Twisted Hessian curves

cr.yp.to/papers.html#hessian

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Joint work with:

Chitchanok Chuengsatiansup
Technische Universiteit Eindhoven

David Kohel
Aix-Marseille Université

Tanja Lange
Technische Universiteit Eindhoven

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 $P \mapsto 2P$.

Hessian curves

to/papers.html#hessian

. Bernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

rk with:

nok Chuengsatiansup
che Universiteit Eindhoven

ohel
seille Université

ange
che Universiteit Eindhoven

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 pre
models o
lying in
for other
coordina
increasin
4 basic r

Short W
$y^2 = x^3$

Jacobi in
$s^2 + c^2$

Jacobi q

Hessian:

urves

s.html#hessian

n

is at Chicago &

siteit Eindhoven

gsatiansup

siteit Eindhoven

ersité

siteit Eindhoven

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
models of elliptic
lying in low-dimen
for otherwise the
coordinates and op
increasing. This li
4 basic models of

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

Jacobi intersection
$s^2 + c^2 = 1,\ as^2$

Jacobi quartic: y^2

Hessian: $x^3 + y^3$

essian

ago &
hoven

o
hoven

hoven

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 spa
for otherwise the number of
coordinates and operations i
increasing. This limits us . .
4 basic models of elliptic cu

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

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

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

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

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

udnovsky–Chudnovsky,
ces of numbers
ed by addition
l groups
primality
orization tests":

ucial problem becomes
ce of the model
gebraic group variety,
omputations mod p
east time consuming."

portant computations:
$P, Q \mapsto P + Q$.
$P \mapsto 2P$.

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

"Our exp
expressio
on the c
(d) of ar
by far th

$X_3 = Y_1$
$Y_3 = X_1$
$Z_3 = Z_1$

12**M** for
where **M**
of multip

8.4**M** fo
assuming
of squar

-Chudnovsky,
mbers
tion

tests":

em becomes
model
oup variety,
ns mod p
consuming."

omputations:
$+ Q$.

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

"Our experience s
expression of the l
on the cubic Hessi
(d) of an elliptic c
by far the best and

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

12**M** for ADD,
where **M** is the co
of multiplication in

8.4**M** for DBL,
assuming 0.8**M** fo
of squaring in the

sky,

nes

,

g.”

ns:

“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: $x^3 + y^3 + 1 = 3dxy$.

“Our experience shows that
expression of the law of add
on the cubic Hessian form
(d) of an elliptic curve is
by far the best and the prett

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

12**M** for ADD, where **M** is the cost of multiplication in the field

8.4**M** for DBL, assuming 0.8**M** for the cost of squaring in the field.

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

"Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest."

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

12**M** for ADD, where **M** is the cost of multiplication in the field.

8.4**M** for DBL, assuming 0.8**M** for the cost of squaring in the field.

eferable to use
of elliptic curves
low-dimensional spaces,
rwise the number of
ntes and operations is
ng. This limits us . . . to
models of elliptic curves."

eierstrass:

$+ ax + b$.

ntersection:

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

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

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

"Our experience shows that the
expression of the law of addition
on the cubic Hessian form
(d) of an elliptic curve is
by far the best and the prettiest."

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

12**M** for ADD,
where **M** is the cost
of multiplication in the field.

8.4**M** for DBL,
assuming 0.8**M** for the cost
of squaring in the field.

1990s: E
use shor
in Jacob
for "the

15.2**M** f
much sl

Why is t

use
curves
sional spaces,
number of
perations is
mits us . . . to
elliptic curves.”

n:
$- d^2 = 1.$

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

$+ 1 = 3dxy.$

“Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest.”

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

12**M** for ADD,
where **M** is the cost
of multiplication in the field.

8.4**M** for DBL,
assuming 0.8**M** for the cost
of squaring in the field.

1990s: ECC stand
use short Weierstr
in Jacobian coordi
for “the fastest ari

15.2**M** for ADD,
much slower than

Why is this a good

ces,

s

. to

rves.”

x^2+1.

y.

“Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest.”

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

12**M** for ADD, where **M** is the cost of multiplication in the field.

8.4**M** for DBL, assuming 0.8**M** for the cost of squaring in the field.

1990s: ECC standards instea use short Weierstrass curves in Jacobian coordinates for “the fastest arithmetic”.

15.2**M** for ADD, much slower than Hessian.

Why is this a good idea?

"Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest."

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

12**M** for ADD,
where **M** is the cost
of multiplication in the field.

8.4**M** for DBL,
assuming 0.8**M** for the cost
of squaring in the field.

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for "the fastest arithmetic".

15.2**M** for ADD,
much slower than Hessian.

Why is this a good idea?

"Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest."

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

12**M** for ADD, where **M** is the cost of multiplication in the field.

8.4**M** for DBL, assuming 0.8**M** for the cost of squaring in the field.

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for "the fastest arithmetic".

15.2**M** for ADD, much slower than Hessian.

Why is this a good idea?
Answer: Only 7.2**M** for DBL with Chudnovsky–Chudnovsky formula.

"Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest."

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

12**M** for ADD,
where **M** is the cost
of multiplication in the field.

8.4**M** for DBL,
assuming 0.8**M** for the cost
of squaring in the field.

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for "the fastest arithmetic".

15.2**M** for ADD,
much slower than Hessian.

Why is this a good idea?
Answer: Only 7.2**M** for DBL with Chudnovsky–Chudnovsky formula.

2001 Bernstein: 15**M**, 7**M**.

"Our experience shows that the expression of the law of addition on the cubic Hessian form (d) of an elliptic curve is by far the best and the prettiest."

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

12**M** for ADD, where **M** is the cost of multiplication in the field.

8.4**M** for DBL, assuming 0.8**M** for the cost of squaring in the field.

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for "the fastest arithmetic".

15.2**M** for ADD, much slower than Hessian.

Why is this a good idea? Answer: Only 7.2**M** for DBL with Chudnovsky–Chudnovsky formula.

2001 Bernstein: 15**M**, 7**M**.

Compared to Hessian, Weierstrass saves 4**M** in typical DBL-DBL-DBL-DBL-DBL-ADD.

perience shows that the
on of the law of addition
ubic Hessian form
n elliptic curve is
he best and the prettiest."

$_1X_2 \cdot Y_1Z_2 - Z_1Y_2 \cdot X_1Y_2$,
$_1Z_2 \cdot X_1Y_2 - Y_1X_2 \cdot Z_1X_2$,
$_1Y_2 \cdot Z_1X_2 - X_1Z_2 \cdot Y_1Z_2$.

ADD,
M is the cost
plication in the field.

r DBL,
g 0.8**M** for the cost
ing in the field.

1990s: ECC standards instead
use short Weierstrass curves
in Jacobian coordinates
for "the fastest arithmetic".

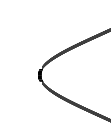
15.2**M** for ADD,
much slower than Hessian.

Why is this a good idea?
Answer: Only 7.2**M** for DBL with
Chudnovsky–Chudnovsky formula.

2001 Bernstein: 15**M**, 7**M**.

Compared to Hessian,
Weierstrass saves 4**M** in typical
DBL-DBL-DBL-DBL-DBL-ADD.

2007 Ed
2007 Be
analyze



Example
Sum of
$((x_1y_2+$
$(y_1y_2-$

hows that the
aw of addition
an form
urve is
d the prettiest."

$_2 - Z_1Y_2 \cdot X_1Y_2,$
$_2 - Y_1X_2 \cdot Z_1X_2,$
$_2 - X_1Z_2 \cdot Y_1Z_2.$

st
n the field.

r the cost
field.

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for "the fastest arithmetic".

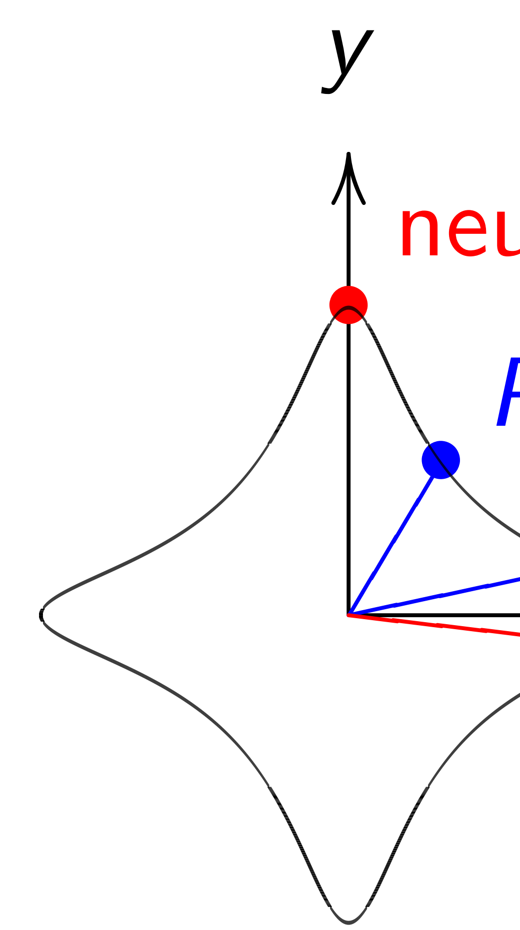
15.2**M** for ADD, much slower than Hessian.

Why is this a good idea?
Answer: Only 7.2**M** for DBL with Chudnovsky–Chudnovsky formula.

2001 Bernstein: 15**M**, 7**M**.

Compared to Hessian, Weierstrass saves 4**M** in typical DBL-DBL-DBL-DBL-DBL-ADD.

2007 Edwards: ne
2007 Bernstein–La
analyze speed, cor



Example: $x^2 + y^2$
Sum of (x_1, y_1) ar
$((x_1y_2+y_1x_2)/(1-$
$(y_1y_2-x_1x_2)/(1-$

the

ition

tiest.”

$X_1 Y_2$,

$Z_1 X_2$,

$Y_1 Z_2$.

.

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for “the fastest arithmetic”.

15.2**M** for ADD, much slower than Hessian.

Why is this a good idea?
Answer: Only 7.2**M** for DBL with Chudnovsky–Chudnovsky formula.

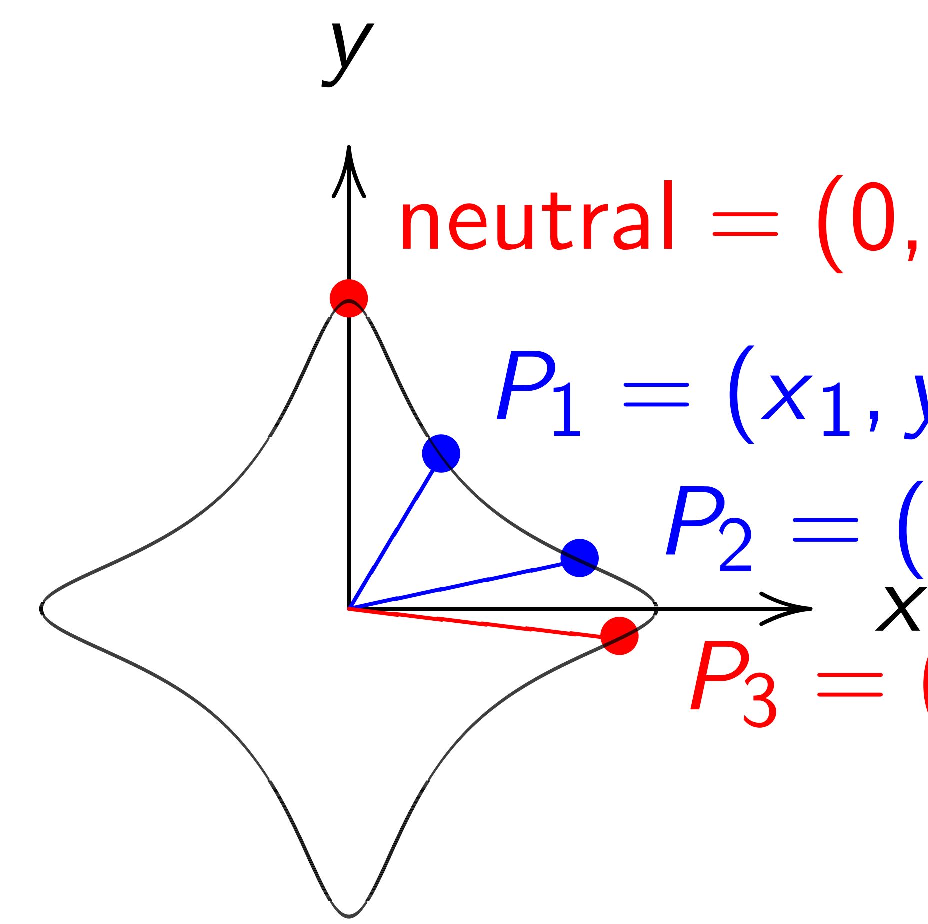
2001 Bernstein: 15**M**, 7**M**.

Compared to Hessian, Weierstrass saves 4**M** in typical DBL-DBL-DBL-DBL-DBL-ADD.

2007 Edwards: new curve sh

2007 Bernstein–Lange: gene

analyze speed, completeness



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

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

$((x_1 y_2 + y_1 x_2)/(1 - 30 x_1 x_2 y$

$(y_1 y_2 - x_1 x_2)/(1 + 30 x_1 x_2 y$

1990s: ECC standards instead use short Weierstrass curves in Jacobian coordinates for “the fastest arithmetic”.

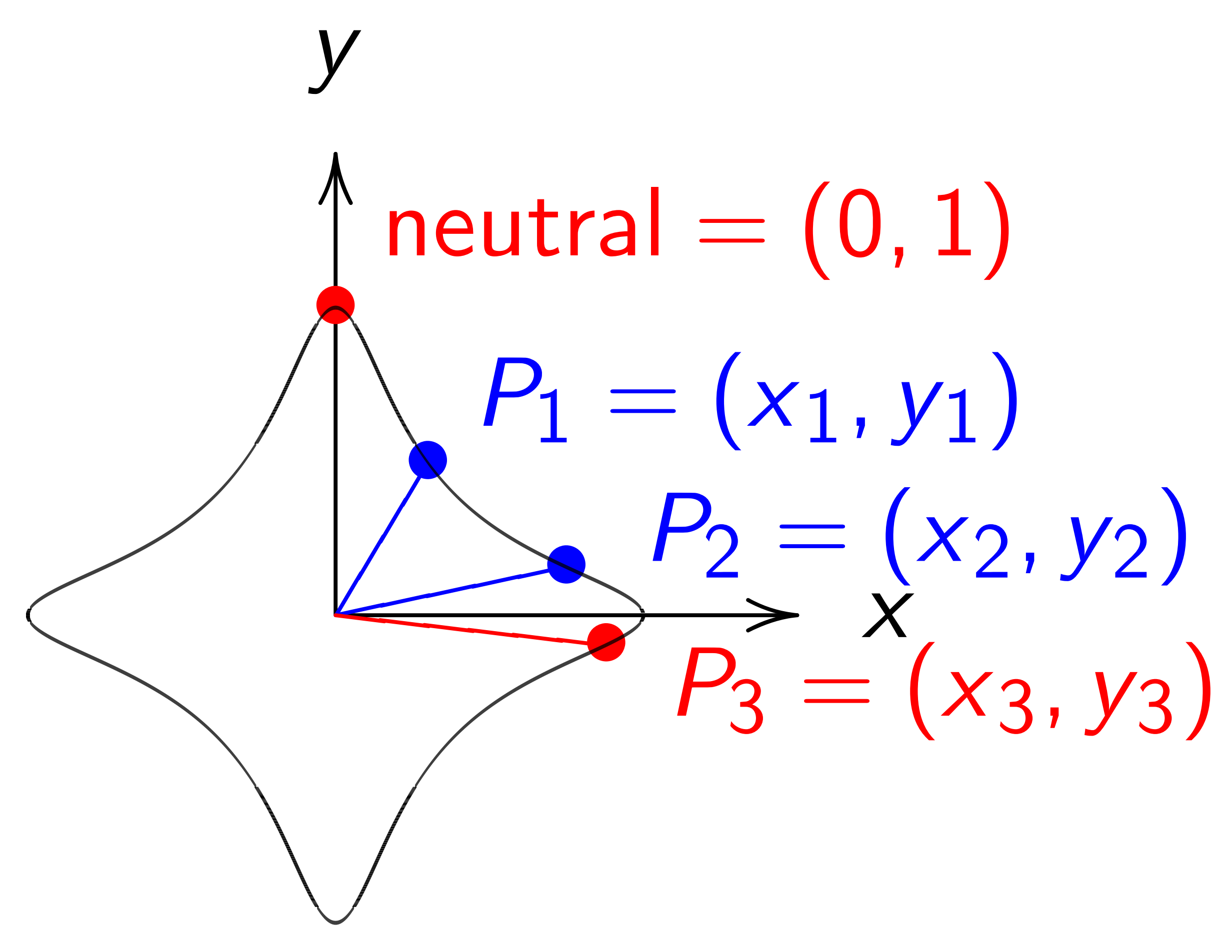
15.2**M** for ADD, much slower than Hessian.

Why is this a good idea?
Answer: Only 7.2**M** for DBL with Chudnovsky–Chudnovsky formula.

2001 Bernstein: 15**M**, 7**M**.

Compared to Hessian, Weierstrass saves 4**M** in typical DBL-DBL-DBL-DBL-DBL-ADD.

2007 Edwards: new curve shape.
2007 Bernstein–Lange: generalize, analyze speed, completeness.



Example: $x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

ECC standards instead
t Weierstrass curves
pian coordinates
fastest arithmetic".

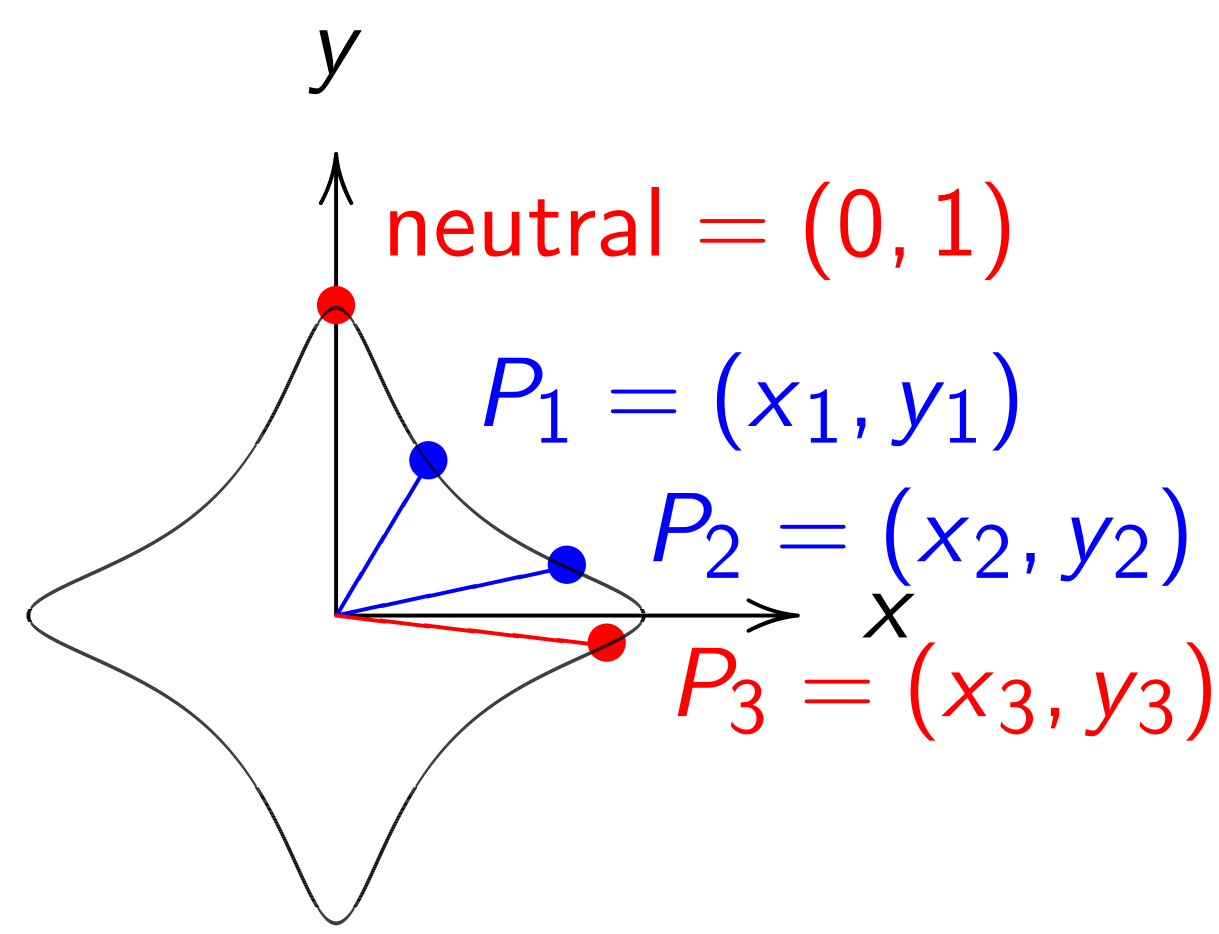
for ADD,
ower than Hessian.

this a good idea?
Only 7.2**M** for DBL with
vsky–Chudnovsky formula.

rnstein: 15**M**, 7**M**.

ed to Hessian,
rass saves 4**M** in typical
BL-DBL-DBL-DBL-ADD.

2007 Edwards: new curve shape.
2007 Bernstein–Lange: generalize,
analyze speed, completeness.



Example: $x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2{+}y_1x_2)/(1{-}30x_1x_2y_1y_2),$
$(y_1y_2{-}x_1x_2)/(1{+}30x_1x_2y_1y_2))$.

2007 Be
10.8**M** f

ards instead
ass curves
nates
ithmetic”.

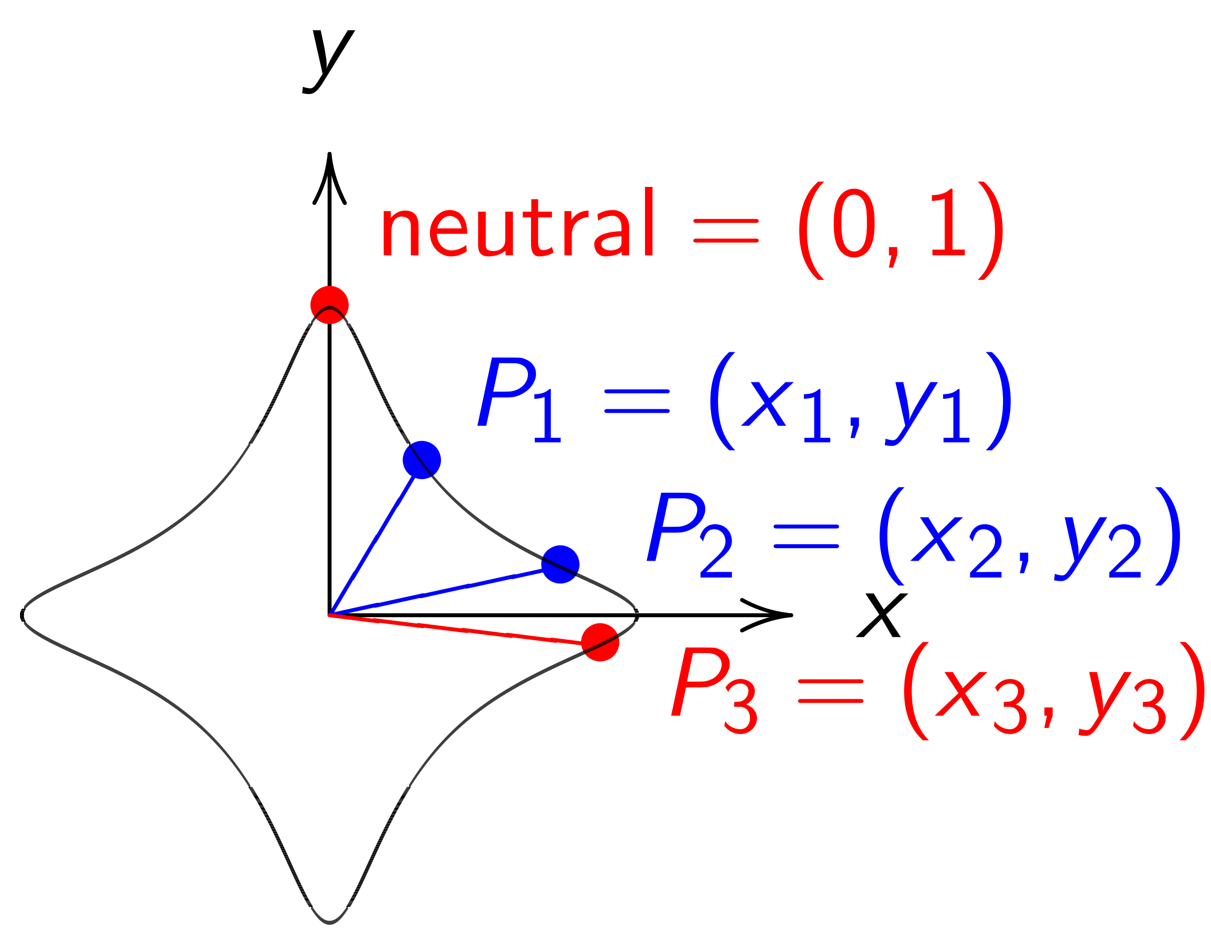
Hessian.

d idea?
M for DBL with
lnovsky formula.

5**M**, 7**M**.

sian,
4**M** in typical
BL-DBL-ADD.

2007 Edwards: new curve shape.
2007 Bernstein–Lange: generalize, analyze speed, completeness.



Example: $x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

2007 Bernstein–La
10.8**M** for ADD, 6

ad

L with

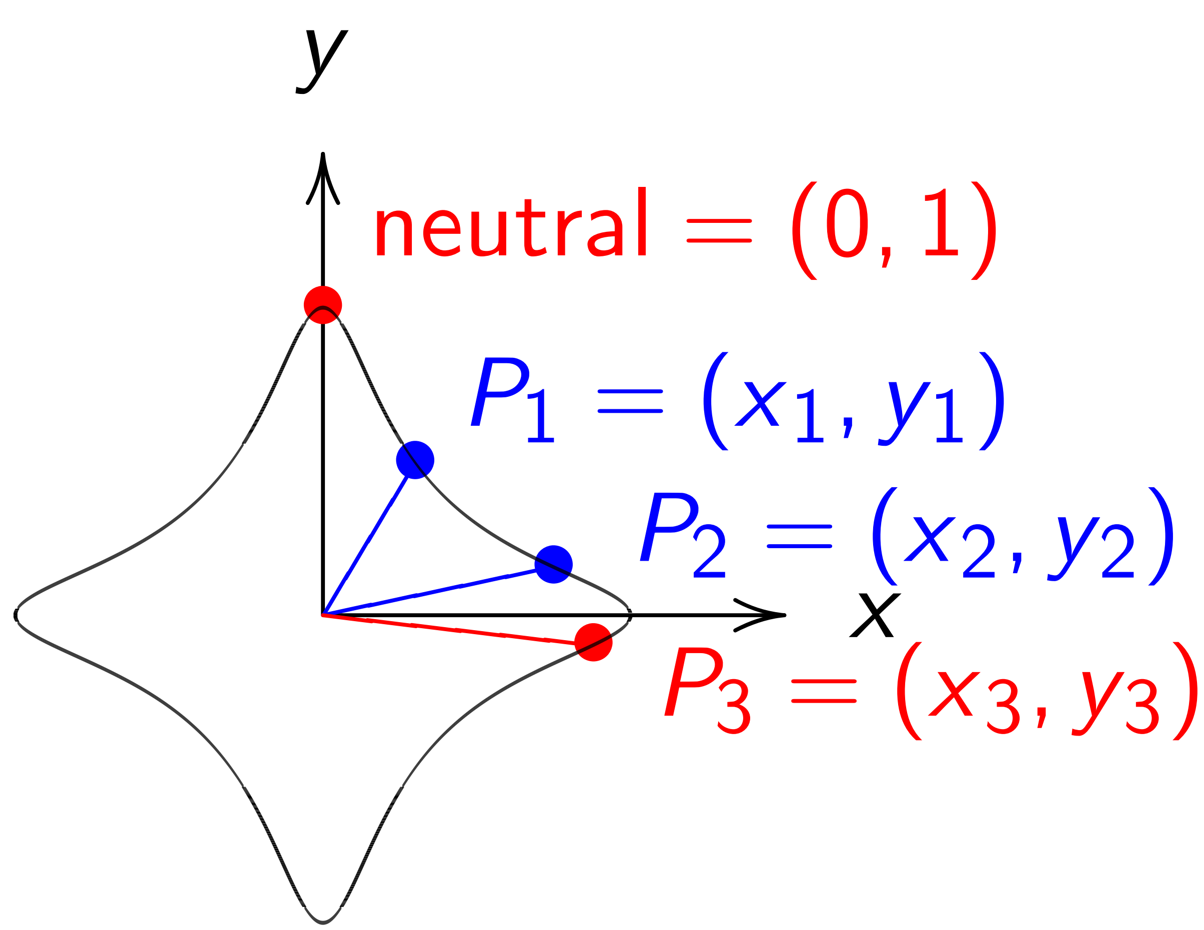
rmula.

ical

ADD.

2007 Edwards: new curve shape.

2007 Bernstein–Lange: generalize, analyze speed, completeness.



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

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

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$

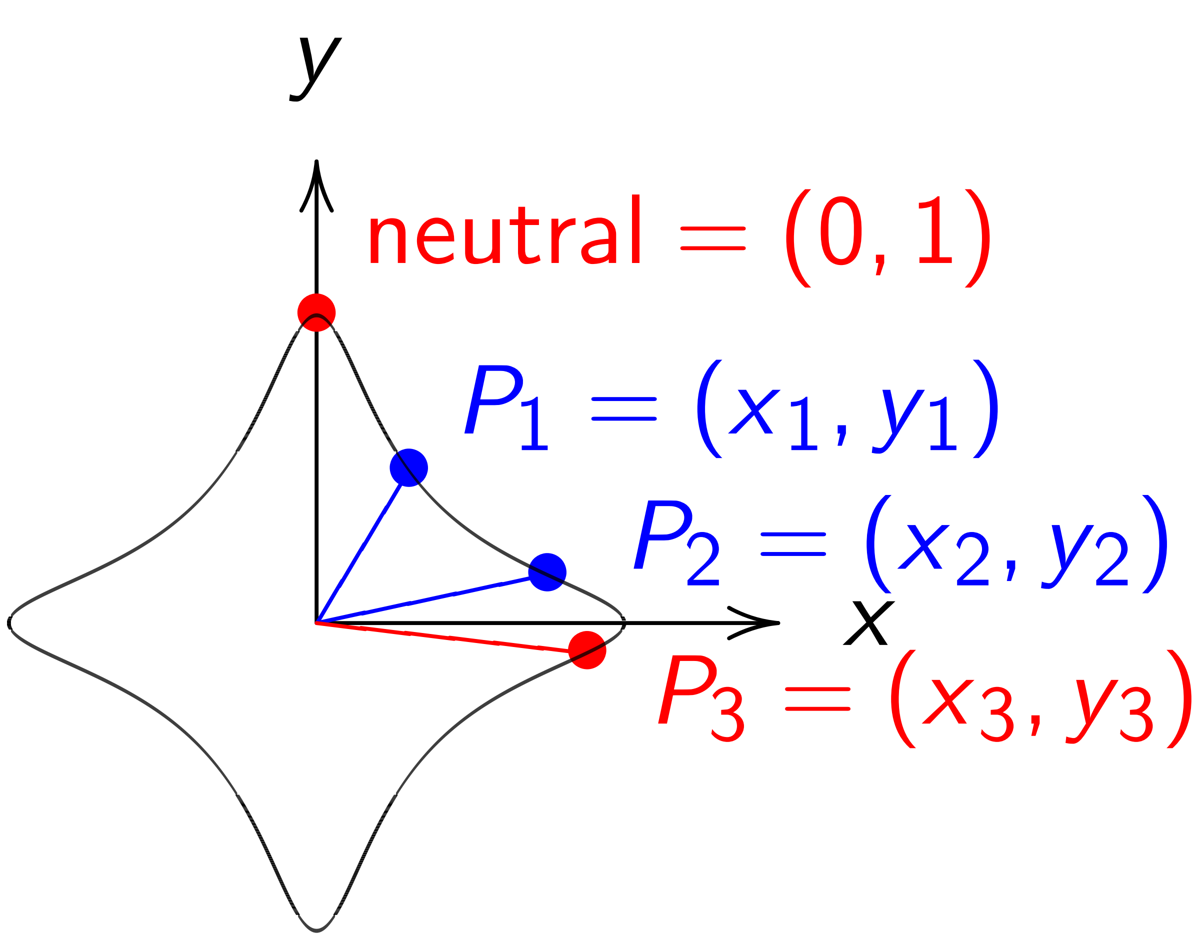
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

2007 Bernstein–Lange:

10.8**M** for ADD, 6.2**M** for D

2007 Edwards: new curve shape.

2007 Bernstein–Lange: generalize, analyze speed, completeness.



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

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

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$

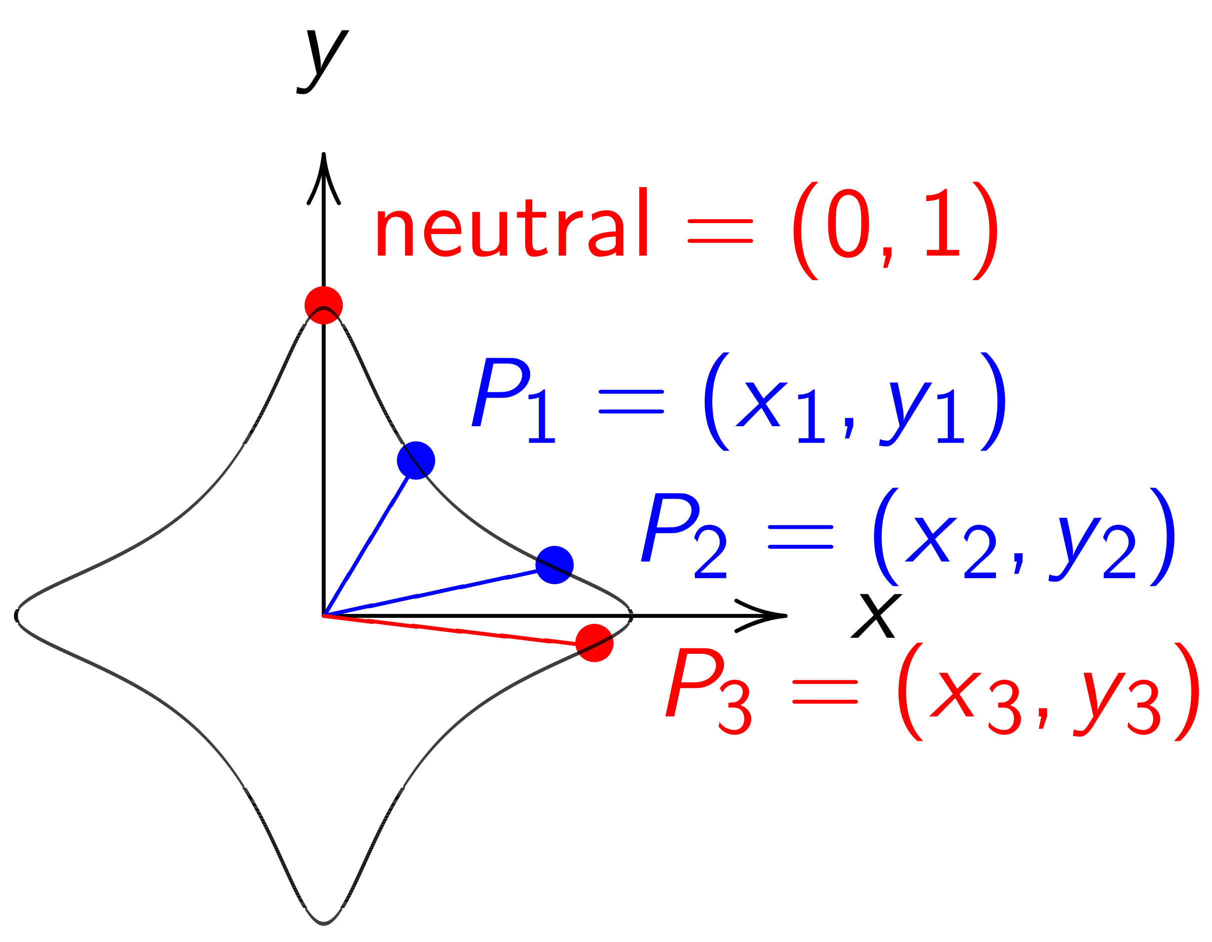
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

2007 Bernstein–Lange:

10.8**M** for ADD, 6.2**M** for DBL.

