Faster formulas for elliptic curves

Hüseyin Hışıl
hisil.huseyin@gmail.com
www.huseyinhisil.net

ECC2010, Redmond

Faster formulas for elliptic curves (A roadmap for formula-hunters)

Hüseyin Hışıl
hisil.huseyin@gmail.com
www.huseyinhisil.net

ECC2010, Redmond

Faster formulas for elliptic curves (A roadmap for formula-hunters) (A roadmap for lazy formula-hunters)

Hüseyin Hışıl
hisil.huseyin@gmail.com
www.huseyinhisil.net

ECC2010, Redmond

Outline

1. Overview
2. Automated tools
3. Inversion-free point addition
4. Conclusion

The classics

1 [CC86] Chudnovsky and Chudnovsky. *Sequences of numbers generated by addition in formal groups and new primality and factorization tests.* Advances in Applied Mathematics, 1986.

2 [Mon87] Montgomery. *Speeding the Pollard and elliptic curve methods of factorization.* Mathematics of Computation, 1987.

3 [CMO98] Cohen, Miyaji, and Ono. *Efficient elliptic curve exponentiation using mixed coordinates.* ASIACRYPT'98.

Remarkable strikes aganist the cubic

1. [LS01] Liardet and Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form.* CHES 2001.

2. [BL07b] Bernstein and Lange, *Faster addition and doubling on elliptic curves.* ASIACRYPT 2007.

Note: There are other papers not listed here.

This investigation

Concrete results for:

1. Short Weierstrass form, $y^2 = x^3 + ax + b$,
2. Extended Jacobi quartic form, $y^2 = dx^4 + 2ax^2 + 1$,
3. Twisted Hessian form, $ax^3 + y^3 + 1 = dxy$,
4. Twisted Edwards form, $ax^2 + y^2 = 1 + dx^2y^2$,
5. Twisted Jacobi intersection form, $bs^2 + c^2 = 1, as^2 + d^2 = 1$.

In fact, many other forms are checked for a better efficiency along the way.

Extended Jacobi quartic curves will be used in all examples in the remainder of the talk.

Extended Jacobi quartics overview

$\mathbb{K}$ denotes a field of odd characteristic.

Definition

An extended Jacobi quartic curve defined over $\mathbb{K}$ is the curve

$$E_{\mathbf{Q},d,a} := \{(x,y) \in \mathbb{A}^2(\overline{\mathbb{K}}) \mid y^2 = dx^4 + 2ax^2 + 1\}.$$

$E_{\mathbf{Q}}$ is non-singular if and only if $d(a^2 - d) \neq 0$.
The projective closure of $E_{\mathbf{Q}}$ is given by the equation

$$\overline{E}_{\mathbf{Q},d,a} : \; Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4.$$

A point $(X : Y : Z)$ with $Z \neq 0$ on $\overline{E}_{\mathbf{Q}}$ corresponds to the affine point $(X/Z, Y/Z)$ on $E_{\mathbf{Q}}$. The point $(0 : 1 : 0)$ on $\overline{E}_{\mathbf{Q}}$ is singular. The resolution of singularities produces two points which are labeled as Ω_1 and Ω_2. These points are defined over $\mathbb{K}(\sqrt{d})$.

Extended Jacobi quartics overview

Let $\mathbb{L} = \mathbb{K}(\sqrt{d})$. With a slight abuse of notation, $\overline{E}_{\mathbf{Q}}(\mathbb{L})$, the set of $\mathbb{L}$-rational points on $\overline{E}_{\mathbf{Q}}$ is denoted by

$$E_{\mathbf{Q}}(\mathbb{L}) = \{(x,y) \in \mathbb{L}^2 \mid y^2 = dx^4 + 2ax^2 + 1\} \cup \{\Omega_1, \Omega_2\}.$$

$E_{\mathbf{Q},d,a}$ is birationally equivalent over $\mathbb{K}$ to the Weierstrass curve

$$E_{\mathbf{W}} : \; v^2 = u^3 - 4au^2 + (4a^2 - 4d)u$$

with the maps

$$\psi : E_{\mathbf{Q}} \to E_{\mathbf{W}}, \; (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$

$$\phi : E_{\mathbf{W}} \to E_{\mathbf{Q}}, \; (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

Extended Jacobi quartics overview

$$\psi\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

Extended Jacobi quartics overview

$$\psi\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

It is trivial to check that $\phi \circ \psi = \mathrm{id}_{E_{\mathbf{Q}}}$ and $\psi \circ \phi = \mathrm{id}_{E_{\mathbf{W}}}$.
The map ψ is regular at all points on $E_{\mathbf{Q}}$ except $(0,1)$ which corresponds to ∞ on $\overline{E}_{\mathbf{W}}$.

