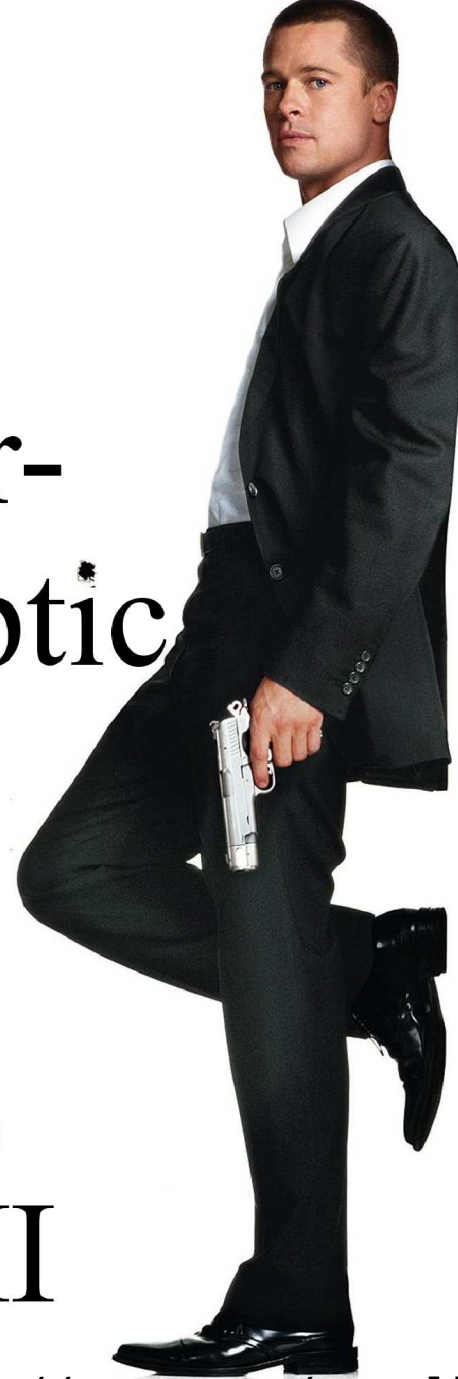




Elliptic vs. Hyper- elliptic



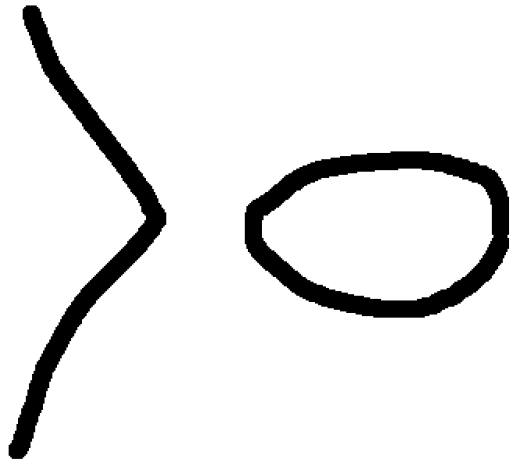
Part III

D. J. Bernstein & T. Lange

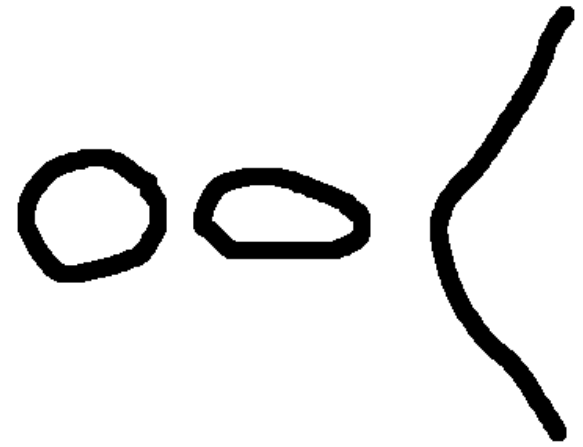
<http://cr.yp.to/newelliptic>

– p. 1

The Opponents



$g = 1$



$g = 2$

(... already after some transformations ...)

