Complete addition laws for all elliptic curves over finite fields

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498

Joint work with:
Tanja Lange
Technische Universiteit Eindhoven

Memories of graduate school

Early 1990s, Berkeley:
Hendrik Lenstra teaches
a rather strange course
on algebraic number theory.

Memories of graduate school

Early 1990s, Berkeley:
Hendrik Lenstra teaches
a rather strange course
on algebraic number theory.

His central objects of study:
orders in number fields.
Primes, class groups, etc.

Memories of graduate school

Early 1990s, Berkeley:
Hendrik Lenstra teaches
a rather strange course
on algebraic number theory.

His central objects of study:
orders in number fields.
Primes, class groups, etc.

Normal textbooks and courses
focus on *maximal* orders,
i.e., orders without singularities:
"Have a non-maximal $\mathbf{Z}[x]/f$?
Yikes! Blow it up!"

Edwards curves

2007 Edwards:

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

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

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

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

2007 Bernstein–Lange:

Over a non-binary finite field k,
$x^2 + y^2 = c^2(1 + dx^2y^2)$
covers more elliptic curves.
Here $c, d \in k^*$ with $dc^4 \neq 1$.

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

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

Can always take $c = 1$. Then
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for addition,
$3\mathbf{M} + 4\mathbf{S}$ for doubling.

Latest news, comparisons:
hyperelliptic.org/EFD

Completeness

2007 Bernstein–Lange:

If d is not a square in k then
$\{(x, y) \in k \times k :$
$$x^2 + y^2 = c^2(1 + dx^2y^2)\}$$

is a commutative group
under this addition law.

The denominators
$c\,(1 + dx_1x_2y_1y_2)$,
$c\,(1 - dx_1x_2y_1y_2)$
are never zero.
No exceptional cases!

Compare to Weierstrass form
$y^2 = x^3 + a_4 x + a_6$.

Standard explicit formulas
for Weierstrass addition
have several different cases:
"chord"; "tangent";
vertical chord; etc.

Conventional wisdom:
Beyond genus 0,
explicit formulas for
multiplication in class group
always need case distinctions.

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

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 $E(\overline{k}) \times E(\overline{k})$, 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 $E(k)$.

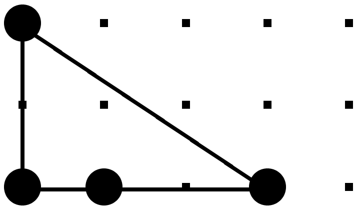
Completeness eases implementations, avoids some cryptographic problems.

What about elliptic curves without points of order 4? What about elliptic curves over binary fields?

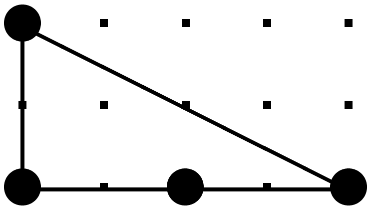
Continuing project (B.–L.): For *every* elliptic curve E, find complete addition law for E with best possible speeds.

Complete laws are useful even if slower than Edwards!

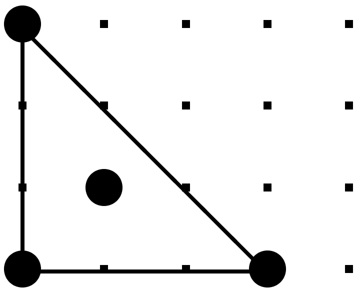
Some Newton polygons



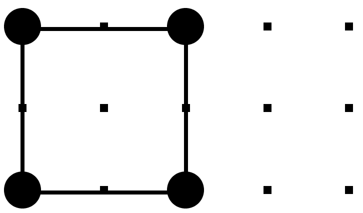
Short Weierstrass



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.

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

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:

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

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 $d_{22} X^2 Y^2 = 0$: i.e., $(1 : 0 : 0)$, $(0 : 1 : 0)$.

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

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.