Extended Jacobi quartics overview

$$\psi\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

It is trivial to check that $\phi \circ \psi = \mathrm{id}_{E_{\mathbf{Q}}}$ and $\psi \circ \phi = \mathrm{id}_{E_{\mathbf{W}}}$.
The map ψ is regular at all points on $E_{\mathbf{Q}}$ except $(0,1)$ which corresponds to ∞ on $\overline{E}_{\mathbf{W}}$. At first glance, it may seem that ψ is not regular at $(0,-1)$. However, it is possible to alter ψ to successfully map all points on $E_{\mathbf{Q}}$ except $(0,1)$. For instance, the point $(0,-1)$ can be sent to $(0,0)$ on $E_{\mathbf{W}}$ with an alternative map given by

$$\psi'\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2dx^2 + 2a(1+y)}{y-1}, \frac{4a(dx^2+2a) - 4d(1-y)}{(1-y)^2}x\right).$$

Extended Jacobi quartics overview

$$\psi\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$

$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

The map ϕ is regular at all points on $E_{\mathbf{W}}$ except in two cases. Before investigating these cases observe that the point $(0,0)$ on $E_{\mathbf{W}}:\ v^2 = u^3 - 4au^2 + (4a^2 - 4d)u$ can be sent to $(0,-1)$ on $E_{\mathbf{Q}}$ with an alternative map given by

$$\phi'\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(\frac{2v}{(u-2a)^2 - 4d}, \frac{u^2 - 4(a^2-d)}{(u-2a)^2 - 4d}\right).$$

Extended Jacobi quartics overview

$$\psi\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$
$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

The map ϕ is regular at all points on $E_{\mathbf{W}}$ except in two cases. Before investigating these cases observe that the point $(0,0)$ on $E_{\mathbf{W}}:\ v^2 = u^3 - 4au^2 + (4a^2 - 4d)u$ can be sent to $(0,-1)$ on $E_{\mathbf{Q}}$ with an alternative map given by

$$\phi'\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(\frac{2v}{(u-2a)^2 - 4d}, \frac{u^2 - 4(a^2-d)}{(u-2a)^2 - 4d}\right).$$

The map ϕ is not regular at two points of the form (u,v) with $u \neq 0$ and $v = 0$. These exceptional points correspond to two points at infinity on the desingularization of $\overline{E}_{\mathbf{Q}}$.

Extended Jacobi quartics overview

$$\psi\colon E_{\mathbf{Q}} \to E_{\mathbf{W}},\ (x,y) \mapsto \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right),$$
$$\phi\colon E_{\mathbf{W}} \to E_{\mathbf{Q}},\ (u,v) \mapsto \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

Note: ϕ is a morphism if d is a non-square in $\mathbb{K}$.

Extended Jacobi quartics overview

Every Weierstrass curve

$$v^2 = u^3 + a_2u^2 + a_4u$$

is birationally equivalent over $\mathbb{K}$ to

$$y^2 = \frac{a_2^2 - 4a_4}{16}x^4 - \frac{a_2}{2}x^2 + 1.$$

The shape $v^2 = u^3 + a_2u^2 + a_4u$ covers all elliptic curves having at least one point of order two.

Therefore every elliptic curve of even order can be written in extended Jacobi quartic form.

This extended model covers approximately $1.33\#\mathbb{K}$ of $2\#\mathbb{K}$ isomorphism classes (assuming $\mathbb{K}$ is finite).

Extended Jacobi quartics overview

Every Weierstrass curve

$$v^2 = u^3 + a_2u^2 + a_4u$$

is birationally equivalent over $\mathbb{K}$ to

$$y^2 = \frac{a_2^2 - 4a_4}{16}x^4 - \frac{a_2}{2}x^2 + 1.$$

The shape $v^2 = u^3 + a_2u^2 + a_4u$ covers all elliptic curves having at least one point of order two.

Therefore every elliptic curve of even order can be written in extended Jacobi quartic form.

This extended model covers approximately $1.33\#\mathbb{K}$ of $2\#\mathbb{K}$ isomorphism classes (assuming $\mathbb{K}$ is finite).

Outline

1. Overview
2. Automated tools
3. Inversion-free point addition
4. Conclusion

Automated Tools

Develop tools to:

1. Automate group law derivation algorithmically.
2. Automate minimal/low degree point doubling/addition formulas derivation.
3. Verify the correctness of derived formulas.
4. Find alternative formulas.

Automated Tools

Theorem (Automated Addition)

Let $W/\mathbb{K}$ and $M/\mathbb{K}$ be affine curves. Assume that W and M are birationally equivalent over $\mathbb{K}$. Let $\phi : W \to M$ and $\psi : M \to W$ be maps such that $\phi \circ \psi$ and $\psi \circ \phi$ are equal to the identity maps id_M and id_W, respectively.

Assume that $\tilde{W}$ and $\tilde{M}$, each with a distinguished $\mathbb{K}$-rational point, are elliptic curves. Let $+_W : W \times W \to W$ be a map which is regular at all but finitely many pairs of points on W, describing some part of the unique addition law on $\tilde{W}$.

The corresponding part of the unique addition law on $\tilde{M}$ is then given by the compositions

$$+_M \quad := \quad \phi \circ +_W \circ (\psi \times \psi)$$

and $+_M$ is regular at all but finitely many pairs of points on M.