Elliptic strikes back



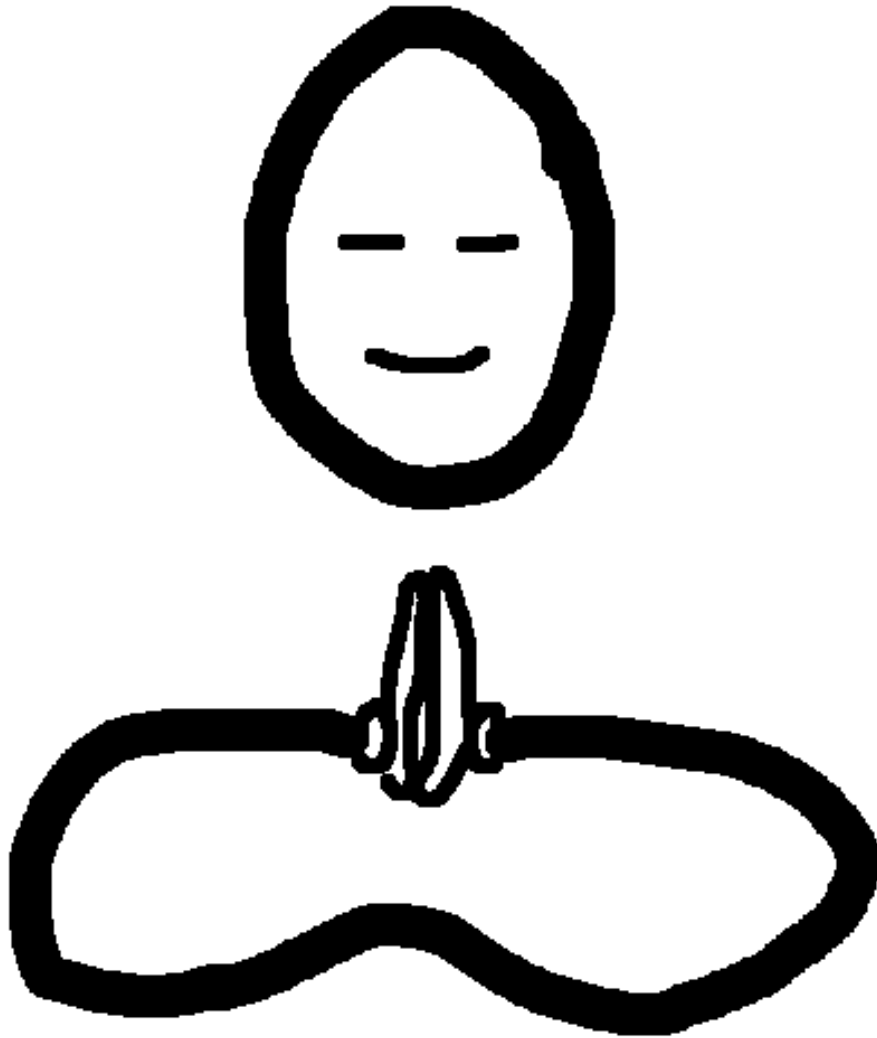
To face the challenge, to take the
competition to a completely new level
...

