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.”
What we think when we hear “addition on elliptic curves”:

Addition on \( y^2 - 5xy = x^3 - 7 \).
\[ \lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)}, \]
\[ x_3 = \lambda^2 - 5\lambda - x_1 - x_2, \]
\[ y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1)) \]
\[ \Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3). \]
\[
\lambda = \frac{y_2 - y_1}{x_2 - x_1},
\]
\[
x_3 = \lambda^2 - 5\lambda - x_1 - x_2,
\]
\[
y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))
\]
\[
\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3).
\]

Oops, this requires \( x_1 \neq x_2 \).

\[
\lambda = \frac{5y_1 + 3x_1^2}{2y_1 - 5x_1},
\]
\[
x_3 = \lambda^2 - 5\lambda - 2x_1,
\]
\[
y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))
\]
\[
\Rightarrow (x_1, y_1) + (x_1, y_1) = (x_3, y_3).
\]
\[
\lambda = (y_2 - y_1)/(x_2 - x_1),
\]
\[
x_3 = \lambda^2 - 5\lambda - x_1 - x_2,
\]
\[
y_3 = 5x_3 - (y_1 + \lambda(x_3 - x_1))
\Rightarrow (x_1, y_1) + (x_2, y_2) = (x_3, y_3).
\]
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
\[
(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \quad \text{with}
\]
\[
x_3 = \frac{x_1 y_2 + y_1 x_2}{1 - x_1 x_2 y_1 y_2},
\]
\[
y_3 = \frac{y_1 y_2 - x_1 x_2}{1 + x_1 x_2 y_1 y_2}.
\]

Euler        Gauss
Edwards, continued:

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

(Euler–Gauss curve \( \equiv \) the
“lemniscatic elliptic curve.”)
Edwards, continued:

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

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

$x^2 + y^2 = a^2(1 + x^2 y^2)$ has
neutral element $(0, a)$, addition
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with
\[
x_3 = \frac{x_1 y_2 + y_1 x_2}{a(1 + x_1 x_2 y_1 y_2)},
\]
\[
y_3 = \frac{y_1 y_2 - x_1 x_2}{a(1 - x_1 x_2 y_1 y_2)}.
\]
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 Chudnovsky²:
17M unified addition formulas for \((S : C : D : Z)\) on Jacobi’s
\[S^2 + C^2 = Z^2, \quad k^2 S^2 + D^2 = Z^2.\]
2007.01.10, ≈ 09:30,
Bernstein–Lange:

Edwards addition law with standard projective \((X : Y : Z)\), standard Karatsuba optimization, common-subexp elimination:

\[10M + 1S + 1A.\]

Faster than anything seen before!

**M**: field multiplication.

**S**: field squaring.

**A**: multiplication by \(a\).

Karatsuba

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.

Edwards \(x^2 + y^2 = \alpha^2(1 + x^2y^2)\) doesn’t rationally include Euler–Gauss \(x^2 + y^2 = 1 - x^2y^2\).

Common generalization, presumably more curves over \(\mathbb{Q}\), presumably more curves over \(\mathbb{F}_q\): \(x^2 + y^2 = c^2(1 + dx^2y^2)\) 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

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

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$
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 $d \in \mathbb{F}_p$.

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

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.
Even if we switched to projective coordinates, we 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 \( p = 47, \ d = 25 \):
denominator \( 1 \pm dx_1 x_2 y_1 y_2 \)
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 \( 1 \pm dx_1 x_2 y_1 y_2 \)
is nonzero for all points
\((x_1, y_1), (x_2, y_2)\) on curve.
Addition law is a group law!
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 \(dx_1x_2y_1y_2 = \pm 1\)
If $x_1^2 + y_1^2 = 1 + dx_1^2 y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2 y_2^2$
and $dx_1 x_2 y_1 y_2 = \pm 1$
then $dx_1^2 y_1^2 (x_2 + y_2)^2$
$= dx_1^2 y_1^2 (x_2^2 + y_2^2 + 2x_2 y_2)$
$= dx_1^2 y_1^2 (dx_2^2 y_2^2 + 1 + 2x_2 y_2)$
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 $dx_1^2y_1^2(x_2 + y_2)^2$

$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
2007 Bernstein–Lange completeness proof for all non-square $d$: 

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

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 $k$. 
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 $E(\bar{k}) \times E(\bar{k})$, where $\bar{k} = \text{algebraic closure of } k$.

