Fast arithmetic on elliptic curves

D. J. Bernstein
University of Illinois at Chicago

EC point counting

1983 (published 1985) Schoof:
Algorithm to count points on
elliptic curves over finite fields.

Input: prime power q; $a, b \in \mathbf{F}_q$
such that $6(4a^3 + 27b^2) \neq 0$.

Output: $\#\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$y^2 = x^3 + ax + b\} + 1$;
i.e., $\#E(\mathbf{F}_q)$ where E is the
elliptic curve $y^2 = x^3 + ax + b$.

Time: $(\log q)^{O(1)}$.

How? See this afternoon's talk.

ithmetic on elliptic curves

ernstein

sity of Illinois at Chicago

EC point counting

1983 (published 1985) Schoof:
Algorithm to count points on
elliptic curves over finite fields.

Input: prime power q; $a, b \in \mathbf{F}_q$
such that $6(4a^3 + 27b^2) \neq 0$.

Output: $\#\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$y^2 = x^3 + ax + b\} + 1$;
i.e., $\#E(\mathbf{F}_q)$ where E is the
elliptic curve $y^2 = x^3 + ax + b$.

Time: $(\log q)^{O(1)}$.

How? See this afternoon's talk.

Elliptic

1984 (
ECM, t
of facto

1984 (
and ind
1984 (
ECC, e

Bosma
Chudno
elliptic-

These
but sha

on elliptic curves

ois at Chicago

EC point counting

1983 (published 1985) Schoof: Algorithm to count points on elliptic curves over finite fields.

Input: prime power q; $a, b \in \mathbf{F}_q$ such that $6(4a^3 + 27b^2) \neq 0$.

Output: $\#\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : y^2 = x^3 + ax + b\} + 1$;
i.e., $\#E(\mathbf{F}_q)$ where E is the elliptic curve $y^2 = x^3 + ax + b$.

Time: $(\log q)^{O(1)}$.

How? See this afternoon's talk.

Elliptic curves ev

1984 (published
ECM, the elliptic
of factoring integ

1984 (published
and independentl
1984 (published
ECC, elliptic-curv

Bosma, Goldwass
Chudnovsky–Chu
elliptic-curve prim

These application
but share many c

curves

cago

EC point counting

1983 (published 1985) Schoof: Algorithm to count points on elliptic curves over finite fields.

Input: prime power q; $a, b \in \mathbf{F}_q$ such that $6(4a^3 + 27b^2) \neq 0$.

Output: $\#\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : y^2 = x^3 + ax + b\} + 1$;
i.e., $\#E(\mathbf{F}_q)$ where E is the elliptic curve $y^2 = x^3 + ax + b$.

Time: $(\log q)^{O(1)}$.

How? See this afternoon's talk.

Elliptic curves everywhere

1984 (published 1987) Len
ECM, the elliptic-curve me
of factoring integers.

1984 (published 1985) Mill
and independently
1984 (published 1987) Kob
ECC, elliptic-curve cryptog

Bosma, Goldwasser–Kilian,
Chudnovsky–Chudnovsky, A
elliptic-curve primality prov

These applications are diffe
but share many optimizatio

EC point counting

1983 (published 1985) Schoof: Algorithm to count points on elliptic curves over finite fields.

Input: prime power q; $a, b \in \mathbf{F}_q$ such that $6(4a^3 + 27b^2) \neq 0$.

Output: $\#\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : y^2 = x^3 + ax + b\} + 1$;
i.e., $\#E(\mathbf{F}_q)$ where E is the elliptic curve $y^2 = x^3 + ax + b$.

Time: $(\log q)^{O(1)}$.

How? See this afternoon's talk.

Elliptic curves everywhere

1984 (published 1987) Lenstra: ECM, the elliptic-curve method of factoring integers.

1984 (published 1985) Miller, and independently
1984 (published 1987) Koblitz: ECC, elliptic-curve cryptography.

Bosma, Goldwasser–Kilian, Chudnovsky–Chudnovsky, Atkin: elliptic-curve primality proving.

These applications are different but share many optimizations.

nt counting

published 1985) Schoof:
hm to count points on
curves over finite fields.

prime power q; $a, b \in \mathbf{F}_q$
hat $6(4a^3 + 27b^2) \neq 0$.

t: $\#\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : y^2 = x^3 + ax + b\} + 1$;
$E(\mathbf{F}_q)$ where E is the
curve $y^2 = x^3 + ax + b$.

$(\log q)^{O(1)}$.

See this afternoon's talk.

Elliptic curves everywhere

1984 (published 1987) Lenstra:
ECM, the elliptic-curve method
of factoring integers.

1984 (published 1985) Miller,
and independently
1984 (published 1987) Koblitz:
ECC, elliptic-curve cryptography.

Bosma, Goldwasser–Kilian,
Chudnovsky–Chudnovsky, Atkin:
elliptic-curve primality proving.

These applications are different
but share many optimizations.

Represe

Crypto
elliptic

Given n
division
comput
"in 26
but car

"It app
represe
in the
Each p
triple (
to the

ng

1985) Schoof:
unt points on
er finite fields.

ver q; $a, b \in \mathbf{F}_q$
$+ 27b^2) \neq 0$.

$) \in \mathbf{F}_q \times \mathbf{F}_q$:
$b\} + 1$;
ere E is the
$= x^3 + ax + b$.
).

fternoon's talk.

Elliptic curves everywhere

1984 (published 1987) Lenstra:
ECM, the elliptic-curve method
of factoring integers.

1984 (published 1985) Miller,
and independently
1984 (published 1987) Koblitz:
ECC, elliptic-curve cryptography.

Bosma, Goldwasser–Kilian,
Chudnovsky–Chudnovsky, Atkin:
elliptic-curve primality proving.

These applications are different
but share many optimizations.

Representing cur

Crypto 1985, Mil
elliptic curves in

Given $n \in \mathbf{Z}$, $P \in$
division-polynom
computes $nP \in$
"in $26 \log_2 n$ mu
but can do bette

"It appears to be
represent the poi
in the following f
Each point is rep
triple (x, y, z) wh
to the point $(x/z$

oof:
on
elds.
$\in \mathbf{F}_q$
0.
$\mathbf{F}_q$:
ne
$c + b$.
talk.

Elliptic curves everywhere

1984 (published 1987) Lenstra: ECM, the elliptic-curve method of factoring integers.

1984 (published 1985) Miller, and independently
1984 (published 1987) Koblitz: ECC, elliptic-curve cryptography.

Bosma, Goldwasser–Kilian, Chudnovsky–Chudnovsky, Atkin: elliptic-curve primality proving.

These applications are different but share many optimizations.

Representing curve points

Crypto 1985, Miller, "Use
elliptic curves in cryptogra

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$,
division-polynomial recurre
computes $nP \in E(\mathbf{F}_q)$
"in $26 \log_2 n$ multiplication
but can do better!

"It appears to be best to represent the points on the
in the following form:
Each point is represented b
triple (x, y, z) which corres
to the point $(x/z^2, y/z^3)$."

Elliptic curves everywhere

1984 (published 1987) Lenstra: ECM, the elliptic-curve method of factoring integers.

1984 (published 1985) Miller, and independently
1984 (published 1987) Koblitz: ECC, elliptic-curve cryptography.

Bosma, Goldwasser–Kilian, Chudnovsky–Chudnovsky, Atkin: elliptic-curve primality proving.

These applications are different but share many optimizations.

Representing curve points

Crypto 1985, Miller, "Use of elliptic curves in cryptography":

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$, division-polynomial recurrence computes $nP \in E(\mathbf{F}_q)$
"in $26 \log_2 n$ multiplications"; but can do better!

"It appears to be best to represent the points on the curve in the following form:
Each point is represented by the triple (x, y, z) which corresponds to the point $(x/z^2, y/z^3)$."

curves everywhere

published 1987) Lenstra:
the elliptic-curve method
bring integers.

published 1985) Miller,
dependently
published 1987) Koblitz:
elliptic-curve cryptography.

, Goldwasser–Kilian,
ovsky–Chudnovsky, Atkin:
-curve primality proving.

applications are different
are many optimizations.

Representing curve points

Crypto 1985, Miller, "Use of elliptic curves in cryptography":

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$,
division-polynomial recurrence
computes $nP \in E(\mathbf{F}_q)$
"in $26 \log_2 n$ multiplications";
but can do better!

"It appears to be best to represent the points on the curve in the following form:
Each point is represented by the triple (x, y, z) which corresponds to the point $(x/z^2, y/z^3)$."

Note th
has ma
in this
e.g., (7
represe
or (126

Can us
to avoi
Most E

Good i
M is co
I is cos
Typical

erywhere

1987) Lenstra:
c-curve method
gers.

1985) Miller,
ly
1987) Koblitz:
ve cryptography.

ser–Kilian,
udnovsky, Atkin:
mality proving.

ns are different
optimizations.

Representing curve points

Crypto 1985, Miller, "Use of elliptic curves in cryptography":

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$, division-polynomial recurrence computes $nP \in E(\mathbf{F}_q)$
"in $26 \log_2 n$ multiplications";
but can do better!

"It appears to be best to represent the points on the curve in the following form:
Each point is represented by the triple (x, y, z) which corresponds to the point $(x/z^2, y/z^3)$."

Note that each p
has many represe
in this traditiona
e.g., $(7/2, 5/3)$ c
represented as (7
or $(126 : 360 : 6)$

Can use this flexi
to avoid, or delay
Most ECC softwa

Good idea if **I**/**M**
M is cost of mul
I is cost of invert
Typical software:

stra:
thod

ler,

blitz:
graphy.

Atkin:
ying.

erent
ons.

Representing curve points

Crypto 1985, Miller, "Use of elliptic curves in cryptography":

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$,
division-polynomial recurrence
computes $nP \in E(\mathbf{F}_q)$
"in $26 \log_2 n$ multiplications";
but can do better!

"It appears to be best to represent the points on the curve in the following form:
Each point is represented by the triple (x, y, z) which corresponds to the point $(x/z^2, y/z^3)$."

Note that each point has many representations in this traditional form: e.g., $(7/2, 5/3)$ can be represented as $(7/2 : 5/3 :$ or $(126 : 360 : 6)$ or ...

Can use this flexibility to avoid, or delay, divisions Most ECC software does th

Good idea if $\mathbf{I}/\mathbf{M}$ is big, w
$\mathbf{M}$ is cost of multiplying in
$\mathbf{I}$ is cost of inverting in $\mathbf{F}_q$.
Typical software: $\mathbf{I}/\mathbf{M} > 1$

Representing curve points

Crypto 1985, Miller, "Use of elliptic curves in cryptography":

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$, division-polynomial recurrence computes $nP \in E(\mathbf{F}_q)$ "in $26 \log_2 n$ multiplications"; but can do better!

"It appears to be best to represent the points on the curve in the following form: Each point is represented by the triple (x, y, z) which corresponds to the point $(x/z^2, y/z^3)$."

Note that each point has many representations in this traditional form: e.g., $(7/2, 5/3)$ can be represented as $(7/2 : 5/3 : 1)$ or $(126 : 360 : 6)$ or ...

Can use this flexibility to avoid, or delay, divisions. Most ECC software does this.

Good idea if $\mathbf{I}/\mathbf{M}$ is big, where $\mathbf{M}$ is cost of multiplying in $\mathbf{F}_q$, $\mathbf{I}$ is cost of inverting in $\mathbf{F}_q$. Typical software: $\mathbf{I}/\mathbf{M} > 10$.

enting curve points

1985, Miller, "Use of
curves in cryptography":

$n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$,
n-polynomial recurrence
tes $nP \in E(\mathbf{F}_q)$
$\log_2 n$ multiplications";
n do better!

pears to be best to
nt the points on the curve
following form:
oint is represented by the
$x, y, z)$ which corresponds
point $(x/z^2, y/z^3)$."

Note that each point
has many representations
in this traditional form:
e.g., $(7/2, 5/3)$ can be
represented as $(7/2 : 5/3 : 1)$
or $(126 : 360 : 6)$ or ...

Can use this flexibility
to avoid, or delay, divisions.
Most ECC software does this.

Good idea if $\mathbf{I}/\mathbf{M}$ is big, where
$\mathbf{M}$ is cost of multiplying in $\mathbf{F}_q$,
$\mathbf{I}$ is cost of inverting in $\mathbf{F}_q$.
Typical software: $\mathbf{I}/\mathbf{M} > 10$.

1986 C
"Seque
generat
in form
and ne
and fac

"The c
the cho
of an a
where
are the

Most i
ADD is
DBL is

ve points

ller, "Use of
cryptography":

$\in E(\mathbf{F}_q)$,
ial recurrence
$E(\mathbf{F}_q)$
ltiplications";
r!

e best to
nts on the curve
form:
presented by the
hich corresponds
$z^2, y/z^3)$."

Note that each point
has many representations
in this traditional form:
e.g., $(7/2, 5/3)$ can be
represented as $(7/2 : 5/3 : 1)$
or $(126 : 360 : 6)$ or ...

Can use this flexibility
to avoid, or delay, divisions.
Most ECC software does this.

Good idea if $\mathbf{I}/\mathbf{M}$ is big, where
$\mathbf{M}$ is cost of multiplying in $\mathbf{F}_q$,
$\mathbf{I}$ is cost of inverting in $\mathbf{F}_q$.
Typical software: $\mathbf{I}/\mathbf{M} > 10$.

1986 Chudnovsky
"Sequences of nu
generated by ado
in formal groups
and new primalit
and factorization

"The crucial prob
the choice of the
of an algebraic g
where computati
are the least time

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

of
phy”:

nce

ns”;

e curve

by the
sponds
”

Note that each point
has many representations
in this traditional form:
e.g., $(7/2, 5/3)$ can be
represented as $(7/2 : 5/3 : 1)$
or $(126 : 360 : 6)$ or ...

Can use this flexibility
to avoid, or delay, divisions.
Most ECC software does this.

Good idea if $\mathbf{I}/\mathbf{M}$ is big, where
$\mathbf{M}$ is cost of multiplying in $\mathbf{F}_q$,
$\mathbf{I}$ is cost of inverting in $\mathbf{F}_q$.
Typical software: $\mathbf{I}/\mathbf{M} > 10$.

1986 Chudnovsky–Chudnov
“Sequences of numbers
generated by addition
in formal groups
and new primality
and factorization tests”:

“The crucial problem beco
the choice of the model
of an algebraic group varie
where computations mod p
are the least time consumi

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

Note that each point
has many representations
in this traditional form:
e.g., $(7/2, 5/3)$ can be
represented as $(7/2 : 5/3 : 1)$
or $(126 : 360 : 6)$ or ...

Can use this flexibility
to avoid, or delay, divisions.
Most ECC software does this.

Good idea if $\mathbf{I}/\mathbf{M}$ is big, where
$\mathbf{M}$ is cost of multiplying in $\mathbf{F}_q$,
$\mathbf{I}$ is cost of inverting in $\mathbf{F}_q$.
Typical software: $\mathbf{I}/\mathbf{M} > 10$.

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 $P \mapsto 2P$.

hat each point
ny representations
traditional form:
$7/2, 5/3)$ can be
nted as $(7/2 : 5/3 : 1)$
$6 : 360 : 6)$ or ...

e this flexibility
d, or delay, divisions.
ECC software does this.

dea if $\mathbf{I}/\mathbf{M}$ is big, where
ost of multiplying in $\mathbf{F}_q$,
st of inverting in $\mathbf{F}_q$.
l software: $\mathbf{I}/\mathbf{M} > 10$.

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 p
models
lying in
for oth
coordin
increas
4 basic

Short W
$y^2 = x$

Jacobi
$s^2 + c^2$

Jacobi

Hessian

oint
entations
l form:
can be
7/2 : 5/3 : 1)
or . . .

ibility
y, divisions.
are does this.

M is big, where
tiplying in $\mathbf{F}_q$,
ting in $\mathbf{F}_q$.
$\mathbf{I}/\mathbf{M} > 10$.

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 t
models of elliptic
lying in low-dime
for otherwise the
coordinates and
increasing. This
4 basic models o

Short Weierstrass
$y^2 = x^3 + ax +$

Jacobi intersectio
$s^2 + c^2 = 1$, as^2

Jacobi quartic: y

Hessian: $x^3 + y^3$

1)

s.

his.

here

$\mathbf{F}_q$,

0.

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 sp
for otherwise the number o
coordinates and operations
increasing. This limits us .
4 basic models of elliptic c

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

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

Jacobi quartic: $y^2 = x^4+2$

Hessian: $x^3 + y^3 + 1 = 3d$

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

Chudnovsky–Chudnovsky,
ences of numbers
ted by addition
nal groups
w primality
ctorization tests”:

crucial problem becomes
oice of the model
lgebraic group variety,
computations mod p
least time consuming.”

mportant computations:
s $P, Q \mapsto P + Q$.
$P \mapsto 2P$.

“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.”

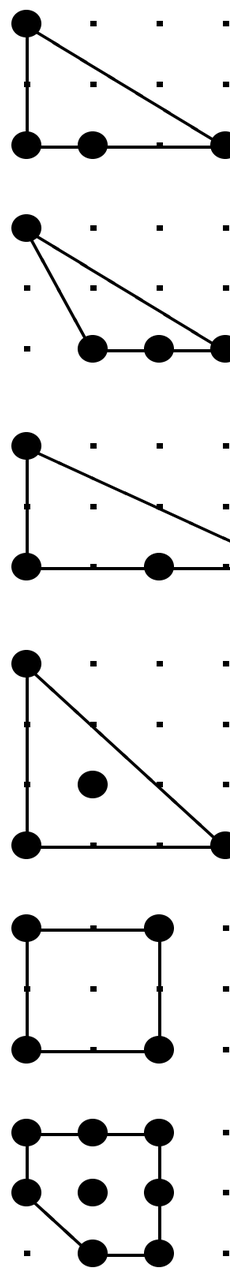
Short Weierstrass:
$y^2 = x^3 + ax + b$.

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

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

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

Some M



y–Chudnovsky,
umbers
dition

y
tests”:

blem becomes
model
roup variety,
ons mod p
e consuming.”

computations:
$P + Q$.

“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.”

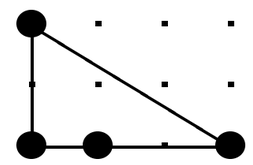
Short Weierstrass:
$y^2 = x^3 + ax + b$.

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

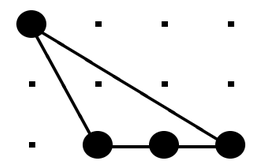
Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.

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

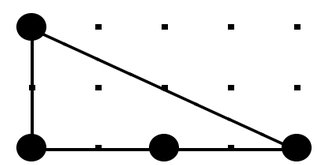
Some Newton po



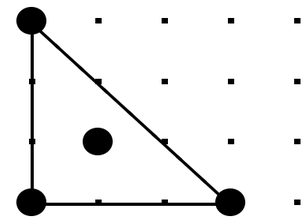
Short W



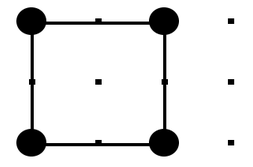
Montg



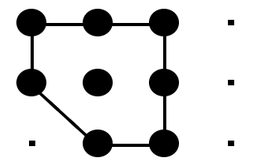
Jacobi



Hessian



Edward



Binary

vsky,

mes

ty,
p
ng."

ons:

"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."

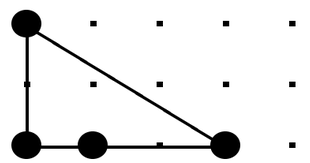
Short Weierstrass:
$y^2 = x^3 + ax + b$.

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

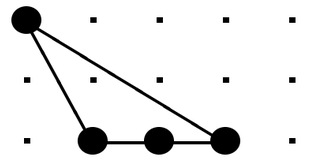
Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.

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

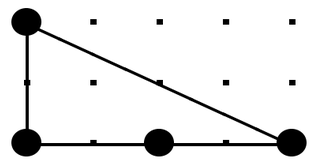
Some Newton polygons



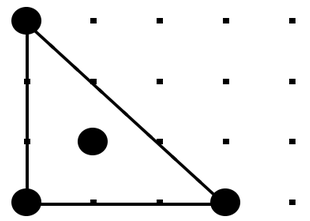
Short Weierstrass



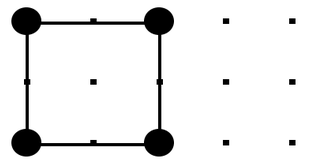
Montgomery



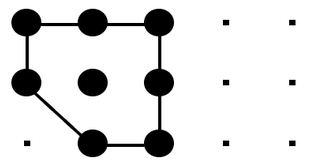
Jacobi quartic



Hessian



Edwards



Binary Edwards

"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."

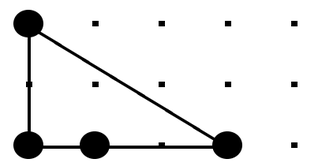
Short Weierstrass:
$y^2 = x^3 + ax + b$.

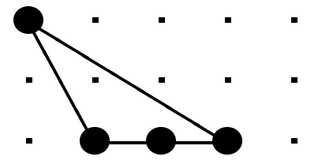
Jacobi intersection:
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

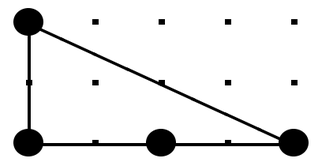
Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$.

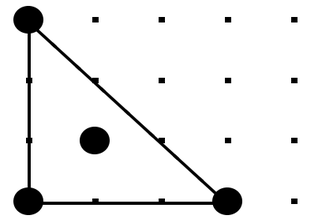
Hessian: $x^3 + y^3 + 1 = 3dxy$.

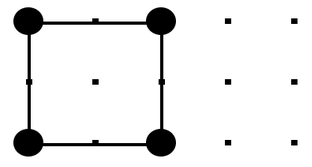
Some Newton polygons

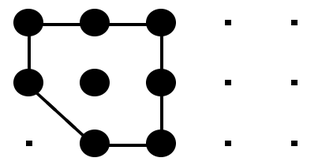

Short Weierstrass


Montgomery


Jacobi quartic


Hessian


Edwards


Binary Edwards

preferable to use
s of elliptic curves
n low-dimensional spaces,
erwise the number of
nates and operations is
ing. This limits us . . . to
models of elliptic curves."

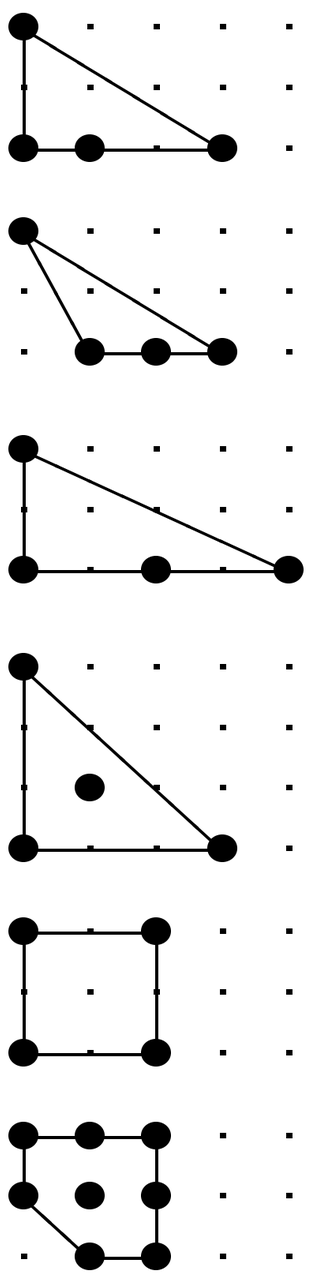
Weierstrass:
$^3 + ax + b$.

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

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

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

Some Newton polygons



Short Weierstrass

Montgomery

Jacobi quartic

Hessian

Edwards

Binary Edwards

Optimi

For "tr
on $y^2 =$
1986 C
state e
10**M** fo

Conseq
$\approx \left(10\right.$
to com
using s
of scala

Notatio

to use
c curves
ensional spaces,
number of
operations is
limits us . . . to
f elliptic curves."

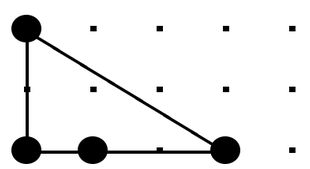
s:
b.

on:
$+ d^2 = 1$.

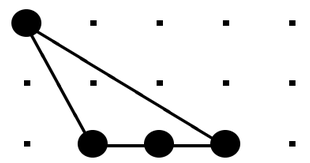
$y^2 = x^4+2ax^2+1$.

$^3 + 1 = 3dxy$.

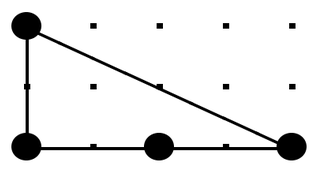
Some Newton polygons



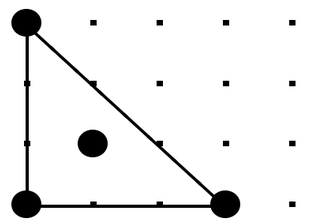
Short Weierstrass



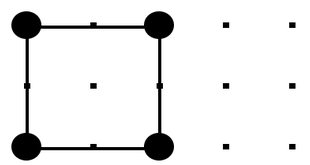
Montgomery



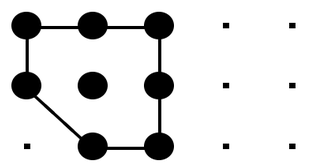
Jacobi quartic



Hessian



Edwards



Binary Edwards

Optimizing Jacob

For "traditional"
on $y^2 = x^3 + ax$
1986 Chudnovsky
state explicit form
10**M** for DBL; 16

Consequence:
$\approx \left(10 \lg n + 16\right.$

to compute n, P
using sliding-win
of scalar multipli

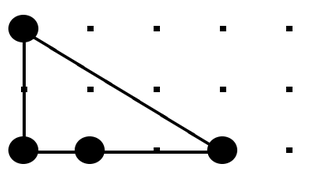
Notation: lg = lo

aces,
of
s is
.. to
urves."

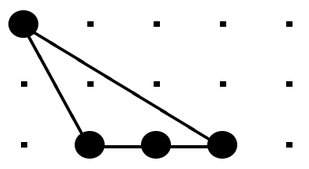
$2ax^2+1$.

dxy.

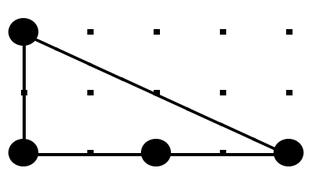
Some Newton polygons



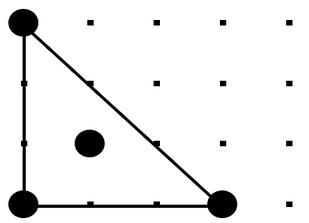
Short Weierstrass



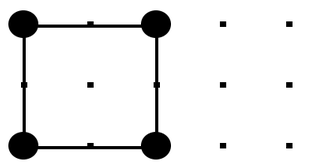
Montgomery



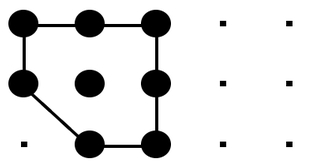
Jacobi quartic



Hessian



Edwards



Binary Edwards

Optimizing Jacobian coord

For "traditional" $(X/Z^2, Y$
on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnov
state explicit formulas usin
10**M** for DBL; 16**M** for AD

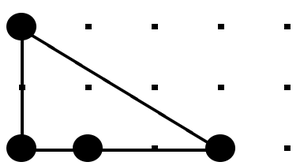
Consequence:

$$\approx \left(10 \lg n + 16 \frac{\lg n}{\lg \lg n}\right)\mathbf{M}$$

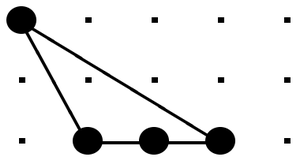
to compute n, $P \mapsto nP$
using sliding-windows meth
of scalar multiplication.

Notation: $\lg = \log_2$.

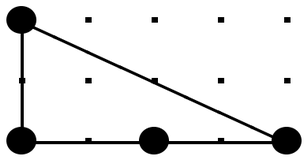
Some Newton polygons



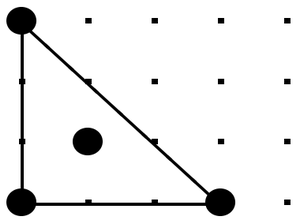
Short Weierstrass



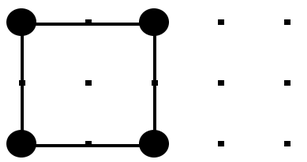
Montgomery



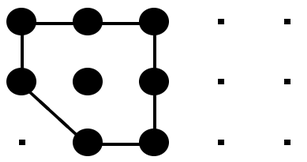
Jacobi quartic



Hessian



Edwards



Binary Edwards

Optimizing Jacobian coordinates

For "traditional" $(X/Z^2, Y/Z^3)$ on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnovsky state explicit formulas using 10**M** for DBL; 16**M** for ADD.

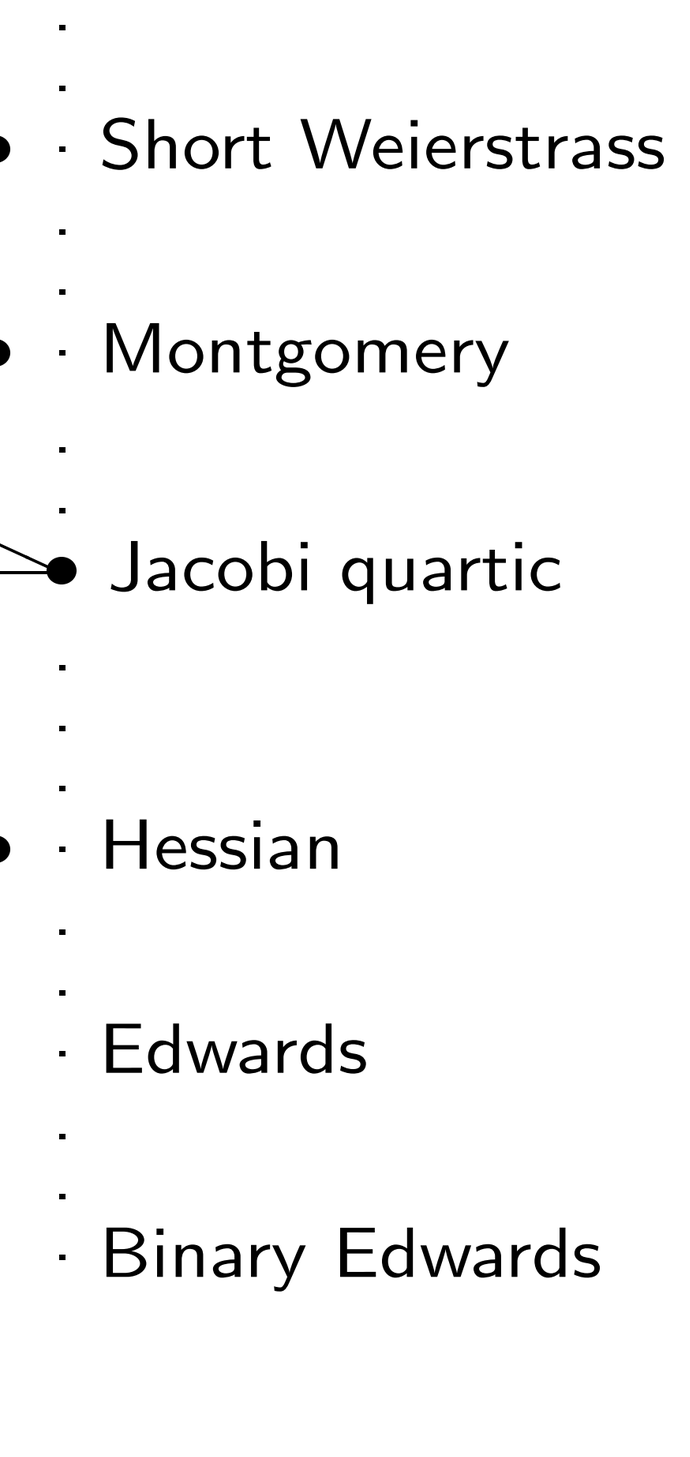
Consequence:

$$\approx \left(10 \lg n + 16 \frac{\lg n}{\lg \lg n}\right) \mathbf{M}$$

to compute n, $P \mapsto nP$ using sliding-windows method of scalar multiplication.

Notation: $\lg = \log_2$.

Newton polygons



Optimizing Jacobian coordinates

For "traditional" $(X/Z^2, Y/Z^3)$ on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnovsky state explicit formulas using 10**M** for DBL; 16**M** for ADD.

Consequence:

$$\approx \left(10 \lg n + 16 \frac{\lg n}{\lg \lg n}\right) \mathbf{M}$$

to compute n, $P \mapsto nP$ using sliding-windows method of scalar multiplication.

Notation: $\lg = \log_2$.

Squarin

Here a

$S =$

$M =$

$T =$

$X_3 =$

$Y_3 =$

$Z_3 =$

Total c

S is th

D is th

The sq

X_1^2, Y_1^2

olygons

Weierstrass

omery

quartic

n

ds

Edwards

Optimizing Jacobian coordinates

For "traditional" $(X/Z^2, Y/Z^3)$ on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnovsky state explicit formulas using 10**M** for DBL; 16**M** for ADD.

Consequence:

$$\approx \left(10 \lg n + 16 \frac{\lg n}{\lg \lg n}\right)\mathbf{M}$$

to compute n, $P \mapsto nP$ using sliding-windows method of scalar multiplication.

Notation: $\lg = \log_2$.

Squaring is faste

Here are the DBL

$S = 4X_1 \cdot Y_1^2;$
$M = 3X_1^2 + aZ$
$T = M^2 - 2S;$
$X_3 = T;$
$Y_3 = M \cdot (S -$
$Z_3 = 2Y_1 \cdot Z_1.$

Total cost 3**M** +
S is the cost of s
D is the cost of

The squarings pr
$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z$

s

Optimizing Jacobian coordinates

For "traditional" $(X/Z^2, Y/Z^3)$ on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnovsky state explicit formulas using 10**M** for DBL; 16**M** for ADD.

Consequence:
$$\approx \left(10 \lg n + 16 \frac{\lg n}{\lg \lg n}\right)\mathbf{M}$$
to compute n, $P \mapsto nP$ using sliding-windows method of scalar multiplication.

Notation: $\lg = \log_2$.

Squaring is faster than **M**.

Here are the DBL formulas
$S = 4X_1 \cdot Y_1^2$;
$M = 3X_1^2 + aZ_1^4$;
$T = M^2 - 2S$;
$X_3 = T$;
$Y_3 = M \cdot (S - T) - 8Y_1^4$
$Z_3 = 2Y_1 \cdot Z_1$.

Total cost 3**M** + 6**S** + 1**D**
S is the cost of squaring in
D is the cost of multiplying

The squarings produce
$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z_1^4, M^2$.

Optimizing Jacobian coordinates

For "traditional" $(X/Z^2, Y/Z^3)$
on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnovsky
state explicit formulas using
10**M** for DBL; 16**M** for ADD.

Consequence:

$$\approx \left(10 \lg n + 16 \frac{\lg n}{\lg \lg n}\right)\mathbf{M}$$

to compute n, $P \mapsto nP$
using sliding-windows method
of scalar multiplication.

Notation: $\lg = \log_2$.

Squaring is faster than **M**.

Here are the DBL formulas:

$S = 4X_1 \cdot Y_1^2$;
$M = 3X_1^2 + aZ_1^4$;
$T = M^2 - 2S$;
$X_3 = T$;
$Y_3 = M \cdot (S - T) - 8Y_1^4$;
$Z_3 = 2Y_1 \cdot Z_1$.

Total cost $3\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ where
S is the cost of squaring in $\mathbf{F}_q$,
D is the cost of multiplying by a.

The squarings produce
$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z_1^4, M^2$.

zing Jacobian coordinates

raditional" $(X/Z^2, Y/Z^3)$
$= x^3 + ax + b$:
Chudnovsky–Chudnovsky
xplicit formulas using
or DBL; 16**M** for ADD.

quence:

$$\lg n + 16\frac{\lg n}{\lg\lg n}\Big)\mathbf{M}$$

pute n, $P \mapsto nP$
liding-windows method
ar multiplication.

on: $\lg = \log_2$.

Squaring is faster than **M**.

Here are the DBL formulas:

$S = 4X_1 \cdot Y_1^2$;
$M = 3X_1^2 + aZ_1^4$;
$T = M^2 - 2S$;
$X_3 = T$;
$Y_3 = M \cdot (S - T) - 8Y_1^4$;
$Z_3 = 2Y_1 \cdot Z_1$.

Total cost $3\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ where
S is the cost of squaring in $\mathbf{F}_q$,
D is the cost of multiplying by a.

The squarings produce
$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z_1^4, M^2$.

Most E
curves

Curve-
1986 C

Can eli
by cho

But "it
to cho

If $a =$
$= 3(X_1$
Replac

Now D

bian coordinates

$(X/Z^2, Y/Z^3)$

$+ b$:

y–Chudnovsky

mulas using

6**M** for ADD.

$$\frac{\lg n}{\lg \lg n}\Big)\mathbf{M}$$

$\mapsto nP$

dows method

cation.

$\log_2$.

Squaring is faster than **M**.

Here are the DBL formulas:

$S = 4X_1 \cdot Y_1^2;$

$M = 3X_1^2 + aZ_1^4;$

$T = M^2 - 2S;$

$X_3 = T;$

$Y_3 = M \cdot (S - T) - 8Y_1^4;$

$Z_3 = 2Y_1 \cdot Z_1.$

Total cost $3\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ where

S is the cost of squaring in $\mathbf{F}_q$,

D is the cost of multiplying by a.

The squarings produce

$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z_1^4, M^2$.

Most ECC standa

curves that make

Curve-choice adv

1986 Chudnovsky

Can eliminate th

by choosing curv

But "it is even s

to choose curve

If $a = -3$ then M

$= 3(X_1 - Z_1^2) \cdot ($

Replace $2\mathbf{S}$ with

Now DBL costs 4

inates

$/Z^3$)

vsky

g

DD.

hod

Squaring is faster than **M**.

Here are the DBL formulas:

$S = 4X_1 \cdot Y_1^2$;
$M = 3X_1^2 + aZ_1^4$;
$T = M^2 - 2S$;
$X_3 = T$;
$Y_3 = M \cdot (S - T) - 8Y_1^4$;
$Z_3 = 2Y_1 \cdot Z_1$.

Total cost $3\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ where
S is the cost of squaring in $\mathbf{F}_q$,
D is the cost of multiplying by a.

The squarings produce
$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z_1^4, M^2$.

Most ECC standards choos
curves that make formulas

Curve-choice advice from
1986 Chudnovsky–Chudno

Can eliminate the 1**D**
by choosing curve with $a =$

But "it is even smarter"
to choose curve with $a =$

If $a = -3$ then $M = 3(X_1^2$
$= 3(X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$
Replace 2**S** with 1**M**.

Now DBL costs $4\mathbf{M} + 4\mathbf{S}$.

Squaring is faster than **M**.

Here are the DBL formulas:

$S = 4X_1 \cdot Y_1^2$;
$M = 3X_1^2 + aZ_1^4$;
$T = M^2 - 2S$;
$X_3 = T$;
$Y_3 = M \cdot (S - T) - 8Y_1^4$;
$Z_3 = 2Y_1 \cdot Z_1$.

Total cost $3\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ where
S is the cost of squaring in $\mathbf{F}_q$,
D is the cost of multiplying by a.

The squarings produce
$X_1^2, Y_1^2, Y_1^4, Z_1^2, Z_1^4, M^2$.

Most ECC standards choose
curves that make formulas faster.

Curve-choice advice from
1986 Chudnovsky–Chudnovsky:

Can eliminate the 1**D**
by choosing curve with $a = 1$.

But "it is even smarter"
to choose curve with $a = -3$.

If $a = -3$ then $M = 3(X_1^2 - Z_1^4)$
$= 3(X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$.
Replace 2**S** with 1**M**.

Now DBL costs $4\mathbf{M} + 4\mathbf{S}$.

ng is faster than **M**.

re the DBL formulas:

$4X_1 \cdot Y_1^2$;

$= 3X_1^2 + aZ_1^4$;

$M^2 - 2S$;

$= T$;

$= M \cdot (S - T) - 8Y_1^4$;

$= 2Y_1 \cdot Z_1$.

cost $3\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ where

e cost of squaring in $\mathbf{F}_q$,

he cost of multiplying by a.

uarings produce

$, Y_1^4, Z_1^2, Z_1^4, M^2$.

Most ECC standards choose curves that make formulas faster.