$$y^2 = x^3 + ax + b$$

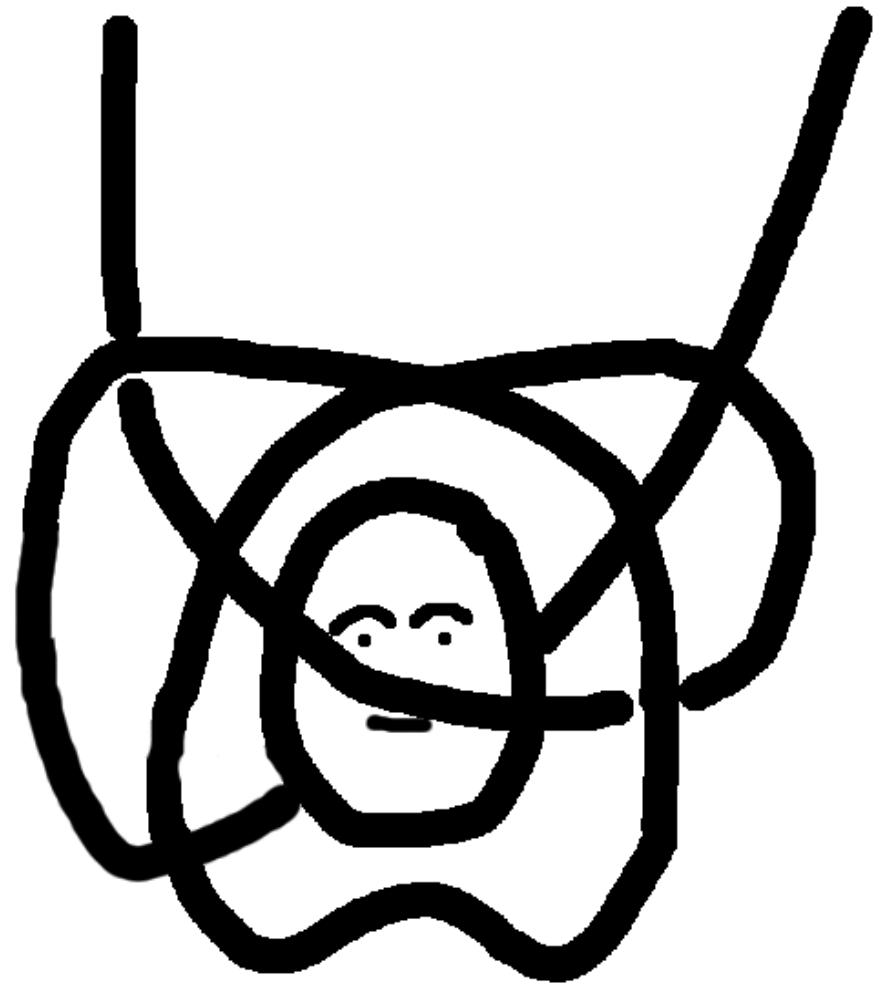
...elliptic has to reconsider its form ...



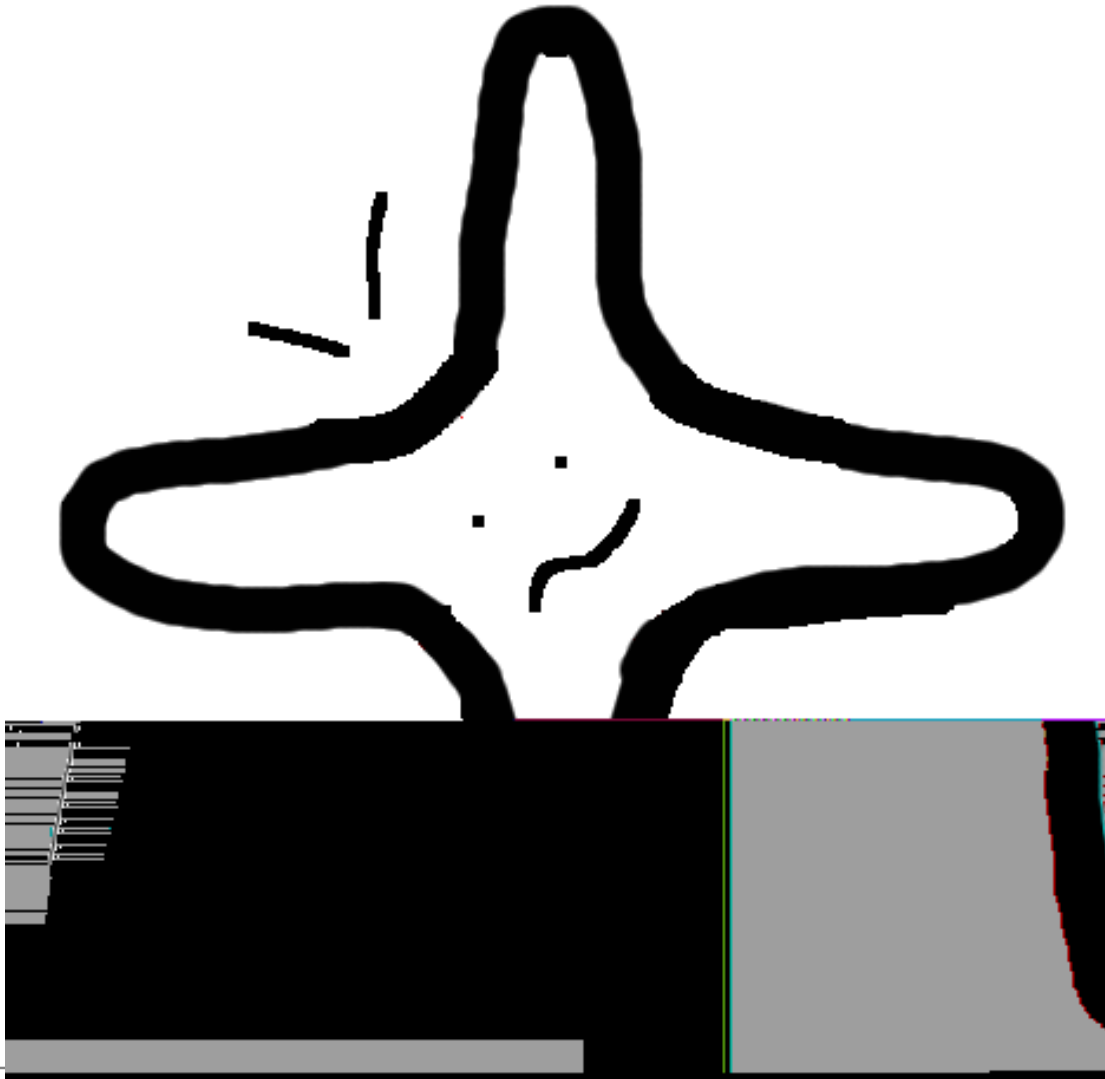
...has to abstract from its Weierstrass form .