Automated Tools

Theorem (Automated Addition)

Let $W/\mathbb{K}$ and $M/\mathbb{K}$ be affine curves. Assume that W and M are birationally equivalent over $\mathbb{K}$. Let $\phi : W \to M$ and $\psi : M \to W$ be maps such that $\phi \circ \psi$ and $\psi \circ \phi$ are equal to the identity maps id_M and id_W, respectively.

Assume that $\tilde{W}$ and $\tilde{M}$, each with a distinguished $\mathbb{K}$-rational point, are elliptic curves. Let $+_W : W \times W \to W$ be a map which is regular at all but finitely many pairs of points on W, describing some part of the unique addition law on $\tilde{W}$.

The corresponding part of the unique addition law on $\tilde{M}$ is then given by the compositions

$$+_M \quad := \quad \phi \circ +_W \circ (\psi \times \psi)$$

and $+_M$ is regular at all but finitely many pairs of points on M.

Automated Tools

Theorem (Automated Addition)

Let $W/\mathbb{K}$ and $M/\mathbb{K}$ be affine curves. Assume that W and M are birationally equivalent over $\mathbb{K}$. Let $\phi : W \to M$ and $\psi : M \to W$ be maps such that $\phi \circ \psi$ and $\psi \circ \phi$ are equal to the identity maps id_M and id_W, respectively.

Assume that $\tilde{W}$ and $\tilde{M}$, each with a distinguished $\mathbb{K}$-rational point, are elliptic curves. Let $+_W : W \times W \to W$ be a map which is regular at all but finitely many pairs of points on W, describing some part of the unique addition law on $\tilde{W}$.

The corresponding part of the unique addition law on $\tilde{M}$ is then given by the compositions

$$+_M \quad := \quad \phi \circ +_W \circ (\psi \times \psi)$$

and $+_M$ is regular at all but finitely many pairs of points on M.

A case study on extended Jacobi quartics

The theorem provides us an automated tool to derive the addition law in a piece-wise fashion.

Let $a_2 = -4a, a_4 = 4(a^2 - d)$. Recall:

$$M : y^2 = dx^4 + 2ax^2 + 1, \quad W : v^2 = u^3 + a_2u^2 + a_4u.$$

$$\psi : \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right), \quad \phi : \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

$$+_W : \Big(\big(\frac{v_2 - v_1}{u_2 - u_1}\big)^2 - a_2 - u_1 - u_2,$$
$$\frac{v_2 - v_1}{u_2 - u_1}(u_1 - (\big(\frac{v_2 - v_1}{u_2 - u_1}\big)^2 - a_2 - u_1 - u_2)) - v_1\Big).$$

$$+_M : \phi \circ +_W \circ (\psi \times \psi).$$

A case study on extended Jacobi quartics

The theorem provides us an automated tool to derive the addition law in a piece-wise fashion.

Let $a_2 = -4a, a_4 = 4(a^2 - d)$. Recall:

$$M : y^2 = dx^4 + 2ax^2 + 1, \quad W : v^2 = u^3 + a_2u^2 + a_4u.$$

$$\psi : \left(\frac{2y+2}{x^2} + 2a, \frac{4y+4}{x^3} + \frac{4a}{x}\right), \quad \phi : \left(2\frac{u}{v}, 2(u-2a)\frac{u^2}{v^2} - 1\right).$$

$$+_W : \Big(\big(\frac{v_2 - v_1}{u_2 - u_1}\big)^2 - a_2 - u_1 - u_2,$$
$$\frac{v_2 - v_1}{u_2 - u_1}(u_1 - (\big(\frac{v_2 - v_1}{u_2 - u_1}\big)^2 - a_2 - u_1 - u_2)) - v_1\Big).$$

$$+_M : \phi \circ +_W \circ (\psi \times \psi).$$

A case study on extended Jacobi quartics

The affine curve: $y^2 = dx^4 + 2ax^2 + 1$.

The derived map $+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$
$\Big(2(((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)^2/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)^2-(2y_1+2)/x_1^2-(2y_2+2)/x_2^2)/(((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)(2(2y_1+2)/x_1^2+2a-((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)^2/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)^2+(2y_2+2)/x_2^2)/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)-(4y_1+4)/x_1^3-4a/x_1),\ 2(((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)^2/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)^2-(2y_1+2)/x_1^2-(2y_2+2)/x_2^2-2a)(((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)^2/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)^2-(2y_1+2)/x_1^2-(2y_2+2)/x_2^2)^2/(((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)(2(2y_1+2)/x_1^2+2a-((4y_1+4)/x_1^3+4a/x_1-(4y_2+4)/x_2^3-4a/x_2)^2/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)^2+(2y_2+2)/x_2^2)/((2y_1+2)/x_1^2-(2y_2+2)/x_2^2)-(4y_1+4)/x_1^3-4a/x_1)^2-1\Big)$.

This map is regular at all but finitely many pairs $(x_1, y_1), (x_2, y_2)$ on M.

Rational simplification

Problem: Well, we expected to see something “simple”, something which can be computed very efficiently.

Solution: Monagan and Pearce’s algorithm [MP06] finds a fraction with minimal total degree sum of the numerator and denominator.

The algorithm: “. . . walk up through the degrees of the numerator and denominator and at each step attempt to solve $N\delta - D\eta \equiv 0 \bmod I$ . . . ”.

