{y_1x_1}{y_1y_1)},$$

$$\frac{_1x_1}{y_1y_1)}.$$

ation before.

novsky[2]:

ition formulas

Z) on Jacobi's

$c^2S^2 + D^2 = Z^2$.

2007.01.10, $\approx$ 09:30,
Bernstein–Lange:

Edwards addition law with
standard projective $(X : Y : Z)$,
standard Karatsuba optimization,
common-subexp elimination:
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A}$.
Faster than anything seen before!

M: field multiplication.

S: field squaring.

A: multiplication by a.

Karatsuba

Edwards paper:
44 (2007), 393–4

Many papers in 2
have now used E
to set speed reco
for critical compu
in elliptic-curve c

Also new speed r
for ECM factoriz
Lange's talk here

Also expect spee
elliptic-curve prim

y_3) with

re.

ulas

bbi's

$^2 = Z^2$.

2007.01.10, $\approx$ 09:30,
Bernstein–Lange:

Edwards addition law with
standard projective $(X : Y : Z)$,
standard Karatsuba optimization,
common-subexp elimination:
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A}$.
Faster than anything seen before!

M: field multiplication.
S: field squaring.
A: multiplication by a.

Karatsuba

Edwards paper: Bulletin A
44 (2007), 393–422.

Many papers in 2007, 2008
have now used Edwards cu
to set speed records
for critical computations
in elliptic-curve cryptograp

Also new speed records
for ECM factorization: see
Lange's talk here on Satur

Also expect speedups in ve
elliptic-curve primality proc

2007.01.10, $\approx$ 09:30,
Bernstein–Lange:

Edwards addition law with
standard projective $(X : Y : Z)$,
standard Karatsuba optimization,
common-subexp elimination:
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A}$.
Faster than anything seen before!

M: field multiplication.
S: field squaring.
A: multiplication by a.


Karatsuba

Edwards paper: Bulletin AMS
44 (2007), 393–422.

Many papers in 2007, 2008, 2009
have now used Edwards curves
to set speed records
for critical computations
in elliptic-curve cryptography.

Also new speed records
for ECM factorization: see
Lange's talk here on Saturday.

Also expect speedups in verifying
elliptic-curve primality proofs.

1.10, $\approx$ 09:30,
ein–Lange:

ds addition law with
rd projective $(X : Y : Z)$,
rd Karatsuba optimization,
on-subexp elimination:
$+ 1\mathbf{S} + 1\mathbf{A}$.
than anything seen before!

ld multiplication.
d squaring.
ltiplication by a.

Karatsuba

Edwards paper: Bulletin AMS
44 (2007), 393–422.

Many papers in 2007, 2008, 2009
have now used Edwards curves
to set speed records
for critical computations
in elliptic-curve cryptography.

Also new speed records
for ECM factorization: see
Lange's talk here on Saturday.

Also expect speedups in verifying
elliptic-curve primality proofs.

Back t

Edward
doesn't
Euler–C

Comm
presum
presum

$x^2 + y$

neutral

$(x_1, y_1$

$x_3 = \frac{}{c}$

$y_3 = \frac{}{c}$

9:30,

:

n law with
ve $(X : Y : Z)$,
uba optimization,
elimination:

hing seen before!

cation.

.

n by a.

uba

Edwards paper: Bulletin AMS **44** (2007), 393–422.

Many papers in 2007, 2008, 2009 have now used Edwards curves to set speed records for critical computations in elliptic-curve cryptography.

Also new speed records for ECM factorization: see Lange's talk here on Saturday.

Also expect speedups in verifying elliptic-curve primality proofs.

Back to B.–L., e

Edwards $x^2 + y^2$

doesn't *rationall*

Euler–Gauss $x^2 +$

Common general

presumably more

presumably more

$x^2 + y^2 = c^2(1 +$

neutral element (

$(x_1, y_1) + (x_2, y_2$

$$x_3 = \frac{x_1y_2 + y}{c(1 + dx_1x}$$

$$y_3 = \frac{y_1y_2 - x}{c(1 - dx_1x}$$

: Z),
zation,
n:

before!

Edwards paper: Bulletin AMS **44** (2007), 393–422.

Many papers in 2007, 2008, 2009 have now used Edwards curves to set speed records for critical computations in elliptic-curve cryptography.

Also new speed records for ECM factorization: see Lange's talk here on Saturday.

Also expect speedups in verifying elliptic-curve primality proofs.

Back to B.–L., early 2007.

Edwards $x^2 + y^2 = a^2(1 +$
doesn't *rationally* include
Euler–Gauss $x^2 + y^2 = 1 -$

Common generalization,
presumably more curves ov
presumably more curves ov

$x^2 + y^2 = c^2(1 + dx^2y^2)$ h
neutral element $(0, c)$, add
$(x_1, y_1) + (x_2, y_2) = (x_3, y$

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}.$$

Edwards paper: Bulletin AMS **44** (2007), 393–422.

Many papers in 2007, 2008, 2009 have now used Edwards curves to set speed records for critical computations in elliptic-curve cryptography.

Also new speed records for ECM factorization: see Lange's talk here on Saturday.

Also expect speedups in verifying elliptic-curve primality proofs.

Back to B.–L., early 2007.

Edwards $x^2 + y^2 = a^2(1 + x^2y^2)$ doesn't *rationally* include Euler–Gauss $x^2 + y^2 = 1 - x^2y^2$.

Common generalization, presumably more curves over $\mathbf{Q}$, presumably more curves over $\mathbf{F}_q$:

$x^2 + y^2 = c^2(1 + dx^2y^2)$ has neutral element $(0, c)$, addition $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}.$$

ds paper: Bulletin AMS
07), 393–422.

papers in 2007, 2008, 2009
ow used Edwards curves
speed records
ical computations
tic-curve cryptography.

ew speed records
M factorization: see
s talk here on Saturday.

xpect speedups in verifying
-curve primality proofs.

Back to B.–L., early 2007.

Edwards $x^2 + y^2 = a^2(1 + x^2y^2)$
doesn't *rationally* include
Euler–Gauss $x^2 + y^2 = 1 - x^2y^2$.

Common generalization,
presumably more curves over $\mathbf{Q}$,
presumably more curves over $\mathbf{F}_q$:

$x^2 + y^2 = c^2(1 + dx^2y^2)$ has
neutral element $(0, c)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}.$$

Conver
for spe

Covers
up to b
$(c, d) \equiv$

$x^2 + y$
neutral
$(x_1, y_1$

$x_3 = \frac{}{1}$

$y_3 = \frac{}{1}$

Bulletin AMS
422.

2007, 2008, 2009
dwards curves
ords
utations
cryptography.

records
ation: see
e on Saturday.

dups in verifying
mality proofs.

Back to B.–L., early 2007.

Edwards $x^2 + y^2 = a^2(1 + x^2y^2)$
doesn't *rationally* include
Euler–Gauss $x^2 + y^2 = 1 - x^2y^2$.

Common generalization,
presumably more curves over $\mathbf{Q}$,
presumably more curves over $\mathbf{F}_q$:

$x^2 + y^2 = c^2(1 + dx^2y^2)$ has
neutral element $(0, c)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}.$$

Convenient to ta
for speed, simplic

Covers same set
up to birational e
$(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx$
neutral element
$(x_1, y_1) + (x_2, y_2$

$$x_3 = \frac{x_1y_2 + y_1}{1 + dx_1x_2y}$$

$$y_3 = \frac{y_1y_2 - x_1}{1 - dx_1x_2y}$$

MS

3, 2009

rves

hy.

day.

erifying

ofs.

Back to B.–L., early 2007.

Edwards $x^2 + y^2 = a^2(1 + x^2y^2)$ doesn't *rationally* include Euler–Gauss $x^2 + y^2 = 1 - x^2y^2$.

Common generalization, presumably more curves over $\mathbf{Q}$, presumably more curves over $\mathbf{F}_q$:

$x^2 + y^2 = c^2(1 + dx^2y^2)$ has neutral element $(0, c)$, addition $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}.$$

Convenient to take $c = 1$ for speed, simplicity.

Covers same set of curves up to birational equivalenc $(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx^2y^2$ has neutral element $(0, 1)$, add $(x_1, y_1) + (x_2, y_2) = (x_3, y$

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Back to B.–L., early 2007.

Edwards $x^2 + y^2 = a^2(1 + x^2y^2)$
doesn't *rationally* include
Euler–Gauss $x^2 + y^2 = 1 - x^2y^2$.

Common generalization,
presumably more curves over $\mathbf{Q}$,
presumably more curves over $\mathbf{F}_q$:

$x^2 + y^2 = c^2(1 + dx^2y^2)$ has
neutral element $(0, c)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}.$$

Convenient to take $c = 1$
for speed, simplicity.

Covers same set of curves
up to birational equivalence:
$(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx^2y^2$ has
neutral element $(0, 1)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

o B.–L., early 2007.

ds $x^2 + y^2 = a^2(1 + x^2y^2)$
t *rationally* include
Gauss $x^2 + y^2 = 1 - x^2y^2$.

on generalization,
ably more curves over $\mathbf{Q}$,
ably more curves over $\mathbf{F}_q$:

$^2 = c^2(1 + dx^2y^2)$ has
element $(0, c)$, addition
$) + (x_2, y_2) = (x_3, y_3)$ with

$$\frac{x_1y_2 + y_1x_2}{(1 + dx_1x_2y_1y_2)},$$

$$\frac{y_1y_2 - x_1x_2}{(1 - dx_1x_2y_1y_2)}.$$

Convenient to take $c = 1$
for speed, simplicity.

Covers same set of curves
up to birational equivalence:
$(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx^2y^2$ has
neutral element $(0, 1)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Hmmm

Easiest
the ge
pull ou

Pick a
Pick cu

Enume
$(x, y) \in$
$x^2 + y$

Use ge
to mak
for all
Check

arly 2007.

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

/ include

$+ y^2 = 1 - x^2y^2$.

ization,

curves over $\mathbf{Q}$,

curves over $\mathbf{F}_q$:

$- dx^2y^2)$ has

$(0, c)$, addition

$_2) = (x_3, y_3)$ with

$$\frac{y_1x_2}{x_2y_1y_2)},$$

$$\frac{x_1x_2}{x_2y_1y_2)}.$$

Convenient to take $c = 1$
for speed, simplicity.

Covers same set of curves
up to birational equivalence:
$(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx^2y^2$ has
neutral element $(0, 1)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Hmmm, does thi

Easiest way to ch
the generalized a
pull out the com

Pick a prime p; e
Pick curve param

Enumerate all af
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$
$x^2 + y^2 = 1 + dx$

Use generalized a
to make an addit
for all pairs of po
Check associativi

$+ x^2y^2)$

$- x^2y^2.$

ver $\mathbf{Q}$,
ver $\mathbf{F}_q$:

nas
ition
$y_3)$ with

Convenient to take $c = 1$
for speed, simplicity.

Covers same set of curves
up to birational equivalence:
$(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx^2y^2$ has
neutral element $(0, 1)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Hmmm, does this really wo

Easiest way to check
the generalized addition law
pull out the computer!

Pick a prime p; e.g. 47.
Pick curve param $d \in \mathbf{F}_p$.

Enumerate all affine points
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$x^2 + y^2 = 1 + dx^2y^2$.

Use generalized addition la
to make an addition table
for all pairs of points.
Check associativity etc.

Convenient to take $c = 1$
for speed, simplicity.

Covers same set of curves
up to birational equivalence:
$(c, d) \equiv (1, dc^4)$.

$x^2 + y^2 = 1 + dx^2y^2$ has
neutral element $(0, 1)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Hmmm, does this really work?

Easiest way to check
the generalized addition law:
pull out the computer!

Pick a prime p; e.g. 47.
Pick curve param $d \in \mathbf{F}_p$.

Enumerate all affine points
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$x^2 + y^2 = 1 + dx^2y^2$.

Use generalized addition law
to make an addition table
for all pairs of points.
Check associativity etc.

nient to take $c = 1$
ed, simplicity.

same set of curves
birational equivalence:
$\equiv (1, dc^4)$.

$^2 = 1 + dx^2y^2$ has
element $(0, 1)$, addition
$) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Hmmm, does this really work?

Easiest way to check
the generalized addition law:
pull out the computer!

Pick a prime p; e.g. 47.
Pick curve param $d \in \mathbf{F}_p$.

Enumerate all affine points
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$x^2 + y^2 = 1 + dx^2y^2$.

Use generalized addition law
to make an addition table
for all pairs of points.
Check associativity etc.

Warnin
comple

Additio
but ca
excepti

Unified
works f
and for
but ca
excepti

Basic p
$1 \pm dx$

ke $c = 1$
city.

of curves
equivalence:

x^2y^2 has
$(0, 1)$, addition
$) = (x_3, y_3)$ with

$$\frac{x_1x_2}{y_1y_2},$$

$$\frac{x_2}{y_1y_2}.$$

Hmmm, does this really work?

Easiest way to check
the generalized addition law:
pull out the computer!

Pick a prime p; e.g. 47.
Pick curve param $d \in \mathbf{F}_p$.

Enumerate all affine points
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$x^2 + y^2 = 1 + dx^2y^2$.

Use generalized addition law
to make an addition table
for all pairs of points.
Check associativity etc.

Warning: Don't
complete additio

Addition law wor
but can fail for s
exceptional pairs

Unified addition
works for generic
and for generic d
but can fail for s
exceptional pairs

Basic problem: D
$1 \pm dx_1x_2y_1y_2$ c

e:

ition

$y_3)$ with

Hmmm, does this really work?

Easiest way to check
the generalized addition law:
pull out the computer!

Pick a prime p; e.g. 47.
Pick curve param $d \in \mathbf{F}_p$.

Enumerate all affine points
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$x^2 + y^2 = 1 + dx^2y^2$.

Use generalized addition law
to make an addition table
for all pairs of points.
Check associativity etc.

Warning: Don't expect
complete addition table.

Addition law works generic
but can fail for some
exceptional pairs of points.

Unified addition law
works for generic additions
and for generic doublings
but can fail for some
exceptional pairs of points.

Basic problem: Denominat
$1 \pm dx_1x_2y_1y_2$ can be zero

Hmmm, does this really work?

Easiest way to check
the generalized addition law:
pull out the computer!

Pick a prime p; e.g. 47.
Pick curve param $d \in \mathbf{F}_p$.

Enumerate all affine points
$(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$x^2 + y^2 = 1 + dx^2y^2$.

Use generalized addition law
to make an addition table
for all pairs of points.
Check associativity etc.

Warning: Don't expect
complete addition table.

Addition law works generically
but can fail for some
exceptional pairs of points.

Unified addition law
works for generic additions
and for generic doublings
but can fail for some
exceptional pairs of points.

Basic problem: Denominators
$1 \pm dx_1x_2y_1y_2$ can be zero.

n, does this really work?

way to check
neralized addition law:
t the computer!

prime p; e.g. 47.
urve param $d \in \mathbf{F}_p$.

rate all affine points
$\in \mathbf{F}_p \times \mathbf{F}_p$ satisfying
$^2 = 1 + dx^2y^2$.

neralized addition law
ke an addition table
pairs of points.
associativity etc.

Warning: Don't expect
complete addition table.

Addition law works generically
but can fail for some
exceptional pairs of points.

Unified addition law
works for generic additions
and for generic doublings
but can fail for some
exceptional pairs of points.

Basic problem: Denominators
$1 \pm dx_1x_2y_1y_2$ can be zero.

Even if
project
would
to fail
produc

1995 B
"The s
comple
on E e

Bosma

s really work?

neck

ddition law:

puter!

e.g. 47.

n $d \in \mathbf{F}_p$.

fine points

satisfying

x^2y^2.

addition law

tion table

oints.

ity etc.

Warning: Don't expect *complete* addition table.

Addition law works generically but can fail for some exceptional pairs of points.

Unified addition law works for generic additions and for generic doublings but can fail for some exceptional pairs of points.

Basic problem: Denominators $1 \pm dx_1x_2y_1y_2$ can be zero.

Even if we switch
projective coordi
would expect add
to fail for some p
producing $(0 : 0$

1995 Bosma–Len
"The smallest ca
complete system
on E equals two.

Bosma

L

ork?

w:

s

w

Warning: Don't expect
complete addition table.

Addition law works generically
but can fail for some
exceptional pairs of points.

Unified addition law
works for generic additions
and for generic doublings
but can fail for some
exceptional pairs of points.

Basic problem: Denominators
$1 \pm dx_1x_2y_1y_2$ can be zero.

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theor
"The smallest cardinality o
complete system of additio
on E equals two."

Bosma

Lenstra

Warning: Don't expect
complete addition table.

