Edwards coordinates for elliptic curves

D. J. Bernstein
University of Illinois at Chicago

Joint work with:
Tanja Lange
Technische Universiteit Eindhoven

Weierstrass coordinates

Fix a field k with $2 \neq 0$.
Fix $a, b \in k$ with $4a^3 + 27b^2 \neq 0$.

Well-known fact:
The points of the "elliptic curve" $E : y^2 = x^3 + ax + b$ over k form a commutative group $E(k)$.

"So the group is $\{(x, y) \in k \times k : y^2 = x^3 + ax + b\}$?"

Not exactly! It's $\{(x, y) \in k \times k : y^2 = x^3 + ax + b\} \cup \{\infty\}$.

Weierstrass coordinates

Fix a field k with $2 \neq 0$.
Fix $a, b \in k$ with $4a^3 + 27b^2 \neq 0$.

Well-known fact:
The points of the "elliptic curve" $E : y^2 = x^3 + ax + b$ over k form a commutative group $E(k)$.

"So the group is $\{(x, y) \in k \times k : y^2 = x^3 + ax + b\}$?"

Not exactly! It's $\{(x, y) \in k \times k : y^2 = x^3 + ax + b\} \cup \{\infty\}$.

To add $(x_1, y_1), (x_2, y_2) \in E(k)$:

Define $x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (y_2 - y_1)/(x_2 - x_1)$.
Then $(x_3, y_3) \in E(k)$.

Geometric interpretation:
$(x_1, y_1), (x_2, y_2), (x_3, -y_3)$ are on the curve $y^2 = x^3 + ax + b$ and on a line;
$(x_3, y_3), (x_3, -y_3)$ are on a vertical line.

"So that's the group law? $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$?"

To add $(x_1, y_1), (x_2, y_2) \in E(k)$:

Define $x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (y_2 - y_1)/(x_2 - x_1)$.
Then $(x_3, y_3) \in E(k)$.

Geometric interpretation:
$(x_1, y_1), (x_2, y_2), (x_3, -y_3)$ are
on the curve $y^2 = x^3 + ax + b$
and on a line;
$(x_3, y_3), (x_3, -y_3)$ are
on a vertical line.

"So that's the group law?
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$?"

Not exactly! Definition of λ
assumes that $x_2 \neq x_1$.

To add $(x_1, y_1), (x_1, y_1) \in E(k)$:

Define $x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (3x_1^2 + a)/2y_1$.
Then $(x_3, y_3) \in E(k)$.

Geometric interpretation:
The curve's tangent line at
(x_1, y_1) passes through $(x_3, -y_3)$.

"So that's the group law?
One special case for doubling?"

Not exactly! Definition of λ assumes that $x_2 \neq x_1$.

To add $(x_1, y_1), (x_1, y_1) \in E(k)$:

Define $x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (3x_1^2 + a)/2y_1$.
Then $(x_3, y_3) \in E(k)$.

Geometric interpretation:
The curve's tangent line at (x_1, y_1) passes through $(x_3, -y_3)$.

"So that's the group law? One special case for doubling?"

Not exactly! More exceptions: e.g., y_1 could be 0.

Six cases overall: $\infty + \infty = \infty$;
$\infty + (x_2, y_2) = (x_2, y_2)$;
$(x_1, y_1) + \infty = (x_1, y_1)$;
$(x_1, y_1) + (x_1, -y_1) = \infty$;
for $y_1 \neq 0$, $(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ with $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, $\lambda = (3x_1^2 + a)/2y_1$;
for $x_1 \neq x_2$, $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

Not exactly! More exceptions:
e.g., y_1 could be 0.

Six cases overall: $\infty + \infty = \infty$;
$\infty + (x_2, y_2) = (x_2, y_2)$;
$(x_1, y_1) + \infty = (x_1, y_1)$;
$(x_1, y_1) + (x_1, -y_1) = \infty$;
for $y_1 \neq 0$, $(x_1, y_1) + (x_1, y_1) =$
(x_3, y_3) with $x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,
$\lambda = (3x_1^2 + a)/2y_1$;
for $x_1 \neq x_2$, $(x_1, y_1) + (x_2, y_2) =$
(x_3, y_3) with $x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,
$\lambda = (y_2 - y_1)/(x_2 - x_1)$.

