Twisted Hessian Curves

Tanja Lange
Technische Universiteit Eindhoven

joint work with
Daniel J. Bernstein
Chitchanok Chuengsatiansup
& David Kohel

cr.yp.to/papers.html#hessian

Diffie-Hellman key exchange

Pick some *generator* P,
i.e. some group element
(using additive notation here).

$$
\begin{tikzcd}
\begin{array}{c}\text{Alice's}\\ \text{secret key } a\end{array} \arrow[d] \arrow[dd, bend right] & & \begin{array}{c}\text{Bob's}\\ \text{secret key } b\end{array} \arrow[d] \arrow[dd, bend left] \\
\begin{array}{c}\text{Alice's}\\ \text{public key}\\ aP\end{array} \arrow[drr] & & \begin{array}{c}\text{Bob's}\\ \text{public key}\\ b\,P\end{array} \arrow[dll] \\
\begin{array}{c}\{\text{Alice}, \text{Bob}\}\text{'s}\\ \text{shared secret}\\ ab\,P\end{array} & = & \begin{array}{c}\{\text{Bob}, \text{Alice}\}\text{'s}\\ \text{shared secret}\\ b\,aP\end{array}
\end{tikzcd}
$$

Diffie-Hellman key exchange

Pick some *generator* P,
i.e. some group element
(using additive notation here).

Alice's secret key a | Bob's secret key b

Alice's public key aP | Bob's public key $b\,P$

$\{\text{Alice}, \text{Bob}\}$'s shared secret $ab\,P$ $=$ $\{\text{Bob}, \text{Alice}\}$'s shared secret $b\,aP$

What does P look like &
how to compute $P + Q$?

Usual lecture on ECC

Can use any field k.

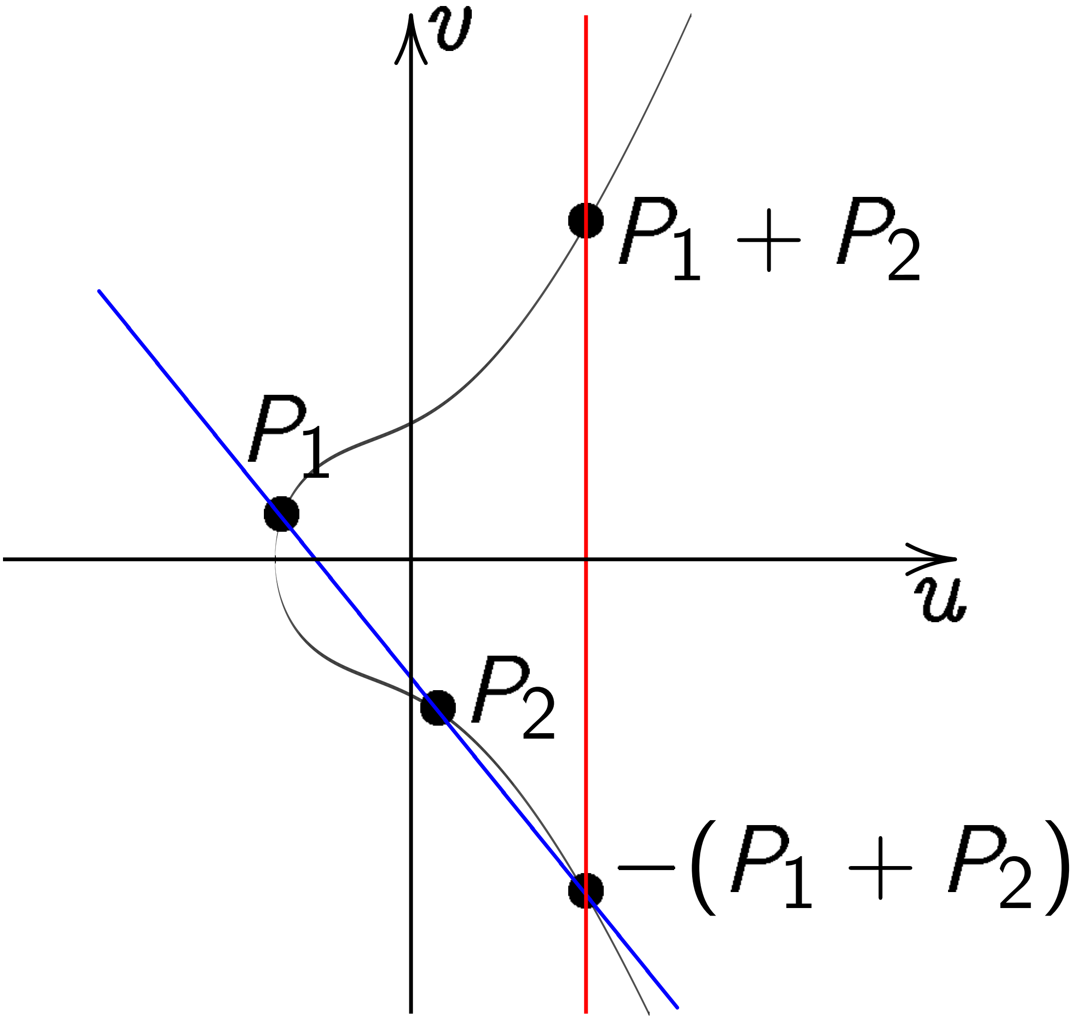
Can use any nonsingular curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

"Nonsingular": no $(x, y) \in \bar{k} \times \bar{k}$ simultaneously satisfies $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

Easy to check nonsingularity.
Almost all curves are nonsingular when k is large.

Addition on Weierstrass curve

$$v^2 = u^3 + u^2 + u + 1$$



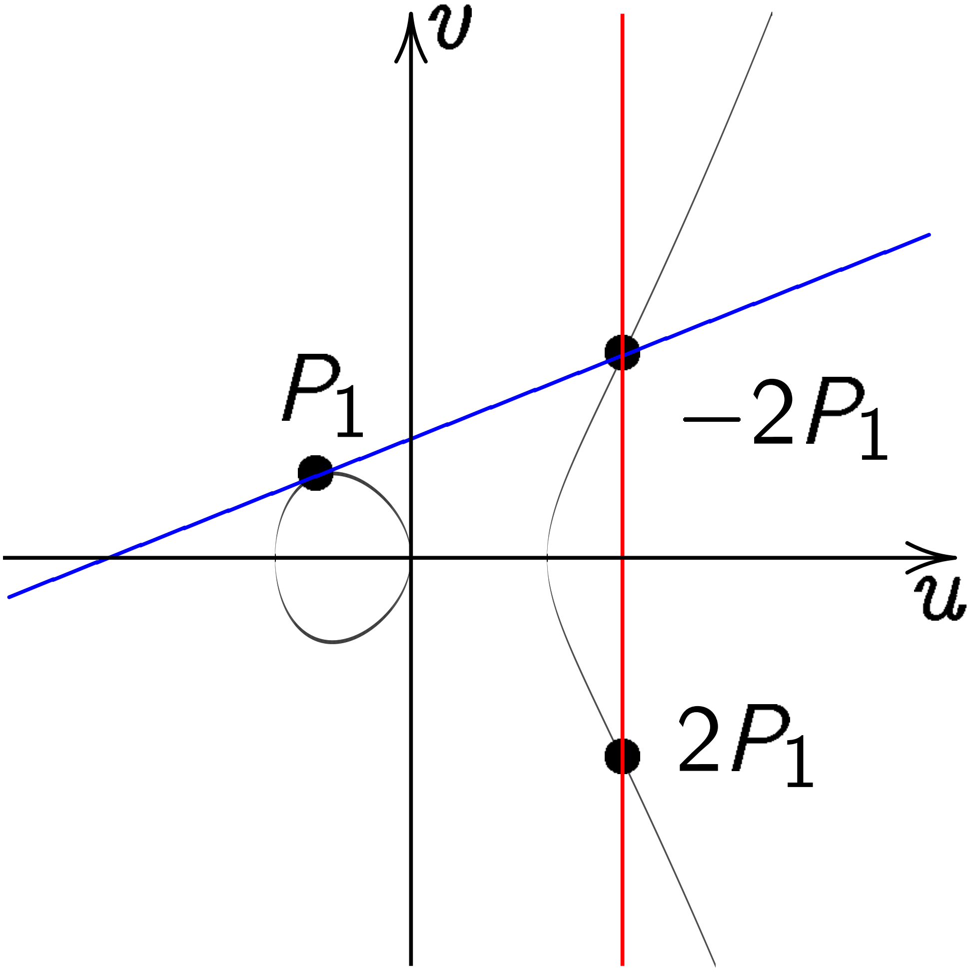
Slope $\lambda = (v_2 - v_1)/(u_2 - u_1)$.