Addition law works generically
but can fail for some
exceptional pairs of points.

Unified addition law
works for generic additions
and for generic doublings
but can fail for some
exceptional pairs of points.

Basic problem: Denominators
$1 \pm dx_1x_2y_1y_2$ can be zero.

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

ng: Don't expect
ete addition table.

on law works generically
n fail for some
onal pairs of points.

addition law
for generic additions
r generic doublings
n fail for some
onal pairs of points.

problem: Denominators
$_1x_2y_1y_2$ can be zero.

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

Try $p =$
denomi
is nonz
$(x_1, y_1$
Edward
associa

expect
n table.

rks generically
ome
of points.

law
additions
oublings
ome
of points.

Denominators
an be zero.

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

Try $p = 47$, $d =$
denominator $1 \pm$
is nonzero for mo
(x_1, y_1), (x_2, y_2)
Edwards addition
associative when

ally

tors

o.

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever define

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

Even if we switched to
projective coordinates,
would expect addition law
to fail for some points,
producing $(0 : 0 : 0)$.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

Bosma

Lenstra

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

f we switched to
ive coordinates,
expect addition law
for some points,
ing $(0 : 0 : 0)$.

Bosma–Lenstra theorem:
mallest cardinality of a
ete system of addition laws
quals two."


Lenstra

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 B
comple
for all

If $x_1^2 +$
and x_2^2
and dx

ned to
nates,
dition law
points,
: 0).

nstra theorem:
rdinality of a
of addition laws
"

Lenstra

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–L
completeness pro
for all non-square

If $x_1^2 + y_1^2 = 1 +$
and $x_2^2 + y_2^2 = 1$
and $dx_1x_2y_1y_2 =$

em:
f a
n laws

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Try $p = 47$, $d = 25$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for most points
(x_1, y_1), (x_2, y_2) on curve.
Edwards addition law is
associative whenever defined.

Try $p = 47$, $d = -1$:
denominator $1 \pm dx_1x_2y_1y_2$
is nonzero for *all* points
(x_1, y_1), (x_2, y_2) on curve.
Addition law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

$= 47$, $d = 25$:

inator $1 \pm dx_1x_2y_1y_2$

ero for most points

), (x_2, y_2) on curve.

ds addition law is

tive whenever defined.

$= 47$, $d = -1$:

inator $1 \pm dx_1x_2y_1y_2$

ero for *all* points

), (x_2, y_2) on curve.

on law is a group law!

vs.

Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

1995 B
"The s
comple
on E e

25:

$dx_1x_2y_1y_2$

ost points

on curve.

n law is

ever defined.

-1:

$dx_1x_2y_1y_2$

points

on curve.

group law!

Z60T

2007 Bernstein–Lange

completeness proof

for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

1995 Bosma–Len

“The smallest ca

complete system

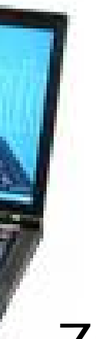
on E equals two.

y_2

ed.

y_2

v!



Z60T

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

1995 Bosma–Lenstra theor
"The smallest cardinality o
complete system of additio
on E equals two."

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two."

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two." ... meaning:
Any addition formula
for a Weierstrass curve E
in projective coordinates
must have exceptional cases
in $E(\overline{k}) \times E(\overline{k})$, where
$\overline{k}$ = algebraic closure of k.

2007 Bernstein–Lange
completeness proof
for all non-square d:

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2$.

Have $x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
either way d is a square. Q.E.D.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two." ... meaning:
Any addition formula
for a Weierstrass curve E
in projective coordinates
must have exceptional cases
in $E(\overline{k}) \times E(\overline{k})$, where
$\overline{k}$ = algebraic closure of k.

Edwards addition formula has
exceptional cases for $E(\overline{k})$
... but not for $E(k)$.
We do computations in $E(k)$.

Bernstein–Lange
teteness proof
non-square d:

$$y_1^2 = 1 + dx_1^2y_1^2$$
$$+ y_2^2 = 1 + dx_2^2y_2^2$$
$$x_1x_2y_1y_2 = \pm 1$$
$$x_1^2y_1^2(x_2 + y_2)^2$$
$$y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$$
$$y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$$
$$^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$$
$$dx_1^2y_1^2 \pm 2x_1y_1$$
$$- y_1^2 \pm 2x_1y_1 = (x_1 \pm y_1)^2.$$

$x_2 + y_2 \neq 0$ or $x_2 - y_2 \neq 0$;
way d is a square. Q.E.D.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two." . . . meaning:
Any addition formula
for a Weierstrass curve E
in projective coordinates
must have exceptional cases
in $E(\overline{k}) \times E(\overline{k})$, where
$\overline{k}$ = algebraic closure of k.

Edwards addition formula has
exceptional cases for $E(\overline{k})$
. . . but not for $E(k)$.
We do computations in $E(k)$.

Summa
$2 \neq 0$ i
Then {

is a co
$(x_1, y_1$
defined

$x_3 = \frac{}{1}$

$y_3 = \frac{}{1}$

Termin
allow a
are "or
non-sq

Lange

oof

e d:

$$dx_1^2y_1^2$$

$$+ dx_2^2y_2^2$$

$$= \pm 1$$

$$+ y_2)^2$$

$$^2_2 + 2x_2y_2)$$

$$+ 1 + 2x_2y_2)$$

$$dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$$

$$x_1y_1$$

$$y_1 = (x_1 \pm y_1)^2.$$

0 or $x_2 - y_2 \neq 0$;

square. Q.E.D.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two." ... meaning:
Any addition formula
for a Weierstrass curve E
in projective coordinates
must have exceptional cases
in $E(\overline{k}) \times E(\overline{k})$, where
$\overline{k}$ = algebraic closure of k.

Edwards addition formula has
exceptional cases for $E(\overline{k})$
... but not for $E(k)$.
We do computations in $E(k)$.

Summary: Assu
$2 \neq 0$ in k; non-s
Then $\{(x, y) \in k$
$x^2 + y^2 =$
is a commutative
$(x_1, y_1) + (x_2, y_2$
defined by Edwar

$$x_3 = \frac{x_1y_2 + y_1}{1 + dx_1x_2y}$$

$$y_3 = \frac{y_1y_2 - x_1}{1 - dx_1x_2y}$$

Terminology: "E
allow arbitrary d
are "original Edw
non-square d are

)

$y_2)$

$dx_1^2y_1^2x_2y_2$

$\pm y_1)^2$.

$y_2 \neq 0$;

.E.D.

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two." ... meaning:
Any addition formula
for a Weierstrass curve E
in projective coordinates
must have exceptional cases
in $E(\overline{k}) \times E(\overline{k})$, where
$\overline{k}$ = algebraic closure of k.

Edwards addition formula has
exceptional cases for $E(\overline{k})$
... but not for $E(k)$.
We do computations in $E(k)$.

Summary: Assume k field;
$2 \neq 0$ in k; non-square $d \in$
Then $\{(x, y) \in k \times k :$

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

is a commutative group wi
$(x_1, y_1) + (x_2, y_2) = (x_3, y$
defined by Edwards additio

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Terminology: "Edwards cu
allow arbitrary $d \in k^*$; $d =$
are "original Edwards curve
non-square d are "complet

1995 Bosma–Lenstra theorem:
"The smallest cardinality of a
complete system of addition laws
on E equals two." ... meaning:
Any addition formula
for a Weierstrass curve E
in projective coordinates
must have exceptional cases
in $E(\overline{k}) \times E(\overline{k})$, where
$\overline{k}$ = algebraic closure of k.

Edwards addition formula has
exceptional cases for $E(\overline{k})$
... but not for $E(k)$.
We do computations in $E(k)$.

Summary: Assume k field;
$2 \neq 0$ in k; non-square $d \in k$.
Then $\{(x, y) \in k \times k :$
$$x^2 + y^2 = 1 + dx^2y^2\}$$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Terminology: "Edwards curves"
allow arbitrary $d \in k^*$; $d = c^4$
are "original Edwards curves";
non-square d are "complete."

Bosma–Lenstra theorem:
mallest cardinality of a
ete system of addition laws
quals two." ... meaning:
ddition formula
Weierstrass curve E
ective coordinates
ave exceptional cases
$) \times E(\overline{k})$, where
gebraic closure of k.

ds addition formula has
onal cases for $E(\overline{k})$
t not for $E(k)$.
computations in $E(k)$.

Summary: Assume k field;
$2 \neq 0$ in k; non-square $d \in k$.
Then $\{(x, y) \in k \times k :$
$$x^2 + y^2 = 1 + dx^2y^2\}$$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Terminology: "Edwards curves"
allow arbitrary $d \in k^*$; $d = c^4$
are "original Edwards curves";
non-square d are "complete."

$d = 0$:
$x^2 + y$
by $(x, y$

Gauss
$x^2 + y$
$(x, y) =$

Abel, J
cover a
but (sm
specialı
or to (

Edward
Edward
Theta

stra theorem:
rdinality of a
of addition laws
" ... meaning:
mula
curve E
rdinates
tional cases
where
sure of k.

formula has
s for $E(\overline{k})$
$E(k)$.
ions in $E(k)$.

Summary: Assume k field;
$2 \neq 0$ in k; non-square $d \in k$.
Then $\{(x, y) \in k \times k :$
$$x^2 + y^2 = 1 + dx^2y^2\}$$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Terminology: "Edwards curves"
allow arbitrary $d \in k^*$; $d = c^4$
are "original Edwards curves";
non-square d are "complete."

$d = 0$: "the cloc
$x^2 + y^2 = 1$, par
by $(x, y) = (\sin,$

Gauss parametriz
$x^2 + y^2 = 1 - x^$
$(x, y) = ($"lemn s

Abel, Jacobi "sn,
cover all elliptic
but (sn, cn) does
specialize to (sin
or to (lemn sin, l

Edwards x is sn;
Edwards y is cn/
Theta view: see

rem:
of a
on laws
aning:

es

has

k).

Summary: Assume k field;
$2 \neq 0$ in k; non-square $d \in k$.
Then $\{(x, y) \in k \times k :$
$$x^2 + y^2 = 1 + dx^2y^2\}$$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Terminology: "Edwards curves"
allow arbitrary $d \in k^*$; $d = c^4$
are "original Edwards curves";
non-square d are "complete."

$d = 0$: "the clock group."
$x^2 + y^2 = 1$, parametrized
by $(x, y) = (\sin, \cos)$.

Gauss parametrized
$x^2 + y^2 = 1 - x^2y^2$ by
$(x, y) =$ ("lemn sin", "lemn

Abel, Jacobi "sn, cn, dn"
cover all elliptic curves,
but (sn, cn) does *not*
specialize to (sin, cos)
or to (lemn sin, lemn cos).

Edwards x is sn;
Edwards y is cn/dn.
Theta view: see Edwards p

Summary: Assume k field;
$2 \neq 0$ in k; non-square $d \in k$.
Then $\{(x, y) \in k \times k :$
$$x^2 + y^2 = 1 + dx^2y^2\}$$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Terminology: "Edwards curves"
allow arbitrary $d \in k^*$; $d = c^4$
are "original Edwards curves";
non-square d are "complete."

$d = 0$: "the clock group."
$x^2 + y^2 = 1$, parametrized
by $(x, y) = (\sin, \cos)$.

Gauss parametrized
$x^2 + y^2 = 1 - x^2y^2$ by
$(x, y) =$ ("lemn sin", "lemn cos").

Abel, Jacobi "sn, cn, dn"
cover all elliptic curves,
but $(\mathrm{sn}, \mathrm{cn})$ does *not*
specialize to $(\sin, \cos)$
or to (lemn sin, lemn cos).

Edwards x is sn;
Edwards y is cn/dn.
Theta view: see Edwards paper.

ary: Assume k field;
n k; non-square $d \in k$.
$(x, y) \in k \times k :$
$x^2 + y^2 = 1 + dx^2y^2\}$
mmutative group with
$) + (x_2, y_2) = (x_3, y_3)$
by Edwards addition law:

$$\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$\frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

ology: "Edwards curves"
rbitrary $d \in k^*$; $d = c^4$
iginal Edwards curves";
uare d are "complete."

$d = 0$: "the clock group."
$x^2 + y^2 = 1$, parametrized
by $(x, y) = (\sin, \cos)$.

Gauss parametrized
$x^2 + y^2 = 1 - x^2y^2$ by
$(x, y) =$ ("lemn sin", "lemn cos").

Abel, Jacobi "sn, cn, dn"
cover all elliptic curves,
but (sn, cn) does *not*
specialize to (sin, cos)
or to (lemn sin, lemn cos).

Edwards x is sn;
Edwards y is cn/dn.
Theta view: see Edwards paper.

Every e
with a
is birat
to an E

Unique
Conven
no nee
accider
excepti

Particu
no nee
attacke
excepti
hearing

me k field;
square $d \in k$.
$: \times k$:
$= 1 + dx^2y^2\}$
e group with
$_2) = (x_3, y_3)$
rds addition law:

$$\frac{x_1y_2 + y_1x_2}{y_1y_2},$$

$$\frac{x_1x_2}{y_1y_2}.$$

dwards curves"
$\in k^*$; $d = c^4$
vards curves";
"complete."

$d = 0$: "the clock group."
$x^2 + y^2 = 1$, parametrized
by $(x, y) = (\sin, \cos)$.

Gauss parametrized
$x^2 + y^2 = 1 - x^2y^2$ by
$(x, y) = (\text{"lemn sin"}, \text{"lemn cos"})$.

Abel, Jacobi "sn, cn, dn"
cover all elliptic curves,
but (sn, cn) does *not*
specialize to (sin, cos)
or to (lemn sin, lemn cos).

Edwards x is sn;
Edwards y is cn/dn.
Theta view: see Edwards paper.

Every elliptic cur
with a point of o
is birationally equ
to an Edwards cu

Unique order-2 p
Convenient for in
no need to worry
accidentally bum
exceptional input

Particularly nice
no need to worry
attackers manufa
exceptional input
hearing case dist

k.

$y^2\}$
th
$y_3)$
on law:

rves"
c^4
es";
e."

$d = 0$: "the clock group."
$x^2 + y^2 = 1$, parametrized
by $(x, y) = (\sin, \cos)$.

Gauss parametrized
$x^2 + y^2 = 1 - x^2y^2$ by
$(x, y) = (\text{"lemn sin"}, \text{"lemn cos"})$.

Abel, Jacobi "sn, cn, dn"
cover all elliptic curves,
but (sn, cn) does *not*
specialize to (sin, cos)
or to (lemn sin, lemn cos).

Edwards x is sn;
Edwards y is cn/dn.
Theta view: see Edwards paper.

Every elliptic curve over k
with a point of order 4
is birationally equivalent
to an Edwards curve.

Unique order-2 point $\Rightarrow$ co
Convenient for implemento
no need to worry about
accidentally bumping into
exceptional inputs.

Particularly nice for crypto
no need to worry about
attackers manufacturing
exceptional inputs,
hearing case distinctions, e

$d = 0$: "the clock group."
$x^2 + y^2 = 1$, parametrized
by $(x, y) = (\sin, \cos)$.

Gauss parametrized
$x^2 + y^2 = 1 - x^2y^2$ by
$(x, y) = (\text{"lemn sin"}, \text{"lemn cos"})$.

Abel, Jacobi "sn, cn, dn"
cover all elliptic curves,
but (sn, cn) does *not*
specialize to (sin, cos)
or to (lemn sin, lemn cos).

Edwards x is sn;
Edwards y is cn/dn.
Theta view: see Edwards paper.

Every elliptic curve over k
with a point of order 4
is birationally equivalent
to an Edwards curve.

Unique order-2 point $\Rightarrow$ complete.
Convenient for implementors:
no need to worry about
accidentally bumping into
exceptional inputs.

Particularly nice for cryptography:
no need to worry about
attackers manufacturing
exceptional inputs,
hearing case distinctions, etc.

“the clock group.”
$^2 = 1$, parametrized
$y) = (\sin, \cos)$.

parametrized
$^2 = 1 - x^2y^2$ by
$= (\text{“lemn sin”}, \text{“lemn cos”})$.

Jacobi “sn, cn, dn”
ll elliptic curves,
n, cn) does *not*
ize to (sin, cos)
lemn sin, lemn cos).

ds x is sn;
ds y is cn/dn.
view: see Edwards paper.

Every elliptic curve over k
with a point of order 4
is birationally equivalent
to an Edwards curve.

Unique order-2 point $\Rightarrow$ complete.
Convenient for implementors:
no need to worry about
accidentally bumping into
exceptional inputs.