Here,
$I = \langle y_1^2 = dx_1^4 + 2ax_1^2 + 1, y_2^2 = dx_2^4 + 2ax_2^2 + 1 \rangle$,
N is the original numerator,
D is the original denominator,
η is a lower-degree numerator candidate,
δ is a lower-degree denominator candidate.

Rational simplification

Good news. An open-source implementation is available in Pearce's thesis. The minimal degree simplified addition map is given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 + x_2^2)(y_1 y_2 - 2a x_1 x_2) - 2x_1 x_2 (1 + d x_1^2 x_2^2)}{(x_1 y_2 - y_1 x_2)^2}\right)$$

with credits to Chudnovsky & Chudnovsky [CC86].

An alternative minimal degree fraction:

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 - x_2^2)^2}{(x_1 y_2 - y_1 x_2)^2}(y_1 y_2 - 2a x_1 x_2 + 1 + d x_1^2 x_2^2) - 1\right).$$

Rational simplification

Good news. An open-source implementation is available in Pearce's thesis. The minimal degree simplified addition map is given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 + x_2^2)(y_1 y_2 - 2a x_1 x_2) - 2x_1 x_2 (1 + d x_1^2 x_2^2)}{(x_1 y_2 - y_1 x_2)^2} \right)$$

with credits to Chudnovsky & Chudnovsky [CC86].

An alternative minimal degree fraction:

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 - x_2^2)^2}{(x_1 y_2 - y_1 x_2)^2} (y_1 y_2 - 2a x_1 x_2 + 1 + d x_1^2 x_2^2) - 1 \right).$$

Rational simplification

Good news. An open-source implementation is available in Pearce's thesis. The minimal degree simplified addition map is given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 + x_2^2)(y_1 y_2 - 2a x_1 x_2) - 2x_1 x_2 (1 + d x_1^2 x_2^2)}{(x_1 y_2 - y_1 x_2)^2} \right)$$

with credits to Chudnovsky & Chudnovsky [CC86].

An alternative minimal degree fraction:

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 - x_2^2)^2}{(x_1 y_2 - y_1 x_2)^2} (y_1 y_2 - 2a x_1 x_2 + 1 + d x_1^2 x_2^2) - 1 \right).$$

More formulas

Problem: When regarded as addition formulas this map does not give a complete description of the group law.

Solution: Find alternative low-degree formulas.

How to: Consider the polynomials $N = x_1^2 - x_2^2$ and $D = x_1 y_2 - y_1 x_2$ in $\mathbb{K}[x_1, x_2, y_1, y_2]$ where $\mathbb{K} = \mathbb{Q}(a, d)$. Since $\mathrm{GCD}(N, D) = 1$, the fraction N/D does not simplify in $\mathbb{K}(x_1, x_2, y_1, y_2)$. Now assume that N/D is a function on $M \times M$ where $a, d \in \mathbb{K}$ with $d(a^2 - d) \neq 0$. Let K be the ideal generated by the polynomials $y_1^2 - dx_1^4 - 2ax_1^2 - 1$ and $y_2^2 - dx_2^4 - 2ax_2^2 - 1$. The reduced Gröbner basis of the colon ideal $J = (\langle D \rangle + K) : \langle N \rangle$ with respect to any graded monomial order must contain a minimal total degree denominator. See [MP06] for core ideas.

More formulas

In addition, it *often* contains other low degree denominators because of the graded order which dominates in reducing the total degree of the generators. Indeed the generators of the reduced Gröbner basis of J with respect to graded reverse lexicographical order with $x_1 > y_1 > x_2 > y_2$ are given by

$$1 - dx_1^2 x_2^2,$$

$$y_1 - dx_1^3 x_2 y_2,$$

$$1 - dy_1^2 x_2^4 + dx_2^4 + 2ax_2^2,$$

$$2a + dx_1^2 - dy_1^2 x_2^2 + dx_2^2,$$

$$\dots$$

Each one of these gives rise to another fraction.

More formulas

For instance, select the denominator $1 - dx_1^2x_2^2$. Now, using a multivariate exact division algorithm the new numerator is computed as $(1 - dx_1^2x_2^2)f/g = x_1y_2 + y_1x_2$. It follows that an alternative (x-coordinate) addition formula is

$$\frac{x_1y_2 + y_1x_2}{1 - dx_1^2x_2^2}$$

with credits to Euler.

Compare with the initial formulas

$$\frac{x_1^2 - x_2^2}{x_1y_2 - y_1x_2}.$$

For an exact division algorithm see [Pea05]. Even more fractions can be obtained by changing the lexicographical ordering.