2007 Edwards: new curve shape.

2007 Bernstein–Lange: generalize, analyze speed, completeness.



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

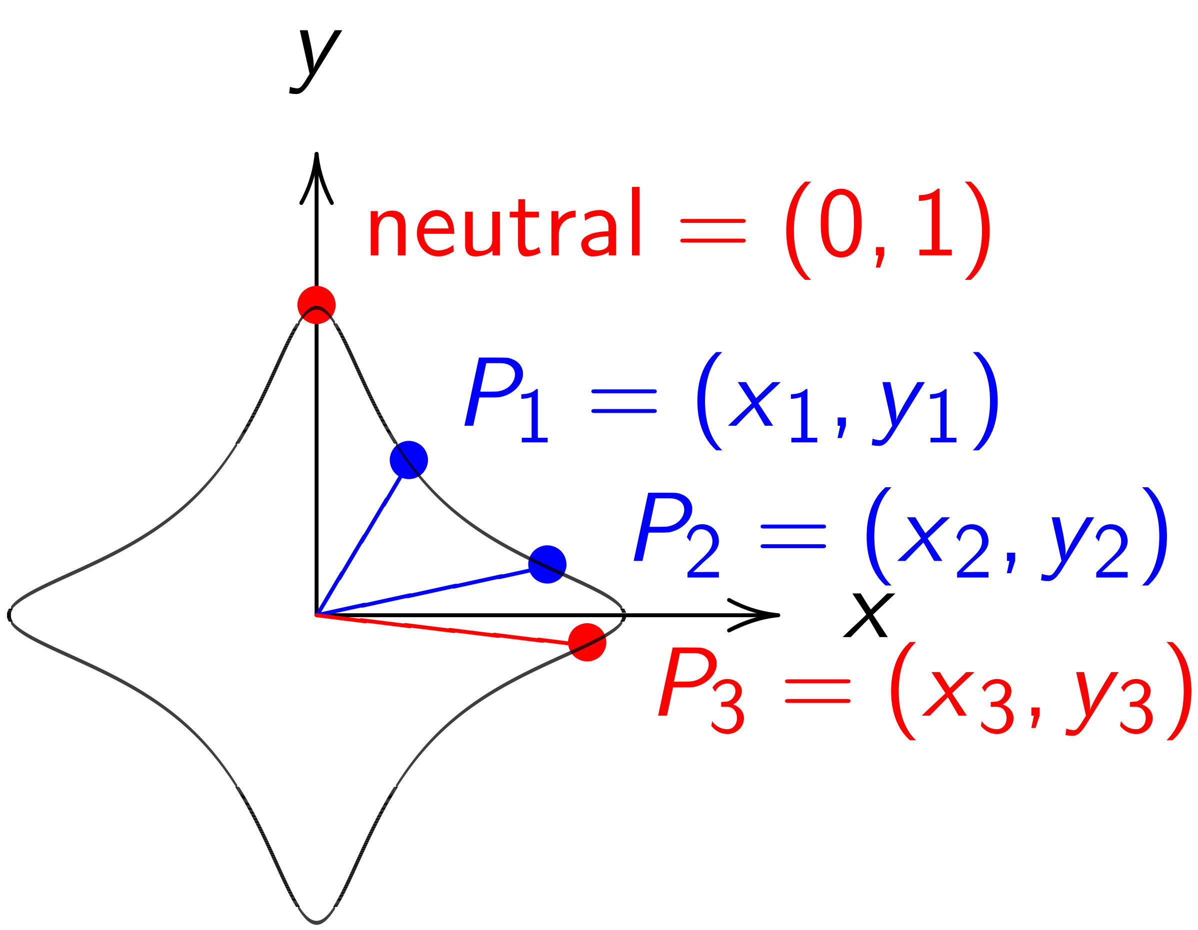
Sum of (x_1, y_1) and (x_2, y_2) is

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

2007 Bernstein–Lange:
10.8**M** for ADD, 6.2**M** for DBL.

2008 Hisil–Wong–Carter–Dawson:
just 8**M** for ADD.

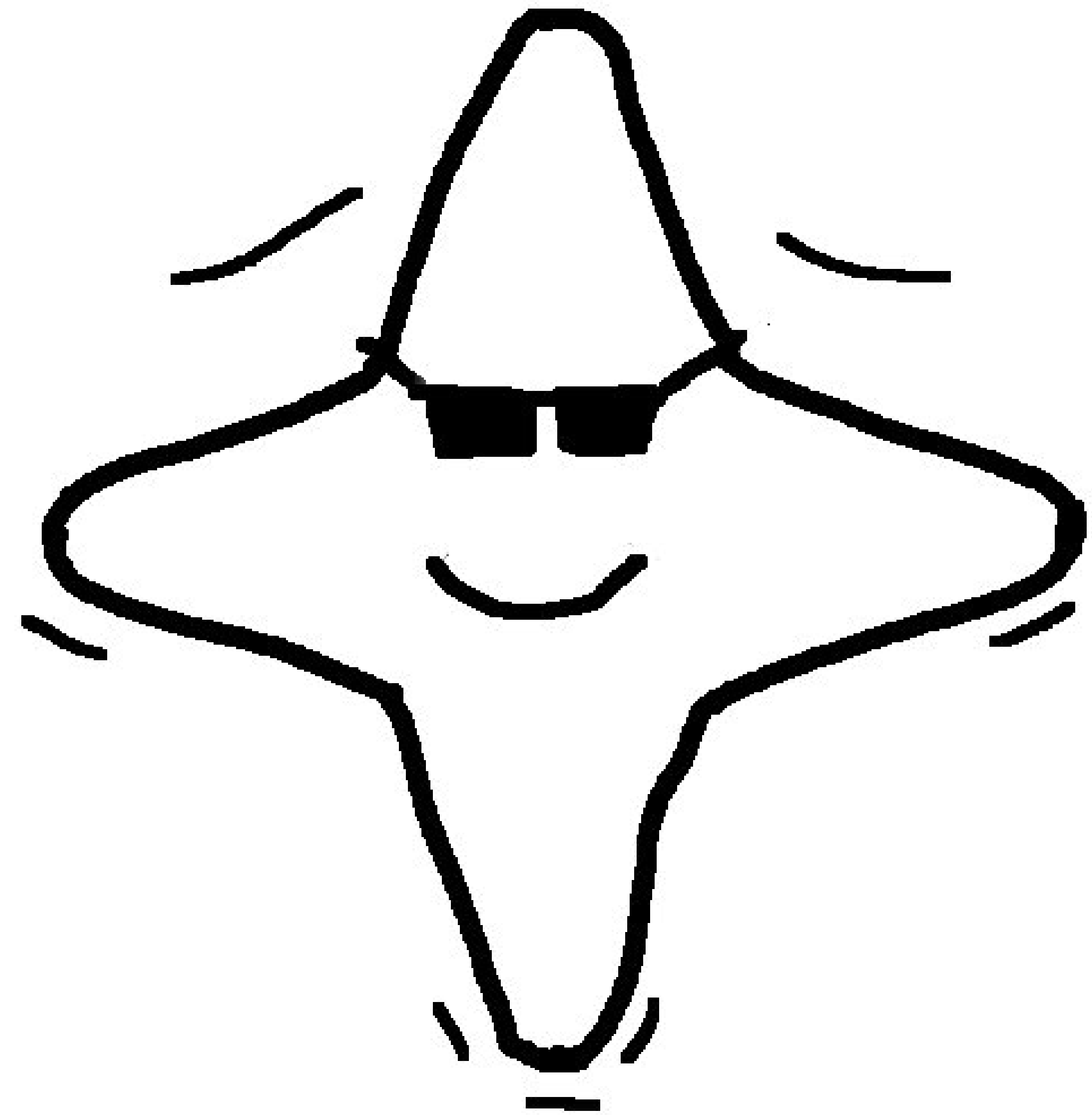
2007 Edwards: new curve shape.
2007 Bernstein–Lange: generalize, analyze speed, completeness.



Example: $x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

2007 Bernstein–Lange:
10.8**M** for ADD, 6.2**M** for DBL.

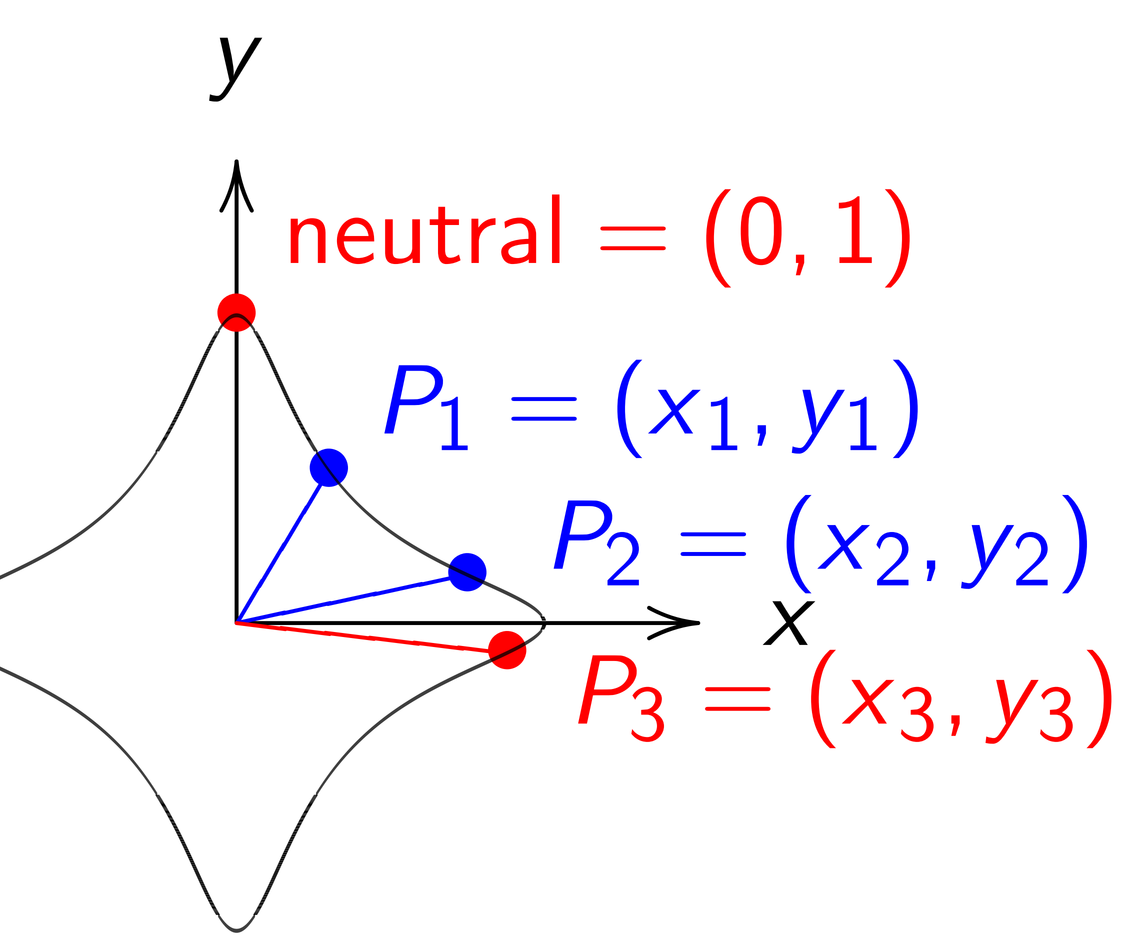
2008 Hisil–Wong–Carter–Dawson:
just 8**M** for ADD.



wards: new curve shape.

rnstein–Lange: generalize,

speed, completeness.



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

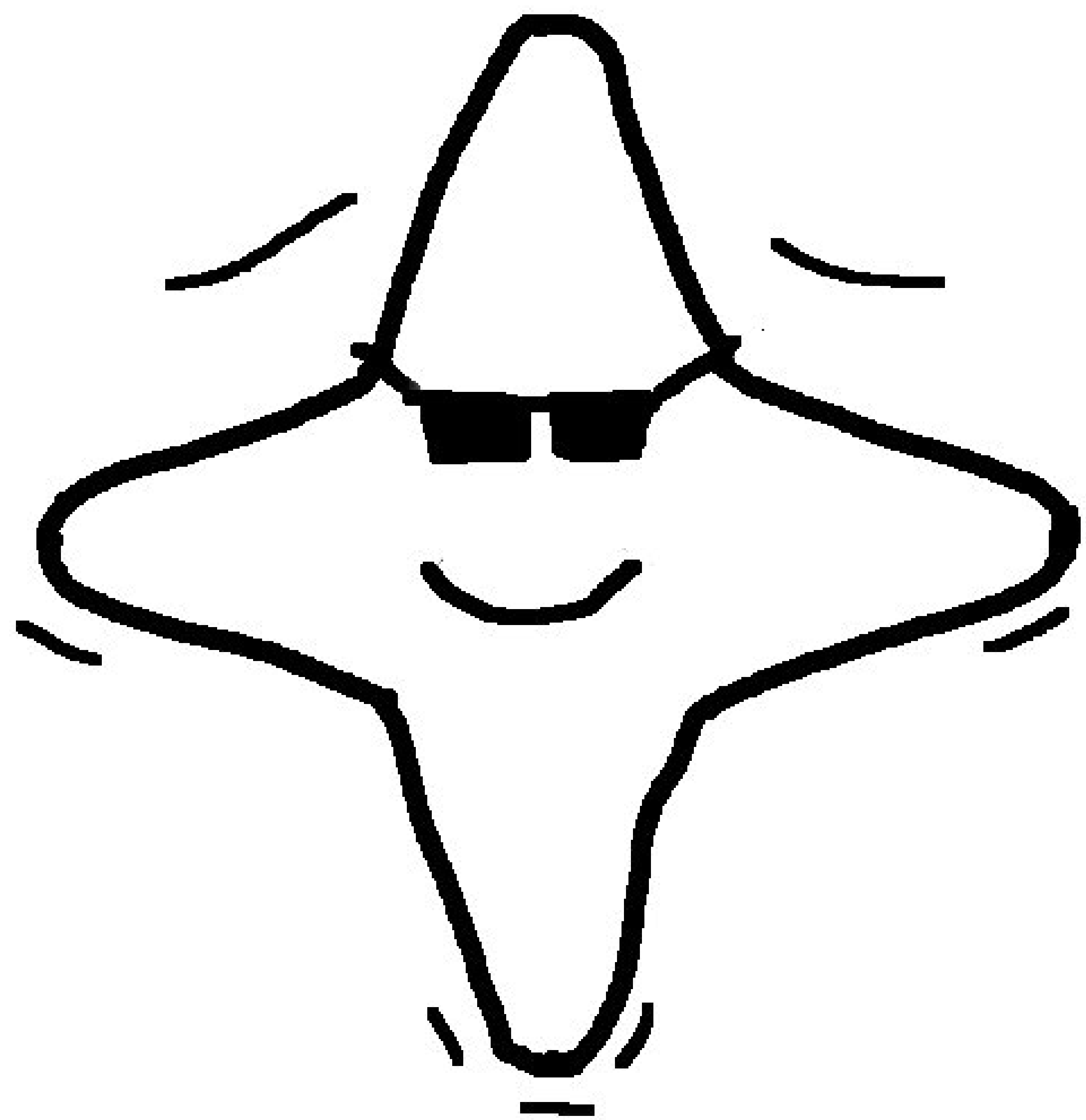
(x_1, y_1) and (x_2, y_2) is

$+y_1x_2)/(1-30x_1x_2y_1y_2)$,

$x_1x_2)/(1+30x_1x_2y_1y_2))$.

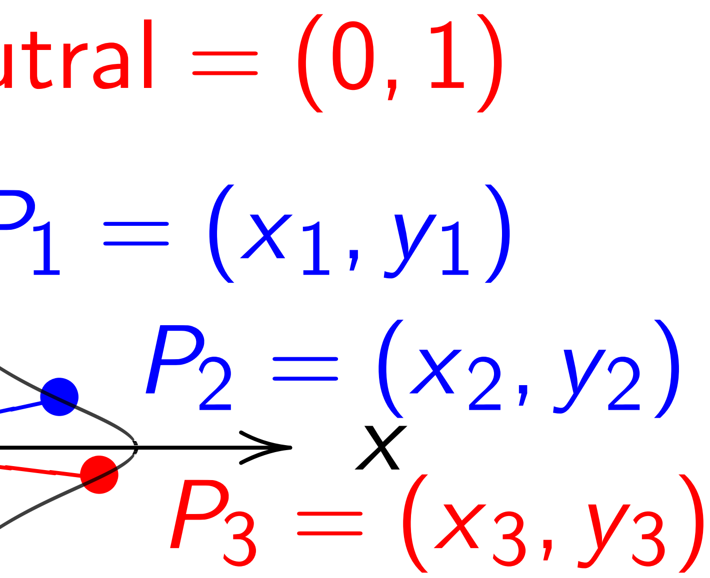
2007 Bernstein–Lange:
10.8**M** for ADD, 6.2**M** for DBL.

2008 Hisil–Wong–Carter–Dawson:
just 8**M** for ADD.



$y^2 = x^3$

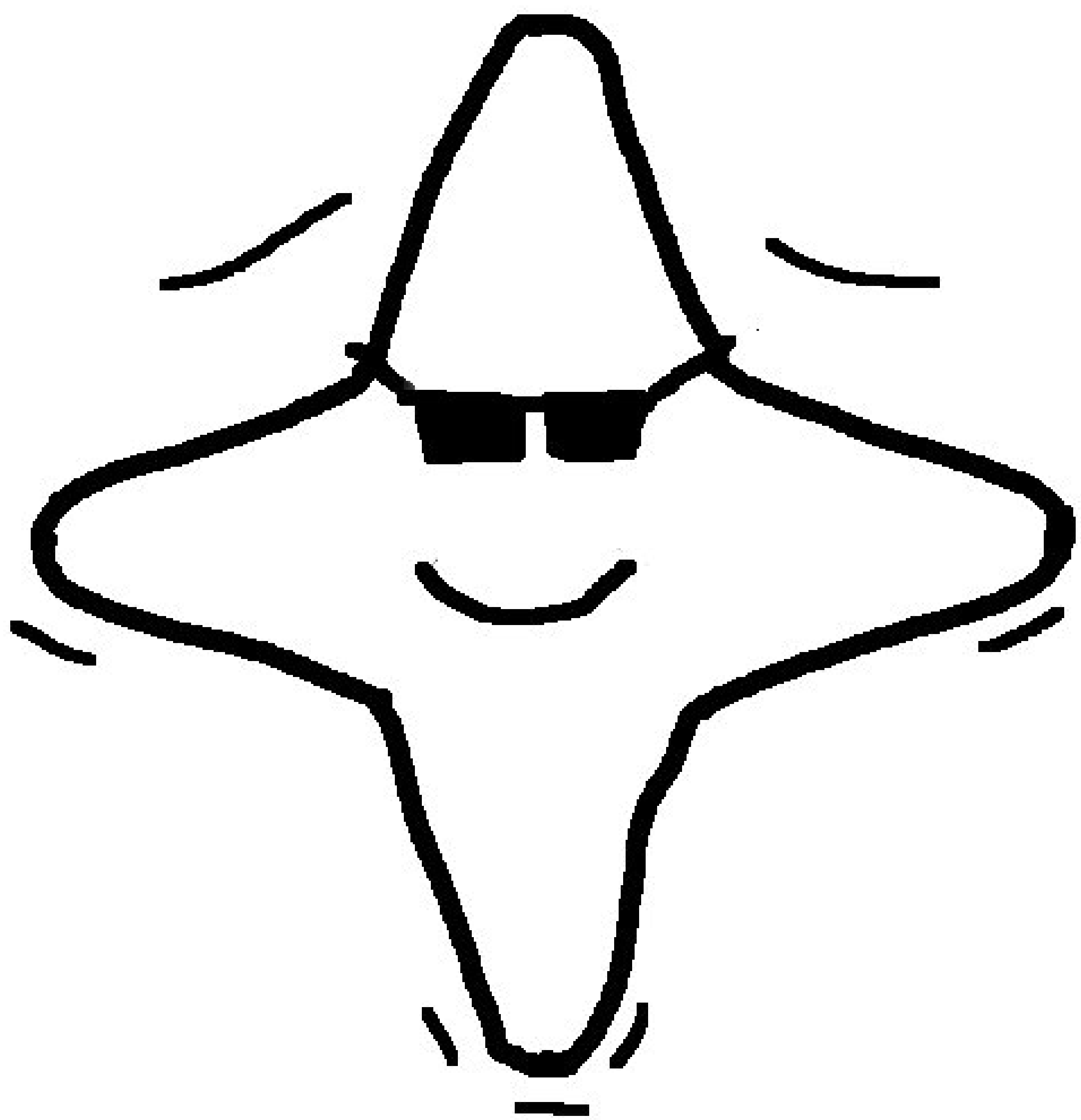
w curve shape.
ange: generalize,
mpleteness.

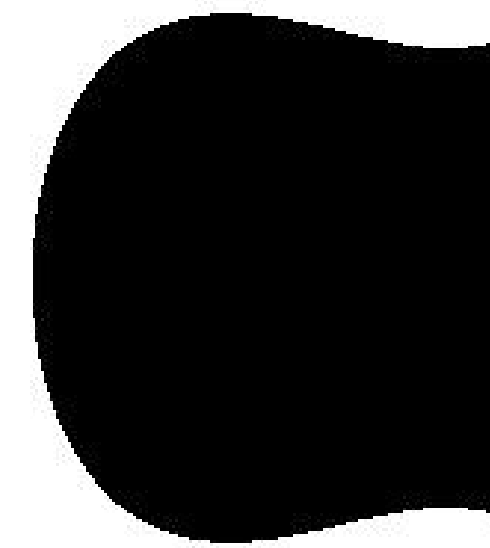


$= 1 - 30x^2y^2$.
nd (x_2, y_2) is
$-30x_1x_2y_1y_2)$,
$+30x_1x_2y_1y_2))$.

2007 Bernstein–Lange:
10.8**M** for ADD, 6.2**M** for DBL.

2008 Hisil–Wong–Carter–Dawson:
just 8**M** for ADD.





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

hape.

eralize,

s.

$1)$

$y_1)$

$x_2, y_2)$

(x_3, y_3)

$x^2 y^2$.

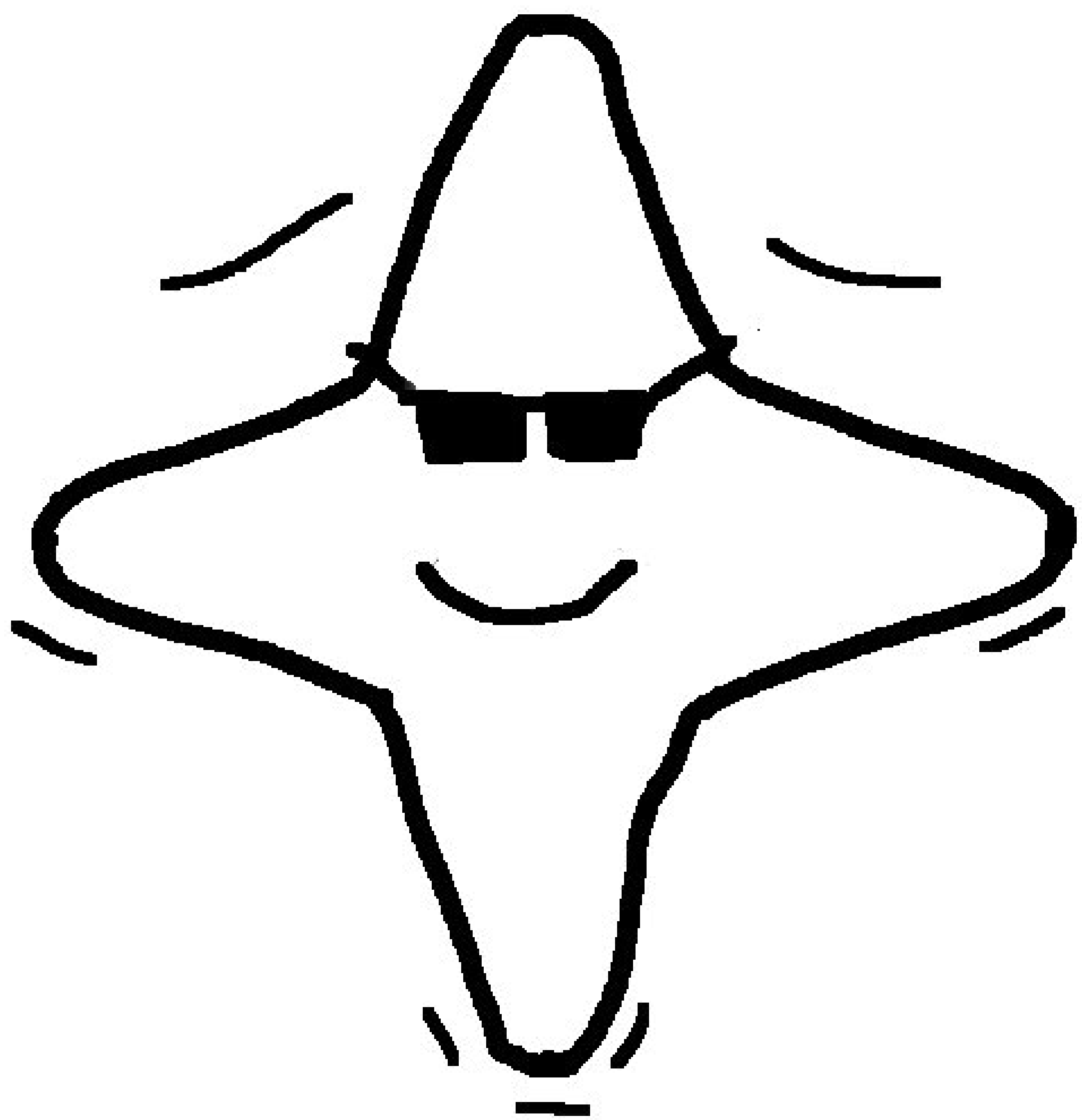
$)$ is

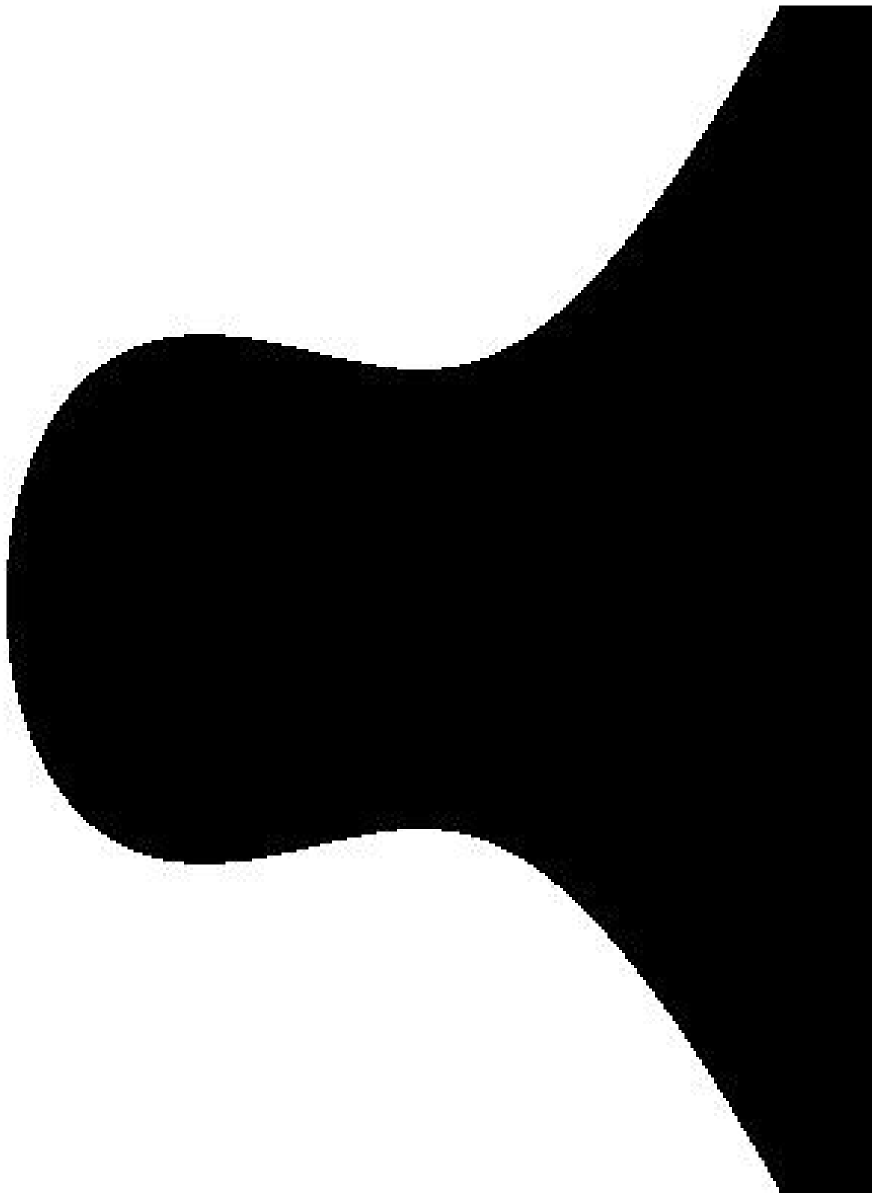
$_1 y_2)$,

$_1 y_2))$.

2007 Bernstein–Lange:
10.8**M** for ADD, 6.2**M** for DBL.

2008 Hisil–Wong–Carter–Dawson:
just 8**M** for ADD.

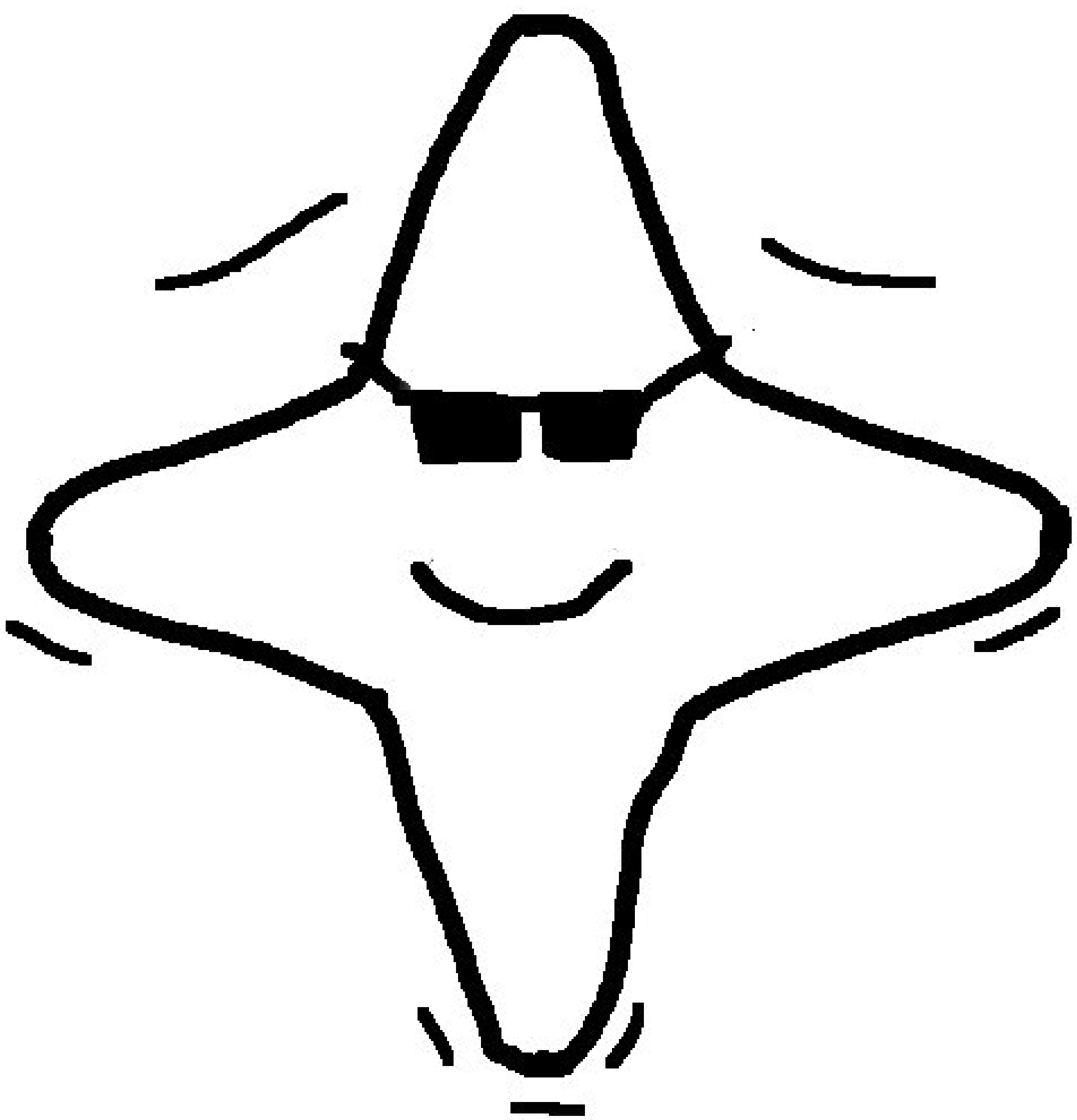


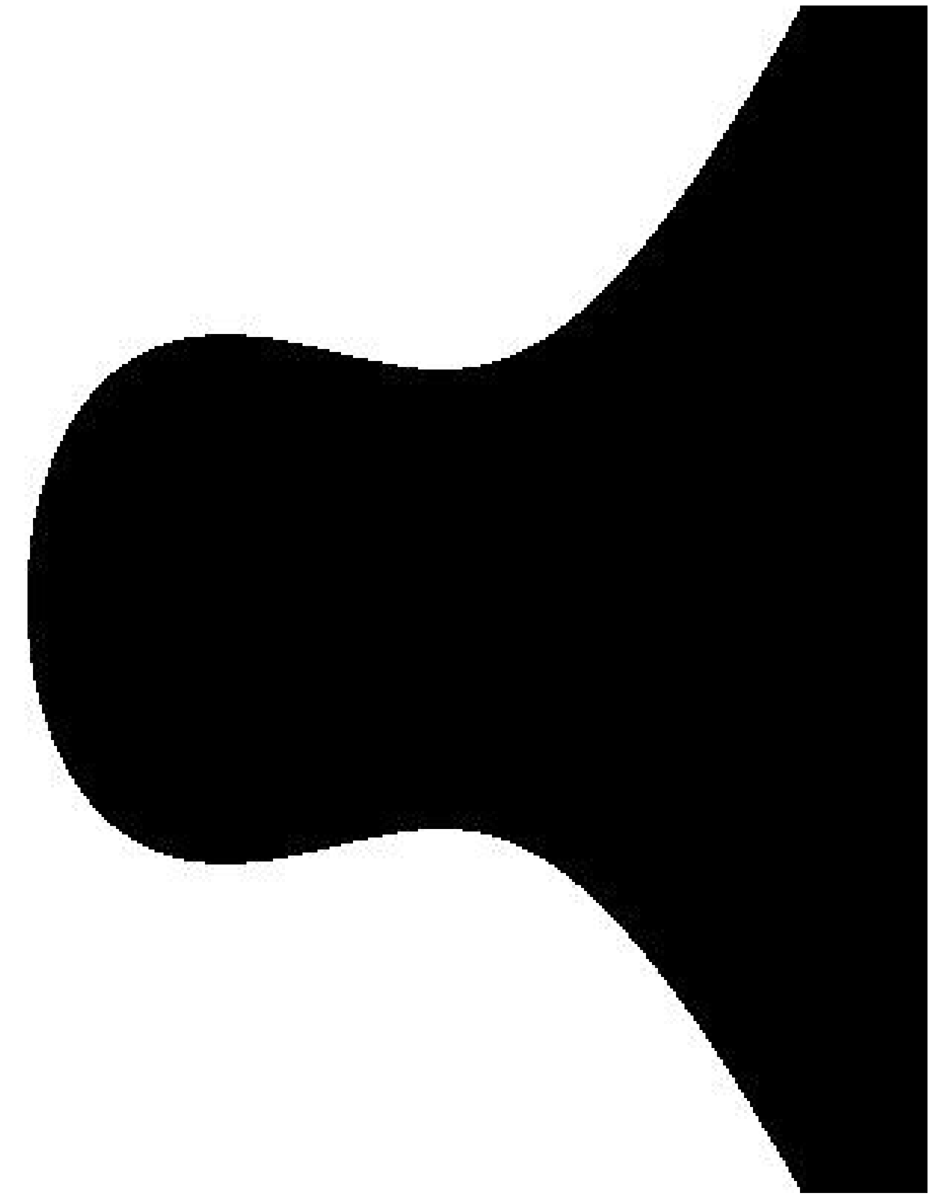


$$y^2 = x^3 - 0.4x + 0.7$$

2007 Bernstein–Lange:
10.8**M** for ADD, 6.2**M** for DBL.

2008 Hisil–Wong–Carter–Dawson:
just 8**M** for ADD.

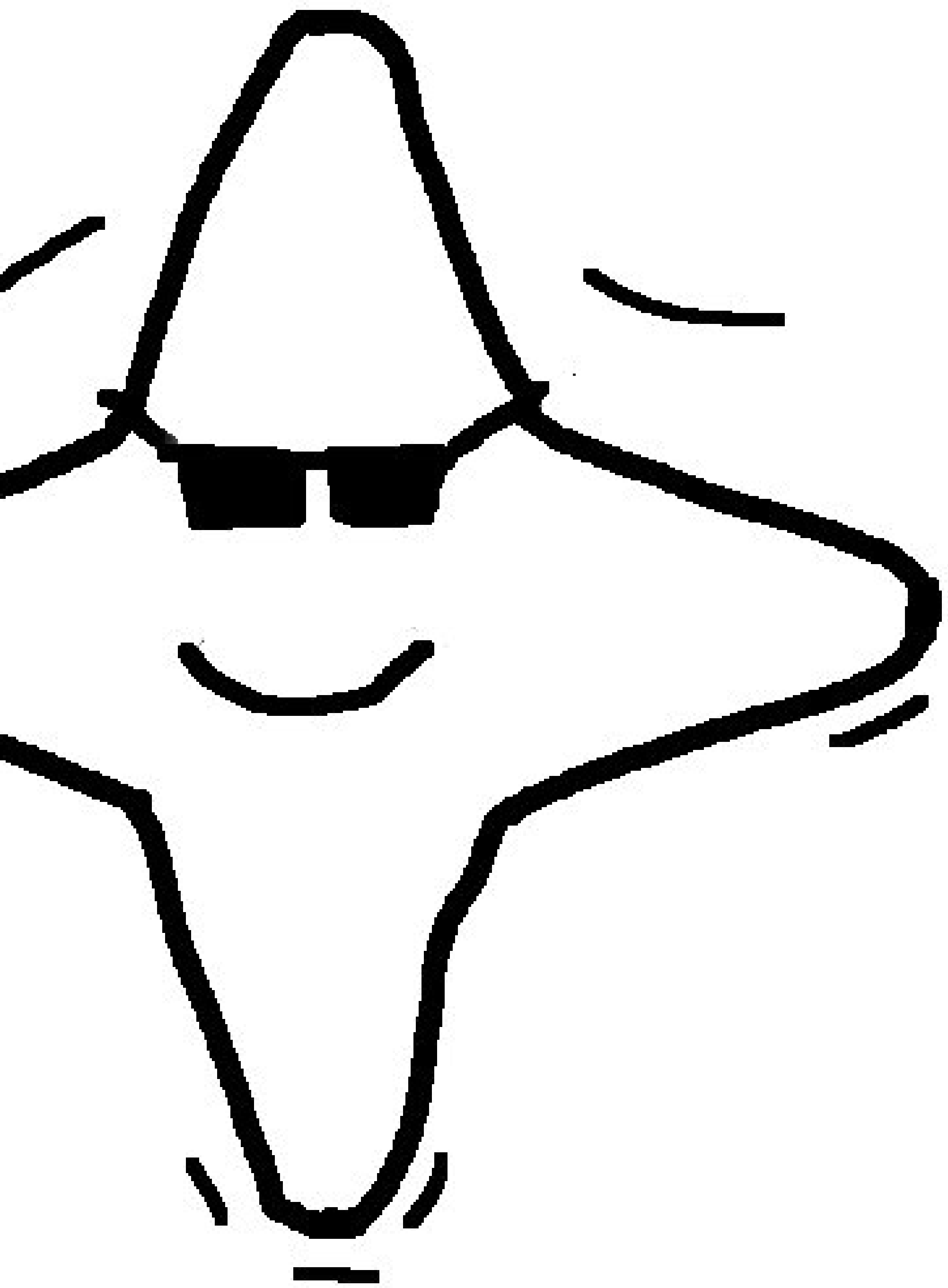


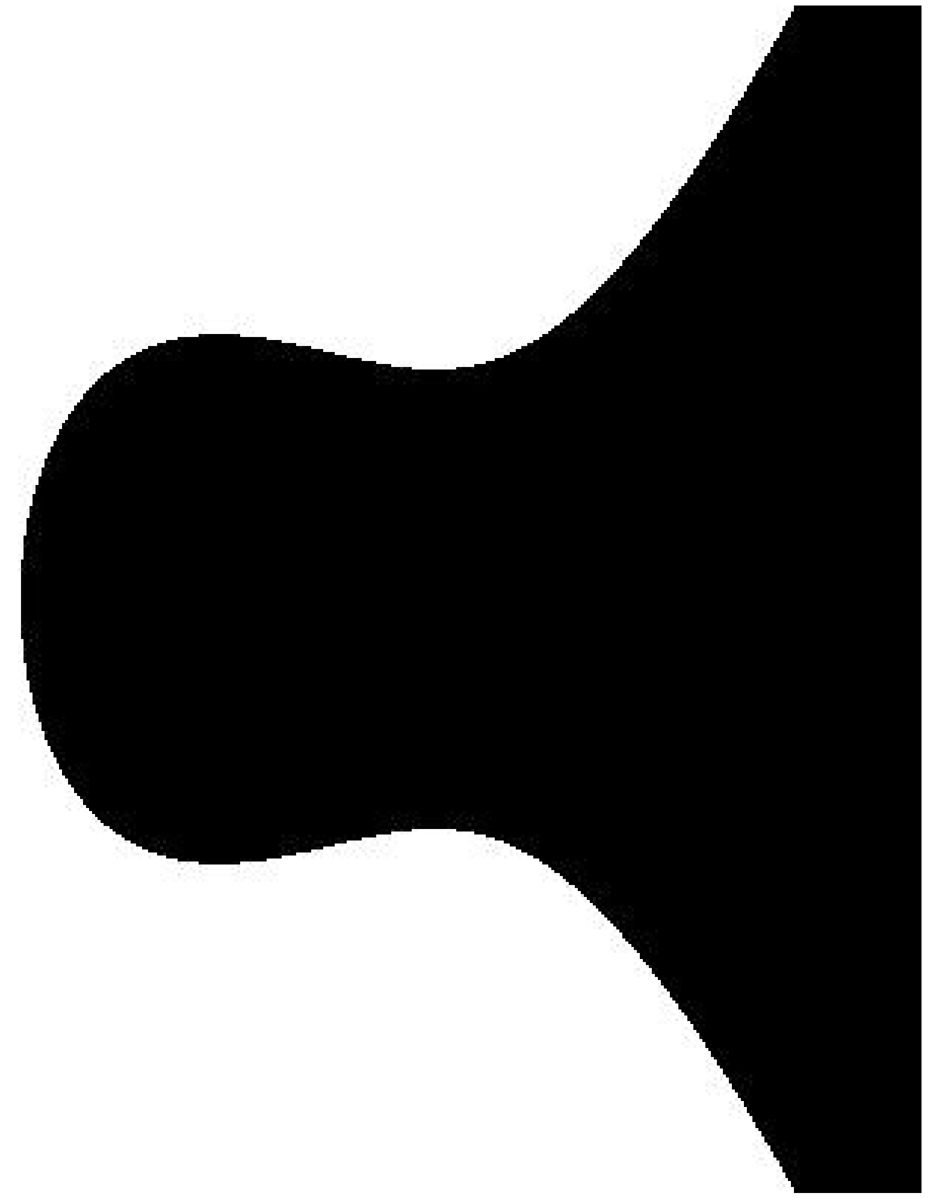


$$y^2 = x^3 - 0.4x + 0.7$$

rnstein–Lange:
or ADD, 6.2**M** for DBL.

sil–Wong–Carter–Dawson:
for ADD.