$E(k)$ is a commutative group:

Has neutral element ∞, and $-$:
$-\infty = \infty$; $-(x, y) = (x, -y)$.

Commutativity: $P + Q = Q + P$.

Associativity:
$(P + Q) + R = P + (Q + R)$.
Straightforward but tedious:
use a computer-algebra system
to check each possible case.
Or relate each $P + Q$ case
to "ideal-class product."
Many other proofs,
but can't escape case analysis.

$E(k)$ is a commutative group:

Has neutral element ∞, and $-$:
$-\infty = \infty$; $-(x, y) = (x, -y)$.

Commutativity: $P + Q = Q + P$.

Associativity:
$(P + Q) + R = P + (Q + R)$.
Straightforward but tedious:
use a computer-algebra system
to check each possible case.
Or relate each $P + Q$ case
to "ideal-class product."
Many other proofs,
but can't escape case analysis.

Projective coordinates

Can eliminate some exceptions.

Define $(X : Y : Z)$, for
$(X, Y, Z) \in k \times k \times k - \{(0, 0, 0)\}$,
as $\{(rX, rY, rZ) : r \in k - \{0\}\}$.

Could split into cases:
$(X : Y : Z) =$
$(X/Z : Y/Z : 1)$ if $Z \neq 0$;
$(X : Y : 0) =$
$(X/Y : 1 : 0)$ if $Y \neq 0$;
$(X : 0 : 0) = (1 : 0 : 0)$.
But scaling unifies all cases.

Projective coordinates

Can eliminate some exceptions.

Define $(X : Y : Z)$, for $(X, Y, Z) \in k \times k \times k - \{(0, 0, 0)\}$, as $\{(rX, rY, rZ) : r \in k - \{0\}\}$.

Could split into cases:

$(X : Y : Z) =$
$(X/Z : Y/Z : 1)$ if $Z \neq 0$;

$(X : Y : 0) =$
$(X/Y : 1 : 0)$ if $Y \neq 0$;

$(X : 0 : 0) = (1 : 0 : 0)$.

But scaling unifies all cases.

Write $\mathbf{P}^2(k) = \{(X : Y : Z)\}$.

Revised definition: $E(k) = \{(X : Y : Z) \in \mathbf{P}^2(k) : Y^2Z = X^3 + aXZ^2 + bZ^3\}$.

Could split into cases:

If $(X : Y : Z) \in E(k)$ and $Z \neq 0$: $(X : Y : Z) = (x : y : 1)$ where $x = X/Z$, $y = Y/Z$. Note that $y^2 = x^3 + ax + b$. Corresponds to previous (x, y).

If $(X : Y : Z) \in E(k)$ and $Z = 0$: $X^3 = 0$ so $X = 0$ so $Y \neq 0$ so $(X : Y : Z) = (0 : 1 : 0)$. Corresponds to previous ∞.

Write $\mathbf{P}^2(k) = \{(X : Y : Z)\}$.
Revised definition: $E(k) = \{(X : Y : Z) \in \mathbf{P}^2(k) : Y^2 Z = X^3 + aXZ^2 + bZ^3\}$.

Could split into cases:

If $(X : Y : Z) \in E(k)$ and $Z \neq 0$:
$(X : Y : Z) = (x : y : 1)$
where $x = X/Z$, $y = Y/Z$.
Note that $y^2 = x^3 + ax + b$.
Corresponds to previous (x, y).

If $(X : Y : Z) \in E(k)$ and $Z = 0$:
$X^3 = 0$ so $X = 0$ so $Y \neq 0$
so $(X : Y : Z) = (0 : 1 : 0)$.
Corresponds to previous ∞.

$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$ where
$U = Y_2 Z_1 - Y_1 Z_2$,
$V = X_2 Z_1 - X_1 Z_2$,
$W = U^2 Z_1 Z_2 - V^3 - 2V^2 X_1 Z_2$,
$X_3 = VW$,
$Y_3 = U(V^2 X_1 Z_2 - W) - V^3 Y_1 Z_2$,
$Z_3 = V^3 Z_1 Z_2$.