Particularly nice for cryptography:
no need to worry about
attackers manufacturing
exceptional inputs,
hearing case distinctions, etc.

What a
withou

What a
over bi

Contin
For *eve*
find co
with be

Comple
even if

k group."
ametrized
cos).

zed
$^2y^2$ by
sin", "lemn cos").

, cn, dn"
curves,
not
, cos)
emn cos).

'dn.
Edwards paper.

Every elliptic curve over k
with a point of order 4
is birationally equivalent
to an Edwards curve.

Unique order-2 point $\Rightarrow$ complete.
Convenient for implementors:
no need to worry about
accidentally bumping into
exceptional inputs.

Particularly nice for cryptography:
no need to worry about
attackers manufacturing
exceptional inputs,
hearing case distinctions, etc.

What about ellip
without points o

What about ellip
over binary fields

Continuing proje
For *every* elliptic
find complete ad
with best possibl

Complete laws ar
even if slower tha

n cos").

paper.

Every elliptic curve over k
with a point of order 4
is birationally equivalent
to an Edwards curve.

Unique order-2 point $\Rightarrow$ complete.
Convenient for implementors:
no need to worry about
accidentally bumping into
exceptional inputs.

Particularly nice for cryptography:
no need to worry about
attackers manufacturing
exceptional inputs,
hearing case distinctions, etc.

What about elliptic curves
without points of order 4?

What about elliptic curves
over binary fields?

Continuing project (B.–L.)
For *every* elliptic curve E,
find complete addition law
with best possible speeds.

Complete laws are useful
even if slower than Edward

Every elliptic curve over k
with a point of order 4
is birationally equivalent
to an Edwards curve.

Unique order-2 point $\Rightarrow$ complete.
Convenient for implementors:
no need to worry about
accidentally bumping into
exceptional inputs.

Particularly nice for cryptography:
no need to worry about
attackers manufacturing
exceptional inputs,
hearing case distinctions, etc.

What about elliptic curves
without points of order 4?

What about elliptic curves
over binary fields?

Continuing project (B.–L.):
For *every* elliptic curve E,
find complete addition law for E
with best possible speeds.

Complete laws are useful
even if slower than Edwards!

elliptic curve over k
point of order 4
ionally equivalent
Edwards curve.

e order-2 point $\Rightarrow$ complete.
nient for implementors:
d to worry about
ntally bumping into
onal inputs.

ılarly nice for cryptography:
d to worry about
ers manufacturing
onal inputs,
g case distinctions, etc.

What about elliptic curves
without points of order 4?

What about elliptic curves
over binary fields?

Continuing project (B.–L.):
For *every* elliptic curve E,
find complete addition law for E
with best possible speeds.

Complete laws are useful
even if slower than Edwards!

2008 B
"twiste
$ax^2 +$
cover a

Almost
brings
to large

2008 B
every e
where
is (1 or
to a tw

ve over k
rder 4
uivalent
urve.

oint $\Rightarrow$ complete.
mplementors:
about
ping into
ts.

for cryptography:
about
acturing
ts,
inctions, etc.

What about elliptic curves
without points of order 4?

What about elliptic curves
over binary fields?

Continuing project (B.–L.):
For *every* elliptic curve E,
find complete addition law for E
with best possible speeds.

Complete laws are useful
even if slower than Edwards!

2008 B.–Birkner-
"twisted Edwards
$ax^2 + y^2 = 1 +$
cover all Montgo

Almost as fast as
brings Edwards s
to larger class of

2008 B.–B.–Joye
every elliptic curv
where 4 divides
is (1 or 2)-isogen
to a twisted Edw

omplete.

ors:

graphy:

tc.

What about elliptic curves
without points of order 4?

What about elliptic curves
over binary fields?

Continuing project (B.–L.):
For *every* elliptic curve E,
find complete addition law for E
with best possible speeds.

Complete laws are useful
even if slower than Edwards!

2008 B.–Birkner–L.–Peters
"twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$
cover all Montgomery curv

Almost as fast as $a = 1$;
brings Edwards speed
to larger class of curves.

2008 B.–B.–Joye–L.–P.:
every elliptic curve over $\mathbf{F}_p$
where 4 divides group orde
is (1 or 2)-isogenous
to a twisted Edwards curve

What about elliptic curves
without points of order 4?

What about elliptic curves
over binary fields?

Continuing project (B.–L.):
For *every* elliptic curve E,
find complete addition law for E
with best possible speeds.

Complete laws are useful
even if slower than Edwards!

2008 B.–Birkner–L.–Peters:
"twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$
cover all Montgomery curves.

Almost as fast as $a = 1$;
brings Edwards speed
to larger class of curves.

2008 B.–B.–Joye–L.–P.:
every elliptic curve over $\mathbf{F}_p$
where 4 divides group order
is (1 or 2)-isogenous
to a twisted Edwards curve.

about elliptic curves
t points of order 4?

about elliptic curves
nary fields?

uing project (B.–L.):
ery elliptic curve E,
mplete addition law for E
est possible speeds.

ete laws are useful
slower than Edwards!

2008 B.–Birkner–L.–Peters:
"twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$
cover all Montgomery curves.

Almost as fast as $a = 1$;
brings Edwards speed
to larger class of curves.

2008 B.–B.–Joye–L.–P.:
every elliptic curve over $\mathbf{F}_p$
where 4 divides group order
is (1 or 2)-isogenous
to a twisted Edwards curve.

Statisti
$\approx$ num

Curves
orig
compl
Ed
twist
4**Z**
all

Differe

Bad ne
comple
$\equiv$ com

tic curves
f order 4?

tic curves
?

ct (B.–L.):
curve E,
dition law for E
e speeds.

re useful
an Edwards!

2008 B.–Birkner–L.–Peters:
"twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$
cover all Montgomery curves.

Almost as fast as $a = 1$;
brings Edwards speed
to larger class of curves.

2008 B.–B.–Joye–L.–P.:
every elliptic curve over $\mathbf{F}_p$
where 4 divides group order
is (1 or 2)-isogenous
to a twisted Edwards curve.

Statistics for ma
$\approx$ number of pai

Curves	total	odd
orig	$\frac{1}{24}p$	0
compl	$\frac{1}{2}p$	0
Ed	$\frac{2}{3}p$	0
twist	$\frac{5}{6}p$	0
$4\mathbf{Z}$	$\frac{5}{6}p$	0
all	$2p$	$\frac{2}{3}p$

Different statistic

Bad news:
complete twisted
$\equiv$ complete Edw

:

for E

s!

2008 B.–Birkner–L.–Peters:
"twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$
cover all Montgomery curves.

Almost as fast as $a = 1$;
brings Edwards speed
to larger class of curves.

2008 B.–B.–Joye–L.–P.:
every elliptic curve over $\mathbf{F}_p$
where 4 divides group order
is (1 or 2)-isogenous
to a twisted Edwards curve.

Statistics for many $p \in 1 +$
$\approx$ number of pairs $(j(E), \pm$

Curves	total	odd	2odd	4odd
orig	$\frac{1}{24}p$	0	0	0
compl	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$
Ed	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$
twist	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$
$4\mathbf{Z}$	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$
all	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$

Different statistics for $3 +$

Bad news:
complete twisted Edwards
$\equiv$ complete Edwards!

2008 B.–Birkner–L.–Peters:
"twisted Edwards curves"
$ax^2 + y^2 = 1 + dx^2y^2$
cover all Montgomery curves.

Almost as fast as $a = 1$;
brings Edwards speed
to larger class of curves.

2008 B.–B.–Joye–L.–P.:
every elliptic curve over $\mathbf{F}_p$
where 4 divides group order
is (1 or 2)-isogenous
to a twisted Edwards curve.

Statistics for many $p \in 1 + 4\mathbf{Z}$,
$\approx$ number of pairs $(j(E), \#E)$:

Curves	total	odd	2odd	4odd	8odd
orig	$\frac{1}{24}p$	0	0	0	0
compl	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$	$\frac{1}{8}p$
Ed	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$	$\frac{3}{16}p$
twist	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
$4\mathbf{Z}$	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
all	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

Different statistics for $3 + 4\mathbf{Z}$.

Bad news:
complete twisted Edwards
$\equiv$ complete Edwards!

.–Birkner–L.–Peters:
ed Edwards curves"
$y^2 = 1 + dx^2y^2$
ll Montgomery curves.

as fast as $a = 1$;
Edwards speed
er class of curves.

.–B.–Joye–L.–P.:
lliptic curve over $\mathbf{F}_p$
4 divides group order
r 2)-isogenous
wisted Edwards curve.

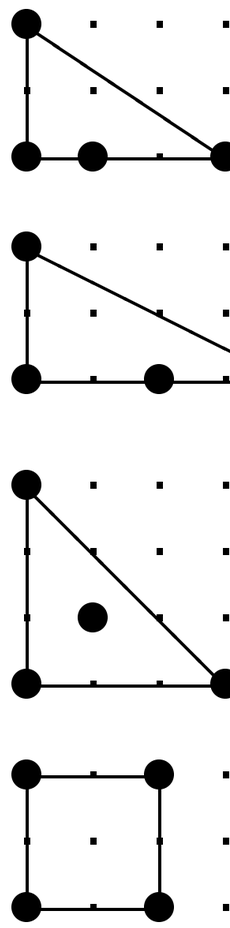
Statistics for many $p \in 1 + 4\mathbf{Z}$,
$\approx$ number of pairs $(j(E), \#E)$:

Curves	total	odd	2odd	4odd	8odd
orig	$\frac{1}{24}p$	0	0	0	0
compl	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$	$\frac{1}{8}p$
Ed	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$	$\frac{3}{16}p$
twist	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
$4\mathbf{Z}$	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
all	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

Different statistics for $3 + 4\mathbf{Z}$.

Bad news:
complete twisted Edwards
$\equiv$ complete Edwards!

Some M



1893 B
numbe

2000 P
classifi

–L.–Peters:
s curves"
dx^2y^2
omery curves.

s $a = 1$;
peed
curves.

–L.–P.:
ve over $\mathbf{F}_p$
group order
nous
vards curve.

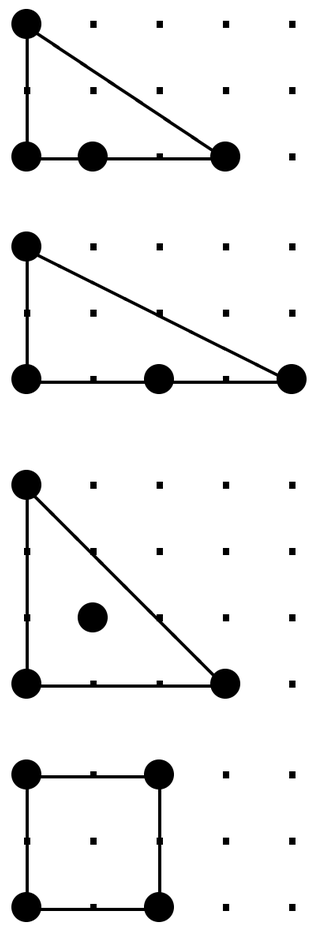
Statistics for many $p \in 1 + 4\mathbf{Z}$,
$\approx$ number of pairs $(j(E), \#E)$:

Curves	total	odd	2odd	4odd	8odd
orig	$\frac{1}{24}p$	0	0	0	0
compl	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$	$\frac{1}{8}p$
Ed	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$	$\frac{3}{16}p$
twist	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
$4\mathbf{Z}$	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
all	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

Different statistics for $3 + 4\mathbf{Z}$.

Bad news:
complete twisted Edwards
$\equiv$ complete Edwards!

Some Newton po



Short W
Jacobi
Hessian
Edward

1893 Baker: gen
number of interio

2000 Poonen–Ro
classified genus-1

es.

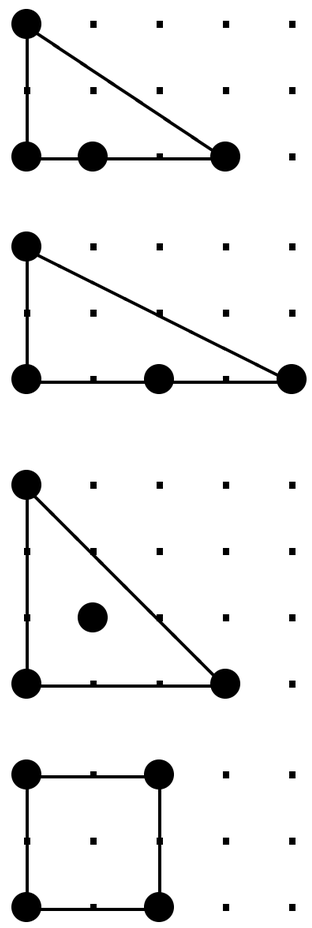
Statistics for many $p \in 1 + 4\mathbf{Z}$,
$\approx$ number of pairs $(j(E), \#E)$:

Curves	total	odd	2odd	4odd	8odd
orig	$\frac{1}{24}p$	0	0	0	0
compl	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$	$\frac{1}{8}p$
Ed	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$	$\frac{3}{16}p$
twist	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
$4\mathbf{Z}$	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
all	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

Different statistics for $3 + 4\mathbf{Z}$.

Bad news:
complete twisted Edwards
$\equiv$ complete Edwards!

Some Newton polygons



Short Weierstrass

Jacobi quartic

Hessian

Edwards

1893 Baker: genus is gene
number of interior points.

2000 Poonen–Rodriguez-V
classified genus-1 polygons

Statistics for many $p \in 1 + 4\mathbf{Z}$,
$\approx$ number of pairs $(j(E), \#E)$:

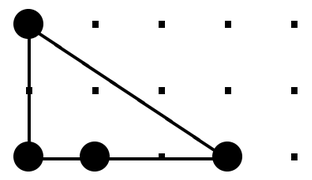
Curves	total	odd	2odd	4odd	8odd
orig	$\frac{1}{24}p$	0	0	0	0
compl	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$	$\frac{1}{8}p$
Ed	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$	$\frac{3}{16}p$
twist	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
$4\mathbf{Z}$	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
all	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

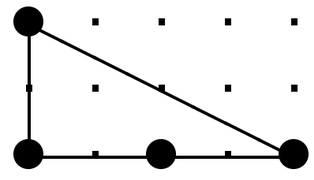
Different statistics for $3 + 4\mathbf{Z}$.

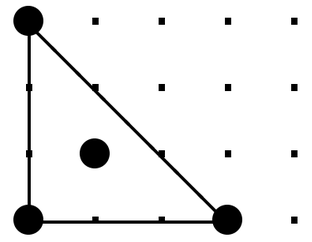
Bad news:

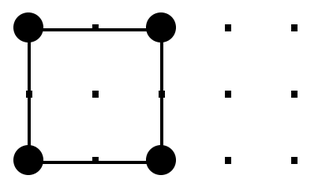
complete twisted Edwards
$\equiv$ complete Edwards!

Some Newton polygons


Short Weierstrass


Jacobi quartic


Hessian


Edwards

1893 Baker: genus is generically number of interior points.

2000 Poonen–Rodriguez-Villegas classified genus-1 polygons.

ics for many $p \in 1 + 4\mathbf{Z}$,
ber of pairs $(j(E), \#E)$:

s	total	odd	2odd	4odd	8odd
	$\frac{1}{24}p$	0	0	0	0
	$\frac{1}{2}p$	0	0	$\frac{1}{4}p$	$\frac{1}{8}p$
	$\frac{2}{3}p$	0	0	$\frac{1}{4}p$	$\frac{3}{16}p$
	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
	$\frac{5}{6}p$	0	0	$\frac{5}{12}p$	$\frac{3}{16}p$
	$2p$	$\frac{2}{3}p$	$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

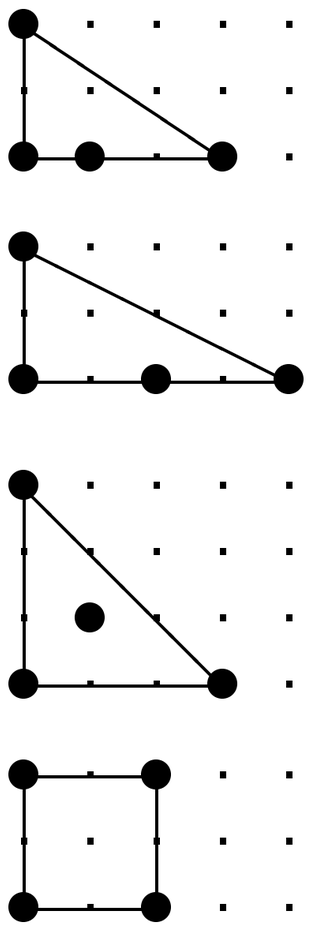
nt statistics for $3 + 4\mathbf{Z}$.

ews:

ete twisted Edwards

plete Edwards!