Edwards addition formula has exceptional cases for $E(\bar{k})$ . . . 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:

\[
x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + dx_1 x_2 y_1 y_2},
\]

\[
y_3 = \frac{y_1 y_2 - x_1 x_2}{1 - dx_1 x_2 y_1 y_2}.
\]

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."

\[ x^2 + y^2 = 1, \text{ parametrized by } (x, y) = (\sin, \cos). \]

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

Abel, Jacobi "sn, cn, dn"
handle all elliptic curves,
but (sn, cn) does not specialize to (lemn sin, lemn cos).
Bad generalization of (sin, 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.
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!
\[ ax^2 + y^2 = 1 + dx^2 y^2 \]
cover all Montgomery curves.

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

where 4 divides group order
is (1 or 2)-isogenous
to a twisted Edwards curve.
Statistics for many $p \in 1 + 4\mathbb{Z}$, 
$\approx$ number of pairs $(j(E), \#E)$:

<table>
<thead>
<tr>
<th>Curves</th>
<th>total</th>
<th>odd</th>
<th>2odd</th>
<th>4odd</th>
<th>8odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>orig</td>
<td>$\frac{1}{24} , p$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>compl</td>
<td>$\frac{1}{2} , p$</td>
<td>0</td>
<td>0</td>
<td>$\frac{1}{4} , p$</td>
<td>$\frac{1}{8} , p$</td>
</tr>
<tr>
<td>Ed</td>
<td>$\frac{2}{3} , p$</td>
<td>0</td>
<td>0</td>
<td>$\frac{1}{4} , p$</td>
<td>$\frac{3}{16} , p$</td>
</tr>
<tr>
<td>twist</td>
<td>$\frac{5}{6} , p$</td>
<td>0</td>
<td>0</td>
<td>$\frac{5}{12} , p$</td>
<td>$\frac{3}{16} , p$</td>
</tr>
<tr>
<td>4Z</td>
<td>$\frac{5}{6} , p$</td>
<td>0</td>
<td>0</td>
<td>$\frac{5}{12} , p$</td>
<td>$\frac{3}{16} , p$</td>
</tr>
<tr>
<td>all</td>
<td>$2p$</td>
<td>$\frac{2}{3} , p$</td>
<td>$\frac{1}{2} , p$</td>
<td>$\frac{5}{12} , p$</td>
<td>$\frac{3}{16} , p$</td>
</tr>
</tbody>
</table>

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

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.

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 $d_{22} = 0$:

\[
\begin{pmatrix}
\begin{array}{ll}
d_{20} & d_{21} \\
d_{10} & d_{11} \\
d_{00} & d_{10} \\
\end{array}
\end{pmatrix}
\]

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 $\infty$ 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:

$$
\begin{align*}
&d_{00}z^3 + d_{10}(1 + y)z^2 + \\
&d_{11}yz + d_{20}(1 + y^2)z + \\
&d_{21}y(1 + y) = 0.
\end{align*}
$$

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 $\infty$ 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 $k$. 
In particular $d_{20} \neq 0$:

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

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.
\[ d_1(x + y) + d_2(x^2 + y^2) = (x + x^2)(y + y^2). \]
Covers all ordinary elliptic curves over \( \mathbb{F}_{2^n} \) for \( n \geq 3 \).
Also surprisingly fast, especially if \( d_1 = d_2 \).
\[ d_1(x + y) + d_2(x^2 + y^2) = (x + x^2)(y + y^2). \]
Covers all ordinary elliptic curves over \( \mathbb{F}_{2^n} \) 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
\[
\begin{align*}
787510180411117252545420999954 \\
t = 76717646453854506081463020284 \\
1395651175859201799
\end{align*}
\]
over \( \mathbb{F}_p \) where \( p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 \).