Disaster if $u_1 = u_2$.

Crypto needs to deal with adversarial inputs.

Doubling on Weierstrass curve

$v^2 = u^3 - u$



Slope $\lambda = (3u_1^2 - 1)/(2v_1)$.

Disaster if $v_1 = 0$.

In most cases

$(u_1, v_1) + (u_2, v_2) =$
(u_3, v_3) where $(u_3, v_3) =$
$(\lambda^2 - u_1 - u_2, \lambda(u_1 - u_3) - v_1)$.

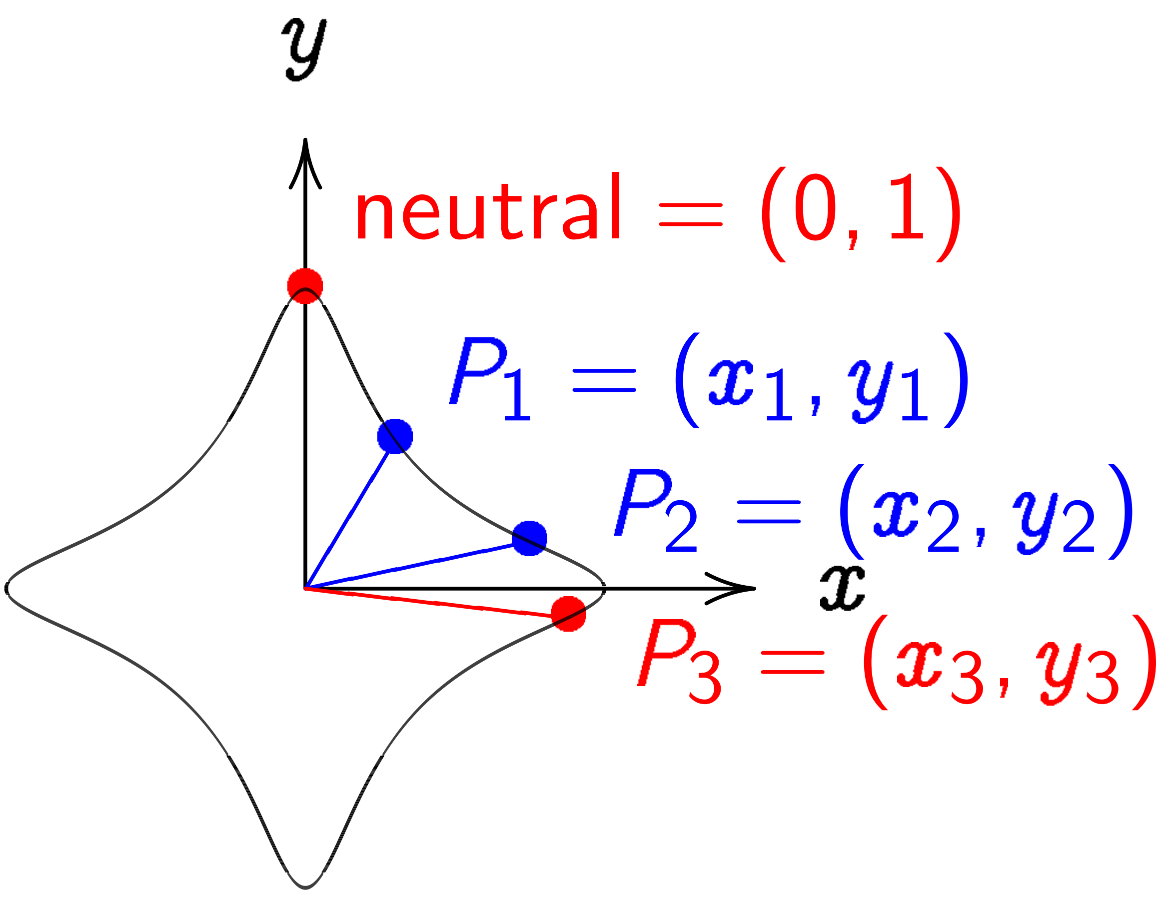
$u_1 \neq u_2$, "addition" (alert!):
$\lambda = (v_2 - v_1)/(u_2 - u_1)$.
Total cost $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}$.

$(u_1, v_1) = (u_2, v_2)$ and $v_1 \neq 0$,
"doubling" (alert!):
$\lambda = (3u_1^2 + 2a_2u_1 + a_4)/(2v_1)$.
Total cost $1\mathbf{I} + 2\mathbf{M} + 2\mathbf{S}$.

Also handle some exceptions:
$(u_1, v_1) = (u_2, -v_2)$; ∞ as input.

Fun lecture on ECC (=Edwards)

Change the curve on which Alice and Bob work.



$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$\ (y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The Edwards addition law

$(x_1, y_1) + (x_2, y_2) =$
$((x_1 y_2 + y_1 x_2)/(1 - 30 x_1 x_2 y_1 y_2),$
$(y_1 y_2 - x_1 x_2)/(1 + 30 x_1 x_2 y_1 y_2))$
is a group law for the curve
$x^2 + y^2 = 1 - 30 x^2 y^2$.

Some calculation required:
addition result is on curve;
addition law is associative.

Other parts of proof are easy:
addition law is commutative;
$(0, 1)$ is neutral element;
$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

Can use addition law for doubling.

Addition law is **strongly unified**.

Can use addition law for doubling.
Addition law is **strongly unified**.

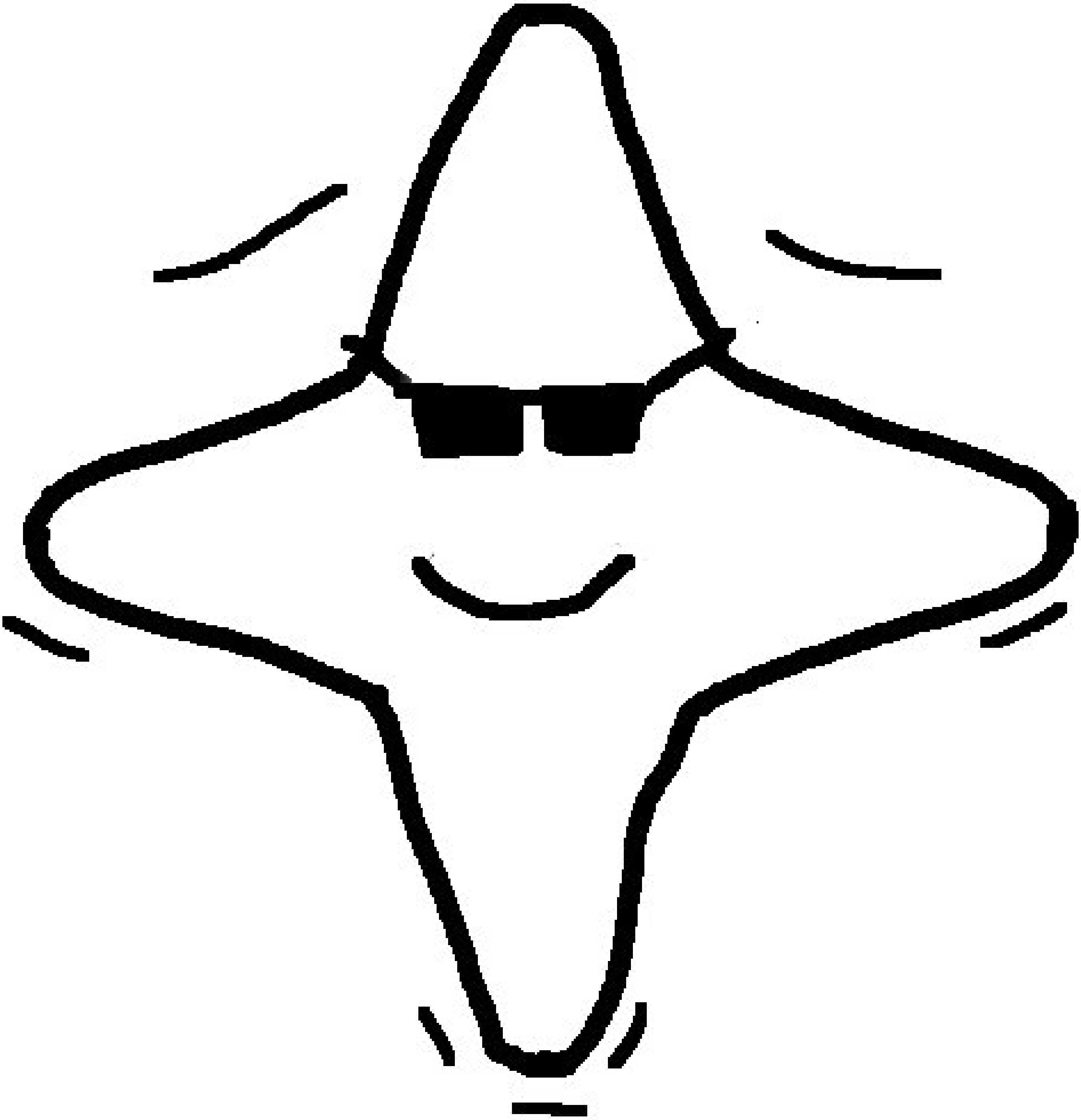
Can prove that
the denominators are never 0.
Addition law is **complete**.