Some Newton polygons



Short Weierstrass

Jacobi quartic

Hessian

Edwards

1893 Baker: genus is generically number of interior points.

2000 Poonen–Rodriguez-Villegas classified genus-1 polygons.

How to

Design

quadra

Design

$x \leftrightarrow y$

Curve s

$d_{11}xy$

$d_{21}xy($

ny $p \in 1 + 4\mathbf{Z}$,
rs $(j(E), \#E)$:

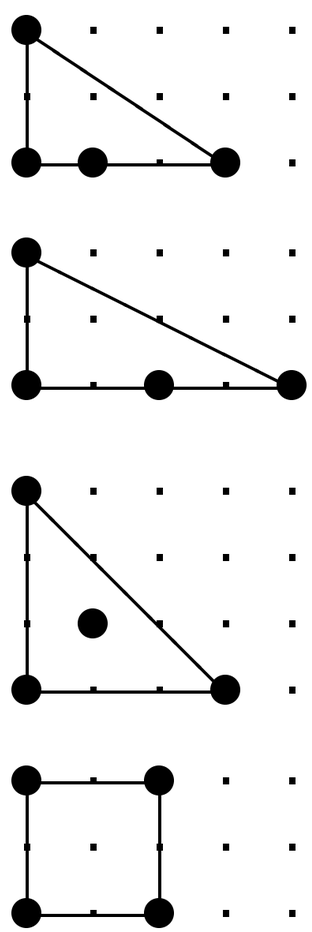
2odd	4odd	8odd
0	0	0
0	$\frac{1}{4}p$	$\frac{1}{8}p$
0	$\frac{1}{4}p$	$\frac{3}{16}p$
0	$\frac{5}{12}p$	$\frac{3}{16}p$
0	$\frac{5}{12}p$	$\frac{3}{16}p$
$\frac{1}{2}p$	$\frac{5}{12}p$	$\frac{3}{16}p$

cs for $3 + 4\mathbf{Z}$.

Edwards

ards!

Some Newton polygons



Short Weierstrass

Jacobi quartic

Hessian

Edwards

1893 Baker: genus is generically number of interior points.

2000 Poonen–Rodriguez-Villegas classified genus-1 polygons.

How to generaliz

Design decision:
quadratic in x ar

Design decision:
$x \leftrightarrow y$ symmetry

d_{20} d

d_{10} d

d_{00} d

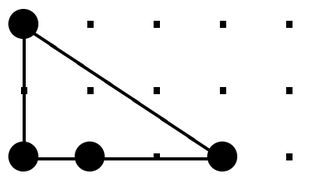
Curve shape d_{00}
$d_{11}xy + d_{20}(x^2$
$d_{21}xy(x + y) +$

$- 4\mathbf{Z}$,
$\#E)$:

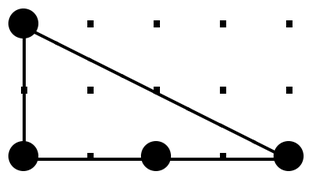
d	8odd
0	0
p	$\frac{1}{8}p$
p	$\frac{3}{16}p$
p	$\frac{3}{16}p$
p	$\frac{3}{16}p$

$4\mathbf{Z}$.

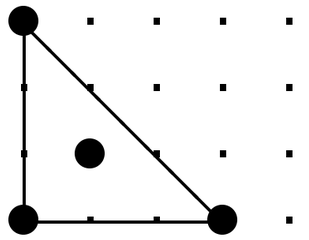
Some Newton polygons



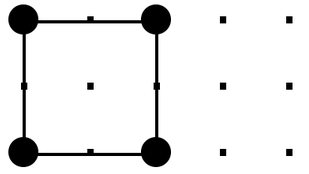
Short Weierstrass



Jacobi quartic



Hessian



Edwards

1893 Baker: genus is generically number of interior points.

2000 Poonen–Rodriguez-Villegas classified genus-1 polygons.

How to generalize Edwards

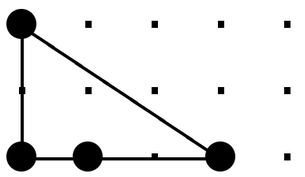
Design decision: want quadratic in x and in y.

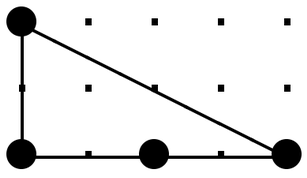
Design decision: want $x \leftrightarrow y$ symmetry.

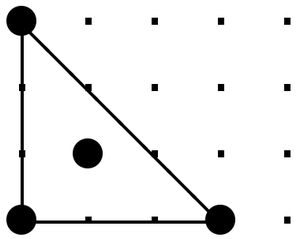
$$\begin{matrix} d_{20} & d_{21} & d_{22} \\ d_{10} & d_{11} & d_{21} \\ d_{00} & d_{10} & d_{20} \end{matrix}$$

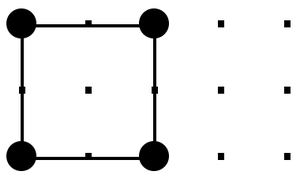
Curve shape $d_{00} + d_{10}(x +$
$d_{11}xy + d_{20}(x^2 + y^2) +$
$d_{21}xy(x + y) + d_{22}x^2y^2 =$

Some Newton polygons


Short Weierstrass


Jacobi quartic


Hessian


Edwards

1893 Baker: genus is generically number of interior points.

2000 Poonen–Rodriguez-Villegas classified genus-1 polygons.

How to generalize Edwards?

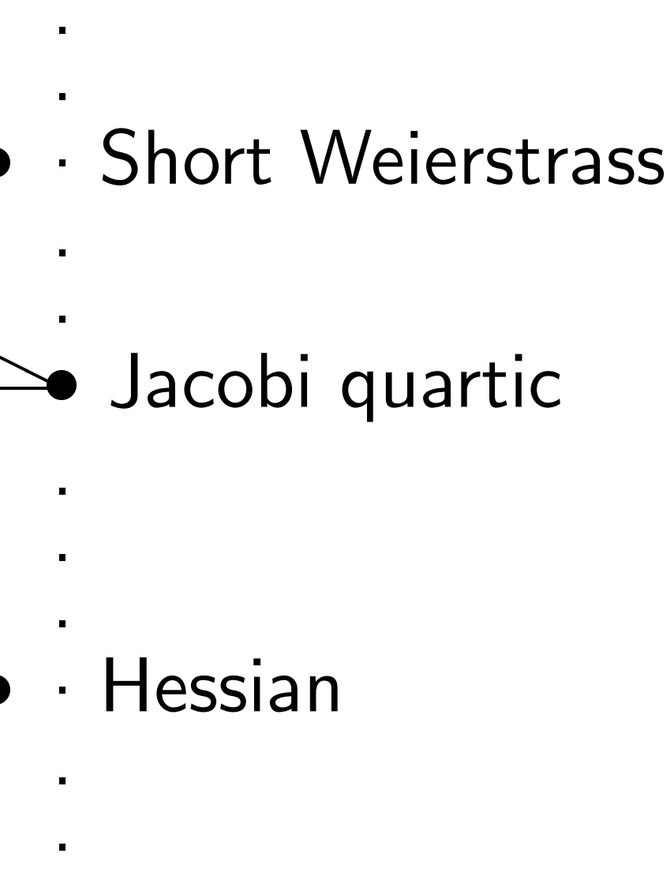
Design decision: want quadratic in x and in y.

Design decision: want $x \leftrightarrow y$ symmetry.

$$\begin{matrix} d_{20} & d_{21} & d_{22} \\ d_{10} & d_{11} & d_{21} \\ d_{00} & d_{10} & d_{20} \end{matrix}$$

Curve shape $d_{00} + d_{10}(x + y) + d_{11}xy + d_{20}(x^2 + y^2) + d_{21}xy(x + y) + d_{22}x^2y^2 = 0$.

Newton polygons



Baker: genus is generically
r of interior points.

Poonen–Rodriguez-Villegas
ed genus-1 polygons.

How to generalize Edwards?

Design decision: want
quadratic in x and in y.

Design decision: want
$x \leftrightarrow y$ symmetry.

$$\begin{matrix} d_{20} & d_{21} & d_{22} \\ d_{10} & d_{11} & d_{21} \\ d_{00} & d_{10} & d_{20} \end{matrix}$$

Curve shape $d_{00} + d_{10}(x + y) +$
$d_{11}xy + d_{20}(x^2 + y^2) +$
$d_{21}xy(x + y) + d_{22}x^2y^2 = 0.$

Suppos

Genus
interior

Homog
$d_{00}Z^3$
$d_{11}XY$
$d_{21}XY$

olygons

Weierstrass

quartic

n

ds

us is generically
or points.

odriguez-Villegas
polygons.

How to generalize Edwards?

Design decision: want
quadratic in x and in y.

Design decision: want
$x \leftrightarrow y$ symmetry.

$$d_{20} \quad d_{21} \quad d_{22}$$

$$d_{10} \quad d_{11} \quad d_{21}$$

$$d_{00} \quad d_{10} \quad d_{20}$$

Curve shape $d_{00} + d_{10}(x + y) +$
$d_{11}xy + d_{20}(x^2 + y^2) +$
$d_{21}xy(x + y) + d_{22}x^2y^2 = 0.$

Suppose that d_{22}

$$d_{20} \quad d$$

$$d_{10} \quad d$$

$$d_{00} \quad d$$

Genus $1 \Rightarrow (1, 1)$
interior point $\Rightarrow$

Homogenize:
$d_{00}Z^3 + d_{10}(X +$
$d_{11}XYZ + d_{20}(X$
$d_{21}XY(X + Y) =$

s

rically

illegas

.

How to generalize Edwards?

Design decision: want
quadratic in x and in y.

Design decision: want
$x \leftrightarrow y$ symmetry.

$$\begin{array}{ccc} d_{20} & d_{21} & d_{22} \\ \\ d_{10} & d_{11} & d_{21} \\ \\ d_{00} & d_{10} & d_{20} \end{array}$$

Curve shape $d_{00} + d_{10}(x + y) +$
$d_{11}xy + d_{20}(x^2 + y^2) +$
$d_{21}xy(x + y) + d_{22}x^2y^2 = 0.$

Suppose that $d_{22} = 0$:

$$\begin{array}{ccc} d_{20} & d_{21} & \cdot \\ \\ d_{10} & d_{11} & d_{21} \\ \\ d_{00} & d_{10} & d_{20} \end{array}$$

Genus 1 $\Rightarrow (1, 1)$ is an
interior point $\Rightarrow d_{21} \neq 0$.

Homogenize:
$d_{00}Z^3 + d_{10}(X + Y)Z^2 +$
$d_{11}XYZ + d_{20}(X^2 + Y^2)Z$
$d_{21}XY(X + Y) = 0.$

How to generalize Edwards?

Design decision: want
quadratic in x and in y.

Design decision: want
$x \leftrightarrow y$ symmetry.

$$\begin{array}{ccc} d_{20} & d_{21} & d_{22} \\ \\ d_{10} & d_{11} & d_{21} \\ \\ d_{00} & d_{10} & d_{20} \end{array}$$

Curve shape $d_{00} + d_{10}(x + y) +$
$d_{11}xy + d_{20}(x^2 + y^2) +$
$d_{21}xy(x + y) + d_{22}x^2y^2 = 0.$

Suppose that $d_{22} = 0$:

$$\begin{array}{ccc} d_{20} & d_{21} & \cdot \\ \\ d_{10} & d_{11} & d_{21} \\ \\ d_{00} & d_{10} & d_{20} \end{array}$$

Genus 1 $\Rightarrow (1, 1)$ is an
interior point $\Rightarrow d_{21} \neq 0$.

Homogenize:
$d_{00}Z^3 + d_{10}(X + Y)Z^2 +$
$d_{11}XYZ + d_{20}(X^2 + Y^2)Z +$
$d_{21}XY(X + Y) = 0.$

o generalize Edwards?

decision: want
tic in x and in y.

decision: want
symmetry.

$$d_{20} \quad d_{21} \quad d_{22}$$

$$d_{10} \quad d_{11} \quad d_{21}$$

$$d_{00} \quad d_{10} \quad d_{20}$$

shape $d_{00} + d_{10}(x + y) +$
$+ d_{20}(x^2 + y^2) +$
$x + y) + d_{22}x^2y^2 = 0.$

Suppose that $d_{22} = 0$:

$$d_{20} \quad d_{21} \quad .$$

$$d_{10} \quad d_{11} \quad d_{21}$$

$$d_{00} \quad d_{10} \quad d_{20}$$

Genus $1 \Rightarrow (1, 1)$ is an
interior point $\Rightarrow d_{21} \neq 0$.

Homogenize:
$d_{00}Z^3 + d_{10}(X + Y)Z^2 +$
$d_{11}XYZ + d_{20}(X^2 + Y^2)Z +$
$d_{21}XY(X + Y) = 0.$

Points
with d_2
$(1 : 0 :$

Study
$y = Y/$
in hom
$d_{00}z^3 +$
$d_{11}yz +$
$d_{21}y(1$

Nonzer
so $(1 :$
Additio
(unless

e Edwards?

want

nd in y.

want

.

$$d_{21} \quad d_{22}$$

$$d_{11} \quad d_{21}$$

$$d_{10} \quad d_{20}$$

$$+ d_{10}(x+y) +$$

$$+ y^2) +$$

$$d_{22}x^2y^2 = 0.$$

Suppose that $d_{22} = 0$:

$$d_{20} \quad d_{21} \quad .$$

$$d_{10} \quad d_{11} \quad d_{21}$$

$$d_{00} \quad d_{10} \quad d_{20}$$

Genus 1 $\Rightarrow (1,1)$ is an interior point $\Rightarrow d_{21} \neq 0$.

Homogenize:
$d_{00}Z^3 + d_{10}(X+Y)Z^2 +$
$d_{11}XYZ + d_{20}(X^2+Y^2)Z +$
$d_{21}XY(X+Y) = 0.$

Points at ∞ are
with $d_{21}XY(X+$
$(1:0:0), (0:1$

Study $(1:0:0)$
$y = Y/X$, $z = Z$
in homogeneous
$d_{00}z^3 + d_{10}(1+$
$d_{11}yz + d_{20}(1+$
$d_{21}y(1+y) = 0.$

Nonzero coefficie
so $(1:0:0)$ is n
Addition law can
(unless k is tiny)

s?

$+ y) +$

$= 0.$

Suppose that $d_{22} = 0$:

$$\begin{array}{ccc} d_{20} & d_{21} & \cdot \\ d_{10} & d_{11} & d_{21} \\ d_{00} & d_{10} & d_{20} \end{array}$$

Genus 1 $\Rightarrow (1,1)$ is an interior point $\Rightarrow d_{21} \neq 0$.

Homogenize:
$d_{00}Z^3 + d_{10}(X+Y)Z^2 +$
$d_{11}XYZ + d_{20}(X^2+Y^2)Z +$
$d_{21}XY(X+Y) = 0.$

Points at ∞ are $(X:Y:0$
with $d_{21}XY(X+Y) = 0$:
$(1:0:0)$, $(0:1:0)$, $(1:-$

Study $(1:0:0)$ by setting
$y = Y/X$, $z = Z/X$
in homogeneous curve equa
$d_{00}z^3 + d_{10}(1+y)z^2 +$
$d_{11}yz + d_{20}(1+y^2)z +$
$d_{21}y(1+y) = 0.$

Nonzero coefficient of y
so $(1:0:0)$ is nonsingular
Addition law cannot be co
(unless k is tiny).

Suppose that $d_{22} = 0$:

$$\begin{matrix} d_{20} & d_{21} \end{matrix} .$$

$$\begin{matrix} d_{10} & d_{11} & d_{21} \end{matrix}$$

$$\begin{matrix} d_{00} & d_{10} & d_{20} \end{matrix}$$

Genus 1 $\Rightarrow (1,1)$ is an interior point $\Rightarrow d_{21} \neq 0$.

Homogenize:
$d_{00}Z^3 + d_{10}(X+Y)Z^2 +$
$d_{11}XYZ + d_{20}(X^2+Y^2)Z +$
$d_{21}XY(X+Y) = 0.$

Points at ∞ are $(X:Y:0)$
with $d_{21}XY(X+Y) = 0$: i.e.,
$(1:0:0)$, $(0:1:0)$, $(1:-1:0)$.