Curve-choice advice from 1986 Chudnovsky–Chudnovsky:

Can eliminate the $1\mathbf{D}$ by choosing curve with $a = 1$.

But "it is even smarter" to choose curve with $a = -3$.

If $a = -3$ then $M = 3(X_1^2 - Z_1^4)$ $= 3(X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$.
Replace $2\mathbf{S}$ with $1\mathbf{M}$.

Now DBL costs $4\mathbf{M} + 4\mathbf{S}$.

2001 B

$3\mathbf{M} + 5$

$11\mathbf{M} +$

How?

instead

comput

DBL fo

comput

Same i

but hav

to elim

r than **M**.

L formulas:

Z_1^4;

;

$T) - 8Y_1^4$;

$6\mathbf{S} + 1\mathbf{D}$ where
squaring in $\mathbf{F}_q$,
multiplying by a.

oduce
Z_1^4, M^2.

Most ECC standards choose
curves that make formulas faster.

Curve-choice advice from
1986 Chudnovsky–Chudnovsky:

Can eliminate the $1\mathbf{D}$
by choosing curve with $a = 1$.

But "it is even smarter"
to choose curve with $a = -3$.

If $a = -3$ then $M = 3(X_1^2 - Z_1^4)$
$= 3(X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$.
Replace $2\mathbf{S}$ with $1\mathbf{M}$.

Now DBL costs $4\mathbf{M} + 4\mathbf{S}$.

2001 Bernstein:
$3\mathbf{M} + 5\mathbf{S}$ for DB
$11\mathbf{M} + 5\mathbf{S}$ for AD

How? Easy $\mathbf{S}$ –
instead of compu
compute $(Y_1 + Z$
DBL formulas we
computing Y_1^2 an

Same idea for th
but have to scale
to eliminate divis

s:

;

where
$\mathbf{F}_q$,
g by a.

Most ECC standards choose
curves that make formulas faster.

Curve-choice advice from
1986 Chudnovsky–Chudnovsky:

Can eliminate the 1**D**
by choosing curve with $a = 1$.

But "it is even smarter"
to choose curve with $a = -3$.

If $a = -3$ then $M = 3(X_1^2 - Z_1^4)$
$= 3(X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$.
Replace 2**S** with 1**M**.

Now DBL costs $4\mathbf{M} + 4\mathbf{S}$.

2001 Bernstein:
$3\mathbf{M} + 5\mathbf{S}$ for DBL.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.

How? Easy $\mathbf{S} - \mathbf{M}$ tradeof
instead of computing $2Y_1 \cdot$
compute $(Y_1 + Z_1)^2 - Y_1^2$
DBL formulas were already
computing Y_1^2 and Z_1^2.

Same idea for the ADD for
but have to scale X, Y, Z
to eliminate divisions by 2.

Most ECC standards choose
curves that make formulas faster.

Curve-choice advice from
1986 Chudnovsky–Chudnovsky:

Can eliminate the 1**D**
by choosing curve with $a = 1$.

But "it is even smarter"
to choose curve with $a = -3$.

If $a = -3$ then $M = 3(X_1^2 - Z_1^4)$
$= 3(X_1 - Z_1^2) \cdot (X_1 + Z_1^2)$.
Replace 2**S** with 1**M**.

Now DBL costs $4\mathbf{M} + 4\mathbf{S}$.

2001 Bernstein:
$3\mathbf{M} + 5\mathbf{S}$ for DBL.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.

How? Easy $\mathbf{S} - \mathbf{M}$ tradeoff:
instead of computing $2Y_1 \cdot Z_1$,
compute $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.
DBL formulas were already
computing Y_1^2 and Z_1^2.

Same idea for the ADD formulas,
but have to scale X, Y, Z
to eliminate divisions by 2.

ECC standards choose
that make formulas faster.

choice advice from
Chudnovsky–Chudnovsky:

minate the 1**D**
osing curve with $a = 1$.

t is even smarter"
ose curve with $a = -3$.

-3 then $M = 3(X_1^2 - Z_1^4)$
$_1 - Z_1^2) \cdot (X_1 + Z_1^2)$.
e 2**S** with 1**M**.

BL costs $4\mathbf{M} + 4\mathbf{S}$.

2001 Bernstein:
$3\mathbf{M} + 5\mathbf{S}$ for DBL.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.

How? Easy $\mathbf{S} - \mathbf{M}$ tradeoff:
instead of computing $2Y_1 \cdot Z_1$,
compute $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.
DBL formulas were already
computing Y_1^2 and Z_1^2.

Same idea for the ADD formulas,
but have to scale X, Y, Z
to eliminate divisions by 2.

ADD fo
$U_1 = X$
$S_1 = Y$
many m

1986 C
"We su
additio
$(X, Y, Z$

Disadv
Allocat
Pay 1**S**

Advant
Save 2
Save 1

ards choose
e formulas faster.

vice from
y–Chudnovsky:

e 1**D**
e with $a = 1$.

marter"
with $a = -3$.

$M = 3(X_1^2 - Z_1^4)$
$X_1 + Z_1^2)$.
1**M**.

4**M** + 4**S**.

2001 Bernstein:
3**M** + 5**S** for DBL.
11**M** + 5**S** for ADD.

How? Easy **S** − **M** tradeoff:
instead of computing $2Y_1 \cdot Z_1$,
compute $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.
DBL formulas were already
computing Y_1^2 and Z_1^2.

Same idea for the ADD formulas,
but have to scale X, Y, Z
to eliminate divisions by 2.

ADD for $y^2 = x^3$
$U_1 = X_1 Z_2^2$, $U_2 =$
$S_1 = Y_1 Z_2^3$, $S_2 =$
many more comp

1986 Chudnovsky
"We suggest to w
addition formulas
(X, Y, Z, Z^2, Z^3)

Disadvantages:
Allocate space fo
Pay 1**S** + 1**M** in A

Advantages:
Save 2**S** + 2**M** at
Save 1**S** at start

se
faster.

vsky:

$= 1$.

-3.

$- Z_1^4)$

.

2001 Bernstein:
$3\mathbf{M} + 5\mathbf{S}$ for DBL.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.

How? Easy $\mathbf{S} - \mathbf{M}$ tradeoff:
instead of computing $2Y_1 \cdot Z_1$,
compute $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.
DBL formulas were already
computing Y_1^2 and Z_1^2.

Same idea for the ADD formulas,
but have to scale X, Y, Z
to eliminate divisions by 2.

ADD for $y^2 = x^3 + ax + b$
$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,
many more computations.

1986 Chudnovsky–Chudnov
"We suggest to write
addition formulas involving
(X, Y, Z, Z^2, Z^3)."

Disadvantages:
Allocate space for Z^2, Z^3.
Pay $1\mathbf{S} + 1\mathbf{M}$ in ADD and

Advantages:
Save $2\mathbf{S} + 2\mathbf{M}$ at start of A
Save $1\mathbf{S}$ at start of DBL.

2001 Bernstein:
$3\mathbf{M} + 5\mathbf{S}$ for DBL.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.

How? Easy $\mathbf{S} - \mathbf{M}$ tradeoff:
instead of computing $2Y_1 \cdot Z_1$,
compute $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.
DBL formulas were already
computing Y_1^2 and Z_1^2.

Same idea for the ADD formulas,
but have to scale X, Y, Z
to eliminate divisions by 2.

ADD for $y^2 = x^3 + ax + b$:
$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,
many more computations.

1986 Chudnovsky–Chudnovsky:
"We suggest to write
addition formulas involving
(X, Y, Z, Z^2, Z^3)."

Disadvantages:
Allocate space for Z^2, Z^3.
Pay $1\mathbf{S} + 1\mathbf{M}$ in ADD and in DBL.

Advantages:
Save $2\mathbf{S} + 2\mathbf{M}$ at start of ADD.
Save $1\mathbf{S}$ at start of DBL.

Bernstein:
$5\mathbf{S}$ for DBL.
$+ 5\mathbf{S}$ for ADD.

Easy $\mathbf{S} - \mathbf{M}$ tradeoff:
of computing $2Y_1 \cdot Z_1$,
te $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.
ormulas were already
ting Y_1^2 and Z_1^2.

dea for the ADD formulas,
ve to scale X, Y, Z
inate divisions by 2.

ADD for $y^2 = x^3 + ax + b$:
$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,
many more computations.

1986 Chudnovsky–Chudnovsky:
"We suggest to write
addition formulas involving
(X, Y, Z, Z^2, Z^3)."

Disadvantages:
Allocate space for Z^2, Z^3.
Pay $1\mathbf{S} + 1\mathbf{M}$ in ADD and in DBL.

Advantages:
Save $2\mathbf{S} + 2\mathbf{M}$ at start of ADD.
Save $1\mathbf{S}$ at start of DBL.

1998 C
Store p
If point
also ca
No cos
If point
reuse Z

Best Ja
includi
$3\mathbf{M} + 5$
$11\mathbf{M} +$
$10\mathbf{M} +$
$7\mathbf{M} + 4$

L.

DD.

M tradeoff:

uting $2Y_1 \cdot Z_1$,

$Z_1)^2 - Y_1^2 - Z_1^2$.

ere already

nd Z_1^2.

e ADD formulas,

e X, Y, Z

sions by 2.

ADD for $y^2 = x^3 + ax + b$:

$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,

$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,

many more computations.

1986 Chudnovsky–Chudnovsky:

"We suggest to write

addition formulas involving

(X, Y, Z, Z^2, Z^3)."

Disadvantages:

Allocate space for Z^2, Z^3.

Pay $1\mathbf{S} + 1\mathbf{M}$ in ADD and in DBL.

Advantages:

Save $2\mathbf{S} + 2\mathbf{M}$ at start of ADD.

Save $1\mathbf{S}$ at start of DBL.

1998 Cohen–Miy

Store point as $(X$

If point is input t

also cache Z^2 an

No cost, aside fr

If point is input t

reuse Z^2, Z^3. Sa

Best Jacobian sp

including $\mathbf{S} - \mathbf{M}$

$3\mathbf{M} + 5\mathbf{S}$ for DB

$11\mathbf{M} + 5\mathbf{S}$ for AD

$10\mathbf{M} + 4\mathbf{S}$ for re

$7\mathbf{M} + 4\mathbf{S}$ for mA

f:
Z_1,
$- Z_1^2$.
y

rmulas,

ADD for $y^2 = x^3 + ax + b$:
$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,
many more computations.

1986 Chudnovsky–Chudnovsky:
"We suggest to write
addition formulas involving
(X, Y, Z, Z^2, Z^3)."

Disadvantages:
Allocate space for Z^2, Z^3.
Pay $1\mathbf{S} + 1\mathbf{M}$ in ADD and in DBL.

Advantages:
Save $2\mathbf{S} + 2\mathbf{M}$ at start of ADD.
Save $1\mathbf{S}$ at start of DBL.

1998 Cohen–Miyaji–Ono:
Store point as $(X : Y : Z)$.
If point is input to ADD,
also cache Z^2 and Z^3.
No cost, aside from space.
If point is input to another
reuse Z^2, Z^3. Save $1\mathbf{S} + 1$

Best Jacobian speeds toda
including $\mathbf{S} - \mathbf{M}$ tradeoffs:
$3\mathbf{M} + 5\mathbf{S}$ for DBL if $a =$
$11\mathbf{M} + 5\mathbf{S}$ for ADD.
$10\mathbf{M} + 4\mathbf{S}$ for reADD.
$7\mathbf{M} + 4\mathbf{S}$ for mADD (i.e. Z

ADD for $y^2 = x^3 + ax + b$:
$U_1 = X_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
$S_1 = Y_1 Z_2^3$, $S_2 = Y_2 Z_1^3$,
many more computations.

1986 Chudnovsky–Chudnovsky:
"We suggest to write
addition formulas involving
(X, Y, Z, Z^2, Z^3)."

Disadvantages:
Allocate space for Z^2, Z^3.
Pay $1\mathbf{S} + 1\mathbf{M}$ in ADD and in DBL.

Advantages:
Save $2\mathbf{S} + 2\mathbf{M}$ at start of ADD.
Save $1\mathbf{S}$ at start of DBL.

1998 Cohen–Miyaji–Ono:
Store point as $(X : Y : Z)$.
If point is input to ADD,
also cache Z^2 and Z^3.
No cost, aside from space.
If point is input to another ADD,
reuse Z^2, Z^3. Save $1\mathbf{S} + 1\mathbf{M}$!

Best Jacobian speeds today,
including $\mathbf{S} - \mathbf{M}$ tradeoffs:
$3\mathbf{M} + 5\mathbf{S}$ for DBL if $a = -3$.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.
$10\mathbf{M} + 4\mathbf{S}$ for reADD.
$7\mathbf{M} + 4\mathbf{S}$ for mADD (i.e. $Z_2 = 1$).

or $y^2 = x^3 + ax + b$:
$X_1Z_2^2$, $U_2 = X_2Z_1^2$,
$Y_1Z_2^3$, $S_2 = Y_2Z_1^3$,
more computations.

Chudnovsky–Chudnovsky:
uggest to write
n formulas involving
Z, Z^2, Z^3)."

antages:
te space for Z^2, Z^3.
$5+1\mathbf{M}$ in ADD and in DBL.

tages:
$\mathbf{S}+2\mathbf{M}$ at start of ADD.
$\mathbf{S}$ at start of DBL.

1998 Cohen–Miyaji–Ono:
Store point as $(X : Y : Z)$.
If point is input to ADD,
also cache Z^2 and Z^3.
No cost, aside from space.
If point is input to another ADD,
reuse Z^2, Z^3. Save $1\mathbf{S}+1\mathbf{M}$!

Best Jacobian speeds today,
including $\mathbf{S}-\mathbf{M}$ tradeoffs:
$3\mathbf{M}+5\mathbf{S}$ for DBL if $a=-3$.
$11\mathbf{M}+5\mathbf{S}$ for ADD.
$10\mathbf{M}+4\mathbf{S}$ for reADD.
$7\mathbf{M}+4\mathbf{S}$ for mADD (i.e. $Z_2=1$).

Compa
curves
in proj
(2007
$3\mathbf{M}+$
$10\mathbf{M}+$
$9\mathbf{M}+$

Inverte
(2007
$3\mathbf{M}+$
$9\mathbf{M}+$
$8\mathbf{M}+$

Latest
2008.1

$^3 + ax + b$:
$= X_2Z_1^2$,
$= Y_2Z_1^3$,
putations.

y–Chudnovsky:
write
s involving
."

or Z^2, Z^3.
ADD and in DBL.

t start of ADD.
of DBL.

1998 Cohen–Miyaji–Ono:
Store point as $(X : Y : Z)$.
If point is input to ADD,
also cache Z^2 and Z^3.
No cost, aside from space.
If point is input to another ADD,
reuse Z^2, Z^3. Save $1\mathbf{S} + 1\mathbf{M}$!

Best Jacobian speeds today,
including $\mathbf{S} - \mathbf{M}$ tradeoffs:
$3\mathbf{M} + 5\mathbf{S}$ for DBL if $a = -3$.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.
$10\mathbf{M} + 4\mathbf{S}$ for reADD.
$7\mathbf{M} + 4\mathbf{S}$ for mADD (i.e. $Z_2 = 1$).

Compare to spee
curves $x^2 + y^2 =$
in projective coo
(2007 Bernstein–
$3\mathbf{M} + 4\mathbf{S}$ for DB
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ f

Inverted Edwards
(2007 Bernstein–
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ f
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ f
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ f

Latest Edwards s
2008.12 Hisil–Wo

:

vsky:

in DBL.

ADD.

1998 Cohen–Miyaji–Ono:
Store point as $(X : Y : Z)$.
If point is input to ADD,
also cache Z^2 and Z^3.
No cost, aside from space.
If point is input to another ADD,
reuse Z^2, Z^3. Save $1\mathbf{S} + 1\mathbf{M}$!

Best Jacobian speeds today,
including $\mathbf{S} - \mathbf{M}$ tradeoffs:
$3\mathbf{M} + 5\mathbf{S}$ for DBL if $a = -3$.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.
$10\mathbf{M} + 4\mathbf{S}$ for reADD.
$7\mathbf{M} + 4\mathbf{S}$ for mADD (i.e. $Z_2 = 1$).

Compare to speeds for Edw
curves $x^2 + y^2 = 1 + dx^2y$
in projective coordinates
(2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S}$ for DBL.
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Inverted Edwards coordinat
(2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Latest Edwards speed news
2008.12 Hisil–Wong–Carter

1998 Cohen–Miyaji–Ono:
Store point as $(X : Y : Z)$.
If point is input to ADD,
also cache Z^2 and Z^3.
No cost, aside from space.
If point is input to another ADD,
reuse Z^2, Z^3. Save $1\mathbf{S} + 1\mathbf{M}$!

Best Jacobian speeds today,
including $\mathbf{S} - \mathbf{M}$ tradeoffs:
$3\mathbf{M} + 5\mathbf{S}$ for DBL if $a = -3$.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.
$10\mathbf{M} + 4\mathbf{S}$ for reADD.
$7\mathbf{M} + 4\mathbf{S}$ for mADD (i.e. $Z_2 = 1$).

Compare to speeds for Edwards
curves $x^2 + y^2 = 1 + dx^2y^2$
in projective coordinates
(2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S}$ for DBL.
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Inverted Edwards coordinates
(2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Latest Edwards speed news:
2008.12 Hisil–Wong–Carter–Dawson.

Cohen–Miyaji–Ono:
point as $(X : Y : Z)$.
t is input to ADD,
che Z^2 and Z^3.
t, aside from space.
t is input to another ADD,
Z^2, Z^3. Save $1\mathbf{S} + 1\mathbf{M}$!

acobian speeds today,
ng $\mathbf{S} - \mathbf{M}$ tradeoffs:
$5\mathbf{S}$ for DBL if $a = -3$.
$5\mathbf{S}$ for ADD.
$4\mathbf{S}$ for reADD.
$4\mathbf{S}$ for mADD (i.e. $Z_2 = 1$).

Compare to speeds for Edwards curves $x^2 + y^2 = 1 + dx^2y^2$
in projective coordinates
(2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S}$ for DBL.
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Inverted Edwards coordinates
(2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Latest Edwards speed news:
2008.12 Hisil–Wong–Carter–Dawson.

$y^2 = x$

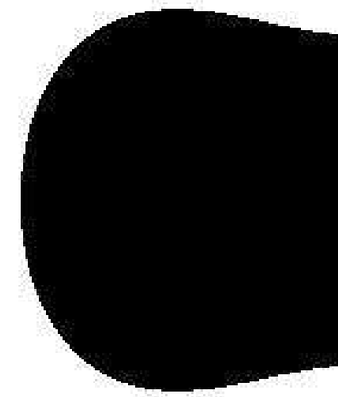
aji–Ono:
$K : Y : Z$).
to ADD,
nd Z^3.
om space.
to another ADD,
ave $1\mathbf{S} + 1\mathbf{M}$!

peeds today,
tradeoffs:
L if $a = -3$.
DD.
ADD.
DD (i.e. $Z_2 = 1$).

Compare to speeds for Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ in projective coordinates (2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S}$ for DBL.
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Inverted Edwards coordinates (2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Latest Edwards speed news:
2008.12 Hisil–Wong–Carter–Dawson.



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

ADD,
M!

y,

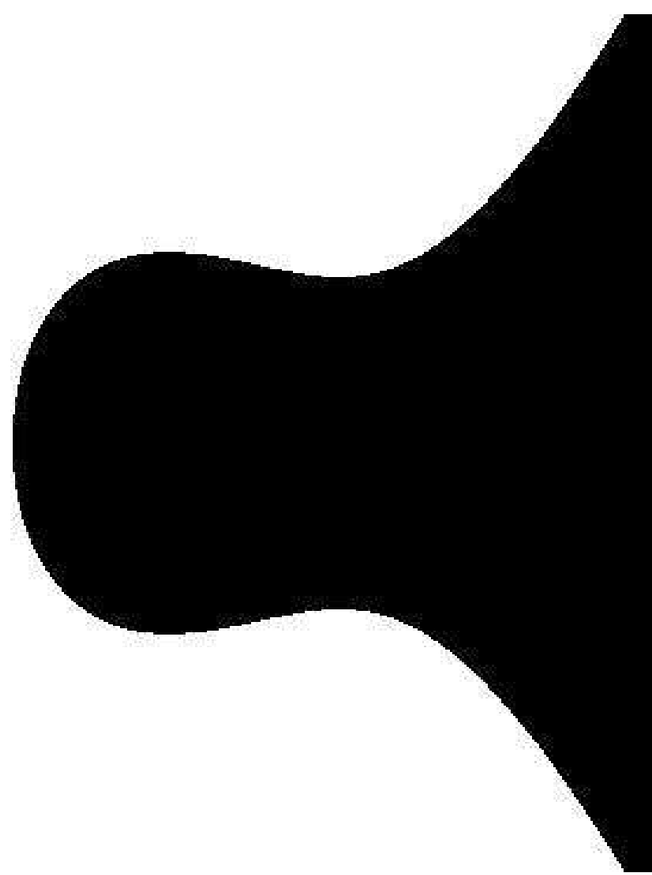
+3.

$Z_2 = 1$).

Compare to speeds for Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ in projective coordinates (2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S}$ for DBL.
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Inverted Edwards coordinates (2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Latest Edwards speed news:
2008.12 Hisil–Wong–Carter–Dawson.

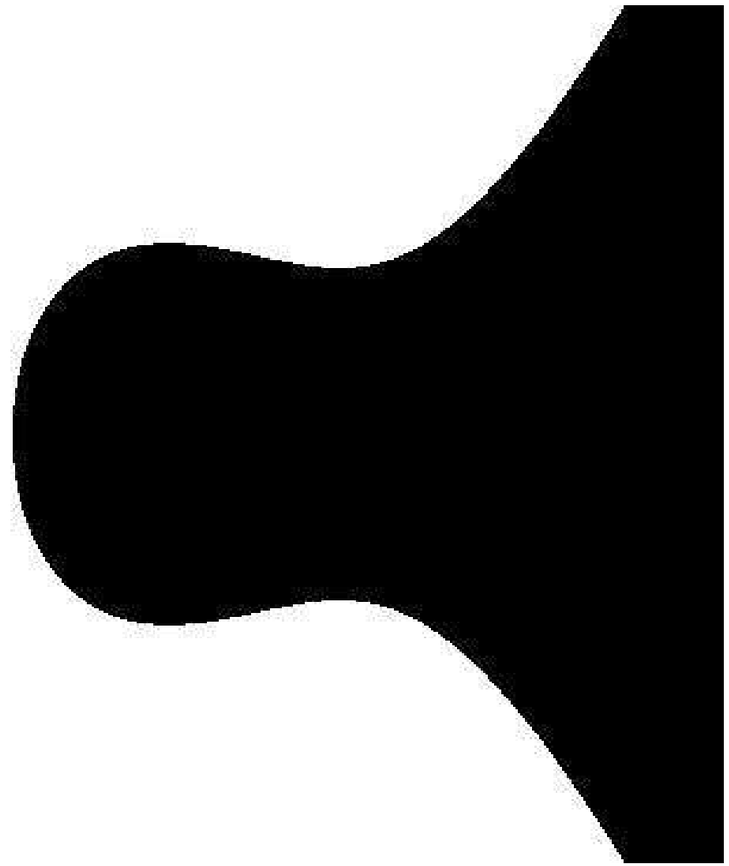


$y^2 = x^3 - 0.4x + 0.7$

Compare to speeds for Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ in projective coordinates (2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S}$ for DBL.
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Inverted Edwards coordinates (2007 Bernstein–Lange):
$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Latest Edwards speed news:
2008.12 Hisil–Wong–Carter–Dawson.

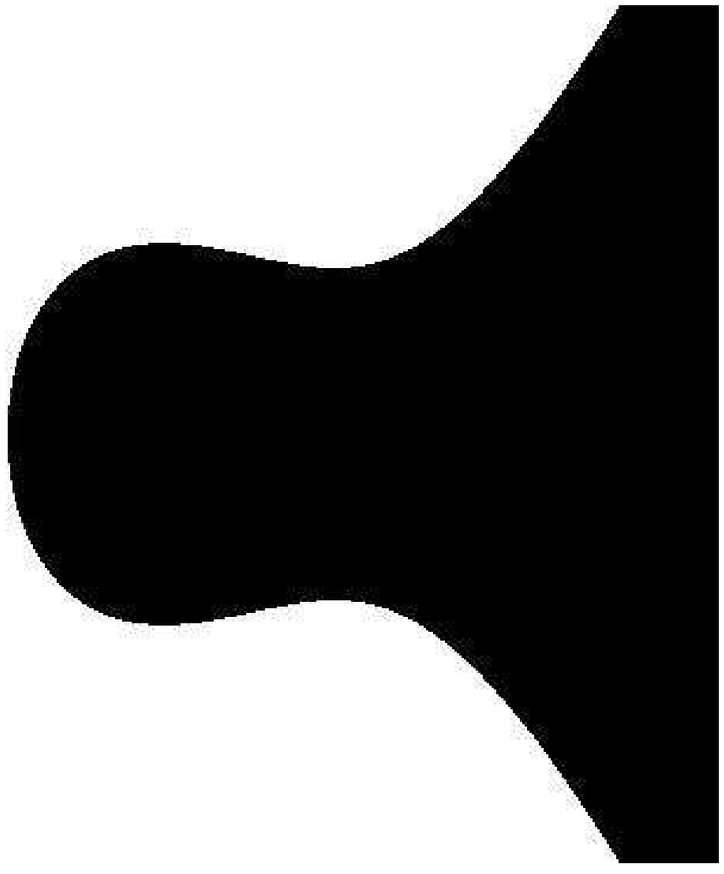


$y^2 = x^3 - 0.4x + 0.7$

re to speeds for Edwards
$x^2 + y^2 = 1 + dx^2y^2$
ective coordinates
Bernstein–Lange):
4**S** for DBL.
$+ 1\mathbf{S} + 1\mathbf{D}$ for ADD.
$1\mathbf{S} + 1\mathbf{D}$ for mADD.

d Edwards coordinates
Bernstein–Lange):
$4\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{S} + 1\mathbf{D}$ for ADD.
$1\mathbf{S} + 1\mathbf{D}$ for mADD.

Edwards speed news:
2 Hisil–Wong–Carter–Dawson.



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

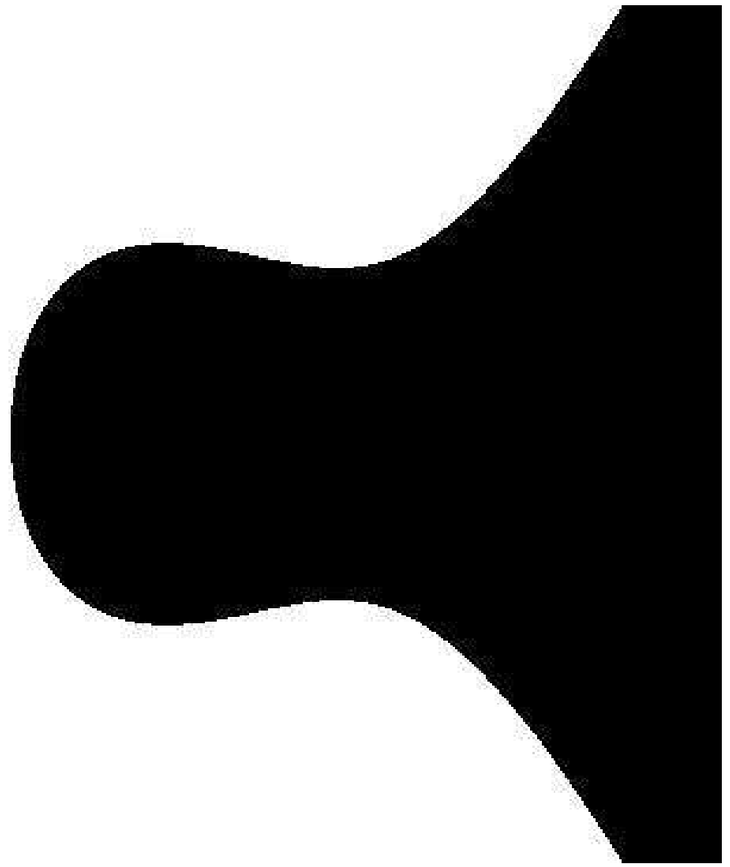
The W
turtle:
and slo
(picture

(Thank
for the

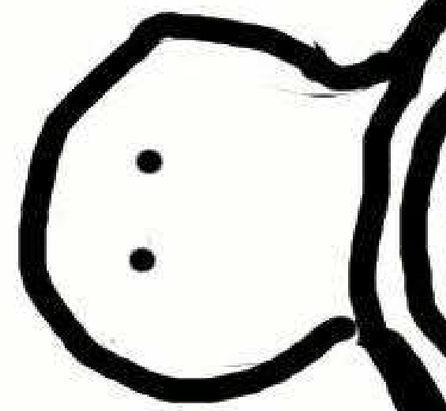
ds for Edwards
$= 1 + dx^2y^2$
rdinates
-Lange):
L.
for ADD.
or mADD.

s coordinates
-Lange):
or DBL.
or ADD.
or mADD.

speed news:
ong–Carter–Dawson.



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



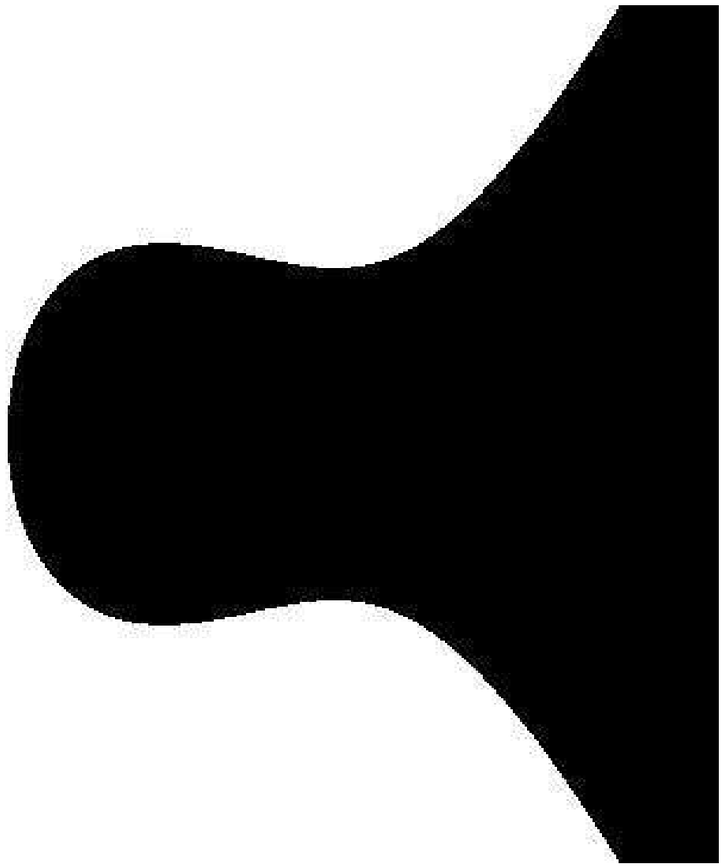
The Weierstrass-
turtle: old, truste
and slow. Warnin
(picture) incomple

(Thanks to Tanja
for the pictures.)

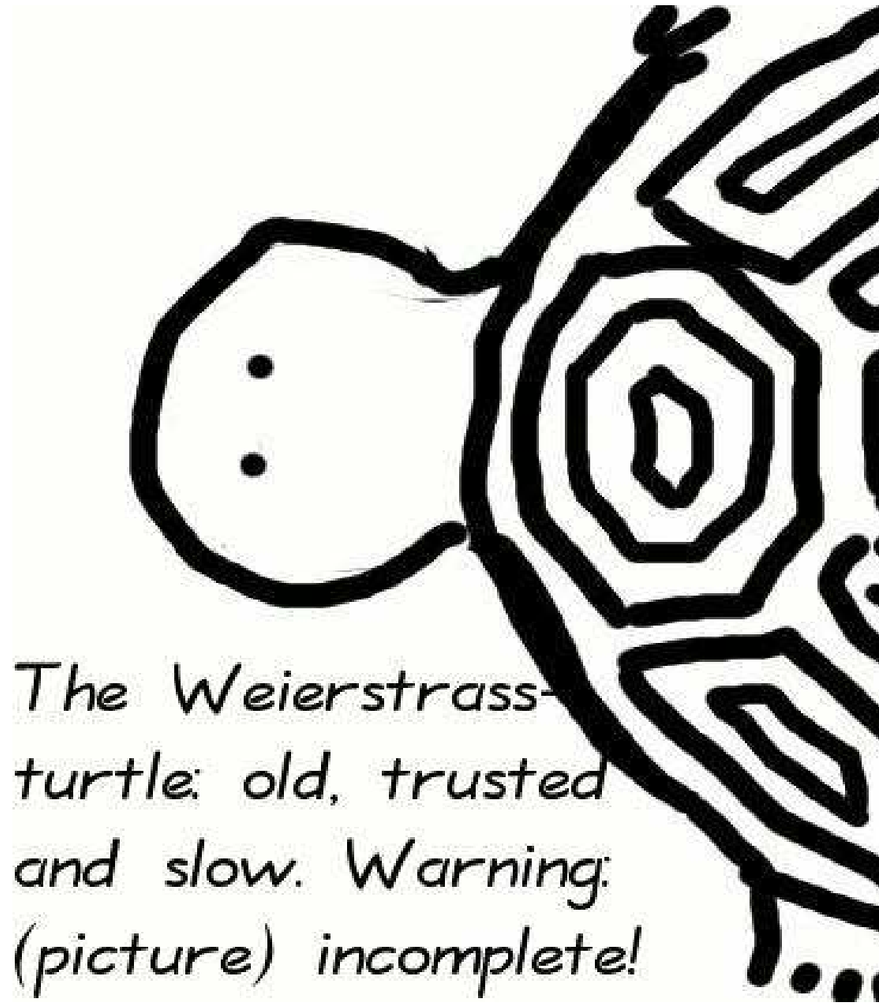
vards
y^2

tes

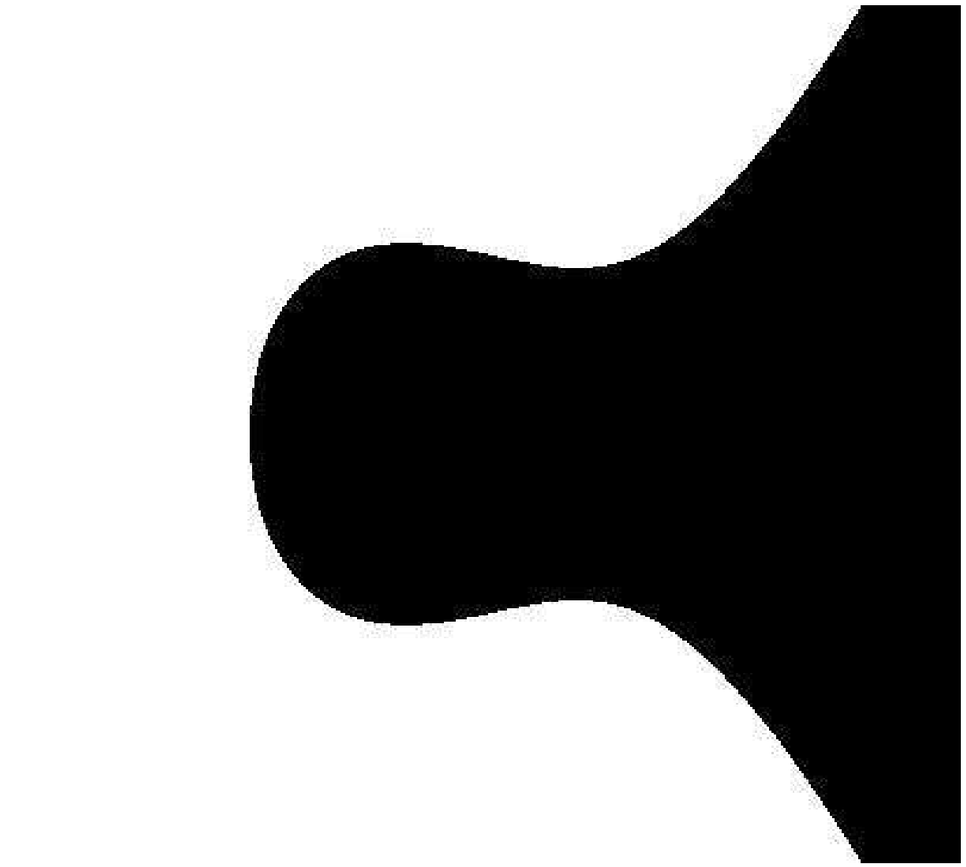
s:
r–Dawson.



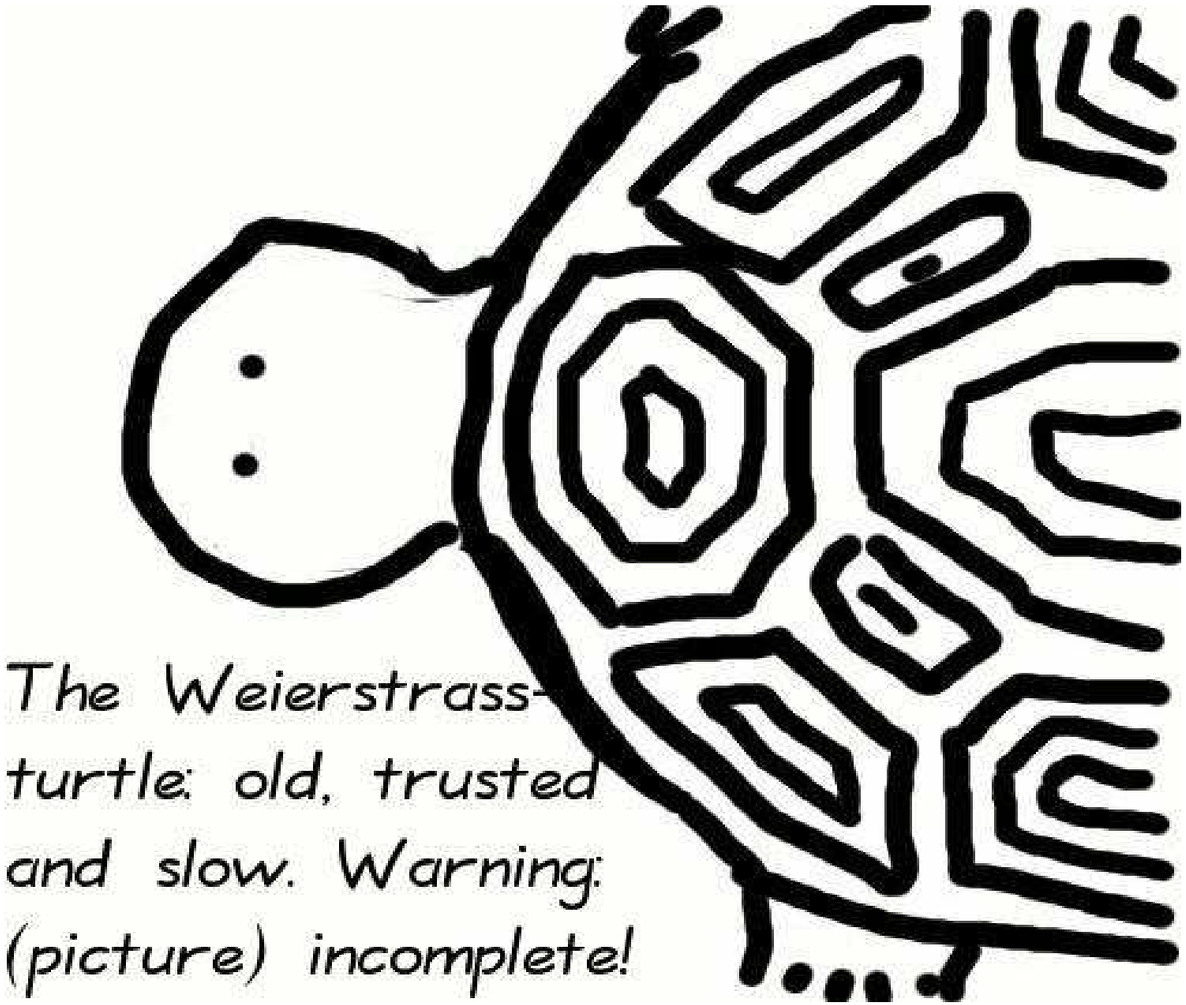
$y^2 = x^3 - 0.4x + 0.7$



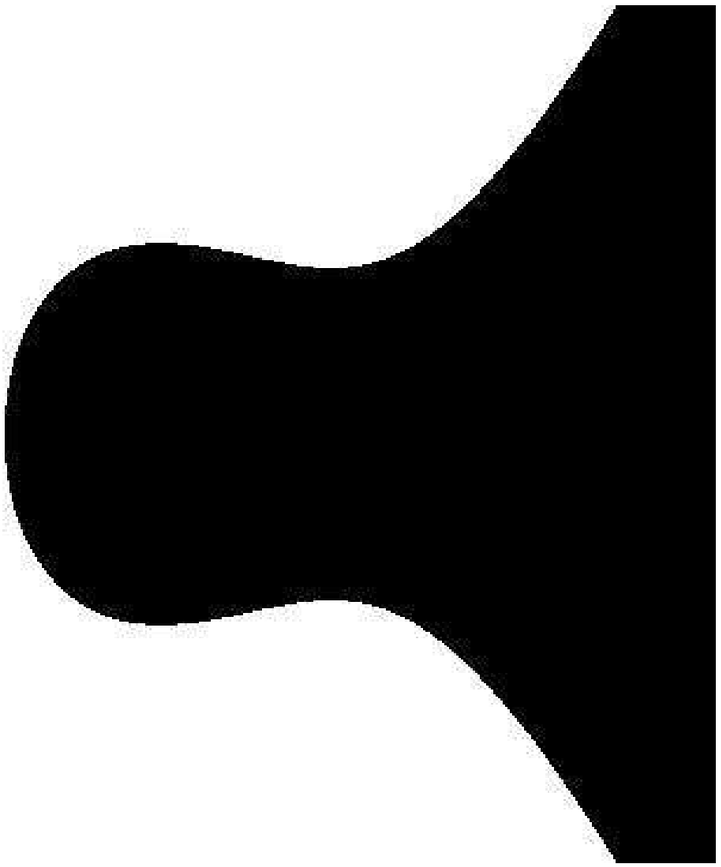
(Thanks to Tanja Lange for the pictures.)