More formulas

Some more alternatives for the y-coordinate:

$$\frac{y_1y_2 + 2ax_1x_2 \pm \sqrt{d}x_1^2 \pm \sqrt{d}x_2^2}{(1 \mp \sqrt{d}x_1x_2)^2} \mp \sqrt{d}x_3^2,$$

$$\frac{(x_1 - x_2)(y_1 + y_2 + dx_1x_2(x_1^2y_2 + y_1x_2^2))}{(x_1y_2 - y_1x_2)(1 - dx_1^2x_2^2)} - 1,$$

$$\frac{2(x_1y_1 - x_2y_2) - (x_1y_2 - y_1x_2)(y_1y_2 + 2ax_1x_2)}{(x_1y_2 - y_1x_2)(1 - dx_1^2x_2^2)},$$

$$\frac{(x_1^2 - x_2^2)^2 - (x_1y_2 - y_1x_2)(x_1^3y_2 - y_1x_2^3)}{x_1x_2(x_1y_2 - y_1x_2)^2}, \text{[CC86]}$$

$$\frac{(1 \pm \sqrt{d}x_1x_2)(x_1y_1 - x_2y_2 \pm \sqrt{d}x_1^3y_2 \mp \sqrt{d}y_1x_2^3)}{(x_1y_2 - y_1x_2)(1 - dx_1^2x_2^2)} \mp \sqrt{d}x_3^2,$$

$$\frac{(x_1 - x_2)(1 \pm \sqrt{d}x_1x_2)}{(x_1y_2 - y_1x_2)(1 - dx_1^2x_2^2)}(y_1 + y_2 \pm \sqrt{d}x_1^2y_2 \pm \sqrt{d}y_1x_2^2) \mp \sqrt{d}x_3^2 - 1.$$

Special cases

Consider the minimal degree simplified addition map given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 + x_2^2)(y_1 y_2 - 2a x_1 x_2) - 2x_1 x_2 (1 + d x_1^2 x_2^2)}{(x_1 y_2 - y_1 x_2)^2} \right).$$

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $x_1 y_2 - y_1 x_2 = 0$.
If $x_1 y_2 - y_1 x_2 = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity.

Let's investigate...

Special cases

Consider the minimal degree simplified addition map given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \frac{(x_1^2 + x_2^2)(y_1 y_2 - 2a x_1 x_2) - 2x_1 x_2 (1 + d x_1^2 x_2^2)}{(x_1 y_2 - y_1 x_2)^2} \right).$$

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $x_1 y_2 - y_1 x_2 = 0$.
If $x_1 y_2 - y_1 x_2 = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity.

Let's investigate...

Special cases

Lemma

Let $a, d \in \mathbb{K}$ *with* $d(a^2 - d) \neq 0$.

Fix $\delta \in \mathbb{K}$ *so that* $\delta^2 = d$.

Fix $x_1 \in \mathbb{K} - \{0\}$ *and* $y_1 \in \mathbb{K}$ *such that* $y_1^2 = dx_1^4 + 2ax_1^2 + 1$.

Let $x_2, y_2 \in \mathbb{K}$ *such that* $y_2^2 = dx_2^4 + 2ax_2^2 + 1$.

Then $x_1y_2 - y_1x_2 = 0$ *if and only if* $(x_2, y_2) \in S$ *where*

$$S = \left[(x_1, y_1), (-x_1, -y_1), \left(\frac{1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\right), \left(\frac{-1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\right)\right].$$

Special cases

Consider the low-degree addition map given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1 y_2 + y_1 x_2}{1 - d x_1^2 x_2^2}, \frac{(y_1 y_2 + 2a x_1 x_2)(1 + d x_1^2 x_2^2) + 2d x_1 x_2 (x_1^2 + x_2^2)}{(1 - d x_1^2 x_2^2)^2} \right)$$

with credits to Billet & Joye (2003).

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $1 - d x_1^2 x_2^2 = 0$.
If $1 - d x_1^2 x_2^2 = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity.

Let's investigate...

Special cases

Consider the low-degree addition map given by

$$+_M : M \times M \to M, ((x_1, y_1), (x_2, y_2)) \mapsto$$

$$\left(\frac{x_1 y_2 + y_1 x_2}{1 - d x_1^2 x_2^2}, \frac{(y_1 y_2 + 2a x_1 x_2)(1 + d x_1^2 x_2^2) + 2d x_1 x_2 (x_1^2 + x_2^2)}{(1 - d x_1^2 x_2^2)^2} \right)$$

with credits to Billet & Joye (2003).

If $(x_1, y_1) + (x_2, y_2)$ is a point at infinity then $1 - d x_1^2 x_2^2 = 0$.
If $1 - d x_1^2 x_2^2 = 0$ then $(x_1, y_1) + (x_2, y_2)$ may not be a point at infinity.

Let's investigate...