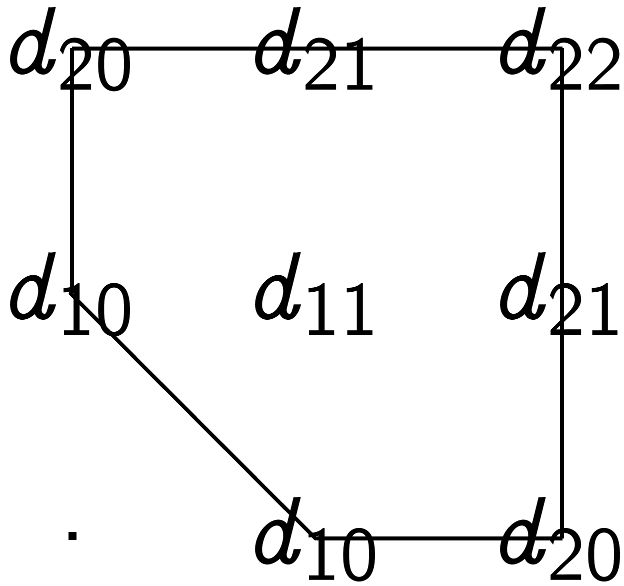
In particular $d_{20} \neq 0$:

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

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.

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 $d_1 = d_2$.

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

$$t = \begin{array}{r} 787510180411172525454209999954 \\ 767176464538545060814630202840 \\ 13956511758592017799 \end{array}$$

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:

$$x_3 = \frac{\begin{array}{l} x_1+x_2+(t-2)x_1x_2+ \\ (x_1-y_1)(x_2-y_2)+ \\ dx_1^2(x_2y_1+x_2y_2-y_1y_2) \end{array}}{\begin{array}{l} 1-2dx_1x_2y_2- \\ dx_1^2(x_2+y_2+(t-2)x_2y_2) \end{array}};$$

$$y_3 = \frac{\begin{array}{l} y_1+y_2+(t-2)y_1y_2+ \\ (y_1-x_1)(y_2-x_2)+ \\ dy_1^2(y_2x_1+y_2x_2-x_1x_2) \end{array}}{\begin{array}{l} 1-2dy_1y_2x_2- \\ dy_1^2(y_2+x_2+(t-2)y_2x_2) \end{array}}.$$

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: $x=v/(u^2-d)$;

$y=((t+2)u-v-d)/(u^2-d)$.

Completeness

$$x_3 = \frac{x_1 + x_2 + (t-2)x_1x_2 + (x_1 - y_1)(x_2 - y_2) + dx_1^2(x_2y_1 + x_2y_2 - y_1y_2)}{1 - 2dx_1x_2y_2 - dx_1^2(x_2 + y_2 + (t-2)x_2y_2)};$$

$$y_3 = \frac{y_1 + y_2 + (t-2)y_1y_2 + (y_1 - x_1)(y_2 - x_2) + dy_1^2(y_2x_1 + y_2x_2 - x_1x_2)}{1 - 2dy_1y_2x_2 - dy_1^2(y_2 + x_2 + (t-2)y_2x_2)}.$$

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;
$27d \neq (2-t)^3$;
$x_1^2 + y_1^2 = x_1 + y_1 + tx_1y_1 + dx_1^2y_1^2$;
$x_2^2 + y_2^2 = x_2 + y_2 + tx_2y_2 + dx_2^2y_2^2$.
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

$$1 - 2dx_1x_2y_2 - dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$$

Proof: Suppose that

$$1 - 2dx_1x_2y_2 - dx_1^2(x_2 + y_2 + (t-2)x_2y_2) = 0.$$

Note that $x_1 \neq 0$.

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$_1$ times $1/x_1^2$:

$1 + y_1^2/x_1^2 =$

$1/x_1 + y_1(1/x_1^2 + t/x_1) + dy_1^2$.

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 $1/x_1 = dx_2^2$:

$1 + d^2y_1^2x_2^4 =$

$dx_2^2 + dy_1(dx_2^4 + x_2^2t) + dy_1^2$.

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 $2x_2^2=2x_2+tx_2^2+dx_2^4$:

$(1-dy_1x_2^2)^2=d(x_2-y_1)^2$.

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 $1 = dx_2^3$.

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.