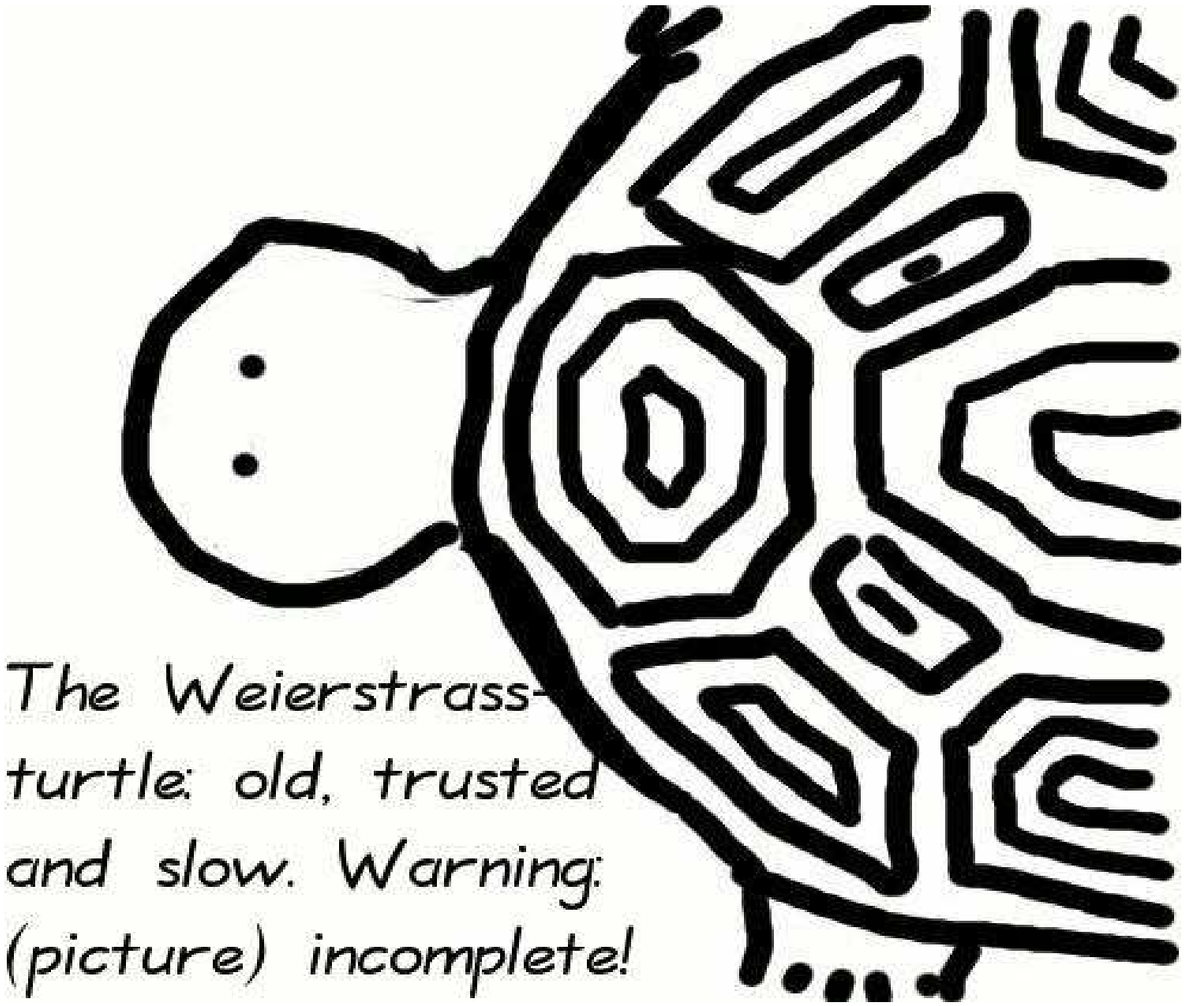
$y^2 = x^3 - 0.4x + 0.7$



(Thanks to Tanja Lange
for the pictures.)

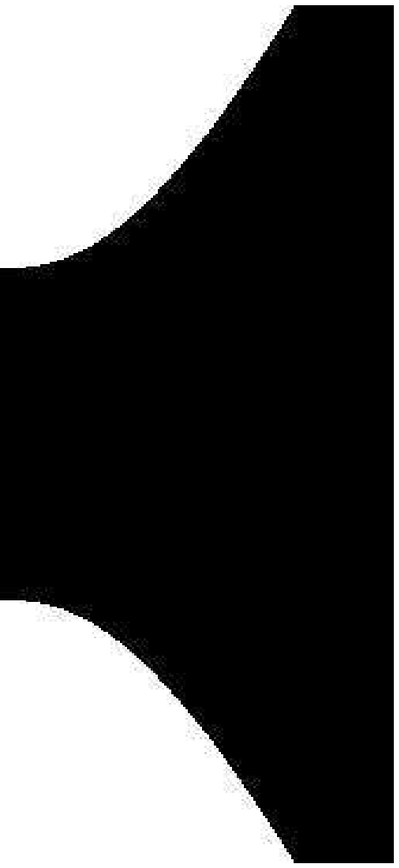


$^3 - 0.4x + 0.7$

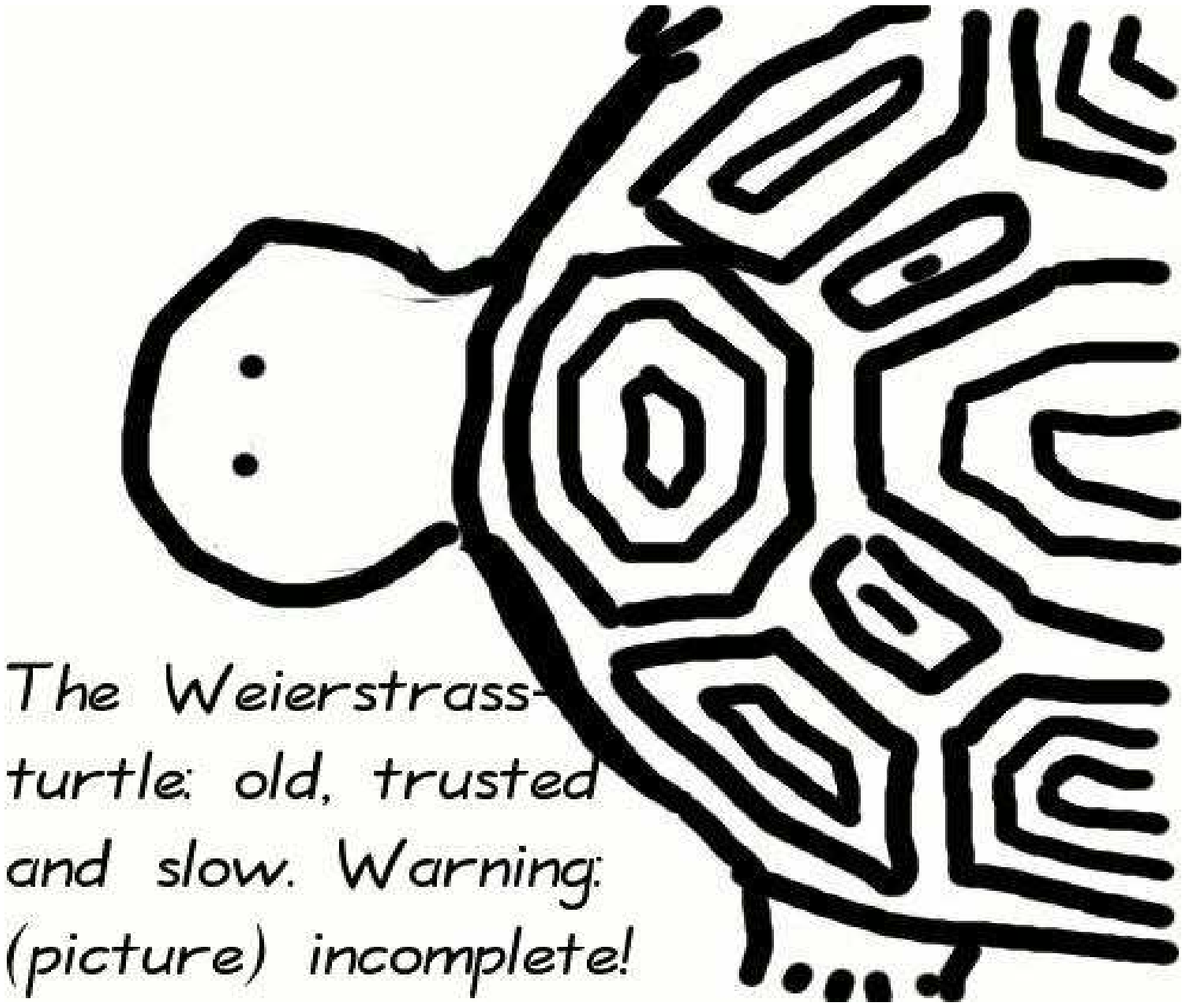


(Thanks to Tanja Lange
for the pictures.)

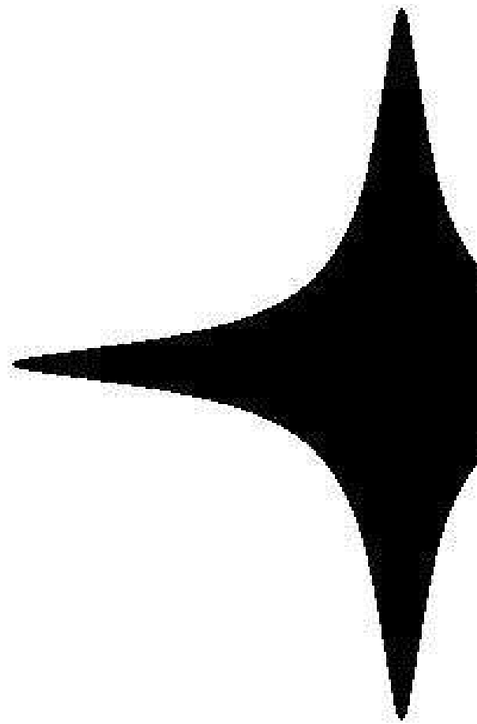
$x^2 + y$



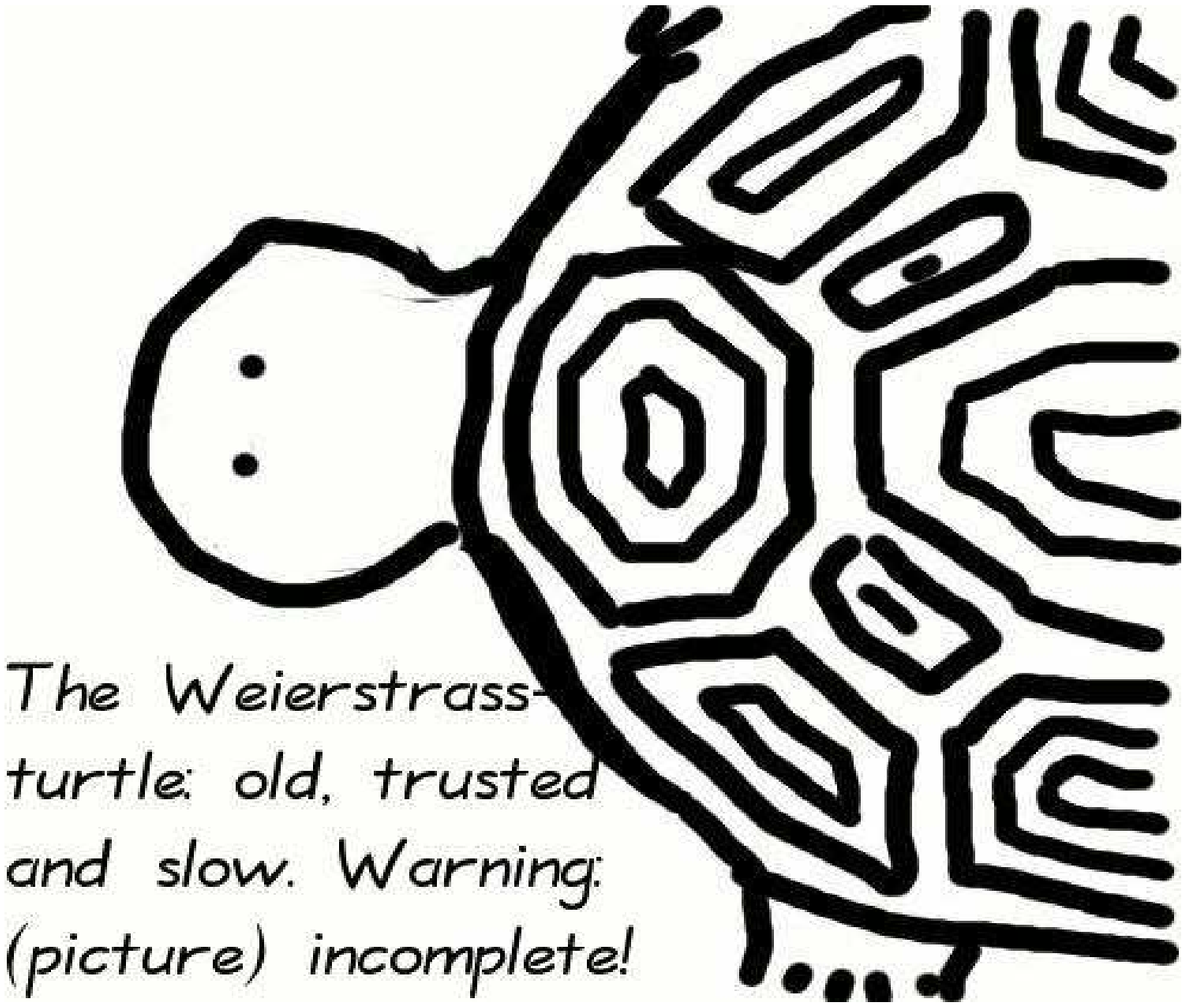
$+ 0.7$



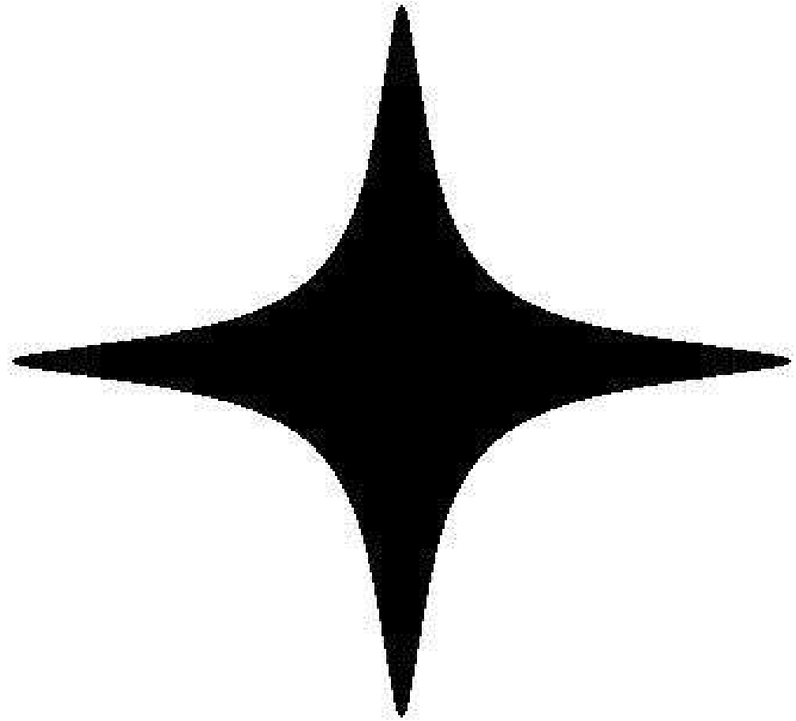
(Thanks to Tanja Lange
for the pictures.)



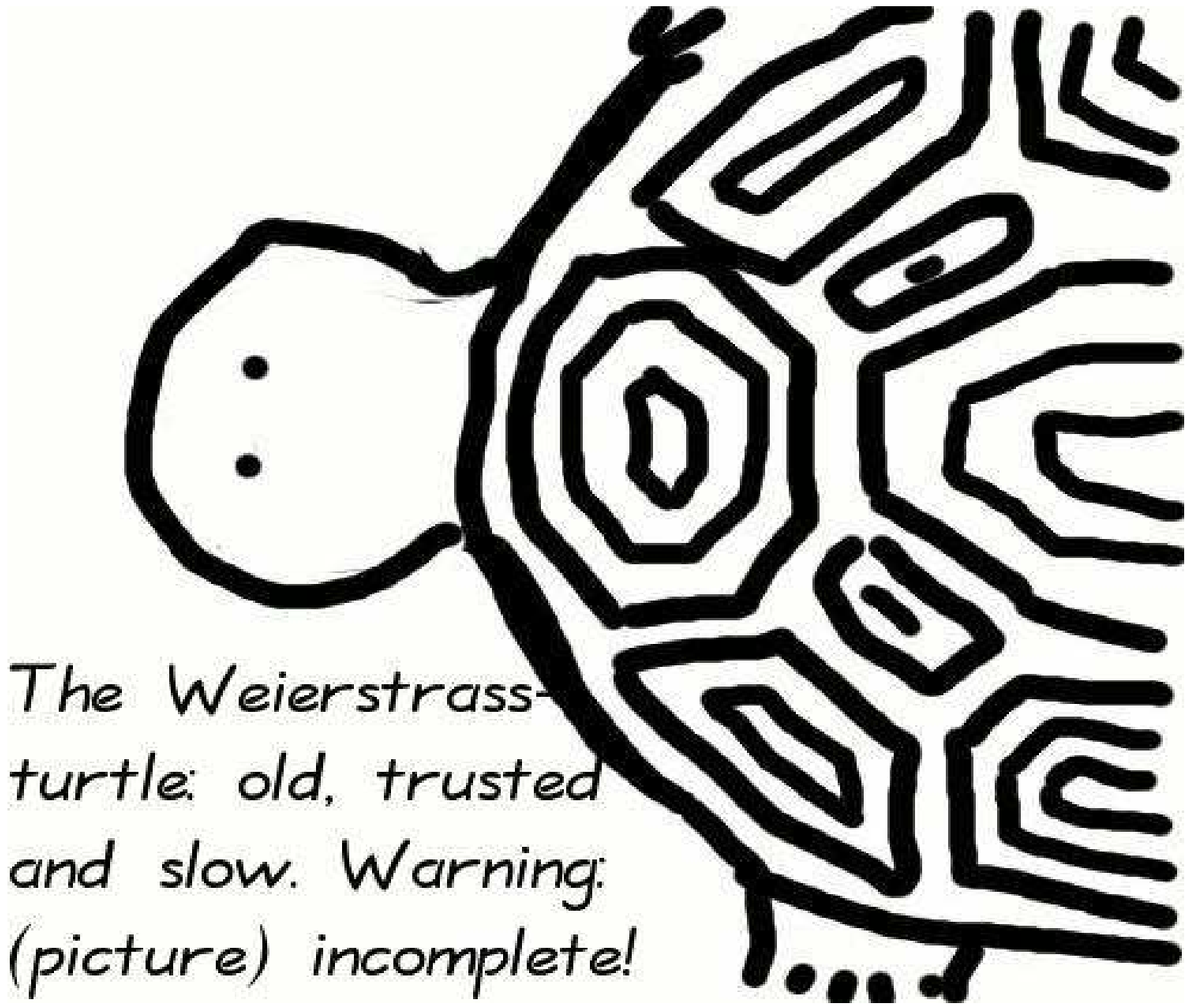
$x^2 + y^2 = 1 - 30$



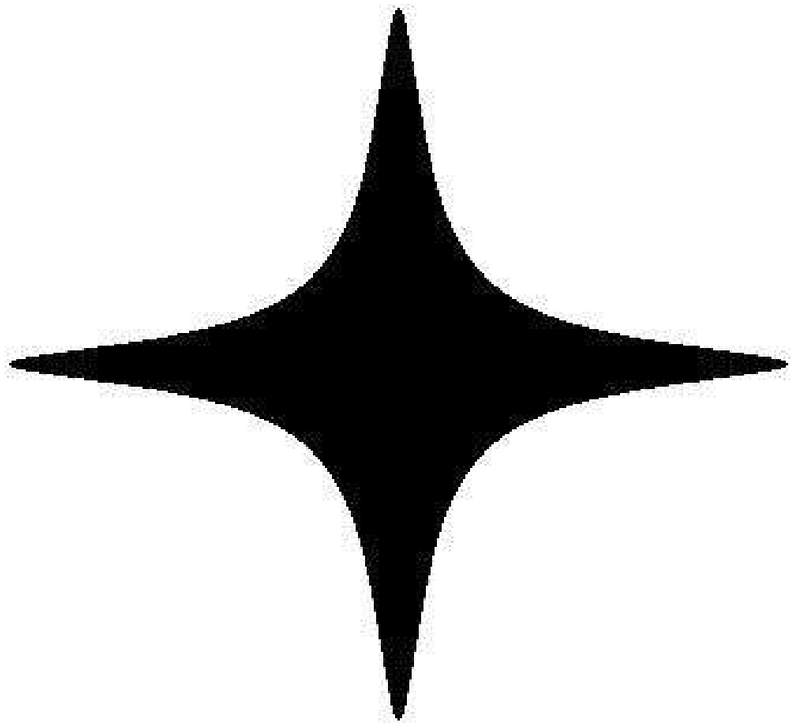
(Thanks to Tanja Lange
for the pictures.)



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

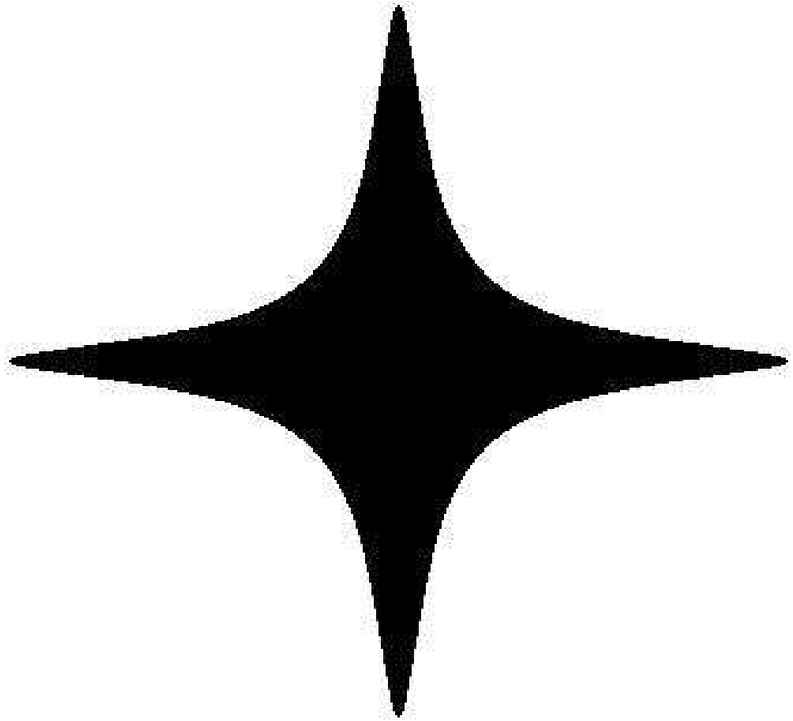


(Thanks to Tanja Lange
for the pictures.)

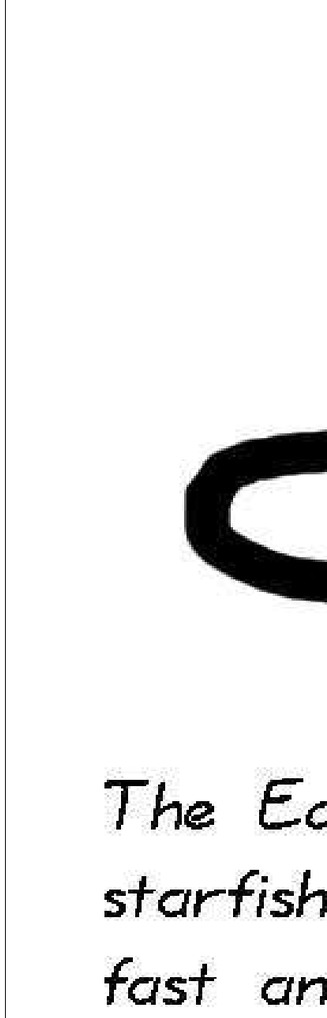


$$x^2 + y^2 = 1 - 300x^2y^2$$

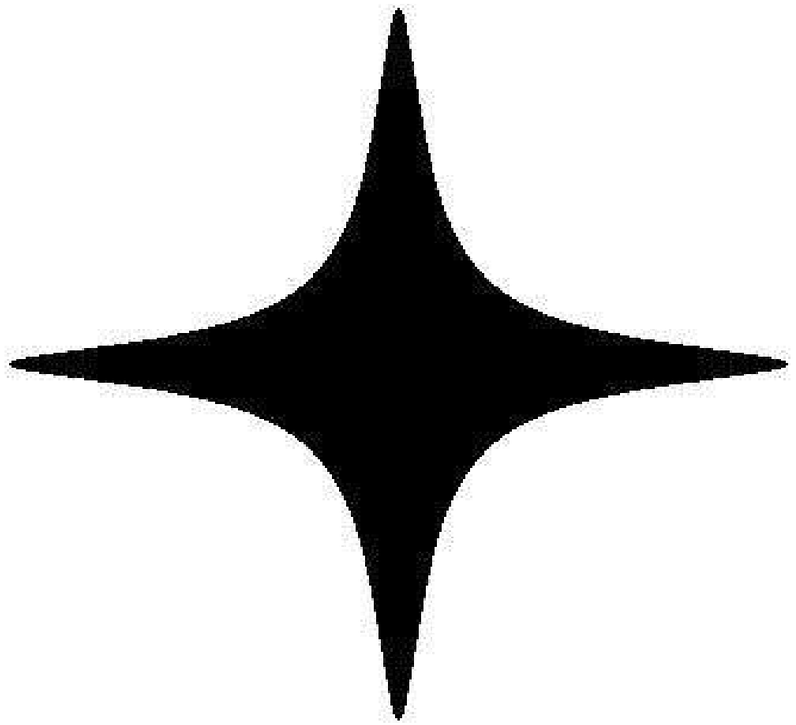
ks to Tanja Lange
pictures.)