Can use addition law for doubling.
Addition law is **strongly unified**.

Can prove that
the denominators are never 0.
Addition law is **complete**.

The proof relies on
choosing *non-square* d
in $x^2 + y^2 = 1 + dx^2y^2$.

Edwards curves are cool



1986 Chudnovsky–Chudnovsky,
"Sequences of numbers
generated by addition
in formal groups
and new primality
and factorization tests":

"The crucial problem becomes
the choice of the model
of an algebraic group variety,
where computations mod p
are the least time consuming."

Most important computations:
ADD is $P, Q \mapsto P + Q$.
DBL is $P \mapsto 2P$.

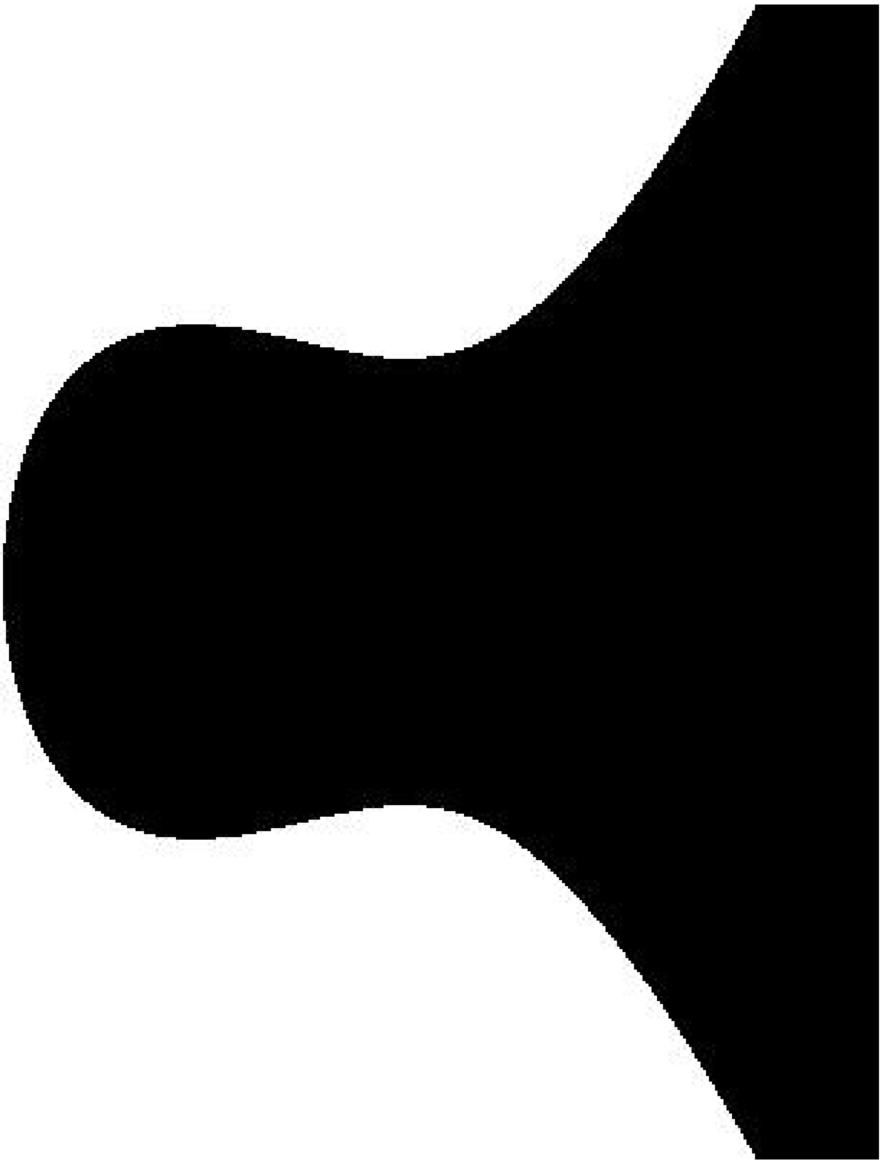
"It is preferable to use models of elliptic curves lying in low-dimensional spaces, for otherwise the number of coordinates and operations is increasing. This limits us . . . to 4 basic models of elliptic curves."

Short Weierstrass:
$y^2 = x^3 + ax + b$.

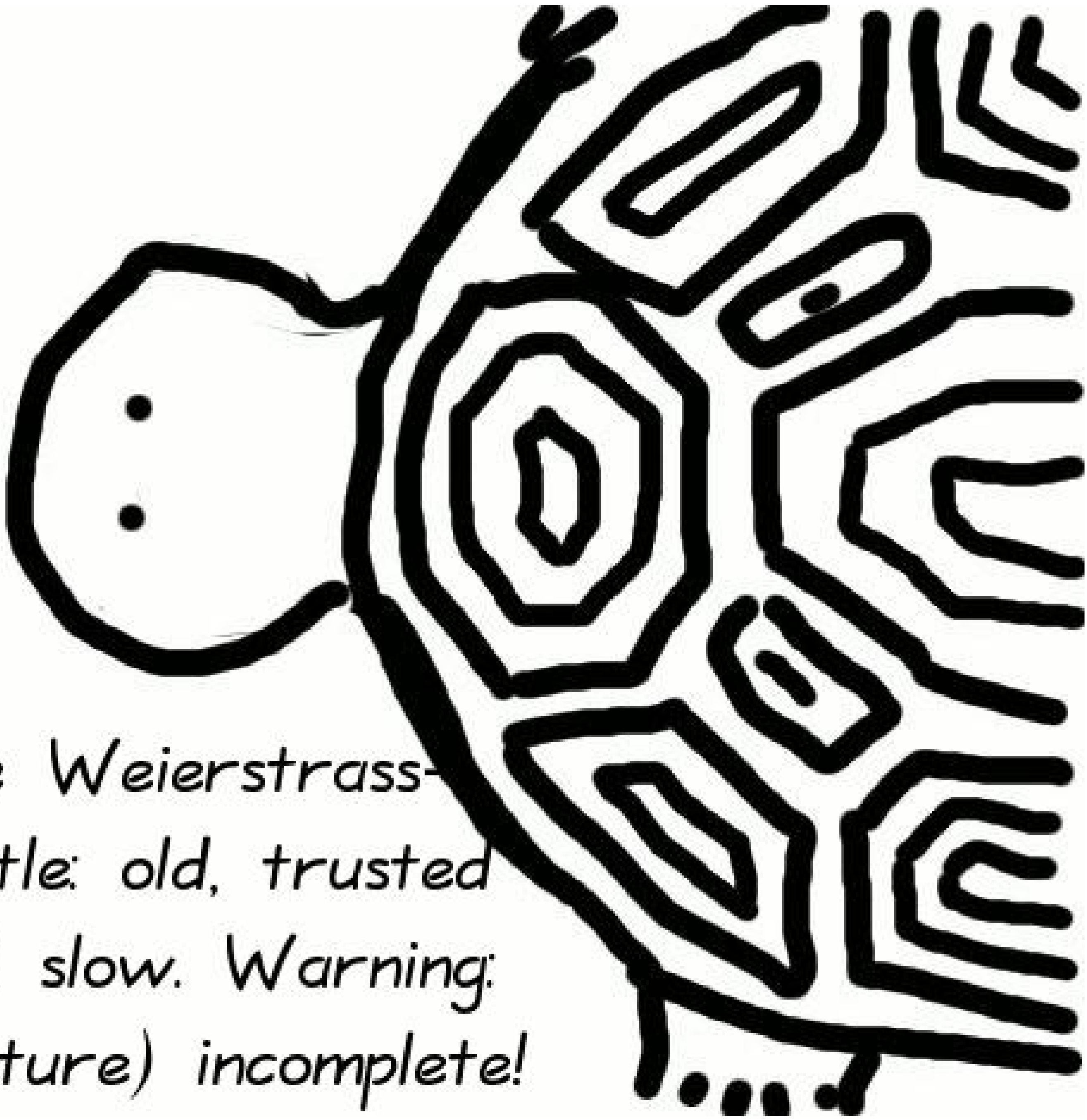
Jacobi intersection:
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.