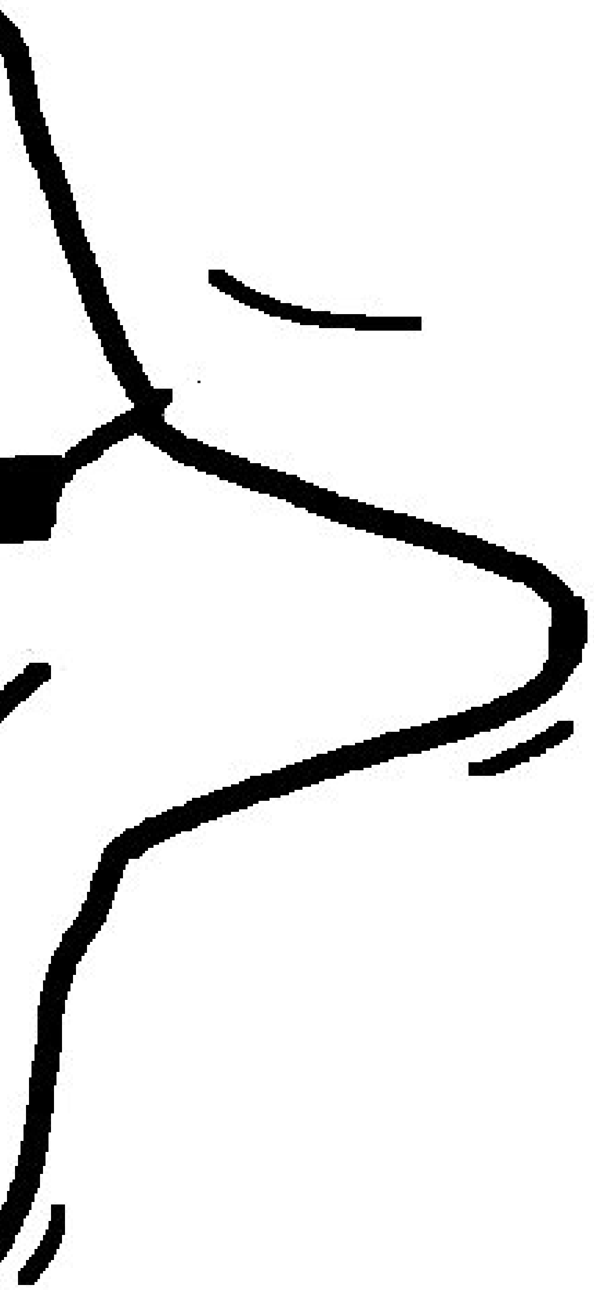
$y^2 = x^3 - 0.4x + 0.7$

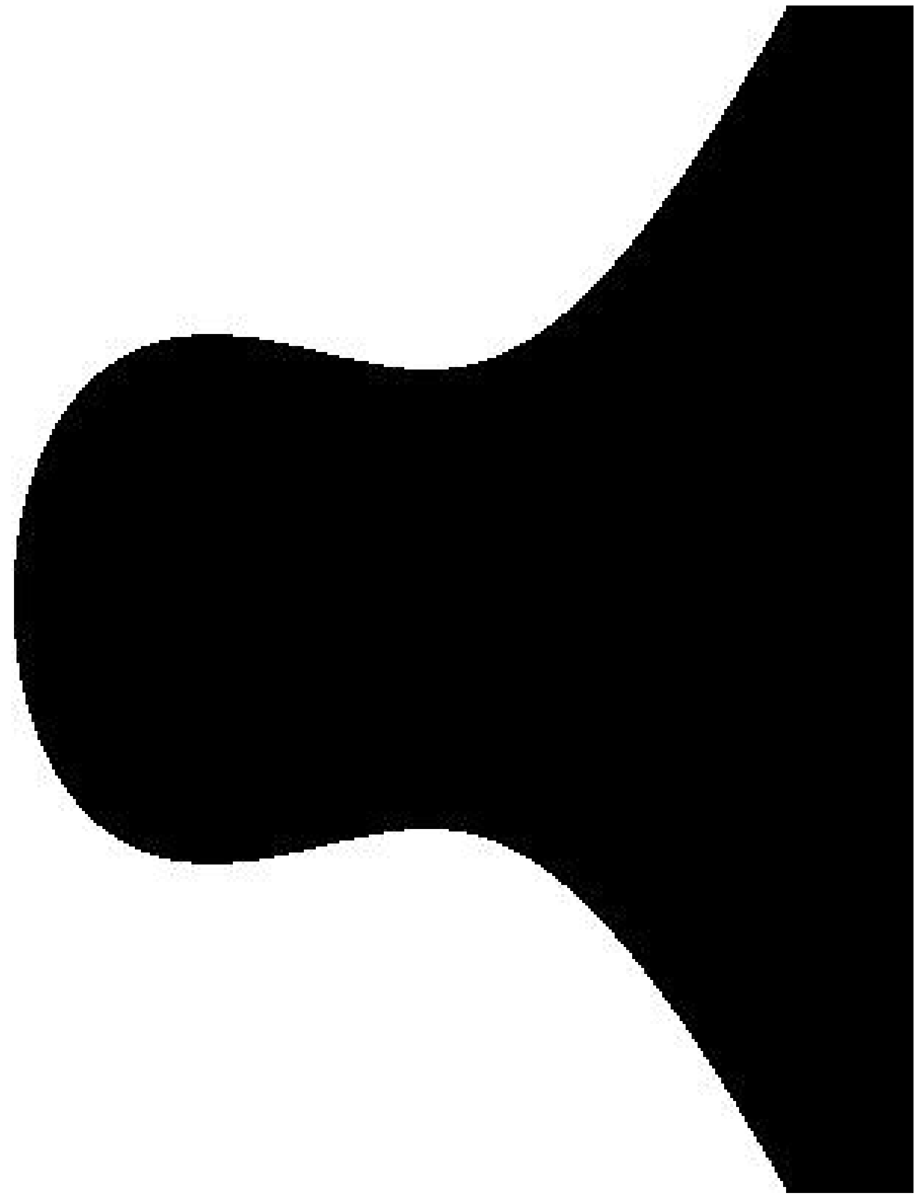
The We
turtle: o
and slow
(picture)

ange:

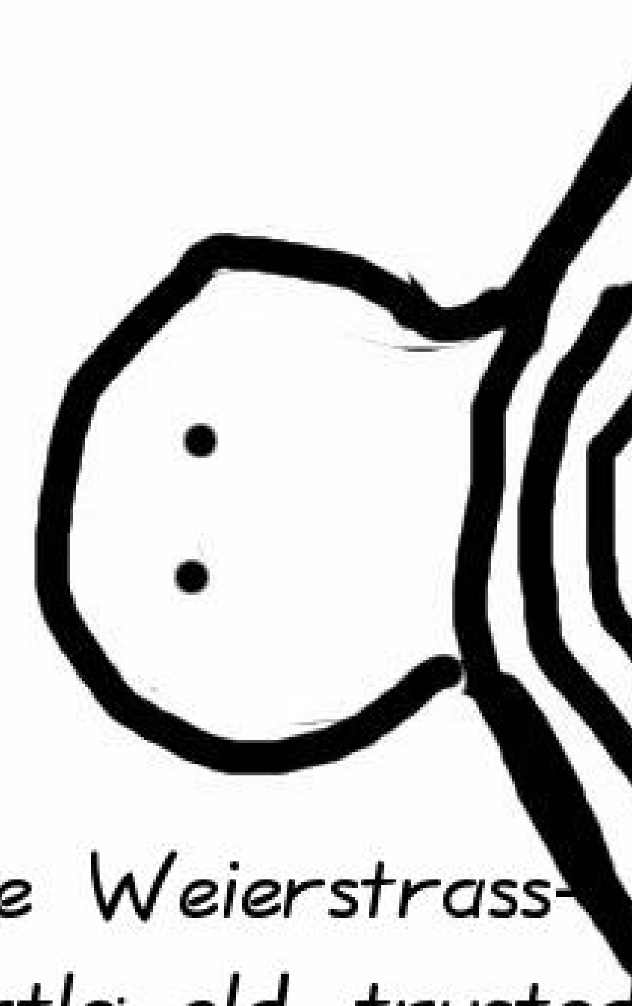
6.2**M** for DBL.

Carter–Dawson:





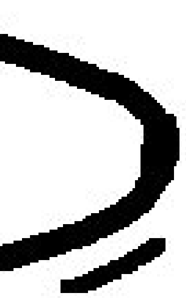
$$y^2 = x^3 - 0.4x + 0.7$$

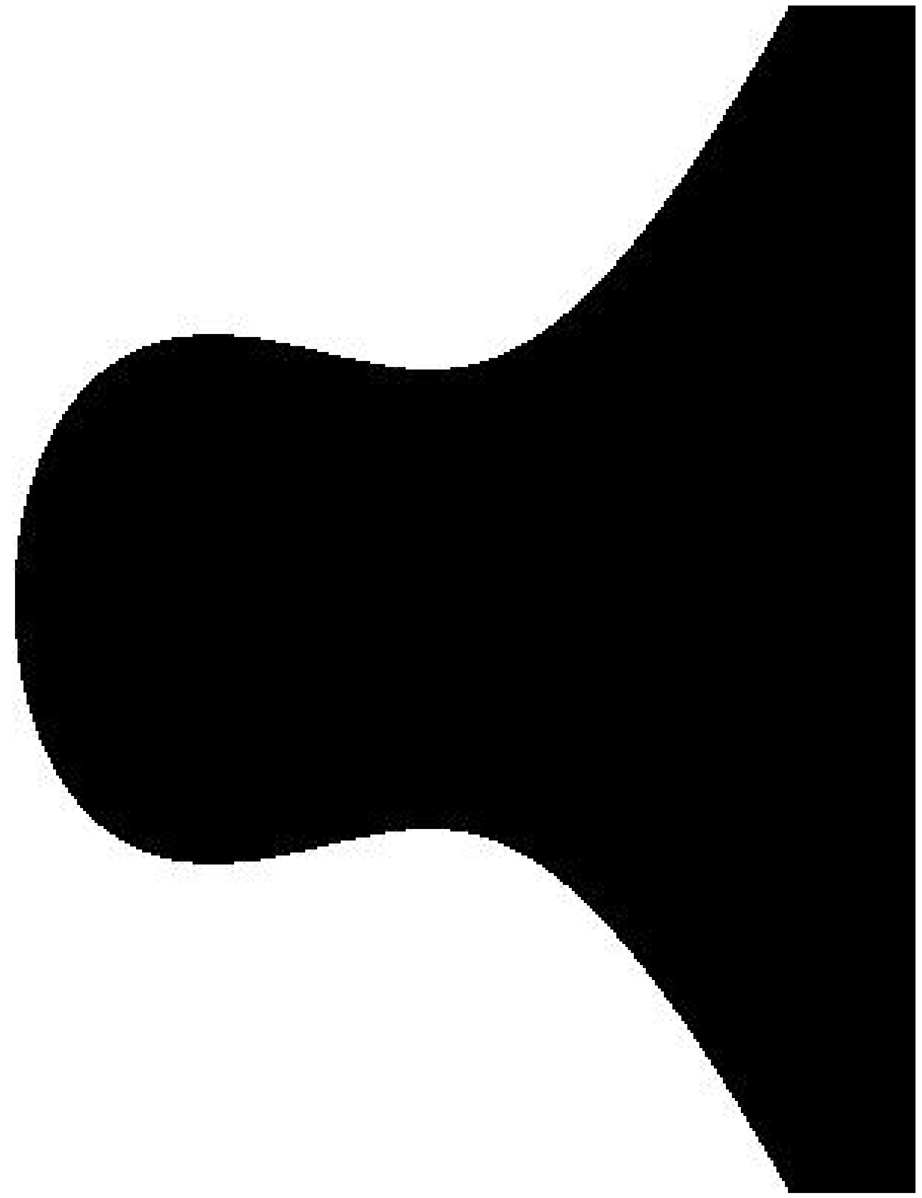


The Weierstrass-
turtle: old, trusted
and slow. Warning
(picture) incomplete

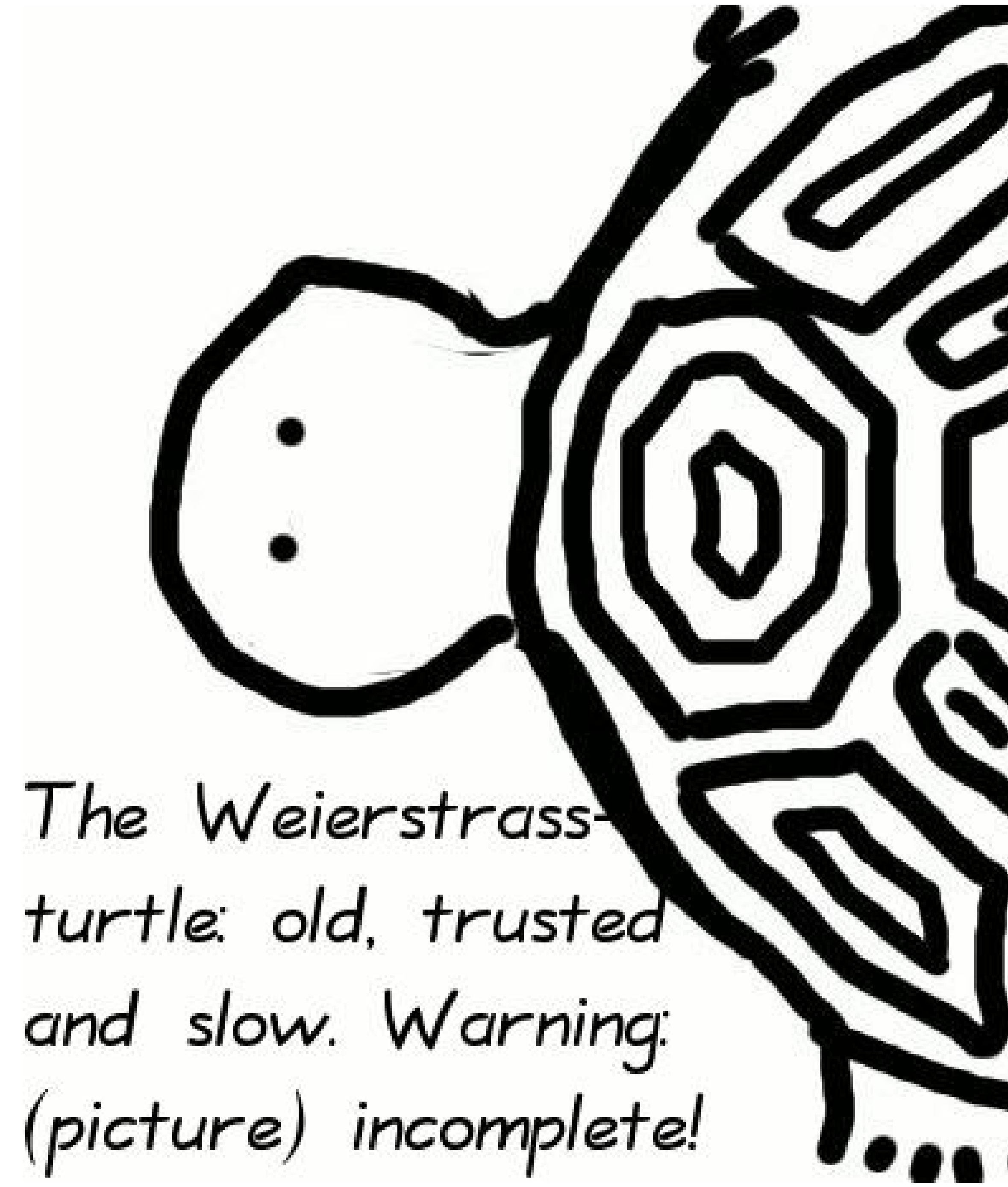
OBL.

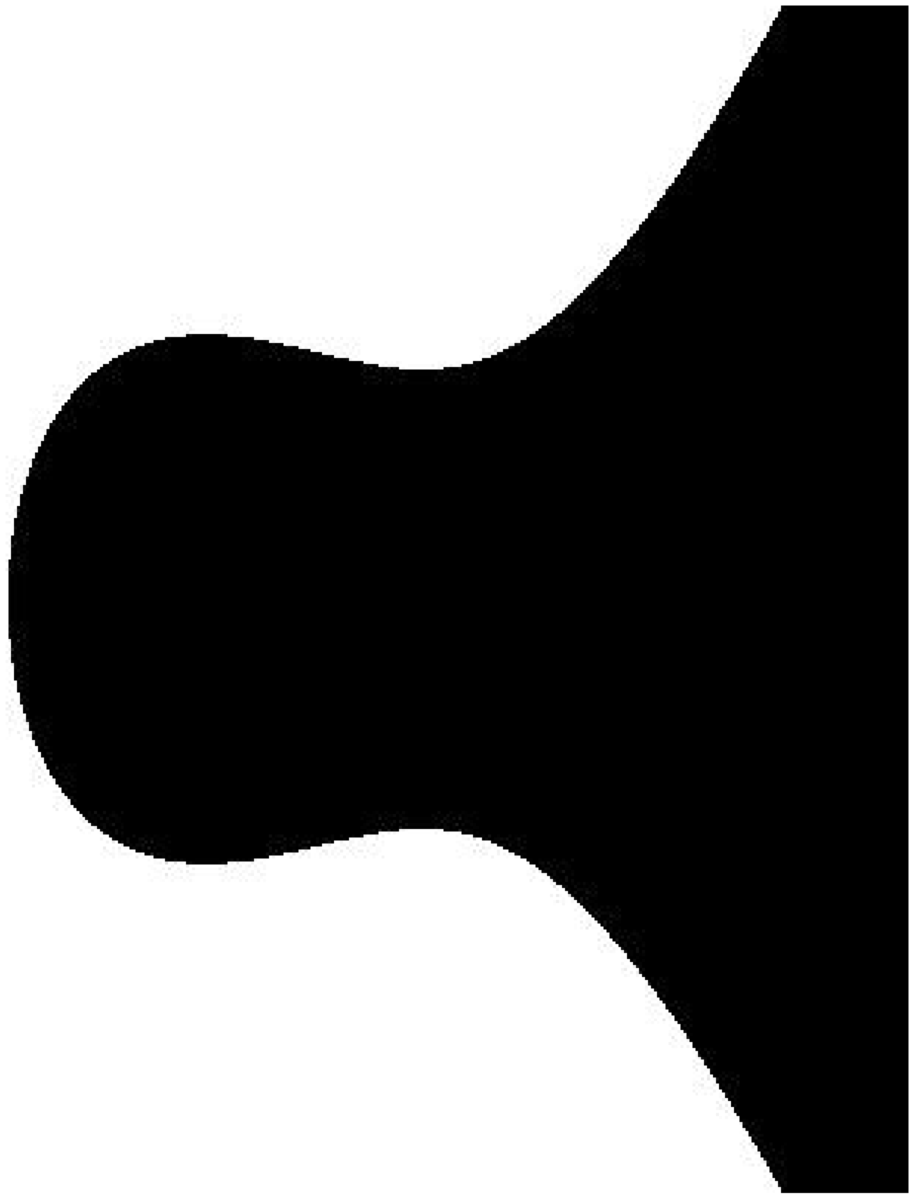
wson:



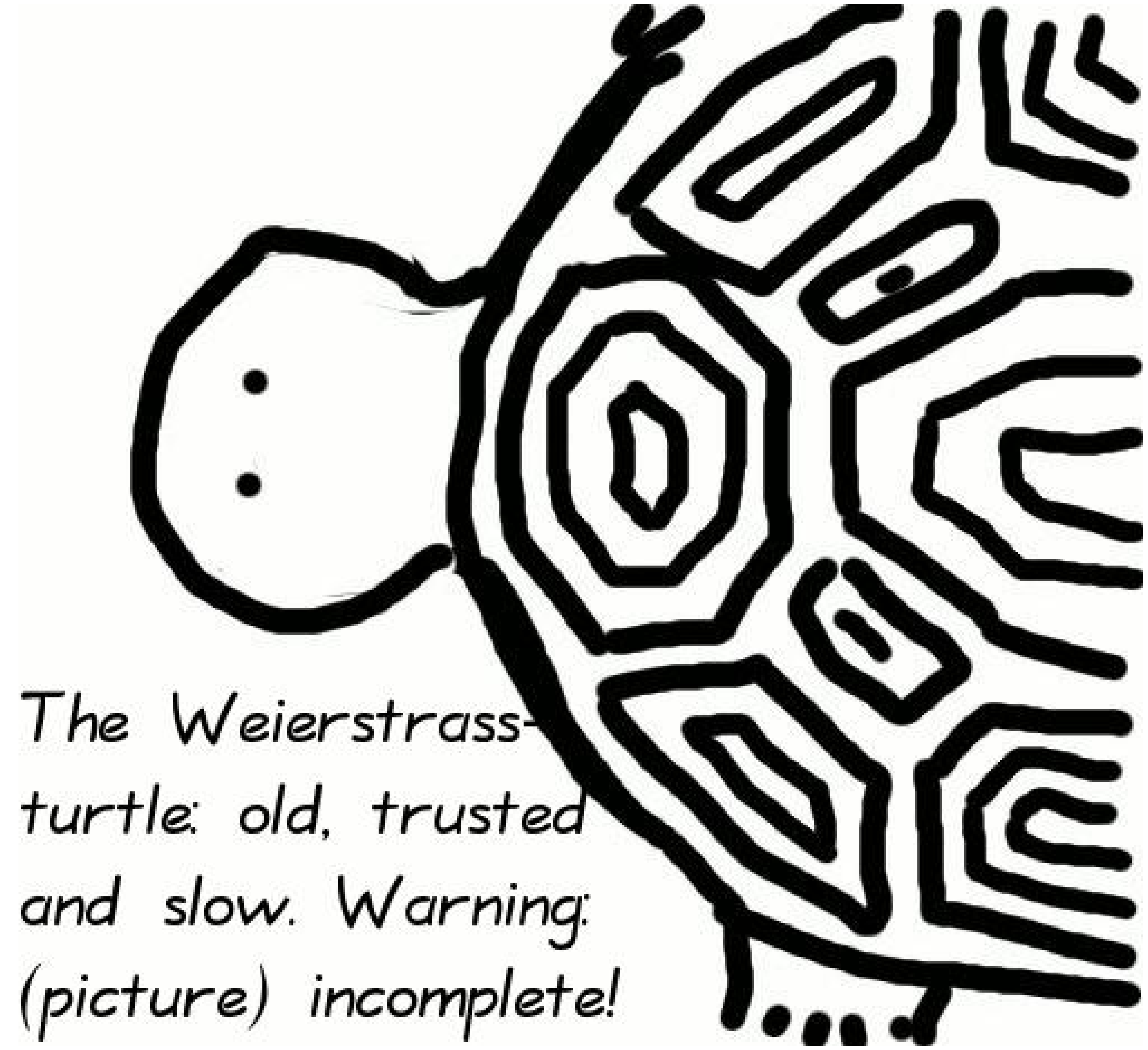


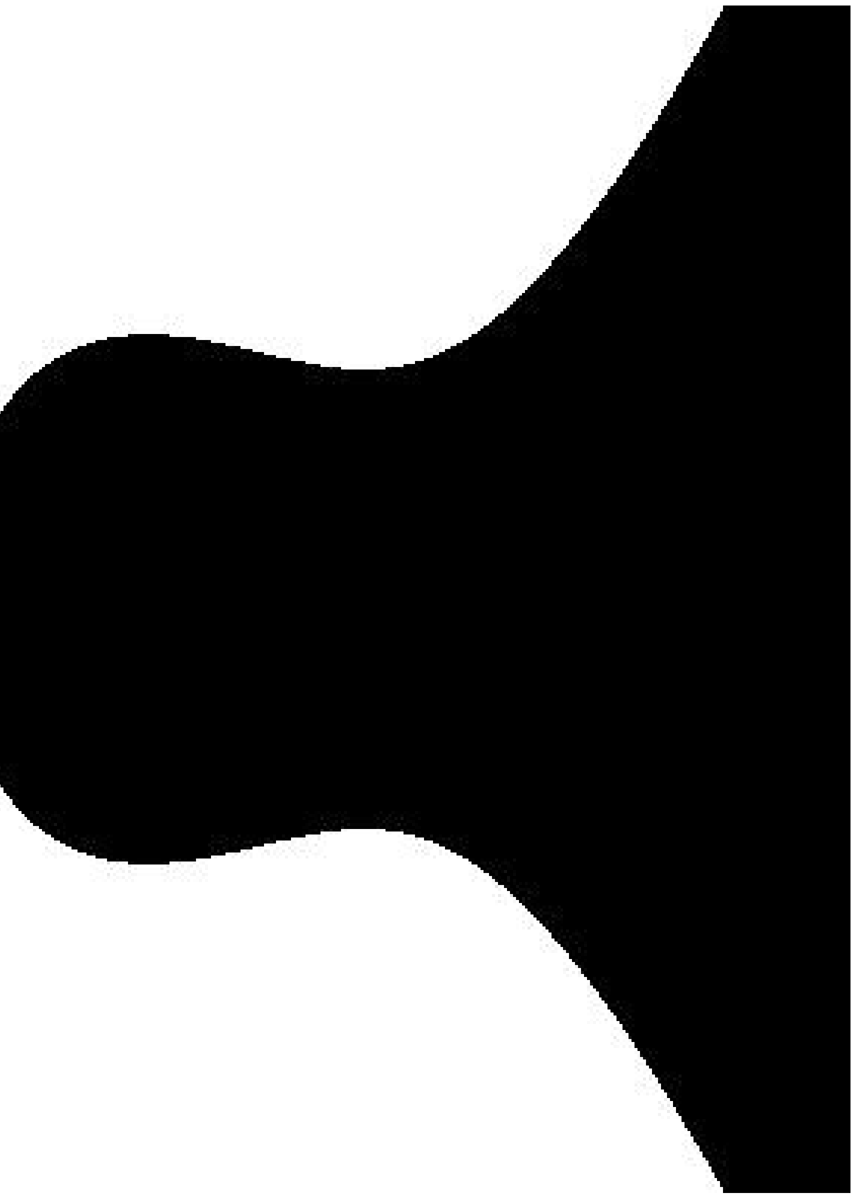
$$y^2 = x^3 - 0.4x + 0.7$$



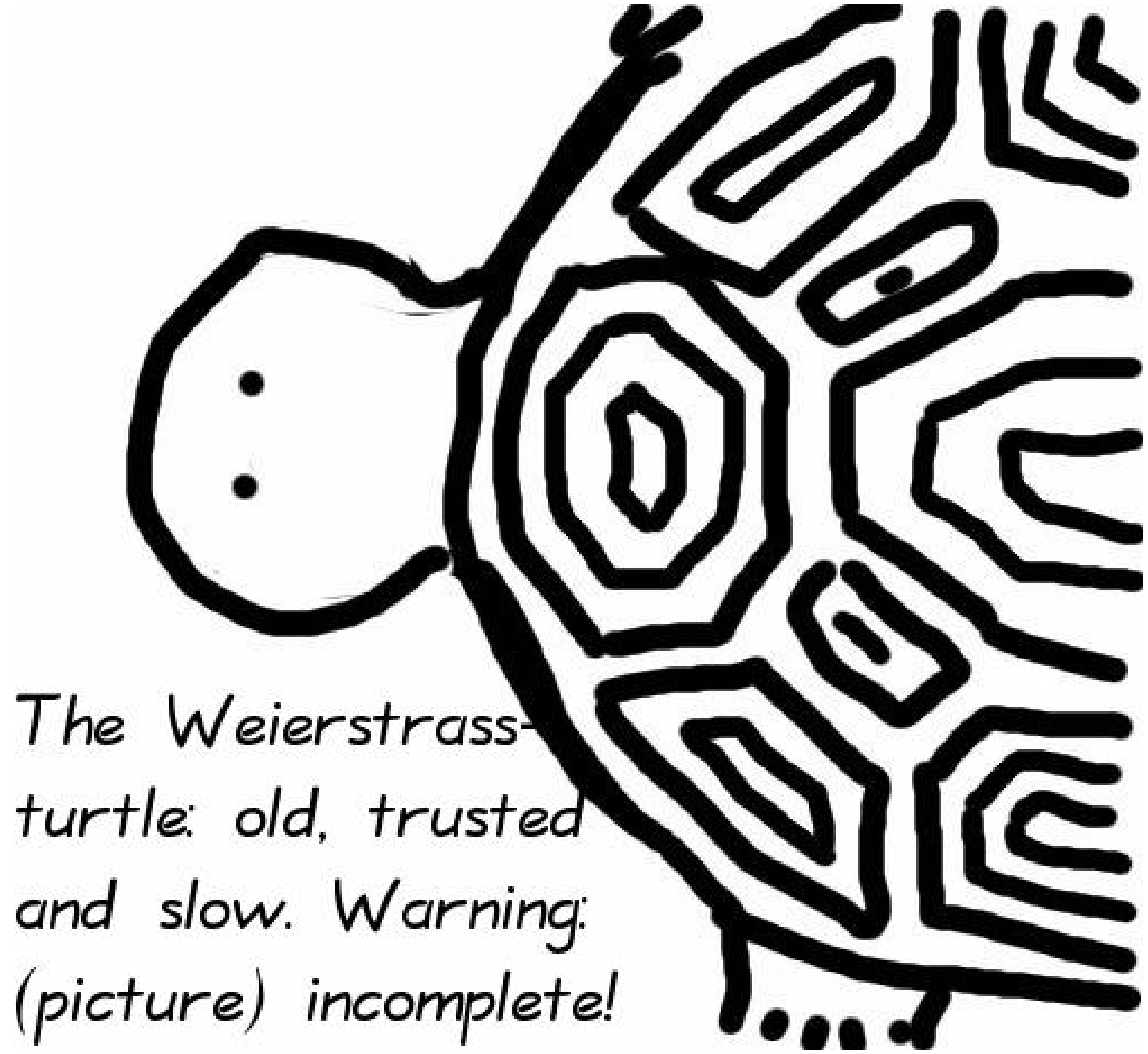


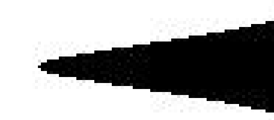
$$y^2 = x^3 - 0.4x + 0.7$$


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

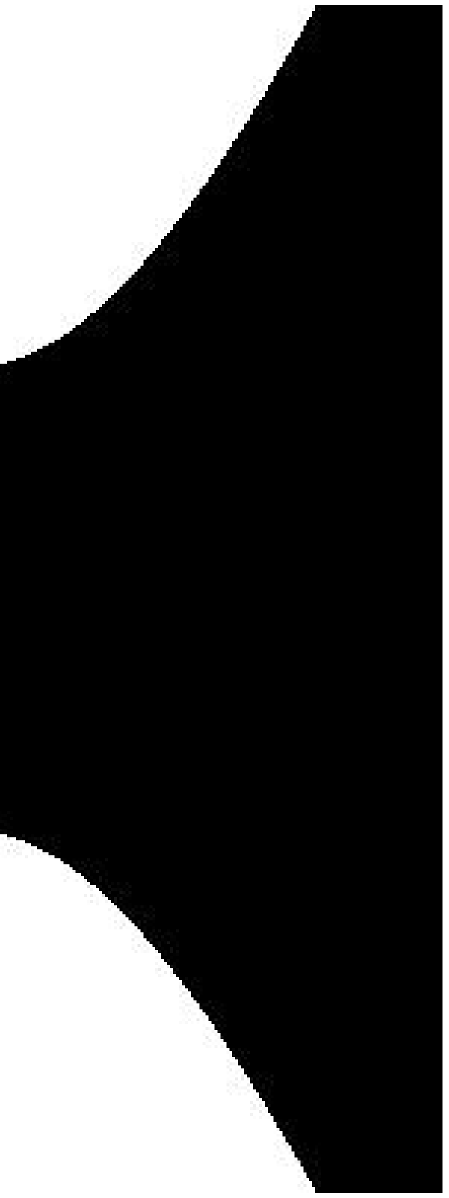


$- 0.4x + 0.7$

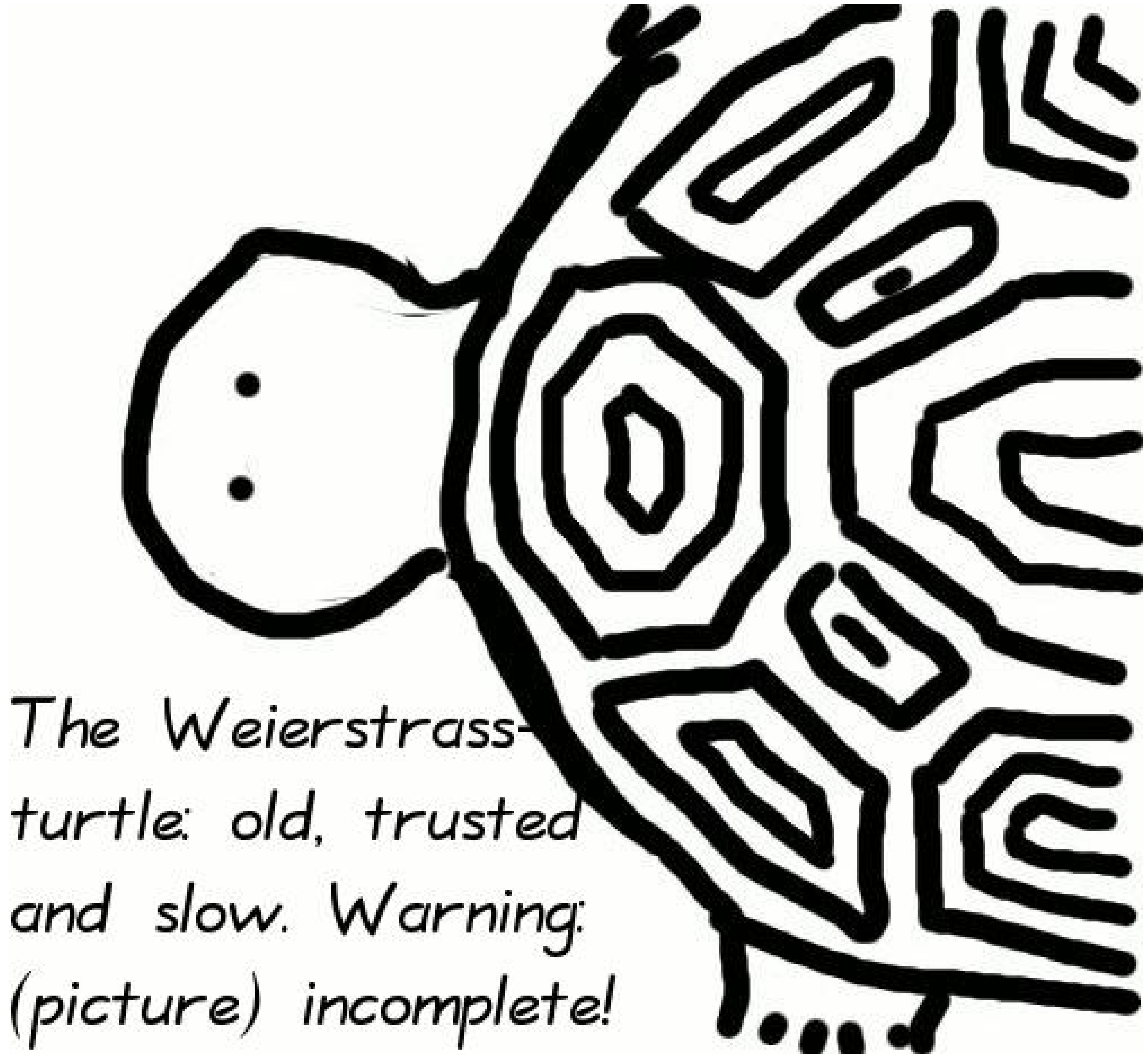

The Weierstrass-
turtle: old, trusted
and slow. Warning:
(picture) incomplete!