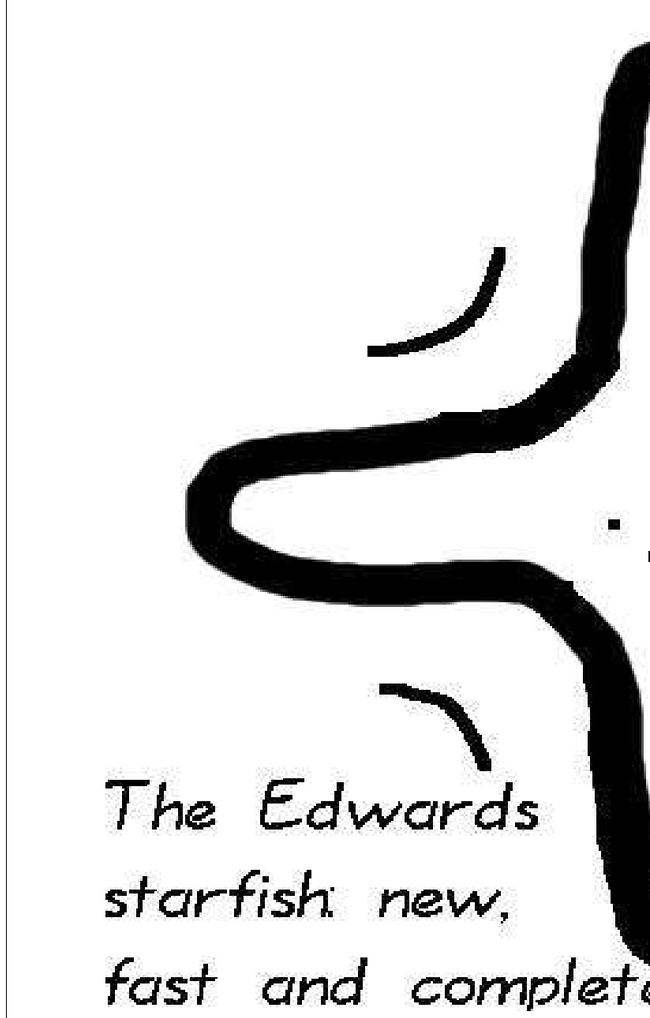
$$x^2 + y^2 = 1 - 300x^2y^2$$

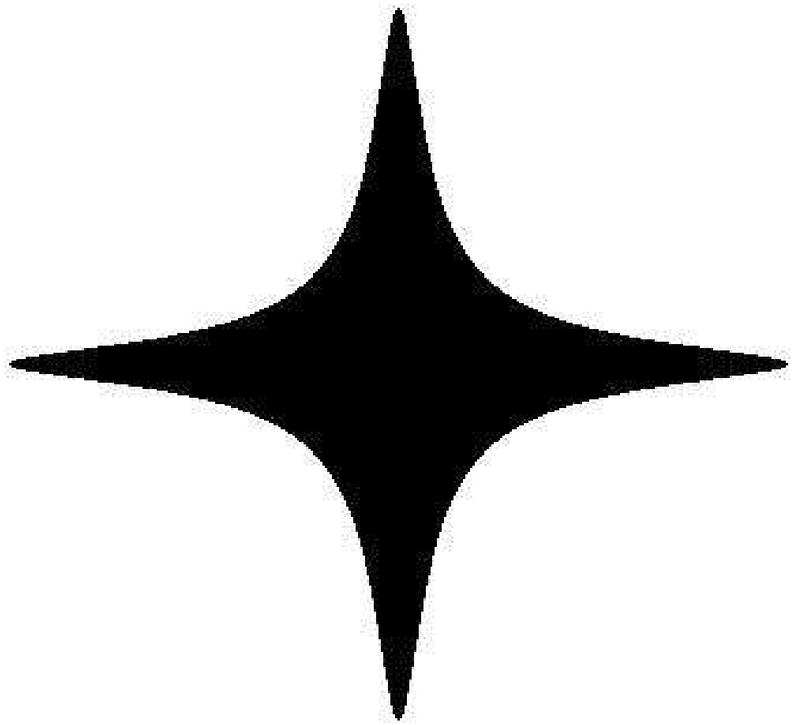


a Lange

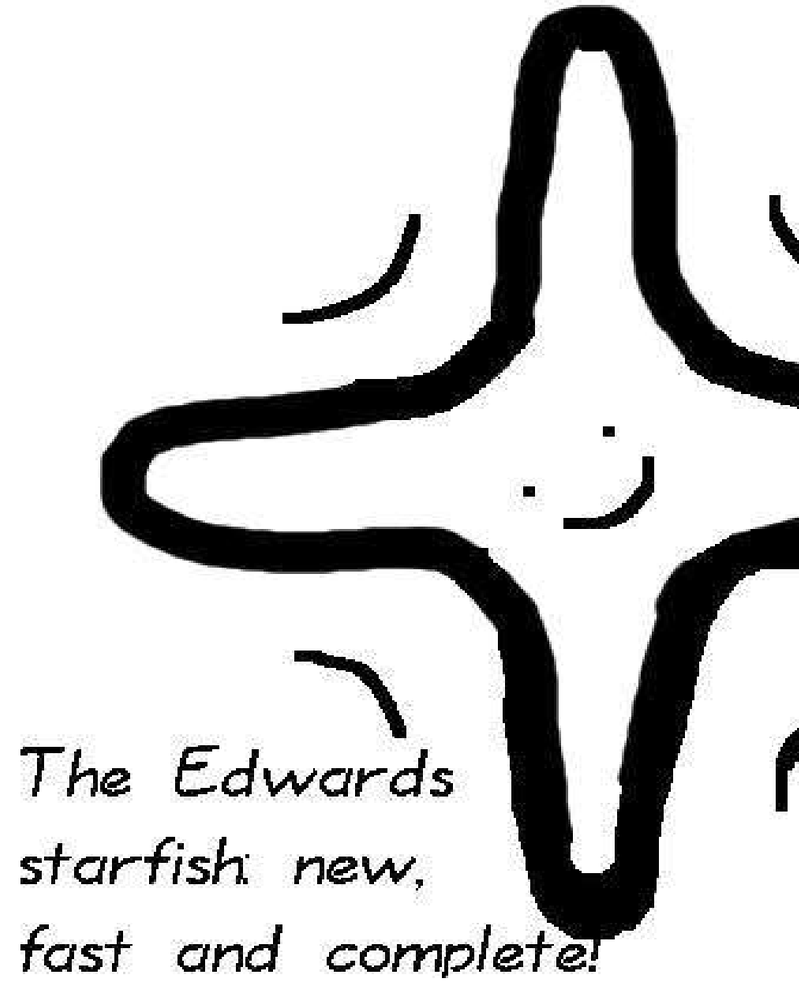


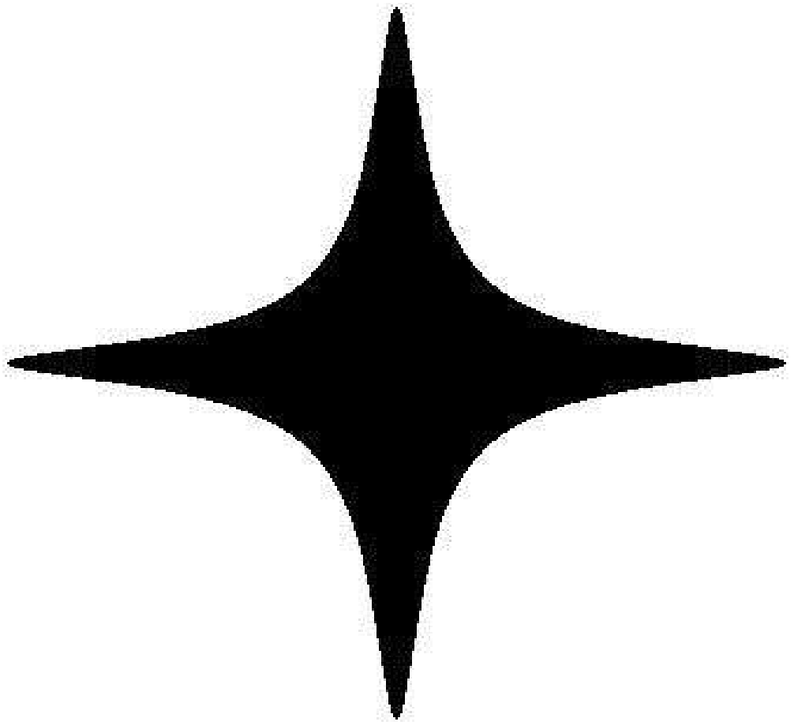
$$x^2 + y^2 = 1 - 300x^2y^2$$



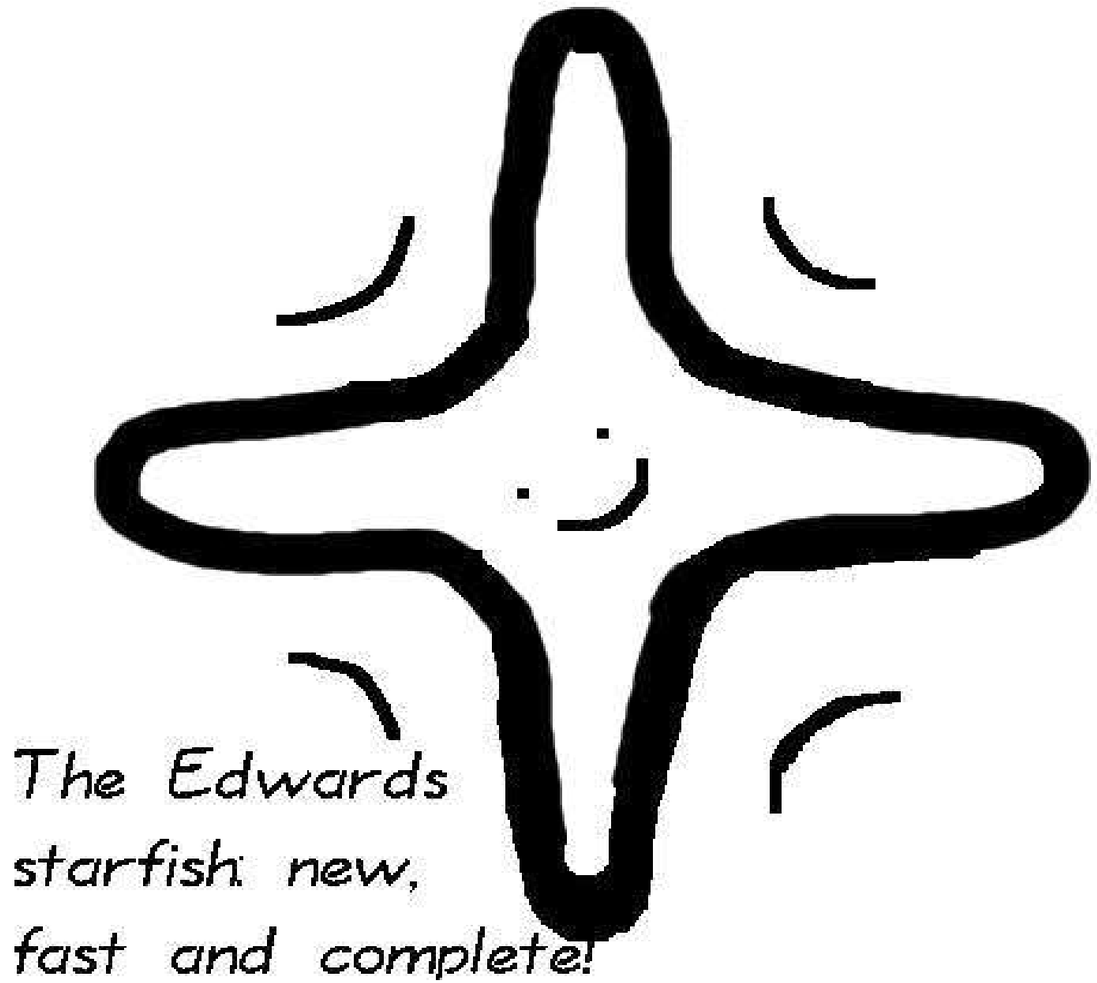


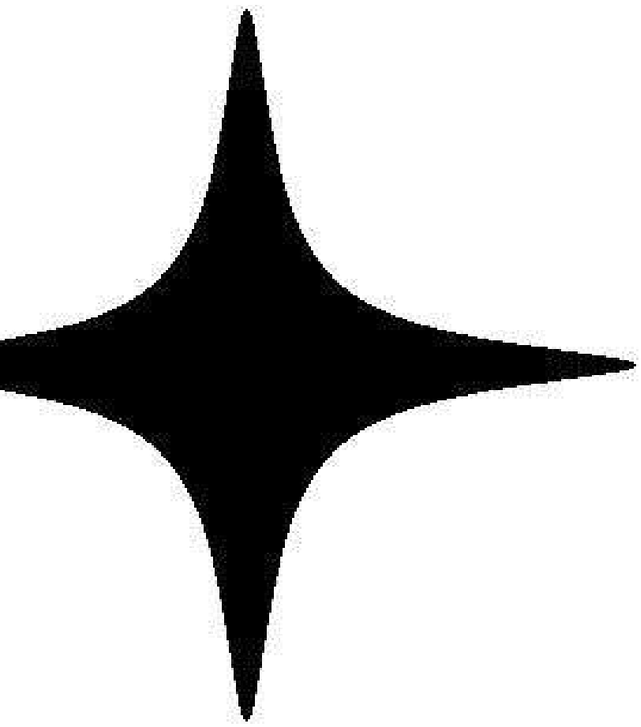
$$x^2 + y^2 = 1 - 300x^2y^2$$



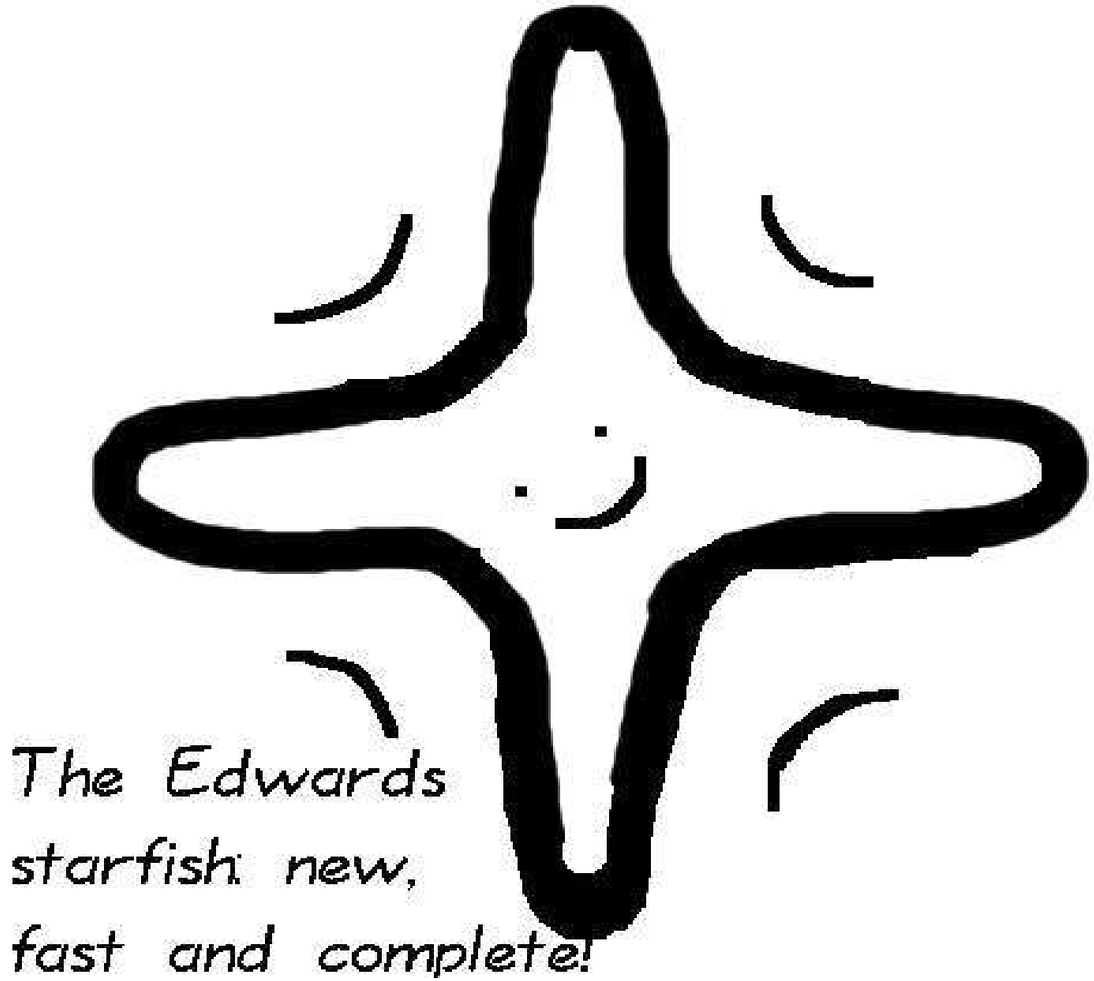


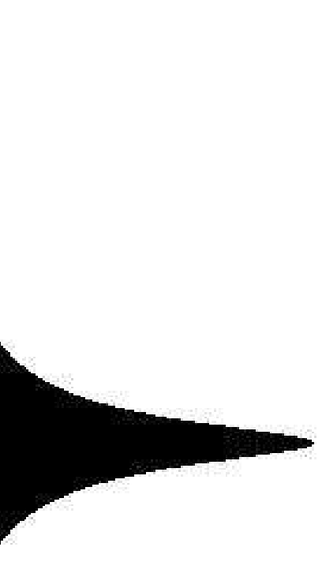
$$x^2 + y^2 = 1 - 300x^2y^2$$



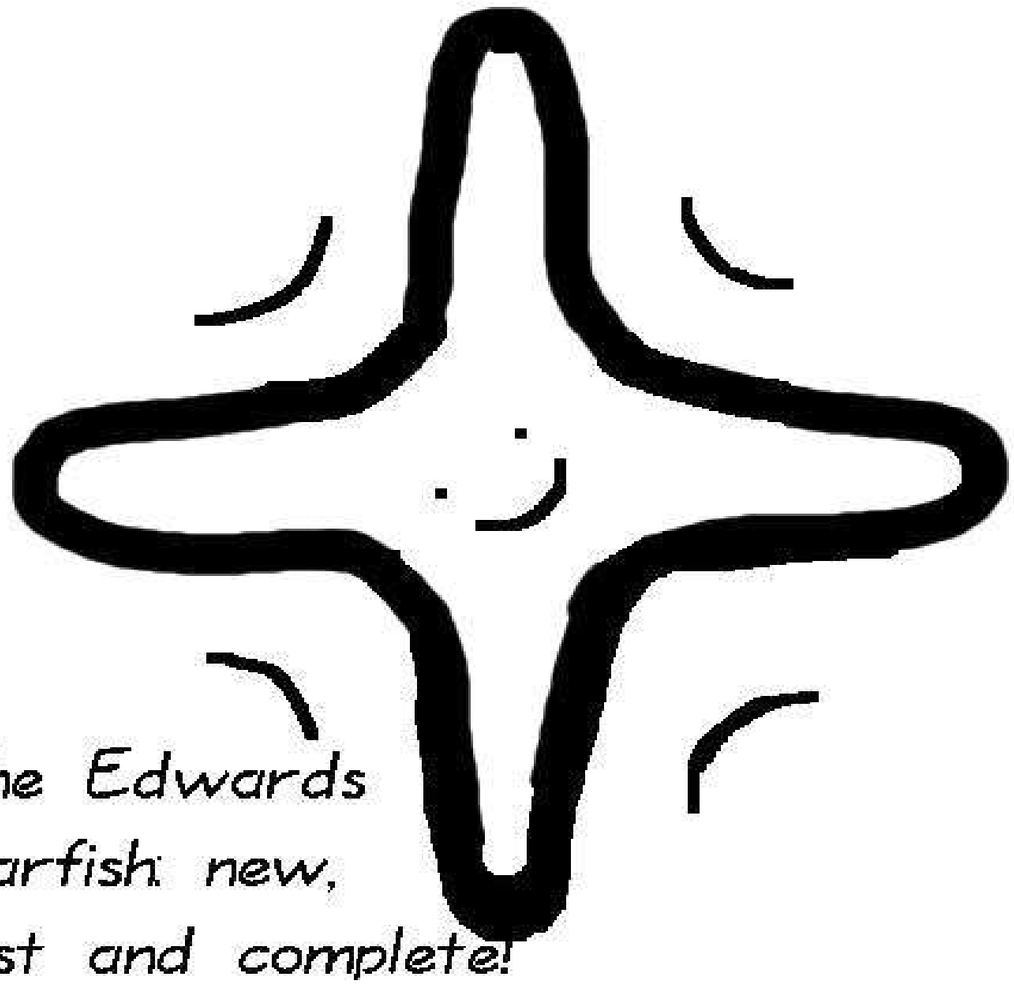


$$x^2 = 1 - 300x^2y^2$$

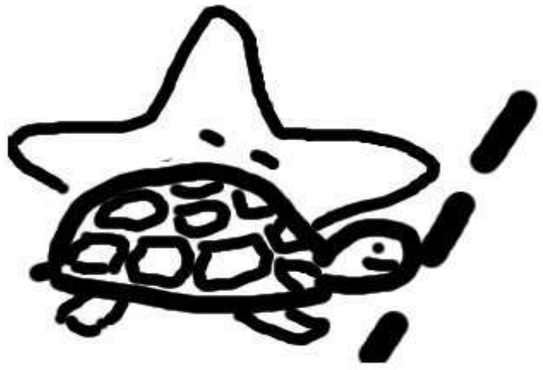




$00x^2y^2$

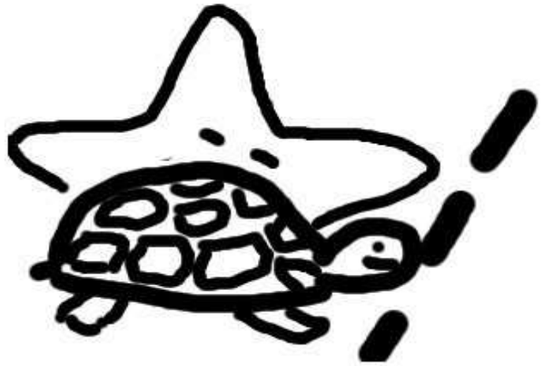


The Edwards starfish: new, fast and complete!

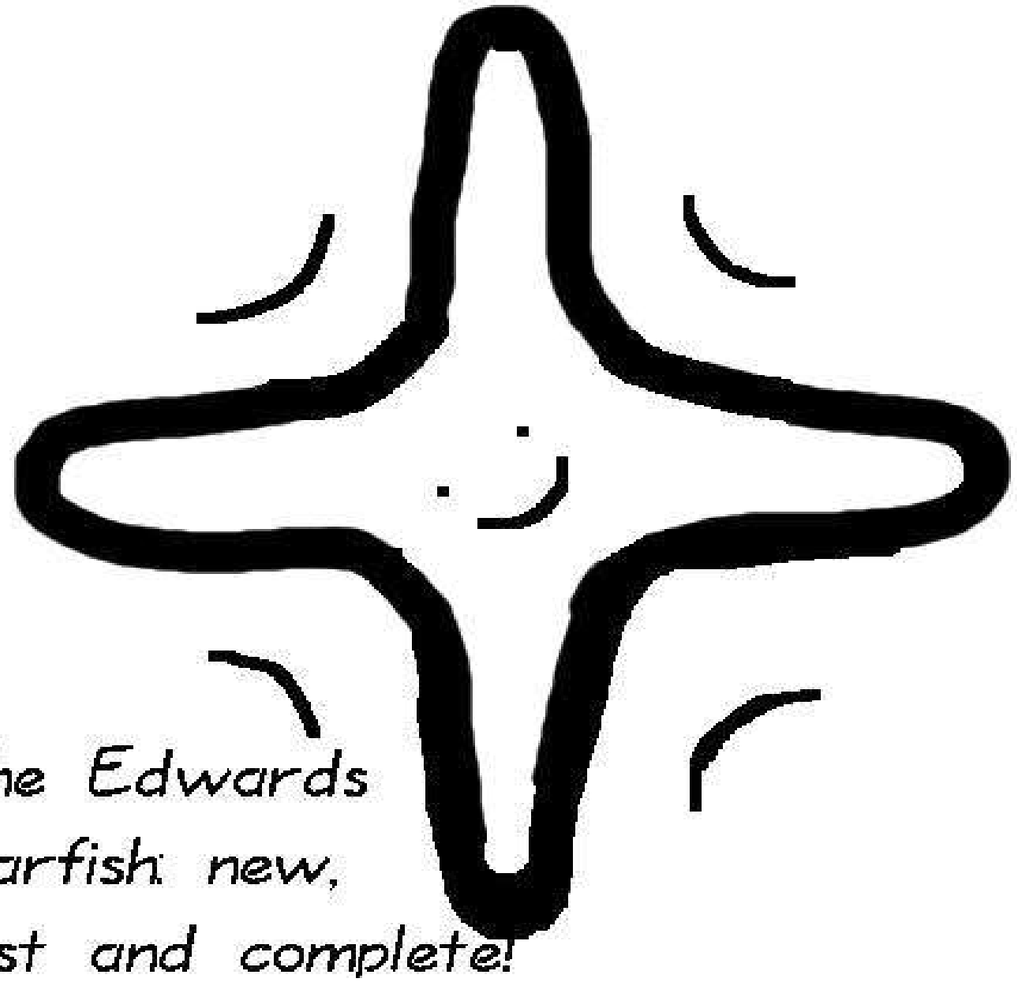


Start!

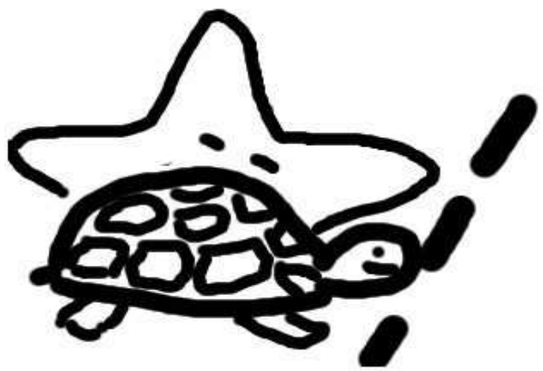
The Edwards starfish: new, fast and complete!



Start!



The Edwards starfish: new, fast and complete!

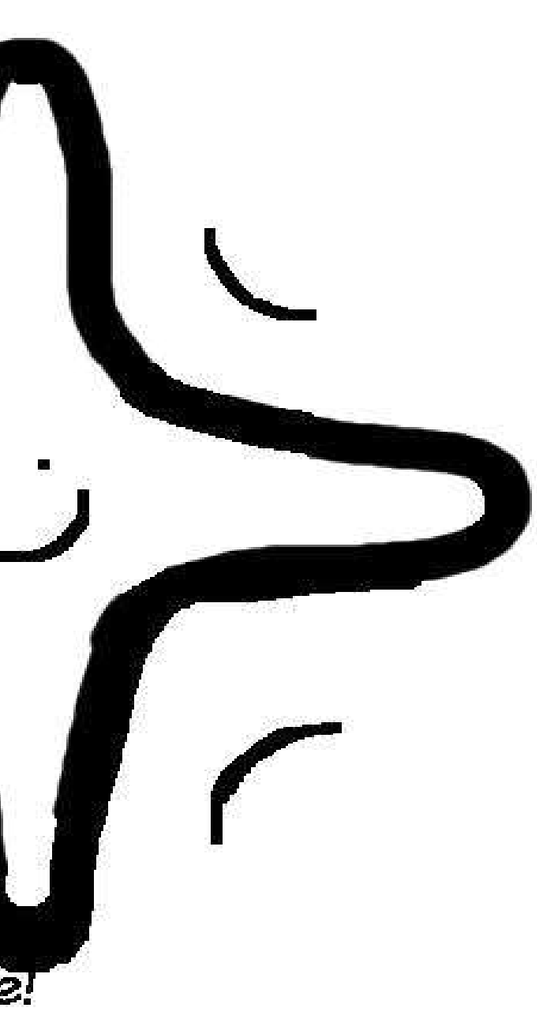


Start!

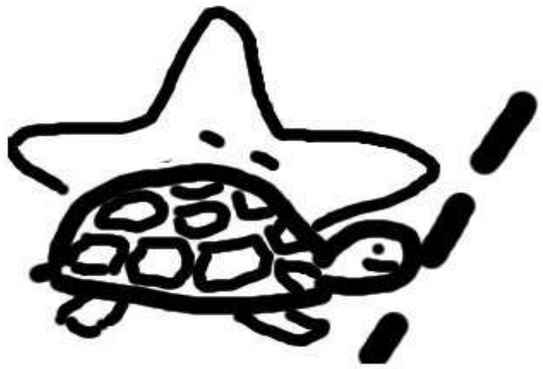
dwards
new,
d complete!

Start!

Weierstr
left behin

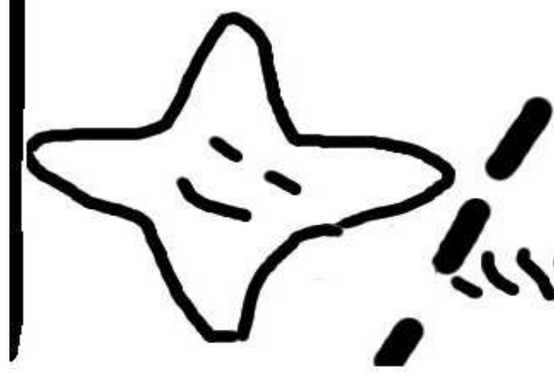


e!

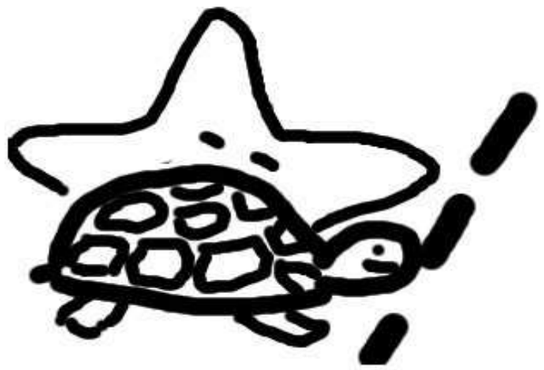


Start!

1985



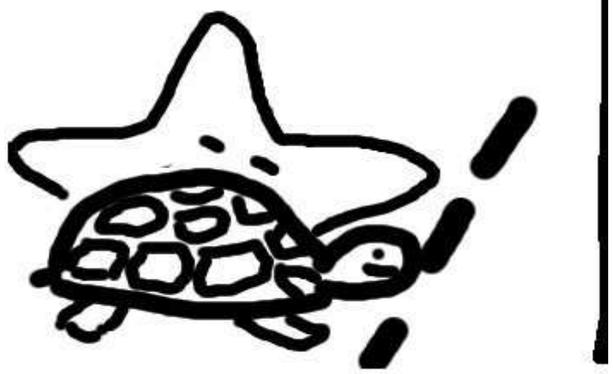
Weierstrass sets off. E
left behind sleeping



Start!

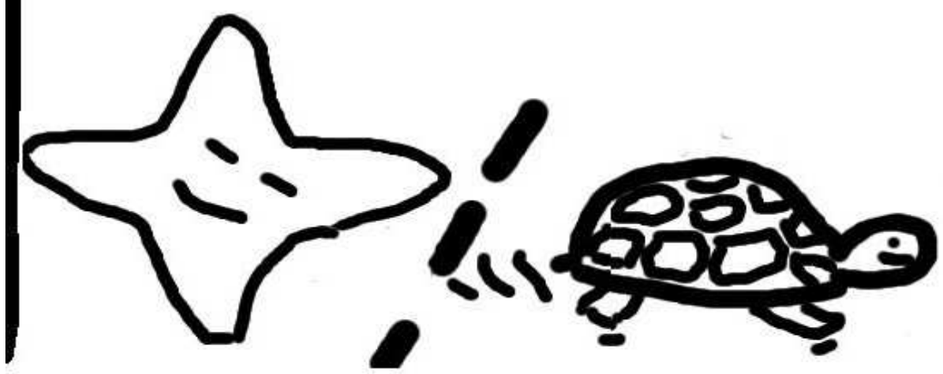
1985

Weierstrass sets off. Edwards left behind sleeping

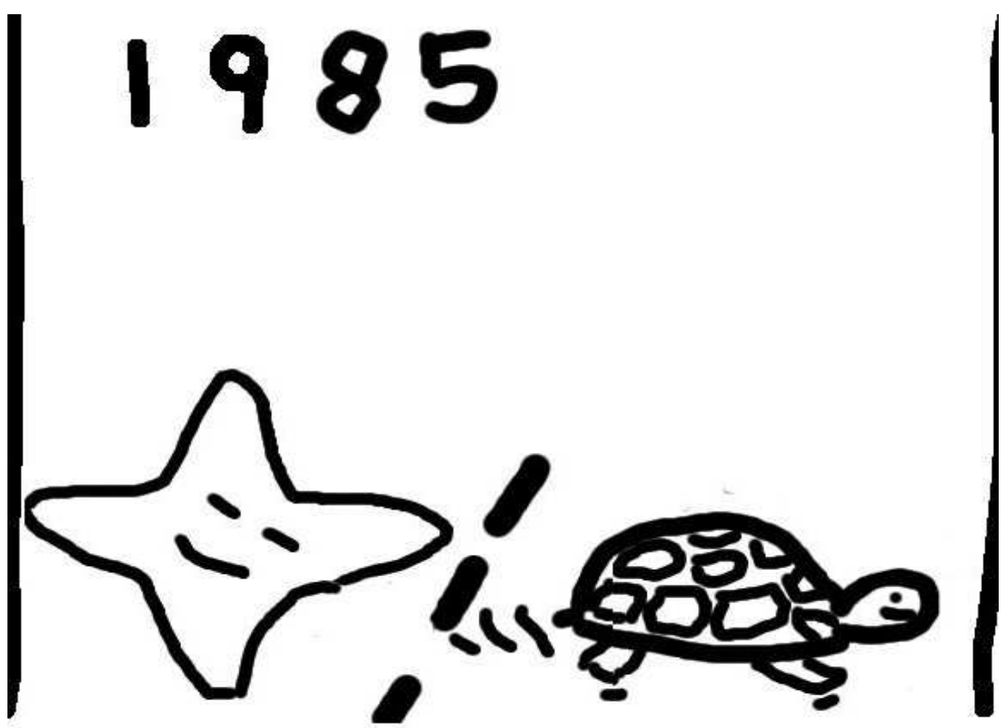


Start!

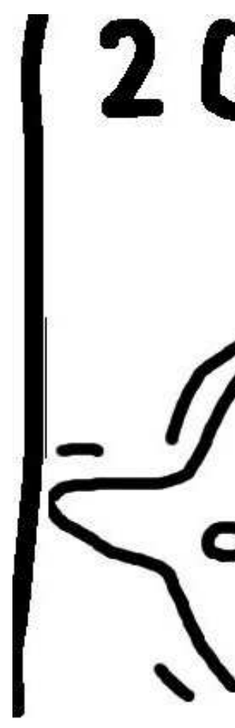
1985



Weierstrass sets off. Edwards left behind sleeping



Weierstrass sets off. Edwards
left behind sleeping

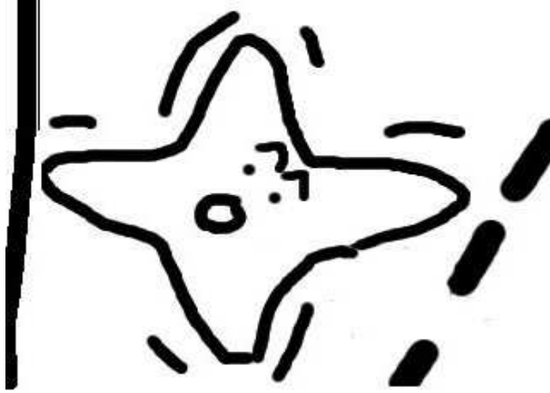


Weierstr
finally E

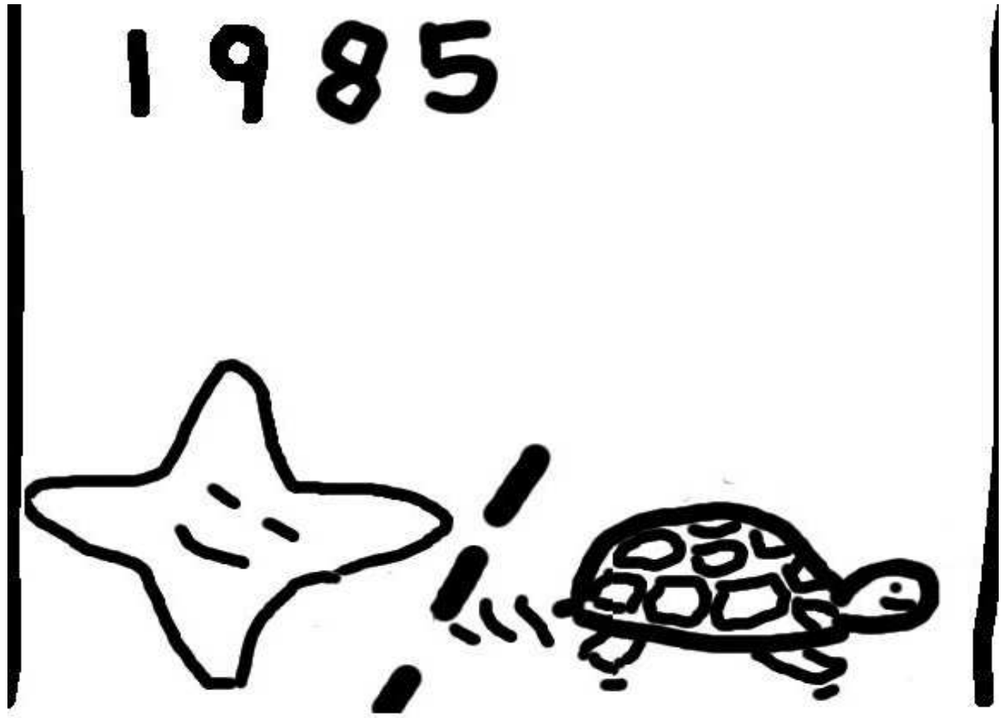
1985

Weierstrass sets off, Edwards
left behind sleeping

2007-

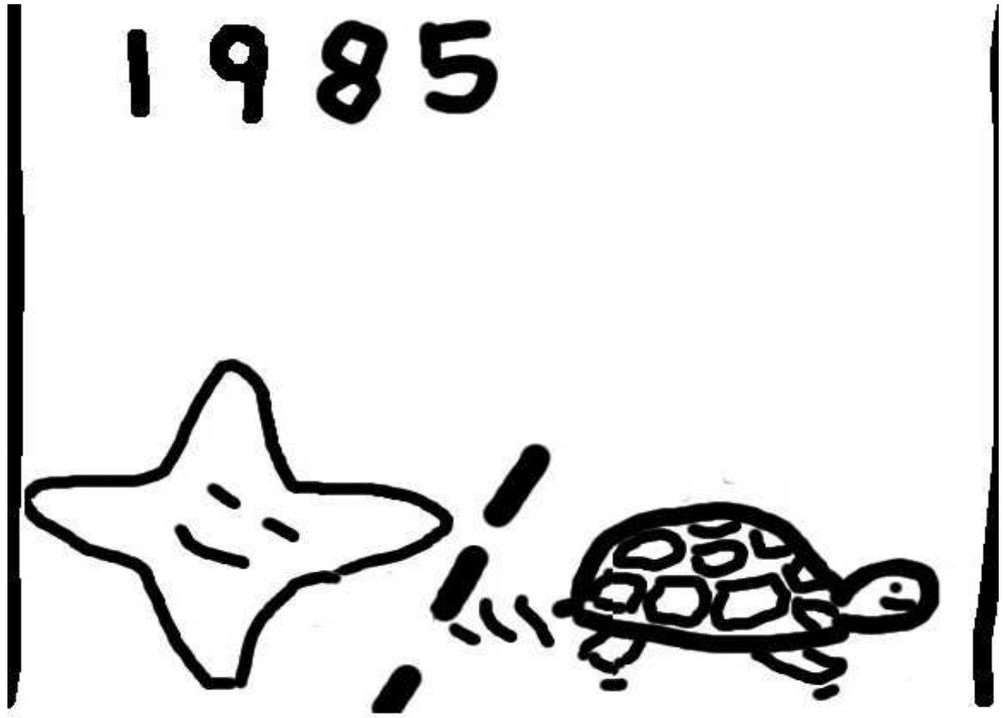


Weierstrass has made
finally Edwards wakes



Weierstrass sets off, Edwards left behind sleeping

Weierstrass has made some progress finally Edwards wakes up.



Weierstrass sets off. Edwards left behind sleeping

Weierstrass has made some progress - finally Edwards wakes up.

985

ass sets off. Edwards
d sleeping

2007-Jan

Weierstrass has made some progress -
finally Edwards wakes up.

Fe

Exciting
about t

Edwards

Weierstrass has made some progress -
finally Edwards wakes up.

Exciting progress: Edw
about to overtake!!

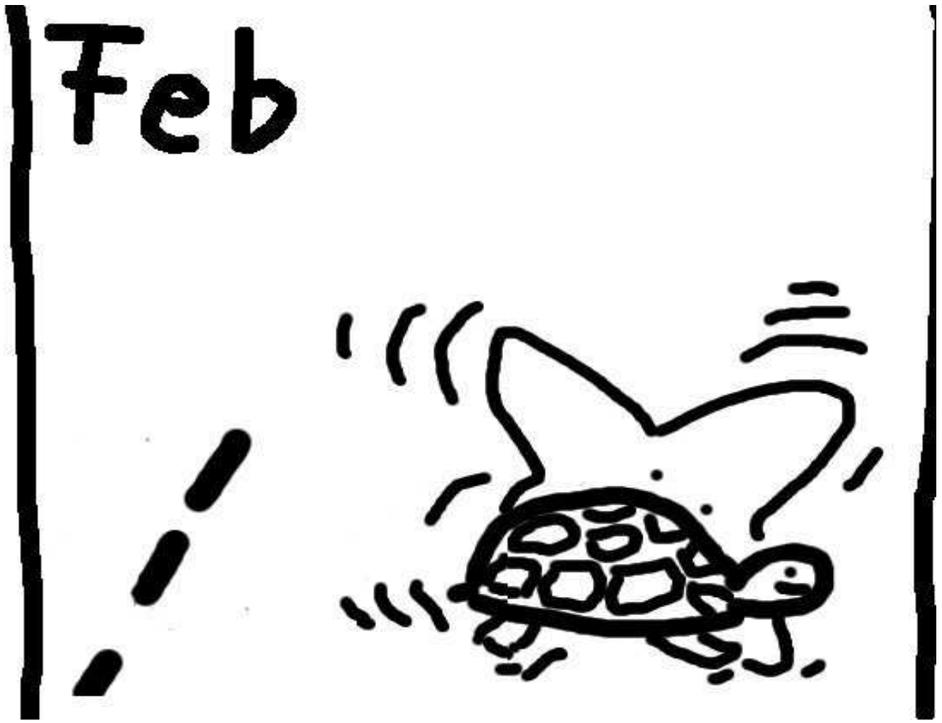
2007-Jan

Weierstrass has made some progress - finally Edwards wakes up.

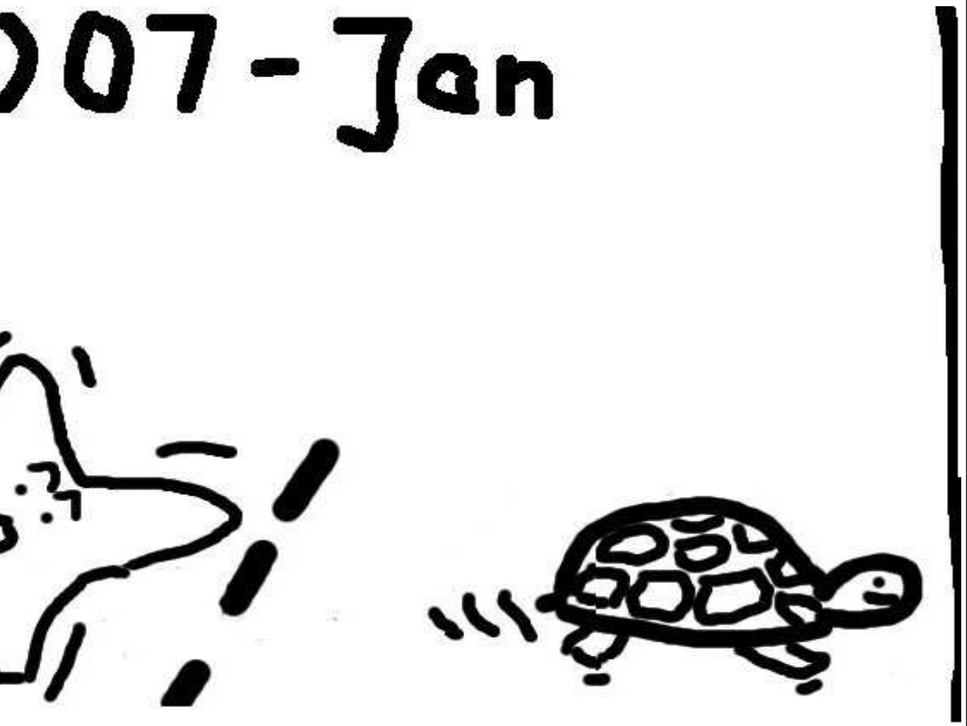
Feb

Exciting progress: Edwards about to overtake!!

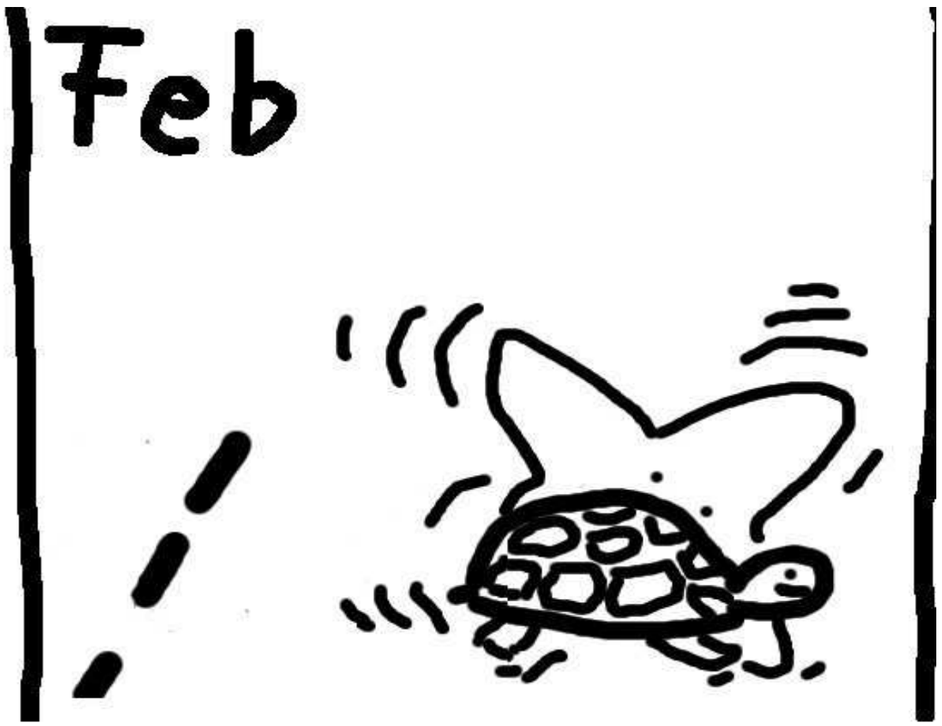
Weierstrass has made some progress - finally Edwards wakes up.



Exciting progress: Edwards about to overtake!!



ass has made some progress -
dwards wakes up.



Exciting progress: Edwards
about to overtake!!

And the

Jan

some progress -
s up.

Feb

Exciting progress: Edwards
about to overtake!!

Mar

And the winner is: Ed

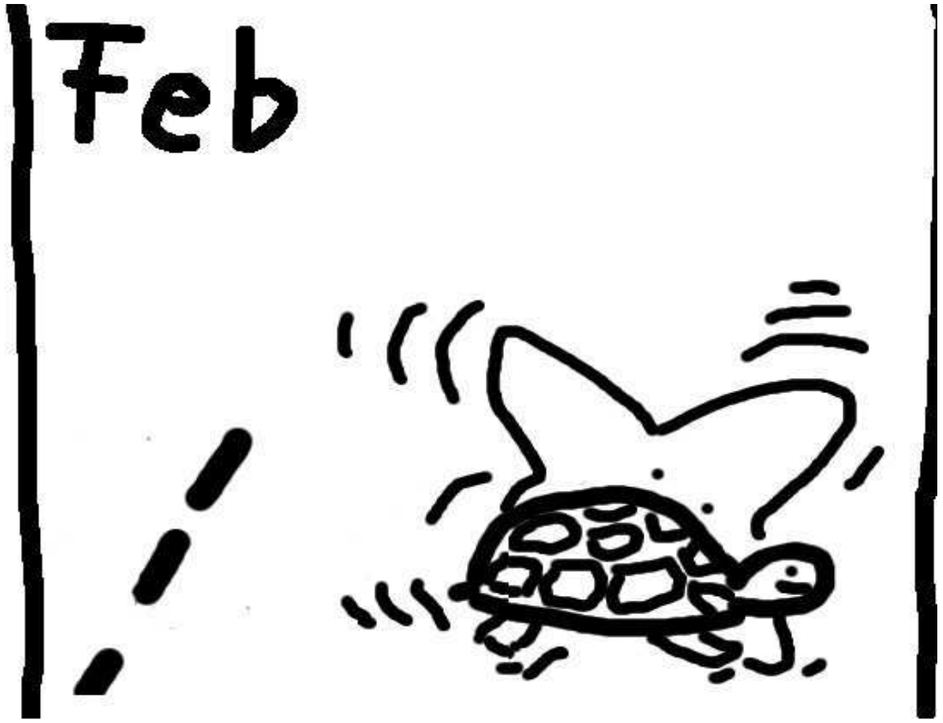
s -

Feb

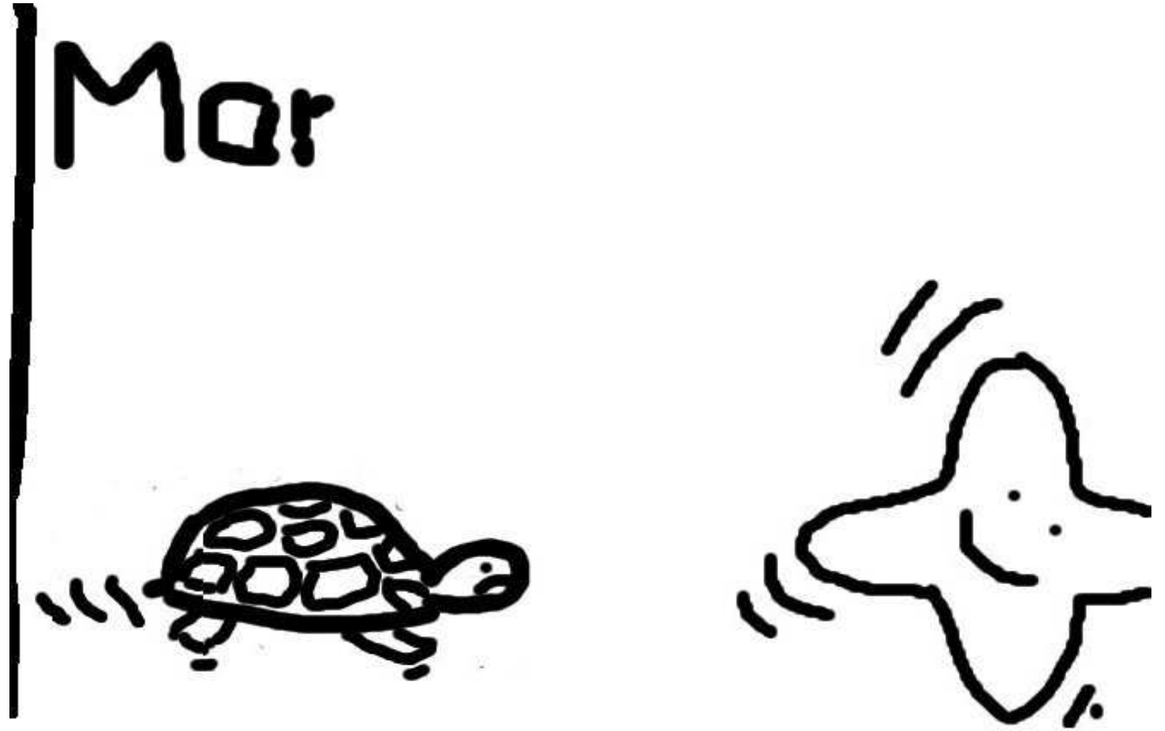
Exciting progress: Edwards about to overtake!!