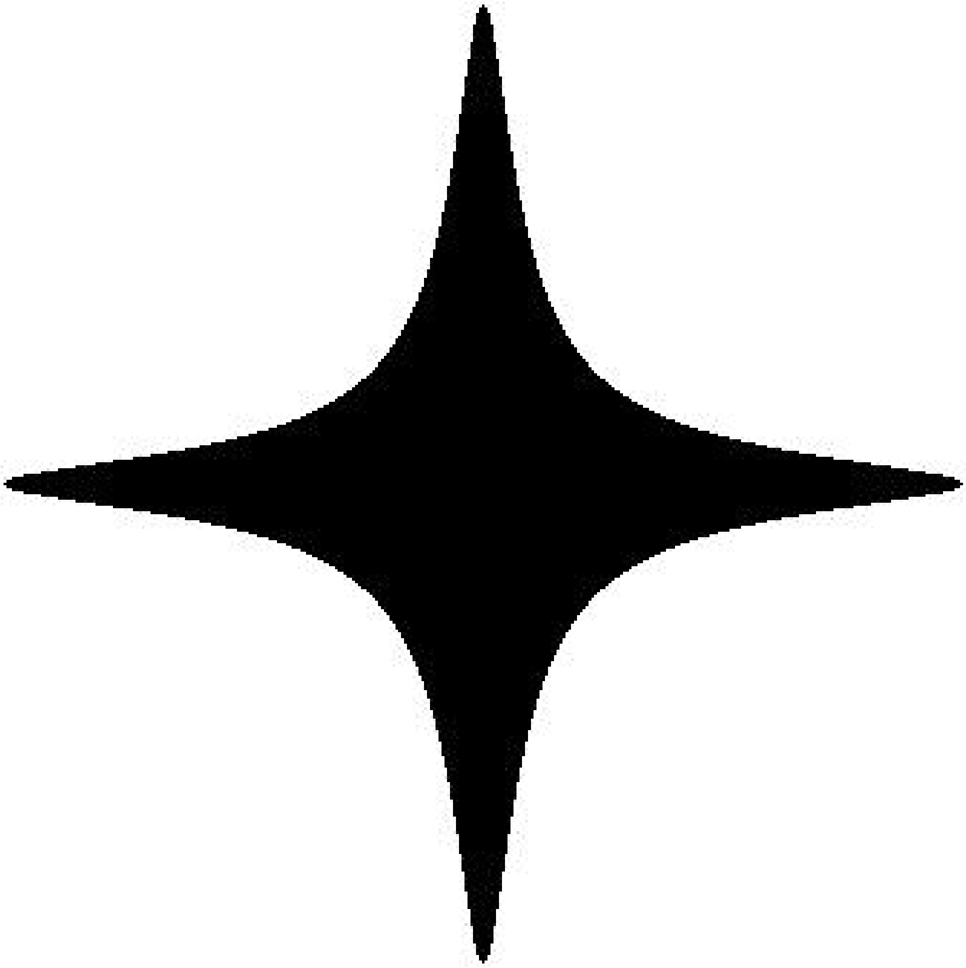
Hessian: $x^3 + y^3 + 1 = 3dxy$.