"Aha! No more divisions by 0."

Compare to previous formulas:
$x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$
$= (X_3 : Y_3 : Z_3)$ where
$U = Y_2 Z_1 - Y_1 Z_2$,
$V = X_2 Z_1 - X_1 Z_2$,
$W = U^2 Z_1 Z_2 - V^3 - 2V^2 X_1 Z_2$,
$X_3 = VW$,
$Y_3 = U(V^2 X_1 Z_2 - W) - V^3 Y_1 Z_2$,
$Z_3 = V^3 Z_1 Z_2$.

"Aha! No more divisions by 0."

Compare to previous formulas:
$x_3 = \lambda^2 - x_1 - x_2$
and $y_3 = \lambda(x_1 - x_3) - y_1$
where $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

Oops, still have exceptions!

Formulas give bogus
$(X_3, Y_3, Z_3) = (0, 0, 0)$
if $(X_1 : Y_1 : Z_1) = (0 : 1 : 0)$.

Same problem for doubling.

Formulas produce $(0 : 1 : 0)$ for
$(X_1 : Y_1 : Z_1) + (X_1 : -Y_1 : Z_1)$
if $Y_1 \neq 0$ and $Z_1 \neq 0$
but not if $Y_1 = 0$.

To define complete group law,
use six cases as before.

Oops, still have exceptions!

Formulas give bogus $(X_3, Y_3, Z_3) = (0, 0, 0)$ if $(X_1 : Y_1 : Z_1) = (0 : 1 : 0)$.

Same problem for doubling.

Formulas produce $(0 : 1 : 0)$ for $(X_1 : Y_1 : Z_1) + (X_1 : -Y_1 : Z_1)$ if $Y_1 \neq 0$ and $Z_1 \neq 0$ but not if $Y_1 = 0$.

To define complete group law, use six cases as before.

Jacobian coordinates

"Weighted projective coordinates using weights $2, 3, 1$":

Redefine $(X : Y : Z)$ as $\{(r^2X, r^3Y, rZ) : r \in k - \{0\}\}$.

Redefine $E(k)$ using $Y^2 = X^3 + aXZ^4 + bZ^6$.

Could again split into cases for $(X : Y : Z) \in E(k)$: if $Z \neq 0$ then $(X : Y : Z) = (X/Z^2 : Y/Z^3 : 1)$; if $Z = 0$ then $(X : Y : Z) = (1 : 1 : 0)$.

Jacobian coordinates

"Weighted projective coordinates using weights $2, 3, 1$":

Redefine $(X : Y : Z)$ as $\{(r^2X, r^3Y, rZ) : r \in k - \{0\}\}$.

Redefine $E(k)$ using $Y^2 = X^3 + aXZ^4 + bZ^6$.

Could again split into cases for $(X : Y : Z) \in E(k)$: if $Z \neq 0$ then $(X : Y : Z) = (X/Z^2 : Y/Z^3 : 1)$; if $Z = 0$ then $(X : Y : Z) = (1 : 1 : 0)$.

$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$
$= (X_3 : Y_3 : Z_3)$ where
$U_1 = X_1Z_2^2$, $U_2 = X_2Z_1^2$,
$S_1 = Y_1Z_2^3$, $S_2 = Y_2Z_1^3$,
$H = U_2 - U_1$, $J = S_2 - S_1$,
$X_3 = -H^3 - 2U_1H^2 + J^2$,
$Y_3 = -S_1H^3 + J(U_1H^2 - X_3)$,
$Z_3 = Z_1Z_2H$.

Streamlined algorithm uses 16 multiplications, of which 4 are squarings. (1986 Chudnovsky/Chudnovsky)

5 squarings. (2001 Bernstein)

$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$
$= (X_3 : Y_3 : Z_3)$ where
$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,
$H = U_2 - U_1$, $J = S_2 - S_1$,
$X_3 = -H^3 - 2U_1 H^2 + J^2$,
$Y_3 = -S_1 H^3 + J(U_1 H^2 - X_3)$,
$Z_3 = Z_1 Z_2 H$.

Streamlined algorithm
uses 16 multiplications,
of which 4 are squarings.
(1986 Chudnovsky/Chudnovsky)

5 squarings. (2001 Bernstein)

Still need all six cases.