Mar

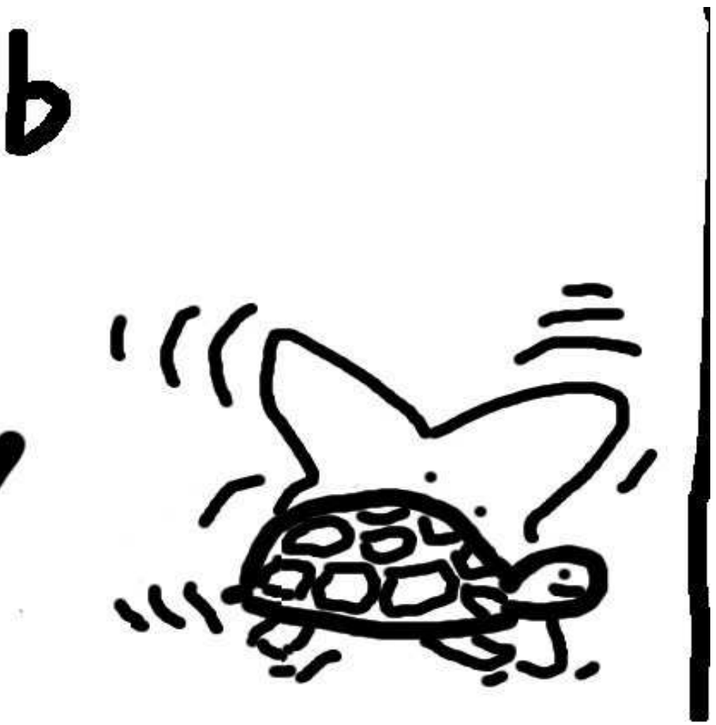
And the winner is: Edwards!

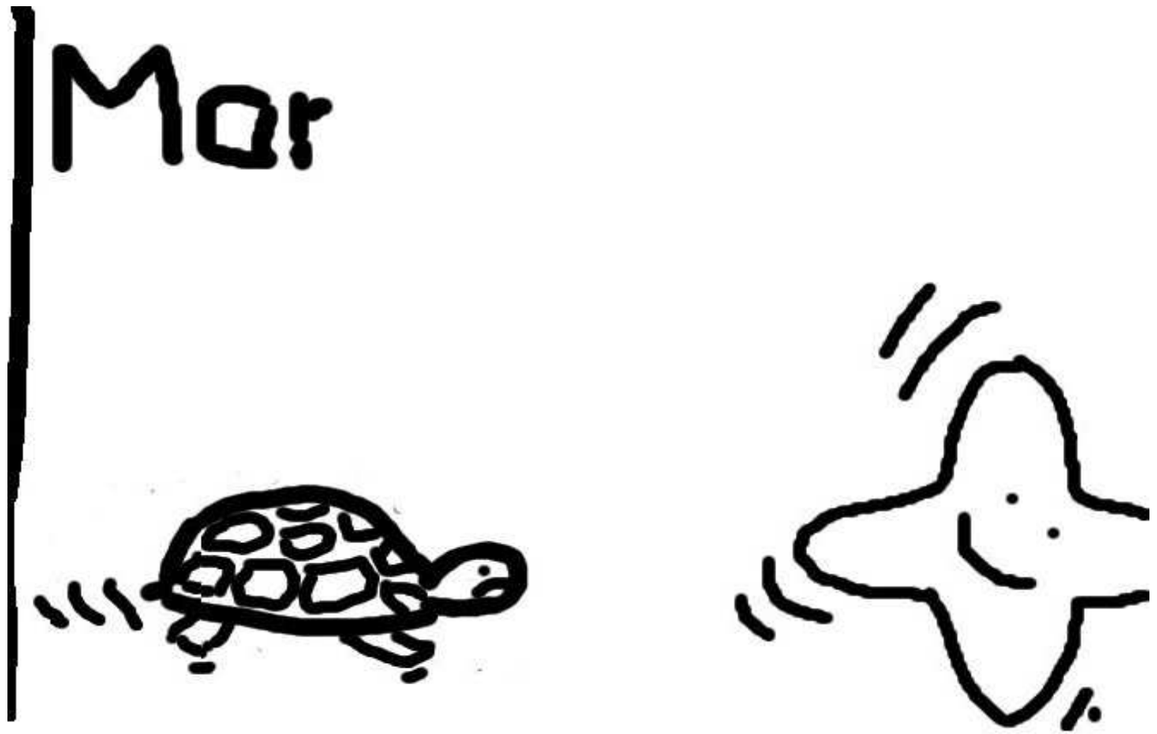


Exciting progress: Edwards about to overtake!!



And the winner is: Edwards!





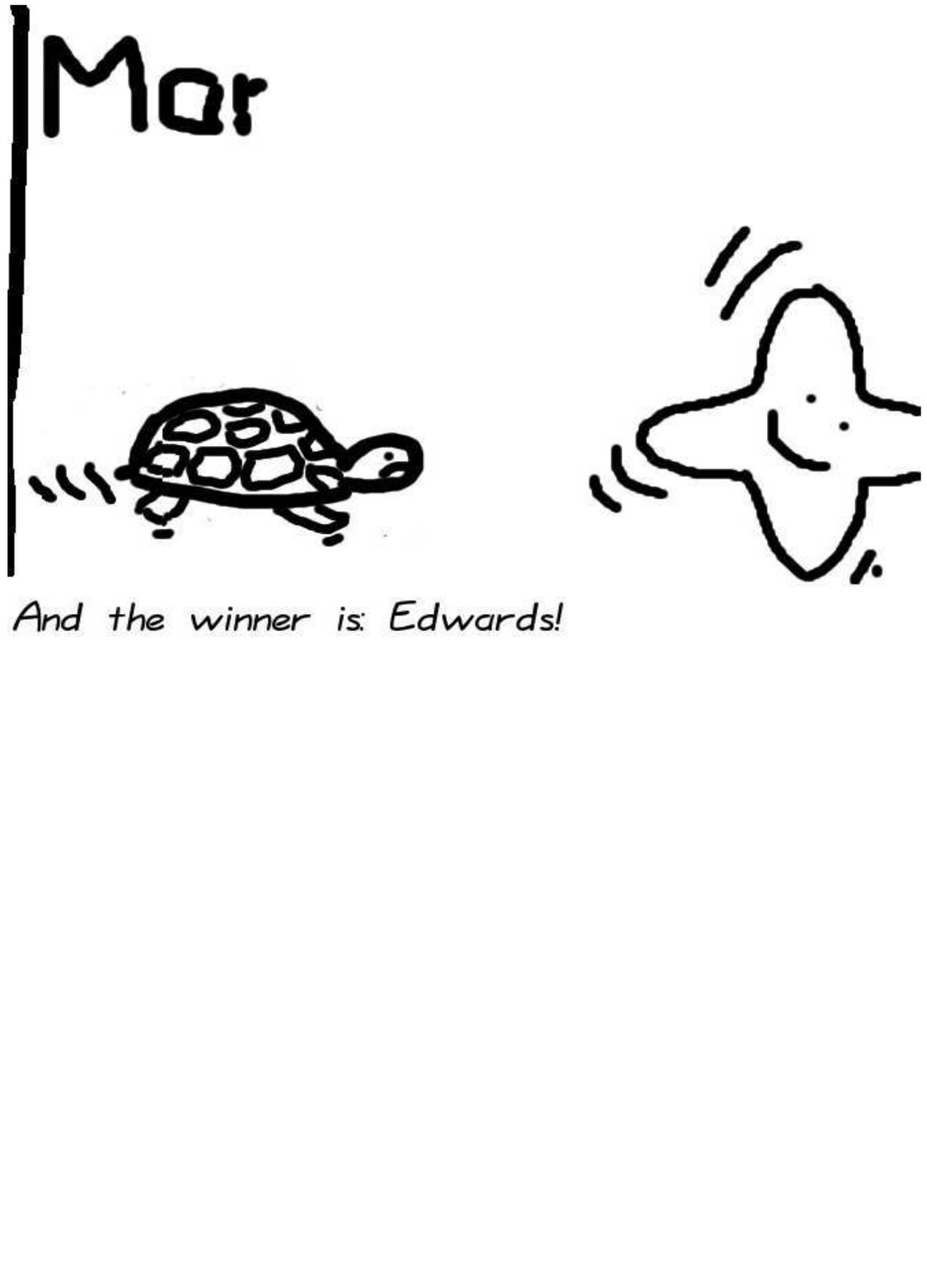
Speed-

2000 IB
uses W
in Jaco
to "pro
arithme
Also sp
choosin

2000 N
standar

2005 N
two of
the onl
for U.S

wards



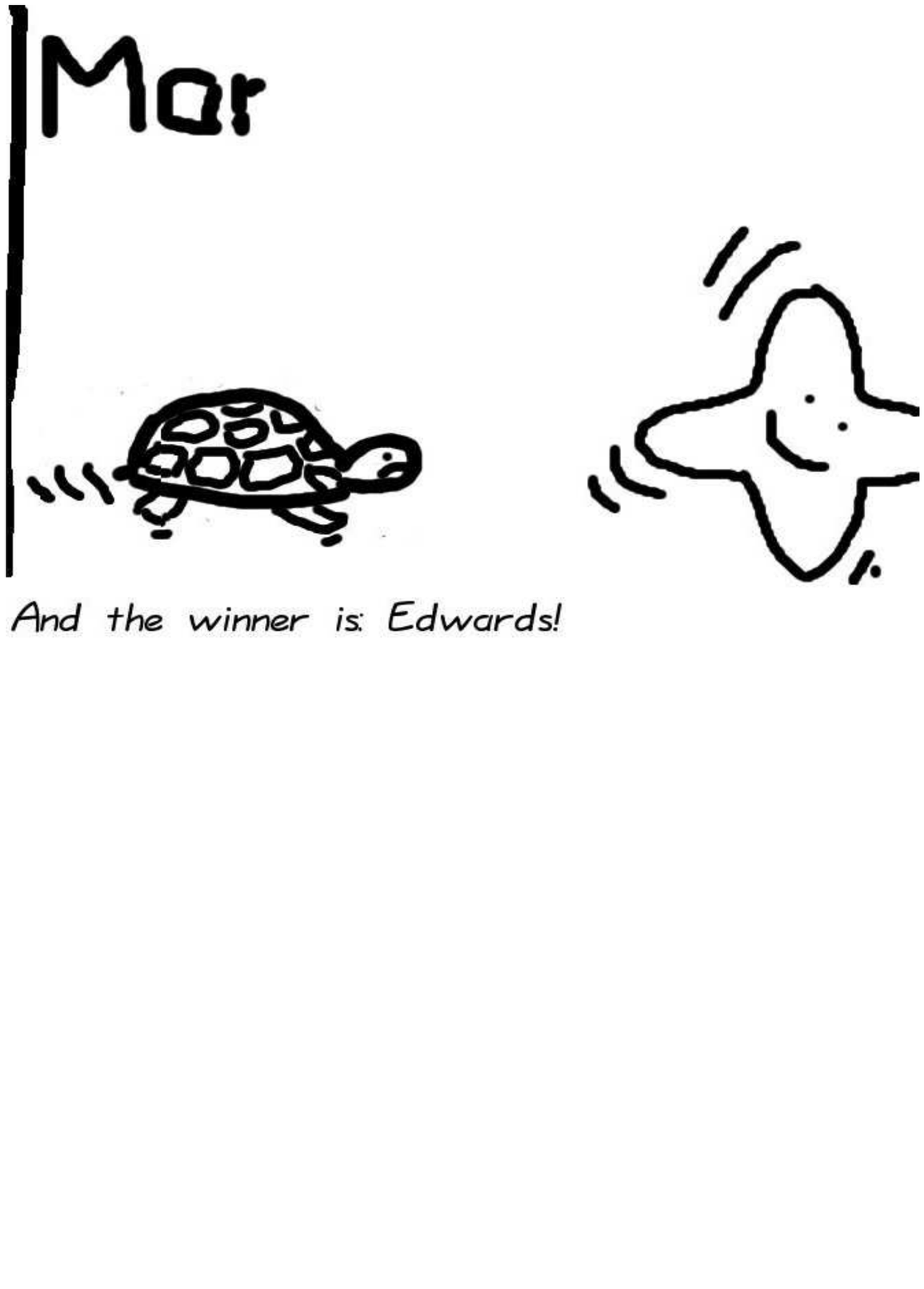
And the winner is: Edwards!

Speed-oriented J

2000 IEEE "Std
uses Weierstrass
in Jacobian coor
to "provide the f
arithmetic on elli
Also specifies a r
choosing curves

2000 NIST "FIPS
standardizes five

2005 NSA "Suite
two of the NIST
the only public-k
for U.S. governm

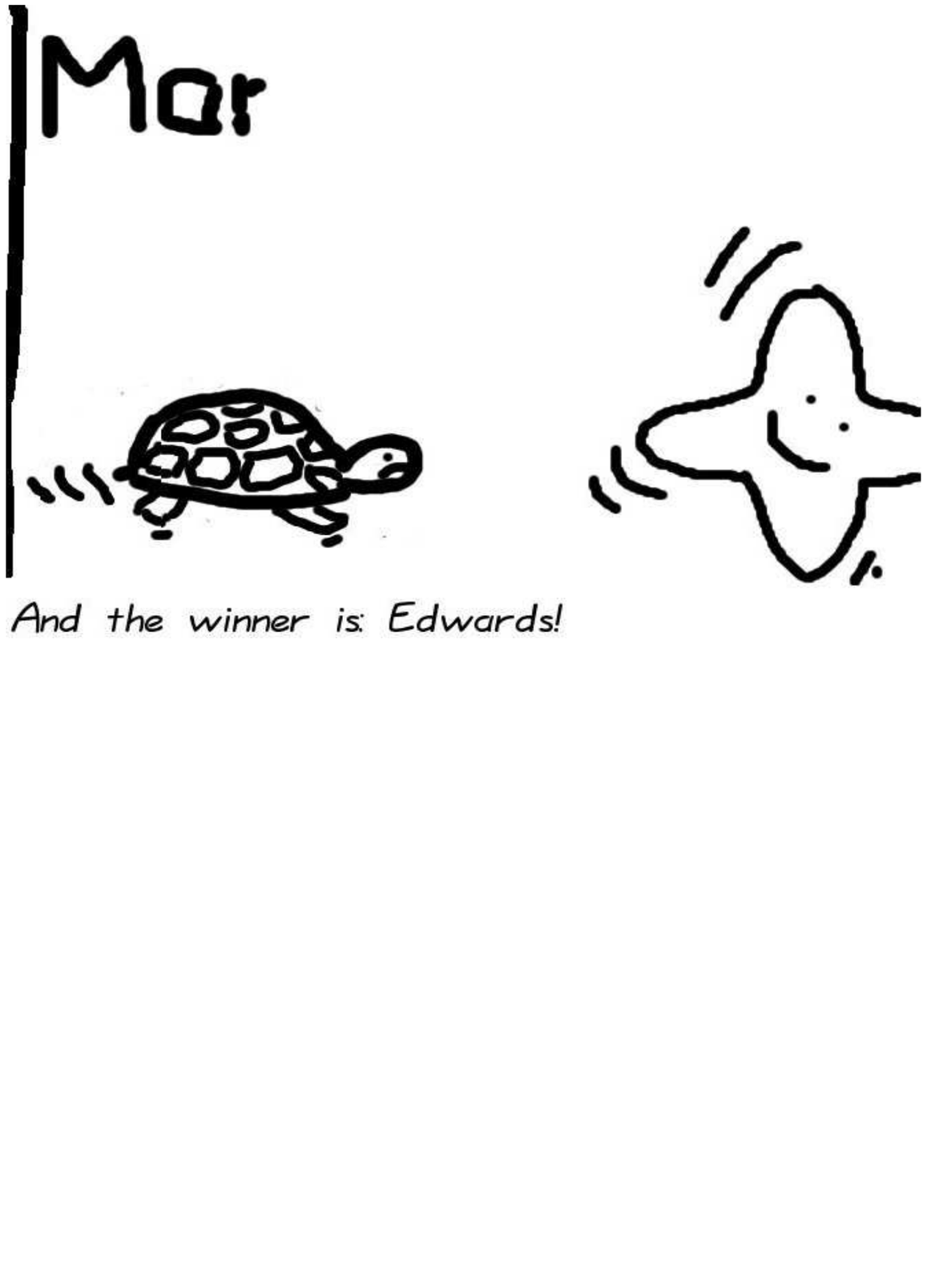


Speed-oriented Jacobian st

2000 IEEE "Std 1363"
uses Weierstrass curves
in Jacobian coordinates
to "provide the fastest
arithmetic on elliptic curve
Also specifies a method of
choosing curves $y^2 = x^3 -$

2000 NIST "FIPS 186–2"
standardizes five such curv

2005 NSA "Suite B" recon
two of the NIST curves as
the only public-key cryptos
for U.S. government use.



Speed-oriented Jacobian standards

2000 IEEE "Std 1363"
uses Weierstrass curves
in Jacobian coordinates
to "provide the fastest
arithmetic on elliptic curves."
Also specifies a method of
choosing curves $y^2 = x^3 - 3x + b$.

2000 NIST "FIPS 186–2"
standardizes five such curves.

2005 NSA "Suite B" recommends
two of the NIST curves as
the only public-key cryptosystems
for U.S. government use.

ar

winner is: Edwards!

Speed-oriented Jacobian standards

2000 IEEE "Std 1363"
uses Weierstrass curves
in Jacobian coordinates
to "provide the fastest
arithmetic on elliptic curves."
Also specifies a method of
choosing curves $y^2 = x^3 - 3x + b$.

2000 NIST "FIPS 186–2"
standardizes five such curves.

2005 NSA "Suite B" recommends
two of the NIST curves as
the only public-key cryptosystems
for U.S. government use.

Project

1986 C
Speed
$(X/Z^2$
$7\mathbf{M} + 3$
$12\mathbf{M} +$
$12\mathbf{M} +$

Option
DBL d
But AD
some a
batch s

wards!

Speed-oriented Jacobian standards

2000 IEEE "Std 1363"
uses Weierstrass curves
in Jacobian coordinates
to "provide the fastest
arithmetic on elliptic curves."
Also specifies a method of
choosing curves $y^2 = x^3 - 3x + b$.

2000 NIST "FIPS 186–2"
standardizes five such curves.

2005 NSA "Suite B" recommends
two of the NIST curves as
the only public-key cryptosystems
for U.S. government use.

Projective for We

1986 Chudnovsky
Speed up ADD b
$(X/Z^2, Y/Z^3)$ to
$7\mathbf{M} + 3\mathbf{S}$ for DB
$12\mathbf{M} + 2\mathbf{S}$ for AD
$12\mathbf{M} + 2\mathbf{S}$ for re

Option has been
DBL dominates i
But ADD domina
some application
batch signature v

Speed-oriented Jacobian standards

2000 IEEE "Std 1363"
uses Weierstrass curves
in Jacobian coordinates
to "provide the fastest
arithmetic on elliptic curves."
Also specifies a method of
choosing curves $y^2 = x^3 - 3x + b$.

2000 NIST "FIPS 186–2"
standardizes five such curves.

2005 NSA "Suite B" recommends
two of the NIST curves as
the only public-key cryptosystems
for U.S. government use.

Projective for Weierstrass

1986 Chudnovsky–Chudnov
Speed up ADD by switchin
$(X/Z^2, Y/Z^3)$ to $(X/Z, Y/$
$7\mathbf{M} + 3\mathbf{S}$ for DBL if $a = -$
$12\mathbf{M} + 2\mathbf{S}$ for ADD.
$12\mathbf{M} + 2\mathbf{S}$ for reADD.

Option has been mostly ign
DBL dominates in ECDH e
But ADD dominates in
some applications: e.g.,
batch signature verification

Speed-oriented Jacobian standards

2000 IEEE "Std 1363"
uses Weierstrass curves
in Jacobian coordinates
to "provide the fastest
arithmetic on elliptic curves."
Also specifies a method of
choosing curves $y^2 = x^3 - 3x + b$.

2000 NIST "FIPS 186–2"
standardizes five such curves.

2005 NSA "Suite B" recommends
two of the NIST curves as
the only public-key cryptosystems
for U.S. government use.

Projective for Weierstrass

1986 Chudnovsky–Chudnovsky:
Speed up ADD by switching from
$(X/Z^2, Y/Z^3)$ to $(X/Z, Y/Z)$.
$7\mathbf{M} + 3\mathbf{S}$ for DBL if $a = -3$.
$12\mathbf{M} + 2\mathbf{S}$ for ADD.
$12\mathbf{M} + 2\mathbf{S}$ for reADD.

Option has been mostly ignored:
DBL dominates in ECDH etc.
But ADD dominates in
some applications: e.g.,
batch signature verification.

oriented Jacobian standards

EEE "Std 1363"
Veierstrass curves
obian coordinates
ovide the fastest
etic on elliptic curves."
pecifies a method of
ng curves $y^2 = x^3 - 3x + b$.

IIST "FIPS 186–2"
rdizes five such curves.

ISA "Suite B" recommends
the NIST curves as
y public-key cryptosystems
S. government use.

Projective for Weierstrass

1986 Chudnovsky–Chudnovsky:
Speed up ADD by switching from
$(X/Z^2, Y/Z^3)$ to $(X/Z, Y/Z)$.
$7\mathbf{M} + 3\mathbf{S}$ for DBL if $a = -3$.
$12\mathbf{M} + 2\mathbf{S}$ for ADD.
$12\mathbf{M} + 2\mathbf{S}$ for reADD.

Option has been mostly ignored:
DBL dominates in ECDH etc.
But ADD dominates in
some applications: e.g.,
batch signature verification.

Montg

1987 M

Use by
Choose

$2(x_2, y$

$\Rightarrow x_4 =$

$(x_3, y_3$
$(x_3, y_3$

$\Rightarrow x_5 =$

acobian standards

1363”
curves
dinates
astest
ptic curves.”
method of
$y^2 = x^3 - 3x + b$.

S 186–2”
such curves.

e B” recommends
curves as
ey cryptosystems
nent use.

Projective for Weierstrass

1986 Chudnovsky–Chudnovsky:
Speed up ADD by switching from
$(X/Z^2, Y/Z^3)$ to $(X/Z, Y/Z)$.
$7\mathbf{M} + 3\mathbf{S}$ for DBL if $a = -3$.
$12\mathbf{M} + 2\mathbf{S}$ for ADD.
$12\mathbf{M} + 2\mathbf{S}$ for reADD.

Option has been mostly ignored:
DBL dominates in ECDH etc.
But ADD dominates in
some applications: e.g.,
batch signature verification.

Montgomery curv

1987 Montgomer

Use $by^2 = x^3 +$
Choose small $(a$

$2(x_2, y_2) = (x_4,$

$$\Rightarrow x_4 = \frac{(x_2^2}{4x_2(x_2^2}$$

$(x_3, y_3) - (x_2, y_2$
$(x_3, y_3) + (x_2, y_2$

$$\Rightarrow x_5 = \frac{(x_2x_3 -}{x_1(x_2 -}$$

tandards

s."

$3x + b$.

es.

mmends

systems

Projective for Weierstrass

1986 Chudnovsky–Chudnovsky:
Speed up ADD by switching from
$(X/Z^2, Y/Z^3)$ to $(X/Z, Y/Z)$.
$7\mathbf{M} + 3\mathbf{S}$ for DBL if $a = -3$.
$12\mathbf{M} + 2\mathbf{S}$ for ADD.
$12\mathbf{M} + 2\mathbf{S}$ for reADD.

Option has been mostly ignored:
DBL dominates in ECDH etc.
But ADD dominates in
some applications: e.g.,
batch signature verification.

Montgomery curves

1987 Montgomery:

Use $by^2 = x^3 + ax^2 + x$.
Choose small $(a + 2)/4$.

$2(x_2, y_2) = (x_4, y_4)$

$$\Rightarrow x_4 = \frac{(x_2^2 - 1)^2}{4x_2(x_2^2 + ax_2 + 1}$$

$(x_3, y_3) - (x_2, y_2) = (x_1, y$
$(x_3, y_3) + (x_2, y_2) = (x_5, y$

$$\Rightarrow x_5 = \frac{(x_2x_3 - 1)^2}{x_1(x_2 - x_3)^2}.$$

Projective for Weierstrass

1986 Chudnovsky–Chudnovsky:

Speed up ADD by switching from $(X/Z^2, Y/Z^3)$ to $(X/Z, Y/Z)$.

$7\mathbf{M} + 3\mathbf{S}$ for DBL if $a = -3$.

$12\mathbf{M} + 2\mathbf{S}$ for ADD.

$12\mathbf{M} + 2\mathbf{S}$ for reADD.

Option has been mostly ignored:
DBL dominates in ECDH etc.
But ADD dominates in
some applications: e.g.,
batch signature verification.

Montgomery curves

1987 Montgomery:

Use $by^2 = x^3 + ax^2 + x$.
Choose small $(a + 2)/4$.

$$2(x_2, y_2) = (x_4, y_4)$$

$$\Rightarrow x_4 = \frac{(x_2^2 - 1)^2}{4x_2(x_2^2 + ax_2 + 1)}.$$

$$(x_3, y_3) - (x_2, y_2) = (x_1, y_1),$$
$$(x_3, y_3) + (x_2, y_2) = (x_5, y_5)$$

$$\Rightarrow x_5 = \frac{(x_2x_3 - 1)^2}{x_1(x_2 - x_3)^2}.$$

tive for Weierstrass

Chudnovsky–Chudnovsky:
up ADD by switching from
$, Y/Z^3)$ to $(X/Z, Y/Z)$.
3**S** for DBL if $a = -3$.
+ 2**S** for ADD.
+ 2**S** for reADD.

has been mostly ignored:
ominates in ECDH etc.
DD dominates in
pplications: e.g.,
signature verification.

Montgomery curves

1987 Montgomery:

Use $by^2 = x^3 + ax^2 + x$.
Choose small $(a + 2)/4$.

$$2(x_2, y_2) = (x_4, y_4)$$
$$\Rightarrow x_4 = \frac{(x_2^2 - 1)^2}{4x_2(x_2^2 + ax_2 + 1)}.$$

$$(x_3, y_3) - (x_2, y_2) = (x_1, y_1),$$
$$(x_3, y_3) + (x_2, y_2) = (x_5, y_5)$$
$$\Rightarrow x_5 = \frac{(x_2x_3 - 1)^2}{x_1(x_2 - x_3)^2}.$$

Represe
as $(X:$

$B = (X$
$C = (X$
$D = B$
$Z_4 = D$
$2(X_2:Z$

$(X_3:Z_3$
$E = (X$
$F = (X$
$X_5 = Z$
$Z_5 = X$
$(X_3:Z_3$

eierstrass

y–Chudnovsky:
by switching from
$(X/Z, Y/Z)$.
L if $a = -3$.
DD.
ADD.

mostly ignored:
n ECDH etc.
ates in
s: e.g.,
verification.

Montgomery curves

1987 Montgomery:

Use $by^2 = x^3 + ax^2 + x$.
Choose small $(a + 2)/4$.

$$2(x_2, y_2) = (x_4, y_4)$$
$$\Rightarrow x_4 = \frac{(x_2^2 - 1)^2}{4x_2(x_2^2 + ax_2 + 1)}.$$

$$(x_3, y_3) - (x_2, y_2) = (x_1, y_1),$$
$$(x_3, y_3) + (x_2, y_2) = (x_5, y_5)$$
$$\Rightarrow x_5 = \frac{(x_2x_3 - 1)^2}{x_1(x_2 - x_3)^2}.$$

Represent (x, y)
as $(X{:}Z)$ satisfyi

$B = (X_2 + Z_2)^2$,
$C = (X_2 - Z_2)^2$,
$D = B - C$, X_4
$Z_4 = D \cdot (C + D$
$2(X_2{:}Z_2) = (X_4$

$(X_3{:}Z_3) - (X_2{:}Z$
$E = (X_3 - Z_3) \cdot$
$F = (X_3 + Z_3) \cdot$
$X_5 = Z_1 \cdot (E +$
$Z_5 = X_1 \cdot (E -$
$(X_3{:}Z_3) + (X_2{:}Z$

vsky:
ng from
Z).
-3.

nored:
etc.

n.

Montgomery curves

1987 Montgomery:

Use $by^2 = x^3 + ax^2 + x$.
Choose small $(a+2)/4$.

$2(x_2, y_2) = (x_4, y_4)$

$$\Rightarrow x_4 = \frac{(x_2^2 - 1)^2}{4x_2(x_2^2 + ax_2 + 1)}.$$

$(x_3, y_3) - (x_2, y_2) = (x_1, y_1)$,
$(x_3, y_3) + (x_2, y_2) = (x_5, y_5)$

$$\Rightarrow x_5 = \frac{(x_2x_3 - 1)^2}{x_1(x_2 - x_3)^2}.$$

Represent (x, y)
as $(X{:}Z)$ satisfying $x = X/$

$B = (X_2 + Z_2)^2$,
$C = (X_2 - Z_2)^2$,
$D = B - C$, $X_4 = B \cdot C$,
$Z_4 = D \cdot (C + D(a+2)/4$
$2(X_2{:}Z_2) = (X_4{:}Z_4)$.

$(X_3{:}Z_3) - (X_2{:}Z_2) = (X_1$
$E = (X_3 - Z_3) \cdot (X_2 + Z_2$
$F = (X_3 + Z_3) \cdot (X_2 - Z_2$
$X_5 = Z_1 \cdot (E + F)^2$,
$Z_5 = X_1 \cdot (E - F)^2 \Rightarrow$
$(X_3{:}Z_3) + (X_2{:}Z_2) = (X_5$

Montgomery curves

1987 Montgomery:

Use $by^2 = x^3 + ax^2 + x$.
Choose small $(a + 2)/4$.

$2(x_2, y_2) = (x_4, y_4)$

$$\Rightarrow x_4 = \frac{(x_2^2 - 1)^2}{4x_2(x_2^2 + ax_2 + 1)}.$$

$(x_3, y_3) - (x_2, y_2) = (x_1, y_1)$,
$(x_3, y_3) + (x_2, y_2) = (x_5, y_5)$

$$\Rightarrow x_5 = \frac{(x_2x_3 - 1)^2}{x_1(x_2 - x_3)^2}.$$

Represent (x, y)
as $(X{:}Z)$ satisfying $x = X/Z$.

$B = (X_2 + Z_2)^2$,
$C = (X_2 - Z_2)^2$,
$D = B - C$, $X_4 = B \cdot C$,
$Z_4 = D \cdot (C + D(a + 2)/4) \Rightarrow$
$2(X_2{:}Z_2) = (X_4{:}Z_4)$.

$(X_3{:}Z_3) - (X_2{:}Z_2) = (X_1{:}Z_1)$,
$E = (X_3 - Z_3) \cdot (X_2 + Z_2)$,
$F = (X_3 + Z_3) \cdot (X_2 - Z_2)$,
$X_5 = Z_1 \cdot (E + F)^2$,
$Z_5 = X_1 \cdot (E - F)^2 \Rightarrow$
$(X_3{:}Z_3) + (X_2{:}Z_2) = (X_5{:}Z_5)$.

omery curves

Montgomery:

$^2 = x^3 + ax^2 + x.$

e small $(a+2)/4$.

$_2) = (x_4, y_4)$

$$= \frac{(x_2^2-1)^2}{4x_2(x_2^2+ax_2+1)}.$$

$) - (x_2, y_2) = (x_1, y_1),$

$) + (x_2, y_2) = (x_5, y_5)$

$$= \frac{(x_2x_3-1)^2}{x_1(x_2-x_3)^2}.$$

Represent (x, y)
as $(X{:}Z)$ satisfying $x = X/Z$.

$B = (X_2 + Z_2)^2,$
$C = (X_2 - Z_2)^2,$
$D = B - C,\ X_4 = B \cdot C,$
$Z_4 = D \cdot (C + D(a+2)/4) \Rightarrow$
$2(X_2{:}Z_2) = (X_4{:}Z_4).$

$(X_3{:}Z_3) - (X_2{:}Z_2) = (X_1{:}Z_1),$
$E = (X_3 - Z_3) \cdot (X_2 + Z_2),$
$F = (X_3 + Z_3) \cdot (X_2 - Z_2),$
$X_5 = Z_1 \cdot (E+F)^2,$
$Z_5 = X_1 \cdot (E-F)^2 \Rightarrow$
$(X_3{:}Z_3) + (X_2{:}Z_2) = (X_5{:}Z_5).$

This re
does n
DADD
Q, R, Q

e.g. $2R$
e.g. $3R$
e.g. $6R$

$2\mathbf{M} + 2$
$4\mathbf{M} + 2$
Save 1

Easily
$\approx \lg n$
Almost
Relativ

ves

ry:

$ax^2 + x.$

$+ 2)/4.$

$y_4)$

$\frac{}{}$

$\frac{}{}$

$+ ax_2 + 1)$

$_2) = (x_1, y_1),$

$_2) = (x_5, y_5)$

$\frac{}{}$

$- 1)^2$

$- x_3)^2$

Represent (x, y)
as $(X{:}Z)$ satisfying $x = X/Z$.

$B = (X_2 + Z_2)^2,$
$C = (X_2 - Z_2)^2,$
$D = B - C,\ X_4 = B \cdot C,$
$Z_4 = D \cdot (C + D(a + 2)/4) \Rightarrow$
$2(X_2{:}Z_2) = (X_4{:}Z_4).$

$(X_3{:}Z_3) - (X_2{:}Z_2) = (X_1{:}Z_1),$
$E = (X_3 - Z_3) \cdot (X_2 + Z_2),$
$F = (X_3 + Z_3) \cdot (X_2 - Z_2),$
$X_5 = Z_1 \cdot (E + F)^2,$
$Z_5 = X_1 \cdot (E - F)^2 \Rightarrow$
$(X_3{:}Z_3) + (X_2{:}Z_2) = (X_5{:}Z_5).$

This representati
does not allow A
DADD, "differen
$Q, R, Q - R \mapsto Q$

e.g. $2P, P, P \mapsto$
e.g. $3P, 2P, P \mapsto$
e.g. $6P, 5P, P \mapsto$

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ f
$4\mathbf{M} + 2\mathbf{S}$ for DA
Save $1\mathbf{M}$ if $Z_1 =$

Easily compute n
$\approx \lg n$ DBL, $\approx$ lg
Almost as fast as
Relatively slow fo

$\overline{)}$.

$y_1)$,

$y_5)$

Represent (x, y)
as $(X{:}Z)$ satisfying $x = X/Z$.

$B = (X_2 + Z_2)^2$,
$C = (X_2 - Z_2)^2$,
$D = B - C$, $X_4 = B \cdot C$,
$Z_4 = D \cdot (C + D(a + 2)/4) \Rightarrow$
$2(X_2{:}Z_2) = (X_4{:}Z_4)$.

$(X_3{:}Z_3) - (X_2{:}Z_2) = (X_1{:}Z_1)$,
$E = (X_3 - Z_3) \cdot (X_2 + Z_2)$,
$F = (X_3 + Z_3) \cdot (X_2 - Z_2)$,
$X_5 = Z_1 \cdot (E + F)^2$,
$Z_5 = X_1 \cdot (E - F)^2 \Rightarrow$
$(X_3{:}Z_3) + (X_2{:}Z_2) = (X_5{:}Z_5)$.

This representation
does not allow ADD but it
DADD, "differential additi
$Q, R, Q - R \mapsto Q + R$.

e.g. $2P, P, P \mapsto 3P$.
e.g. $3P, 2P, P \mapsto 5P$.
e.g. $6P, 5P, P \mapsto 11P$.

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for DBL.
$4\mathbf{M} + 2\mathbf{S}$ for DADD.
Save $1\mathbf{M}$ if $Z_1 = 1$.

Easily compute $n(X_1 : Z_1)$
$\approx \lg n$ DBL, $\approx \lg n$ DADD
Almost as fast as Edwards
Relatively slow for $mP + n$

Represent (x, y)
as $(X{:}Z)$ satisfying $x = X/Z$.

$B = (X_2 + Z_2)^2$,
$C = (X_2 - Z_2)^2$,
$D = B - C$, $X_4 = B \cdot C$,
$Z_4 = D \cdot (C + D(a + 2)/4) \Rightarrow$
$2(X_2{:}Z_2) = (X_4{:}Z_4)$.

$(X_3{:}Z_3) - (X_2{:}Z_2) = (X_1{:}Z_1)$,
$E = (X_3 - Z_3) \cdot (X_2 + Z_2)$,
$F = (X_3 + Z_3) \cdot (X_2 - Z_2)$,
$X_5 = Z_1 \cdot (E + F)^2$,
$Z_5 = X_1 \cdot (E - F)^2 \Rightarrow$
$(X_3{:}Z_3) + (X_2{:}Z_2) = (X_5{:}Z_5)$.

This representation
does not allow ADD but it allows
DADD, "differential addition":
$Q, R, Q - R \mapsto Q + R$.

e.g. $2P, P, P \mapsto 3P$.
e.g. $3P, 2P, P \mapsto 5P$.
e.g. $6P, 5P, P \mapsto 11P$.

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for DBL.
$4\mathbf{M} + 2\mathbf{S}$ for DADD.
Save $1\mathbf{M}$ if $Z_1 = 1$.

Easily compute $n(X_1 : Z_1)$ using
$\approx \lg n$ DBL, $\approx \lg n$ DADD.
Almost as fast as Edwards nP.
Relatively slow for $mP + nQ$ etc.

ent (x, y)

$Z)$ satisfying $x = X/Z$.

$X_2 + Z_2)^2$,

$X_2 - Z_2)^2$,

$- C$, $X_4 = B \cdot C$,

$D \cdot (C + D(a + 2)/4) \Rightarrow$

$Z_2) = (X_4{:}Z_4)$.

$) - (X_2{:}Z_2) = (X_1{:}Z_1)$,

$X_3 - Z_3) \cdot (X_2 + Z_2)$,

$X_3 + Z_3) \cdot (X_2 - Z_2)$,

$Z_1 \cdot (E + F)^2$,

$X_1 \cdot (E - F)^2 \Rightarrow$

$) + (X_2{:}Z_2) = (X_5{:}Z_5)$.

This representation
does not allow ADD but it allows
DADD, "differential addition":
$Q, R, Q - R \mapsto Q + R$.

e.g. $2P, P, P \mapsto 3P$.

e.g. $3P, 2P, P \mapsto 5P$.

e.g. $6P, 5P, P \mapsto 11P$.

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for DBL.

$4\mathbf{M} + 2\mathbf{S}$ for DADD.

Save $1\mathbf{M}$ if $Z_1 = 1$.

Easily compute $n(X_1 : Z_1)$ using
$\approx \lg n$ DBL, $\approx \lg n$ DADD.
Almost as fast as Edwards nP.
Relatively slow for $mP + nQ$ etc.

Doubli

2006 D

Use y^2

Choose

Use $(X$

to repr

$3\mathbf{M} +$

How?

where

2007 B

$2\mathbf{M} +$

on the

ng $x = X/Z$.

$= B \cdot C$,
$(a+2)/4) \Rightarrow$
$Z_4)$.

$Z_2) = (X_1{:}Z_1)$,
$(X_2 + Z_2)$,
$(X_2 - Z_2)$,
$)^2$,
$)^2 \Rightarrow$
$Z_2) = (X_5{:}Z_5)$.

This representation
does not allow ADD but it allows
DADD, "differential addition":
$Q, R, Q - R \mapsto Q + R$.

e.g. $2P, P, P \mapsto 3P$.
e.g. $3P, 2P, P \mapsto 5P$.
e.g. $6P, 5P, P \mapsto 11P$.

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for DBL.
$4\mathbf{M} + 2\mathbf{S}$ for DADD.
Save $1\mathbf{M}$ if $Z_1 = 1$.

Easily compute $n(X_1 : Z_1)$ using
$\approx \lg n$ DBL, $\approx \lg n$ DADD.
Almost as fast as Edwards nP.
Relatively slow for $mP + nQ$ etc.

Doubling-oriente

2006 Doche–Icar

Use $y^2 = x^3 + a$
Choose small a.

Use $(X : Y : Z :$
to represent $(X/$

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ f
How? Factor DB
where φ is a 2-is

2007 Bernstein–L
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ f
on the same curv

$/Z$.

$) \Rightarrow$

$Z_1)$,
$)$,
$)$,

$Z_5)$.

This representation
does not allow ADD but it allows
DADD, "differential addition":
$Q, R, Q - R \mapsto Q + R$.

e.g. $2P, P, P \mapsto 3P$.
e.g. $3P, 2P, P \mapsto 5P$.
e.g. $6P, 5P, P \mapsto 11P$.

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for DBL.
$4\mathbf{M} + 2\mathbf{S}$ for DADD.
Save $1\mathbf{M}$ if $Z_1 = 1$.

Easily compute $n(X_1 : Z_1)$ using
$\approx \lg n$ DBL, $\approx \lg n$ DADD.
Almost as fast as Edwards nP.
Relatively slow for $mP + nQ$ etc.