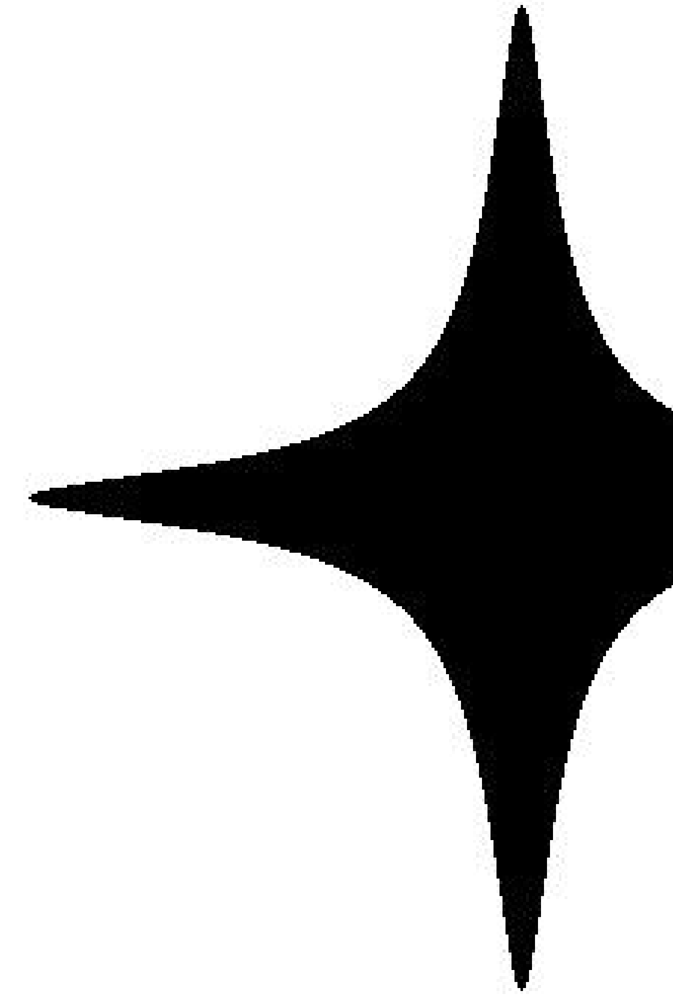


$x^2 + y^2$

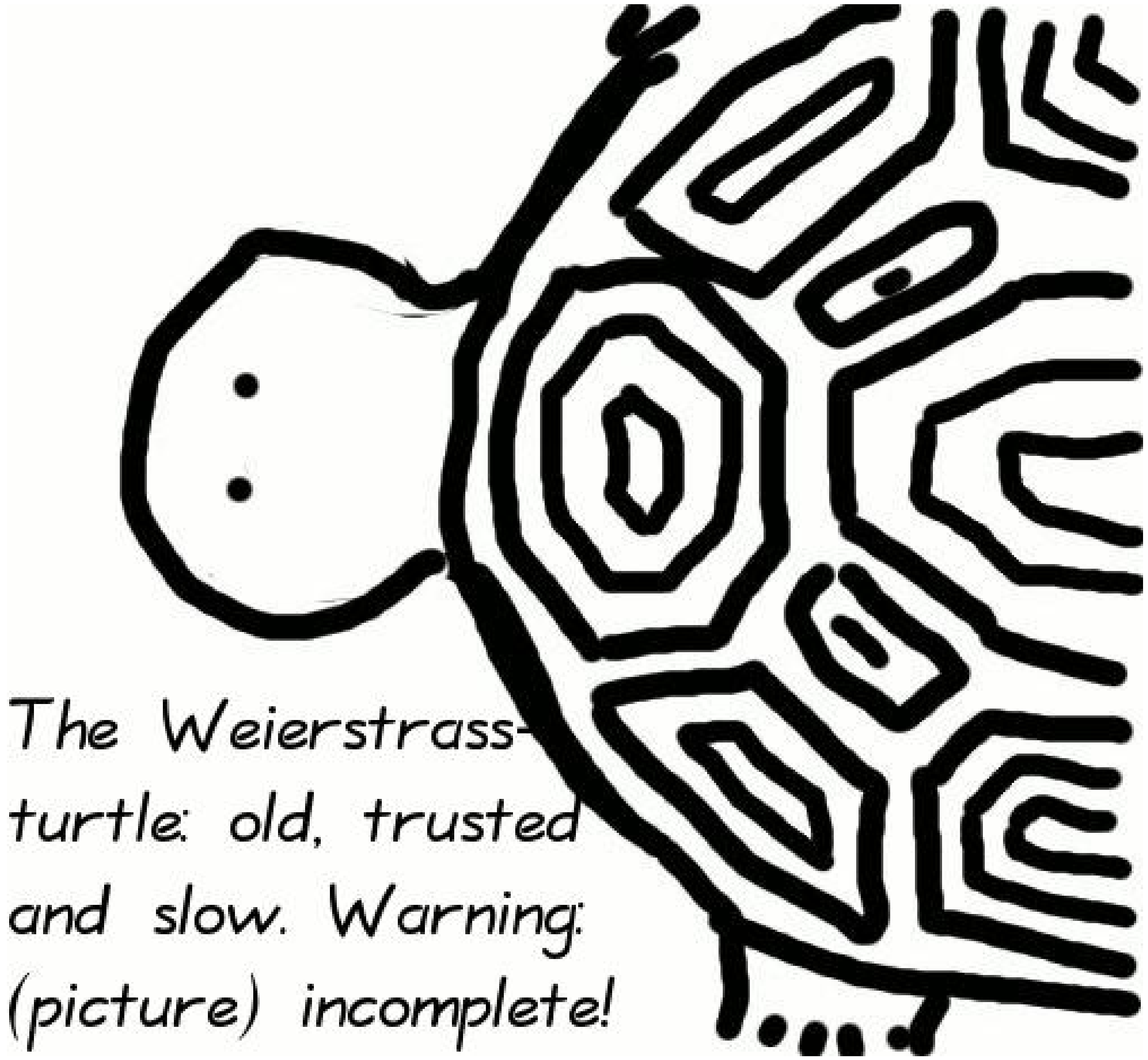


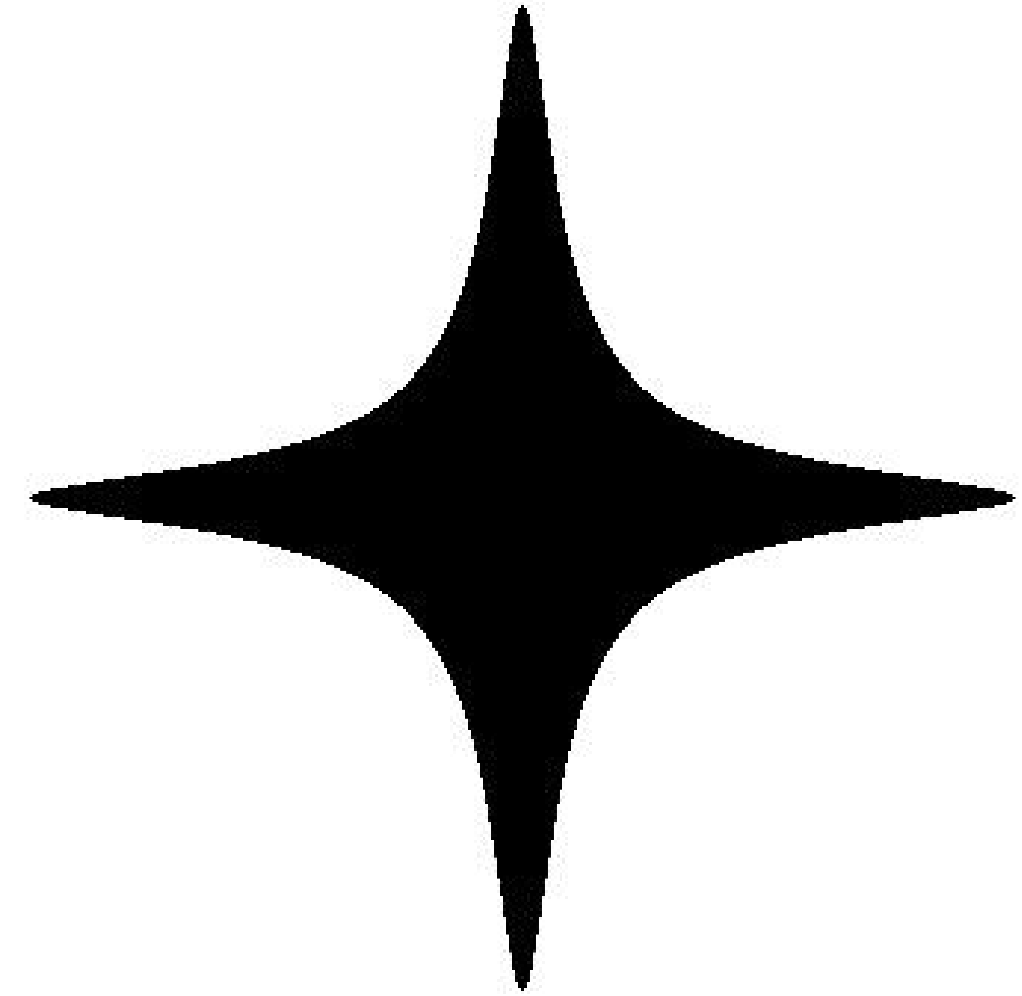
0.7


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

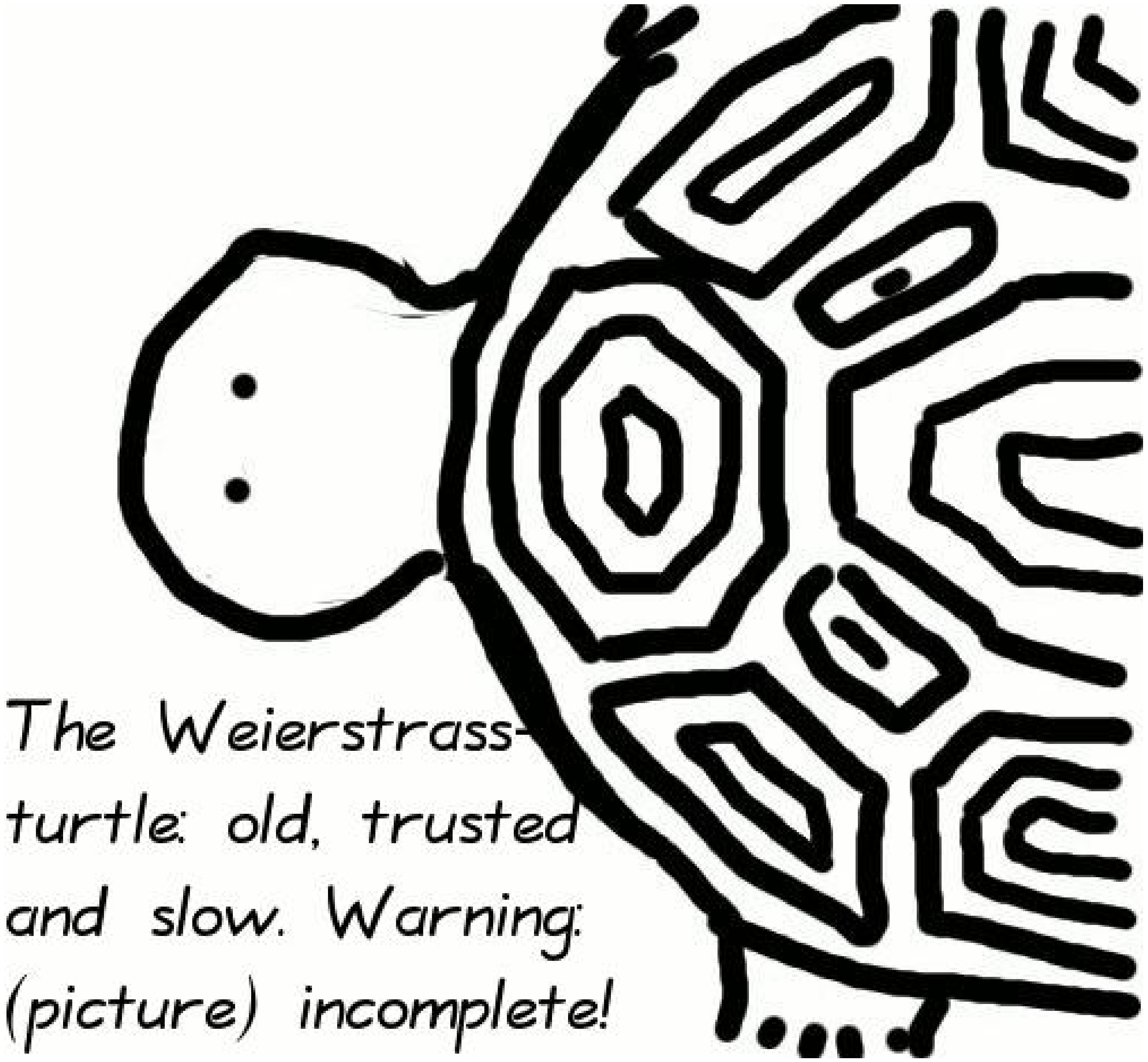


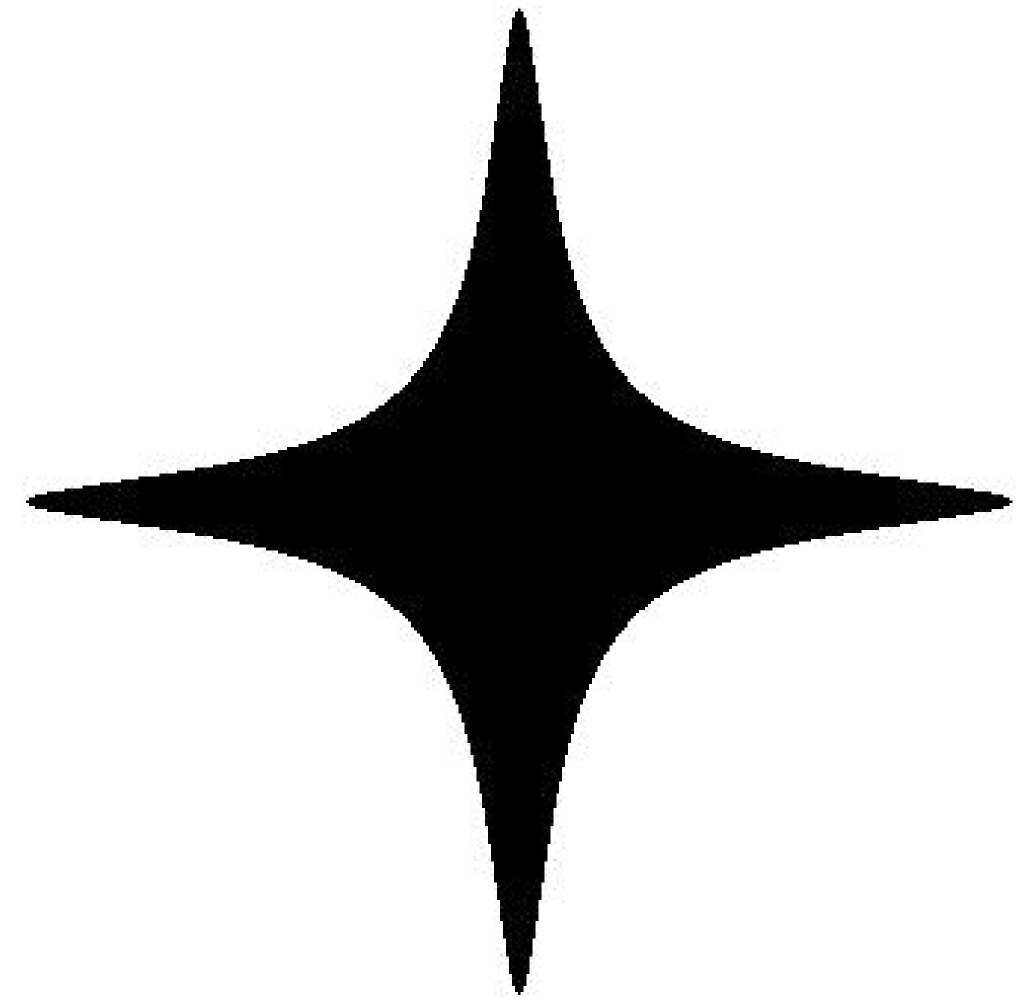
$x^2 + y^2 = 1 - 300$





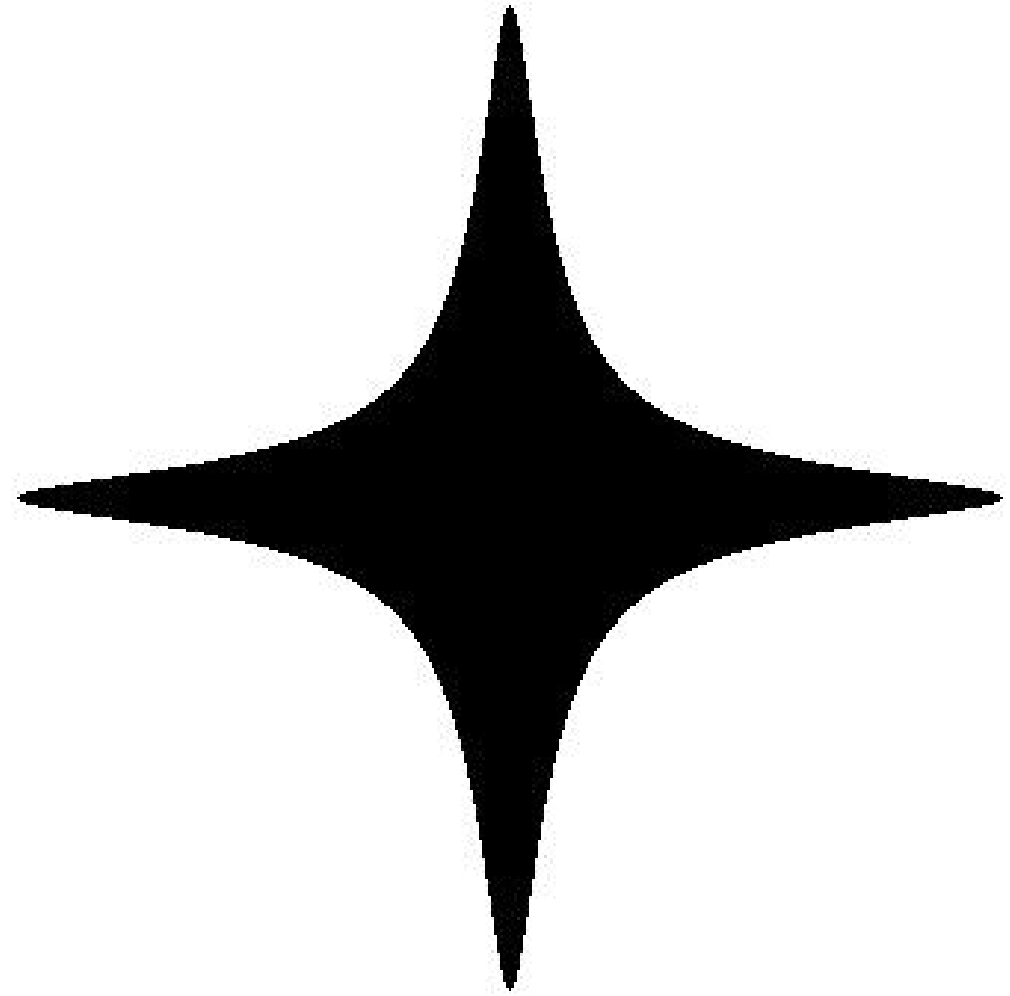
$$x^2 + y^2 = 1 - 300x^2y^2$$



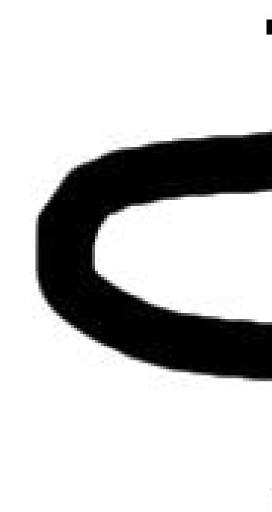


$$x^2 + y^2 = 1 - 300x^2y^2$$

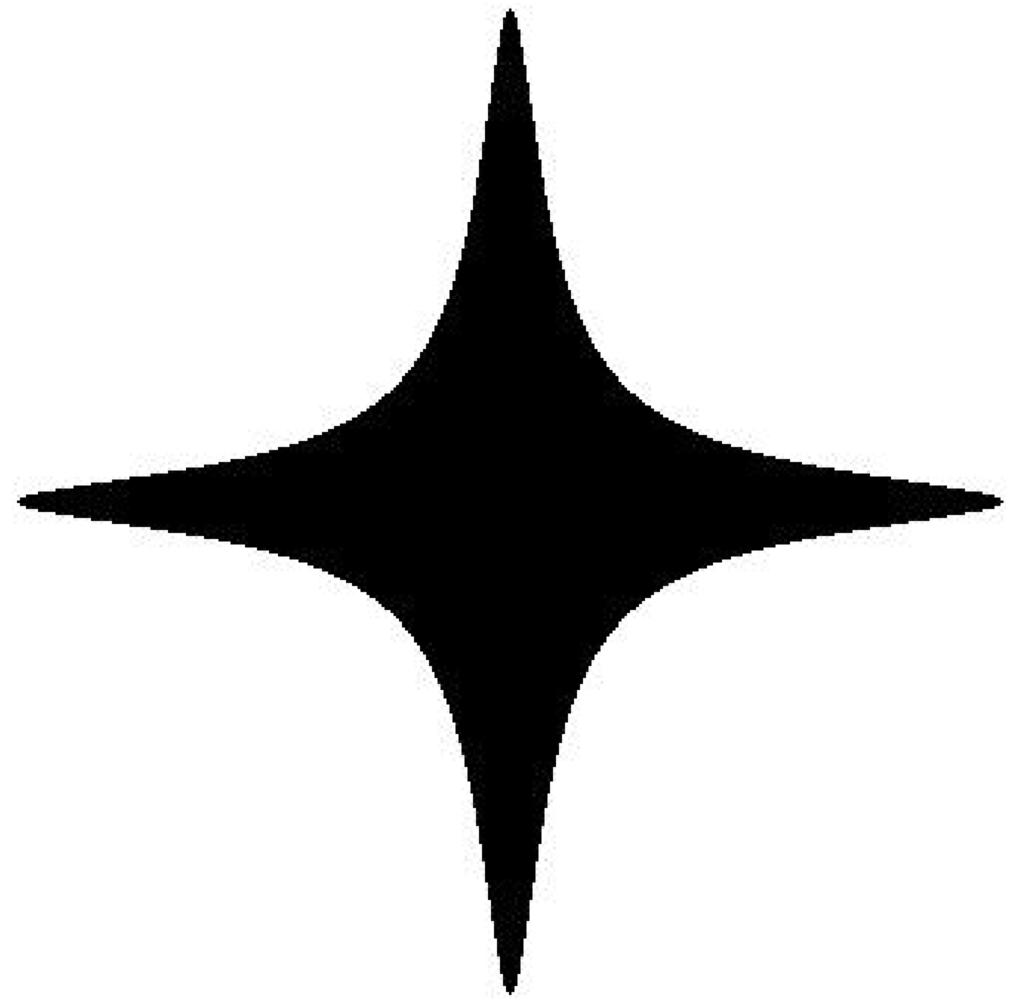
ierstrass-
ld, trusted
v. Warning:
incomplete!