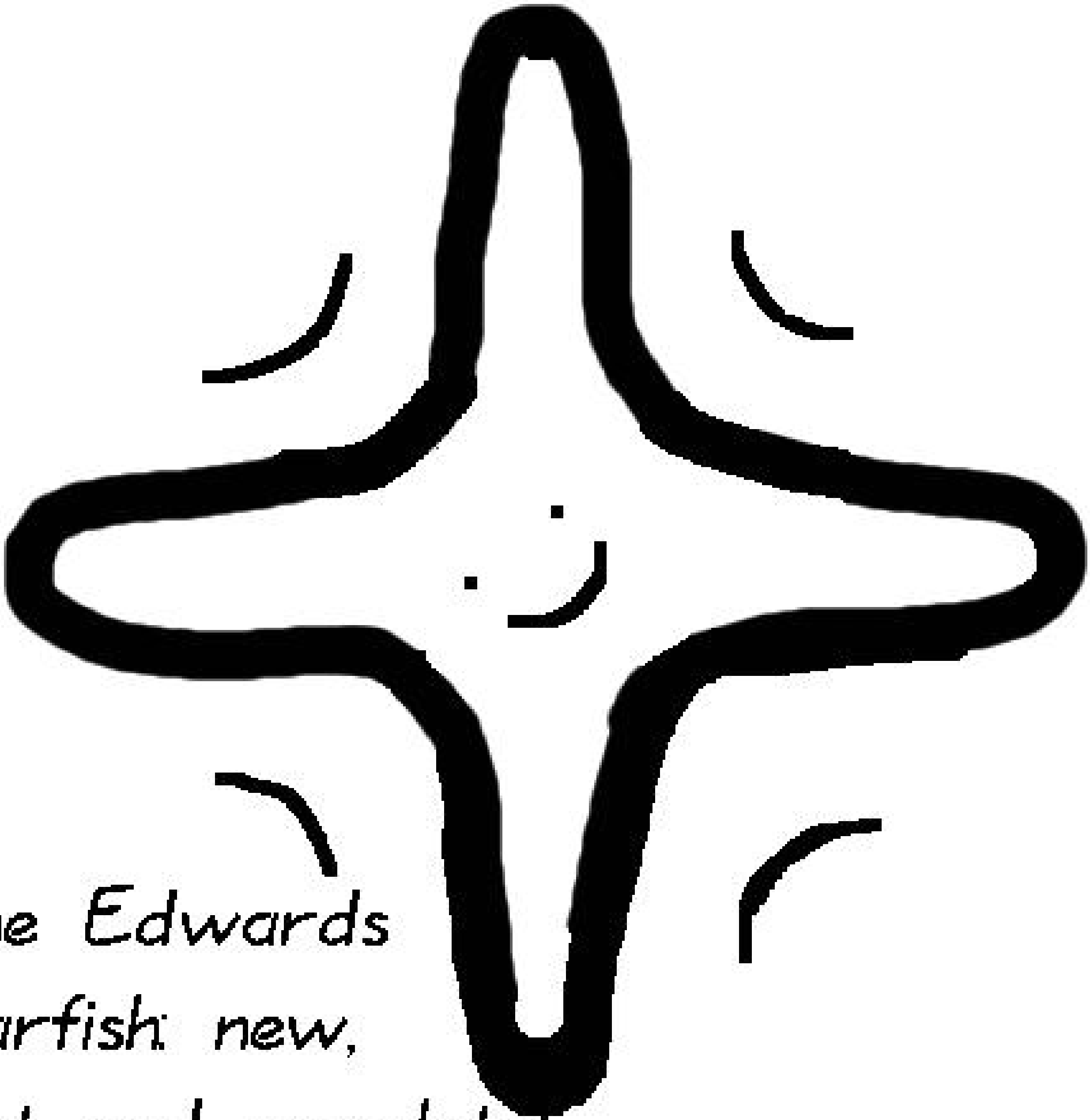
$$y^2 = x^3 - 0.4x + 0.7$$



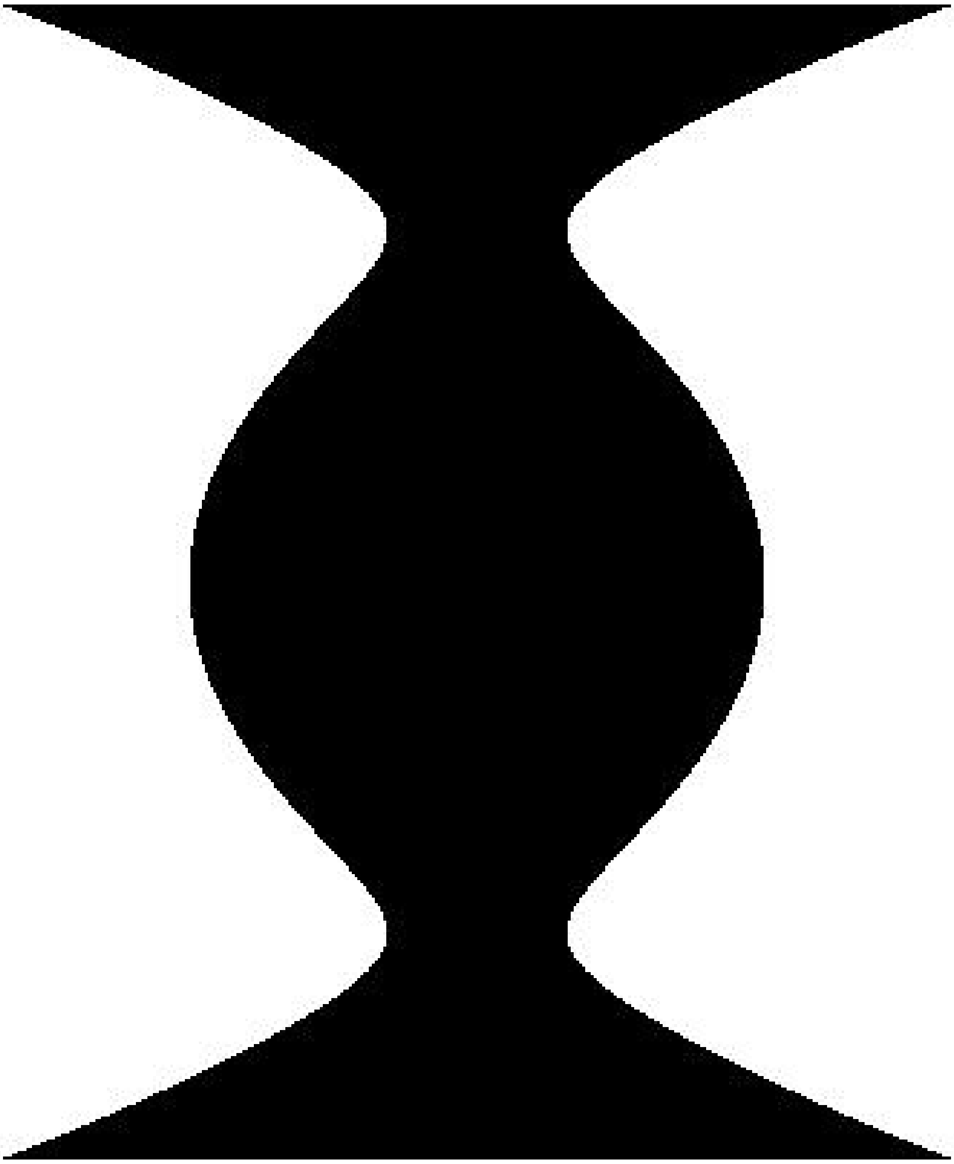
The Weierstrass-turtle: old, trusted and slow. Warning: (picture) incomplete!



$$x^2 + y^2 = 1 - 300x^2y^2$$

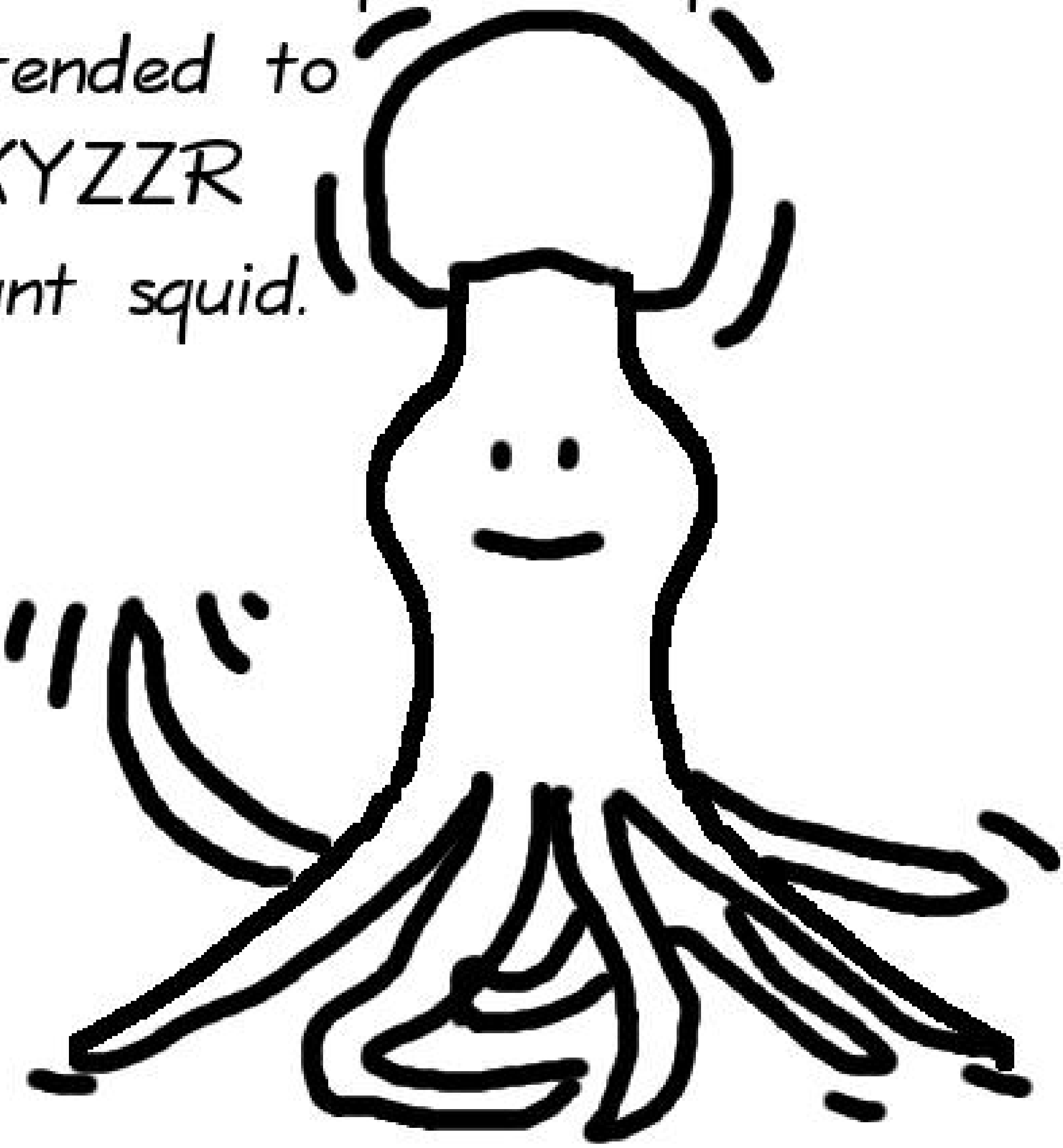


The Edwards starfish: new, fast and complete!



$$x^2 = y^4 - 1.9y^2 + 1$$

The Jacobi-quartic squid: can be extended to XXYZZR giant squid.