<u>Doubling-oriented curves</u>

2006 Doche–Icart–Kohel:

Use $y^2 = x^3 + ax^2 + 16ax$
Choose small a.

Use $(X : Y : Z : Z^2)$
to represent $(X/Z, Y/Z^2)$.

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ for DBL.
How? Factor DBL as $\hat{\varphi}(\varphi$
where φ is a 2-isogeny.

2007 Bernstein–Lange:
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for DBL
on the same curves.

This representation
does not allow ADD but it allows
DADD, "differential addition":
$Q, R, Q - R \mapsto Q + R$.

e.g. $2P, P, P \mapsto 3P$.
e.g. $3P, 2P, P \mapsto 5P$.
e.g. $6P, 5P, P \mapsto 11P$.

$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for DBL.
$4\mathbf{M} + 2\mathbf{S}$ for DADD.
Save $1\mathbf{M}$ if $Z_1 = 1$.

Easily compute $n(X_1 : Z_1)$ using
$\approx \lg n$ DBL, $\approx \lg n$ DADD.
Almost as fast as Edwards nP.
Relatively slow for $mP + nQ$ etc.

Doubling-oriented curves

2006 Doche–Icart–Kohel:

Use $y^2 = x^3 + ax^2 + 16ax$.
Choose small a.

Use $(X : Y : Z : Z^2)$
to represent $(X/Z, Y/Z^2)$.

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ for DBL.
How? Factor DBL as $\hat{\varphi}(\varphi)$
where φ is a 2-isogeny.

2007 Bernstein–Lange:
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for DBL
on the same curves.

epresentation

ot allow ADD but it allows

, "differential addition":

$Q - R \mapsto Q + R$.

$P, P, P \mapsto 3P$.

$P, 2P, P \mapsto 5P$.

$P, 5P, P \mapsto 11P$.

$2\mathbf{S} + 1\mathbf{D}$ for DBL.

$2\mathbf{S}$ for DADD.

$\mathbf{M}$ if $Z_1 = 1$.

compute $n(X_1 : Z_1)$ using

DBL, $\approx \lg n$ DADD.

as fast as Edwards nP.

ely slow for $mP + nQ$ etc.

Doubling-oriented curves

2006 Doche–Icart–Kohel:

Use $y^2 = x^3 + ax^2 + 16ax$.
Choose small a.

Use $(X : Y : Z : Z^2)$
to represent $(X/Z, Y/Z^2)$.

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ for DBL.
How? Factor DBL as $\hat{\varphi}(\varphi)$
where φ is a 2-isogeny.

2007 Bernstein–Lange:
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for DBL
on the same curves.

$12\mathbf{M} +$

Slower

typicall

of the

But isc

Examp

fast DB

genus-2

using s

Tricky

tripling

(see 20

double-

on
DD but it allows
tial addition":
$Q + R$.

$3P$.
$5P$.
$11P$.

or DBL.
DD.
$= 1$.

$n(X_1 : Z_1)$ using
$g\, n$ DADD.
s Edwards nP.
or $mP + nQ$ etc.

Doubling-oriented curves

2006 Doche–Icart–Kohel:

Use $y^2 = x^3 + ax^2 + 16ax$.
Choose small a.

Use $(X : Y : Z : Z^2)$
to represent $(X/Z, Y/Z^2)$.

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ for DBL.
How? Factor DBL as $\hat{\varphi}(\varphi)$
where φ is a 2-isogeny.

2007 Bernstein–Lange:
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for DBL
on the same curves.

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$
Slower ADD tha
typically outweig
of the very fast D

But isogenies are
Example, 2005 G
fast DBL+DADD
genus-2 hyperelli
using similar fact

Tricky but poten
tripling-oriented
(see 2006 Doche
double-base chai

allows
on":

using
.
nP.
nQ etc.

Doubling-oriented curves

2006 Doche–Icart–Kohel:

Use $y^2 = x^3 + ax^2 + 16ax$.
Choose small a.

Use $(X : Y : Z : Z^2)$
to represent $(X/Z, Y/Z^2)$.

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ for DBL.
How? Factor DBL as $\hat{\varphi}(\varphi)$
where φ is a 2-isogeny.

2007 Bernstein–Lange:
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for DBL
on the same curves.

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for ADD.
Slower ADD than other sys
typically outweighing benef
of the very fast DBL.

But isogenies are useful.
Example, 2005 Gaudry:
fast DBL+DADD on Jacob
genus-2 hyperelliptic curves
using similar factorization.

Tricky but potentially helpf
tripling-oriented curves
(see 2006 Doche–Icart–Koh
double-base chains, ...

Doubling-oriented curves

2006 Doche–Icart–Kohel:

Use $y^2 = x^3 + ax^2 + 16ax$.
Choose small a.

Use $(X : Y : Z : Z^2)$
to represent $(X/Z, Y/Z^2)$.

$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ for DBL.
How? Factor DBL as $\hat{\varphi}(\varphi)$
where φ is a 2-isogeny.

2007 Bernstein–Lange:
$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for DBL
on the same curves.

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for ADD.
Slower ADD than other systems,
typically outweighing benefit
of the very fast DBL.

But isogenies are useful.
Example, 2005 Gaudry:
fast DBL+DADD on Jacobians of
genus-2 hyperelliptic curves,
using similar factorization.

Tricky but potentially helpful:
tripling-oriented curves
(see 2006 Doche–Icart–Kohel),
double-base chains, ...

ng-oriented curves

Doche–Icart–Kohel:

$= x^3 + ax^2 + 16ax$.

e small a.

$X : Y : Z : Z^2$)

esent $(X/Z, Y/Z^2)$.

$4\mathbf{S} + 2\mathbf{D}$ for DBL.

Factor DBL as $\hat{\varphi}(\varphi)$

φ is a 2-isogeny.

Bernstein–Lange:

$5\mathbf{S} + 2\mathbf{D}$ for DBL

same curves.

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for ADD.

Slower ADD than other systems,
typically outweighing benefit
of the very fast DBL.

But isogenies are useful.

Example, 2005 Gaudry:
fast DBL+DADD on Jacobians of
genus-2 hyperelliptic curves,
using similar factorization.

Tricky but potentially helpful:
tripling-oriented curves
(see 2006 Doche–Icart–Kohel),
double-base chains, ...

Hessian

Credite
by 198

$(X : Y$
on x^3

$12\mathbf{M}$ fo

$X_3 = Y$

$Y_3 = X$

$Z_3 = Z$

$6\mathbf{M} + 3$

d curves

t–Kohel:

$x^2 + 16ax$.

$Z^2)$

$Z, Y/Z^2)$.

or DBL.

BL as $\hat{\varphi}(\varphi)$

ogeny.

Lange:

or DBL

ves.

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for ADD.
Slower ADD than other systems,
typically outweighing benefit
of the very fast DBL.

But isogenies are useful.
Example, 2005 Gaudry:
fast DBL+DADD on Jacobians of
genus-2 hyperelliptic curves,
using similar factorization.

Tricky but potentially helpful:
tripling-oriented curves
(see 2006 Doche–Icart–Kohel),
double-base chains, ...

Hessian curves

Credited to Sylve
by 1986 Chudnov

$(X : Y : Z)$ repre
on $x^3 + y^3 + 1 =$

$12\mathbf{M}$ for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z$
$Y_3 = X_1Z_2 \cdot X_1Y$
$Z_3 = Z_1Y_2 \cdot Z_1X$

$6\mathbf{M} + 3\mathbf{S}$ for DB

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for ADD.
Slower ADD than other systems,
typically outweighing benefit
of the very fast DBL.

But isogenies are useful.
Example, 2005 Gaudry:
fast DBL+DADD on Jacobians of
genus-2 hyperelliptic curves,
using similar factorization.

Tricky but potentially helpful:
tripling-oriented curves
(see 2006 Doche–Icart–Kohel),
double-base chains, ...

Hessian curves

Credited to Sylvester
by 1986 Chudnovsky–Chud

$(X : Y : Z)$ represent $(X/Z$
on $x^3 + y^3 + 1 = 3dxy$.

$12\mathbf{M}$ for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2$
$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2$
$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2$

$6\mathbf{M} + 3\mathbf{S}$ for DBL.

$12\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for ADD.
Slower ADD than other systems,
typically outweighing benefit
of the very fast DBL.

But isogenies are useful.
Example, 2005 Gaudry:
fast DBL+DADD on Jacobians of
genus-2 hyperelliptic curves,
using similar factorization.

Tricky but potentially helpful:
tripling-oriented curves
(see 2006 Doche–Icart–Kohel),
double-base chains, ...

Hessian curves

Credited to Sylvester
by 1986 Chudnovsky–Chudnovsky:

$(X : Y : Z)$ represent $(X/Z, Y/Z)$
on $x^3 + y^3 + 1 = 3dxy$.

$12\mathbf{M}$ for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,
$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,
$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

$6\mathbf{M} + 3\mathbf{S}$ for DBL.

$+ 5\mathbf{S} + 1\mathbf{D}$ for ADD.
ADD than other systems,
ly outweighing benefit
very fast DBL.

ogenies are useful.
le, 2005 Gaudry:
BL+DADD on Jacobians of
2 hyperelliptic curves,
imilar factorization.

but potentially helpful:
g-oriented curves
006 Doche–Icart–Kohel),
-base chains, ...

Hessian curves

Credited to Sylvester
by 1986 Chudnovsky–Chudnovsky:

$(X : Y : Z)$ represent $(X/Z, Y/Z)$
on $x^3 + y^3 + 1 = 3dxy$.

$12\mathbf{M}$ for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,
$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,
$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

$6\mathbf{M} + 3\mathbf{S}$ for DBL.

2001 J
$2(X_1 :$
$(Z_1 : X$
so can

"Unifie
helpful
But no
need to

2008.0
$(X : Y$
$: 2$
$6\mathbf{M} + 6$
$3\mathbf{M} + 6$

for ADD.
n other systems,
hing benefit
DBL.

e useful.
Gaudry:
D on Jacobians of
ptic curves,
torization.

tially helpful:
curves
–Icart–Kohel),
ns, ...

Hessian curves

Credited to Sylvester
by 1986 Chudnovsky–Chudnovsky:

$(X : Y : Z)$ represent $(X/Z, Y/Z)$
on $x^3 + y^3 + 1 = 3dxy$.

12**M** for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,
$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,
$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

$6\mathbf{M} + 3\mathbf{S}$ for DBL.

2001 Joye–Quisq
$2(X_1 : Y_1 : Z_1) =$
$(Z_1 : X_1 : Y_1) +$
so can use ADD

"Unified addition
helpful against si
But not strongly
need to permute

2008.02 Hisil–Wo
$(X : Y : Z : X^2 :$
$: 2XY : 2XZ$
$6\mathbf{M} + 6\mathbf{S}$ for AD
$3\mathbf{M} + 6\mathbf{S}$ for DB

stems,
fit

bians of
s,

ful:

hel),

Hessian curves

Credited to Sylvester
by 1986 Chudnovsky–Chudnovsky:

$(X : Y : Z)$ represent $(X/Z, Y/Z)$
on $x^3 + y^3 + 1 = 3dxy$.

12**M** for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,
$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,
$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

$6\mathbf{M} + 3\mathbf{S}$ for DBL.

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

"Unified addition formulas,
helpful against side channe
But not strongly unified:
need to permute inputs.

2008.02 Hisil–Wong–Carter
$(X : Y : Z : X^2 : Y^2 : Z^2$
$: 2XY : 2XZ : 2YZ)$.
$6\mathbf{M} + 6\mathbf{S}$ for ADD.
$3\mathbf{M} + 6\mathbf{S}$ for DBL.

Hessian curves

Credited to Sylvester
by 1986 Chudnovsky–Chudnovsky:

$(X : Y : Z)$ represent $(X/Z, Y/Z)$
on $x^3 + y^3 + 1 = 3dxy$.

12**M** for ADD:
$X_3 = Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,
$Y_3 = X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,
$Z_3 = Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

$6\mathbf{M} + 3\mathbf{S}$ for DBL.

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 not strongly unified:
need to permute inputs.

2008.02 Hisil–Wong–Carter–Dawson:
$(X : Y : Z : X^2 : Y^2 : Z^2$
$: 2XY : 2XZ : 2YZ)$.
$6\mathbf{M} + 6\mathbf{S}$ for ADD.
$3\mathbf{M} + 6\mathbf{S}$ for DBL.

n curves

ed to Sylvester

6 Chudnovsky–Chudnovsky:

$: Z)$ represent $(X/Z, Y/Z)$

$+ y^3 + 1 = 3dxy$.

or ADD:

$Y_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,

$X_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,

$Z_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

3**S** for DBL.

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 not strongly unified:

need to permute inputs.

2008.02 Hisil–Wong–Carter–Dawson:

$(X : Y : Z : X^2 : Y^2 : Z^2$

$: 2XY : 2XZ : 2YZ)$.

$6\mathbf{M} + 6\mathbf{S}$ for ADD.

$3\mathbf{M} + 6\mathbf{S}$ for DBL.

$x^3 - y$

ester

vsky–Chudnovsky:

esent $(X/Z, Y/Z)$

$= 3dxy$.

$Y_2 - Z_1Y_2 \cdot X_1Y_2$,

$Y_2 - Y_1X_2 \cdot Z_1X_2$,

$X_2 - X_1Z_2 \cdot Y_1Z_2$.

L.

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 not strongly unified:

need to permute inputs.

2008.02 Hisil–Wong–Carter–Dawson:

$(X : Y : Z : X^2 : Y^2 : Z^2$

$: 2XY : 2XZ : 2YZ)$.

$6\mathbf{M} + 6\mathbf{S}$ for ADD.

$3\mathbf{M} + 6\mathbf{S}$ for DBL.

$x^3 - y^3 + 1 = 0$.

lnovsky:

$Z, Y/Z)$

$+ X_1Y_2,$

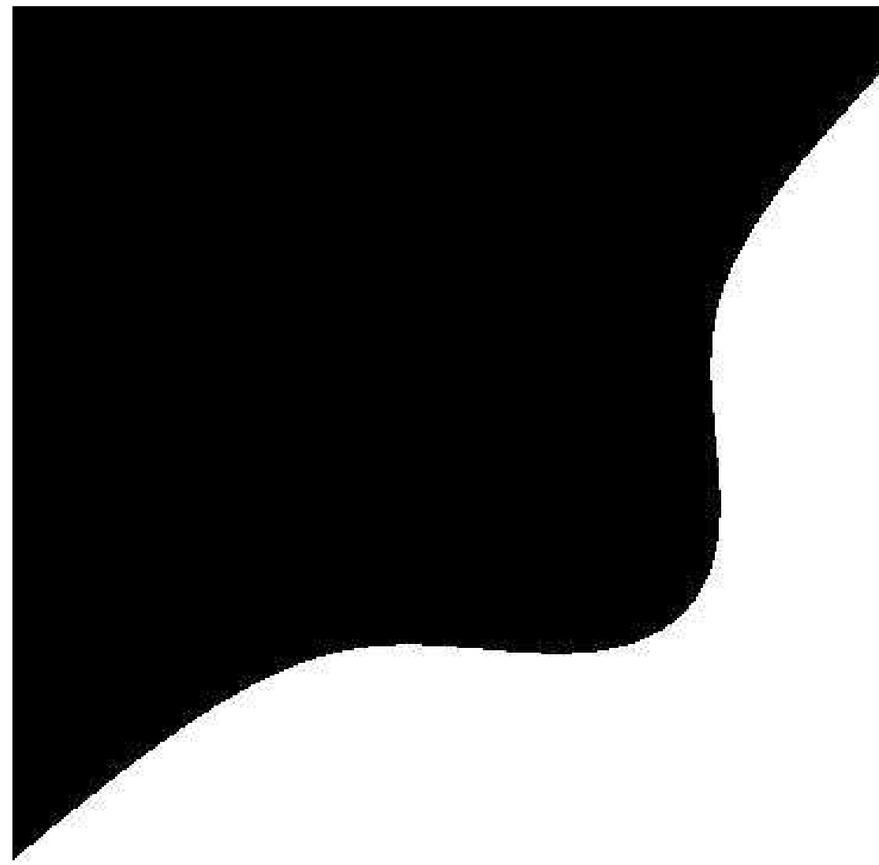
$\cdot Z_1X_2,$

$\cdot Y_1Z_2.$

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 not strongly unified:
need to permute inputs.

2008.02 Hisil–Wong–Carter–Dawson:
$(X : Y : Z : X^2 : Y^2 : Z^2$
$: 2XY : 2XZ : 2YZ).$
$6\mathbf{M} + 6\mathbf{S}$ for ADD.
$3\mathbf{M} + 6\mathbf{S}$ for DBL.

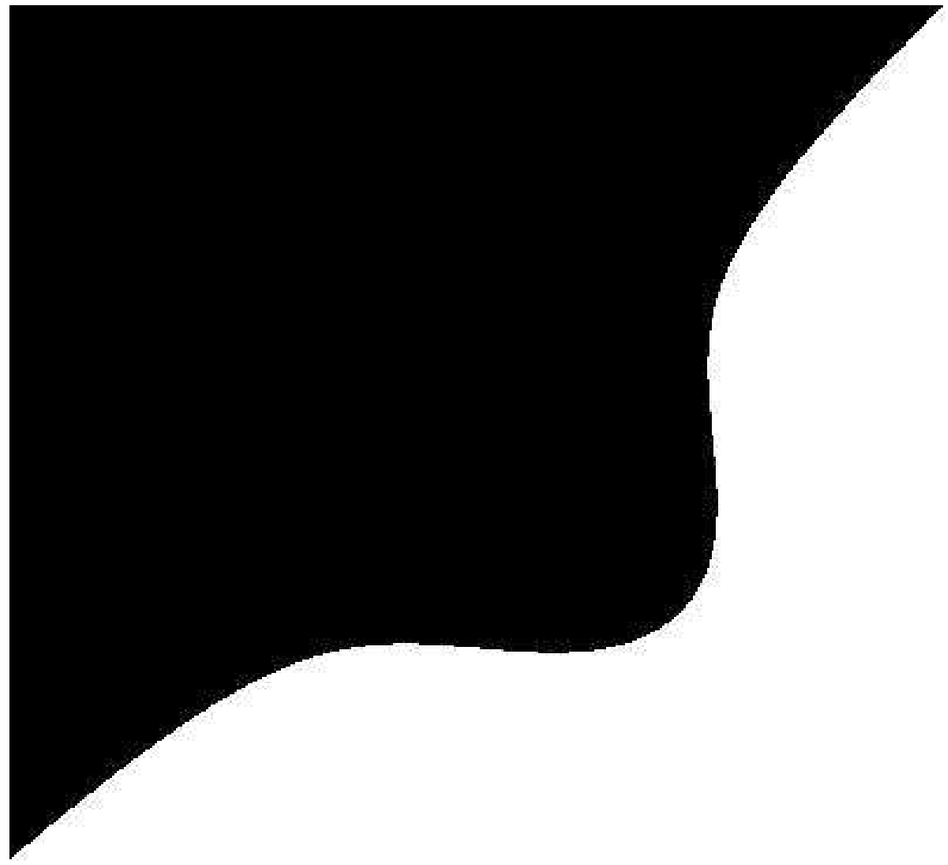


$x^3 - y^3 + 1 = 0.3xy$

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 not strongly unified:
need to permute inputs.

2008.02 Hisil–Wong–Carter–Dawson:
$(X : Y : Z : X^2 : Y^2 : Z^2$
$: 2XY : 2XZ : 2YZ)$.
$6\mathbf{M} + 6\mathbf{S}$ for ADD.
$3\mathbf{M} + 6\mathbf{S}$ for DBL.



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

oye–Quisquater:

$Y_1 : Z_1) =$

$X_1 : Y_1) + (Y_1 : Z_1 : X_1)$

use ADD to double.

ed addition formulas,"

against side channels.

t strongly unified:

o permute inputs.

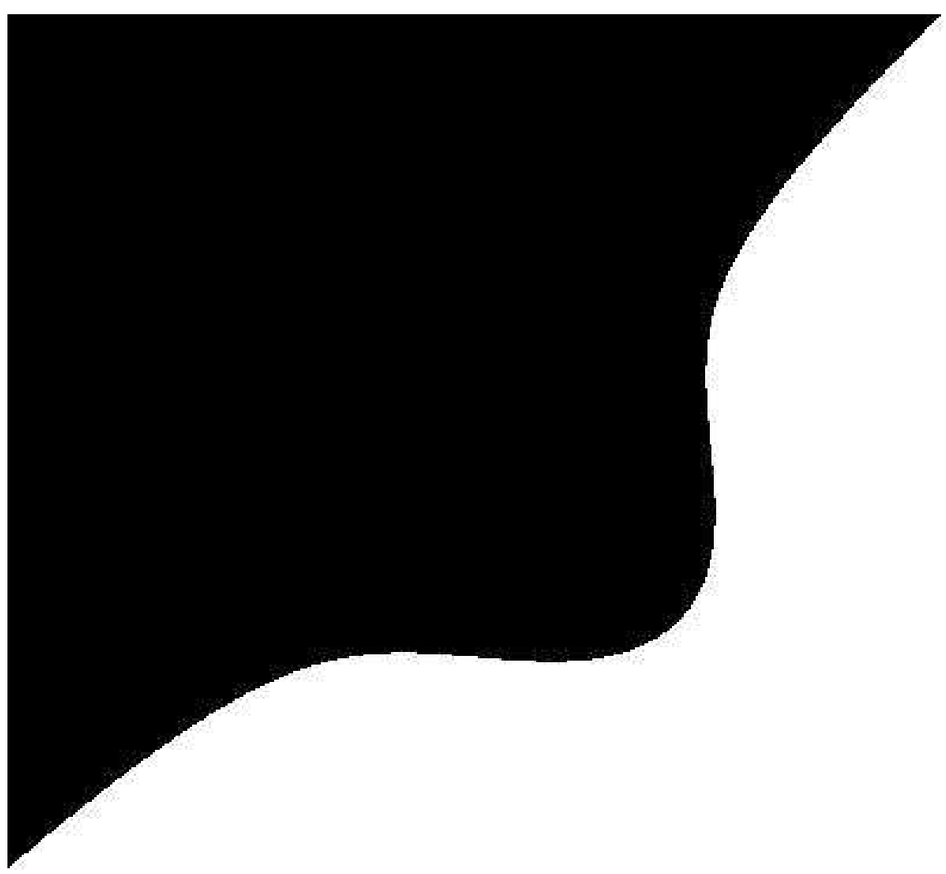
2 Hisil–Wong–Carter–Dawson:

$: Z : X^2 : Y^2 : Z^2$

$2XY : 2XZ : 2YZ$).

6**S** for ADD.

6**S** for DBL.



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

uater:

=

$(Y_1 : Z_1 : X_1)$

to double.

formulas,"

de channels.

unified:

inputs.

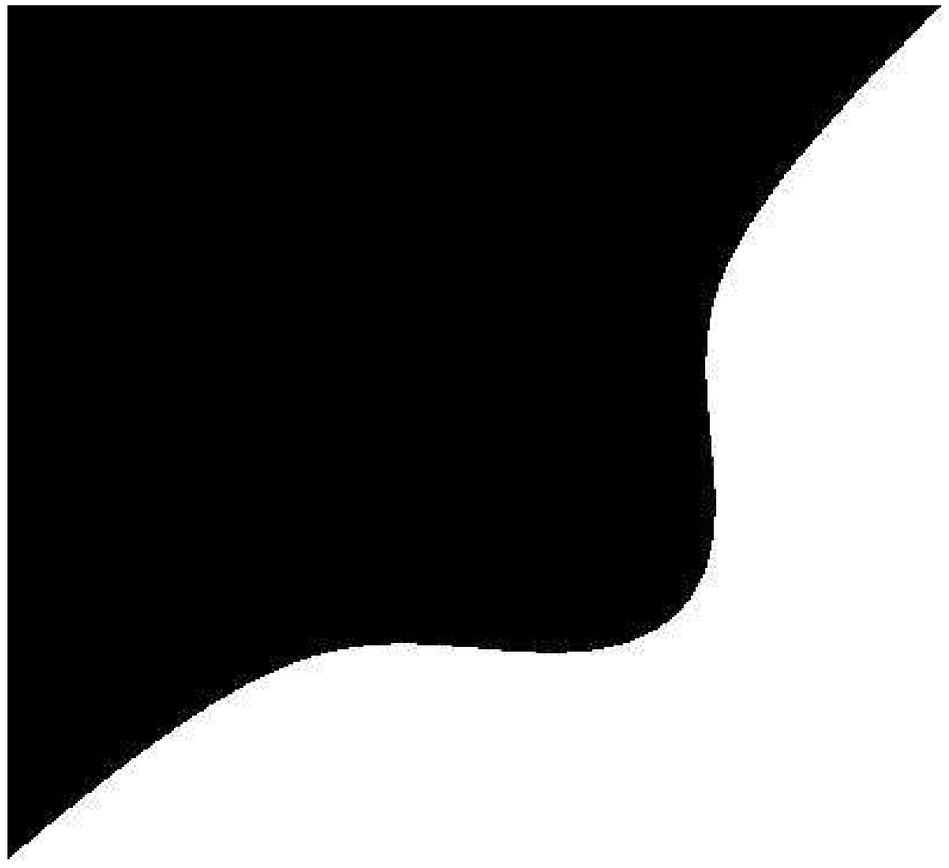
ong–Carter–Dawson:

$Y^2 : Z^2$

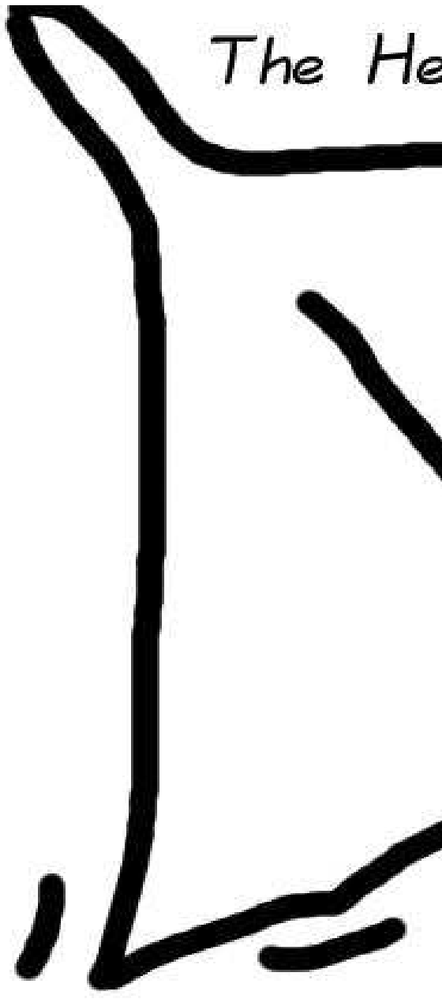
$Z : 2YZ$).

D.

L.



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



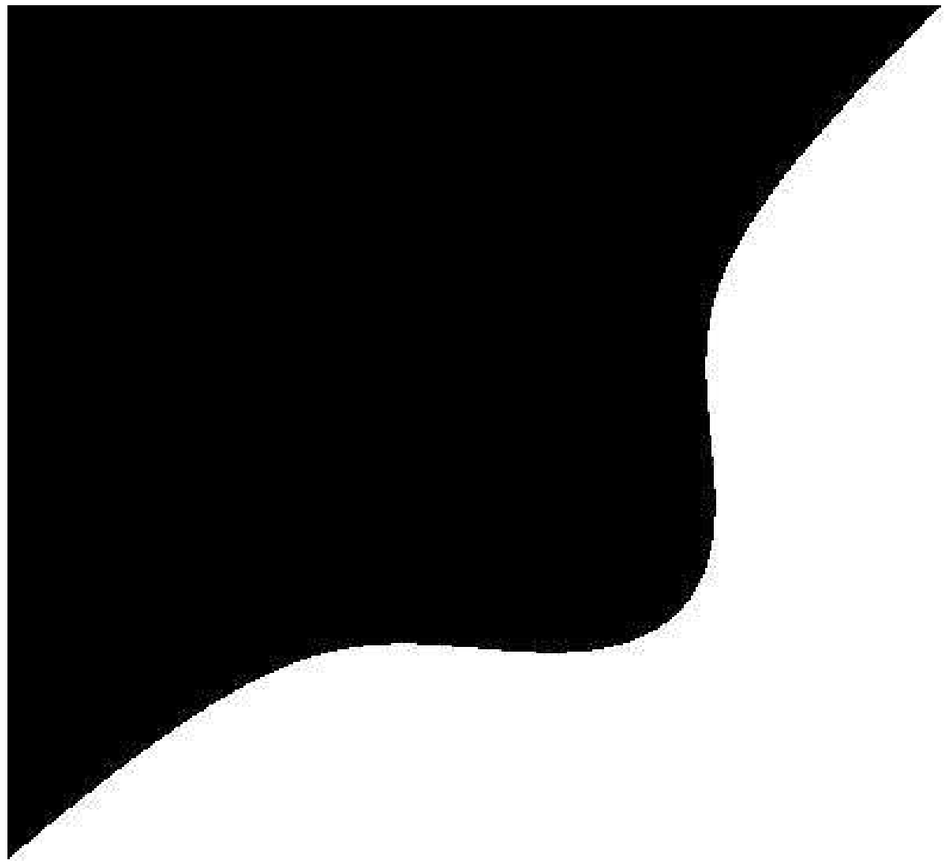
X_1)

.

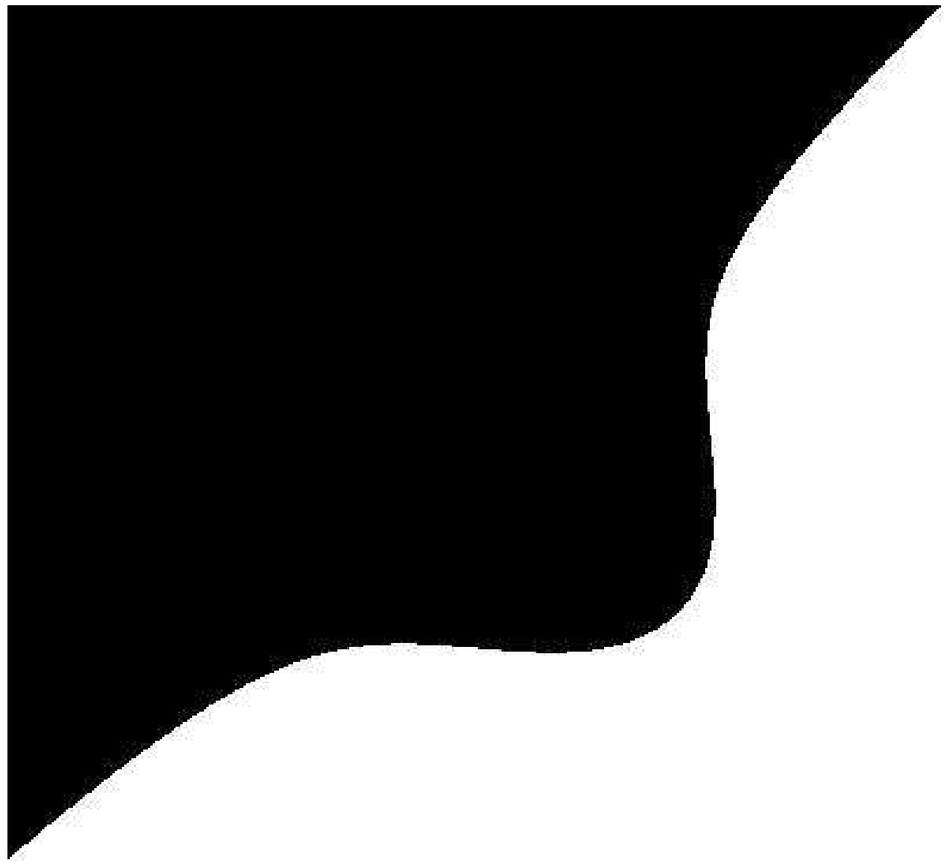
,"

els.

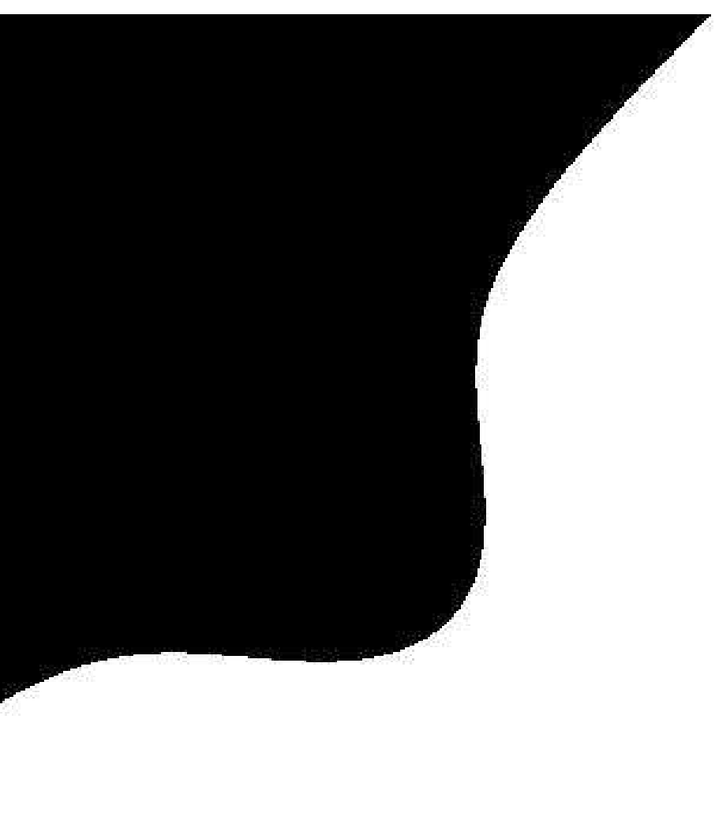
r–Dawson:



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



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



$$s^3 + 1 = 0.3xy$$

Jacobi

1986 C

$(S : C$
$(S/Z, C$
$s^2 + c^2$

$14\mathbf{M} +$
"Treme
of bein

$5\mathbf{M} + 3$
"Perha
efficien
which
coeffici

$3xy$

Jacobi intersectio

1986 Chudnovsky

$(S : C : D : Z)$ r
$(S/Z, C/Z, D/Z)$
$s^2 + c^2 = 1$, as^2

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$
"Tremendous adv
of being strongly

$5\mathbf{M} + 3\mathbf{S}$ for DB
"Perhaps (?) . . .
efficient duplicati
which do not dep
coefficients of an

Jacobi intersections

1986 Chudnovsky–Chudnov

$(S : C : D : Z)$ represent
$(S/Z, C/Z, D/Z)$ on
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
"Tremendous advantage"
of being strongly unified.

$5\mathbf{M} + 3\mathbf{S}$ for DBL.
"Perhaps (?) ... the most
efficient duplication formul
which do not depend on th
coefficients of an elliptic cu

Jacobi intersections

1986 Chudnovsky–Chudnovsky:

$(S : C : D : Z)$ represent
$(S/Z, C/Z, D/Z)$ on
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
"Tremendous advantage"
of being strongly unified.

$5\mathbf{M} + 3\mathbf{S}$ for DBL.
"Perhaps (?) ... the most
efficient duplication formulas
which do not depend on the
coefficients of an elliptic curve."

Jacobi intersections

1986 Chudnovsky–Chudnovsky:

$(S : C : D : Z)$ represent
$(S/Z, C/Z, D/Z)$ on
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
"Tremendous advantage"
of being strongly unified.

$5\mathbf{M} + 3\mathbf{S}$ for DBL.
"Perhaps (?) . . . the most
efficient duplication formulas
which do not depend on the
coefficients of an elliptic curve."

2001 L
$13\mathbf{M} +$
$4\mathbf{M} + 3$

2007 B
$3\mathbf{M} + 4$

2008.0
$13\mathbf{M} +$
$2\mathbf{M} + 5$
Also (S
$11\mathbf{M} +$
$2\mathbf{M} + 5$

Jacobi intersections

1986 Chudnovsky–Chudnovsky:

$(S : C : D : Z)$ represent
$(S/Z, C/Z, D/Z)$ on
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
"Tremendous advantage"
of being strongly unified.

$5\mathbf{M} + 3\mathbf{S}$ for DBL.
"Perhaps (?) ... the most
efficient duplication formulas
which do not depend on the
coefficients of an elliptic curve."

2001 Liardet–Sm
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$
$4\mathbf{M} + 3\mathbf{S}$ for DB

2007 Bernstein–L
$3\mathbf{M} + 4\mathbf{S}$ for DB

2008.02 Hisil–Wo
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ f
Also $(S : C : D :$
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ f

Jacobi intersections

1986 Chudnovsky–Chudnovsky:

$(S : C : D : Z)$ represent
$(S/Z, C/Z, D/Z)$ on
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
"Tremendous advantage"
of being strongly unified.

$5\mathbf{M} + 3\mathbf{S}$ for DBL.
"Perhaps (?) . . . the most
efficient duplication formulas
which do not depend on the
coefficients of an elliptic curve."

2001 Liardet–Smart:
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$4\mathbf{M} + 3\mathbf{S}$ for DBL.

2007 Bernstein–Lange:
$3\mathbf{M} + 4\mathbf{S}$ for DBL.

2008.02 Hisil–Wong–Carter
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.
Also $(S : C : D : Z : SC :$
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.

Jacobi intersections

1986 Chudnovsky–Chudnovsky:

$(S : C : D : Z)$ represent
$(S/Z, C/Z, D/Z)$ on
$s^2 + c^2 = 1$, $as^2 + d^2 = 1$.

$14\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
"Tremendous advantage"
of being strongly unified.

$5\mathbf{M} + 3\mathbf{S}$ for DBL.
"Perhaps (?) ... the most
efficient duplication formulas
which do not depend on the
coefficients of an elliptic curve."

2001 Liardet–Smart:
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$4\mathbf{M} + 3\mathbf{S}$ for DBL.

2007 Bernstein–Lange:
$3\mathbf{M} + 4\mathbf{S}$ for DBL.

2008.02 Hisil–Wong–Carter–Dawson:
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.
Also $(S : C : D : Z : SC : DZ)$:
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.

intersections

Chudnovsky–Chudnovsky:

$: D : Z)$ represent
$C/Z, D/Z)$ on
$^2 = 1$, $as^2 + d^2 = 1$.

$+ 2\mathbf{S} + 1\mathbf{D}$ for ADD.
endous advantage"
g strongly unified.

$3\mathbf{S}$ for DBL.
ps (?) . . . the most
t duplication formulas
do not depend on the
ents of an elliptic curve."

2001 Liardet–Smart:
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$4\mathbf{M} + 3\mathbf{S}$ for DBL.

2007 Bernstein–Lange:
$3\mathbf{M} + 4\mathbf{S}$ for DBL.

2008.02 Hisil–Wong–Carter–Dawson:
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.
Also $(S : C : D : Z : SC : DZ)$:
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.

Jacobi

$(X:Y:Z$
on $y^2 =$

1986 C
$3\mathbf{M} + 6$
Slow A

2002 B
New ch
$10\mathbf{M} +$
strongl

2007 B
$1\mathbf{M} + 9$

ons

y–Chudnovsky:

epresent
) on
$+ d^2 = 1$.

for ADD.
vantage"
unified.

L.
the most
ion formulas
pend on the
elliptic curve."

2001 Liardet–Smart:
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$4\mathbf{M} + 3\mathbf{S}$ for DBL.

2007 Bernstein–Lange:
$3\mathbf{M} + 4\mathbf{S}$ for DBL.

2008.02 Hisil–Wong–Carter–Dawson:
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.
Also $(S : C : D : Z : SC : DZ)$:
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.

Jacobi quartics

$(X:Y:Z)$ represen
on $y^2 = x^4 + 2a$

1986 Chudnovsky
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ f
Slow ADD.

2002 Billet–Joye:
New choice of ne
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$
strongly unified.

2007 Bernstein–L
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ f

vsky:

as
ne
urve."

2001 Liardet–Smart:
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$4\mathbf{M} + 3\mathbf{S}$ for DBL.

2007 Bernstein–Lange:
$3\mathbf{M} + 4\mathbf{S}$ for DBL.

2008.02 Hisil–Wong–Carter–Dawson:
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.
Also $(S : C : D : Z : SC : DZ)$:
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.

<u>Jacobi quartics</u>

$(X{:}Y{:}Z)$ represent $(X/Z, Y$
on $y^2 = x^4 + 2ax^2 + 1$.

1986 Chudnovsky–Chudnov
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.
Slow ADD.

2002 Billet–Joye:
New choice of neutral elem
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ for ADD,
strongly unified.