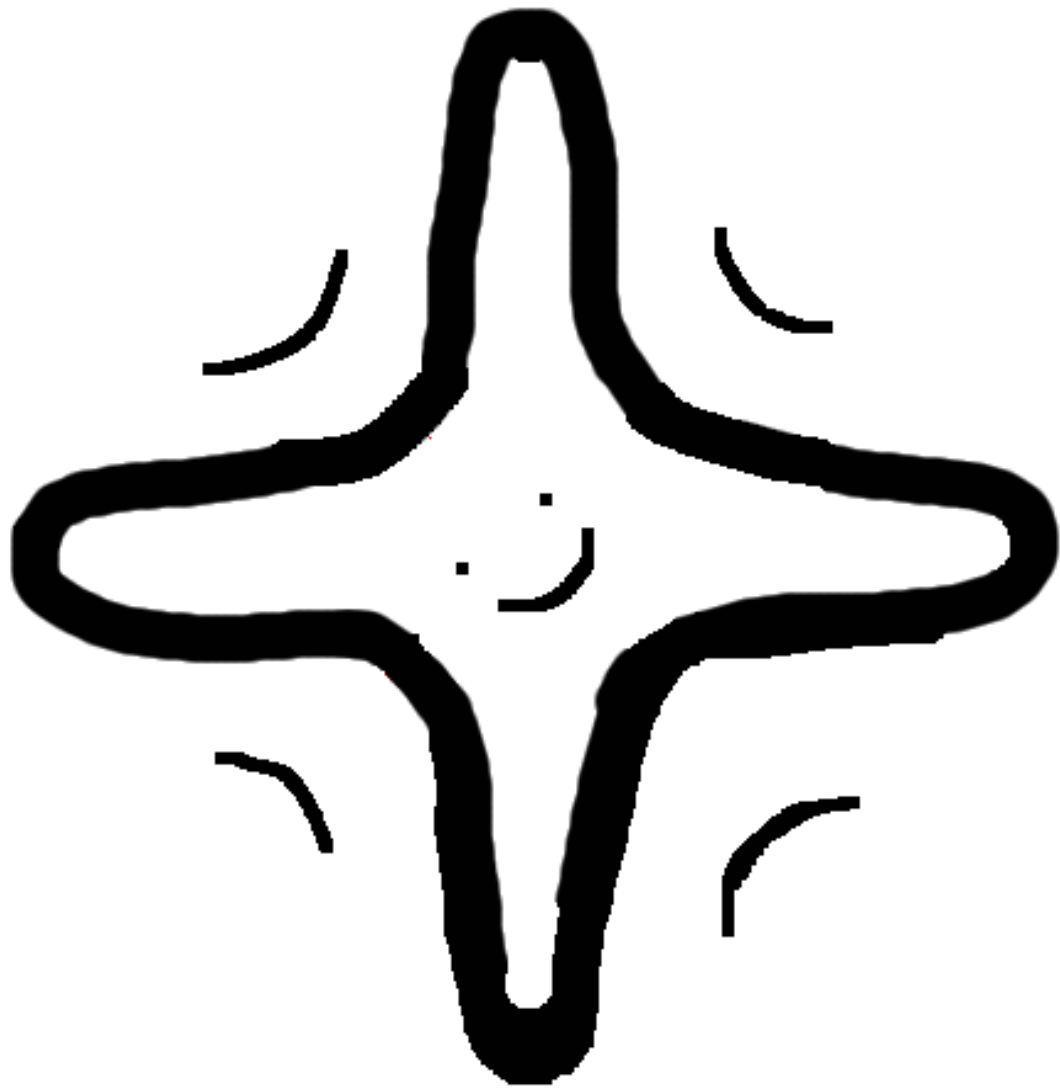
... has to undergo severe isomorphic transformations ...