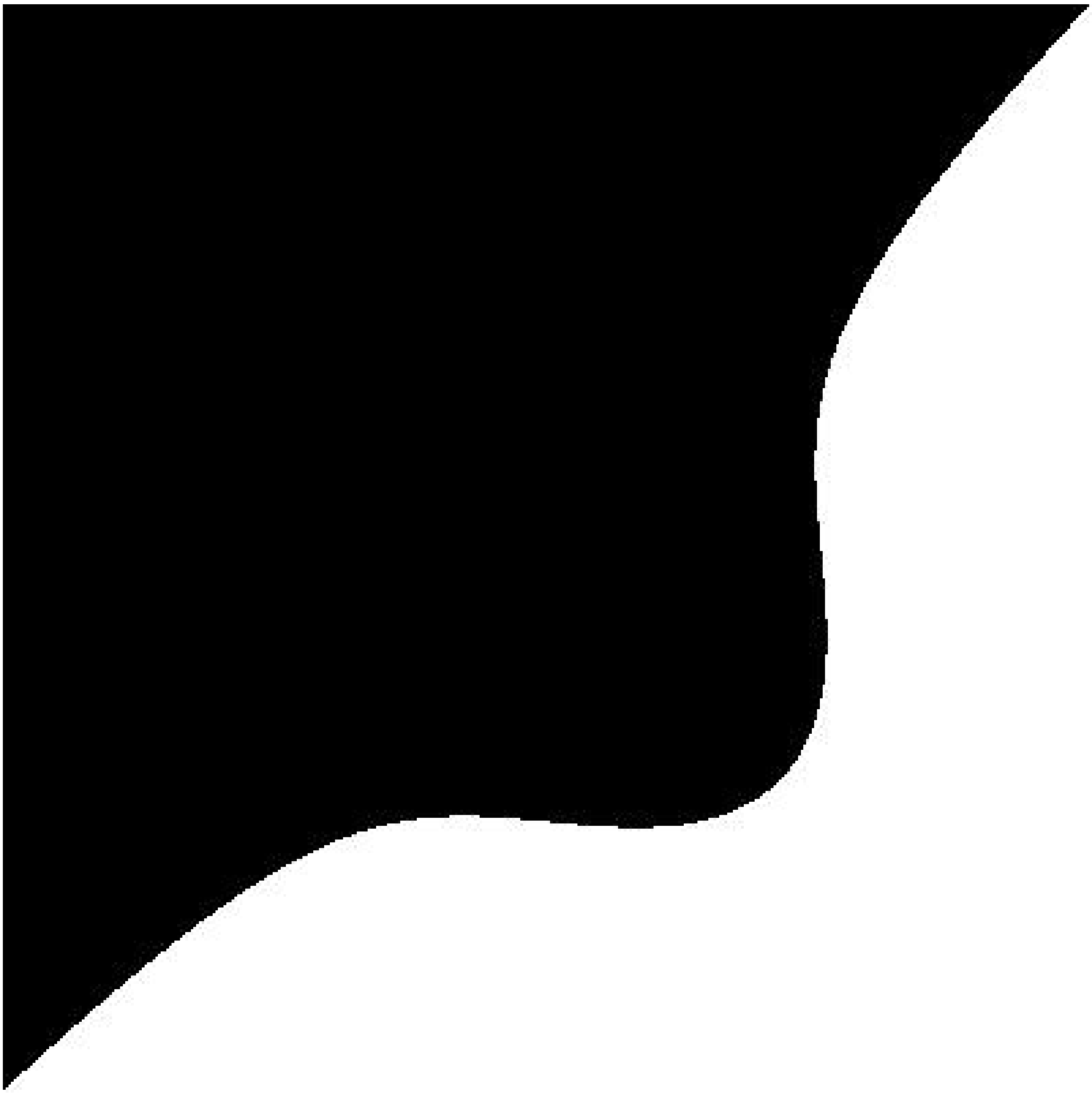
Hessian curves $X^3+Y^3+Z^3=dXYZ$

Credited to Sylvester
by 1986 Chudnovsky–Chudnovsky:

$$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2,$$
$$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2,$$
$$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2.$$

2001 Joye–Quisquater:
$2(X_1 : Y_1 : Z_1) =$
$(Z_1 : X_1 : Y_1) + (Y_1 : Z_1 : X_1)$
so can use ADD to double.

"Unified addition formulas,"
helpful against side channels.
But need to permute inputs.