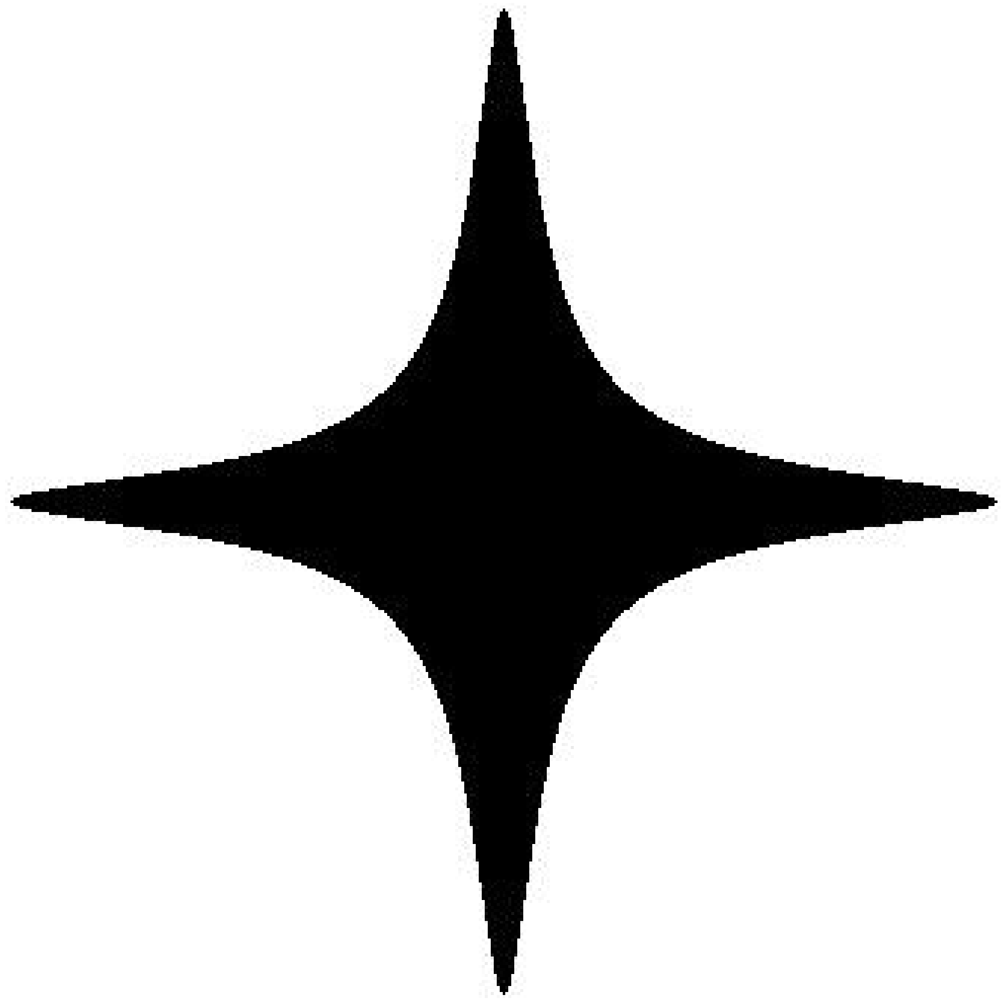
$$x^2 + y^2 = 1 - 300x^2y^2$$



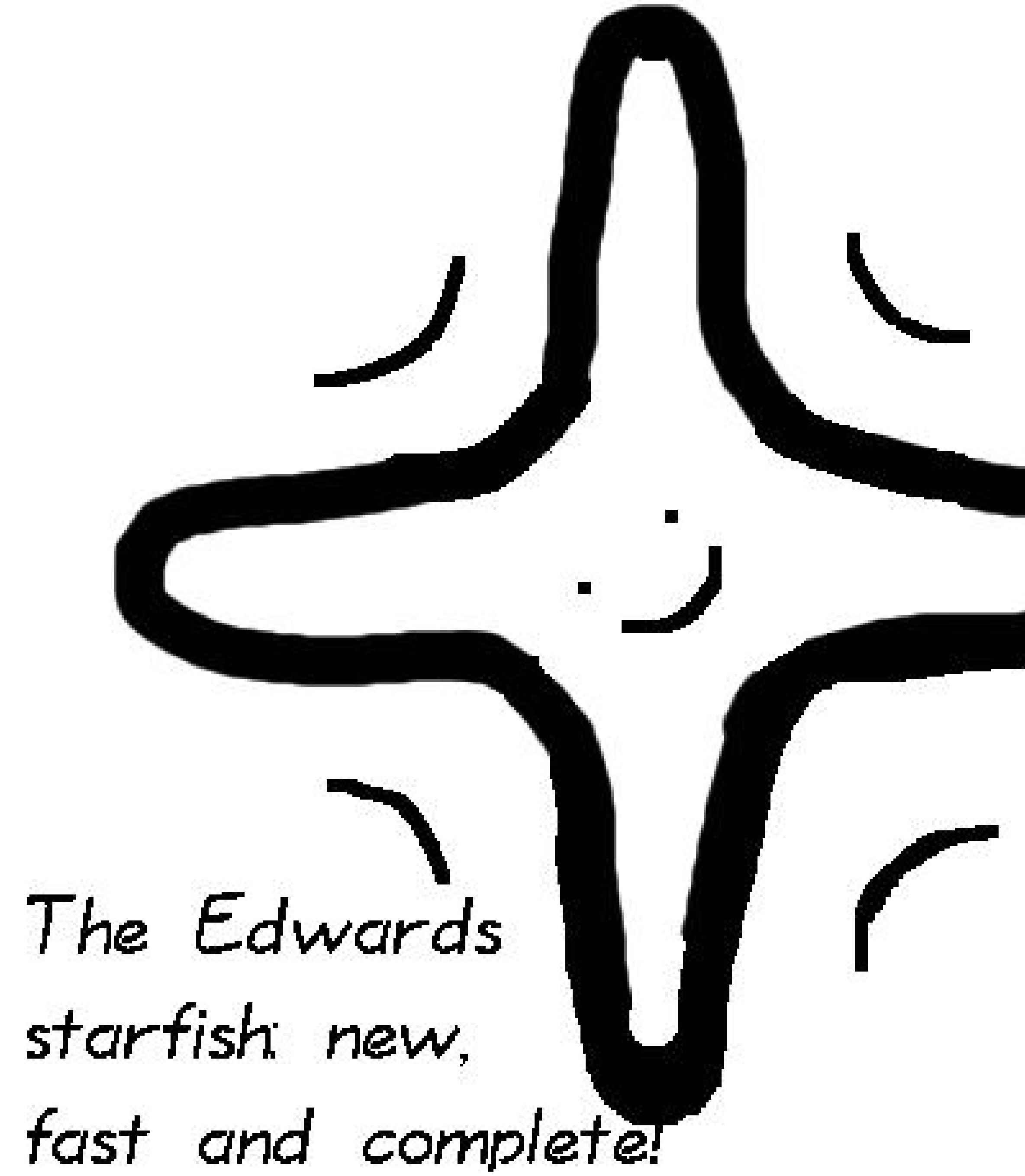
The Edv
starfish:
fast and

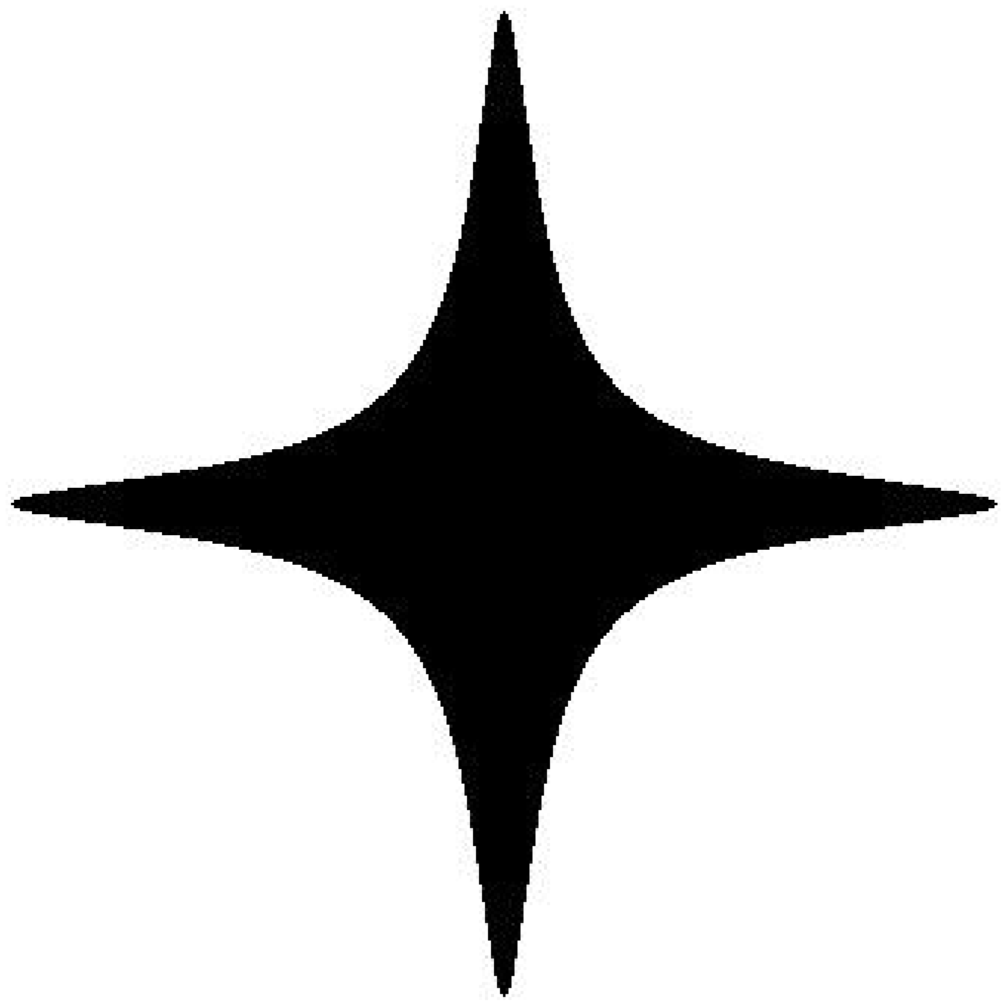


$$x^2 + y^2 = 1 - 300x^2y^2$$

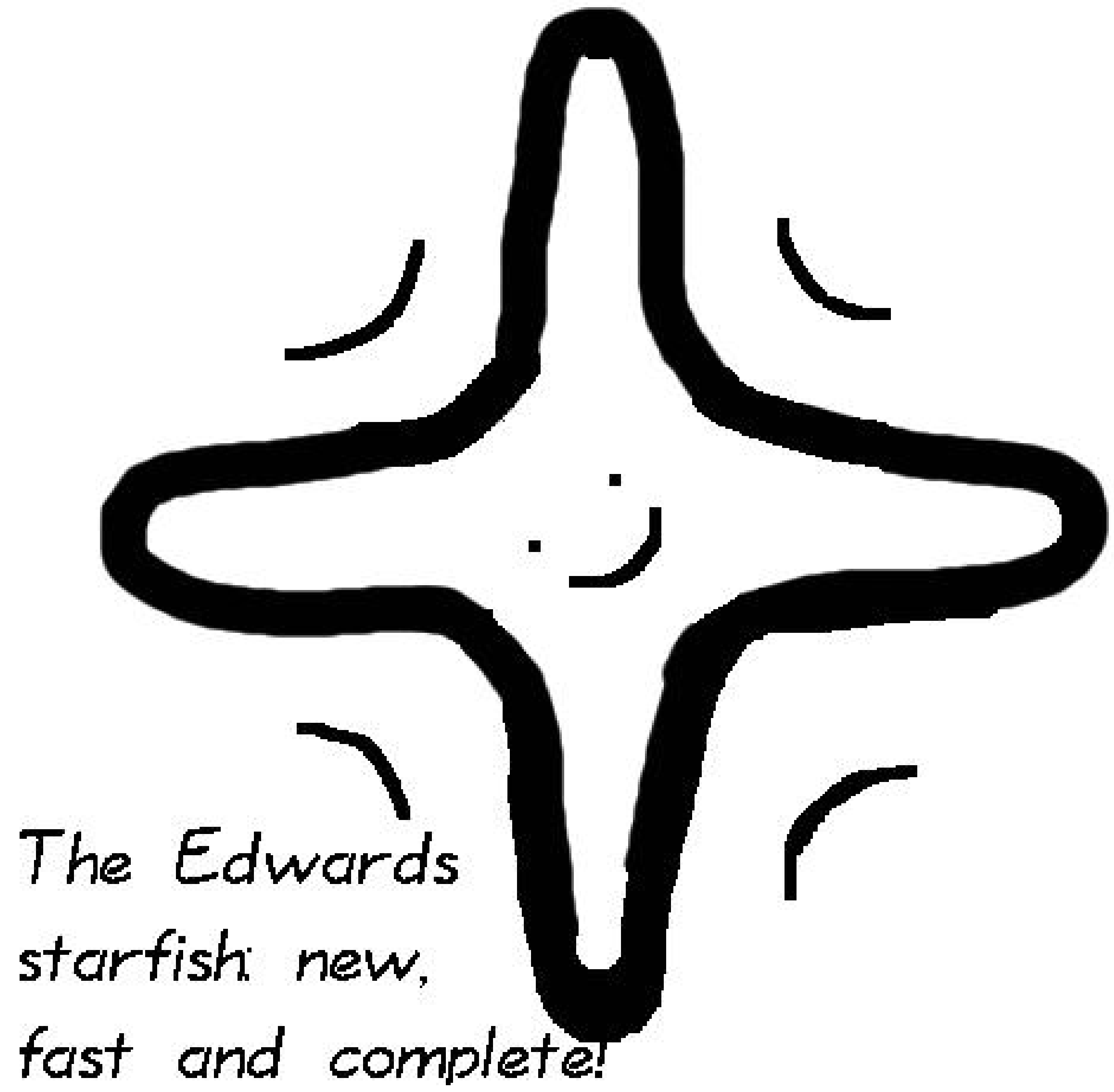


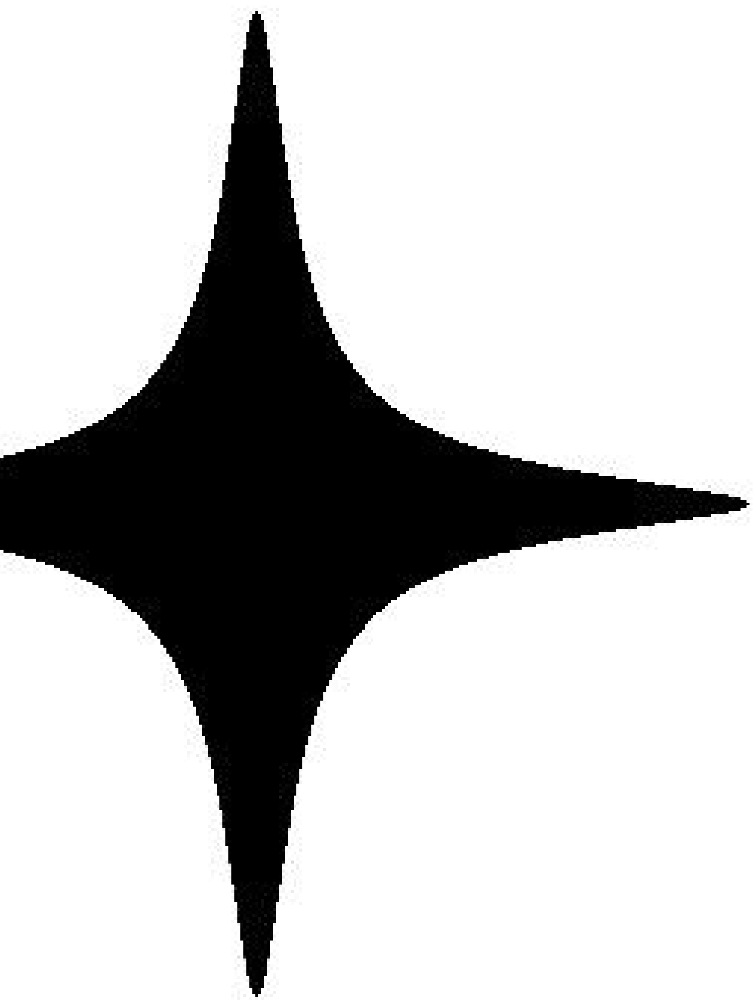
$$x^2 + y^2 = 1 - 300x^2y^2$$



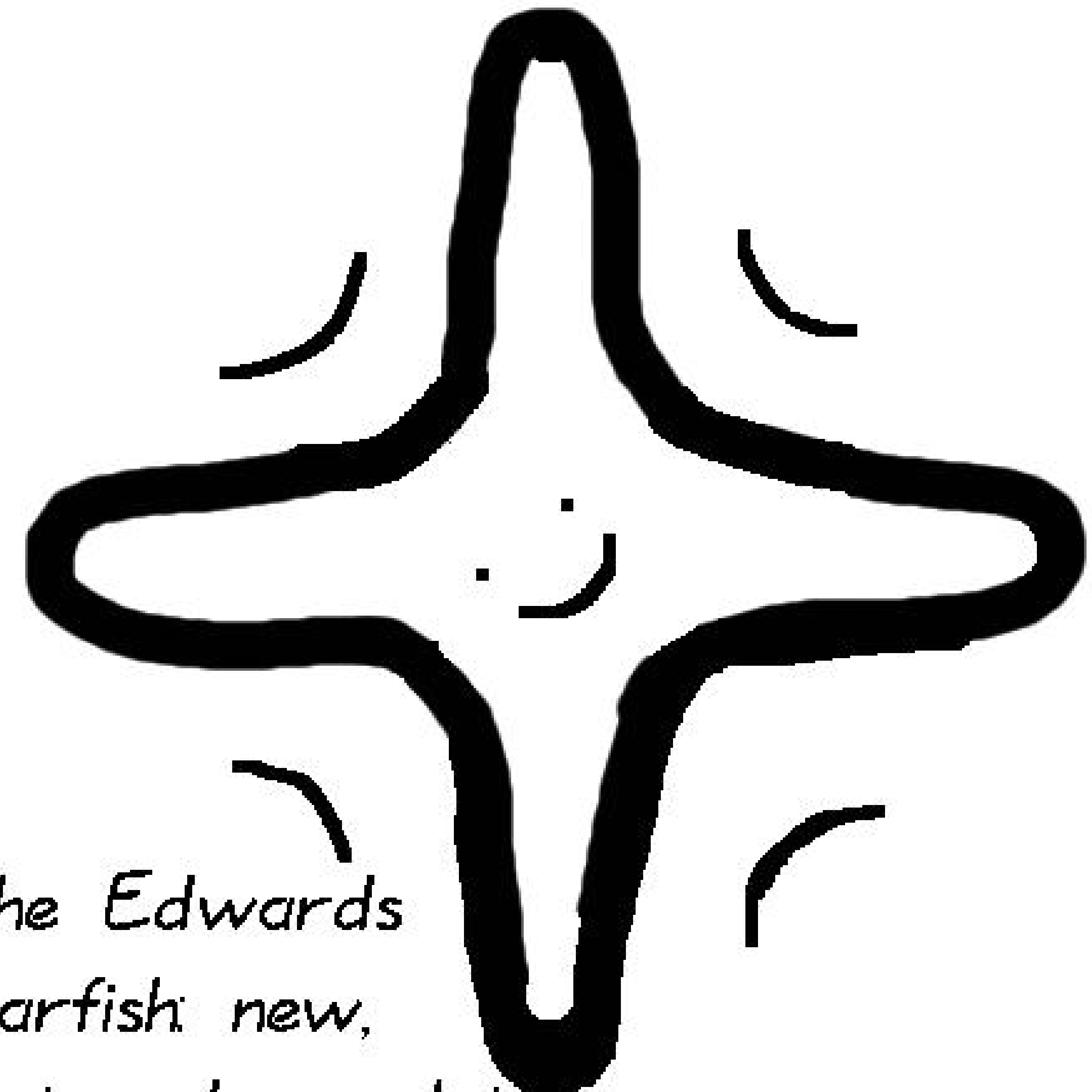


$$x^2 + y^2 = 1 - 300x^2y^2$$

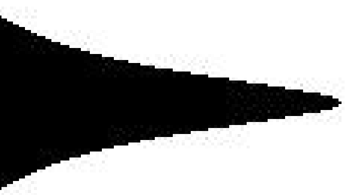




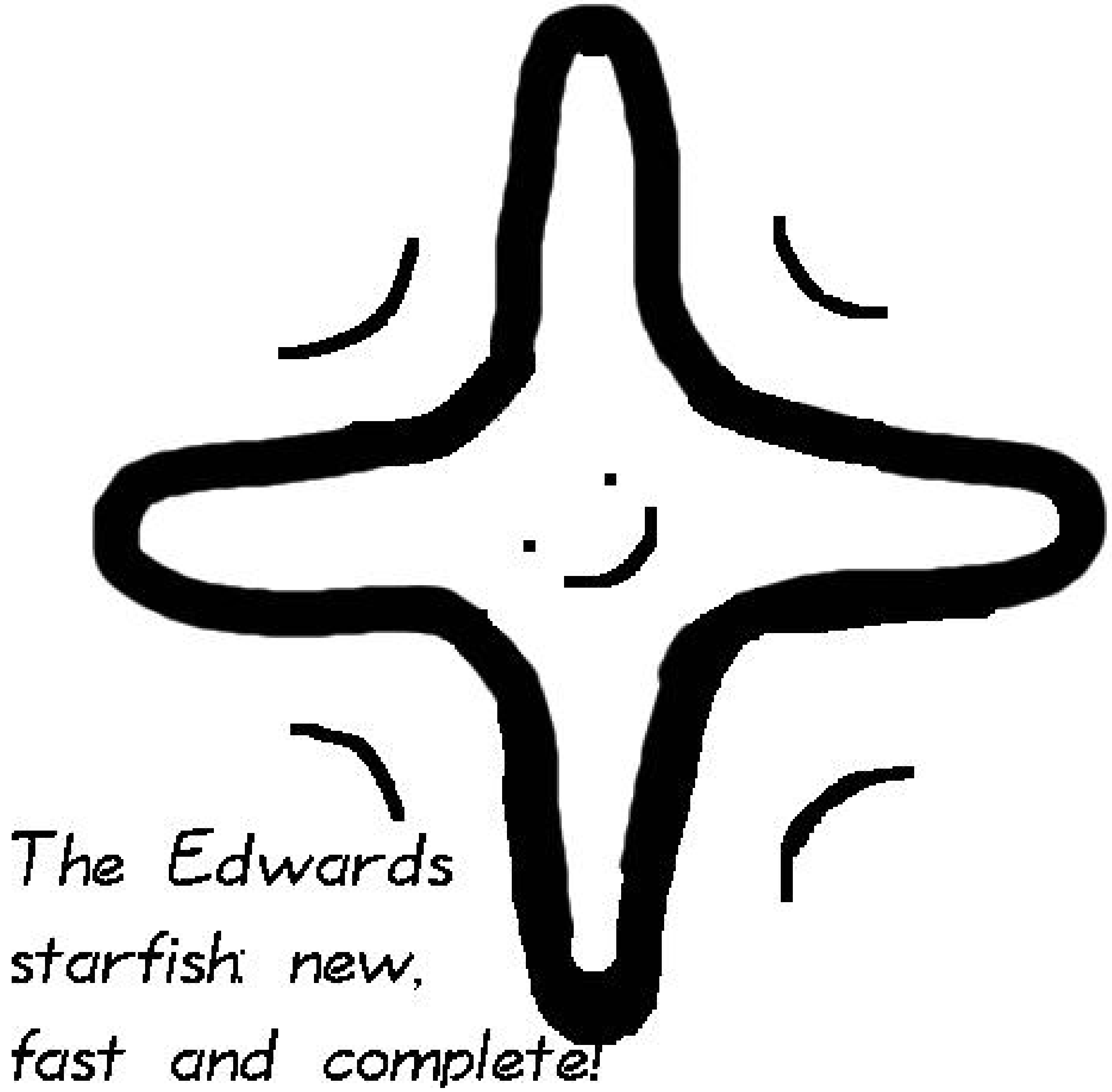
$= 1 - 300x^2y^2$

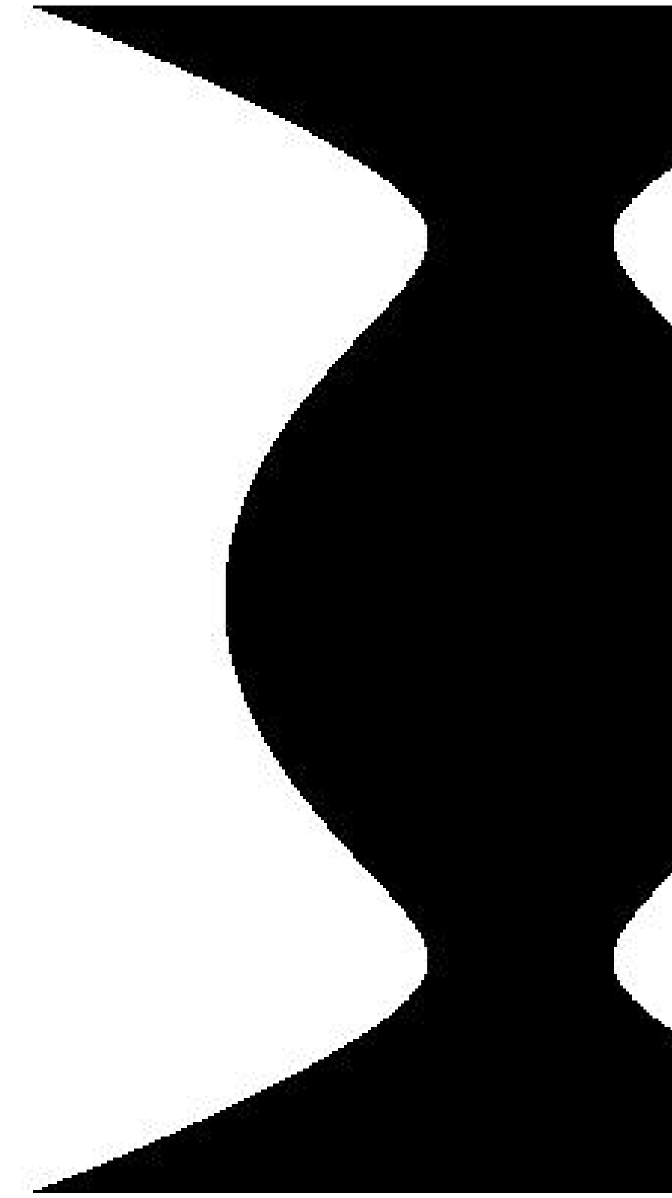


$x^2 = y^4$

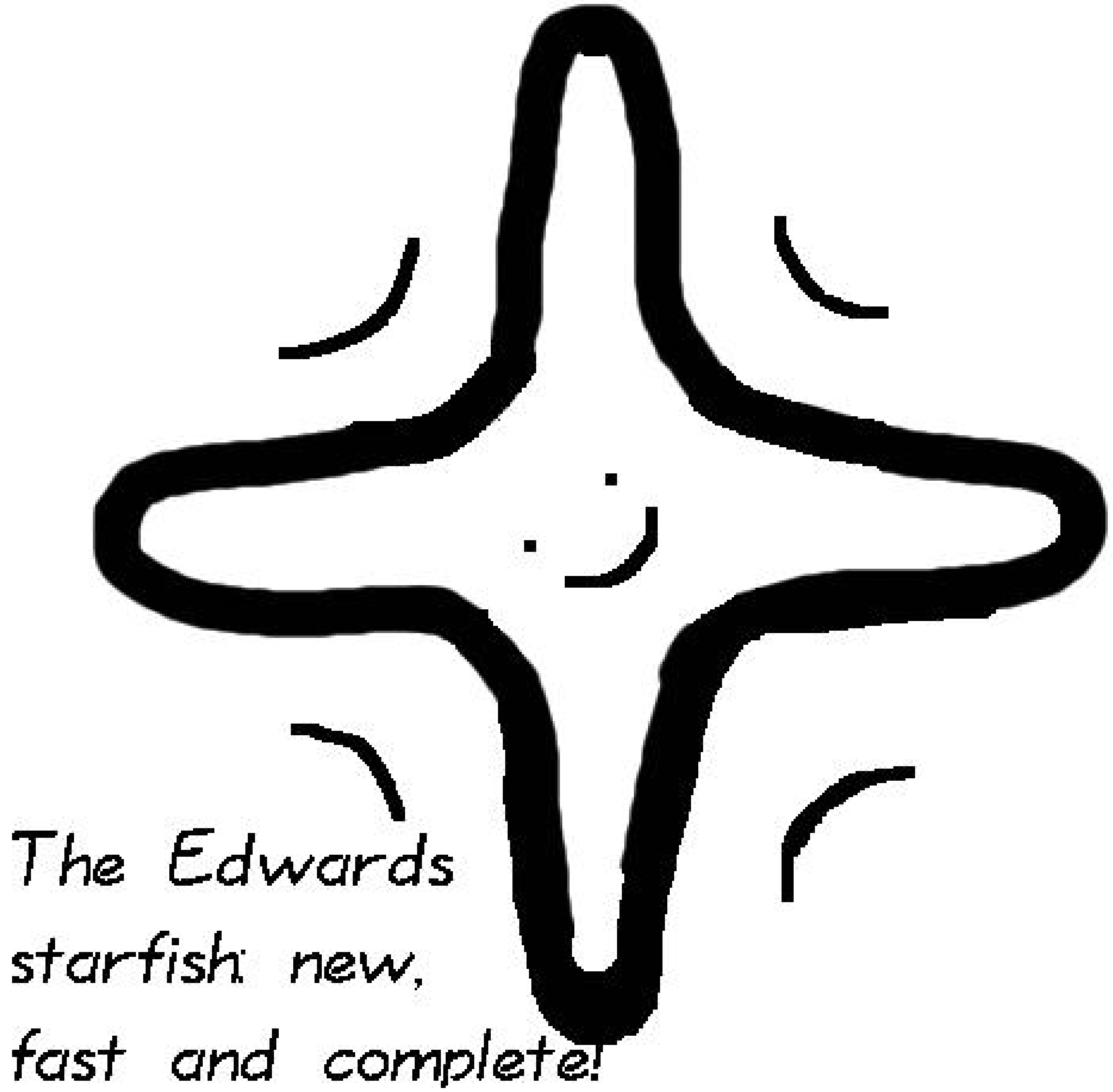


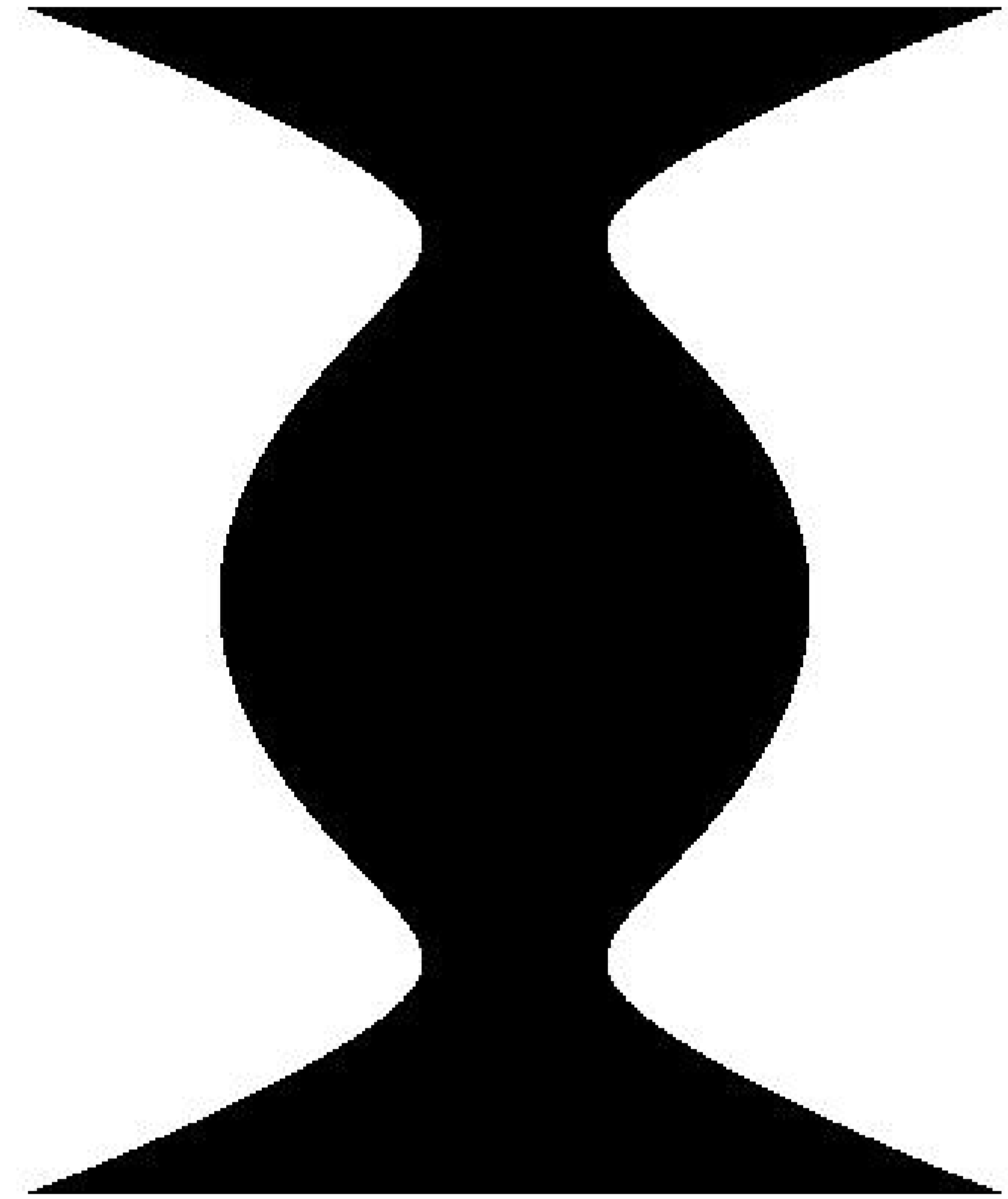
$0x^2y^2$



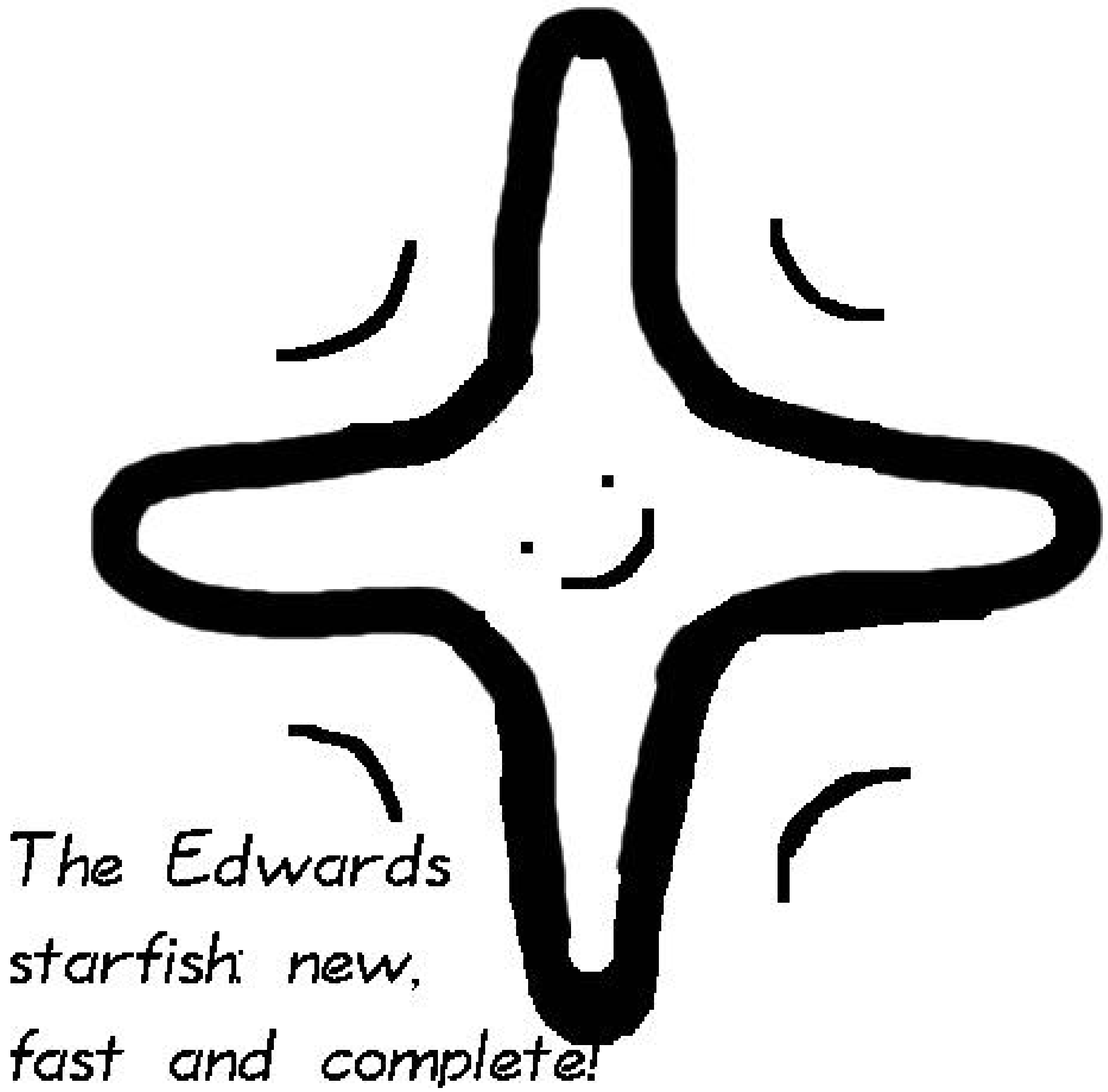


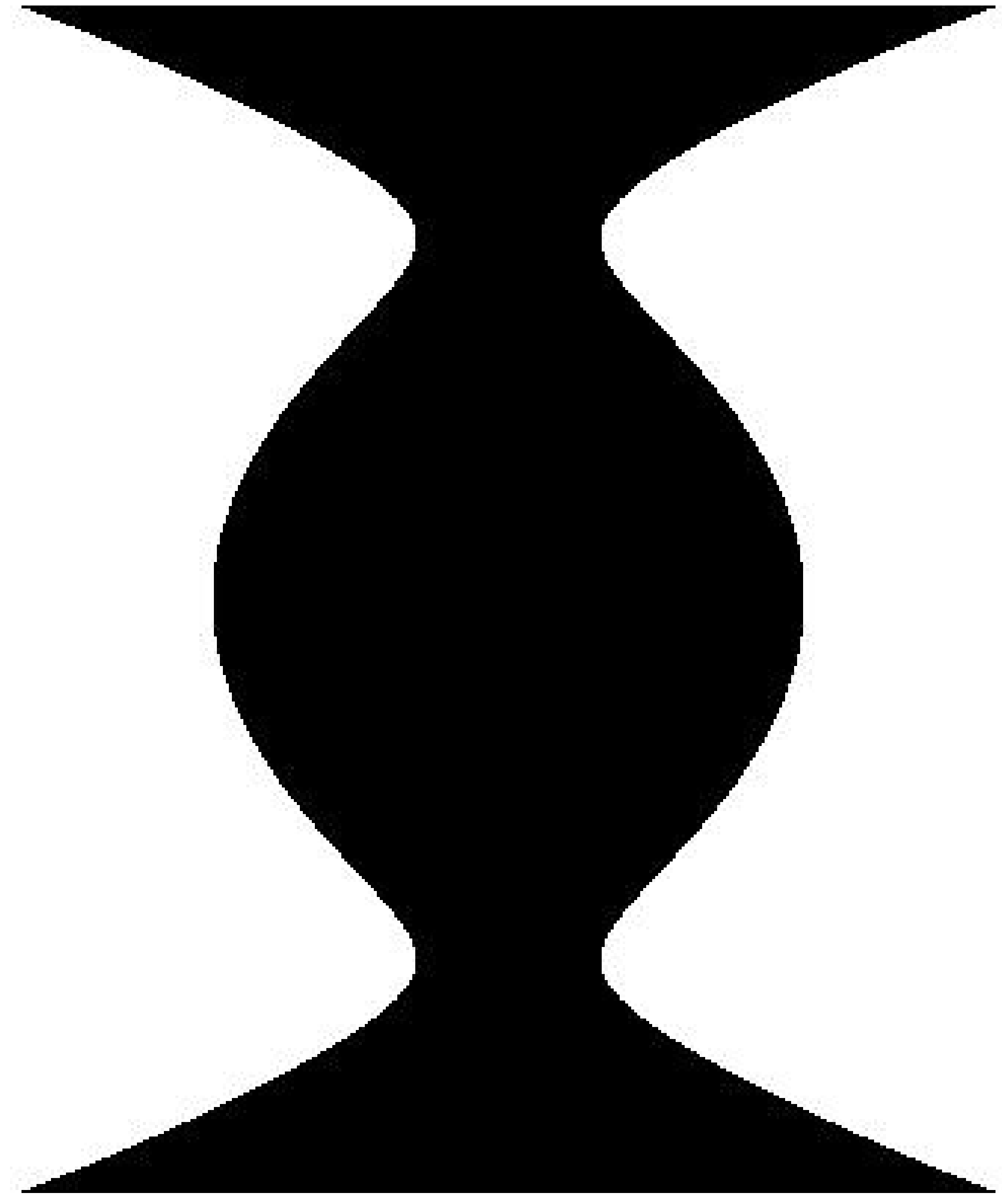
$x^2 = y^4 - 1.9y^2 +$



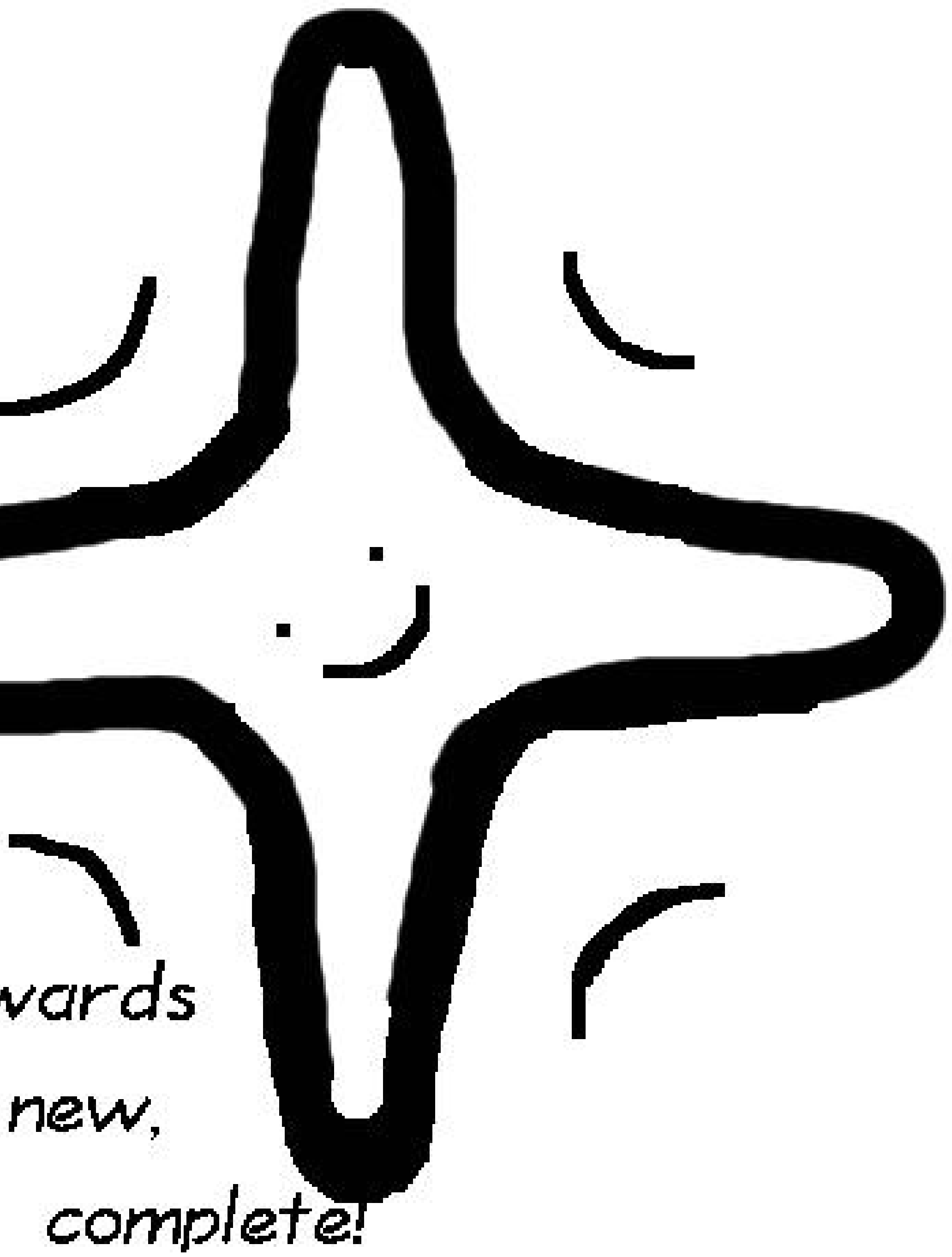


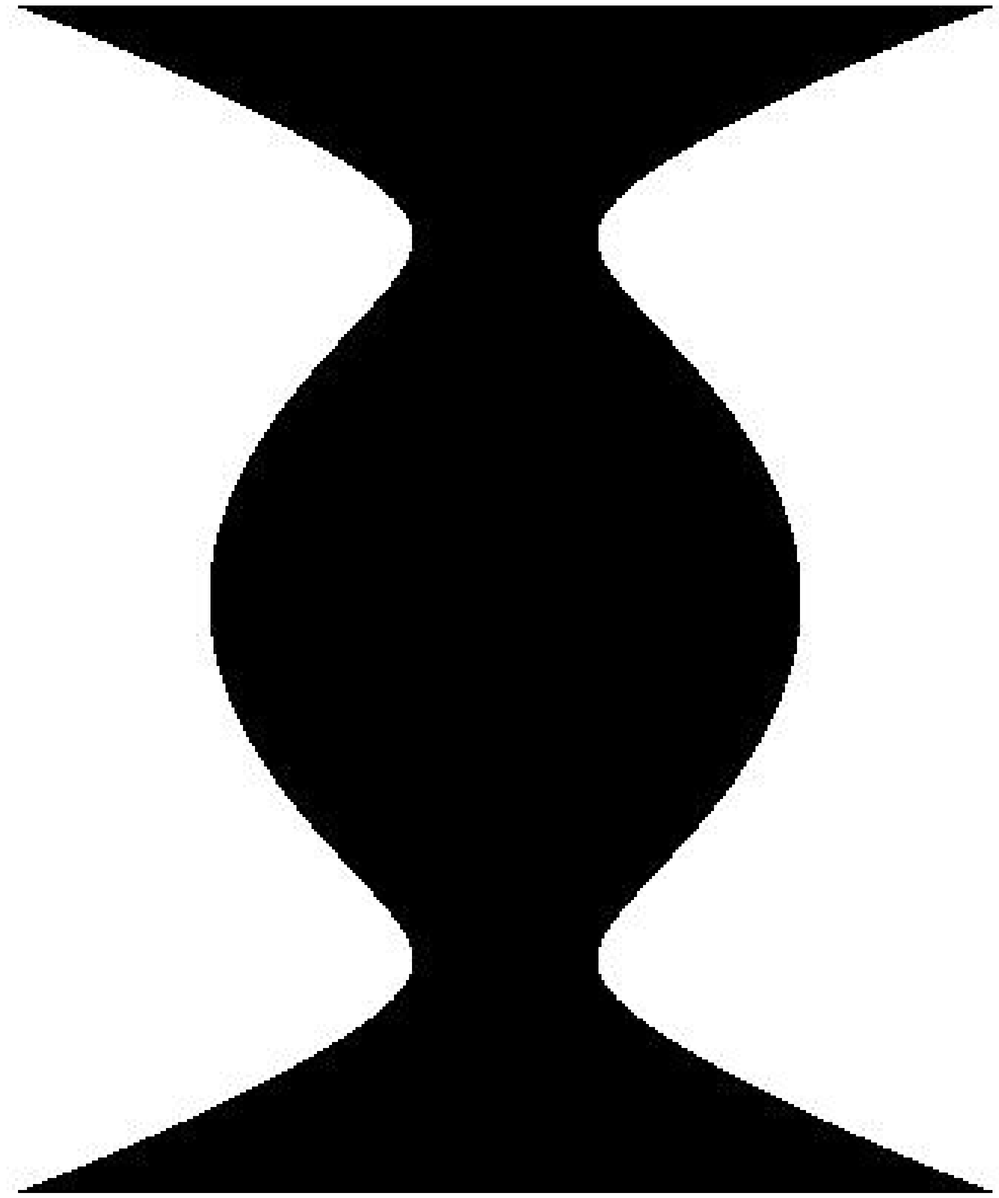
$$x^2 = y^4 - 1.9y^2 + 1$$





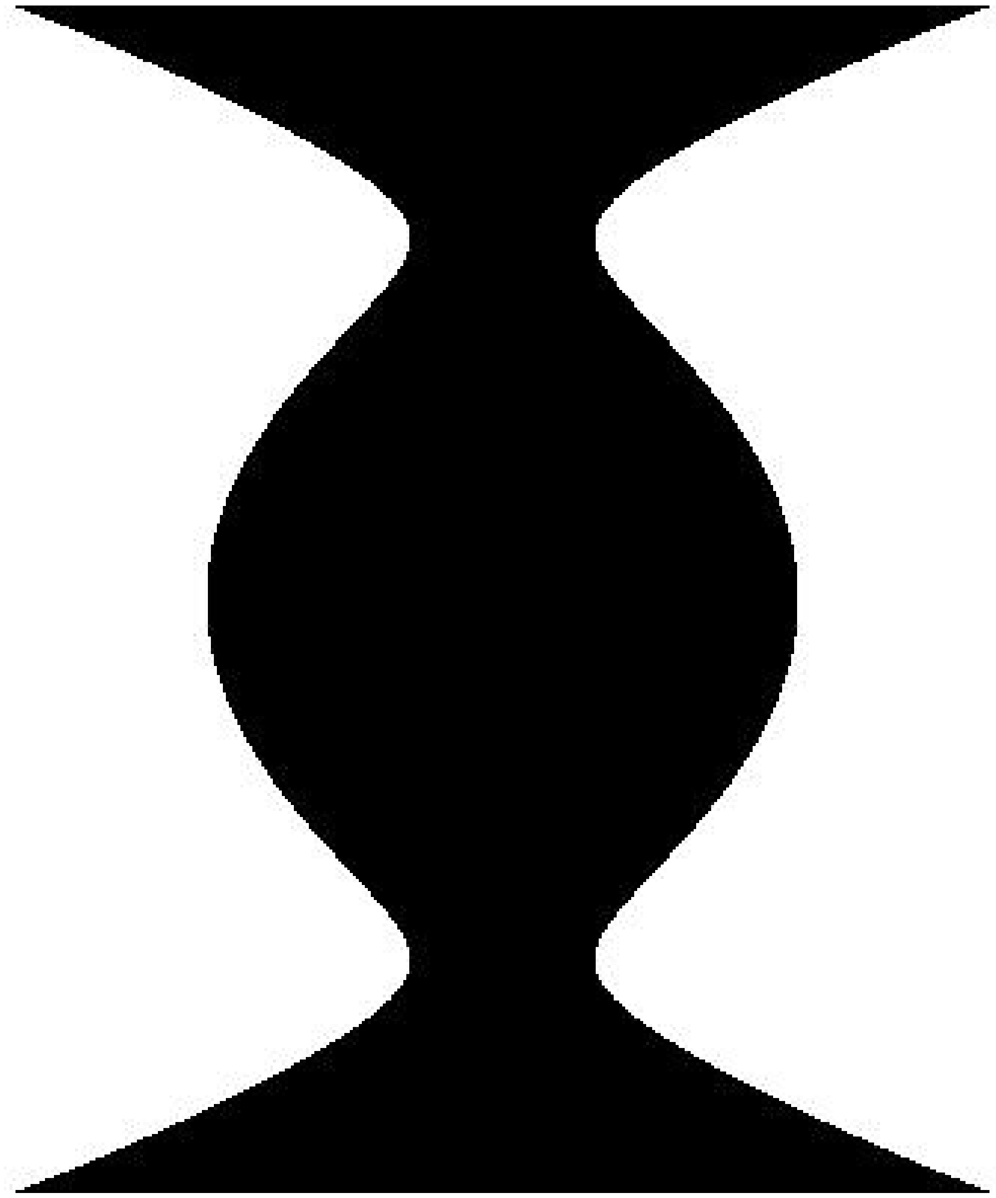
$x^2 = y^4 - 1.9y^2 + 1$