Study $(1:0:0)$ by setting
$y = Y/X$, $z = Z/X$
in homogeneous curve equation:
$d_{00}z^3 + d_{10}(1+y)z^2 +$
$d_{11}yz + d_{20}(1+y^2)z +$
$d_{21}y(1+y) = 0.$

Nonzero coefficient of y
so $(1:0:0)$ is nonsingular.
Addition law cannot be complete
(unless k is tiny).

se that $d_{22} = 0$:

$$d_{20} \quad d_{21} \qquad .$$

$$d_{10} \quad d_{11} \quad d_{21}$$

$$d_{00} \quad d_{10} \quad d_{20}$$

$1 \Rightarrow (1,1)$ is an
r point $\Rightarrow d_{21} \neq 0$.

genize:

$+ d_{10}(X+Y)Z^2 +$
$Z + d_{20}(X^2+Y^2)Z +$
$(X+Y) = 0.$

Points at ∞ are $(X : Y : 0)$
with $d_{21}XY(X+Y) = 0$: i.e.,
$(1:0:0)$, $(0:1:0)$, $(1:-1:0)$.

Study $(1:0:0)$ by setting
$y = Y/X$, $z = Z/X$
in homogeneous curve equation:
$d_{00}z^3 + d_{10}(1+y)z^2 +$
$d_{11}yz + d_{20}(1+y^2)z +$
$d_{21}y(1+y) = 0.$

Nonzero coefficient of y
so $(1:0:0)$ is nonsingular.
Addition law cannot be complete
(unless k is tiny).

So we

Points

with d_2

$(1:0:$

Study

$d_{00}z^4 -$

$d_{11}yz^2$

$d_{21}y(1$

Coeffic

so $(1:$

$_2 = 0$:

$_{21}$.

$_{11}$ d_{21}

$_{10}$ d_{20}

) is an

$d_{21} \neq 0$.

$+Y)Z^2 +$

$X^2 + Y^2)Z +$

$= 0$.

Points at ∞ are $(X : Y : 0)$
with $d_{21}XY(X + Y) = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$, $(1 : -1 : 0)$.

Study $(1 : 0 : 0)$ by setting
$y = Y/X$, $z = Z/X$
in homogeneous curve equation:
$d_{00}z^3 + d_{10}(1 + y)z^2 +$
$d_{11}yz + d_{20}(1 + y^2)z +$
$d_{21}y(1 + y) = 0$.

Nonzero coefficient of y
so $(1 : 0 : 0)$ is nonsingular.
Addition law cannot be complete
(unless k is tiny).

So we require d_{2}

Points at ∞ are
with $d_{22}X^2Y^2 =$
$(1 : 0 : 0)$, $(0 : 1$

Study $(1 : 0 : 0)$
$d_{00}z^4 + d_{10}(1 +$
$d_{11}yz^2 + d_{20}(1 +$
$d_{21}y(1 + y)z + d$

Coefficients of 1,
so $(1 : 0 : 0)$ is si

Points at ∞ are $(X : Y : 0)$
with $d_{21}XY(X+Y) = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$, $(1 : -1 : 0)$.

Study $(1 : 0 : 0)$ by setting
$y = Y/X$, $z = Z/X$
in homogeneous curve equation:
$d_{00}z^3 + d_{10}(1+y)z^2 +$
$d_{11}yz + d_{20}(1+y^2)z +$
$d_{21}y(1+y) = 0.$

Nonzero coefficient of y
so $(1 : 0 : 0)$ is nonsingular.
Addition law cannot be complete
(unless k is tiny).

So we require $d_{22} \neq 0$.

Points at ∞ are $(X : Y : 0$
with $d_{22}X^2Y^2 = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$.

Study $(1 : 0 : 0)$ again:
$d_{00}z^4 + d_{10}(1+y)z^3 +$
$d_{11}yz^2 + d_{20}(1+y^2)z^2 +$
$d_{21}y(1+y)z + d_{22}y^2 = 0.$

Coefficients of $1, y, z$ are 0
so $(1 : 0 : 0)$ is singular.

Points at ∞ are $(X : Y : 0)$
with $d_{21}XY(X+Y) = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$, $(1 : -1 : 0)$.

Study $(1 : 0 : 0)$ by setting
$y = Y/X$, $z = Z/X$
in homogeneous curve equation:
$d_{00}z^3 + d_{10}(1+y)z^2 +$
$d_{11}yz + d_{20}(1+y^2)z +$
$d_{21}y(1+y) = 0.$

Nonzero coefficient of y
so $(1 : 0 : 0)$ is nonsingular.
Addition law cannot be complete
(unless k is tiny).

So we require $d_{22} \neq 0$.

Points at ∞ are $(X : Y : 0)$
with $d_{22}X^2Y^2 = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$.

Study $(1 : 0 : 0)$ again:
$d_{00}z^4 + d_{10}(1+y)z^3 +$
$d_{11}yz^2 + d_{20}(1+y^2)z^2 +$
$d_{21}y(1+y)z + d_{22}y^2 = 0.$

Coefficients of $1, y, z$ are 0
so $(1 : 0 : 0)$ is singular.

at ∞ are $(X : Y : 0)$

$_{21}XY(X+Y) = 0$: i.e.,

$0)$, $(0 : 1 : 0)$, $(1 : -1 : 0)$.

$(1 : 0 : 0)$ by setting

$/X$, $z = Z/X$

ogeneous curve equation:

$+ d_{10}(1+y)z^2 +$

$+ d_{20}(1+y^2)z +$

$+ y) = 0.$

ro coefficient of y

$0 : 0)$ is nonsingular.

on law cannot be complete

k is tiny).

So we require $d_{22} \neq 0$.

Points at ∞ are $(X : Y : 0)$
with $d_{22}X^2Y^2 = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$.

Study $(1 : 0 : 0)$ again:
$d_{00}z^4 + d_{10}(1+y)z^3 +$
$d_{11}yz^2 + d_{20}(1+y^2)z^2 +$
$d_{21}y(1+y)z + d_{22}y^2 = 0.$

Coefficients of $1, y, z$ are 0
so $(1 : 0 : 0)$ is singular.

Put y
to blow

$d_{00}z^2$
$d_{11}uz$
$d_{21}u(1$

Substit
points
$d_{20} + d$

We req
$d_{20} + d$
to be i
Special
$1 - du$

$(X : Y : 0)$

$+ Y) = 0$: i.e.,

$: 0), (1 : -1 : 0).$

by setting

$/X$

curve equation:

$y)z^2 +$

$y^2)z +$

ent of y

onsingular.

not be complete

.

So we require $d_{22} \neq 0$.

Points at ∞ are $(X : Y : 0)$
with $d_{22}X^2Y^2 = 0$: i.e.,
$(1 : 0 : 0), (0 : 1 : 0)$.

Study $(1 : 0 : 0)$ again:
$d_{00}z^4 + d_{10}(1 + y)z^3 +$
$d_{11}yz^2 + d_{20}(1 + y^2)z^2 +$
$d_{21}y(1 + y)z + d_{22}y^2 = 0.$

Coefficients of $1, y, z$ are 0
so $(1 : 0 : 0)$ is singular.

Put $y = uz$, divi
to blow up singu

$d_{00}z^2 + d_{10}(1 +$
$d_{11}uz + d_{20}(1 +$
$d_{21}u(1 + uz) +$

Substitute $z = 0$
points above sing
$d_{20} + d_{21}u + d_{22}$

We require the q
$d_{20} + d_{21}u + d_{22}$
to be irreducible
Special case: co
$1 - du^2$ irreducib

)

i.e.,

$-1 : 0)$.

ation:

.

mplete

So we require $d_{22} \neq 0$.

Points at ∞ are $(X : Y : 0)$
with $d_{22}X^2Y^2 = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$.

Study $(1 : 0 : 0)$ again:
$d_{00}z^4 + d_{10}(1 + y)z^3 +$
$d_{11}yz^2 + d_{20}(1 + y^2)z^2 +$
$d_{21}y(1 + y)z + d_{22}y^2 = 0.$

Coefficients of $1, y, z$ are 0
so $(1 : 0 : 0)$ is singular.

Put $y = uz$, divide by z^2
to blow up singularity:

$d_{00}z^2 + d_{10}(1 + uz)z +$
$d_{11}uz + d_{20}(1 + u^2z^2) +$
$d_{21}u(1 + uz) + d_{22}u^2 = 0$

Substitute $z = 0$ to find
points above singularity:
$d_{20} + d_{21}u + d_{22}u^2 = 0.$

We require the quadratic
$d_{20} + d_{21}u + d_{22}u^2$
to be irreducible in k.
Special case: complete Edw
$1 - du^2$ irreducible in k.

So we require $d_{22} \neq 0$.

Points at ∞ are $(X : Y : 0)$
with $d_{22}X^2Y^2 = 0$: i.e.,
$(1 : 0 : 0)$, $(0 : 1 : 0)$.

Study $(1 : 0 : 0)$ again:
$d_{00}z^4 + d_{10}(1 + y)z^3 +$
$d_{11}yz^2 + d_{20}(1 + y^2)z^2 +$
$d_{21}y(1 + y)z + d_{22}y^2 = 0.$

Coefficients of $1, y, z$ are 0
so $(1 : 0 : 0)$ is singular.

Put $y = uz$, divide by z^2
to blow up singularity:

$d_{00}z^2 + d_{10}(1 + uz)z +$
$d_{11}uz + d_{20}(1 + u^2z^2) +$
$d_{21}u(1 + uz) + d_{22}u^2 = 0.$

Substitute $z = 0$ to find
points above singularity:
$d_{20} + d_{21}u + d_{22}u^2 = 0.$

We require the quadratic
$d_{20} + d_{21}u + d_{22}u^2$
to be irreducible in k.
Special case: complete Edwards,
$1 - du^2$ irreducible in k.

require $d_{22} \neq 0$.

at ∞ are $(X : Y : 0)$
$_{22}X^2Y^2 = 0$: i.e.,
$0)$, $(0 : 1 : 0)$.

$(1 : 0 : 0)$ again:
$+ d_{10}(1 + y)z^3 +$
$+ d_{20}(1 + y^2)z^2 +$
$+ y)z + d_{22}y^2 = 0.$

ients of $1, y, z$ are 0
$0 : 0)$ is singular.

Put $y = uz$, divide by z^2
to blow up singularity:

$d_{00}z^2 + d_{10}(1 + uz)z +$
$d_{11}uz + d_{20}(1 + u^2z^2) +$
$d_{21}u(1 + uz) + d_{22}u^2 = 0.$

Substitute $z = 0$ to find
points above singularity:
$d_{20} + d_{21}u + d_{22}u^2 = 0.$

We require the quadratic
$d_{20} + d_{21}u + d_{22}u^2$
to be irreducible in k.
Special case: complete Edwards,
$1 - du^2$ irreducible in k.

In part

Design
a devia
Choose
$d_{00} =$

Can va
Warnin
surprisi

$_2 \neq 0$.

$(X : Y : 0)$

0: i.e.,

$: 0)$.

again:

$y)z^3 +$

$+ y^2)z^2 +$

$d_{22}y^2 = 0.$

y, z are 0

ngular.

Put $y = uz$, divide by z^2
to blow up singularity:

$d_{00}z^2 + d_{10}(1 + uz)z +$
$d_{11}uz + d_{20}(1 + u^2z^2) +$
$d_{21}u(1 + uz) + d_{22}u^2 = 0.$

Substitute $z = 0$ to find
points above singularity:
$d_{20} + d_{21}u + d_{22}u^2 = 0.$

We require the quadratic
$d_{20} + d_{21}u + d_{22}u^2$
to be irreducible in k.
Special case: complete Edwards,
$1 - du^2$ irreducible in k.

In particular d_{20}

d_{20} —— d

d_{10} d

d_{00} d

Design decision:
a deviation from
Choose neutral e
$d_{00} = 0$; $d_{10} \neq 0$

Can vary neutral

Warning: bad ch
surprisingly exper

)

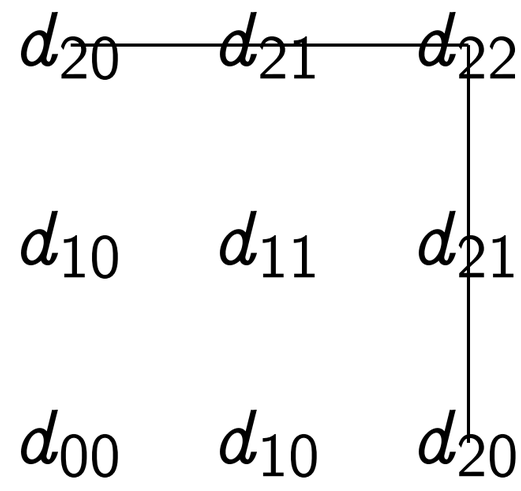
Put $y = uz$, divide by z^2
to blow up singularity:

$d_{00}z^2 + d_{10}(1 + uz)z +$
$d_{11}uz + d_{20}(1 + u^2z^2) +$
$d_{21}u(1 + uz) + d_{22}u^2 = 0.$

Substitute $z = 0$ to find
points above singularity:
$d_{20} + d_{21}u + d_{22}u^2 = 0.$

We require the quadratic
$d_{20} + d_{21}u + d_{22}u^2$
to be irreducible in k.
Special case: complete Edwards,
$1 - du^2$ irreducible in k.

In particular $d_{20} \neq 0$:



Design decision: Explore
a deviation from Edwards.
Choose neutral element (0,
$d_{00} = 0$; $d_{10} \neq 0$.

Can vary neutral element.
Warning: bad choice can p
surprisingly expensive nega

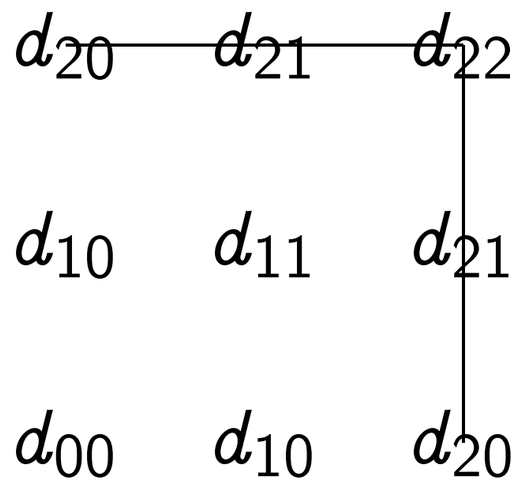
Put $y = uz$, divide by z^2
to blow up singularity:

$d_{00}z^2 + d_{10}(1 + uz)z +$
$d_{11}uz + d_{20}(1 + u^2z^2) +$
$d_{21}u(1 + uz) + d_{22}u^2 = 0.$

Substitute $z = 0$ to find
points above singularity:
$d_{20} + d_{21}u + d_{22}u^2 = 0.$

We require the quadratic
$d_{20} + d_{21}u + d_{22}u^2$
to be irreducible in k.
Special case: complete Edwards,
$1 - du^2$ irreducible in k.

In particular $d_{20} \neq 0$:



Design decision: Explore
a deviation from Edwards.
Choose neutral element $(0, 0)$.
$d_{00} = 0$; $d_{10} \neq 0$.

Can vary neutral element.
Warning: bad choice can produce
surprisingly expensive negation.

$= uz$, divide by z^2

w up singularity:

$$+ d_{10}(1+uz)z +$$
$$+ d_{20}(1+u^2z^2) +$$
$$+uz) + d_{22}u^2 = 0.$$

tute $z = 0$ to find

above singularity:

$d_{21}u + d_{22}u^2 = 0.$

quire the quadratic

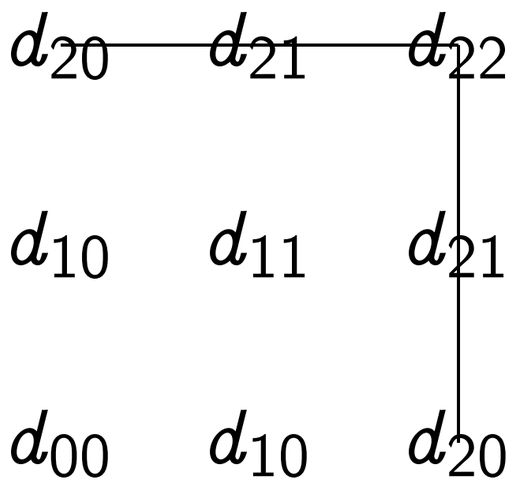
$d_{21}u + d_{22}u^2$

rreducible in k.

l case: complete Edwards,

^{2} irreducible in k.

In particular $d_{20} \neq 0$:



Design decision: Explore a deviation from Edwards.

Choose neutral element $(0, 0)$.