Why use Jacobian coordinates?
8 mults (including 5 squarings)
for Jacobian-coordinate doubling
if $a = -3$ (e.g. NIST's curves):

If $Y_1 \neq 0$ then
$(X_1 : Y_1 : Z_1) + (X_1 : Y_1 : Z_1)$
$= (X_3, Y_3, Z_3)$ where
$T = Z_1^2$, $U = Y_1^2$, $V = X_1 U$,
$W = 3(X_1 - T)(X_1 + T)$,
$X_3 = W^2 - 8V$,
$Z_3 = (Y_1 + Z_1)^2 - U - T$,
$Y_3 = W(4V - X_3) - 8U^2$.

Still need all six cases.

Why use Jacobian coordinates?
8 mults (including 5 squarings)
for Jacobian-coordinate doubling
if $a = -3$ (e.g. NIST's curves):

If $Y_1 \neq 0$ then
$(X_1 : Y_1 : Z_1) + (X_1 : Y_1 : Z_1)$
$= (X_3, Y_3, Z_3)$ where
$T = Z_1^2$, $U = Y_1^2$, $V = X_1 U$,
$W = 3(X_1 - T)(X_1 + T)$,
$X_3 = W^2 - 8V$,
$Z_3 = (Y_1 + Z_1)^2 - U - T$,
$Y_3 = W(4V - X_3) - 8U^2$.

Unified addition laws

Do addition laws
have to fail for doublings?
Not necessarily!

Example: "Jacobi intersection"
$s^2 + c^2 = t^2$, $as^2 + d^2 = t^2$
has 17-multiplication addition
formula that works for doublings.
(1986 Chudnovsky/Chudnovsky)

16. (2001 Liardet/Smart)

Many more "unified formulas."
But always find exceptions:
points not added by formulas.

Unified addition laws

Do addition laws have to fail for doublings? Not necessarily!

Example: "Jacobi intersection" $s^2 + c^2 = t^2$, $as^2 + d^2 = t^2$ has 17-multiplication addition formula that works for doublings. (1986 Chudnovsky/Chudnovsky)

16. (2001 Liardet/Smart)

Many more "unified formulas." But always find exceptions: points not added by formulas.

Do we need 6 cases? No!

Can cover $E(k) \times E(k)$ using 3 addition laws. (1985 H. Lange/Ruppert)

How about just *one* law that covers $E(k) \times E(k)$? One complete addition law?

Bad news: "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma/H. Lenstra)

Do we need 6 cases? No!

Can cover $E(k) \times E(k)$
using 3 addition laws.
(1985 H. Lange/Ruppert)

How about just *one* law
that covers $E(k) \times E(k)$?
One complete addition law?

Bad news: "Theorem 1.
The smallest cardinality of a
complete system of addition laws
on E equals two."
(1995 Bosma/H. Lenstra)

Interlude: The circle

Fix a field k with $2 \neq 0$.
Fix $c \in k$ with $c \neq 0$.

$\{(x, y) \in k \times k : x^2 + y^2 = c^2\}$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
where $x_3 = (x_1 y_2 + y_1 x_2)/c$
and $y_3 = (y_1 y_2 - x_1 x_2)/c$.

Exercise: on curve.
Exercise: associative.

Look, a complete addition law!
But it's not elliptic.

Interlude: The circle

Fix a field k with $2 \neq 0$.
Fix $c \in k$ with $c \neq 0$.

$\{(x, y) \in k \times k : x^2 + y^2 = c^2\}$
is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
where $x_3 = (x_1 y_2 + y_1 x_2)/c$
and $y_3 = (y_1 y_2 - x_1 x_2)/c$.

Exercise: on curve.
Exercise: associative.

Look, a complete addition law!
But it's not elliptic.

Edwards curves

Fix a field k with $2 \neq 0$.
Fix $c, d \in k$ with $cd(1 - dc^4) \neq 0$
and with d not a square.

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

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{c(1 + dx_1x_2y_1y_2)},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{c(1 - dx_1x_2y_1y_2)}.$$

Edwards curves

Fix a field k with $2 \neq 0$.
Fix $c, d \in k$ with $cd(1 - dc^4) \neq 0$ and with d not a square.