Special cases

Lemma

Let $a, d \in \mathbb{K}$ with $d(a^2 - d) \neq 0$. Fix $\delta \in \mathbb{K}$ so that $\delta^2 = d$. Fix $x_1 \in \mathbb{K} - \{0\}$ and $y_1 \in \mathbb{K}$ such that $y_1^2 = dx_1^4 + 2ax_1^2 + 1$. Let $x_2, y_2 \in \mathbb{K}$ such that $y_2^2 = dx_2^4 + 2ax_2^2 + 1$. Then $1 - dx_1^2x_2^2 = 0$ if and only if $(x_2, y_2) \in S'$ where

$$S' = \left[\left(\frac{1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\right), \left(\frac{-1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\right), \left(\frac{1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\right), \left(\frac{-1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\right)\right].$$

Compare with the exceptions of the minimal degree addition formulas:

$$S = \left[(x_1, y_1), (-x_1, -y_1), \left(\frac{1}{\delta x_1}, \frac{y_1}{\delta x_1^2}\right), \left(\frac{-1}{\delta x_1}, \frac{-y_1}{\delta x_1^2}\right)\right].$$

The first two entries of both S and S' do not end up in point at infinity when added to (x_1, y_1).

input : $P_1, P_2, \Omega_1, \Omega_2 \in E_{\mathbf{Q},d,a}(\mathbb{K})$ and fixed $\delta \in \mathbb{K}$ such that $\delta^2 = d$.

output : $P_1 + P_2$.

if $P_1 \in \{\Omega_1, \Omega_2\}$ **then** $P_t \leftarrow P_1$, $P_1 \leftarrow P_2$, $P_2 \leftarrow P_t$.
if $P_2 = \Omega_1$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,-1)$.
  else if $P_1 = (0,1)$ **then return** Ω_1. **else if** $P_1 = (0,-1)$ **then return** Ω_2.
  else return $(-1/(\delta x_1), y_1/(\delta x_1^2))$.
else if $P_2 = \Omega_2$ **then**
  if $P_1 = \Omega_1$ **then return** $(0,-1)$. **else if** $P_1 = \Omega_2$ **then return** $(0,1)$.
  else if $P_1 = (0,-1)$ **then return** Ω_1. **else if** $P_1 = (0,1)$ **then return** Ω_2.
  else return $(1/(\delta x_1), -y_1/(\delta x_1^2))$.
else if $x_1y_2 - y_1x_2 \neq 0$ **then**
  $x_3 \leftarrow (x_1^2 - x_2^2)/(x_1y_2 - y_1x_2)$.
  $y_3 \leftarrow ((x_1^2 + x_2^2)(y_1y_2 - 2ax_1x_2) - 2x_1x_2(1 + dx_1^2x_2^2))/(x_1y_2 - y_1x_2)^2$.
  return (x_3, y_3).
else if $1 - dx_1^2x_2^2 \neq 0$ **then**
  $x_3 \leftarrow (x_1y_2 + y_1x_2)/(1 - dx_1^2x_2^2)$.
  $y_3 \leftarrow ((y_1y_2 + 2ax_1x_2)(1 + dx_1^2x_2^2) + 2dx_1x_2(x_1^2 + x_2^2))/(1 - dx_1^2x_2^2)^2$.
  return (x_3, y_3).
else
  if $P_2 = (1/(\delta x_1), y_1/(\delta x_1^2))$ **then return** Ω_1. **else return** Ω_2.
end

Outline

1. Overview
2. Automated tools
3. Inversion-free point addition
4. Conclusion

Projective Group Laws

1. Efficient group laws.
2. New low-degree inversion-free formulae.
3. New and faster algorithms.
4. New coordinate systems. New mixed coordinates.

Operation Counts

For the best speed which space should we embed extended Jacobi quartic curves into? Operation counts ($a = -1/2$):

	ADD
$y^2 = dx^4 + 2ax^2 + 1$ in $\mathbb{A}^2$	$\mathbf{I} + 5\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
$Y^2Z^4 = dX^4T^2 + 2aX^2T^2Z^2 + T^2Z^4$ in $\mathbb{P}^1 \times \mathbb{P}^1$	$21\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$
$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2$, [His10]	$10\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$
$Y^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2_w$, [BJ03]	$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
$Y^2 = dT^2 + 2aX^2 + Z^2 \bigcap X^2 = TZ$ in $\mathbb{P}^3$, [HWCD09]	$7\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
	DBL
$y^2 = dx^4 + 2ax^2 + 1$ in $\mathbb{A}^2$	$\mathbf{I} + 2\mathbf{M} + 2\mathbf{S}$
$Y^2Z^4 = dX^4T^2 + 2aX^2T^2Z^2 + T^2Z^4$ in $\mathbb{P}^1 \times \mathbb{P}^1$	$10\mathbf{M} + 2\mathbf{S}$
$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2$, [HWCD09]	$2\mathbf{M} + 5\mathbf{S}$
$Y^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2_w$,	$2\mathbf{M} + 6\mathbf{S}$
$Y^2 = dT^2 + 2aX^2 + Z^2 \bigcap X^2 = TZ$ in $\mathbb{P}^3$, [HWCD09]	$8\mathbf{S}$

Operation Counts

For the best speed which space should we embed extended Jacobi quartic curves into? Operation counts ($a = -1/2$):