$d_{00} = 0$; $d_{10} \neq 0$.

Can vary neutral element.

Warning: bad choice can produce surprisingly expensive negation.

Now ha

for gen

By scal

and sca

can lim

to thre

de by z^2

larity:

$$uz)z +$$
$$u^2z^2) +$$
$$d_{22}u^2 = 0.$$

to find

gularity:

$$_2u^2 = 0.$$

uadratic

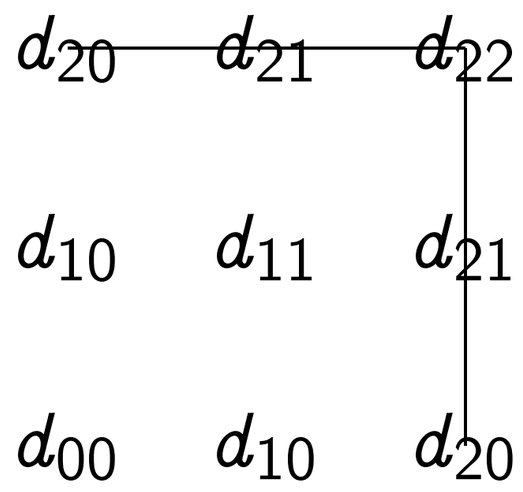
$$_2u^2$$

in k.

mplete Edwards,

ble in k.

In particular $d_{20} \neq 0$:



Design decision: Explore a deviation from Edwards.

Choose neutral element $(0, 0)$.

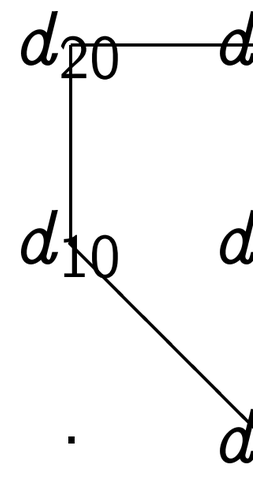
$d_{00} = 0$; $d_{10} \neq 0$.

Can vary neutral element.

Warning: bad choice can produce surprisingly expensive negation.

Now have a New

for generalized E



By scaling x, y

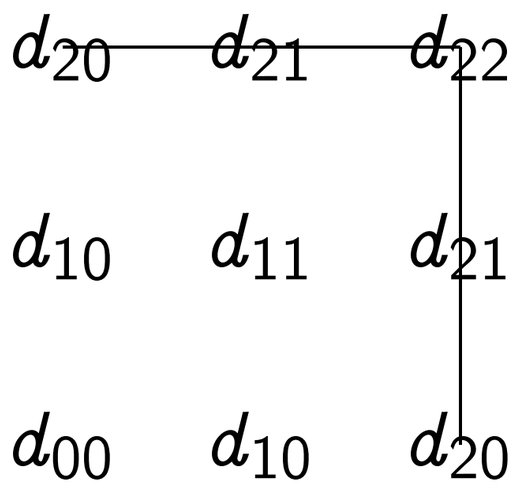
and scaling curve

can limit d_{10}, d_{11}

to three degrees

wards,

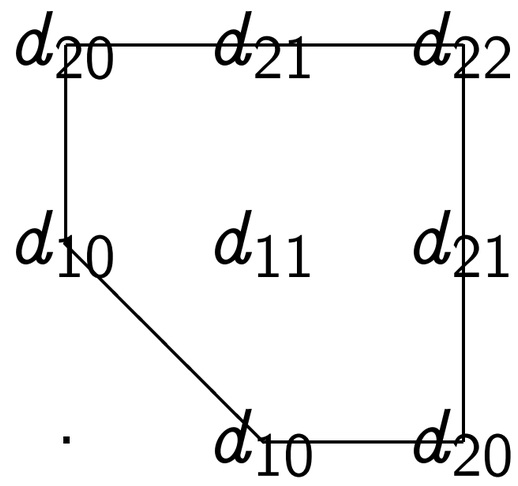
In particular $d_{20} \neq 0$:



Design decision: Explore
a deviation from Edwards.
Choose neutral element $(0, 0)$.
$d_{00} = 0$; $d_{10} \neq 0$.

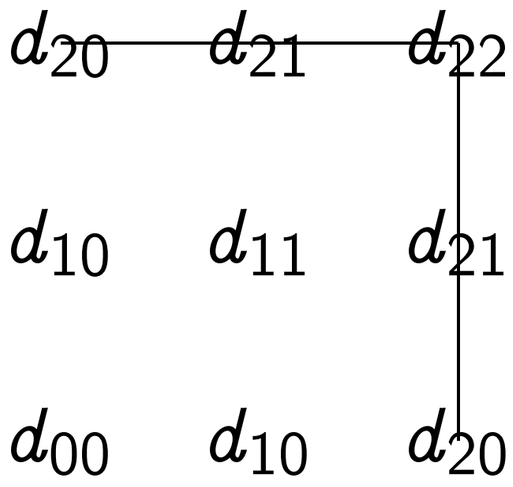
Can vary neutral element.
Warning: bad choice can produce
surprisingly expensive negation.

Now have a Newton polyg
for generalized Edwards cu



By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}$,
to three degrees of freedon

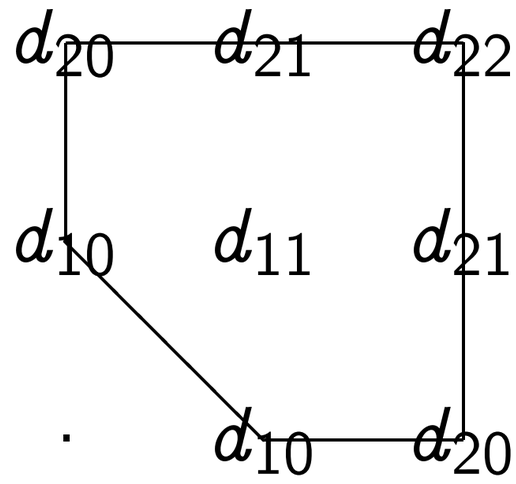
In particular $d_{20} \neq 0$:



Design decision: Explore
a deviation from Edwards.
Choose neutral element $(0, 0)$.
$d_{00} = 0$; $d_{10} \neq 0$.

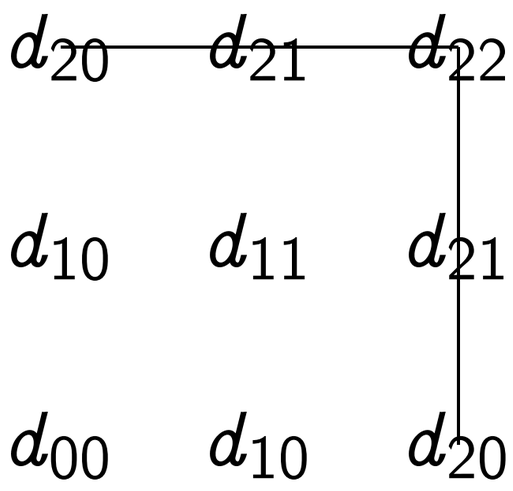
Can vary neutral element.
Warning: bad choice can produce
surprisingly expensive negation.

Now have a Newton polygon
for generalized Edwards curves:



By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
to three degrees of freedom.

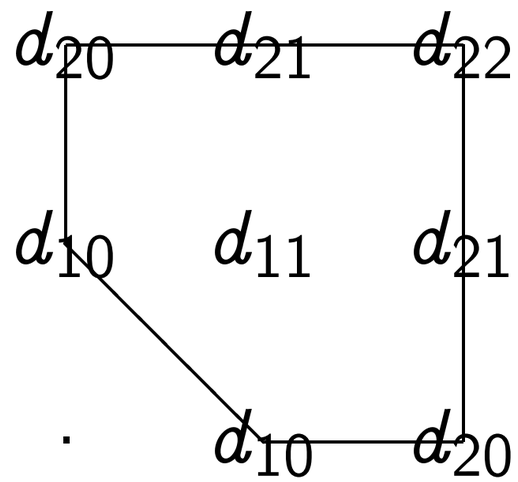
icular $d_{20} \neq 0$:



decision: Explore
tion from Edwards.
e neutral element $(0, 0)$.
0; $d_{10} \neq 0$.

ry neutral element.
g: bad choice can produce
ngly expensive negation.

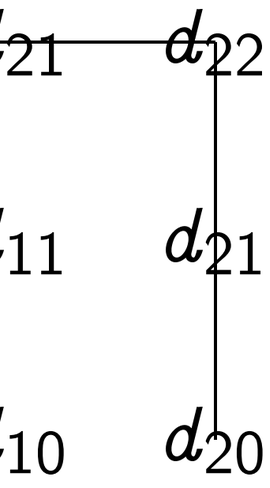
Now have a Newton polygon
for generalized Edwards curves:



By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
to three degrees of freedom.

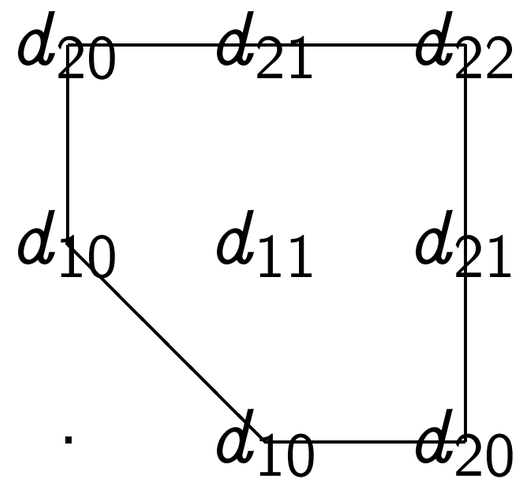
2008 B
comple
"binary
$d_1(x +$
$(x + x^$
Covers
over $\mathbf{F}_2$
Also su
especia

$\neq 0$:



Explore
Edwards.
lement $(0, 0)$.
.
element.
oice can produce
nsive negation.

Now have a Newton polygon
for generalized Edwards curves:



By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
to three degrees of freedom.

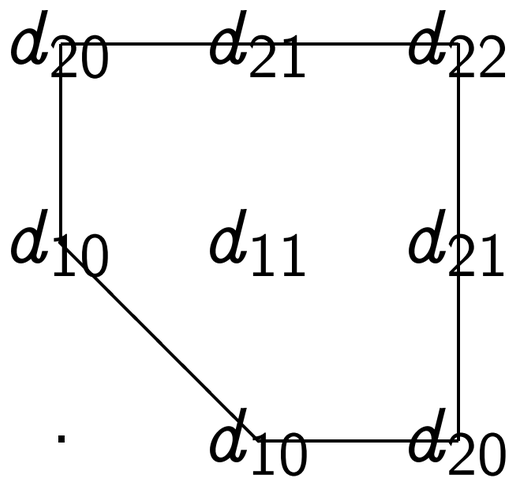
2008 B.–L.–Reza
complete additio
"binary Edwards
$d_1(x + y) + d_2(x$
$(x + x^2)(y + y^2)$
Covers all ordina
over $\mathbf{F}_{2^n}$ for $n \geq$
Also surprisingly
especially if $d_1 =$

, 0).

produce

tion.

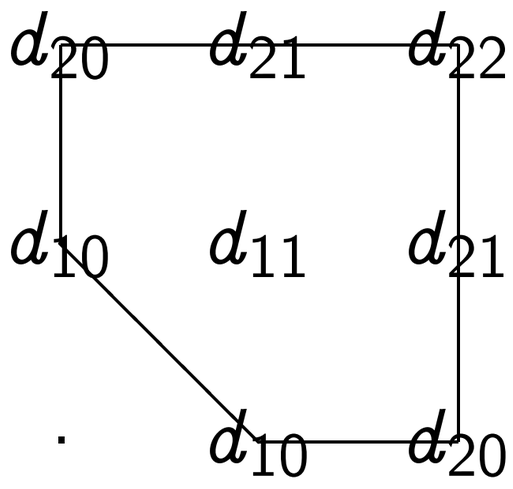
Now have a Newton polygon
for generalized Edwards curves:



By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
to three degrees of freedom.

2008 B.–L.–Rezaeian Faras
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2) =$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

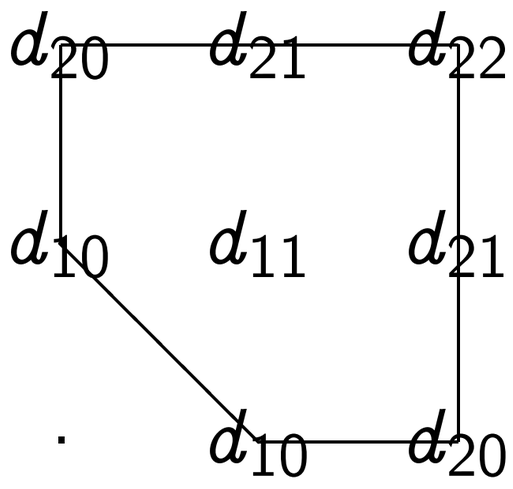
Now have a Newton polygon
for generalized Edwards curves:



By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
to three degrees of freedom.

2008 B.–L.–Rezaeian Farashahi:
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2) =$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic curves
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

Now have a Newton polygon
for generalized Edwards curves:

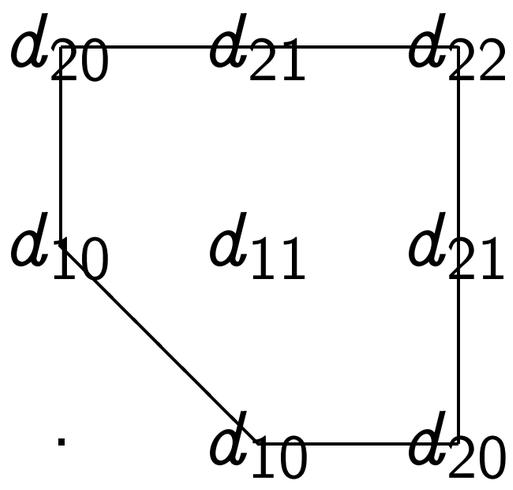


By scaling x, y
and scaling curve equation
can limit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
to three degrees of freedom.

2008 B.–L.–Rezaeian Farashahi:
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2) =$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic curves
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

2009 B.–L.:
complete addition law for
another specialization
covering all the "NIST curves"
over *non-binary* fields.

ave a Newton polygon
eralized Edwards curves:



ling x, y
aling curve equation
nit $d_{10}, d_{11}, d_{20}, d_{21}, d_{22}$
e degrees of freedom.

2008 B.–L.–Rezaeian Farashahi:
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2) =$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic curves
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

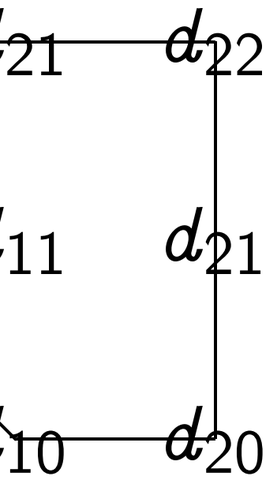
2009 B.–L.:
complete addition law for
another specialization
covering all the "NIST curves"
over *non-binary* fields.

Consid
$x^2 + y$
with d
$t = 7875$
7671

over $\mathbf{F}_p$
$2^{192} +$
Note:

Biratio
standar
$v^2 = u$
$a_6 = 04$
41

ton polygon
dwards curves:



e equation
$_1, d_{20}, d_{21}, d_{22}$
of freedom.

2008 B.–L.–Rezaeian Farashahi:
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2) =$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic curves
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

2009 B.–L.:
complete addition law for
another specialization
covering all the "NIST curves"
over *non-binary* fields.

Consider, e.g., th
$x^2 + y^2 = x + y$
with $d = -1$ and
$t = \begin{matrix} 7875101804111725 \\ 7671764645385450 \\ 1395651 \end{matrix}$
over $\mathbf{F}_p$ where p
$2^{192} + 2^{96} - 1$.
Note: d is non-s

Birationally equiv
standard "NIST
$v^2 = u^3 - 3u +$
$a_6 = \begin{matrix} 4105836372515214 \\ 0472684091144410 \\ 525631 \end{matrix}$

on
rves:

d_{22}
n.