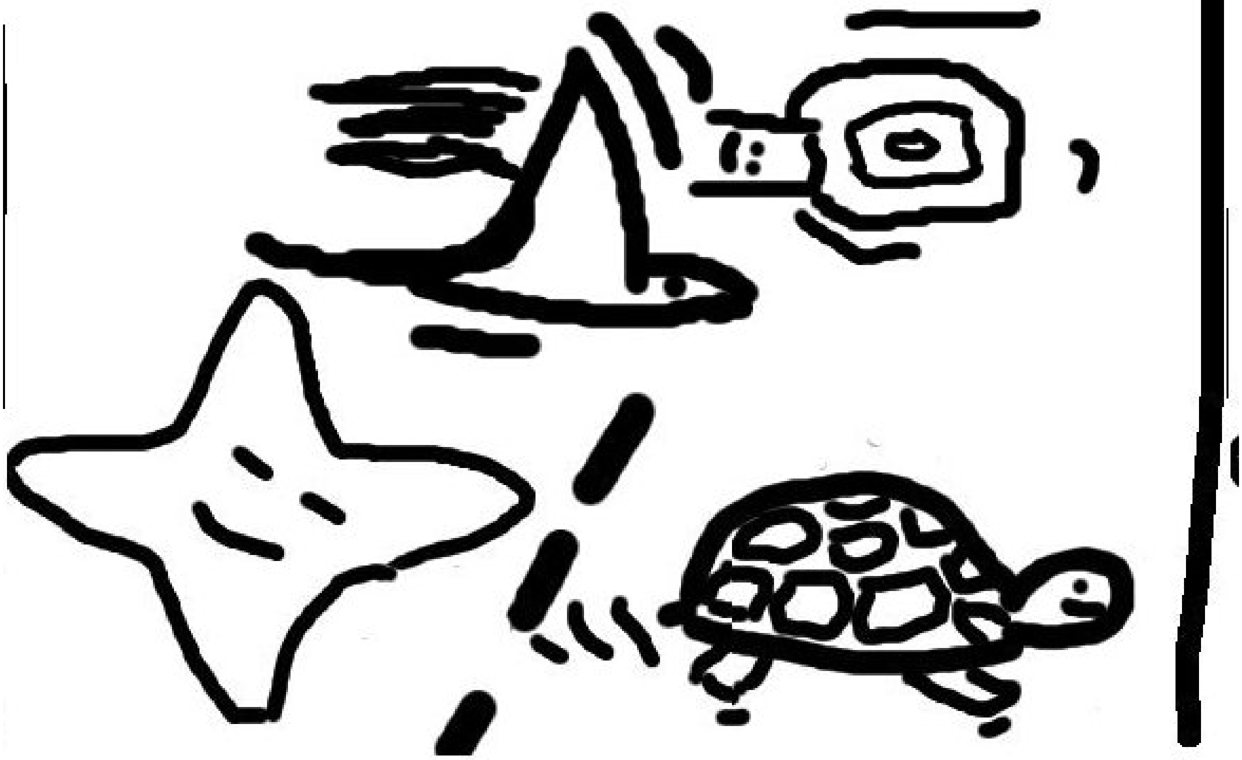


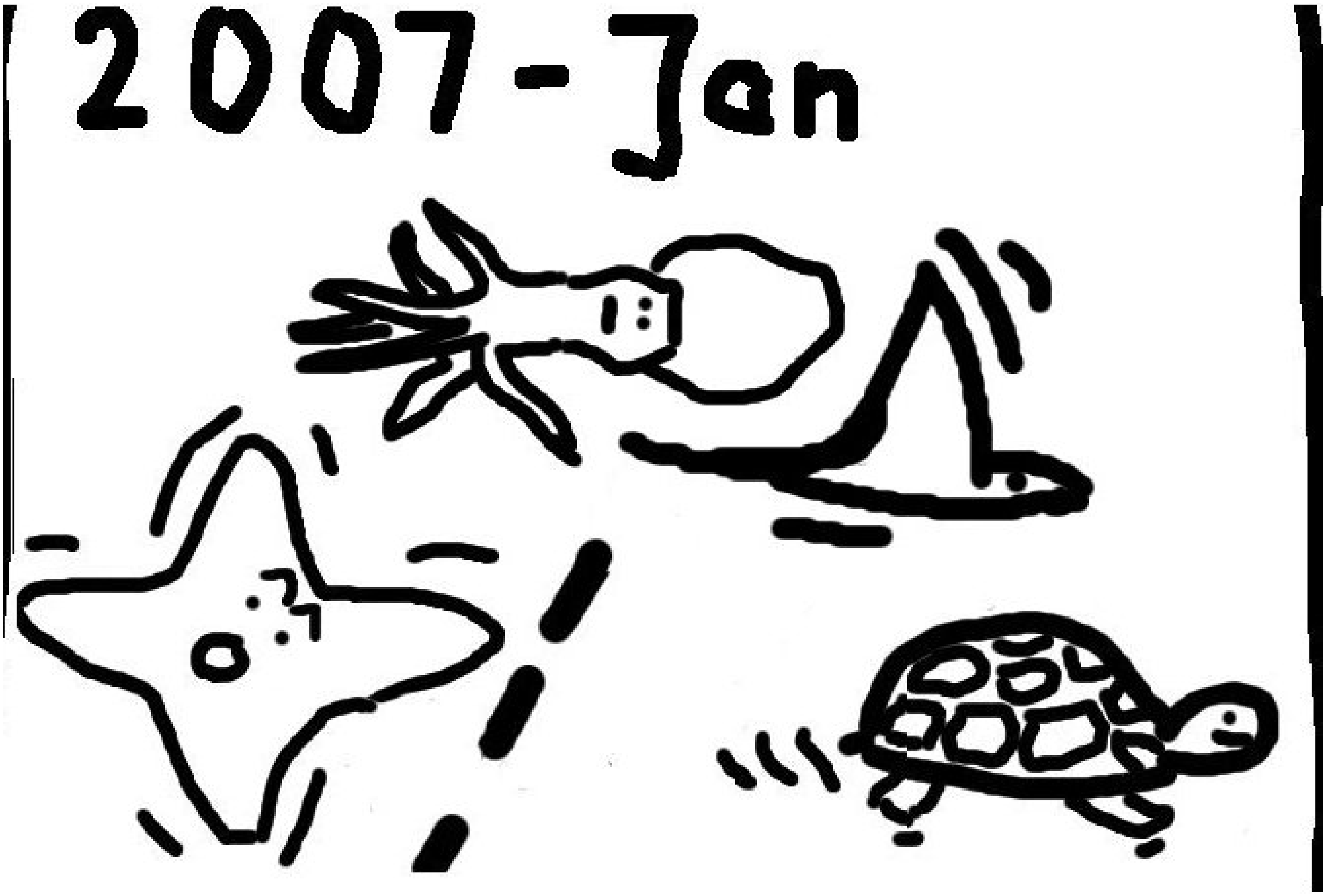
$$x^3 - y^3 + 1 = 0.3xy$$


The Hessian-ray: uniform
but
not strongly so

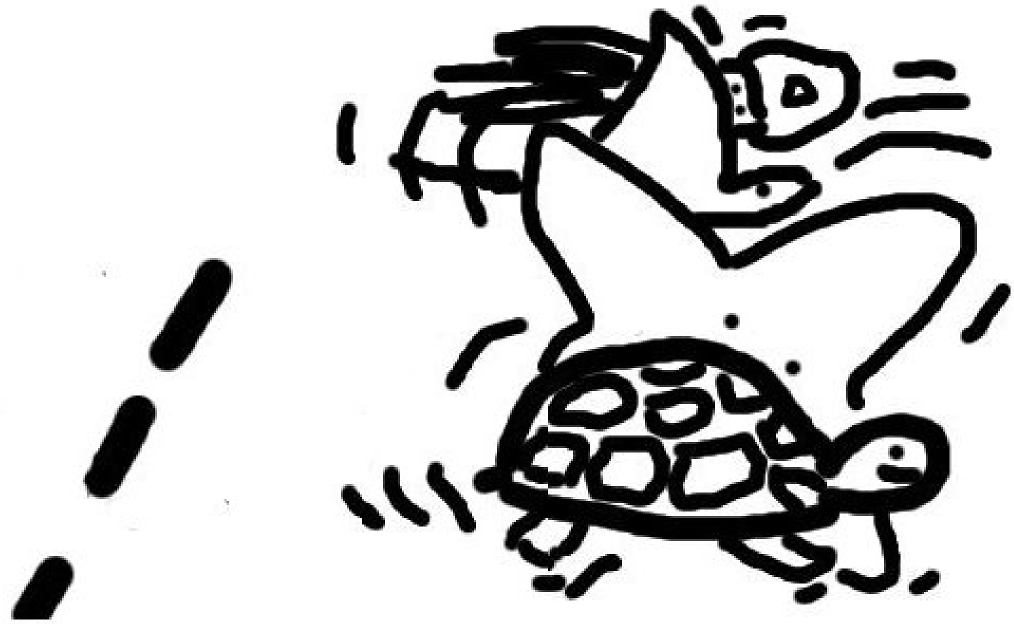

START

1985

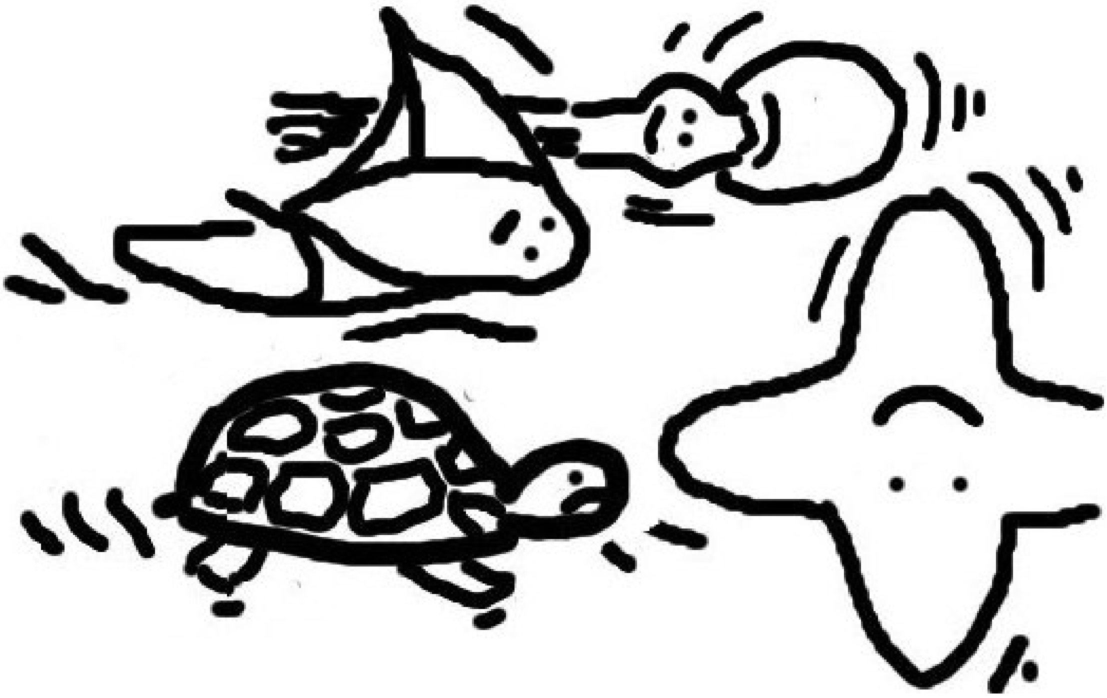



2007-Jan

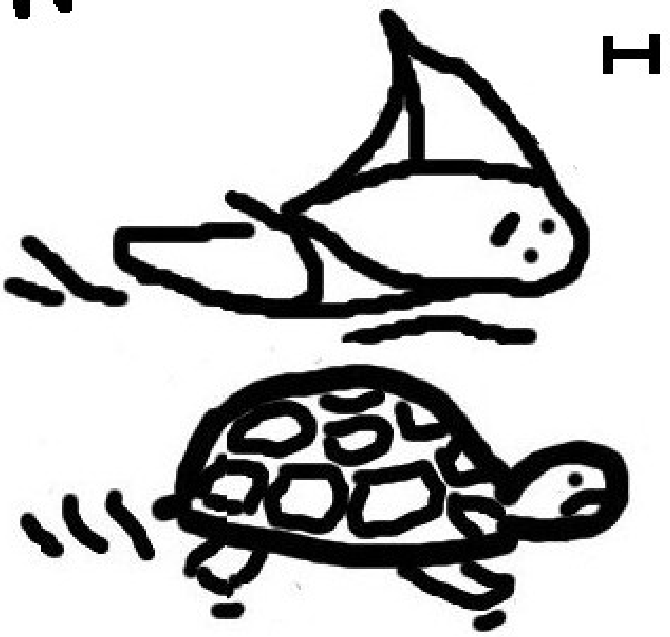
Feb



Mar



Zoom



Twisted Hessian curves

2009 Bernstein–Kohel–Lange

2015 B–Chuengsatiansup–K–L

Permute coordinates, introduce parameter a.

$H/k : aX^3 + Y^3 + Z^3 = dXYZ$, with $a(27a - d^3) \neq 0$.

Use (0:−1:1) as neutral element.

$-(X_1 : Y_1 : Z_1) = (X_1 : Z_1 : Y_1)$.

Addition

$X_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1$,

$Y_3 = Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1$,

$Z_3 = Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1$.

Fails for doubling.

Rotated addition

$X_3' = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2$,
$Y_3' = Y_2^2 Y_1 Z_1 - a X_1^2 X_2 Z_2$,
$Z_3' = a X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2$.

Works for doubling.

Works for any two points if a is not a cube in k.

Complete addition law for twisted Hessian curves.

Addition much faster than on Weierstrass curves.

Doubling not much slower.