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

is a commutative group with $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ defined by Edwards addition law:

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

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

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = c^2(1 + dx_1^2y_1^2)$ and $x_2^2 + y_2^2 = c^2(1 + dx_2^2y_2^2)$ then $dx_1x_2y_1y_2$ can't be ± 1.

Outline of proof:
If $(dx_1x_2y_1y_2)^2 = 1$ then curve equation implies $(x_1 + dx_1x_2y_1y_2y_1)^2 = dx_1^2y_1^2(x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = c^2(1 + dx_1^2 y_1^2)$
and $x_2^2 + y_2^2 = c^2(1 + dx_2^2 y_2^2)$
then $dx_1x_2y_1y_2$ can't be ± 1.

Outline of proof:
If $(dx_1x_2y_1y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1x_2y_1y_2y_1)^2 =$
$dx_1^2y_1^2(x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

So (x_3, y_3) is always defined:

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

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

Neutral element $(0, c)$.
Commutative. $-(x, y) = (-x, y)$.

Exercise: on curve.

Exercise: associative.

Magma computer-algebra system
solves both exercises in 20 secs.

So (x_3, y_3) is always defined:

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{c(1 + d x_1 x_2 y_1 y_2)},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{c(1 - d x_1 x_2 y_1 y_2)}.$$

Neutral element $(0, c)$.
Commutative. $-(x, y) = (-x, y)$.

Exercise: on curve.

Exercise: associative.

Magma computer-algebra system solves both exercises in 20 secs.

Is this elliptic (after desingularization)? Yes!

Transform to $z^2 =$ quartic:
$y^2(1 - dc^2x^2) = c^2 - x^2$
so $z^2 = (1 - dc^2x^2)(c^2 - x^2)$
where $z = y(1 - dc^2x^2)$.

Or transform to $v^2 =$ cubic:
$v^2 = eu^3 + (4 - 2e)u^2 + eu$
where $u = (c + y)/(c - y)$,
$v = 2cu/x$, $e = 1 - dc^4$.

Obtain every elliptic curve having a point of order 4 and a unique point of order 2.

Is this elliptic
(after desingularization)? Yes!

Transform to $z^2 =$ quartic:
$y^2(1 - dc^2x^2) = c^2 - x^2$
so $z^2 = (1 - dc^2x^2)(c^2 - x^2)$
where $z = y(1 - dc^2x^2)$.

Or transform to $v^2 =$ cubic:
$v^2 = eu^3 + (4 - 2e)u^2 + eu$
where $u = (c + y)/(c - y)$,
$v = 2cu/x$, $e = 1 - dc^4$.

Obtain every elliptic curve
having a point of order 4
and a unique point of order 2.

So many elliptic curves have a
complete addition law.

What about Bosma/Lenstra?
Recall "Theorem 1.
The smallest cardinality of a
complete system of addition laws
on E equals two."

"Complete" in the theorem
means "covers $E(\overline{k}) \times E(\overline{k})$";
$\overline{k}$ is the algebraic closure of k.

The Edwards addition law has
exceptions defined over $k(\sqrt{d})$,
but no exceptions defined over k.

So many elliptic curves have a complete addition law.

What about Bosma/Lenstra? Recall "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two."

"Complete" in the theorem means "covers $E(\overline{k}) \times E(\overline{k})$"; $\overline{k}$ is the algebraic closure of k.

The Edwards addition law has exceptions defined over $k(\sqrt{d})$, but no exceptions defined over k.

Historical notes on the addition law:

Euler/Gauss: $c = 1$, $d = -1$ over field with $\sqrt{-1}$.

2007 Edwards: $d = 1$, general c. Theorem: over $\overline{k}$, obtain all elliptic curves.

2007 Bernstein/Lange: general d. In particular: complete for non-square d. Also streamlined formulas, coming next!

Historical notes
on the addition law:

Euler/Gauss: $c = 1$, $d = -1$
over field with $\sqrt{-1}$.

2007 Edwards: $d = 1$, general c.
Theorem: over $\overline{k}$,
obtain all elliptic curves.

2007 Bernstein/Lange:
general d. In particular:
complete for non-square d.
Also streamlined formulas,
coming next!

Computations on Edwards curves

Take $c = 1$ for simplicity, speed;
no loss of generality.