2008 B.–L.–Rezaeian Farashahi:
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2)=$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic curves
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

2009 B.–L.:
complete addition law for
another specialization
covering all the "NIST curves"
over *non-binary* fields.

Consider, e.g., the curve
$x^2+y^2 = x+y+txy+d$
with $d=-1$ and

$$t = \begin{array}{r} 787510180411172525454209999 54 \\ 767176464538545060814630202 84 \\ 13956511758592017 99 \end{array}$$

over $\mathbf{F}_p$ where $p = 2^{256} -$
$2^{192}+2^{96}-1$.
Note: d is non-square in $\mathbf{F}$

Birationally equivalent to
standard "NIST P-256" cu
$v^2 = u^3 - 3u + a_6$ where

$$a_6 = \begin{array}{r} 410583637251521421293261297 80 \\ 047268409114441015993725554 83 \\ 52563140394674012 91 \end{array}$$

2008 B.–L.–Rezaeian Farashahi:
complete addition law for
"binary Edwards curves"
$d_1(x+y)+d_2(x^2+y^2)=$
$(x+x^2)(y+y^2)$.
Covers all ordinary elliptic curves
over $\mathbf{F}_{2^n}$ for $n \geq 3$.
Also surprisingly fast,
especially if $d_1 = d_2$.

2009 B.–L.:
complete addition law for
another specialization
covering all the "NIST curves"
over *non-binary* fields.

Consider, e.g., the curve
$x^2+y^2 = x+y+txy+dx^2y^2$
with $d=-1$ and

$$t = \begin{array}{r} 787510180411172525454209999 54 \\ 767176464538545060814630202 84 \\ 1395651175859201799 \end{array}$$

over $\mathbf{F}_p$ where $p = 2^{256}-2^{224}+2^{192}+2^{96}-1$.

Note: d is non-square in $\mathbf{F}_p$.

Birationally equivalent to
standard "NIST P-256" curve
$v^2 = u^3 - 3u + a_6$ where

$$a_6 = \begin{array}{r} 410583637251521421293261297 80 \\ 047268409114441015993725554 83. \\ 52563140394674012 91 \end{array}$$

B.–L.–Rezaeian Farashahi:
ete addition law for
y Edwards curves"
$+ y) + d_2(x^2 + y^2) =$
$^2)(y + y^2)$.
all ordinary elliptic curves
2^n for $n \geq 3$.
urprisingly fast,
ally if $d_1 = d_2$.

B.–L.:
ete addition law for
r specialization
g all the "NIST curves"
on-binary fields.

Consider, e.g., the curve
$x^2 + y^2 = x + y + txy + dx^2y^2$
with $d = -1$ and

$$t = \begin{array}{r} 787510180411172525454209999 54 \\ 767176464538545060814630202 84 \\ 13956511758592017 99 \end{array}$$

over $\mathbf{F}_p$ where $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$.

Note: d is non-square in $\mathbf{F}_p$.

Birationally equivalent to
standard "NIST P-256" curve
$v^2 = u^3 - 3u + a_6$ where

$$a_6 = \begin{array}{r} 410583637251521421293261297 80 \\ 047268409114441015993725554 83. \\ 525631403946740129 1 \end{array}$$

An add
$x^2 + y$
comple

$$x_3 = \frac{x}{(}$$

$$y_3 = \frac{y}{(}$$

eian Farashahi:
n law for
curves"
$c^2 + y^2) =$
).
ry elliptic curves
3.
fast,
$= d_2$.

n law for
ation
"NIST curves"
fields.

Consider, e.g., the curve
$x^2 + y^2 = x + y + txy + dx^2y^2$
with $d = -1$ and

$$t = \begin{array}{r} 78751018041117252545420999954 \\ 76717646453854506081463020284 \\ 1395651175859201799 \end{array}$$

over $\mathbf{F}_p$ where $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$.

Note: d is non-square in $\mathbf{F}_p$.

Birationally equivalent to
standard "NIST P-256" curve
$v^2 = u^3 - 3u + a_6$ where

$$a_6 = \begin{array}{r} 41058363725152142129326129780 \\ 04726840911444101599372555483. \\ 52563140394674012 91 \end{array}$$

An addition law
$x^2 + y^2 = x + y$
complete if d is

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + \\ (x_1 - y_1)(x \\ dx_1^2(x_2y_1 + \end{array}}{\begin{array}{l} 1 - 2dx_1x_2 \\ dx_1^2(x_2 + y \end{array}}$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + \\ (y_1 - x_1)(y \\ dy_1^2(y_2x_1 + \end{array}}{\begin{array}{l} 1 - 2dy_1y_2 \\ dy_1^2(y_2 + x \end{array}}$$

shahi:

=

curves

ves"

Consider, e.g., the curve

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

with $d = -1$ and

$$t = \begin{array}{r} 78751018041117252545420999954 \\ 76717646453854506081463020284 \\ 13956511758592017 99 \end{array}$$

over $\mathbf{F}_p$ where $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$.

Note: d is non-square in $\mathbf{F}_p$.

Birationally equivalent to standard "NIST P-256" curve $v^2 = u^3 - 3u + a_6$ where

$$a_6 = \begin{array}{r} 41058363725152142129326129780 \\ 04726840911444101599372555483. \\ 52563140394674012 91 \end{array}$$

An addition law for

$x^2 + y^2 = x + y + txy + d$

complete if d is not a squa

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2 \end{array}}$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2 \end{array}}$$

Consider, e.g., the curve
$x^2 + y^2 = x + y + txy + dx^2y^2$
with $d = -1$ and

$$t = \begin{array}{r} 78751018041117252545420999954 \\ 76717646453854506081463020284 \\ 1395651175859201799 \end{array}$$

over $\mathbf{F}_p$ where $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$.

Note: d is non-square in $\mathbf{F}_p$.

Birationally equivalent to standard "NIST P-256" curve $v^2 = u^3 - 3u + a_6$ where

$$a_6 = \begin{array}{r} 41058363725152142129326129780 \\ 04726840911444101599372555483. \\ 5256314039467401291 \end{array}$$

An addition law for
$x^2 + y^2 = x + y + txy + dx^2y^2$,
complete if d is not a square:

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

er, e.g., the curve

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

$= -1$ and

101804111725254542099954
764645385450608146302028
139565117585920179 9

$_p$ where $p = 2^{256} - 2^{224} +$

$2^{96} - 1$.

d is non-square in $\mathbf{F}_p$.

nally equivalent to

rd "NIST P-256" curve

$^3 - 3u + a_6$ where

058363725152142129326129780
726840911444101599372555483.
525631403946740129 1

An addition law for
$x^2 + y^2 = x + y + txy + dx^2y^2$,
complete if d is not a square:

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Note o
An eas
Rieman
law giv

Are tho
Find lo
Monag
ISSAC
random

Are tho
But alw
find co
among
denomi

ne curve

$+ txy + dx^2y^2$

545420999954
081463020284
175859201799

$= 2^{256} - 2^{224} +$

quare in $\mathbf{F}_p$.

valent to

P-256" curve

a_6 where

42129326129780
01599372555483.
14039467401291

An addition law for
$x^2 + y^2 = x + y + txy + dx^2y^2$,
complete if d is not a square:

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Note on computi
An easy Magma
Riemann–Roch t
law given a curve

Are those laws n
Find lower-degre
Monagan–Pearce
ISSAC 2006; or b
random points or

Are those laws co
But always seems
find complete ad
among low-degre
denominator con

dx^2y^2

$2^{224} +$

p.

rve

.

An addition law for
$x^2 + y^2 = x + y + txy + dx^2y^2$,
complete if d is not a square:

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Note on computing additio
An easy Magma script uses
Riemann–Roch to find add
law given a curve shape.

Are those laws nice? No!
Find lower-degree laws by
Monagan–Pearce algorithm
ISSAC 2006; or by evaluati
random points on random

Are those laws complete?
But always seems easy to
find complete addition laws
among low-degree laws wh
denominator constant term

An addition law for
$x^2 + y^2 = x + y + txy + dx^2y^2$,
complete if d is not a square:

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Note on computing addition laws:
An easy Magma script uses
Riemann–Roch to find addition
law given a curve shape.

Are those laws nice? No!
Find lower-degree laws by
Monagan–Pearce algorithm,
ISSAC 2006; or by evaluation at
random points on random curves.

Are those laws complete? No!
But always seems easy to
find complete addition laws
among low-degree laws where
denominator constant term $\neq 0$.

dition law for

$$^2 = x + y + txy + dx^2y^2,$$

ete if d is not a square:

$$x_1 + x_2 + (t-2)x_1x_2 +$$
$$x_1 - y_1)(x_2 - y_2) +$$
$$\frac{x_1^2(x_2y_1 + x_2y_2 - y_1y_2)}{- 2dx_1x_2y_2 -}$$
$$x_1^2(x_2 + y_2 + (t-2)x_2y_2)$$

$$y_1 + y_2 + (t-2)y_1y_2 +$$
$$y_1 - x_1)(y_2 - x_2) +$$
$$\frac{y_1^2(y_2x_1 + y_2x_2 - x_1x_2)}{- 2dy_1y_2x_2 -}.$$
$$y_1^2(y_2 + x_2 + (t-2)y_2x_2)$$

Note on computing addition laws:
An easy Magma script uses
Riemann–Roch to find addition
law given a curve shape.

Are those laws nice? No!
Find lower-degree laws by
Monagan–Pearce algorithm,
ISSAC 2006; or by evaluation at
random points on random curves.

Are those laws complete? No!
But always seems easy to
find complete addition laws
among low-degree laws where
denominator constant term $\neq 0$.

Biratio

$$x^2 + y$$
$$v^2 - (t$$
$$u^3$$

i.e. v^2

$$(u$$

$$u = (d$$

$$v = \frac{(}{(t$$

Assumi
only ex
$(0, 0)$,

Inverse
$y = ((t$

for
$+ txy + dx^2y^2$,
not a square:

$$(t-2)x_1x_2 +$$
$$x_2 - y_2) +$$
$$- x_2y_2 - y_1y_2)$$
$$\overline{2y_2 -}$$
$$y_2 + (t-2)x_2y_2)$$

$$(t-2)y_1y_2 +$$
$$y_2 - x_2) +$$
$$- y_2x_2 - x_1x_2)$$
$$\overline{x_2 -}$$
$$_2 + (t-2)y_2x_2)$$

Note on computing addition laws:
An easy Magma script uses Riemann–Roch to find addition law given a curve shape.

Are those laws nice? No!
Find lower-degree laws by Monagan–Pearce algorithm, ISSAC 2006; or by evaluation at random points on random curves.

Are those laws complete? No!
But always seems easy to find complete addition laws among low-degree laws where denominator constant term $\neq 0$.

Birational equiva
$x^2 + y^2 = x + y$
$v^2 - (t+2)uv +$
$u^3 - (t+2)$
i.e. $v^2 - (t+2)$
$(u^2 - d)(u$

$u = (dxy + t +$

$v = \frac{((t+2)^2 -}{(t+2)xy +}$

Assuming $t+2$ s
only exceptional
$(0,0)$, mapping t

Inverse: $x = v/($
$y = ((t+2)u -$

dx^2y^2,

re:

$c_2 +$

$y_1y_2)$

;

$)x_2y_2)$

$2 +$

$x_1x_2)$

.

$)y_2x_2)$

Note on computing addition laws:
An easy Magma script uses Riemann–Roch to find addition law given a curve shape.

Are those laws nice? No!
Find lower-degree laws by Monagan–Pearce algorithm, ISSAC 2006; or by evaluation at random points on random curves.

Are those laws complete? No!
But always seems easy to find complete addition laws among low-degree laws where denominator constant term $\neq 0$.

Birational equivalence from

$x^2 + y^2 = x + y + txy + d$

$v^2 - (t+2)uv + dv =$

$u^3 - (t+2)u^2 - du +$

i.e. $v^2 - (t+2)uv + dv =$

$(u^2 - d)(u - (t+2))$

$u = (dxy + t + 2)/(x + y)$

$$v = \frac{((t+2)^2 - d)x}{(t+2)xy + x + y}.$$

Assuming $t+2$ square, d n
only exceptional point is $(0, 0)$, mapping to ∞.

Inverse: $x = v/(u^2 - d)$;
$y = ((t+2)u - v - d)/(u$

Note on computing addition laws:
An easy Magma script uses
Riemann–Roch to find addition
law given a curve shape.

Are those laws nice? No!
Find lower-degree laws by
Monagan–Pearce algorithm,
ISSAC 2006; or by evaluation at
random points on random curves.

Are those laws complete? No!
But always seems easy to
find complete addition laws
among low-degree laws where
denominator constant term $\neq 0$.

Birational equivalence from
$x^2 + y^2 = x + y + txy + dx^2y^2$ to
$v^2 - (t+2)uv + dv =$
$u^3 - (t+2)u^2 - du + (t+2)d$
i.e. $v^2 - (t+2)uv + dv =$
$(u^2 - d)(u - (t+2))$:

$u = (dxy + t + 2)/(x + y)$;

$$v = \frac{((t+2)^2 - d)x}{(t+2)xy + x + y}.$$

Assuming $t + 2$ square, d not:
only exceptional point is
$(0, 0)$, mapping to ∞.

Inverse: $x = v/(u^2 - d)$;
$y = ((t+2)u - v - d)/(u^2 - d)$.

n computing addition laws:
y Magma script uses
nn–Roch to find addition
en a curve shape.

ose laws nice? No!
wer-degree laws by
an–Pearce algorithm,
2006; or by evaluation at
n points on random curves.

ose laws complete? No!
ways seems easy to
mplete addition laws
low-degree laws where
inator constant term $\neq 0$.

Birational equivalence from
$x^2 + y^2 = x + y + txy + dx^2y^2$ to
$v^2 - (t+2)uv + dv =$
$u^3 - (t+2)u^2 - du + (t+2)d$
i.e. $v^2 - (t+2)uv + dv =$
$(u^2 - d)(u - (t+2))$:

$u = (dxy + t + 2)/(x + y)$;

$$v = \frac{((t+2)^2 - d)x}{(t+2)xy + x + y}.$$

Assuming $t+2$ square, d not:
only exceptional point is
$(0, 0)$, mapping to ∞.

Inverse: $x = v/(u^2 - d)$;
$y = ((t+2)u - v - d)/(u^2 - d)$.

Comple

$x_3 =$

$y_3 =$

Can de

ng addition laws:
script uses
o find addition
e shape.

ice? No!
e laws by
e algorithm,
by evaluation at
n random curves.

omplete? No!
s easy to
dition laws
ee laws where
stant term $\neq 0$.

Birational equivalence from
$x^2 + y^2 = x + y + txy + dx^2y^2$ to
$v^2 - (t+2)uv + dv =$
$u^3 - (t+2)u^2 - du + (t+2)d$
i.e. $v^2 - (t+2)uv + dv =$
$(u^2 - d)(u - (t+2))$:

$u = (dxy + t + 2)/(x + y)$;

$$v = \frac{((t+2)^2 - d)x}{(t+2)xy + x + y}.$$

Assuming $t+2$ square, d not:
only exceptional point is
$(0, 0)$, mapping to ∞.

Inverse: $x = v/(u^2 - d)$;
$y = ((t+2)u - v - d)/(u^2 - d)$.

Completeness

$$x_3 = \frac{x_1 + x_2 + (}{(x_1 - y_1)(x}$$
$$\frac{dx_1^2(x_2y_1 +}{1 - 2dx_1x_2}$$
$$dx_1^2(x_2 + y$$

$$y_3 = \frac{y_1 + y_2 + (}{(y_1 - x_1)(y}$$
$$\frac{dy_1^2(y_2x_1 +}{1 - 2dy_1y_2}$$
$$dy_1^2(y_2 + x$$

Can denominator

on laws:
s
ition

n,
ion at
curves.

No!

s
ere
$n \neq 0$.

Birational equivalence from
$x^2 + y^2 = x + y + txy + dx^2y^2$ to
$v^2 - (t+2)uv + dv =$
$u^3 - (t+2)u^2 - du + (t+2)d$
i.e. $v^2 - (t+2)uv + dv =$
$(u^2 - d)(u - (t+2))$:

$u = (dxy + t + 2)/(x + y)$;

$$v = \frac{((t+2)^2 - d)x}{(t+2)xy + x + y}.$$

Assuming $t+2$ square, d not:
only exceptional point is
$(0, 0)$, mapping to ∞.

Inverse: $x = v/(u^2 - d)$;
$y = ((t+2)u - v - d)/(u^2 - d)$.

Completeness

$$x_3 = \frac{x_1 + x_2 + (t-2)x_1x}{(x_1 - y_1)(x_2 - y_2) + dx_1^2(x_2y_1 + x_2y_2 - y}$$
$$1 - 2dx_1x_2y_2 - dx_1^2(x_2 + y_2 + (t-2$$

$$y_3 = \frac{y_1 + y_2 + (t-2)y_1y_2}{(y_1 - x_1)(y_2 - x_2) + dy_1^2(y_2x_1 + y_2x_2 - x}$$
$$1 - 2dy_1y_2x_2 - dy_1^2(y_2 + x_2 + (t-2$$

Can denominators be 0?