	ADD
$y^2 = dx^4 + 2ax^2 + 1$ in $\mathbb{A}^2$	$\mathbf{I} + 5\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
$Y^2Z^4 = dX^4T^2 + 2aX^2T^2Z^2 + T^2Z^4$ in $\mathbb{P}^1 \times \mathbb{P}^1$	$21\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$
$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2$, [His10]	$10\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$
$Y^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2_w$, [BJ03]	$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
Easier to think T as $T = X^2/Z$, [HWCD09]	$7\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
	DBL
$y^2 = dx^4 + 2ax^2 + 1$ in $\mathbb{A}^2$	$\mathbf{I} + 2\mathbf{M} + 2\mathbf{S}$
$Y^2Z^4 = dX^4T^2 + 2aX^2T^2Z^2 + T^2Z^4$ in $\mathbb{P}^1 \times \mathbb{P}^1$	$10\mathbf{M} + 2\mathbf{S}$
$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2$, [HWCD09]	$2\mathbf{M} + 5\mathbf{S}$
$Y^2 = dX^4 + 2aX^2Z^2 + Z^4$ in $\mathbb{P}^2_w$,	$2\mathbf{M} + 6\mathbf{S}$
$Y^2 = dT^2 + 2aX^2 + Z^2 \bigcap X^2 = TZ$ in $\mathbb{P}^3$, [HWCD09]	$8\mathbf{S}$

Operation Counts

Table: Operation counts for extended Jacobi quartic form with $a = -1/2$ in different coordinate systems.

System	DBL	ADD
$\mathcal{Q}^w$	-	10**M**+3**S**+2**D**+14**a**, unified, [BJ03]
$\mathcal{Q}$	3**M**+4**S**+ 4**a**	10**M**+7**S**+2**D**+17**a**, unified
	2**M**+5**S**+ 7**a**	10**M**+5**S**+1**D**+10**a**, dedicated
$\mathcal{Q}^e$	3**M**+5**S**+ 4**a**	8**M**+3**S**+2**D**+17**a**, unified
	8**S**+13**a**	7**M**+3**S**+1**D**+19**a**, dedicated
$\mathcal{Q}^x$	3**M**+4**S**+ 4**a**	7**M**+4**S**+3**D**+19**a**, unified
	2**M**+5**S**+ 7**a**	6**M**+4**S**+2**D**+21**a**, dedicated

$\mathcal{Q}^w$: Weighted, $\mathcal{Q}$: Projective, $\mathcal{Q}^e$: Extended, $\mathcal{Q}^x$: Mixed coordinates.

Operation Counts

Table: Operation counts for (twisted) Edwards form in different coordinate systems.

System	DBL	ADD
$\mathcal{E}$, $(a = 1)$, [BL07a]	3**M**+4**S**	10**M** +1**S**+1**D**, unified
$\mathcal{E}^i$, $(a = 1)$, [BL07b]	3**M**+4**S**+1**D**	9**M** +1**S**+1**D**, unified
$\mathcal{E}$, [BBJLP08]	3**M**+4**S**+1**D**	10**M** +1**S**+2**D**, unified
$\mathcal{E}^i$, [BBJLP08]	3**M**+4**S**+2**D**	9**M** +1**S**+2**D**, unified
$\mathcal{E}^e$	4**M**+4**S**+1**D**	9**M** +2**D**, unified
$\mathcal{E}^e$, $(a = -1)$	4**M**+4**S**	8**M** +1**D**, unified
$\mathcal{E}^x$, $(a = -1)$	3**M**+4**S**	8**M** +1**D**, unified
$\mathcal{E}^x$, $(a = -1)$	3**M**+4**S**	8**M**, dedicated

- $(X_1 : Y_1 : T_1 : Z_1) + (X_2 : Y_2 : T_2 : 1)$ costs only 7**M**.

Operation Counts

Table: Operation counts for (twisted) Jacobi intersection form with $a = 1$ in different coordinate systems.

System	DBL	ADD
$\mathcal{I}$	3**M**+4**S** +6**a**, [BL07]	13**M**+2**S**+1**D**+ 7**a**, unified, [LS01]
	2**M**+5**S**+1**D**+7**a**	13**M**+1**S**+2**D**+15**a**, unified
		12**M** +11**a**, dedicated
$\mathcal{I}^{m2}$	-	11**M**+1**S**+2**D**+15**a**, unified
$\mathcal{I}^{m1}$	3**M**+4**S** +6**a**, *	11**M** + 9**a**, dedicated
	2**M**+5**S**+1**D**+7**a**	-

*: Adapted from [BL07, dbl-2007-bl].

$\mathcal{I}$: Projective, $\mathcal{I}^{m1}$: Modified version 1, $\mathcal{I}^{m2}$: Modified version 2 coordinates.

Operation Counts

Table: Operation counts for (twisted) Hessian form with $a = 1$ in different coordinate systems.

System	DBL	ADD
$\mathcal{H}$	6**M**+3**S**+ 3**a**, [BKL09]	12**M** + 3**a**, unified, [BKL09]
	7**M**+1**S**+ 8**a**	11**M** +17**a**, unified
	3**M**+6**S**+18**a**	12**M** + 3**a**, dedicated
		11**M** +17**a**, dedicated
$\mathcal{H}^e$	9**M**+3**S**+ 3**a**	9**M**+3**S**+ 3**a**, unified
		9**M**+3**S**+ 3**a**, dedicated
	5**M**+6**S**+29**a**	6**M**+6**S**+15**a**, unified
		6**M**+6**S**+15**a**, dedicated

$\mathcal{H}$: Projective, $\mathcal{H}^e$: Extended coordinates.