To avoid divisions, use
$(X : Y : Z)$ with $Z \neq 0$ and
$(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$ to
represent $(X/Z, Y/Z)$ on Edwards
curve $x^2 + y^2 = 1 + dx^2y^2$.

Edwards addition law (for $c = 1$):

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

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

Computations on Edwards curves

Take $c = 1$ for simplicity, speed; no loss of generality.

To avoid divisions, use $(X : Y : Z)$ with $Z \neq 0$ and $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$ to represent $(X/Z, Y/Z)$ on Edwards curve $x^2 + y^2 = 1 + dx^2y^2$.

Edwards addition law (for $c = 1$):

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

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

Clear denominators:

$$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2) \cdot (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2),$$
$$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2) \cdot (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2),$$
$$Z_3 = (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \cdot (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2).$$

Rewrite $x_1y_2 + x_2y_1$ as $(x_1 + y_1)(x_2 + y_2) - x_1x_2 - y_1y_2$, exploit common subexpressions.

12 multiplications (one by d, one a squaring), 7 additions. Still complete.

Clear denominators:

$$X_3 = Z_1 Z_2 (X_1 Y_2 + Y_1 X_2) \cdot (Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2),$$
$$Y_3 = Z_1 Z_2 (Y_1 Y_2 - X_1 X_2) \cdot (Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2),$$
$$Z_3 = (Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2) \cdot (Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2).$$

Rewrite $x_1 y_2 + x_2 y_1$ as $(x_1 + y_1)(x_2 + y_2) - x_1 x_2 - y_1 y_2$, exploit common subexpressions.

12 multiplications (one by d, one a squaring), 7 additions. Still complete.

Comparison of addition costs if curve parameters are small:

System	Cost
Jacobian	$11\mathbf{M} + 5\mathbf{S}$
Jacobi intersection	$13\mathbf{M} + 2\mathbf{S}$
Projective	$12\mathbf{M} + 2\mathbf{S}$
Chudnovsky caching	$10\mathbf{M} + 4\mathbf{S}$
Jacobi quartic	$10\mathbf{M} + 3\mathbf{S}$
Hessian	$12\mathbf{M}$
Edwards	$10\mathbf{M} + 1\mathbf{S}$

Comparison of addition costs

if curve parameters are small:

System	Cost
Jacobian	$11\mathbf{M} + 5\mathbf{S}$
Jacobi intersection	$13\mathbf{M} + 2\mathbf{S}$
Projective	$12\mathbf{M} + 2\mathbf{S}$
Chudnovsky caching	$10\mathbf{M} + 4\mathbf{S}$
Jacobi quartic	$10\mathbf{M} + 3\mathbf{S}$
Hessian	$12\mathbf{M}$
Edwards	$10\mathbf{M} + 1\mathbf{S}$

Can save time in doubling:

rewrite $1 + dx_1^2y_1^2$ as $x_1^2 + y_1^2$

(as suggested by Marc Joye);

rewrite $1 - dx_1^2y_1^2$ as $2 - x_1^2 - y_1^2$;

exploit common subexpressions.

$B = (X_1+Y_1)^2$, $C = X_1^2$, $D = Y_1^2$,

$E = C + D$, $H = Z_1^2$,

$J = E - 2H$, $X_3 = (B - E)J$,

$Y_3 = E(C - D)$, $Z_3 = EJ$.

7 multiplications

(4 of which are squarings),

6 additions.

Can save time in doubling:
rewrite $1 + dx_1^2y_1^2$ as $x_1^2 + y_1^2$
(as suggested by Marc Joye);
rewrite $1 - dx_1^2y_1^2$ as $2 - x_1^2 - y_1^2$;
exploit common subexpressions.

$B = (X_1+Y_1)^2$, $C = X_1^2$, $D = Y_1^2$,
$E = C + D$, $H = Z_1^2$,
$J = E - 2H$, $X_3 = (B - E)J$,
$Y_3 = E(C - D)$, $Z_3 = EJ$.

7 multiplications
(4 of which are squarings),
6 additions.