2007 Bernstein–Lange:
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ for DBL.

2001 Liardet–Smart:
$13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$4\mathbf{M} + 3\mathbf{S}$ for DBL.

2007 Bernstein–Lange:
$3\mathbf{M} + 4\mathbf{S}$ for DBL.

2008.02 Hisil–Wong–Carter–Dawson:
$13\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.
Also $(S : C : D : Z : SC : DZ)$:
$11\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for DBL.

Jacobi quartics

$(X:Y:Z)$ represent $(X/Z, Y/Z^2)$
on $y^2 = x^4 + 2ax^2 + 1$.

1986 Chudnovsky–Chudnovsky:
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.
Slow ADD.

2002 Billet–Joye:
New choice of neutral element.
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ for ADD,
strongly unified.

2007 Bernstein–Lange:
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ for DBL.

iardet–Smart:
$+ 2\mathbf{S} + 1\mathbf{D}$ for ADD.
$3\mathbf{S}$ for DBL.

Bernstein–Lange:
$4\mathbf{S}$ for DBL.

2 Hisil–Wong–Carter–Dawson:
$+ 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$5\mathbf{S} + 1\mathbf{D}$ for DBL.
$S : C : D : Z : SC : DZ$):
$+ 1\mathbf{S} + 2\mathbf{D}$ for ADD.
$5\mathbf{S} + 1\mathbf{D}$ for DBL.

Jacobi quartics

$(X{:}Y{:}Z)$ represent $(X/Z, Y/Z^2)$
on $y^2 = x^4 + 2ax^2 + 1$.

1986 Chudnovsky–Chudnovsky:
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.
Slow ADD.

2002 Billet–Joye:
New choice of neutral element.
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ for ADD,
strongly unified.

2007 Bernstein–Lange:
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ for DBL.

2007 H
$2\mathbf{M} + 6$

2007 F
$2\mathbf{M} + 6$
$1\mathbf{M} +$
on curv

More s
2007 H
2008.0
use $(X$
or $(X$:
Can co
Compe

art:
for ADD.
L.

Lange:
L.

ong–Carter–Dawson:
for ADD.
or DBL.
$Z : SC : DZ$):
for ADD.
or DBL.

Jacobi quartics

$(X{:}Y{:}Z)$ represent $(X/Z, Y/Z^2)$
on $y^2 = x^4 + 2ax^2 + 1$.

1986 Chudnovsky–Chudnovsky:
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.
Slow ADD.

2002 Billet–Joye:
New choice of neutral element.
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ for ADD,
strongly unified.

2007 Bernstein–Lange:
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ for DBL.

2007 Hisil–Carter
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ f

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ f
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ f
on curves chosen

More speedups:
2007 Hisil–Carter
2008.02 Hisil–Wo
use $(X : Y : Z : $
or $(X : Y : Z : X$
Can combine wit
Competitive with

r–Dawson:

DZ):

Jacobi quartics

$(X{:}Y{:}Z)$ represent $(X/Z, Y/Z^2)$
on $y^2 = x^4 + 2ax^2 + 1$.

1986 Chudnovsky–Chudnovsky:
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.
Slow ADD.

2002 Billet–Joye:
New choice of neutral element.
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ for ADD,
strongly unified.

2007 Bernstein–Lange:
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ for DBL.

2007 Hisil–Carter–Dawson:
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ for DBL
on curves chosen with $a^2 +$

More speedups: 2007 Duq
2007 Hisil–Carter–Dawson,
2008.02 Hisil–Wong–Carter
use $(X : Y : Z : X^2 : Z^2)$
or $(X : Y : Z : X^2 : Z^2 : 2$
Can combine with Feng–W
Competitive with Edwards!

Jacobi quartics

$(X{:}Y{:}Z)$ represent $(X/Z, Y/Z^2)$
on $y^2 = x^4 + 2ax^2 + 1$.

1986 Chudnovsky–Chudnovsky:
$3\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.
Slow ADD.

2002 Billet–Joye:
New choice of neutral element.
$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$ for ADD,
strongly unified.

2007 Bernstein–Lange:
$1\mathbf{M} + 9\mathbf{S} + 1\mathbf{D}$ for DBL.

2007 Hisil–Carter–Dawson:
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ for DBL
on curves chosen with $a^2 + c^2 = 1$.

More speedups: 2007 Duquesne,
2007 Hisil–Carter–Dawson,
2008.02 Hisil–Wong–Carter–Dawson:
use $(X : Y : Z : X^2 : Z^2)$
or $(X : Y : Z : X^2 : Z^2 : 2XZ)$.
Can combine with Feng–Wu.
Competitive with Edwards!

quartics

Z) represent $(X/Z, Y/Z^2)$
$= x^4 + 2ax^2 + 1$.

Chudnovsky–Chudnovsky:
$6\mathbf{S} + 2\mathbf{D}$ for DBL.
ADD.

Billet–Joye:
hoice of neutral element.
$+ 3\mathbf{S} + 1\mathbf{D}$ for ADD,
y unified.

Bernstein–Lange:
$9\mathbf{S} + 1\mathbf{D}$ for DBL.

2007 Hisil–Carter–Dawson:
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ for DBL
on curves chosen with $a^2 + c^2 = 1$.

More speedups: 2007 Duquesne,
2007 Hisil–Carter–Dawson,
2008.02 Hisil–Wong–Carter–Dawson:
use $(X : Y : Z : X^2 : Z^2)$
or $(X : Y : Z : X^2 : Z^2 : 2XZ)$.
Can combine with Feng–Wu.
Competitive with Edwards!

$x^2 = y$

nt $(X/Z, Y/Z^2)$
$x^2 + 1$.

y–Chudnovsky:
or DBL.

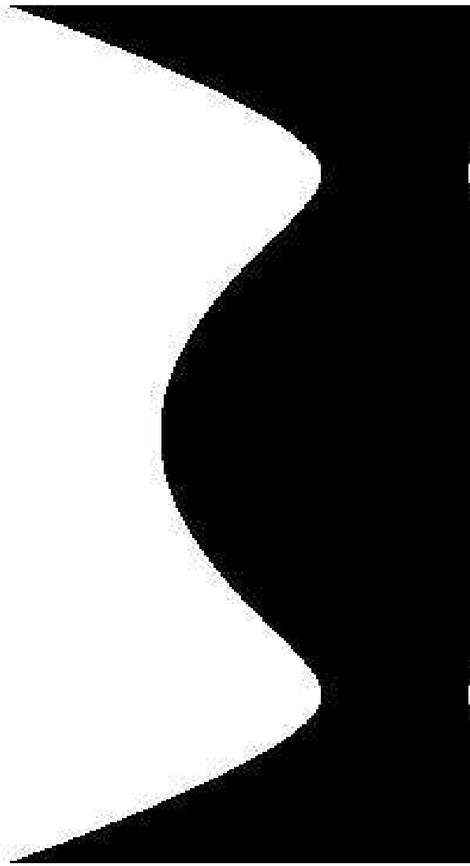
eutral element.
for ADD,

Lange:
or DBL.

2007 Hisil–Carter–Dawson:
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ for DBL
on curves chosen with $a^2 + c^2 = 1$.

More speedups: 2007 Duquesne,
2007 Hisil–Carter–Dawson,
2008.02 Hisil–Wong–Carter–Dawson:
use $(X : Y : Z : X^2 : Z^2)$
or $(X : Y : Z : X^2 : Z^2 : 2XZ)$.
Can combine with Feng–Wu.
Competitive with Edwards!



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

Y/Z^2)

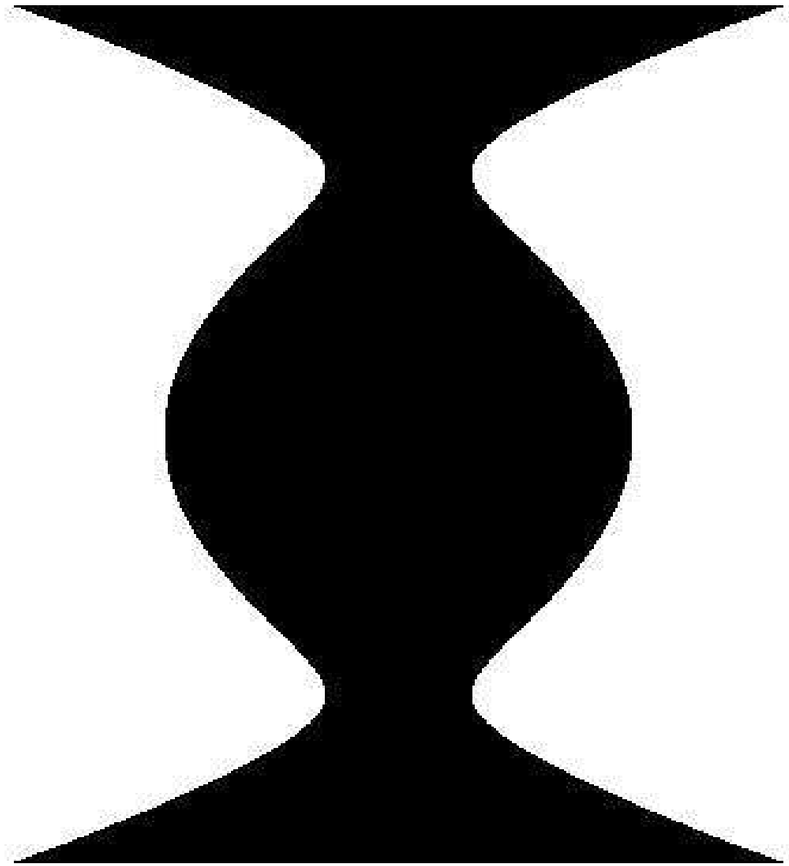
vsky:

nent.

2007 Hisil–Carter–Dawson:
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ for DBL
on curves chosen with $a^2 + c^2 = 1$.

More speedups: 2007 Duquesne,
2007 Hisil–Carter–Dawson,
2008.02 Hisil–Wong–Carter–Dawson:
use $(X : Y : Z : X^2 : Z^2)$
or $(X : Y : Z : X^2 : Z^2 : 2XZ)$.
Can combine with Feng–Wu.
Competitive with Edwards!

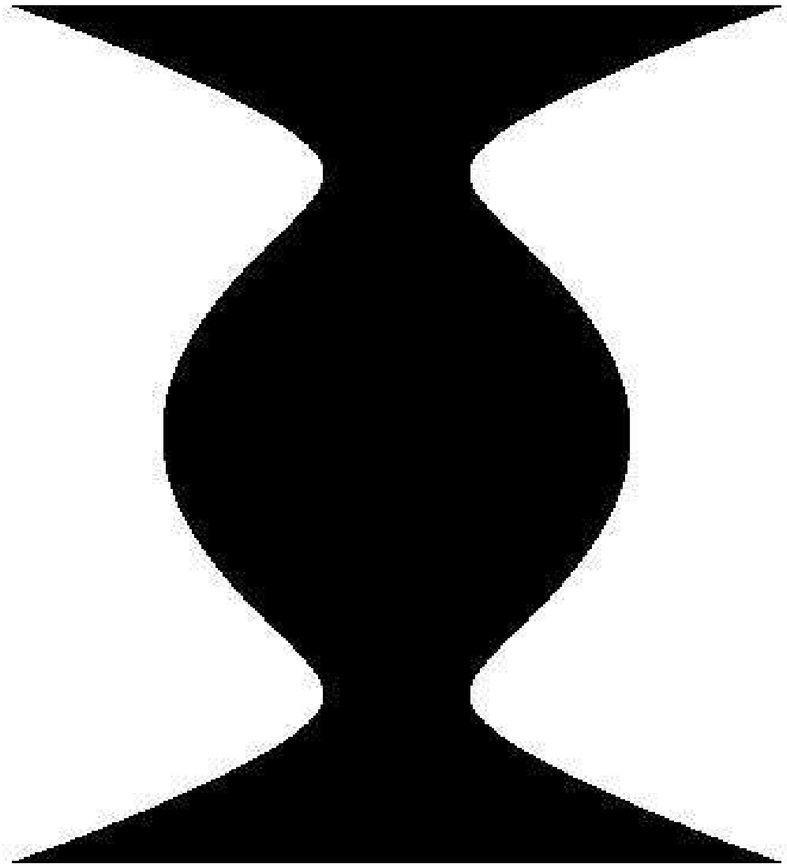


$x^2 = y^4 - 1.9y^2 + 1$

2007 Hisil–Carter–Dawson:
$2\mathbf{M} + 6\mathbf{S} + 2\mathbf{D}$ for DBL.

2007 Feng–Wu:
$2\mathbf{M} + 6\mathbf{S} + 1\mathbf{D}$ for DBL.
$1\mathbf{M} + 7\mathbf{S} + 3\mathbf{D}$ for DBL
on curves chosen with $a^2 + c^2 = 1$.

More speedups: 2007 Duquesne,
2007 Hisil–Carter–Dawson,
2008.02 Hisil–Wong–Carter–Dawson:
use $(X : Y : Z : X^2 : Z^2)$
or $(X : Y : Z : X^2 : Z^2 : 2XZ)$.
Can combine with Feng–Wu.
Competitive with Edwards!

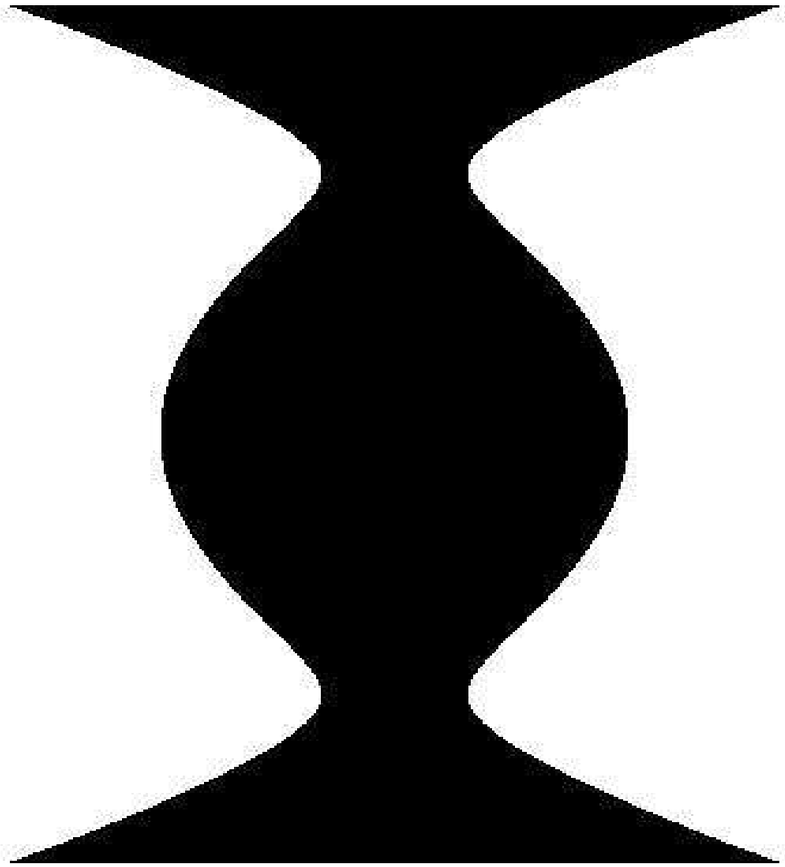


$x^2 = y^4 - 1.9y^2 + 1$

lisil–Carter–Dawson:
$6\mathbf{S} + 2\mathbf{D}$ for DBL.

eng–Wu:
$6\mathbf{S} + 1\mathbf{D}$ for DBL.
$7\mathbf{S} + 3\mathbf{D}$ for DBL
ves chosen with $a^2 + c^2 = 1$.

peedups: 2007 Duquesne,
lisil–Carter–Dawson,
2 Hisil–Wong–Carter–Dawson:
$: Y : Z : X^2 : Z^2)$
$Y : Z : X^2 : Z^2 : 2XZ)$.
mbine with Feng–Wu.
titive with Edwards!

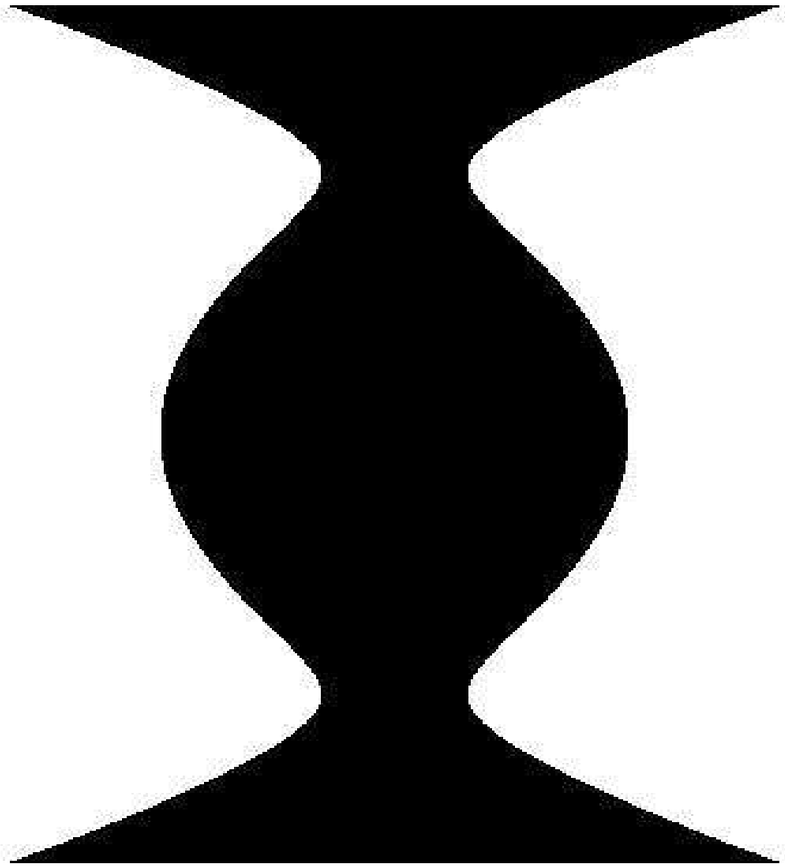


$x^2 = y^4 - 1.9y^2 + 1$

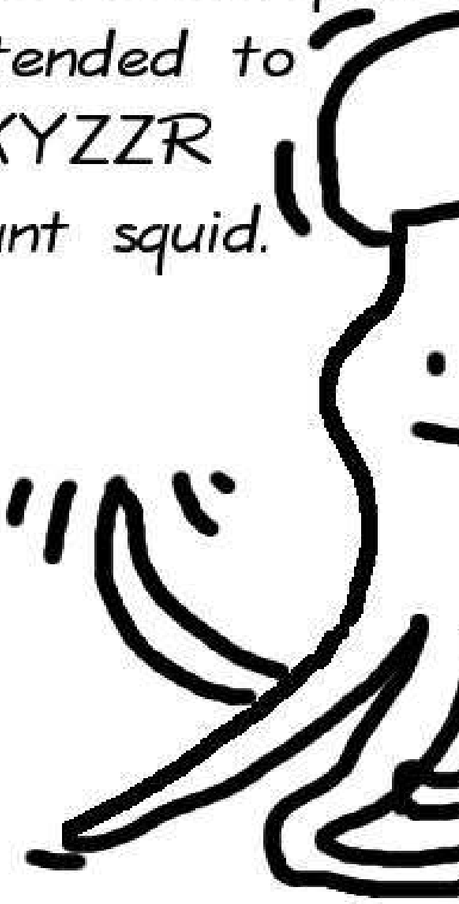
r–Dawson:
or DBL.

or DBL.
or DBL
with $a^2+c^2=1$.

2007 Duquesne,
r–Dawson,
ong–Carter–Dawson:
$X^2 : Z^2)$
$r^2 : Z^2 : 2XZ)$.
h Feng–Wu.
n Edwards!



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



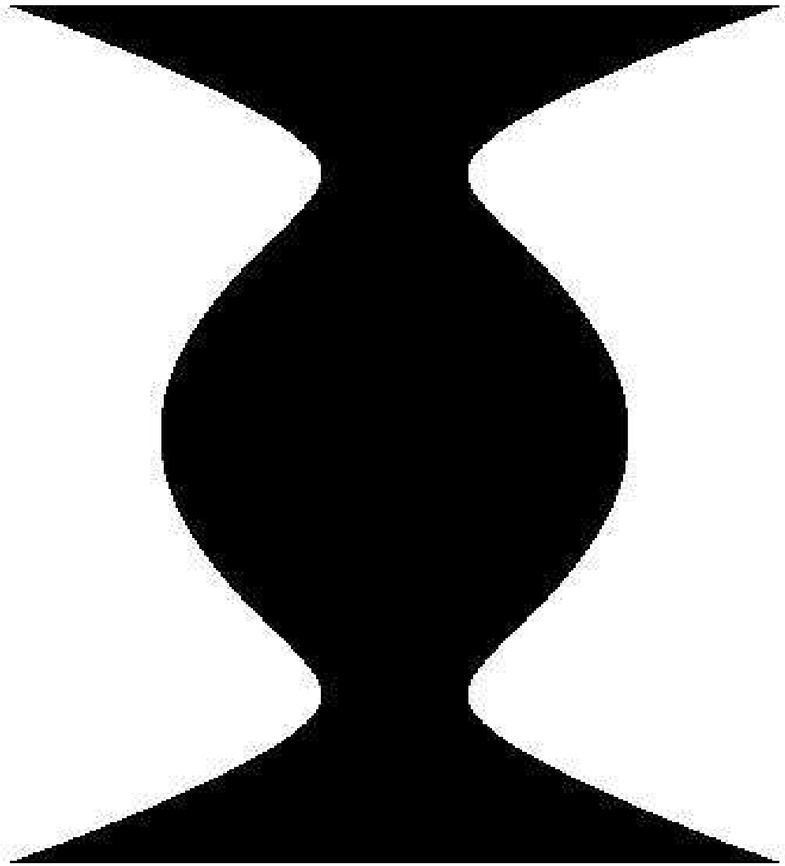
$-c^2 = 1.$

uesne,

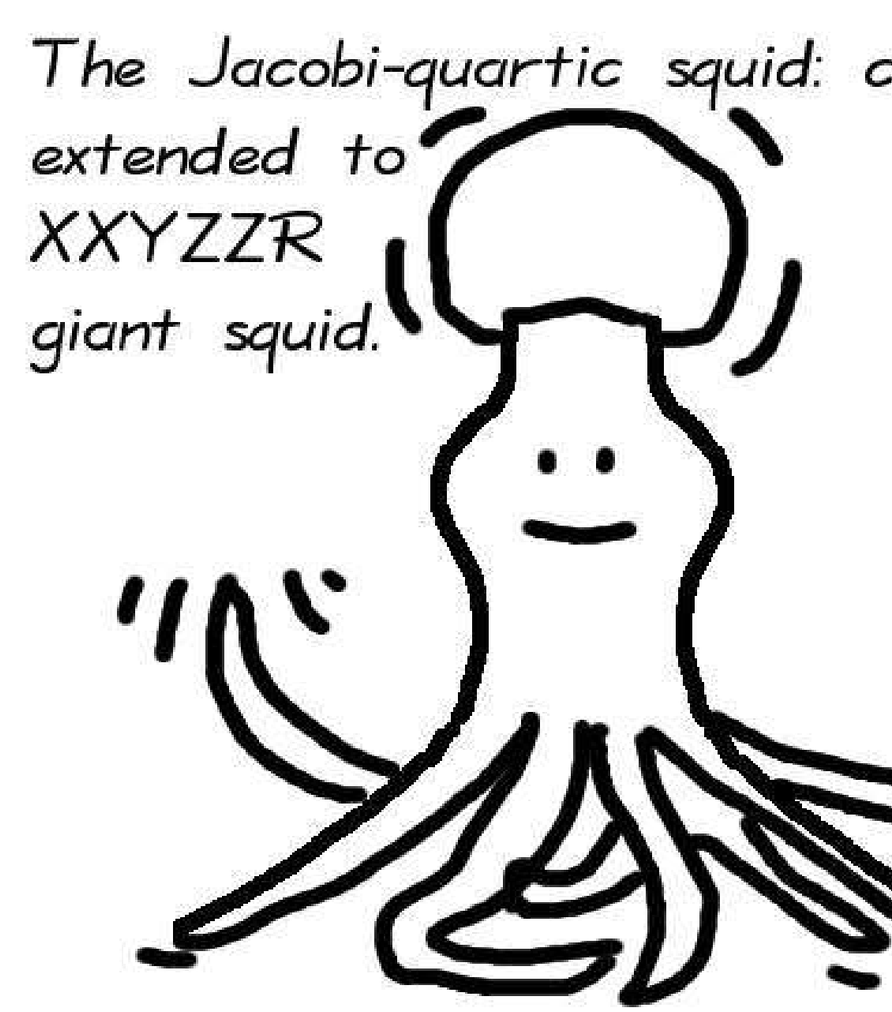
r–Dawson:

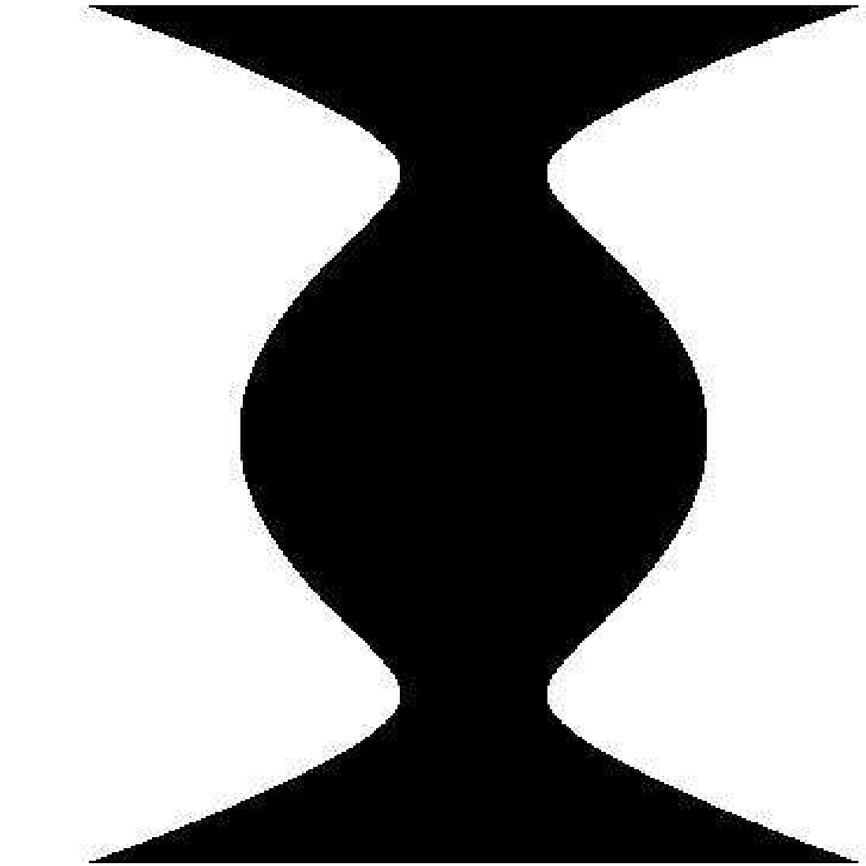
XZ).

/u.



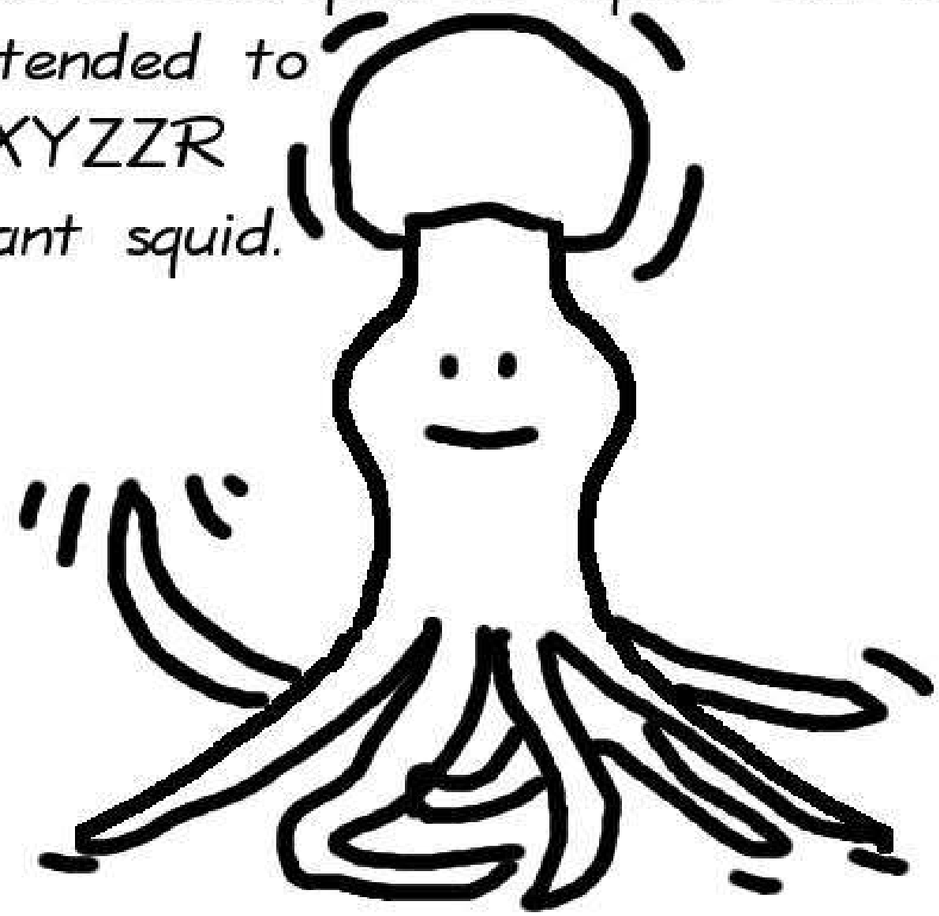
$x^2 = y^4 - 1.9y^2 + 1$

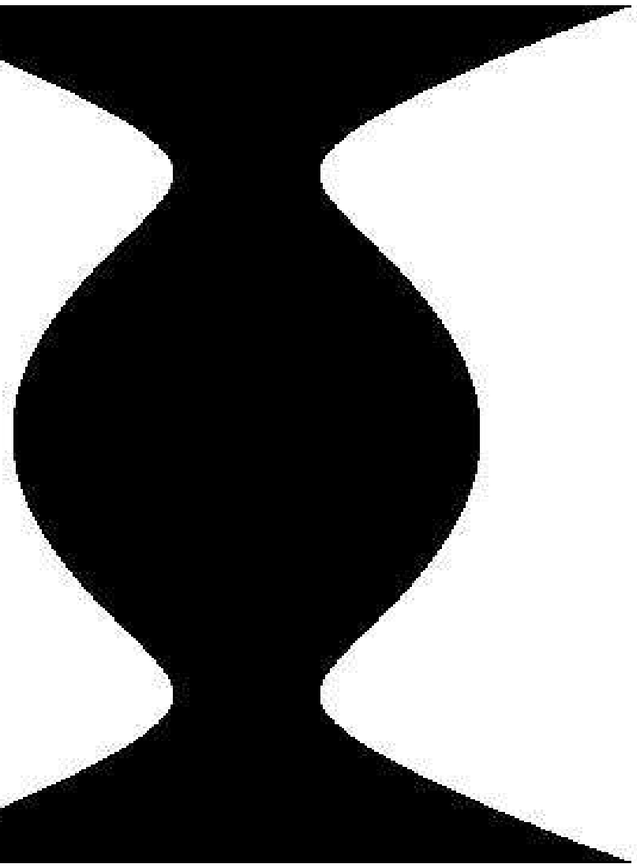




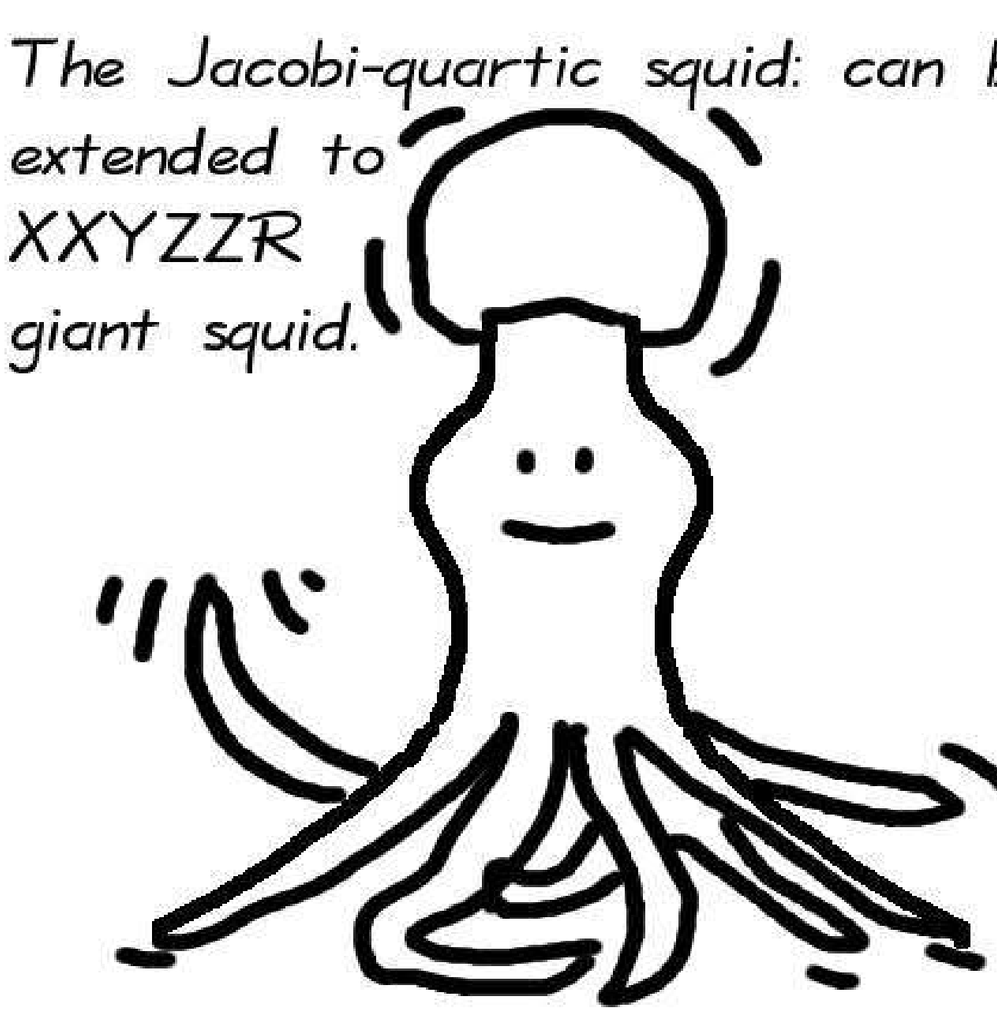
$$x^2 = y^4 - 1.9y^2 + 1$$

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



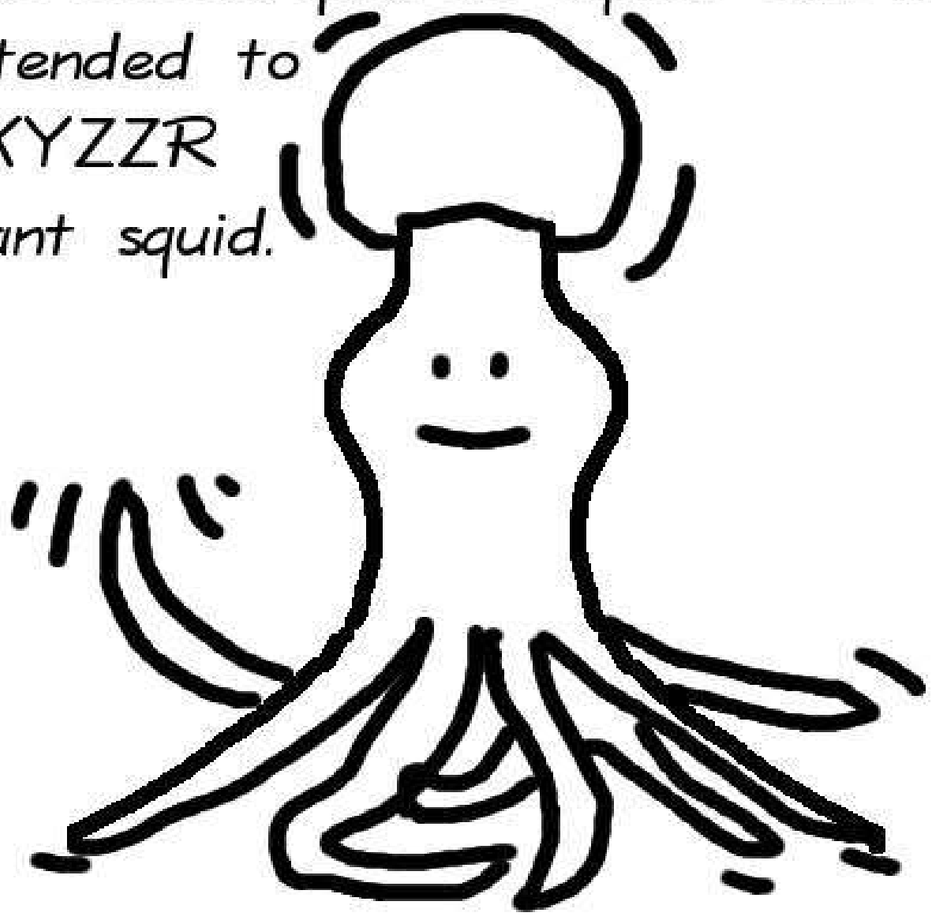


$^4 - 1.9y^2 + 1$

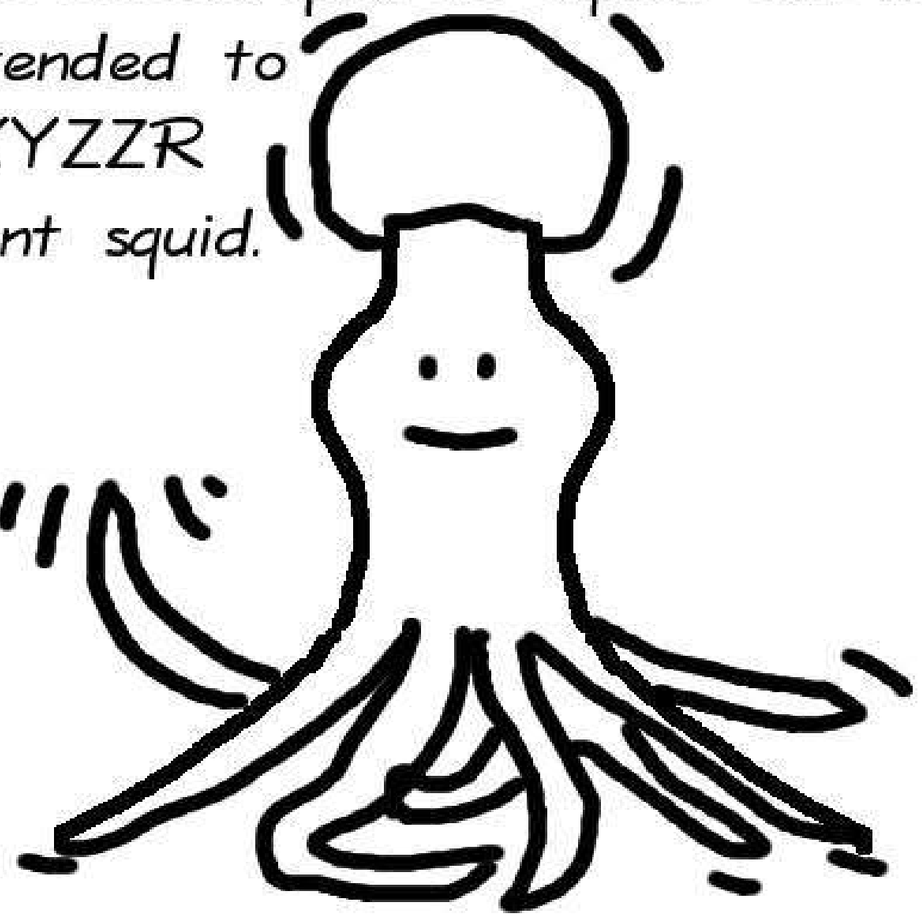

The Jacobi-quartic squid: can be extended to XXYZZR giant squid.