Operation Counts

Table: Operation counts for short Weierstrass form with $a = -3$ in different coordinate systems.

System	DBL	ADD
$\mathcal{P}$, [CC86]	7**M**+3**S**+10**a**, [BL07]	12**M**+ 5**S**+1**D**+10**a**, unified, [BJ02] 11**M**+ 6**S**+1**D**+15**a**, unified, [BL07] 11**M**+ 5**S**+1**D**+16**a**, unified 12**M**+ 2**S** + 7**a**, dedicated, [CMO98]
$\mathcal{J}$, [CC86]	4**M**+4**S**+ 9**a**, [HMV03] 3**M**+5**S**+12**a**, [BL07]	8**M**+10**S**+1**D**+24**a**, unified 12**M**+ 4**S** + 7**a**, dedicated, [CMO98] 11**M**+ 5**S** +11**a**, dedicated, [BL07]
$\mathcal{J}^c$, [CC86]	4**M**+6**S**+ 4**a**, [CMO98]	7**M**+ 9**S**+1**D**+24**a**, unified 11**M**+ 3**S** + 7**a**, dedicated, [CMO98] 10**M**+ 4**S** +13**a**, dedicated, [BL07]

$\mathcal{P}$: Projective, $\mathcal{J}$: Jacobian, $\mathcal{J}^c$: Chudnovsky Jacobian.

Operation Counts

Table: Cost estimate of SMUL per bit of scalar in **M**.

System	OLD	NEW
Twisted Hessian form, $\mathcal{H}$ with $a = 1$	10.58**M**	10.17**M**
Short Weierstrass form, $\mathcal{J}^x$ with $a = -3$	9.92**M**	-
Jacobi intersection form, $\mathcal{I}$ with $a = 1$	9.01**M**	8.43**M**
Extended Jacobi quartic form, $\mathcal{Q}^x$ with $a = -1/2$	10.00**M**	8.07**M**
Twisted Edwards form, $\mathcal{E}^x$ with $a = -1$	8.31**M**	7.87**M**

SMUL

Table: Cycle-counts (rounded to the nearest one thousand) for 256-bit scalar multiplication with variable base-point (for Core 2).

Curve & coordinate system	**Approximate operation counts**	**Cycles**
Short Weierstrass ($a = -3$), $\mathcal{J}$	**I**+1598**M**+1156**S**+ 0 **D**+2896**a**	468,000
(Twisted) Hessian ($a = 1$), $\mathcal{H}$	**I**+2093**M**+ 757 **S**+ 0 **D**+1177**a**	447,000
(Twisted) Jacobi intersection ($b = 1$), $\mathcal{I}^{m1}$	**I**+1295**M**+1011**S**+ 0 **D**+2009**a**	383,000
Extended Jacobi quartic ($a = -1/2$), $\mathcal{Q}^x$	**I**+1162**M**+1110**S**+102**D**+1796**a**	376,000
Twisted Edwards ($a = -1$), $\mathcal{E}^x$	**I**+1202**M**+ 969 **S**+ 0 **D**+2025**a**	362,000

Note: Short Weierstrass ($a = -3$) was the fastest before 2006!

Thanks.

- Eric Brier and Marc Joye, *Weierstraß elliptic curves and side-channel attacks*, PKC 2002, LNCS, vol. 2274, Springer, 2002, pp. 335–345.
- Olivier Billet and Marc Joye, *The Jacobi model of an elliptic curve and side-channel analysis*, AAECC-15, LNCS, vol. 2643, Springer, 2003, pp. 34–42.
- Daniel J. Bernstein, David Kohel, and Tanja Lange, *Twisted Hessian curves*, Explicit-Formulas Database, 2009, `http://www.hyperelliptic.org/EFD/g1p/auto-twistedhe`
- Daniel J. Bernstein and Tanja Lange, *Explicit-formulas database*, 2007, `http://www.hyperelliptic.org/EFD`.
- David V. Chudnovsky and Gregory V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics **7** (1986), no. 4, 385–434.


Henri Cohen, Atsuko Miyaji, and Takatoshi Ono, *Efficient elliptic curve exponentiation using mixed coordinates*, ASIACRYPT'98, LNCS, vol. 1514, Springer, 1998, pp. 51–65.


Huseyin Hisil, *Elliptic curves, group law, and efficient computation*, Ph.D. thesis, Queenslad University of Technology, 2010.


Darrel Hankerson, Alfred J. Menezes, and Scott A. Vanstone, *Guide to elliptic curve cryptography*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.


Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson, *Jacobi quartic curves revisited*, ACISP 2009, LNCS, vol. 5594, Springer, 2009, pp. 452–468.


Pierre Yvan Liardet and Nigel P. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form.*, CHES 2001, LNCS, vol. 2162, Springer, 2001, pp. 391–401.


Michael Monagan and Roman Pearce, *Rational simplification modulo a polynomial ideal*, ISSAC'06, ACM, 2006, pp. 239–245.


Roman Pearce, *Rational expression simplification with side relations*, Master's thesis, Simon Fraser University, 2005.