Comparison of doubling costs
if curve parameters are small:

System	Cost
Projective	5**M** + 6**S**
Projective if $a = -3$	7**M** + 3**S**
Hessian	6**M** + 3**S**
Jacobi quartic	1**M** + 9**S**
Jacobian	1**M** + 8**S**
Jacobian if $a = -3$	3**M** + 5**S**
Jacobi intersection	3**M** + 4**S**
Edwards	3**M** + 4**S**

Comparison of doubling costs if curve parameters are small:

System	Cost
Projective	$5\mathbf{M} + 6\mathbf{S}$
Projective if $a = -3$	$7\mathbf{M} + 3\mathbf{S}$
Hessian	$6\mathbf{M} + 3\mathbf{S}$
Jacobi quartic	$1\mathbf{M} + 9\mathbf{S}$
Jacobian	$1\mathbf{M} + 8\mathbf{S}$
Jacobian if $a = -3$	$3\mathbf{M} + 5\mathbf{S}$
Jacobi intersection	$3\mathbf{M} + 4\mathbf{S}$
Edwards	$3\mathbf{M} + 4\mathbf{S}$

A cryptographic example

"Curve25519":
$v^2 = u^3 + 486662u^2 + u$
over the field $k = \mathbf{Z}/(2^{255} - 19)$.
Software speed records for elliptic-curve Diffie-Hellman.
(2005 Bernstein)

$n, P \mapsto nP$ is very fast using Montgomery coordinates.
(1987 Montgomery)

$n_0, n_1, P_0, P_1 \mapsto n_0 P_0 + n_1 P_1$?
Critical for digital signatures.
Batch verification: many n_i's.

A cryptographic example

"Curve25519":
$v^2 = u^3 + 486662u^2 + u$
over the field $k = \mathbf{Z}/(2^{255} - 19)$.
Software speed records for elliptic-curve Diffie-Hellman.
(2005 Bernstein)

$n, P \mapsto nP$ is very fast using Montgomery coordinates.
(1987 Montgomery)

$n_0, n_1, P_0, P_1 \mapsto n_0 P_0 + n_1 P_1$?
Critical for digital signatures.
Batch verification: many n_i's.

Multi-scalar multiplication:
Montgomery isn't very fast.
Jacobian is faster.
Edwards is the new winner!

Curve25519 is equivalent over k to the Edwards curve
$x^2 + y^2 = 1 + (1 - 1/121666)x^2y^2$.

Transformation is easy:
$x = \sqrt{486664}u/v$,
$y = (u-1)/(u+1)$.
Map points to Edwards curve.
Use Edwards addition law.
Map back to Curve25519—
or use Edwards everywhere!

Multi-scalar multiplication:
Montgomery isn't very fast.
Jacobian is faster.
Edwards is the new winner!

Curve25519 is equivalent over k to the Edwards curve $x^2+y^2=1+(1-1/121666)x^2y^2$.

Transformation is easy:
$x=\sqrt{486664}u/v$,
$y=(u-1)/(u+1)$.
Map points to Edwards curve.
Use Edwards addition law.
Map back to Curve25519—
or use Edwards everywhere!

What about $n \mapsto nQ$ using standard $Q=(9,\ldots)$?
Faster than $n, P \mapsto nP$?

If $n=n_0+2^{16}n_1+\cdots$
then $nQ=n_0Q+2^{16}n_1Q+\cdots$.
Precompute $2^{16}Q$ etc.
Use multi-scalar multiplication.

Edwards curves work well for all of these applications.
Very fast doublings.
Very fast additions.
Complete addition law helps stop secrets from leaking through side channels.

What about $n \mapsto nQ$
using standard $Q = (9, \ldots)$?
Faster than $n, P \mapsto nP$?

If $n = n_0 + 2^{16}n_1 + \cdots$
then $nQ = n_0Q + 2^{16}n_1Q + \cdots$.
Precompute $2^{16}Q$ etc.
Use multi-scalar multiplication.

Edwards curves work well for
all of these applications.
Very fast doublings.
Very fast additions.
Complete addition law
helps stop secrets from
leaking through side channels.

More on Edwards curves:

`http://cr.yp.to`
`/newelliptic.html`