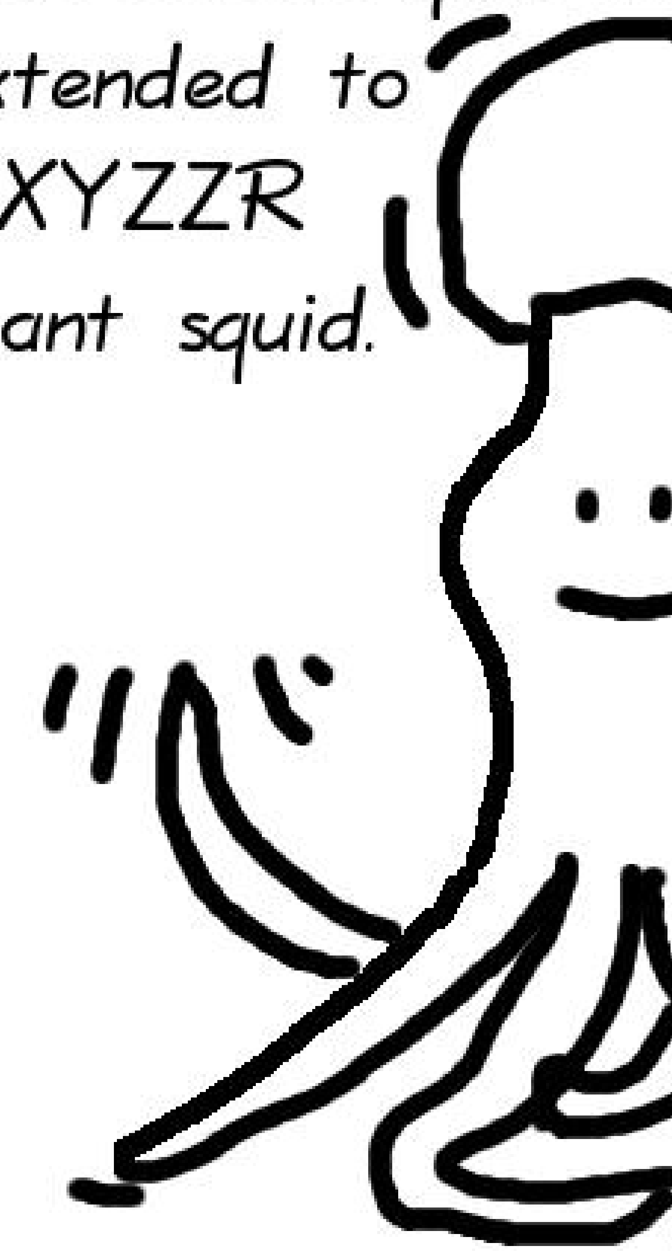
$$x^2 = y^4 - 1.9y^2 + 1$$

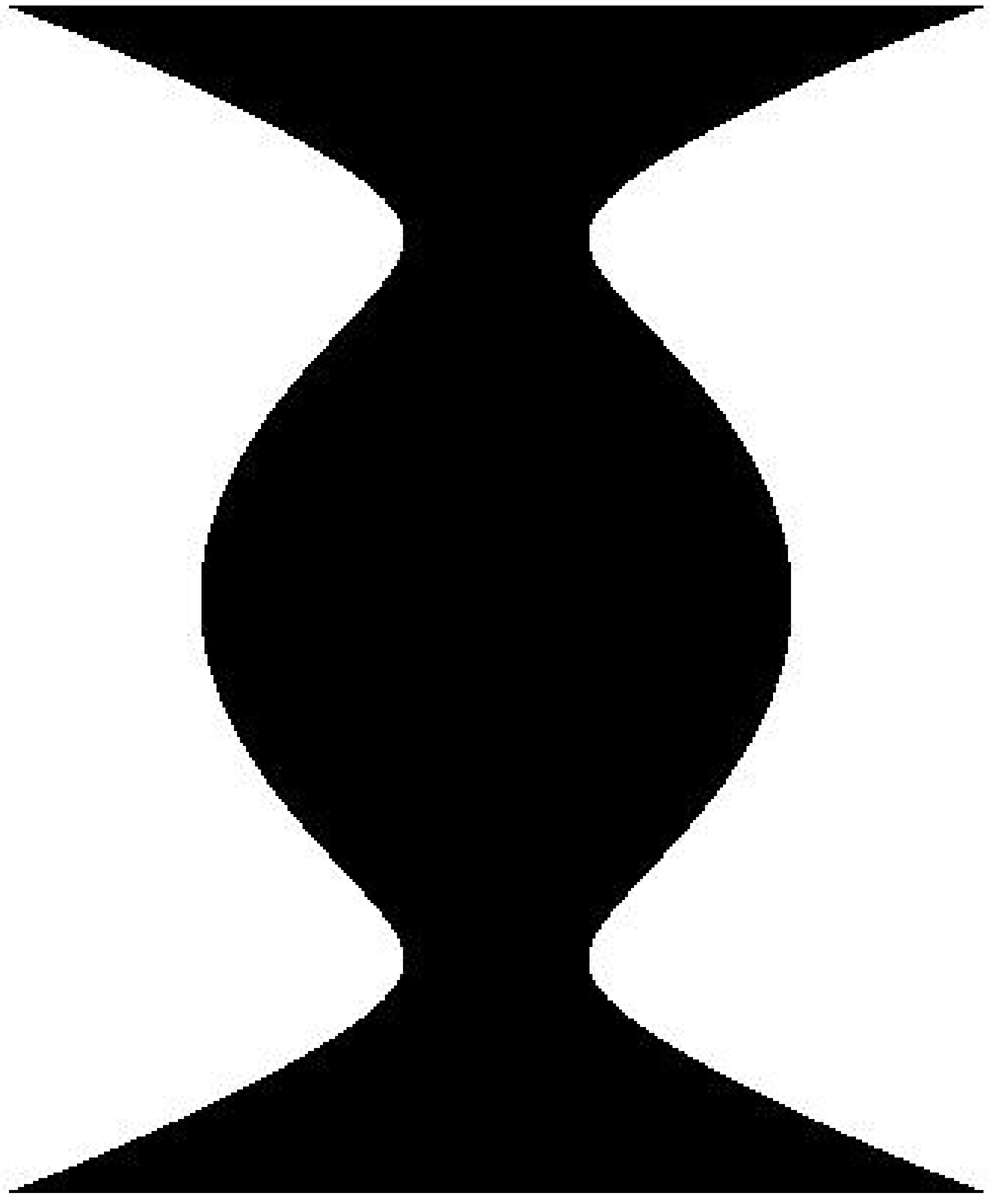
The Jac
extended
XXYZZ
giant sq



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

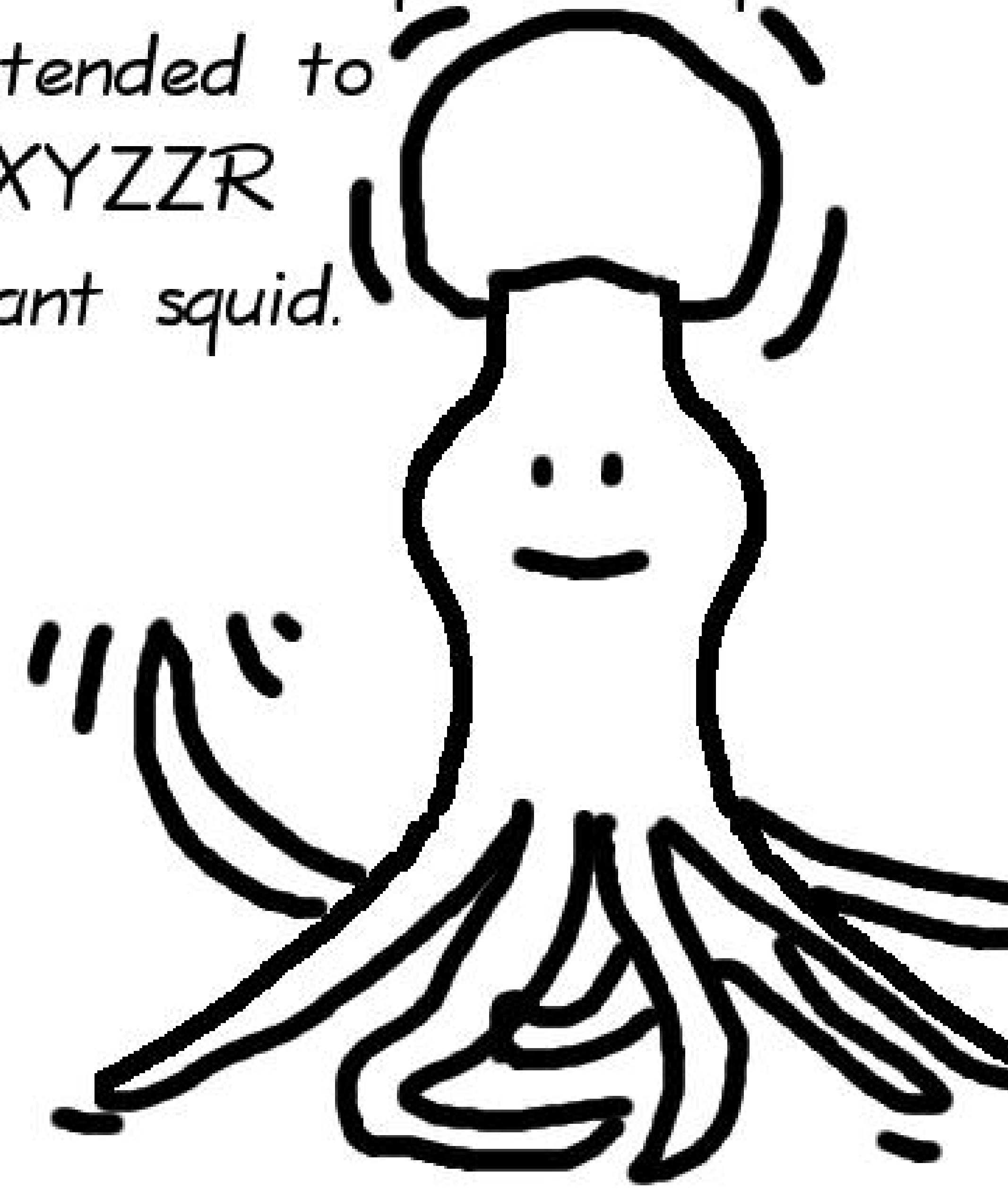
The Jacobi-quartic
extended to
XXYZZR
giant squid.

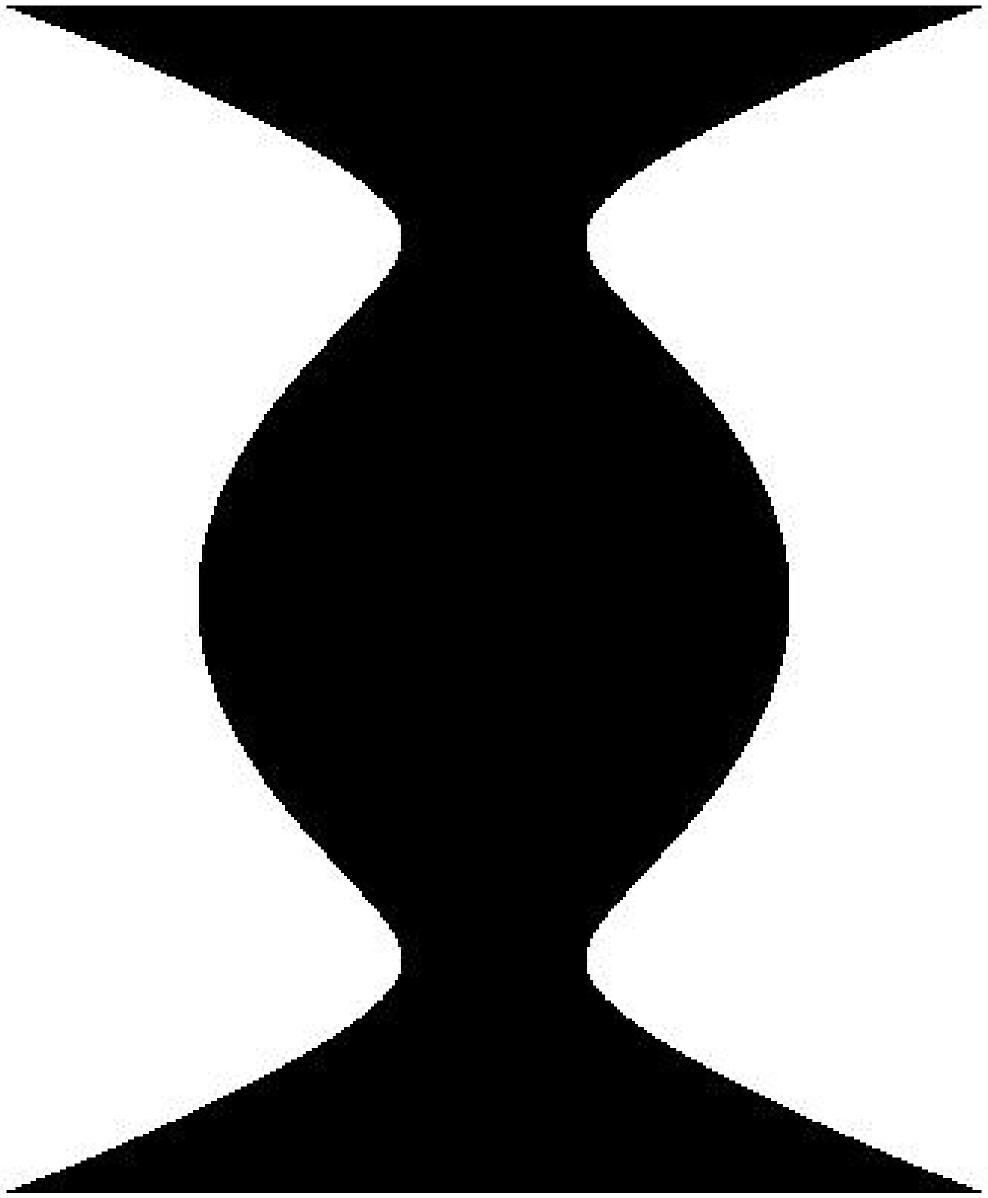




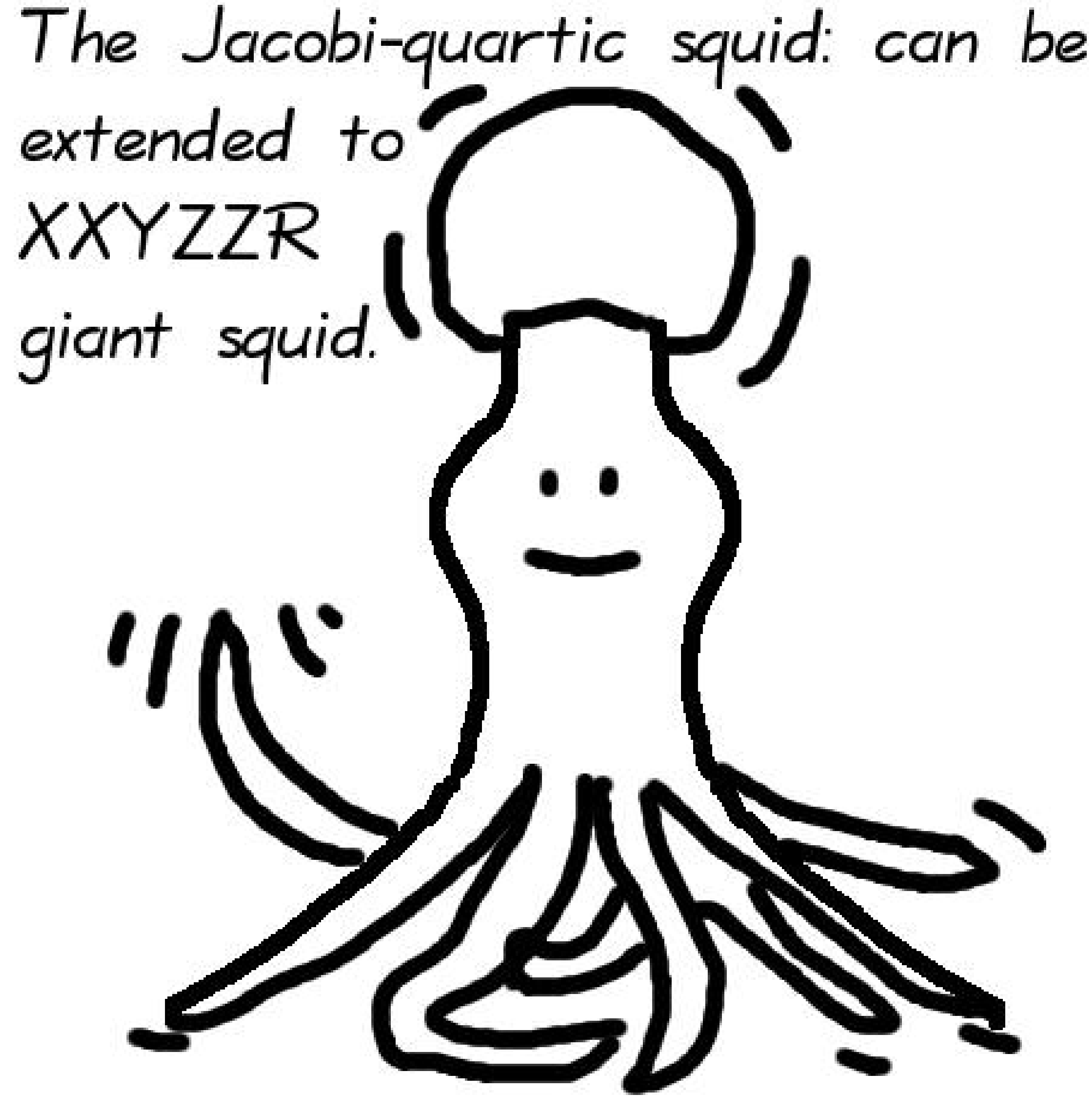
$$x^2 = y^4 - 1.9y^2 + 1$$

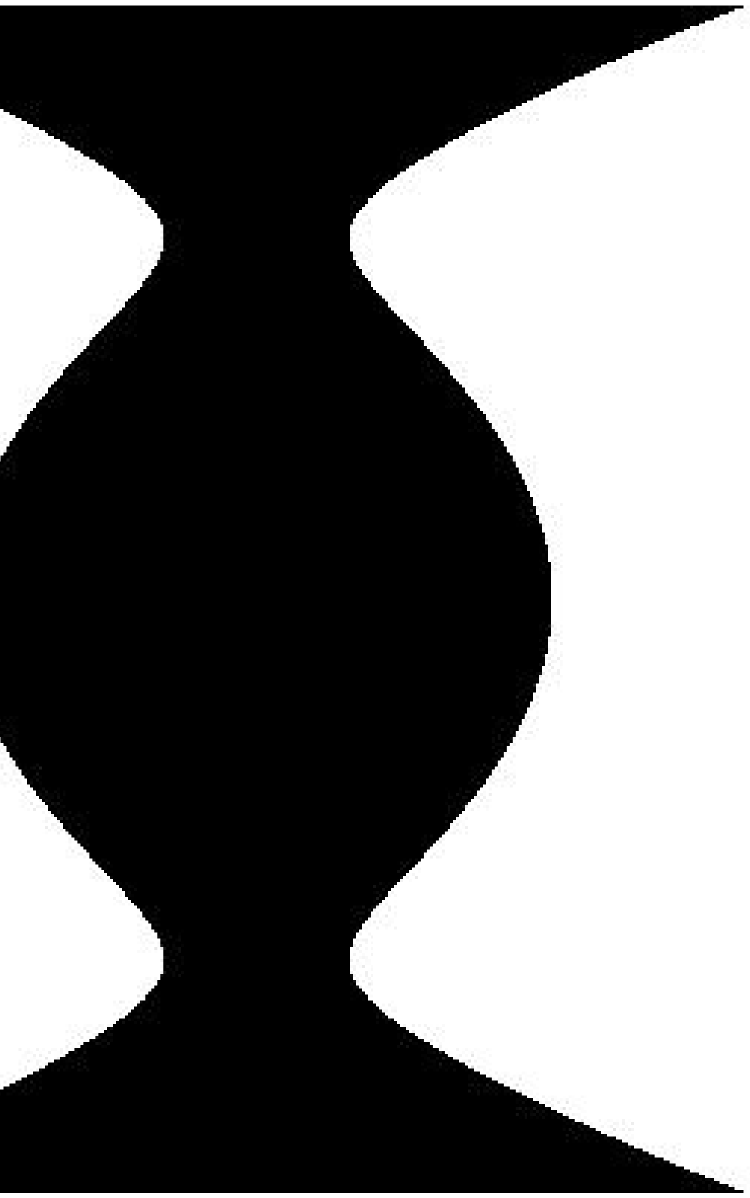
The Jacobi-quartic squid: ca
extended to
XXYZZR
giant squid.



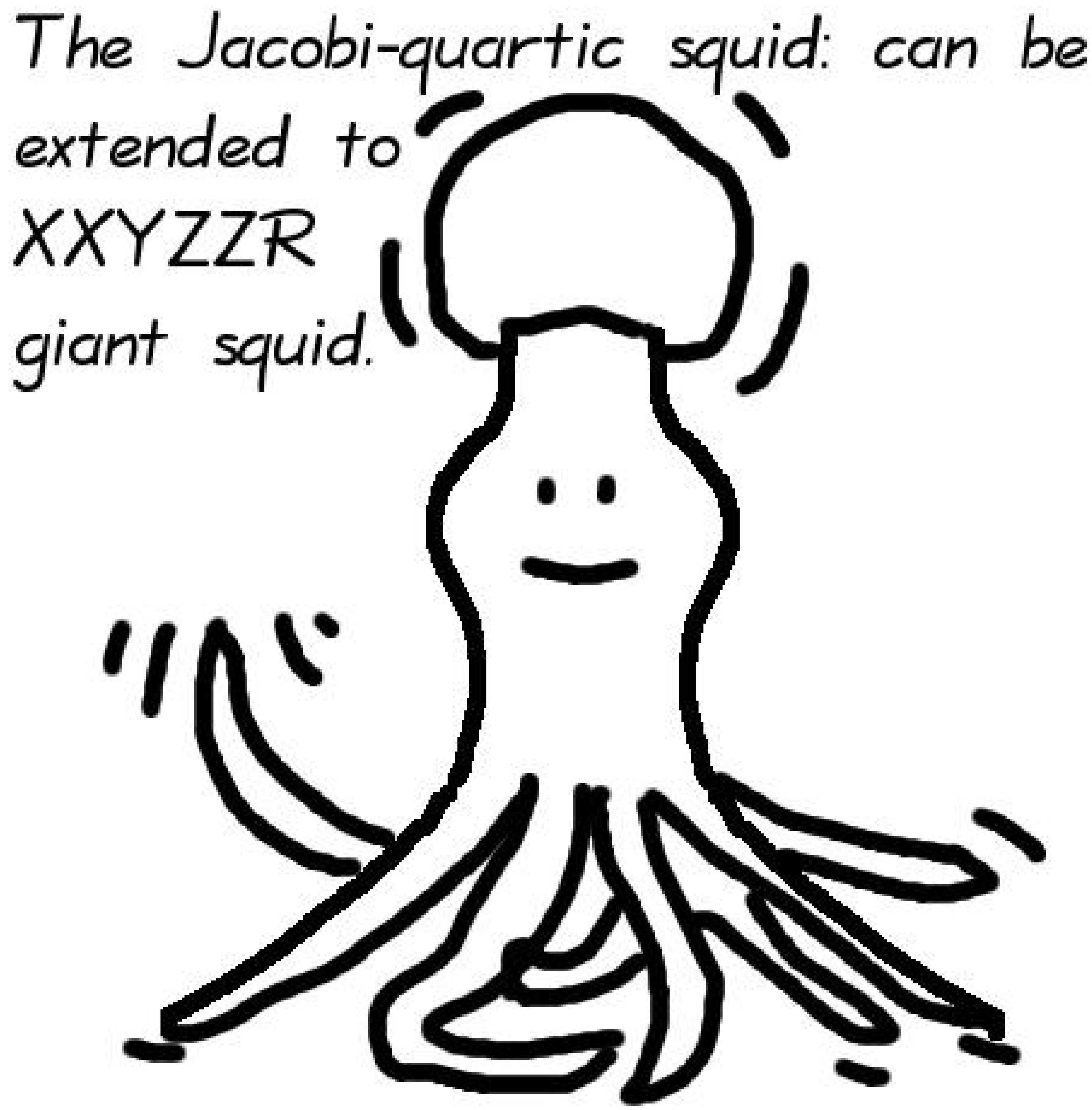


$x^2 = y^4 - 1.9y^2 + 1$

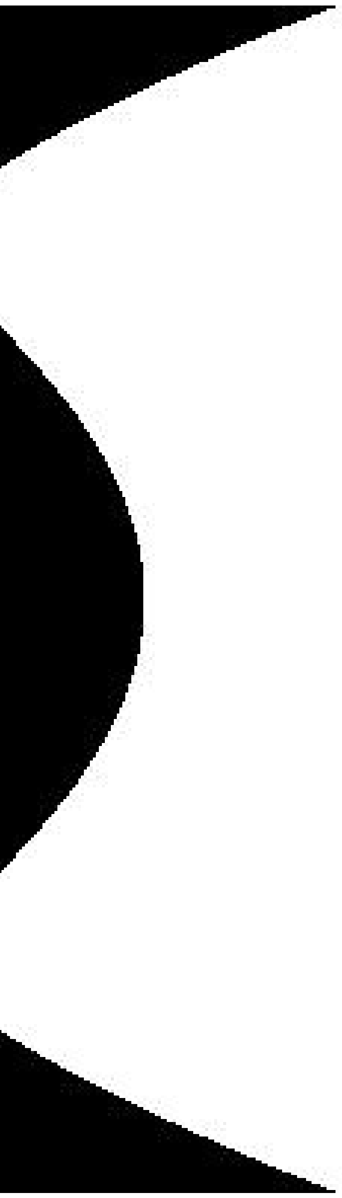

The Jacobi-quartic squid: can be extended to XXYZZR giant squid.



$- 1.9y^2 + 1$

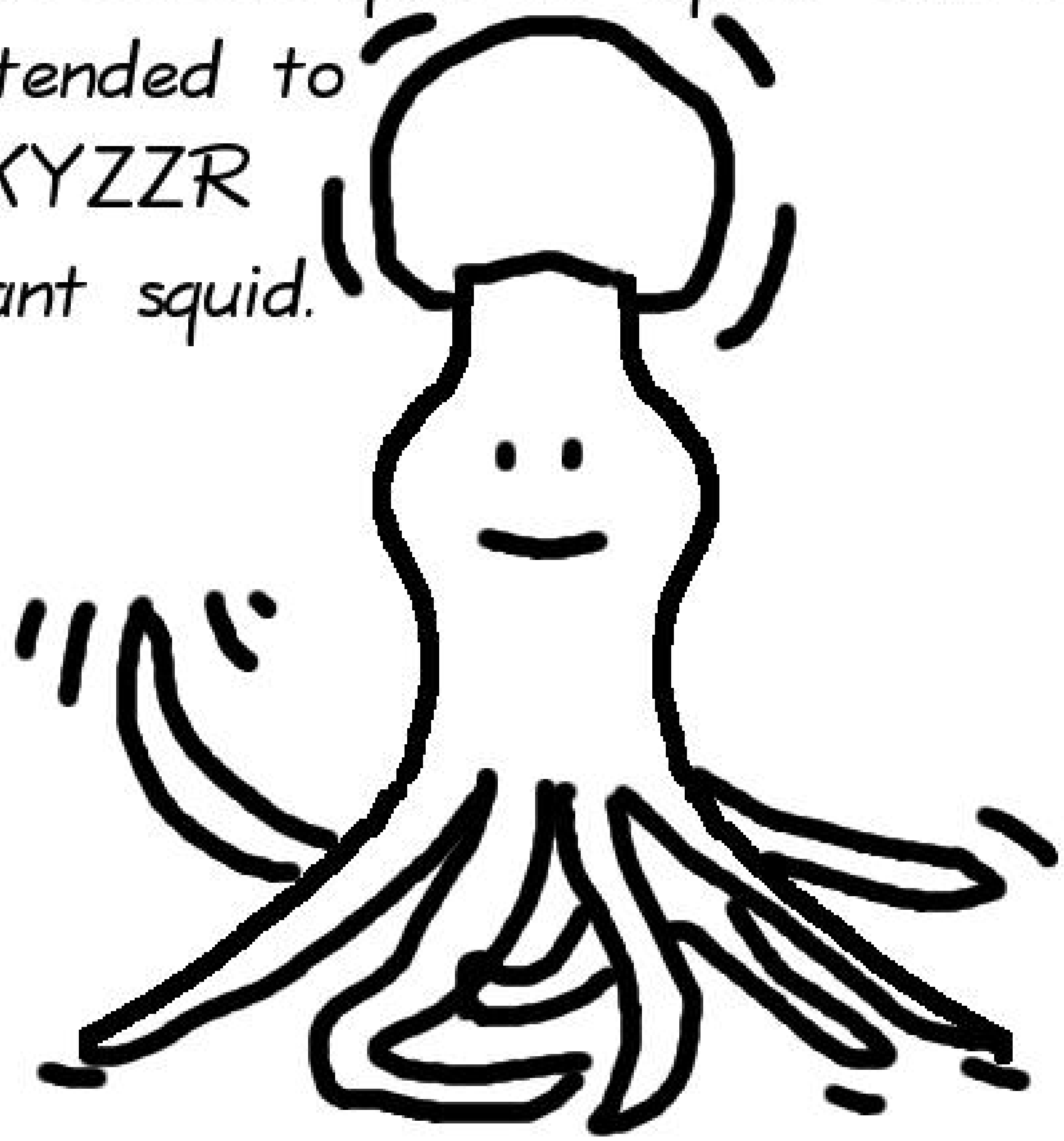

The Jacobi-quartic squid: can be
extended to
XXYZZR
giant squid.

$x^3 - y^3$



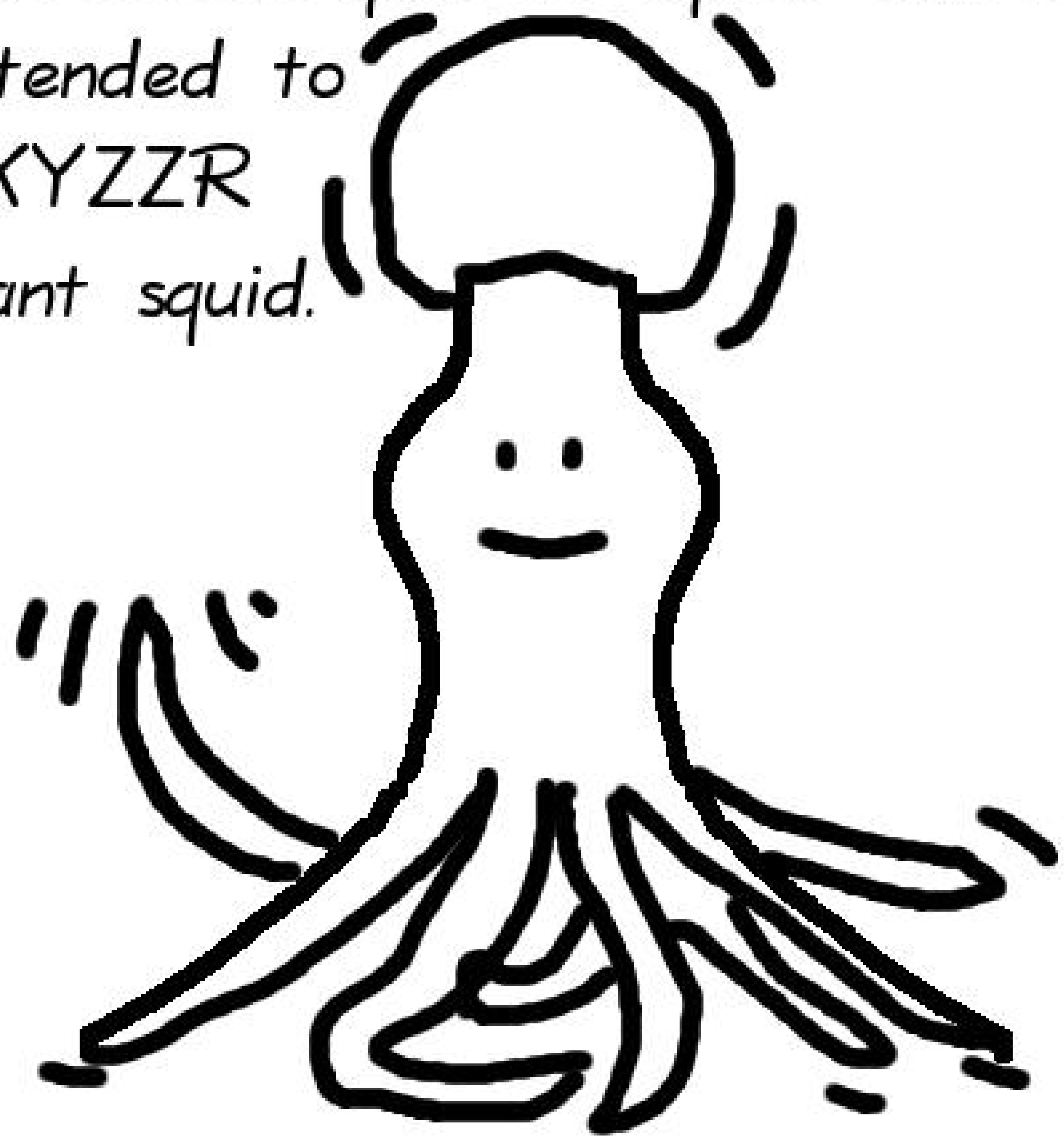
$- 1$

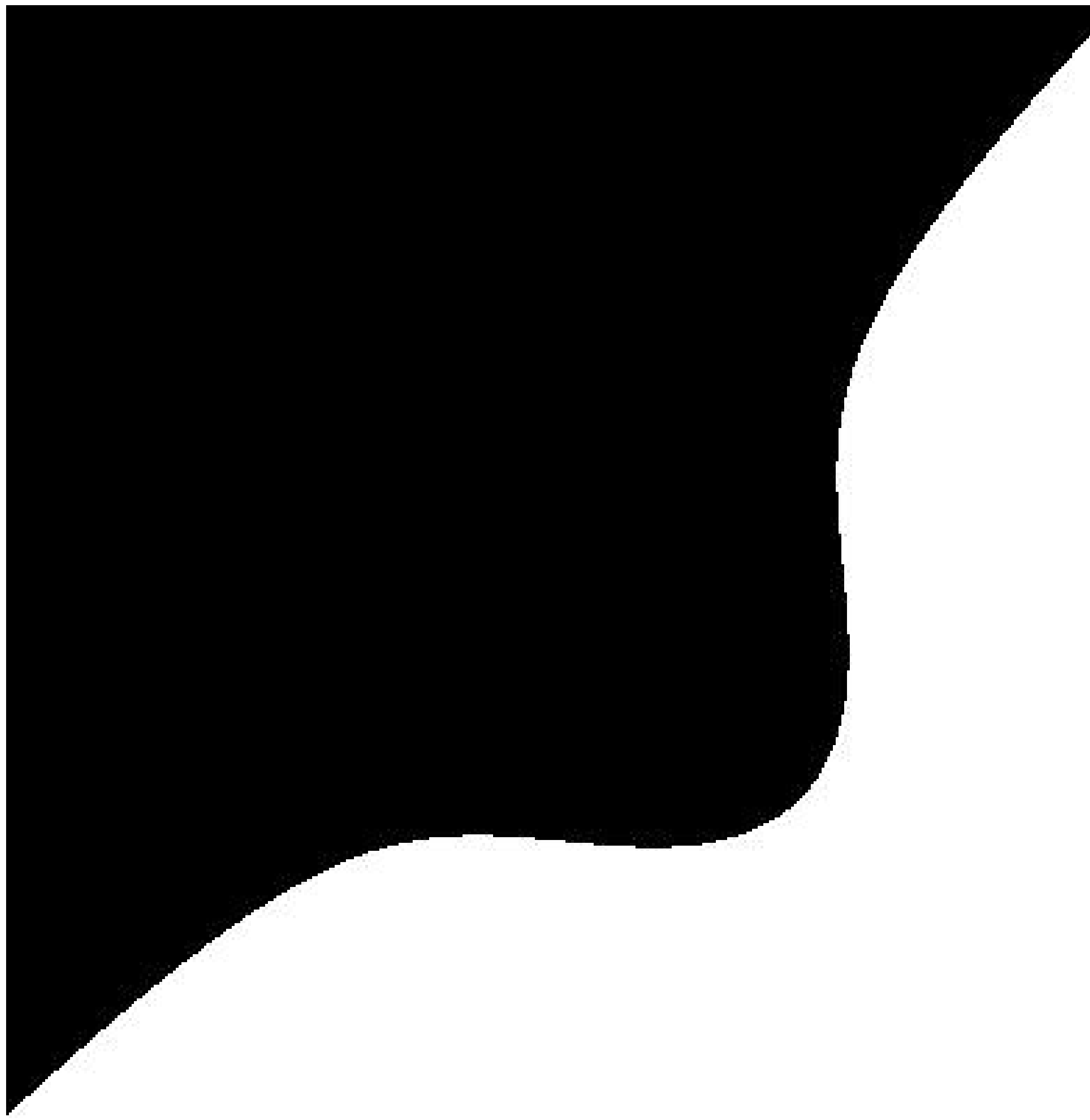
The Jacobi-quartic squid: can be extended to XXYZZR giant squid.