Very efficient tripling formulas.

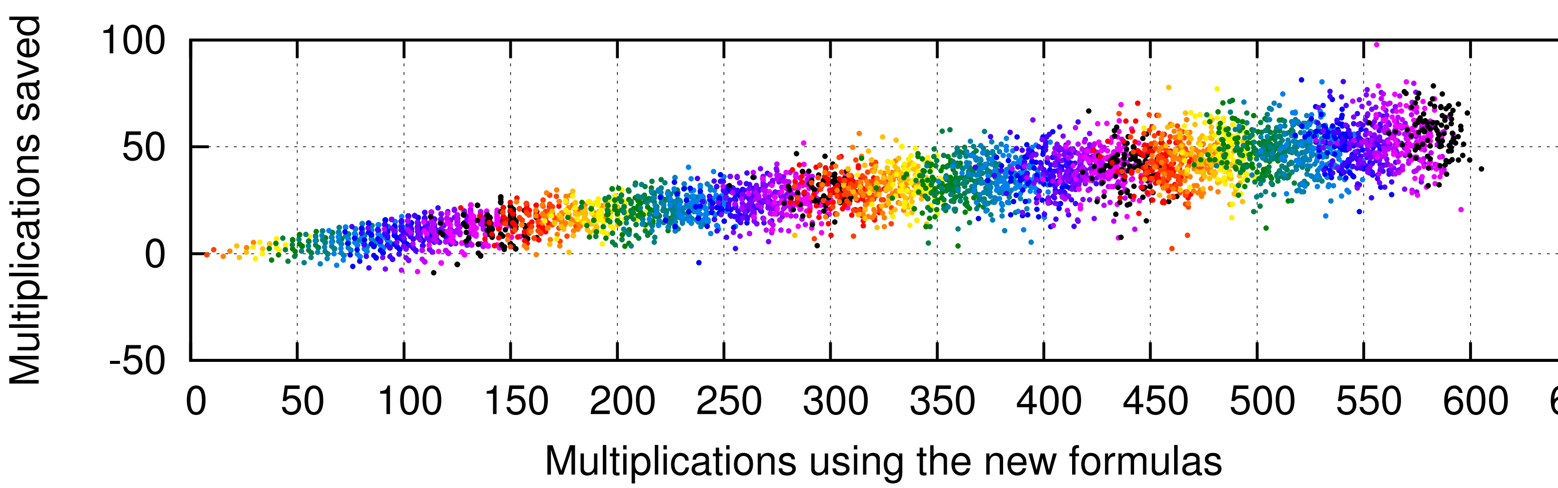
Results

Faster than Weierstrass.

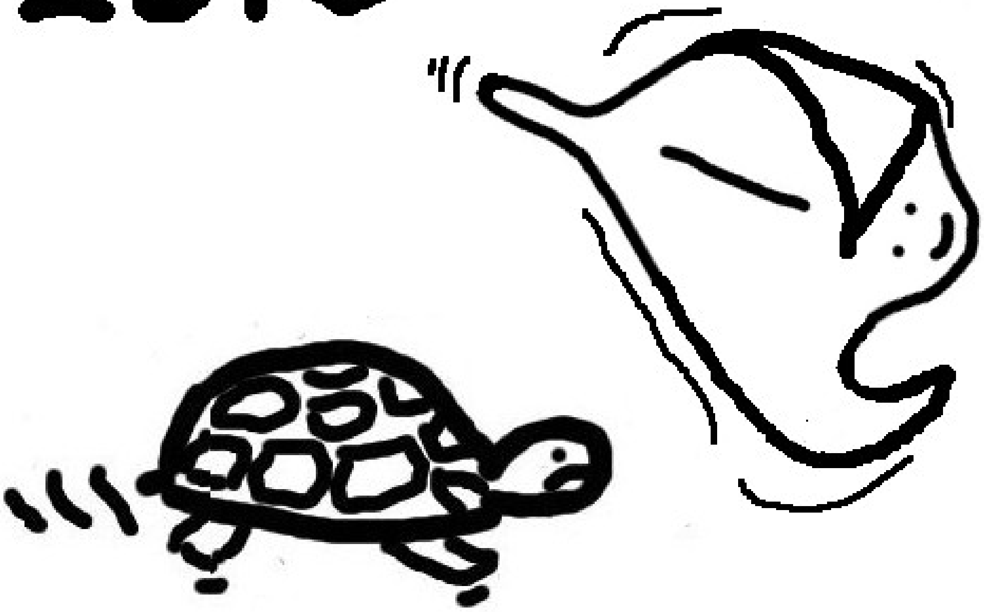
Paper has double-base chain algorithm to use DBL and TPL.

Not good for constant time, fine for signature verification, factorization, math,. . .

Comparison with Weierstrass showing multiplications saved vs. bitlength of scalar.



Mar2015



Twisted Hessian curves beat Weierstrass!

First time cofactor 3 helps.

Something completely different

1985 H. Lange–Ruppert:
$A(\overline{k})$ has a complete system
of addition laws, degree $\le (3,3)$.
Symmetry $\Rightarrow$ degree $\le (2,2)$.

"The proof is nonconstructive. . .
To determine explicitly a
complete system of addition laws
requires tedious computations
already in the easiest case
of an elliptic curve
in Weierstrass normal form."

1985 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for short Weierstrass curves.

Reduce formulas to 53 monomials
by introducing extra variables
$x_i y_j + x_j y_i$, $x_i y_j - x_j y_i$.

1987 Lange–Ruppert:
Explicit complete system
of 3 addition laws
for long Weierstrass curves.

$$
\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3) X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4) X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1) X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2) X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6) X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1) Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6) Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6) X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6) X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2) Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2) Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1) Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4) X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1) Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1) Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1) Z_1 Z_2 + (a_3^3 + 3a_3 a_6) Z_1^2 Z_2^2.
\end{aligned}
$$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2]$.

Previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.

1995 Bosma–Lenstra:
Explicit complete system
of 2 addition laws
for long Weierstrass curves:
$X_3, Y_3, Z_3, X_3', Y_3', Z_3'$
$\in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6,$
$X_1, Y_1, Z_1, X_2, Y_2, Z_2].$

Previous slide in this talk:
Bosma–Lenstra Y_3', Z_3'.
Actually, slide shows
$\text{Publish}(Y_3'), \text{Publish}(Z_3')$,
where Publish introduces typos.

What this means:

For all fields k,
all $\mathbf{P}^2$ Weierstrass curves
$E/k : Y^2Z + a_1XYZ + a_3YZ^2 =$
$X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$,
all $P_1 = (X_1 : Y_1 : Z_1) \in E(k)$,
all $P_2 = (X_2 : Y_2 : Z_2) \in E(k)$:

$(X_3 : Y_3 : Z_3)$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
$(X_3' : Y_3' : Z_3')$
is $P_1 + P_2$ or $(0 : 0 : 0)$;
at most one of these is $(0 : 0 : 0)$.

2009 Bernstein–Lange:

For all fields k with $2 \neq 0$,
all $\mathbf{P}^1 \times \mathbf{P}^1$ Edwards curves E/k :
$X^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2$,

all $P_1, P_2 \in E(k)$,
$P_1 = ((X_1 : Z_1), (Y_1 : T_1))$,
$P_2 = ((X_2 : Z_2), (Y_2 : T_2))$:

$(X_3 : Z_3)$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(X_3' : Z_3')$ is $x(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3 : T_3)$ is $y(P_1 + P_2)$ or $(0 : 0)$;
$(Y_3' : T_3')$ is $y(P_1 + P_2)$ or $(0 : 0)$;
at most one of these is $(0 : 0)$.

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2,$$
$$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2,$$
$$Y_3 = Y_1Y_2Z_1Z_2 - X_1X_2T_1T_2,$$
$$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2,$$

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1,$$
$$Z_3' = X_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1,$$
$$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Much, much, much simpler than Lange–Ruppert, Bosma–Lenstra.

Also much easier to prove.

2015 Bernstein–Chuengsatiansup–Kohel–Lange:

Twisted Hessian curves H/k :
$aX^3 + Y^3 + Z^3 = dXYZ$ in $\mathbf{P}^2$:

$$X_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1,$$
$$Y_3 = Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1,$$
$$Z_3 = Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1.$$

$$X_3' = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2,$$
$$Y_3' = Y_2^2 Y_1 Z_1 - aX_1^2 X_2 Z_2,$$
$$Z_3' = aX_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2.$$

At most one of these is $(0 : 0 : 0)$.

Coincide if both defined.