...until it finds ...



...its true ...



...normal form!

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

Elliptic goes undercover

- Harold M. Edwards Jr., Bulletin of the AMS, electronic April 9, 2007

$$x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$$

describes an elliptic curve.

- Edwards shows that generically every elliptic curve can be written in this form – over some extension field.
- Euler and Gauss (and this is basically the only mention of this form that Edwards and we could dig out) show that

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

is elliptic. To transform this curve we need $\sqrt{-1}$ in the field.

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2), \quad c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an **affine** point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)} \right).$

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2), \quad c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an **affine** point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)} \right)$.
- $[2]P = \left(\frac{x_P y_P + y_P x_P}{c(1 + dx_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - dx_P x_P y_P y_P)} \right)$.

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2), \quad c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an **affine** point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)} \right)$.
- $[2]P = \left(\frac{x_P y_P + y_P x_P}{c(1 + dx_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - dx_P x_P y_P y_P)} \right)$.
- **Unified group operations!**

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2), \quad c, d \neq 0, dc^4 \neq 1.$$

• Neutral element is $(0, c)$, this is an **affine** point!

• $-(x_P, y_P) = (-x_P, y_P)$.

• $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)} \right)$.

$$A = Z_P \cdot Z_Q; \quad B = A^2; \quad C = X_P \cdot X_Q; \quad D = Y_P \cdot Y_Q;$$

$$E = d \cdot C \cdot D; \quad F = B - E; \quad G = B + E;$$

$$X_{P \oplus Q} = A \cdot F \cdot ((X_P + Y_P) \cdot (X_Q + Y_Q) - C - D);$$

$$Y_{P \oplus Q} = A \cdot G \cdot (D - C); \quad Z_{P \oplus Q} = c \cdot F \cdot G.$$

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2), \quad c, d \neq 0, dc^4 \neq 1.$$

• Neutral element is $(0, c)$, this is an **affine** point!

• $-(x_P, y_P) = (-x_P, y_P)$.

•
$$P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)} \right).$$

$$A = Z_P \cdot Z_Q; \quad B = A^2; \quad C = X_P \cdot X_Q; \quad D = Y_P \cdot Y_Q;$$

$$E = d \cdot C \cdot D; \quad F = B - E; \quad G = B + E;$$

$$X_{P \oplus Q} = A \cdot F \cdot ((X_P + Y_P) \cdot (X_Q + Y_Q) - C - D);$$

$$Y_{P \oplus Q} = A \cdot G \cdot (D - C); \quad Z_{P \oplus Q} = c \cdot F \cdot G.$$

Needs **10M + 1S + 1C + 1D + 7A**. At least one of c, d small.