$+1$

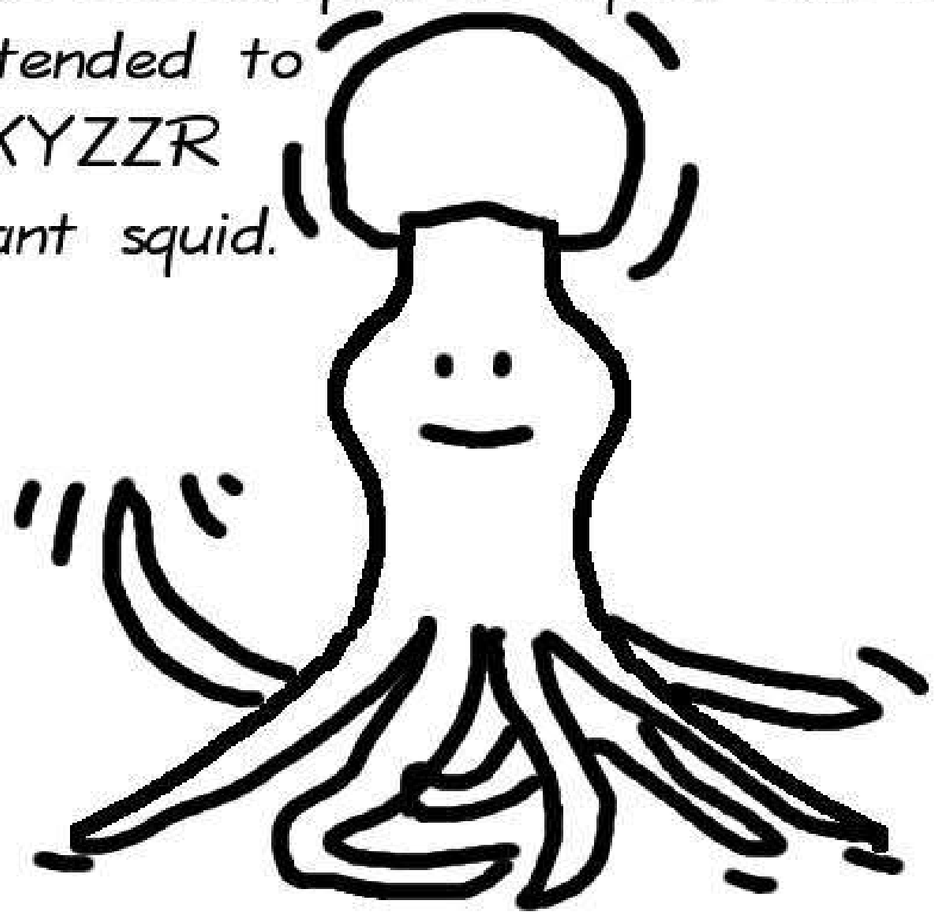
The Jacobi-quartic squid: can be extended to XXYZZR giant squid.



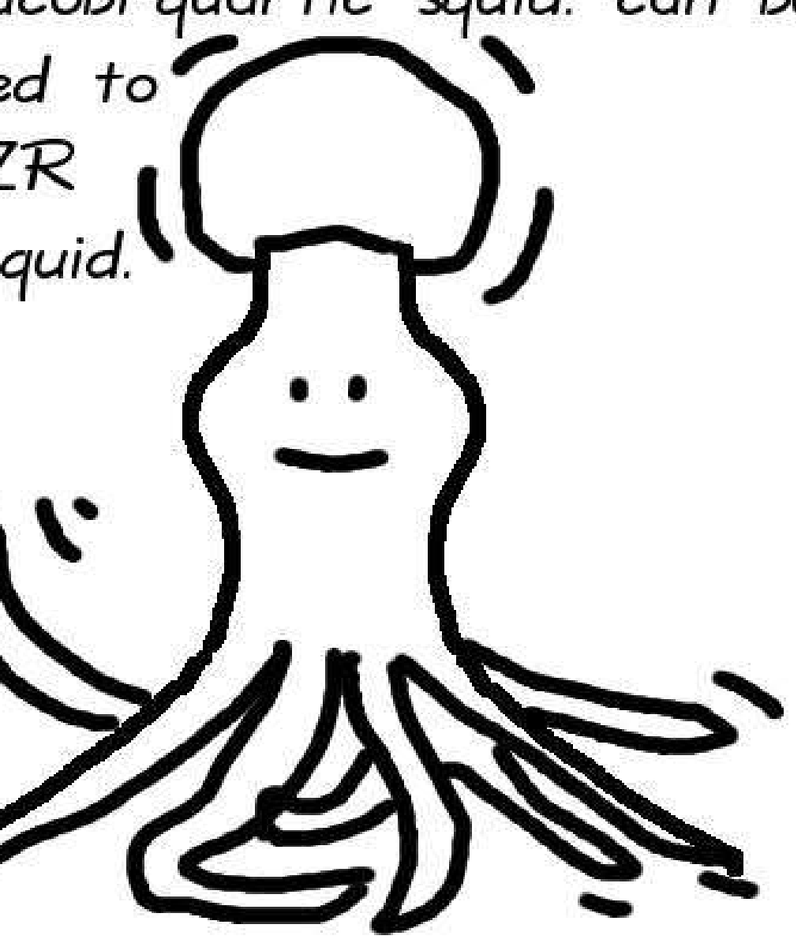
The Jacobi-quartic squid: can be extended to XXYZZR giant squid.



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



acobi-quartic squid: can be
ed to
ZR
quid.



ic squid: can be

1985

can be

1985


START


1985


START

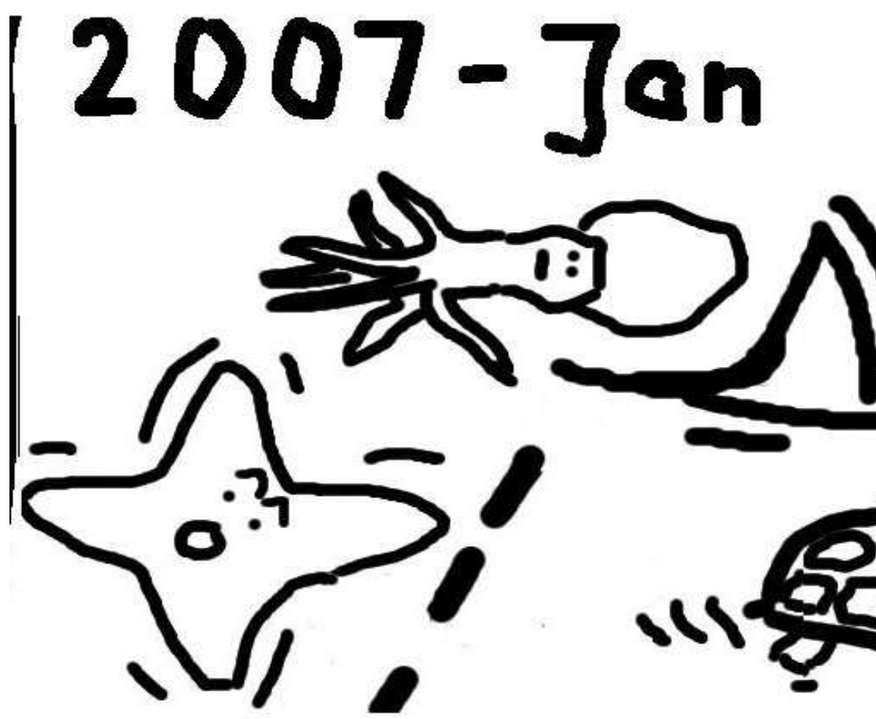

1985


20

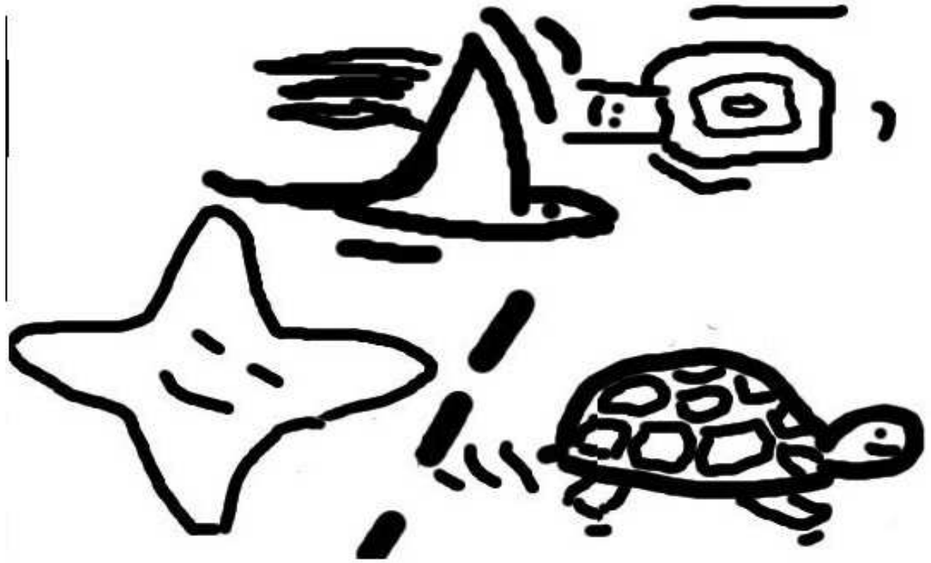
1985

2007-


1985


2007-Jan

1985



2007-Jan


85

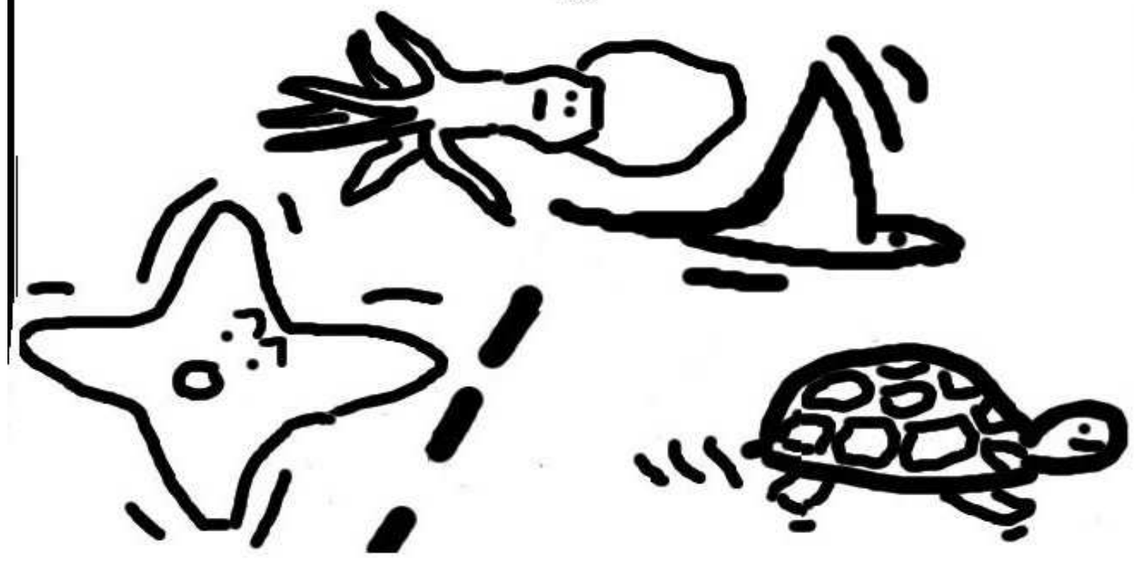

2007-Jan


Fe

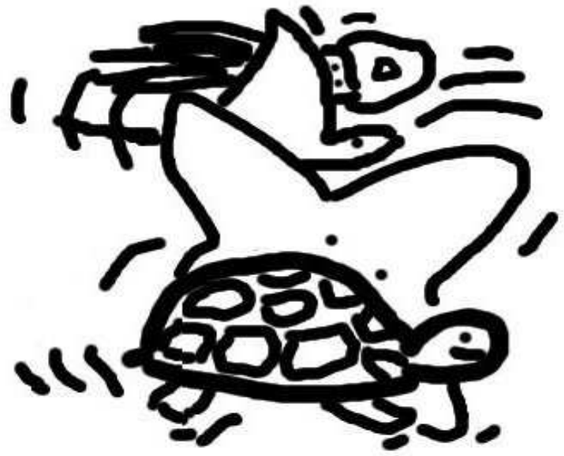

2007-Jan


Feb

2007-Jan

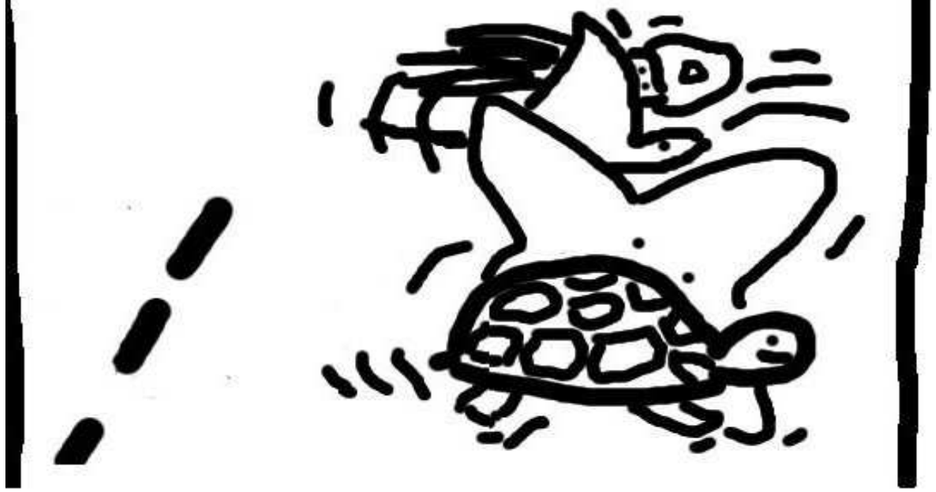


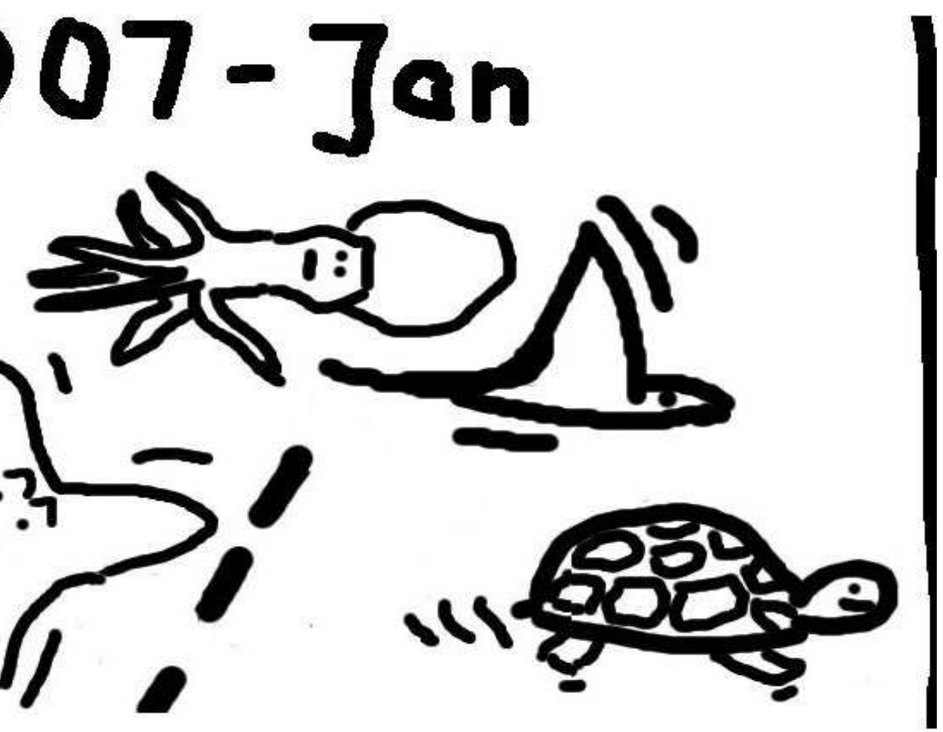
Feb



2007-Jan

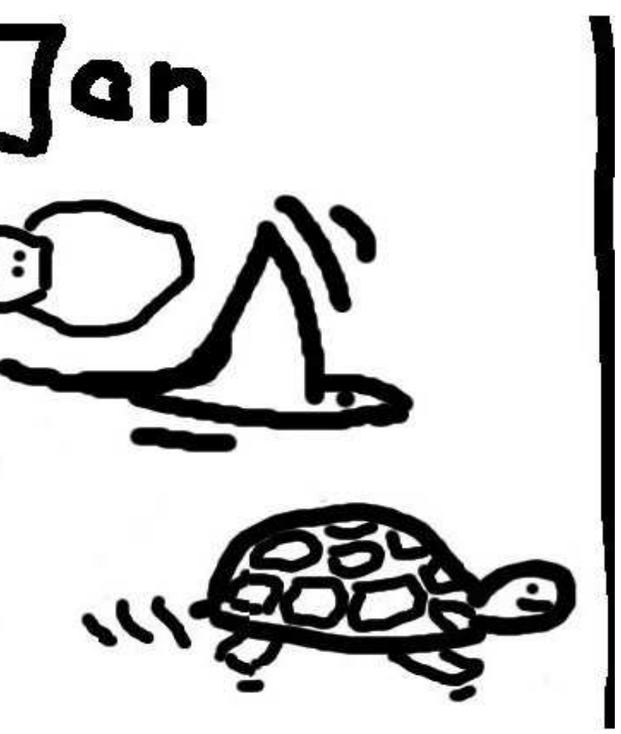
Feb




07-Jan


Feb


Ma


Jan

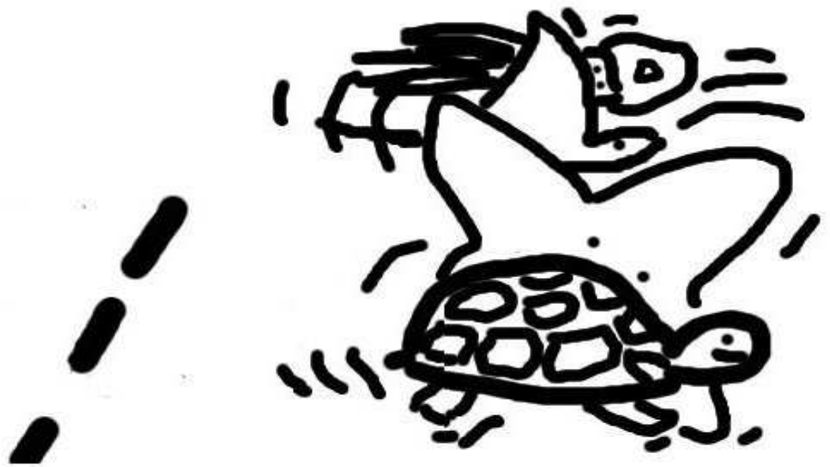

Feb


Mar

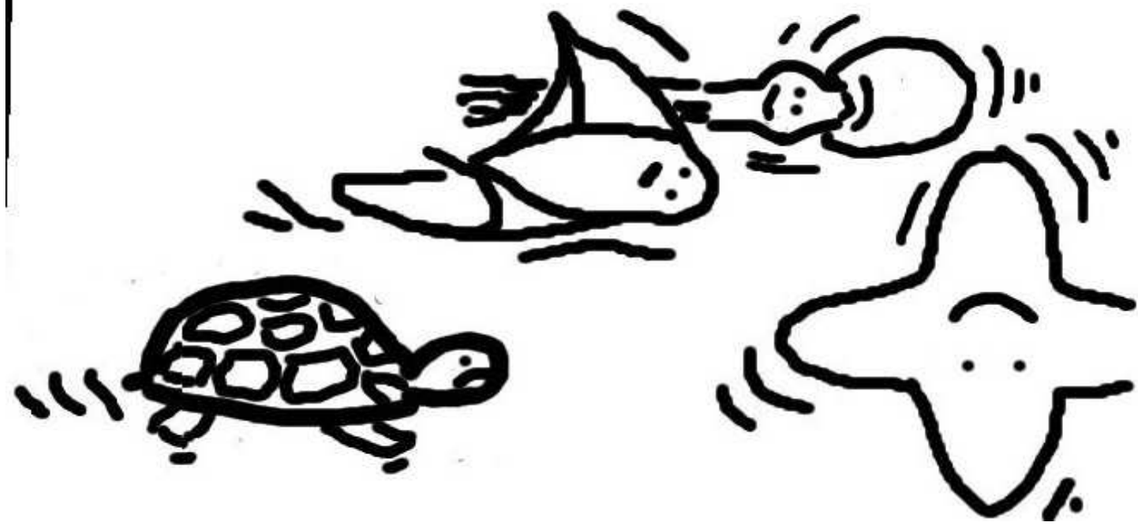

Feb

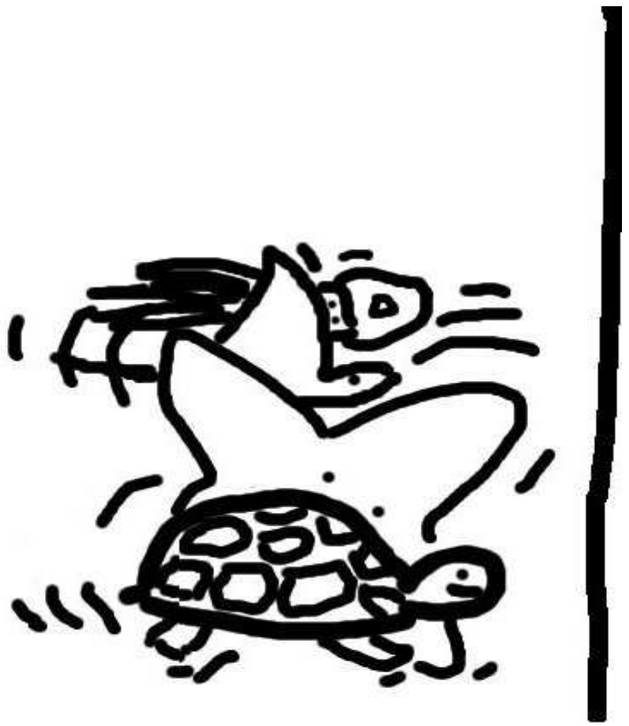

Mar

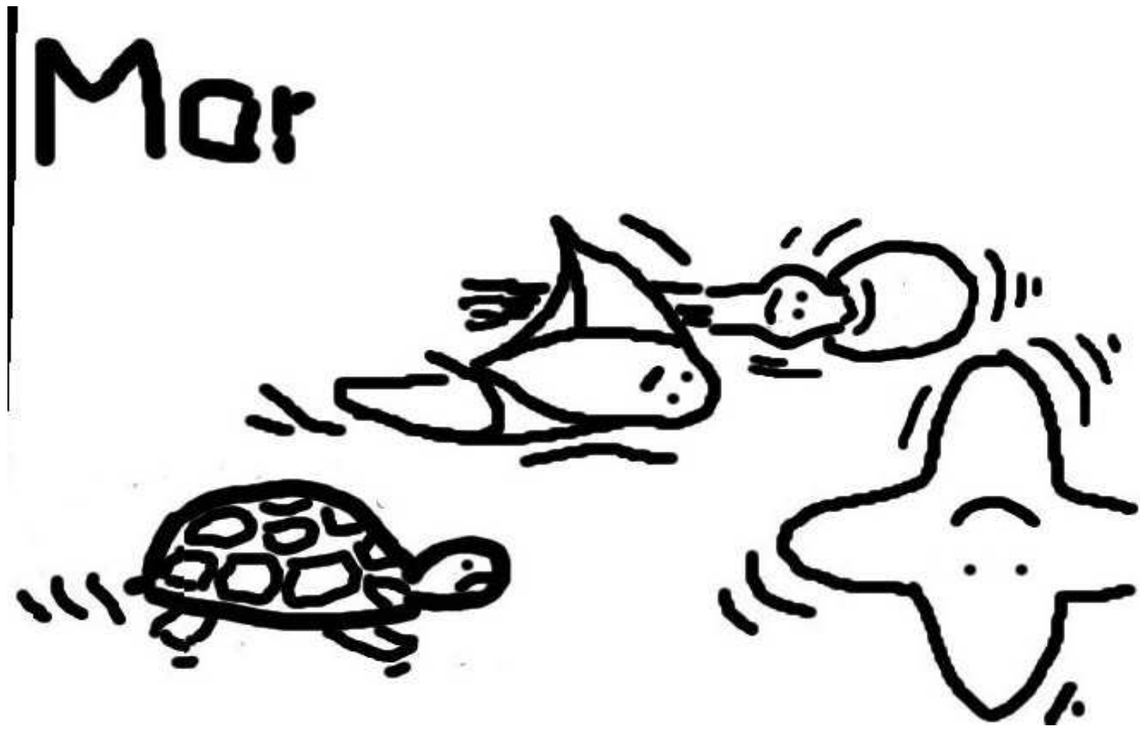
Feb



Mar





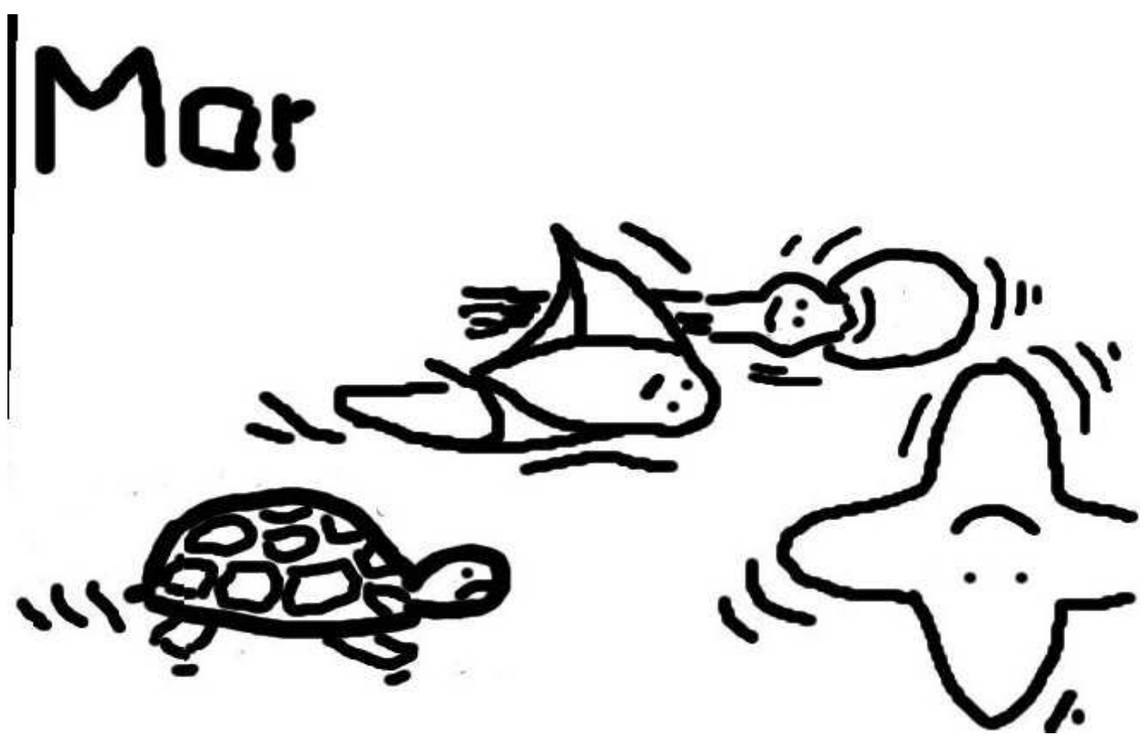


For mo

Explicit
joint w
hypere

EFD ha
formula
for AD
in 22 r
on 8 sh

Not ye
general
(e.g., H
comple
(e.g., c

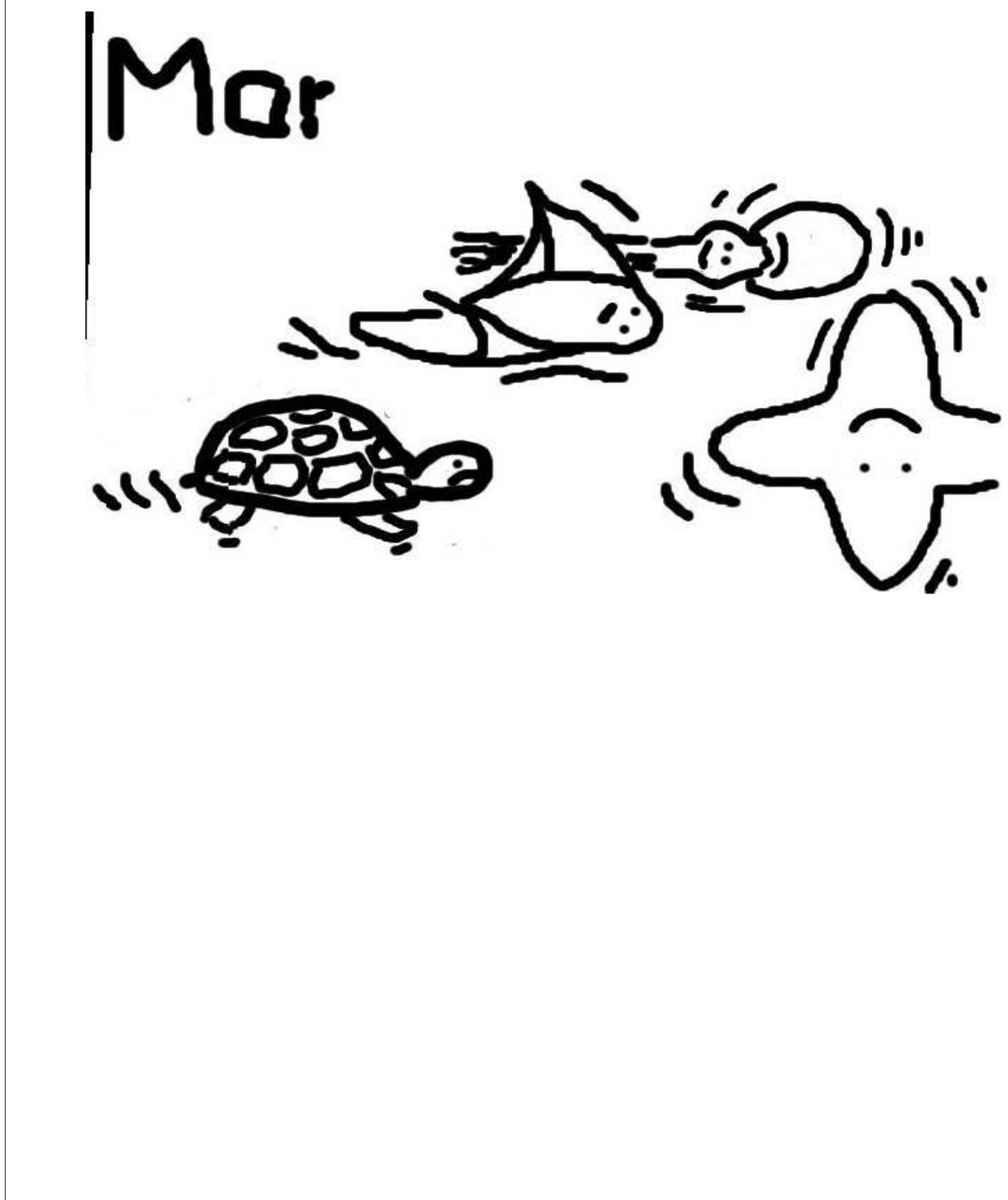


For more informa

Explicit-Formulas
joint work with T
`hyperelliptic`

EFD has 316 con
formulas and ope
for ADD, DBL, e
in 22 representat
on 8 shapes of el

Not yet handled
generality of curv
(e.g., Hessian or
complete additio
(e.g., checking fo

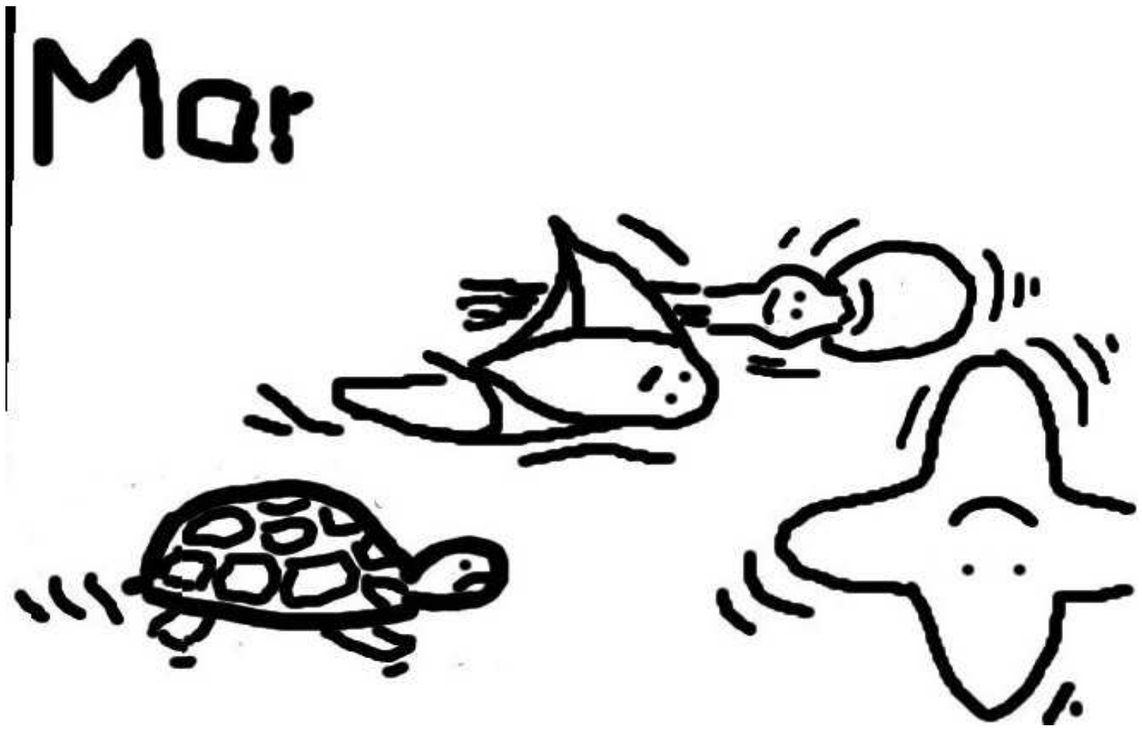


For more information

Explicit-Formulas Database
joint work with Tanja Lang
hyperelliptic.org/EFD

EFD has 316 computer-ver
formulas and operation cou
for ADD, DBL, etc.
in 22 representations
on 8 shapes of elliptic curv

Not yet handled by comput
generality of curve shapes
(e.g., Hessian order $\in 3\mathbf{Z}$);
complete addition algorithm
(e.g., checking for ∞).

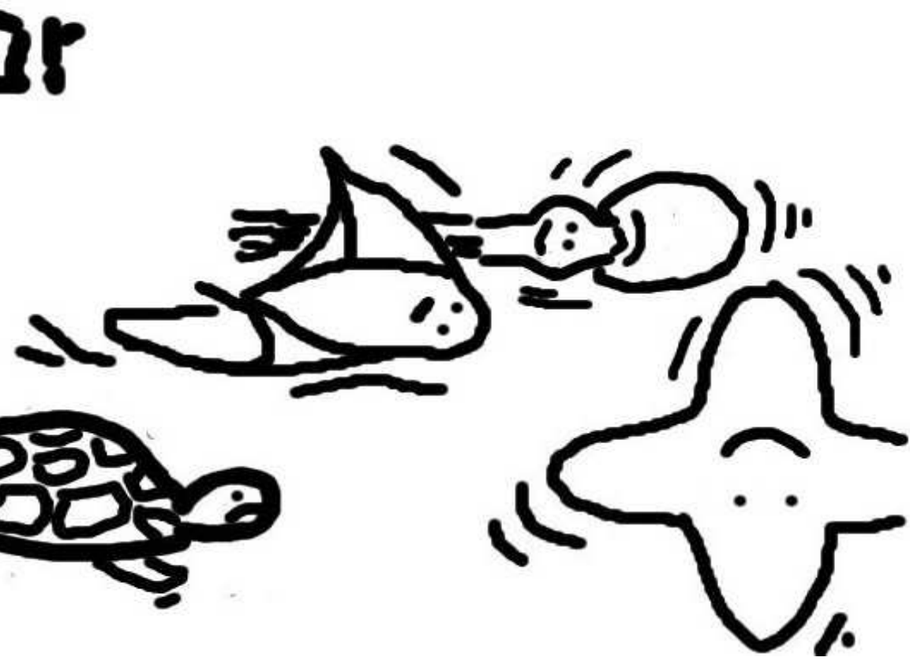


For more information

Explicit-Formulas Database,
joint work with Tanja Lange:
`hyperelliptic.org/EFD`

EFD has 316 computer-verified
formulas and operation counts
for ADD, DBL, etc.
in 22 representations
on 8 shapes of elliptic curves.

Not yet handled by computer:
generality of curve shapes
(e.g., Hessian order $\in 3\mathbf{Z}$);
complete addition algorithms
(e.g., checking for ∞).



For more information

Explicit-Formulas Database,
joint work with Tanja Lange:
hyperelliptic.org/EFD

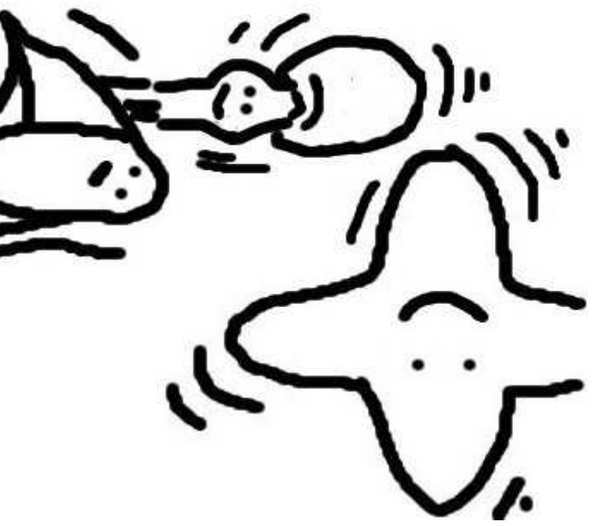
EFD has 316 computer-verified
formulas and operation counts
for ADD, DBL, etc.
in 22 representations
on 8 shapes of elliptic curves.

Not yet handled by computer:
generality of curve shapes
(e.g., Hessian order $\in 3\mathbf{Z}$);
complete addition algorithms
(e.g., checking for ∞).

Can do
for ellip
fields o

Latest
charact

Current
formula
for AD
in 16 r
on 2 sh
and sh
ordinar



For more information

Explicit-Formulas Database,
joint work with Tanja Lange:
`hyperelliptic.org/EFD`

EFD has 316 computer-verified
formulas and operation counts
for ADD, DBL, etc.
in 22 representations
on 8 shapes of elliptic curves.

Not yet handled by computer:
generality of curve shapes
(e.g., Hessian order $\in 3\mathbf{Z}$);
complete addition algorithms
(e.g., checking for ∞).

Can do similar su
for elliptic curves
fields of characte

Latest EFD upda
characteristic-2 f

Currently 102 co
formulas and ope
for ADD, DBL, e
in 16 representat
on 2 shapes (bin
and short Weiers
ordinary binary e

For more information

Explicit-Formulas Database,
joint work with Tanja Lange:
hyperelliptic.org/EFD

EFD has 316 computer-verified
formulas and operation counts
for ADD, DBL, etc.
in 22 representations
on 8 shapes of elliptic curves.

Not yet handled by computer:
generality of curve shapes
(e.g., Hessian order $\in 3\mathbf{Z}$);
complete addition algorithms
(e.g., checking for ∞).

Can do similar survey
for elliptic curves over
fields of characteristic 2.

Latest EFD updates now in
characteristic-2 formulas!

Currently 102 computer-ve
formulas and operation cou
for ADD, DBL, etc.
in 16 representations
on 2 shapes (binary Edwar
and short Weierstrass) of
ordinary binary elliptic curv

For more information

Explicit-Formulas Database,
joint work with Tanja Lange:
hyperelliptic.org/EFD

EFD has 316 computer-verified
formulas and operation counts
for ADD, DBL, etc.
in 22 representations
on 8 shapes of elliptic curves.

Not yet handled by computer:
generality of curve shapes
(e.g., Hessian order $\in 3\mathbf{Z}$);
complete addition algorithms
(e.g., checking for ∞).

Can do similar survey
for elliptic curves over
fields of characteristic 2.

Latest EFD updates now include
characteristic-2 formulas!

Currently 102 computer-verified
formulas and operation counts
for ADD, DBL, etc.
in 16 representations
on 2 shapes (binary Edwards
and short Weierstrass) of
ordinary binary elliptic curves.