Birational equivalence from
$x^2 + y^2 = x + y + txy + dx^2y^2$ to
$v^2 - (t+2)uv + dv =$
$u^3 - (t+2)u^2 - du + (t+2)d$
i.e. $v^2 - (t+2)uv + dv =$
$(u^2 - d)(u - (t+2))$:

$u = (dxy + t + 2)/(x + y)$;

$$v = \frac{((t+2)^2 - d)x}{(t+2)xy + x + y}.$$

Assuming $t + 2$ square, d not:
only exceptional point is
$(0, 0)$, mapping to ∞.

Inverse: $x = v/(u^2 - d)$;
$y = ((t+2)u - v - d)/(u^2 - d)$.

Completeness

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Can denominators be 0?

nal equivalence from
$^2 = x + y + txy + dx^2y^2$ to
$t + 2)uv + dv =$
$^3 - (t+2)u^2 - du + (t+2)d$
$- (t + 2)uv + dv =$
$u^2 - d)(u - (t + 2))$:

$xy + t + 2)/(x + y)$;
$\frac{(t+2)^2 - d)x}{+ 2)xy + x + y}$.

ing $t + 2$ square, d not:
xceptional point is
mapping to ∞.

: $x = v/(u^2 - d)$;
$t + 2)u - v - d)/(u^2 - d)$.

Completeness

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Can denominators be 0?

Only if

Theore
k is a f
d, t, x_1
d is no
$27d \neq$
$x_1^2 + y_1^2$
$x_2^2 + y_2^2$
Then 1
$dx_1^2(x_2$

lence from
$+txy+dx^2y^2$ to
$-dv=$
$u^2-du+(t+2)d$
$uv+dv=$
$-(t+2))$:

$2)/(x+y)$;
$-d)x$
$\overline{x+y}$.

square, d not:
point is
to ∞.

$u^2-d)$;
$v-d)/(u^2-d)$.

Completeness

$$x_3=\frac{\begin{array}{l}x_1+x_2+(t-2)x_1x_2+\\(x_1-y_1)(x_2-y_2)+\\dx_1^2(x_2y_1+x_2y_2-y_1y_2)\end{array}}{\begin{array}{l}1-2dx_1x_2y_2-\\dx_1^2(x_2+y_2+(t-2)x_2y_2)\end{array}};$$

$$y_3=\frac{\begin{array}{l}y_1+y_2+(t-2)y_1y_2+\\(y_1-x_1)(y_2-x_2)+\\dy_1^2(y_2x_1+y_2x_2-x_1x_2)\end{array}}{\begin{array}{l}1-2dy_1y_2x_2-\\dy_1^2(y_2+x_2+(t-2)y_2x_2)\end{array}}.$$

Can denominators be 0?

Only if d is a squ

Theorem: Assum
k is a field with 2
d,t,x_1,y_1,x_2,y_2
d is not a square
$27d\neq(2-t)^3$;
$x_1^2+y_1^2=x_1+y_1$
$x_2^2+y_2^2=x_2+y_2$
Then $1-2dx_1x_2$
$dx_1^2(x_2+y_2+(t$

n
x^2y^2 to

$(t+2)d$

:

);

not:

$^2 - d)$.

Completeness

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Can denominators be 0?

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 +$

$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 +$

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2$

Completeness

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Can denominators be 0?

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;

$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

Completeness

$$x_3 = \frac{\begin{array}{l} x_1 + x_2 + (t-2)x_1x_2 + \\ (x_1 - y_1)(x_2 - y_2) + \\ dx_1^2(x_2y_1 + x_2y_2 - y_1y_2) \end{array}}{\begin{array}{l} 1 - 2dx_1x_2y_2 - \\ dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1 + y_2 + (t-2)y_1y_2 + \\ (y_1 - x_1)(y_2 - x_2) + \\ dy_1^2(y_2x_1 + y_2x_2 - x_1x_2) \end{array}}{\begin{array}{l} 1 - 2dy_1y_2x_2 - \\ dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \end{array}}.$$

Can denominators be 0?

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;

$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry

also $1 - 2dy_1y_2x_2 -$

$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

eteness

$$x_1 + x_2 + (t-2)x_1x_2 +$$
$$x_1 - y_1)(x_2 - y_2) +$$
$$\frac{x_1^2(x_2y_1 + x_2y_2 - y_1y_2)}{- 2dx_1x_2y_2 -}$$
$$x_1^2(x_2 + y_2 + (t-2)x_2y_2)$$

$$y_1 + y_2 + (t-2)y_1y_2 +$$
$$y_1 - x_1)(y_2 - x_2) +$$
$$\frac{y_1^2(y_2x_1 + y_2x_2 - x_1x_2)}{- 2dy_1y_2x_2 -}.$$
$$y_1^2(y_2 + x_2 + (t-2)y_2x_2)$$

enominators be 0?

Only if d is a square!

Theorem: Assume that
k is a field with $2 \neq 0$;
$d, t, x_1, y_1, x_2, y_2 \in k$;
d is not a square in k;
$27d \neq (2-t)^3$;
$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;
$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.
Then $1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry
also $1 - 2dy_1y_2x_2 -$
$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

Proof:
$1 - 2d$
$dx_1^2(x_2$

$(t-2)x_1x_2 +$
$x_2 - y_2) +$
$- x_2y_2 - y_1y_2)$
$\frac{}{}$;
$y_2 -$
$_2 + (t-2)x_2y_2)$

$t-2)y_1y_2 +$
$y_2 - x_2) +$
$- y_2x_2 - x_1x_2)$
$\frac{}{}$.
$x_2 -$
$_2 + (t-2)y_2x_2)$

rs be 0?

Only if d is a square!

Theorem: Assume that
k is a field with $2 \neq 0$;
$d, t, x_1, y_1, x_2, y_2 \in k$;
d is not a square in k;
$27d \neq (2-t)^3$;
$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;
$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.
Then $1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry
also $1 - 2dy_1y_2x_2 -$
$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

Proof: Suppose t
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t$

$c_2 +$

$\frac{y_1 y_2)}{}$;

$)x_2 y_2)$

$2 +$

$\frac{x_1 x_2)}{}$.

$)y_2 x_2)$

Only if d is a square!

Theorem: Assume that
k is a field with $2 \neq 0$;
$d, t, x_1, y_1, x_2, y_2 \in k$;
d is not a square in k;
$27d \neq (2-t)^3$;
$x_1^2 + y_1^2 = x_1 + y_1 + t x_1 y_1 + d x_1^2 y_1^2$;
$x_2^2 + y_2^2 = x_2 + y_2 + t x_2 y_2 + d x_2^2 y_2^2$.
Then $1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry
also $1 - 2dy_1y_2x_2 -$
$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2$

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;

$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry

also $1 - 2dy_1y_2x_2 -$

$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

Proof: Suppose that

$1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0$.

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;

$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry

also $1 - 2dy_1y_2x_2 -$

$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

Proof: Suppose that

$1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0$.

Note that $x_1 \neq 0$.

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;

$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) \neq 0$.

By $x \leftrightarrow y$ symmetry

also $1 - 2dy_1y_2x_2 -$

$dy_1^2(y_2 + x_2 + (t-2)y_2x_2) \neq 0$.

Proof: Suppose that

$1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0$.

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that

$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2$.

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2+y_1^2 = x_1+y_1+tx_1y_1+dx_1^2y_1^2$;

$x_2^2+y_2^2 = x_2+y_2+tx_2y_2+dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2+y_2+(t-2)x_2y_2) \neq 0.$

By $x \leftrightarrow y$ symmetry

also $1 - 2dy_1y_2x_2 -$

$dy_1^2(y_2+x_2+(t-2)y_2x_2) \neq 0.$

Proof: Suppose that

$1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2+y_2+(t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that

$(1-dx_1x_2y_2)^2 = dx_1^2(x_2-y_2)^2.$

By hypothesis d is non-square

so $x_1^2(x_2-y_2)^2 = 0$

and $(1-dx_1x_2y_2)^2 = 0.$

Only if d is a square!

Theorem: Assume that

k is a field with $2 \neq 0$;

$d, t, x_1, y_1, x_2, y_2 \in k$;

d is not a square in k;

$27d \neq (2-t)^3$;

$x_1^2+y_1^2 = x_1+y_1+tx_1y_1+dx_1^2y_1^2$;

$x_2^2+y_2^2 = x_2+y_2+tx_2y_2+dx_2^2y_2^2$.

Then $1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2+y_2+(t-2)x_2y_2) \neq 0.$

By $x \leftrightarrow y$ symmetry

also $1 - 2dy_1y_2x_2 -$

$dy_1^2(y_2+x_2+(t-2)y_2x_2) \neq 0.$

Proof: Suppose that

$1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2+y_2+(t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that

$(1-dx_1x_2y_2)^2 = dx_1^2(x_2-y_2)^2.$

By hypothesis d is non-square

so $x_1^2(x_2-y_2)^2 = 0$

and $(1-dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2$.

d is a square!

m: Assume that

ield with $2 \neq 0$;

$, y_1, x_2, y_2 \in k$;

t a square in k;

$(2-t)^3$;

$= x_1 + y_1 + t x_1 y_1 + d x_1^2 y_1^2$;

$= x_2 + y_2 + t x_2 y_2 + d x_2^2 y_2^2$.

$- 2 d x_1 x_2 y_2 -$

$+ y_2 + (t-2) x_2 y_2) \neq 0$.

$\to y$ symmetry

$- 2 d y_1 y_2 x_2 -$

$+ x_2 + (t-2) y_2 x_2) \neq 0$.

Proof: Suppose that

$1 - 2 d x_1 x_2 y_2 -$

$d x_1^2 (x_2 + y_2 + (t-2) x_2 y_2) = 0$.

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that

$(1 - d x_1 x_2 y_2)^2 = d x_1^2 (x_2 - y_2)^2$.

By hypothesis d is non-square

so $x_1^2 (x_2 - y_2)^2 = 0$

and $(1 - d x_1 x_2 y_2)^2 = 0$.

Hence $x_2 = y_2$ and $1 = d x_1 x_2 y_2$.

Curve e

$1 + y_1^2$

$1/x_1 +$

uare!

ne that

$2 \neq 0$;

$\in k$;

in k;

$$_1 + tx_1y_1 + dx_1^2y_1^2;$$

$$_2 + tx_2y_2 + dx_2^2y_2^2.$$

$$_2y_2 -$$

$$t - 2)x_2y_2) \neq 0.$$

etry

$$x_2 -$$

$$t - 2)y_2x_2) \neq 0.$$

Proof: Suppose that

$1 - 2dx_1x_2y_2 -$

$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that

$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square

so $x_1^2(x_2 - y_2)^2 = 0$

and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2$.

Curve equation$_1$

$1 + y_1^2/x_1^2 =$

$1/x_1 + y_1(1/x_1^2 +$

$-dx_1^2y_1^2;$
$-dx_2^2y_2^2.$

$) \neq 0.$

$) \neq 0.$

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that
$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square
so $x_1^2(x_2 - y_2)^2 = 0$
and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2.$

Curve equation$_1$ times $1/x$
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) +$

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that
$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square
so $x_1^2(x_2 - y_2)^2 = 0$
and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2$.

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that
$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square
so $x_1^2(x_2 - y_2)^2 = 0$
and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2$.

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:
$1 + d^2y_1^2x_2^4 =$
$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that
$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square
so $x_1^2(x_2 - y_2)^2 = 0$
and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2$.

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:
$1 + d^2y_1^2x_2^4 =$
$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:
$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2.$

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that
$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square
so $x_1^2(x_2 - y_2)^2 = 0$
and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2.$

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:
$1 + d^2y_1^2x_2^4 =$
$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:
$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2.$

Thus $x_2 = y_1$ and $1 = dy_1x_2^2.$
Hence $1 = dx_2^3.$

Proof: Suppose that
$1 - 2dx_1x_2y_2 -$
$dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$

Note that $x_1 \neq 0$.

Use curve equation$_2$ to see that
$(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.$

By hypothesis d is non-square
so $x_1^2(x_2 - y_2)^2 = 0$
and $(1 - dx_1x_2y_2)^2 = 0.$

Hence $x_2 = y_2$ and $1 = dx_1x_2y_2.$

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:
$1 + d^2y_1^2x_2^4 =$
$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:
$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2.$

Thus $x_2 = y_1$ and $1 = dy_1x_2^2.$
Hence $1 = dx_2^3.$

Now $2x_2^2 = 2x_2 + tx_2^2 + x_2$
so $3 = (2-t)x_2$ so $27d = (2-t)^3.$
Contradiction.

Suppose that

$x_1x_2y_2 -$

$+ y_2 + (t-2)x_2y_2) = 0.$

hat $x_1 \neq 0$.

rve equation$_2$ to see that

$x_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2$.

othesis d is non-square

$x_2 - y_2)^2 = 0$

$- dx_1x_2y_2)^2 = 0.$

$x_2 = y_2$ and $1 = dx_1x_2y_2$.

Curve equation$_1$ times $1/x_1^2$:

$1 + y_1^2/x_1^2 =$

$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:

$1 + d^2y_1^2x_2^4 =$

$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:

$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2.$

Thus $x_2 = y_1$ and $1 = dy_1x_2^2$.

Hence $1 = dx_2^3$.

Now $2x_2^2 = 2x_2 + tx_2^2 + x_2$

so $3 = (2-t)x_2$ so $27d = (2-t)^3$.

Contradiction.

What's

Make t

Prove

are cov

using W

Make t

Find *fa*

Latest

Have c

for twis

$ax^3 +$

when a

Close i

and co

that

$t-2)x_2y_2) = 0.$

0.

on_2 to see that

$= dx_1^2(x_2-y_2)^2.$

is non-square

$= 0$

$_2)^2 = 0.$

nd $1 = dx_1x_2y_2$.

Curve equation$_1$ times $1/x_1^2$:

$1 + y_1^2/x_1^2 =$

$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:

$1 + d^2y_1^2x_2^4 =$

$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:

$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2.$

Thus $x_2 = y_1$ and $1 = dy_1x_2^2$.

Hence $1 = dx_2^3$.

Now $2x_2^2 = 2x_2 + tx_2^2 + x_2$

so $3 = (2-t)x_2$ so $27d = (2-t)^3$.

Contradiction.

What's next?

Make the mather

Prove that all cu

are covered; shou

using Weil and ra

Make the compu

Find *faster* comp

Latest news, B.–

Have complete a

for twisted Hessi

$ax^3 + y^3 + 1 =$

when a is non-cu

Close in speed to

and covers differe

$) = 0.$

e that

$- y_2)^2.$

are

$c_1 x_2 y_2.$

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2.$

Substitute $1/x_1 = dx_2^2$:
$1 + d^2 y_1^2 x_2^4 =$
$dx_2^2 + dy_1(dx_2^4 + x_2^2 t) + dy_1^2.$

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:
$(1 - dy_1 x_2^2)^2 = d(x_2 - y_1)^2.$

Thus $x_2 = y_1$ and $1 = dy_1 x_2^2$.
Hence $1 = dx_2^3$.

Now $2x_2^2 = 2x_2 + tx_2^2 + x_2$
so $3 = (2-t)x_2$ so $27d = (2-t)^3$.
Contradiction.

What's next?

Make the mathematicians

Prove that all curves
are covered; should be easy
using Weil and rational par

Make the computer happy:
Find *faster* complete laws.

Latest news, B.–Kohel–L.:
Have complete addition law
for twisted Hessian curves
$ax^3 + y^3 + 1 = 3dxy$
when a is non-cube.
Close in speed to Edwards
and covers different curves

Curve equation$_1$ times $1/x_1^2$:
$1 + y_1^2/x_1^2 =$
$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2$.

Substitute $1/x_1 = dx_2^2$:
$1 + d^2y_1^2x_2^4 =$
$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2$.

Substitute $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:
$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2$.

Thus $x_2 = y_1$ and $1 = dy_1x_2^2$.
Hence $1 = dx_2^3$.

Now $2x_2^2 = 2x_2 + tx_2^2 + x_2$
so $3 = (2-t)x_2$ so $27d = (2-t)^3$.
Contradiction.

What's next?

Make the mathematicians happy:
Prove that all curves
are covered; should be easy
using Weil and rational param.

Make the computer happy:
Find *faster* complete laws.

Latest news, B.–Kohel–L.:
Have complete addition law
for twisted Hessian curves
$ax^3 + y^3 + 1 = 3dxy$
when a is non-cube.
Close in speed to Edwards
and covers different curves.