Fastest unified addition-or-doubling formula

System	Cost of unified addition-or-doubling
Projective	11M+6S+1D; see Brier/Joye '03
Jacobian if $a_4 = -1$	13M+3S; see Brier/Joye '02
Jacobi intersection	13M+2S+1D; see Liardet/Smart '01
Jacobi quartic	10M+3S+3D; see Billet/Joye '01
Hessian	12M; see Joye/Quisquater '01
Edwards ($c = 1$)	10M+1S+1D

- Exactly the same formulae for doubling (no re-arrangement like in Hessian; no if-else)
- No exceptional cases** if d is not a square. Formulae correct for all affine inputs (incl. $(0, c), -P$).
- Caveat: Edwards curves have points of order 4, namely $(\pm c, 0)$.

But wait – there's more!

How about non-unified doubling?

$$\begin{aligned}[2]P &= \left(\frac{x_P y_P + y_P x_P}{c(1 + dx_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - dx_P x_P y_P y_P)} \right) \\ &= \left(\frac{2x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)} \right)\end{aligned}$$

How about non-unified doubling?

$$\begin{aligned}[2]P &= \left(\frac{x_P y_P + y_P x_P}{c(1 + dx_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - dx_P x_P y_P y_P)} \right) \\ &= \left(\frac{2x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)} \right) \\ &= \left(\frac{2cx_P y_P}{c^2(1 + d(x_P y_P)^2)}, \frac{c(y_P^2 - x_P^2)}{c^2(2 - (1 + d(x_P y_P)^2))} \right)\end{aligned}$$

Use curve equation $x^2 + y^2 = c^2(1 + dx^2 y^2)$.

How about non-unified doubling?

$$\begin{aligned}[2]P &= \left(\frac{x_P y_P + y_P x_P}{c(1 + dx_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - dx_P x_P y_P y_P)} \right) \\&= \left(\frac{2x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)} \right) \\&= \left(\frac{2cx_P y_P}{c^2(1 + d(x_P y_P)^2)}, \frac{c(y_P^2 - x_P^2)}{c^2(2 - (1 + d(x_P y_P)^2))} \right) \\&= \left(\frac{2cx_P y_P}{x_P^2 + y_P^2}, \frac{c(y_P^2 - x_P^2)}{2c^2 - (x_P^2 + y_P^2)} \right)\end{aligned}$$

How about non-unified doubling?

$$\begin{aligned}[2]P &= \left(\frac{x_P y_P + y_P x_P}{c(1 + dx_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - dx_P x_P y_P y_P)} \right) \\ &= \left(\frac{2x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)} \right) \\ &= \left(\frac{2cx_P y_P}{c^2(1 + d(x_P y_P)^2)}, \frac{c(y_P^2 - x_P^2)}{c^2(2 - (1 + d(x_P y_P)^2))} \right) \\ &= \left(\frac{2cx_P y_P}{x_P^2 + y_P^2}, \frac{c(y_P^2 - x_P^2)}{2c^2 - (x_P^2 + y_P^2)} \right)\end{aligned}$$

Inversion-free version needs $3M + 4S + 3C + 6A$.

Can always choose $c = 1$!

Fastest doubling formulae

System	Cost of doubling
Projective	5M+6S+1D;
Hessian	6M+3S; see Joye/Quisquater '01
Jacobi quartic	1M+9S+1D; see Billet/Joye '01
Jacobian	1M+8S+1D;
Jacobian if $a_4 = -3$	3M+5S; see DJB '01
Jacobi intersection	3M+4S; see Liardet/Smart '01
Edwards ($c = 1$)	3M+4S

- Edwards ADD takes 10M+1S+1D, mixed 9M+1S+1D.
- Edwards faster than Jacobian in DBL & ADD.
- Edwards coordinates allow to use windowing methods
- Montgomery takes 5M+4S+1D per bit.

But wait – there's more!

<http://cr.yp.to/newelliptic>