Note: \( d \) is non-square in \( \mathbb{F}_p \).

Birationally equivalent to
standard “NIST P-256” curve
\[ \nu^2 = \nu^3 - 3\nu + a_6 \]
where
\[
\begin{align*}
41058363725152142129326129780 \\
a_6 = 04726840911444101599372555483. \\
5256314039467401291
\end{align*}
\]
An addition law for
\[ x^2 + y^2 = x + y + txy + dx^2 y^2, \]
complete if \( d \) is not a square:

\begin{align*}
x_3 &= x_1 + x_2 + (t - 2)x_1 x_2 + (x_1 - y_1)(x_2 - y_2) + \frac{dx_1^2 (x_2 y_1 + x_2 y_2 - y_1 y_2)}{1 - 2dx_1 x_2 y_2 - \frac{dx_2^2 (x_2 + y_2 + (t - 2)x_2 y_2)}{1 - 2dy_1 y_2 x_2 - \frac{dy_1^2 (y_2 x_1 + y_2 x_2 - x_1 x_2)}{1 - 2dy_1 y_2 x_2 - \frac{dy_2^2 (y_2 + x_2 + (t - 2)y_2 x_2)}{}}}}
\end{align*}
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 ≠ 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 \( \infty \).

Inverse: \[ x = v/(u^2 - d); \]
\[ y = ((t + 2)u - v - d)/(u^2 - d). \]
Completeness

\[ x_3 = \frac{dx^2_1(x_2 y_1 + x_2 y_2 - y_1 y_2)}{1 - 2dx_1 x_2 y_2} -
\]

\[ dx^2_1(x_2 + y_2 + (t - 2)x_2 y_2) \]

\[ y_3 = \frac{dy^2_1(y_2 x_1 + y_2 x_2 - x_1 x_2)}{1 - 2dy_1 y_2 x_2} -
\]

\[ dy^2_1(y_2 + x_2 + (t - 2)y_2 x_2) \]

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 
\( 1 - 2dx_1x_2y_2 - dx_1^2(x_2 + y_2 + (t - 2)x_2y_2) \neq 0. \)
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 \( k \);  
\( 27d \neq (2 - t)^3 \);  
\[ x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2 y_1^2; \]
\[ x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2 y_2^2. \]
Then \( 1 - 2dx_1 x_2 y_2 - dx_1^2 (x_2 + y_2 + (t - 2)x_2y_2) \neq 0 \).

By \( x \leftrightarrow y \) symmetry  
also \( 1 - 2dy_1 y_2 x_2 - dy_1^2 (y_2 + x_2 + (t - 2)y_2x_2) \neq 0 \).
Proof: Suppose that

\[ 1 - 2dx_1x_2y_2 - dx_1^2(x_2 + y_2 + (t - 2)x_2y_2) = 0. \]
Proof: Suppose that 

\[ 1 - 2dx_1 x_2 y_2 - dx_1^2 (x_2 + y_2 + (t - 2)x_2 y_2) = 0. \]

Note that \( x_1 \neq 0 \).
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
\[
(1 - dx_1x_2y_2)^2 = dx_1^2(x_2 - y_2)^2.
\]
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 \( (1 - dx_1x_2y_2)^2 = 0. \)
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 $\times \frac{1}{x_1^2}$:

$$1 + \frac{y_1^2}{x_1^2} =$$

$$\frac{1}{x_1} + y_1 \left( \frac{1}{x_1^2} + \frac{t}{x_1} \right) + dy_1^2.$$
Curve equation 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 $1/x_1 = dx_2^2$:

$$1 + d^2y_1^2 x_2^4 =
dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2.$$
Curve equation 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 $2x_2^2 = 2x_2 + tx_2^2 + dx_2^4$:

$$(1 - dy_1x_2^2)^2 = d(x_2 - y_1)^2.$$
Curve equation 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 $1 = dx_2^3$. 
Curve equation 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.