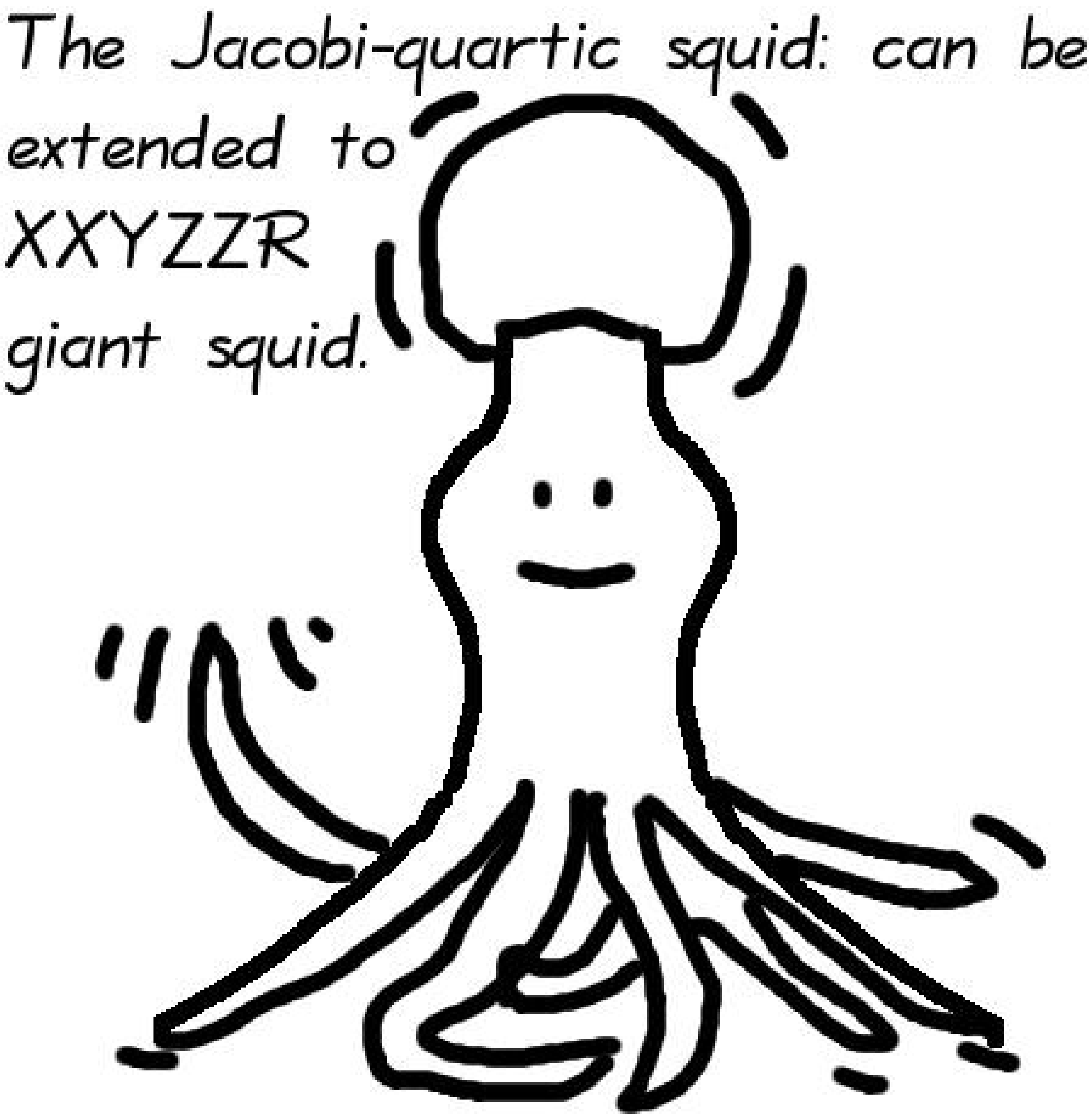
$x^3 - y^3 + 1 = 0.3$

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

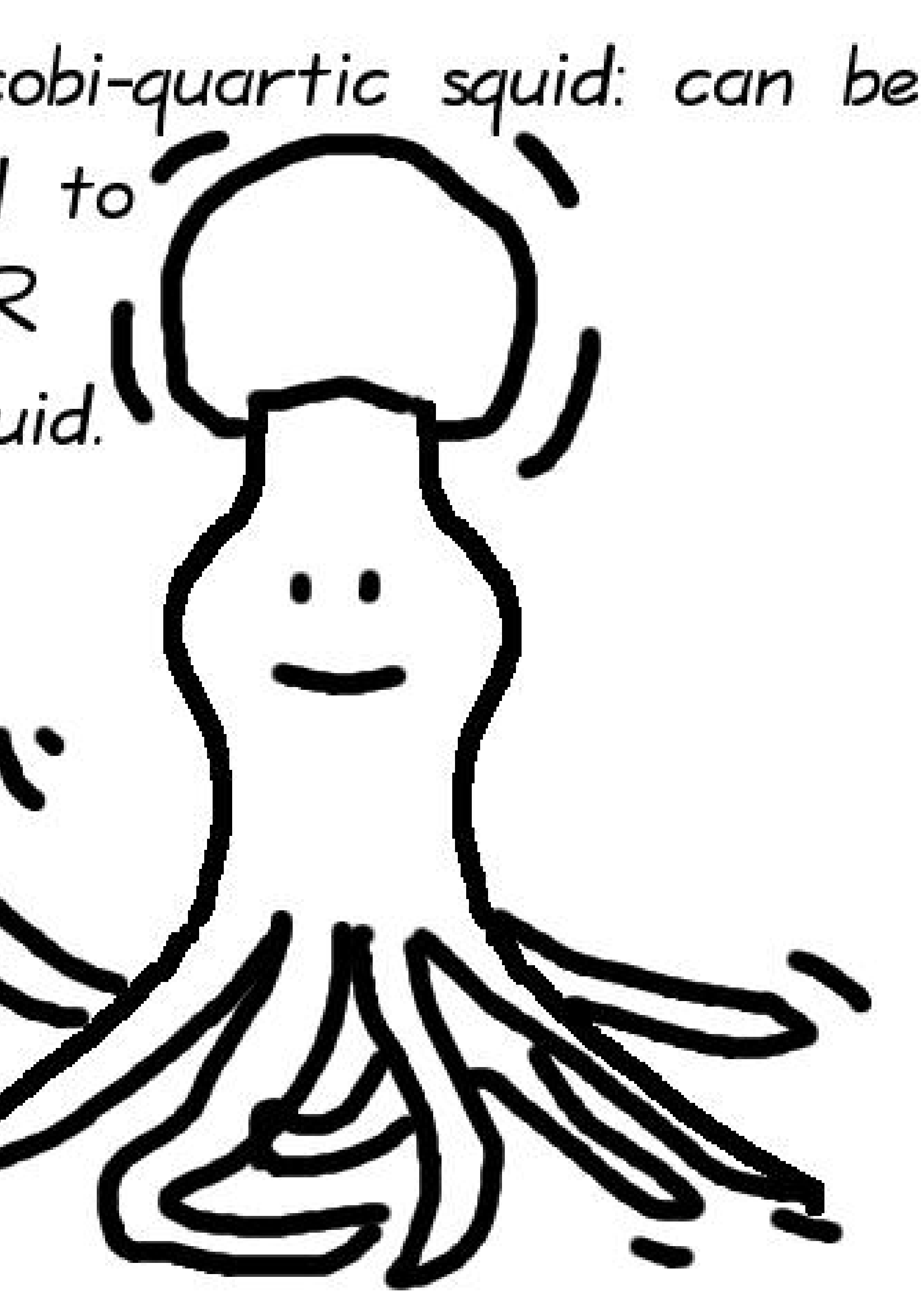




$$x^3 - y^3 + 1 = 0.3xy$$

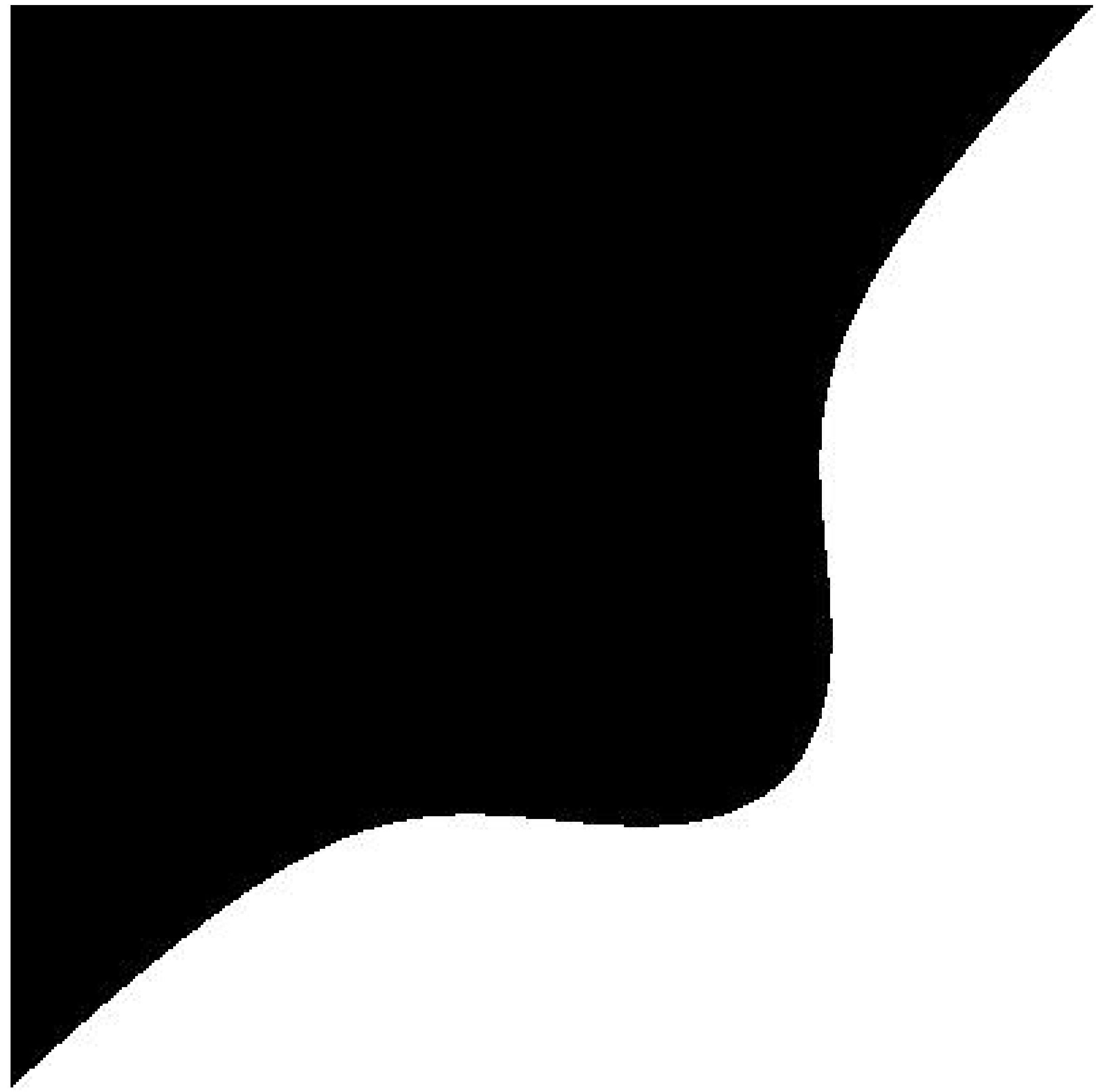

The Jacobi-quartic squid: can be extended to XXYZZR giant squid.

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



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

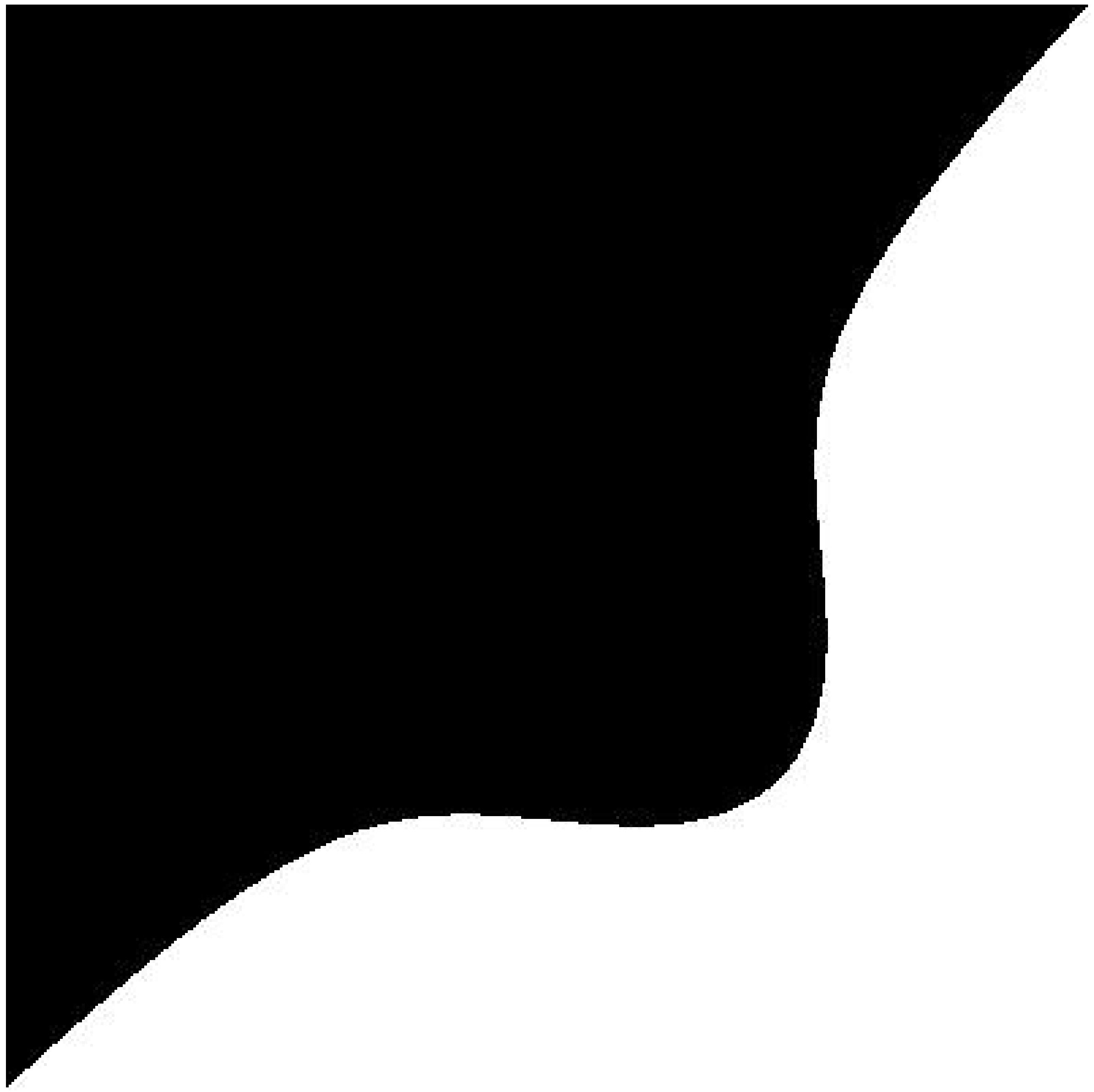
squid: can be



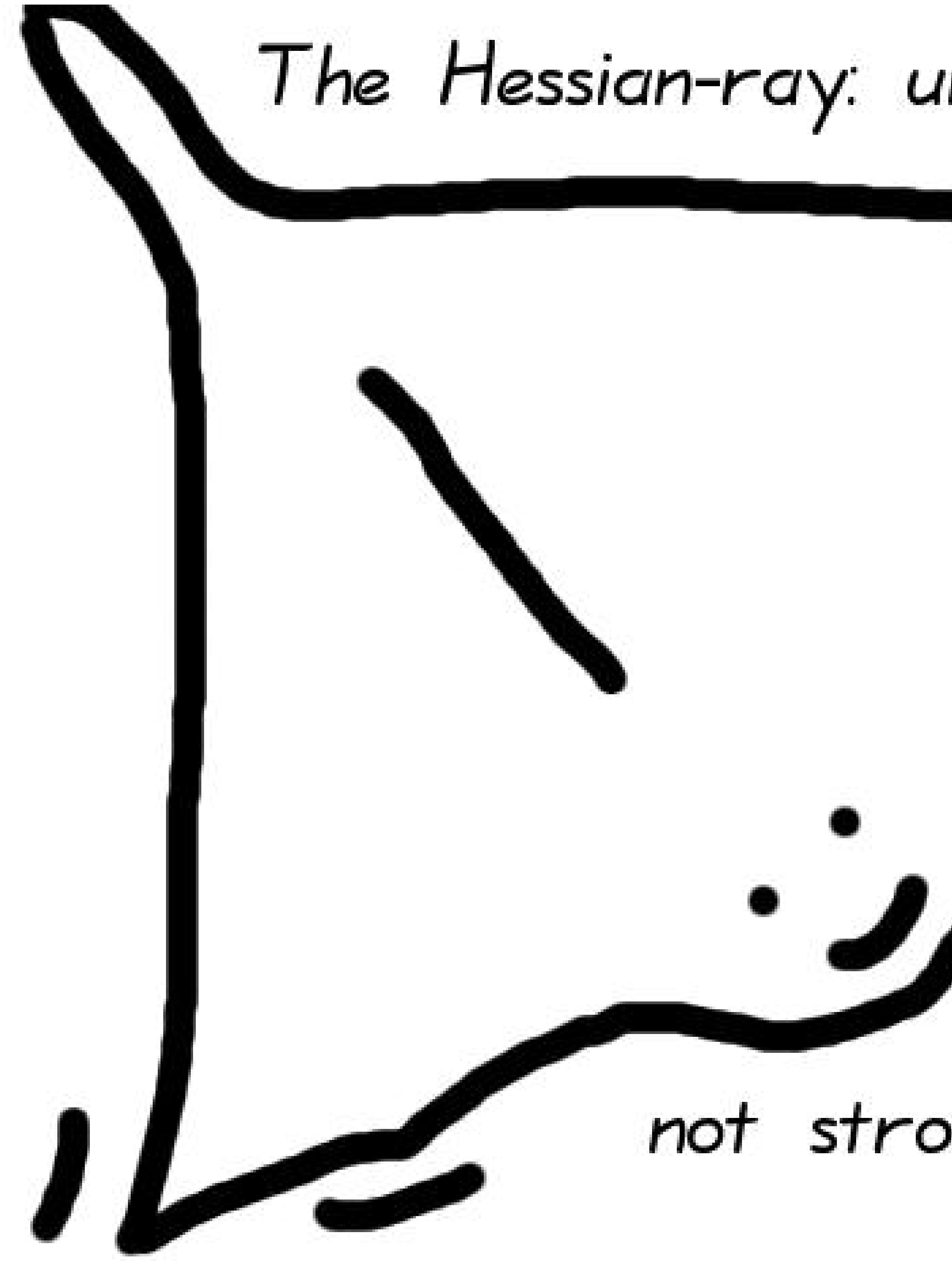
$$x^3 - y^3 + 1 = 0.3xy$$

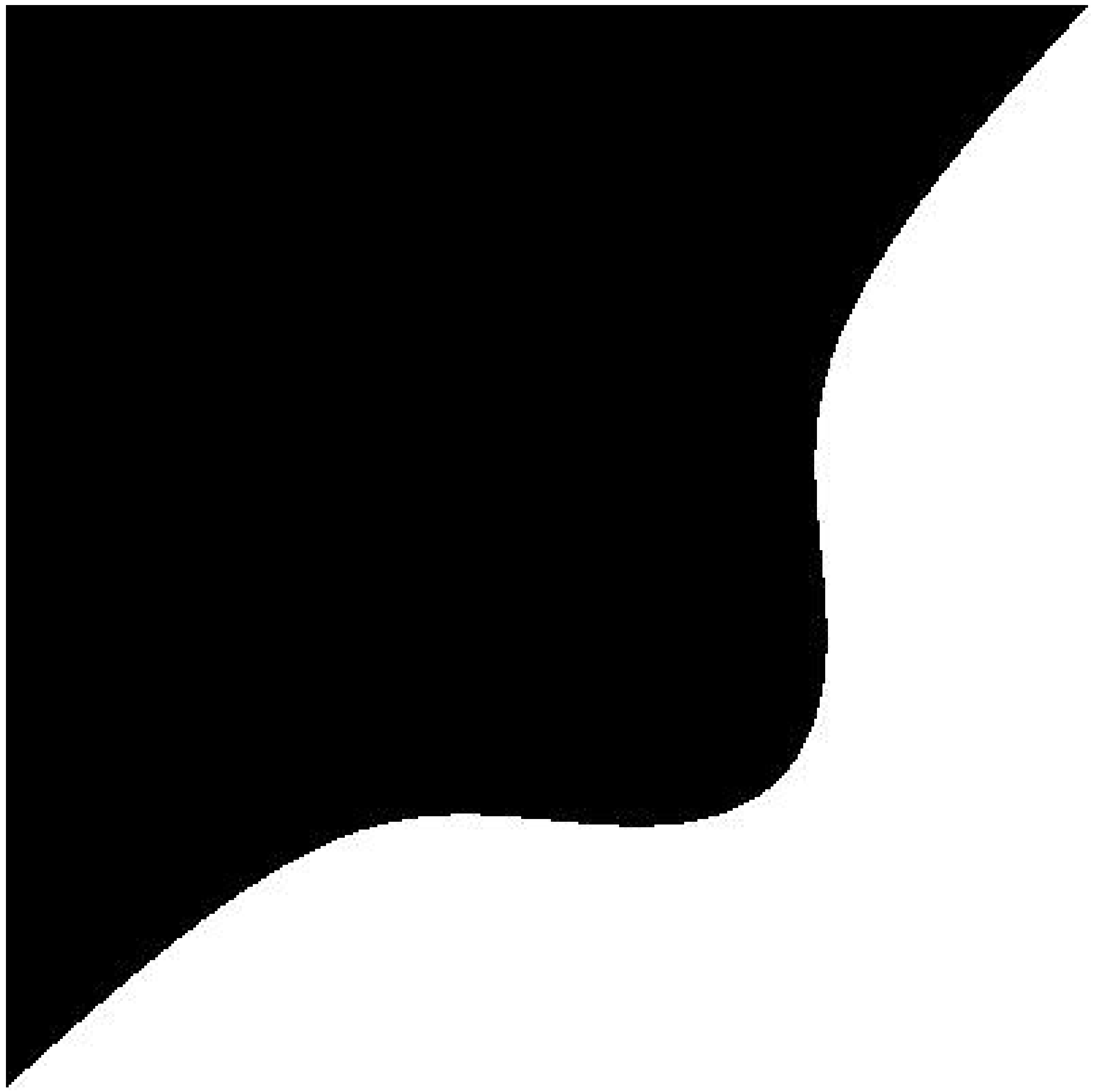
The Hess

n be

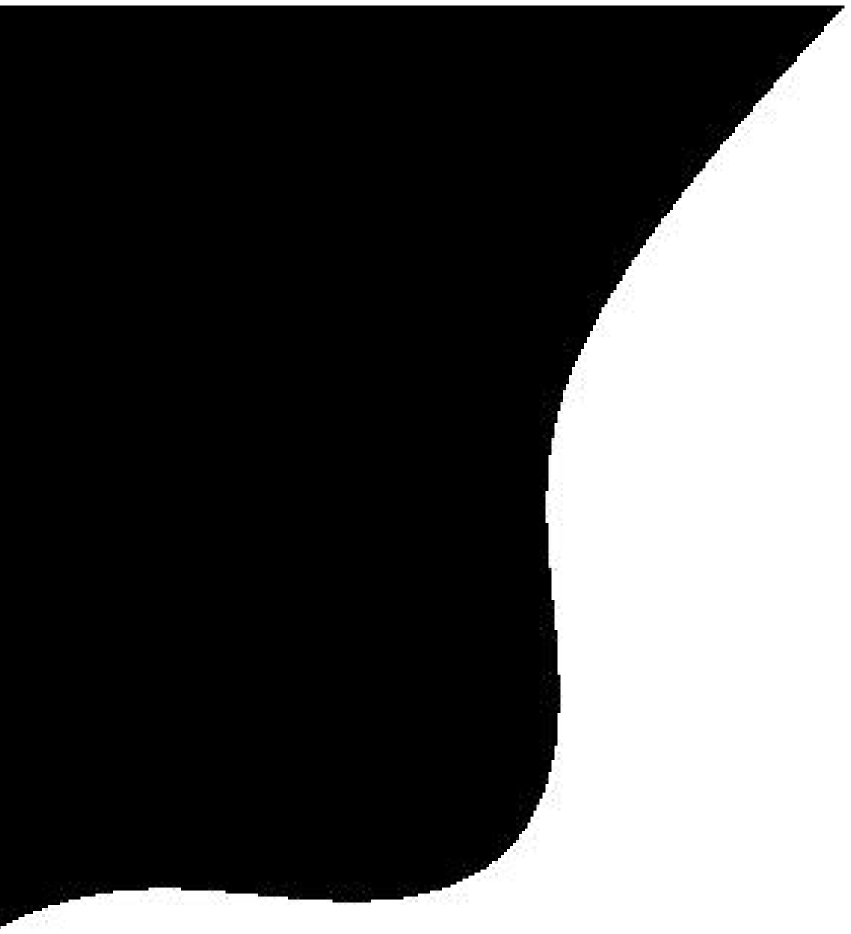


$x^3 - y^3 + 1 = 0.3xy$

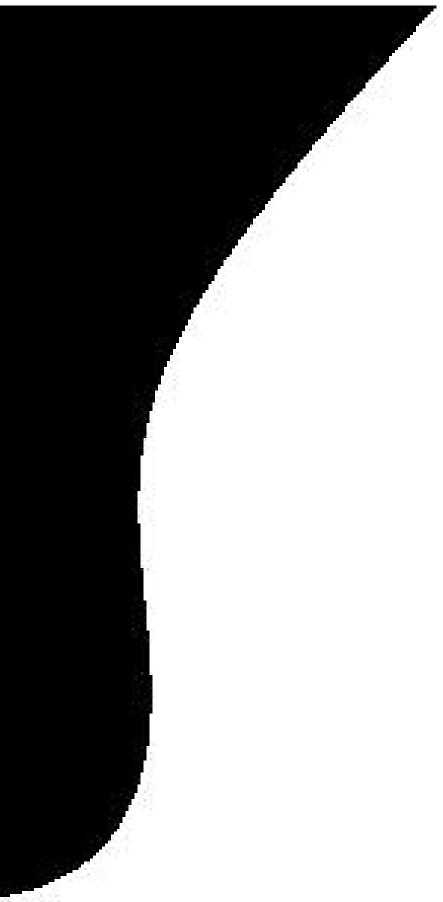




$$x^3 - y^3 + 1 = 0.3xy$$



$+ 1 = 0.3xy$



xy


The Hessian-ray: uniform
but
not strongly so

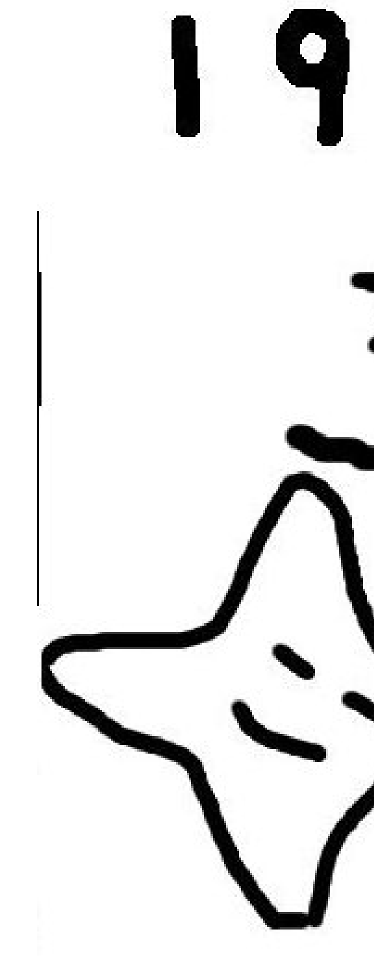

START


The Hessian-ray: uniform
but
not strongly so


START


The Hessian-ray: uniform
but
not strongly so


START


19


sian-ray: uniform
but
not strongly so


START


1985

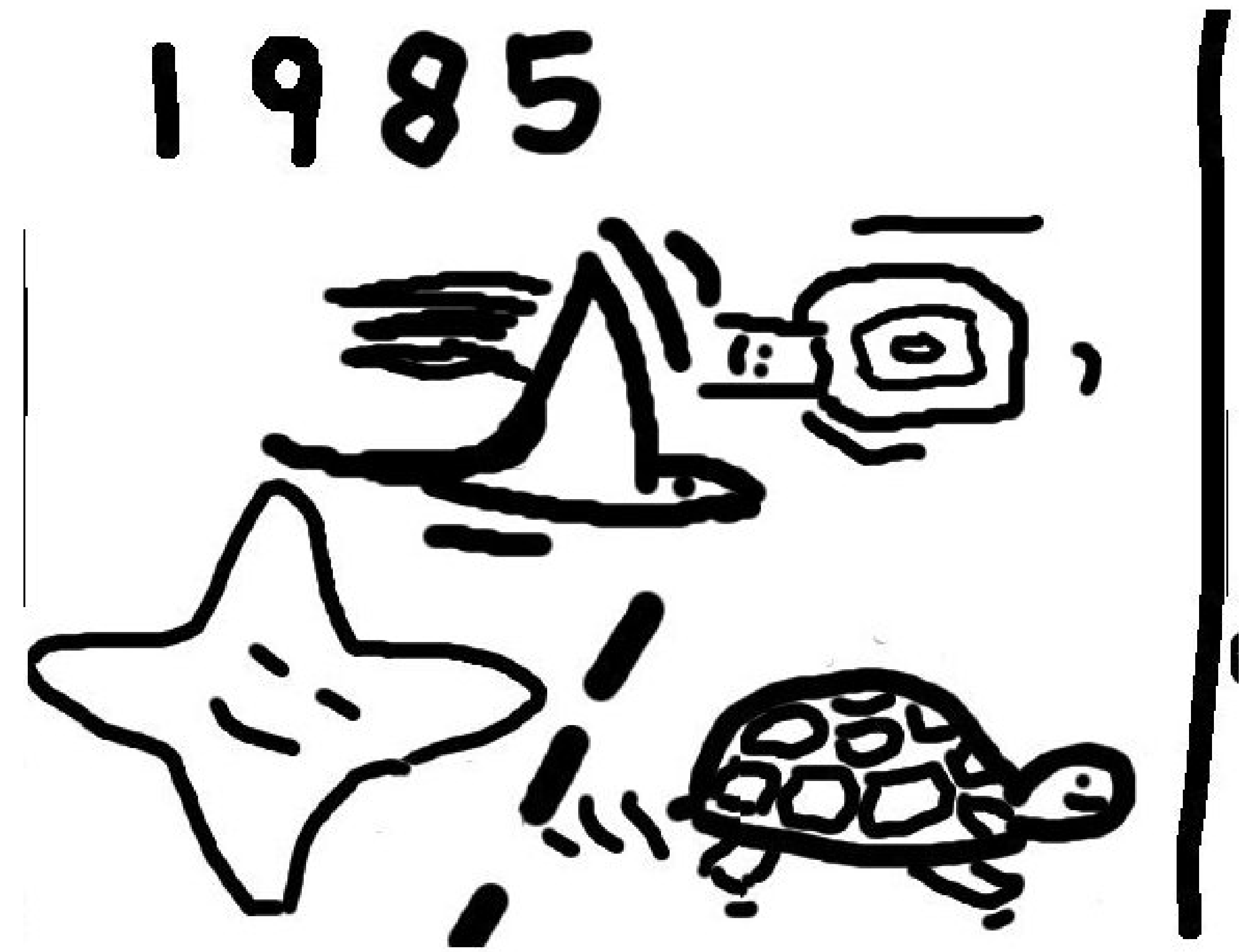
niform

but

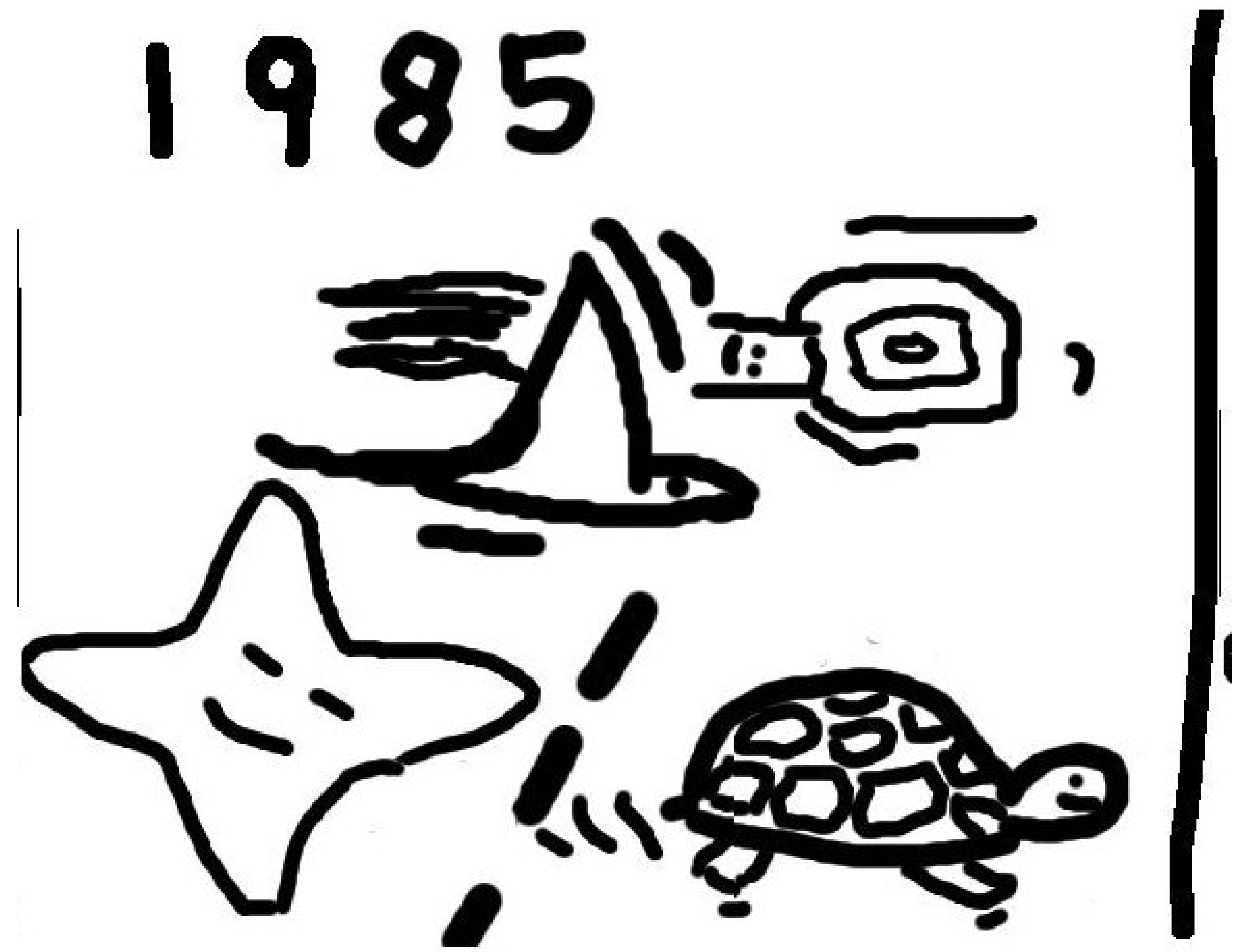
ngly so

1985

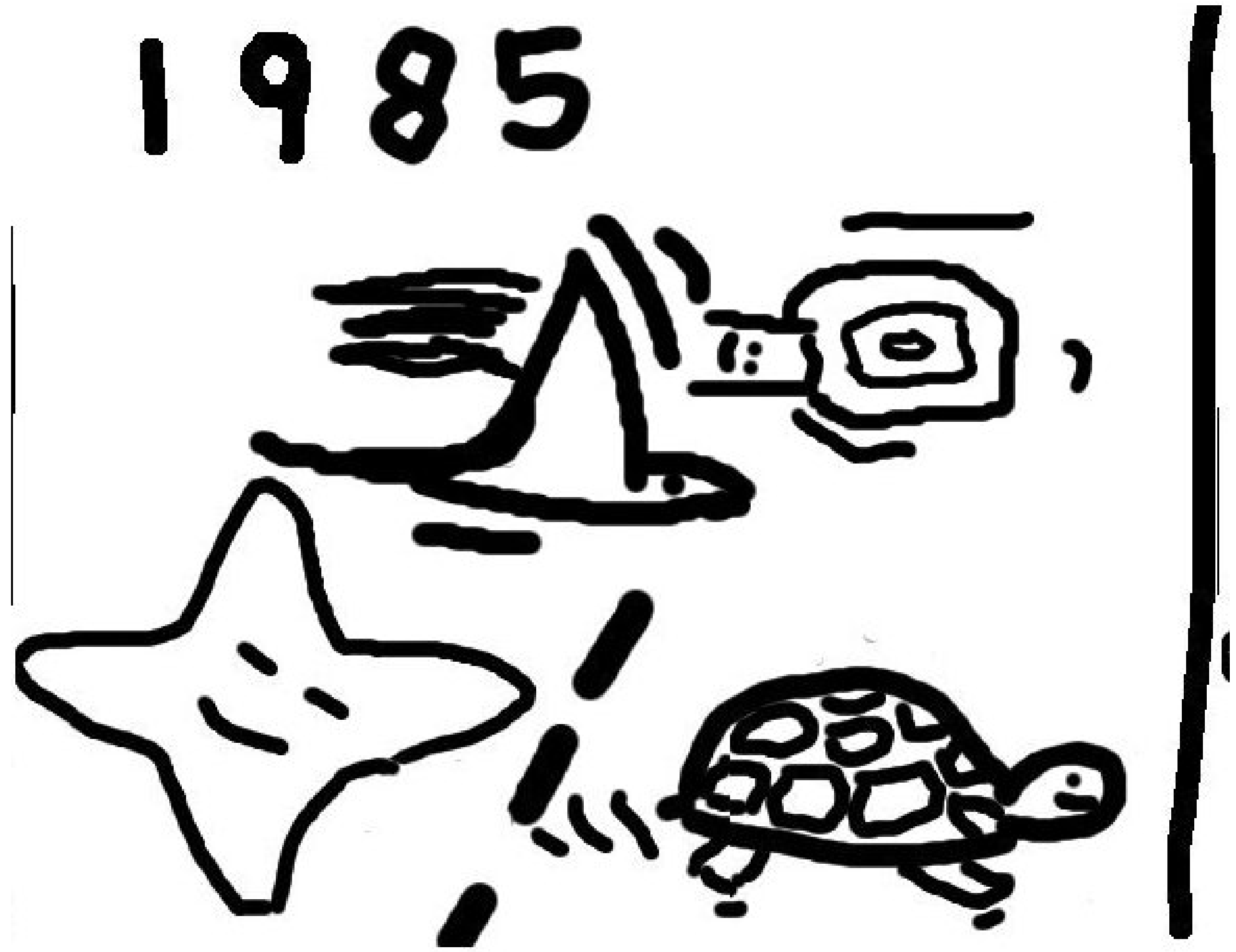

START

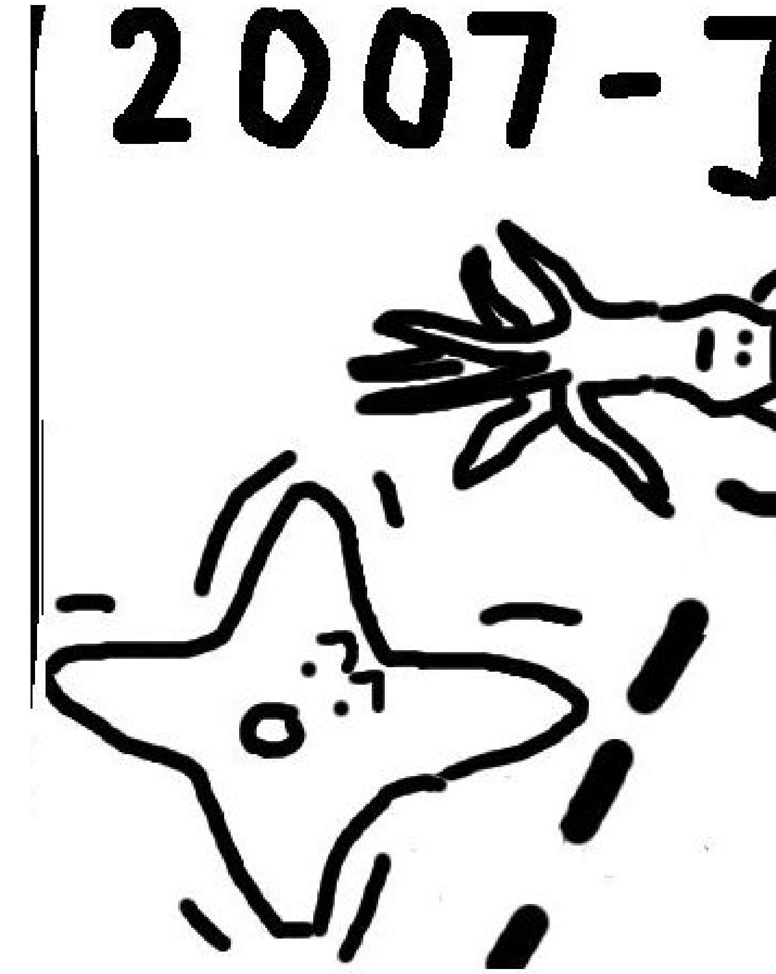

1985

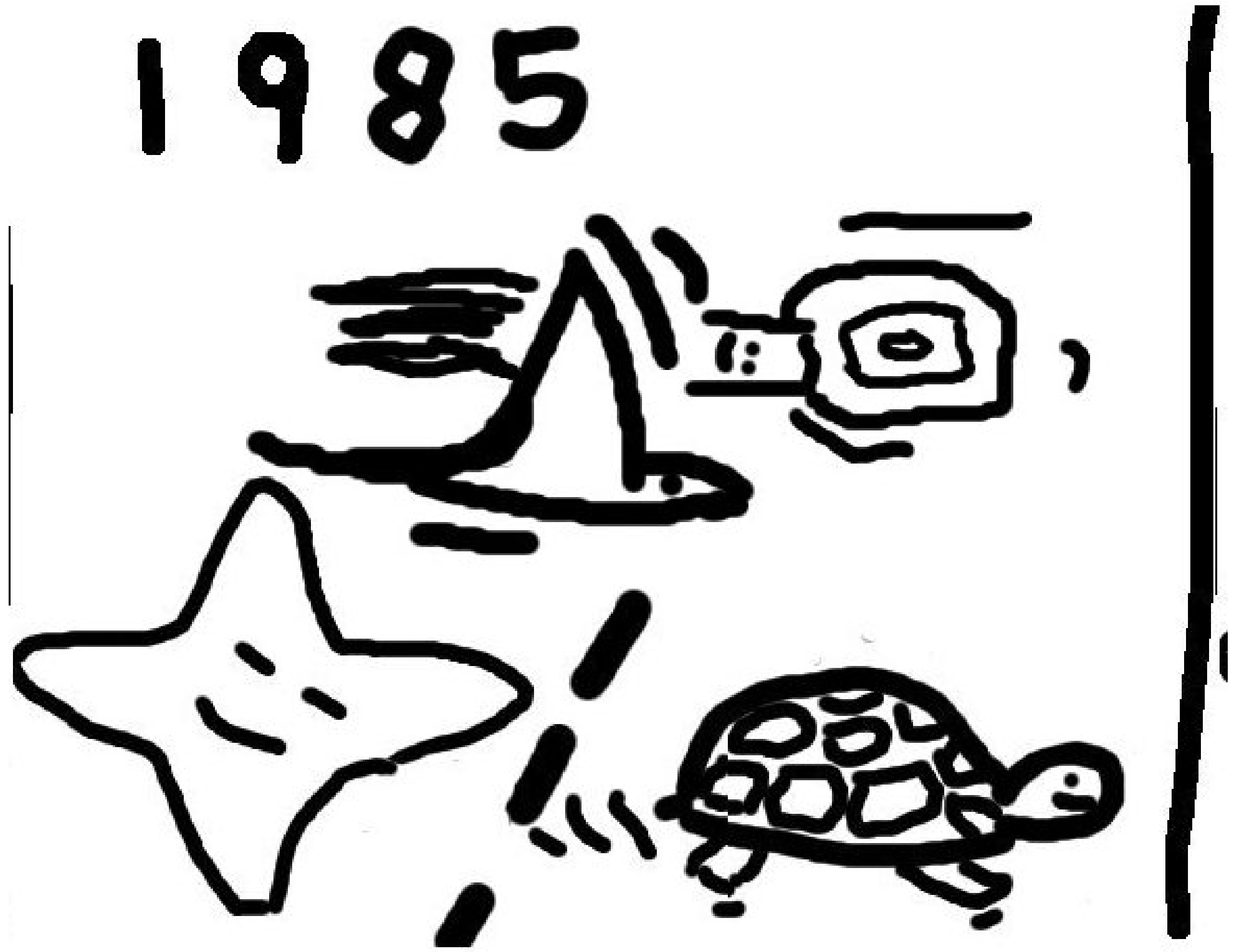

START

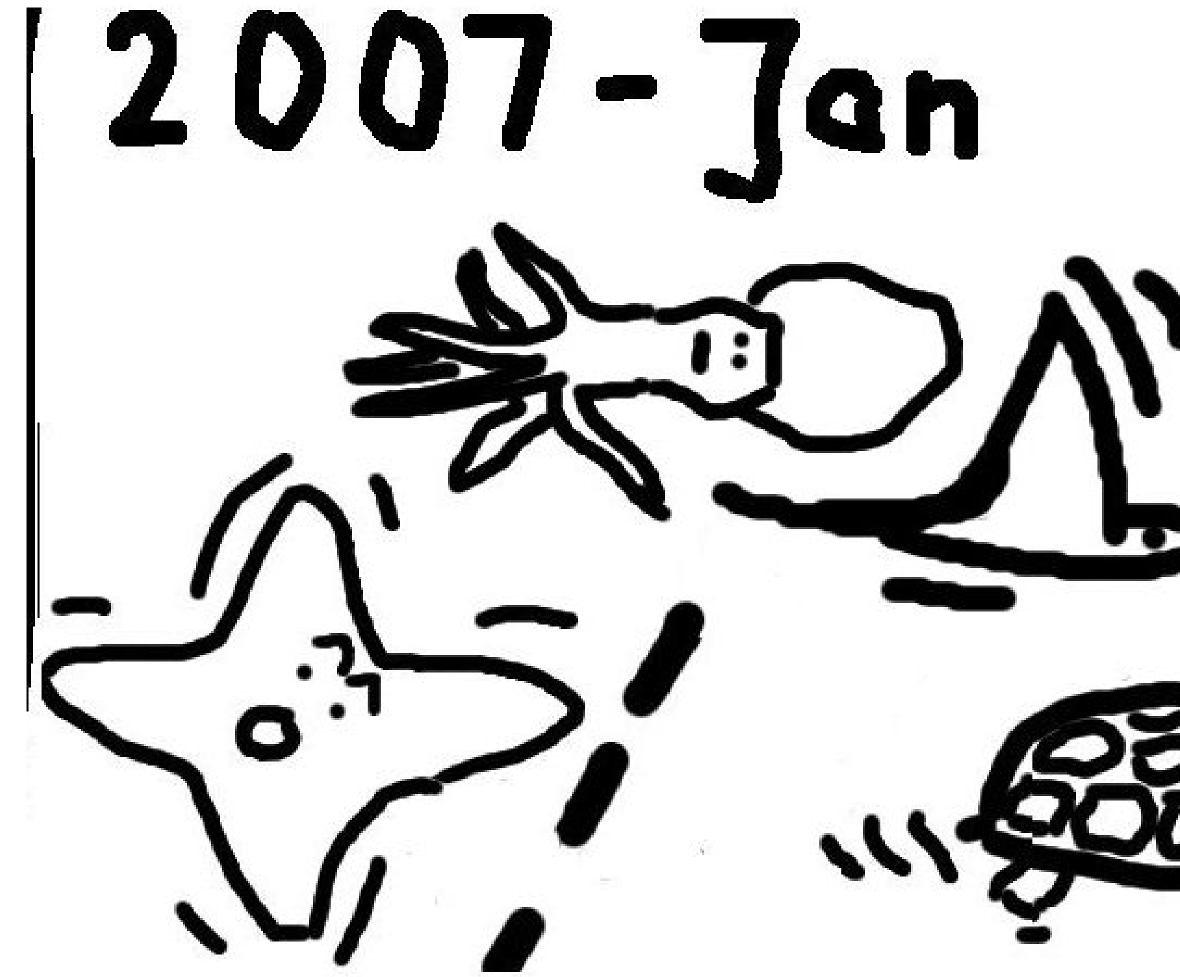

1985

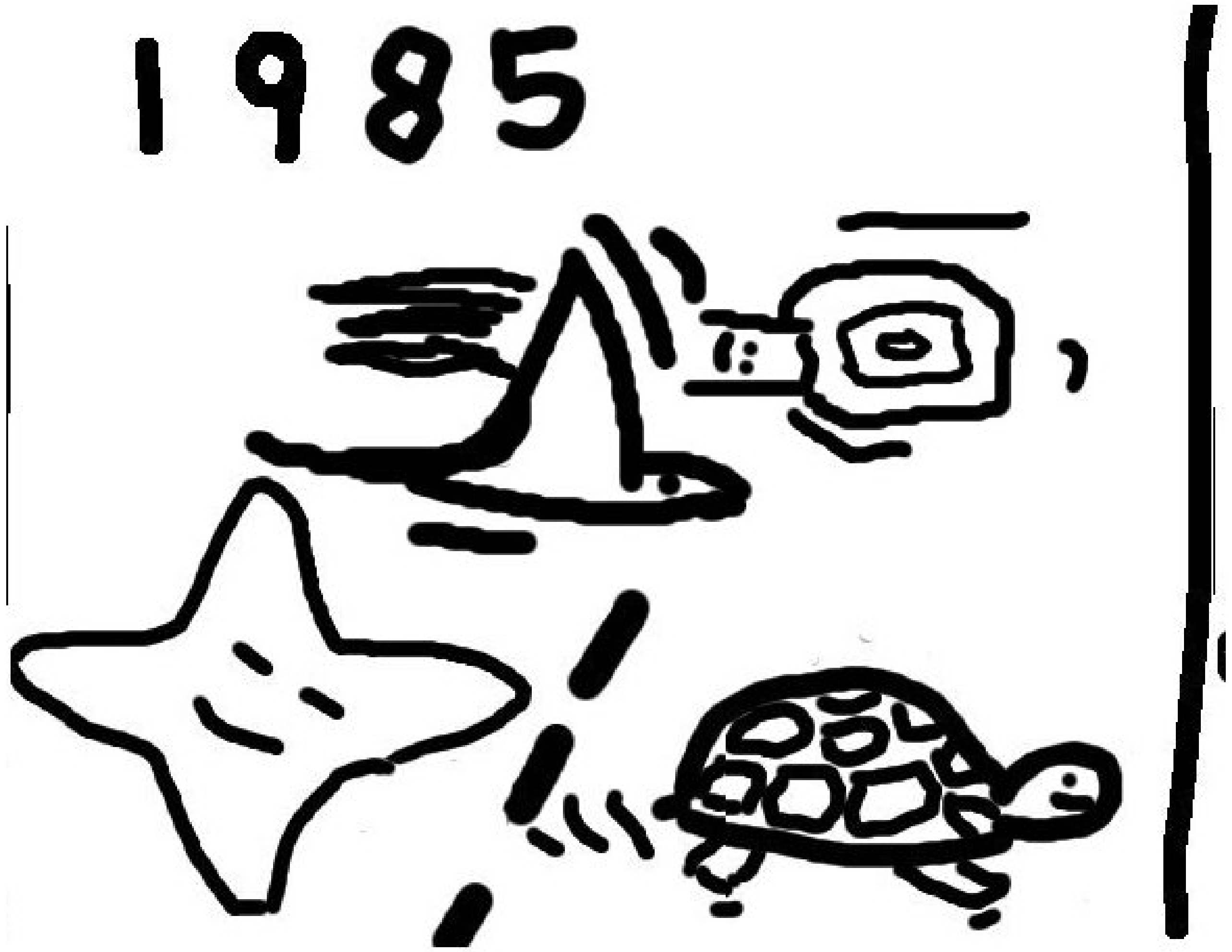

20

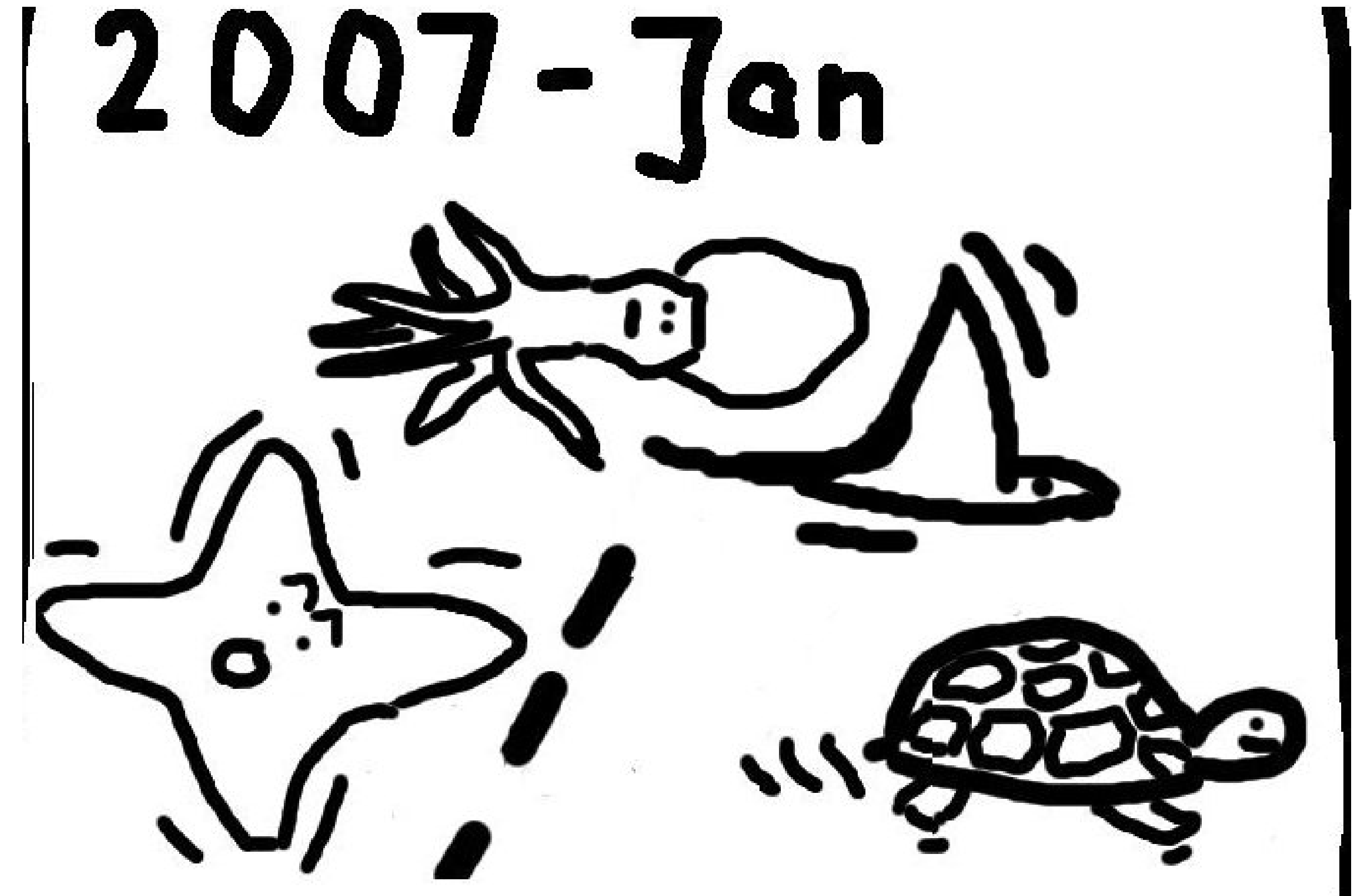

1985


2007-


1985

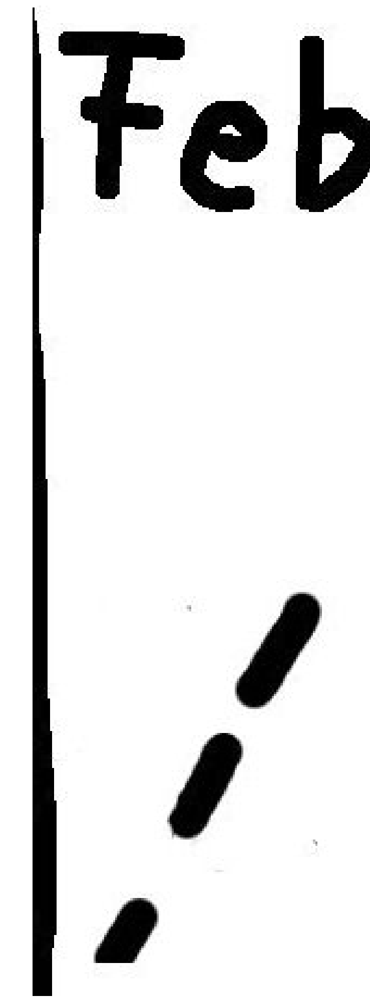

2007-Jan

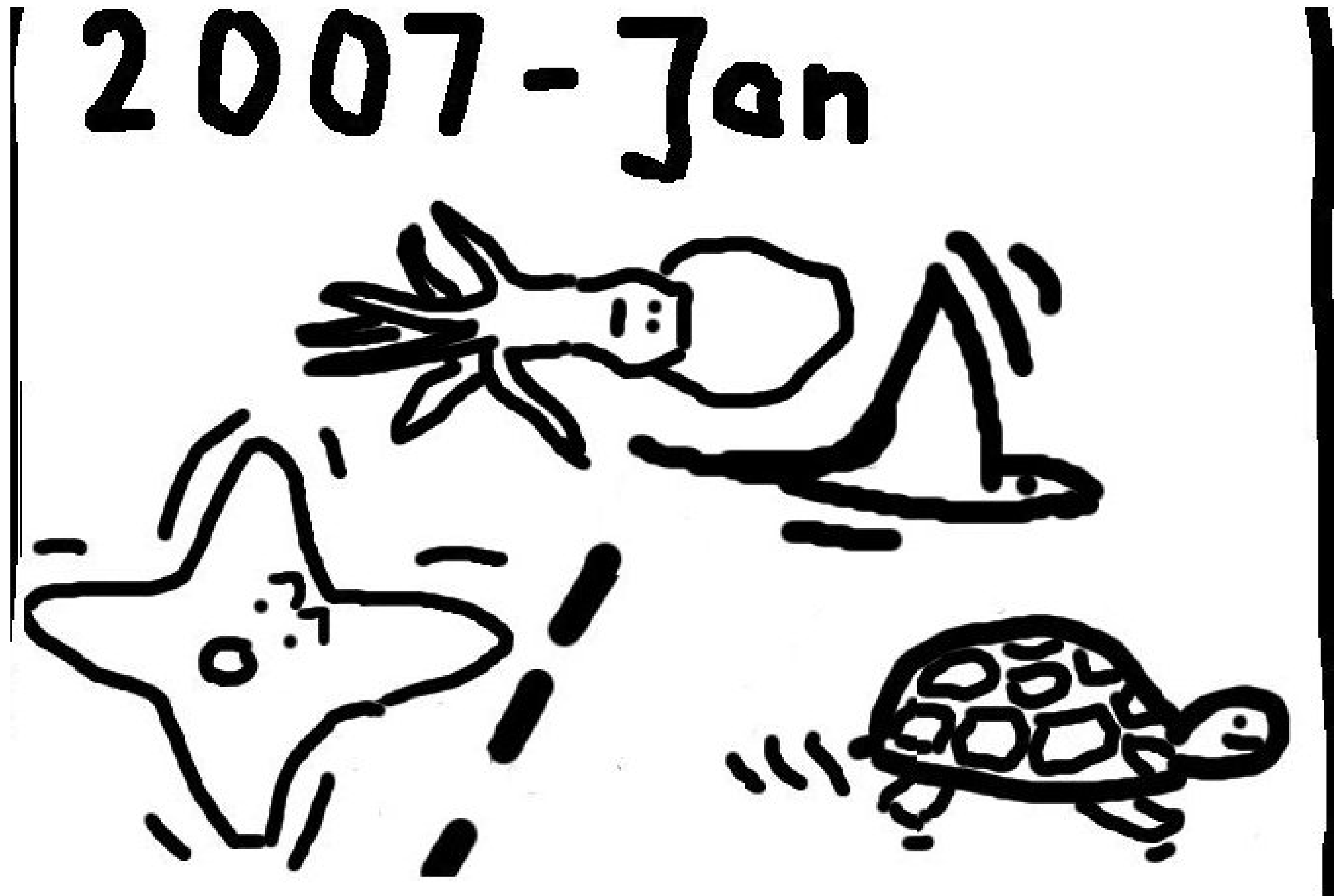

1985


2007-Jan

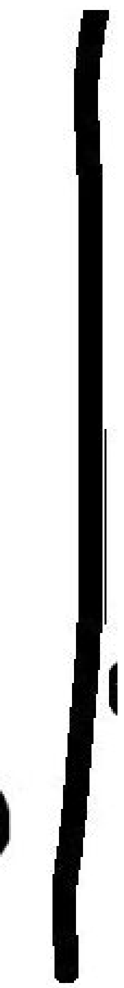

85

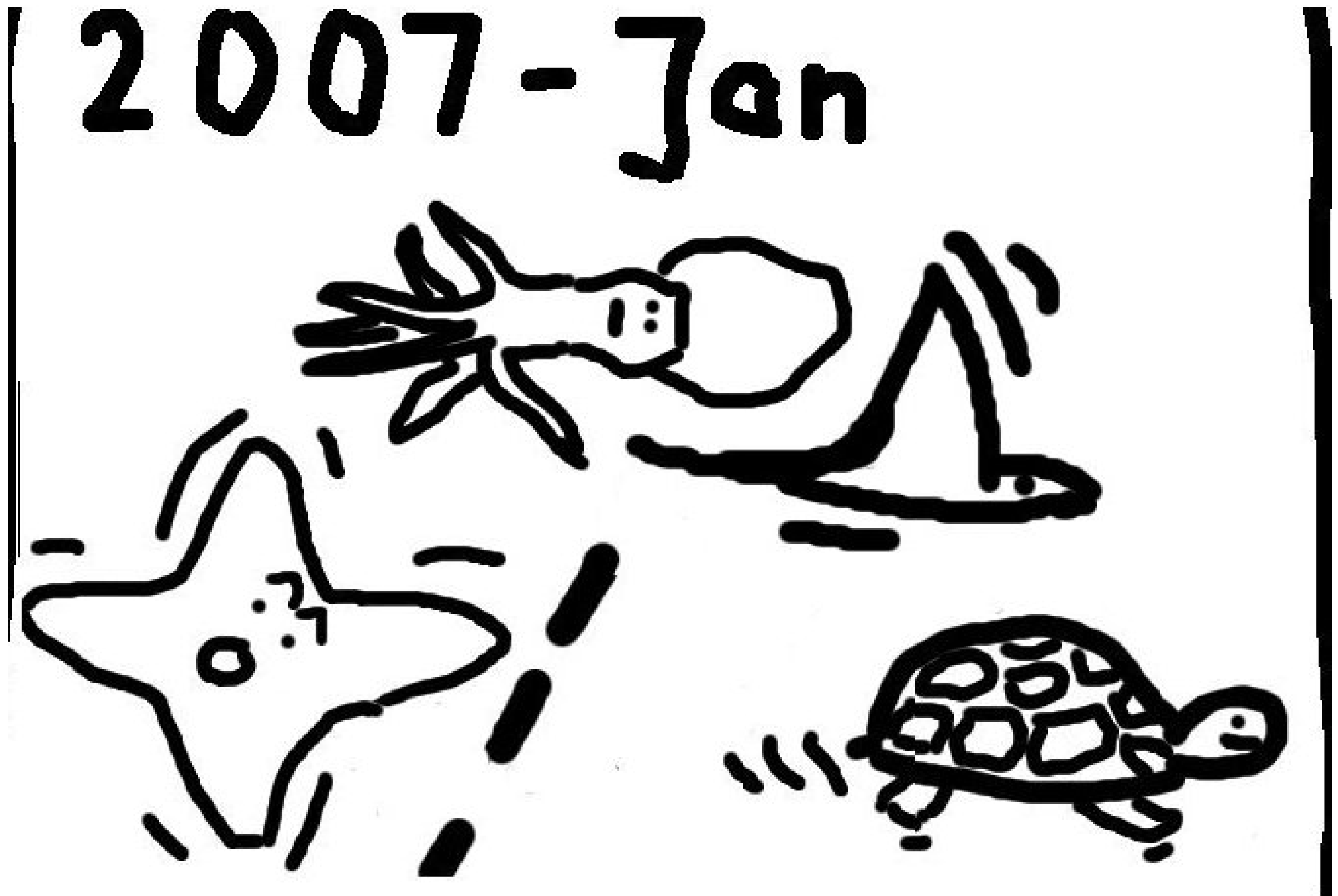

2007-Jan

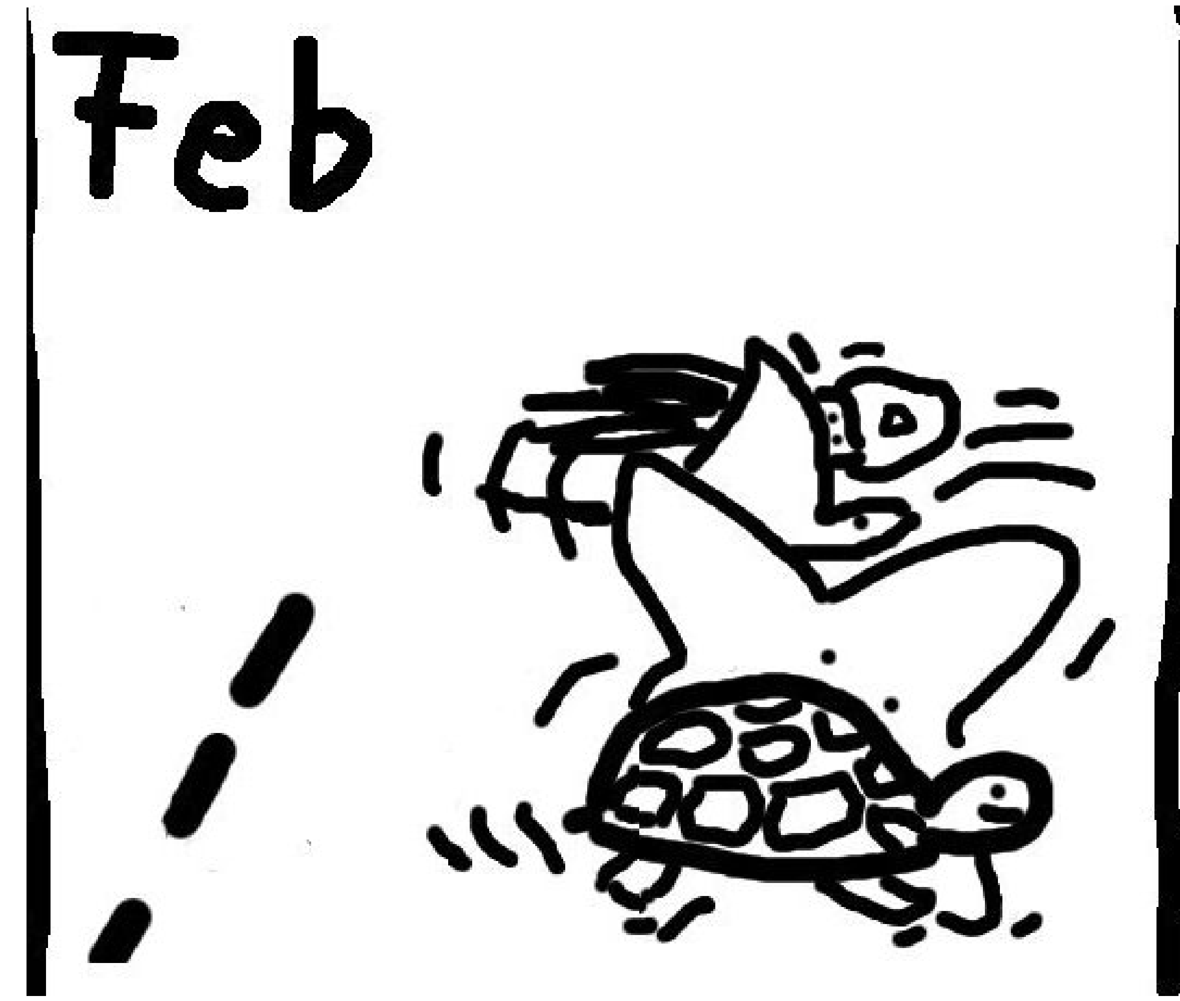

Feb

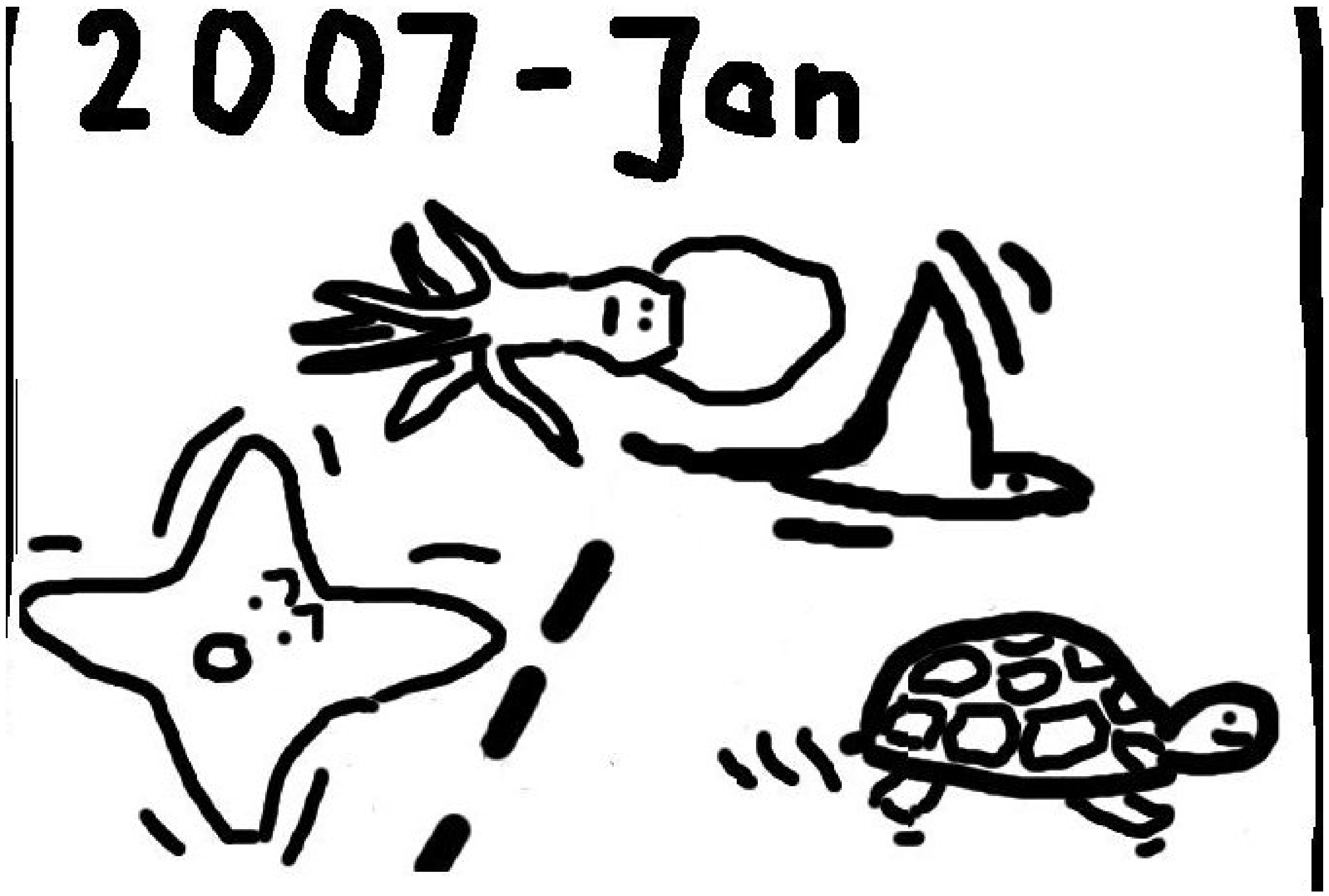

2007-Jan

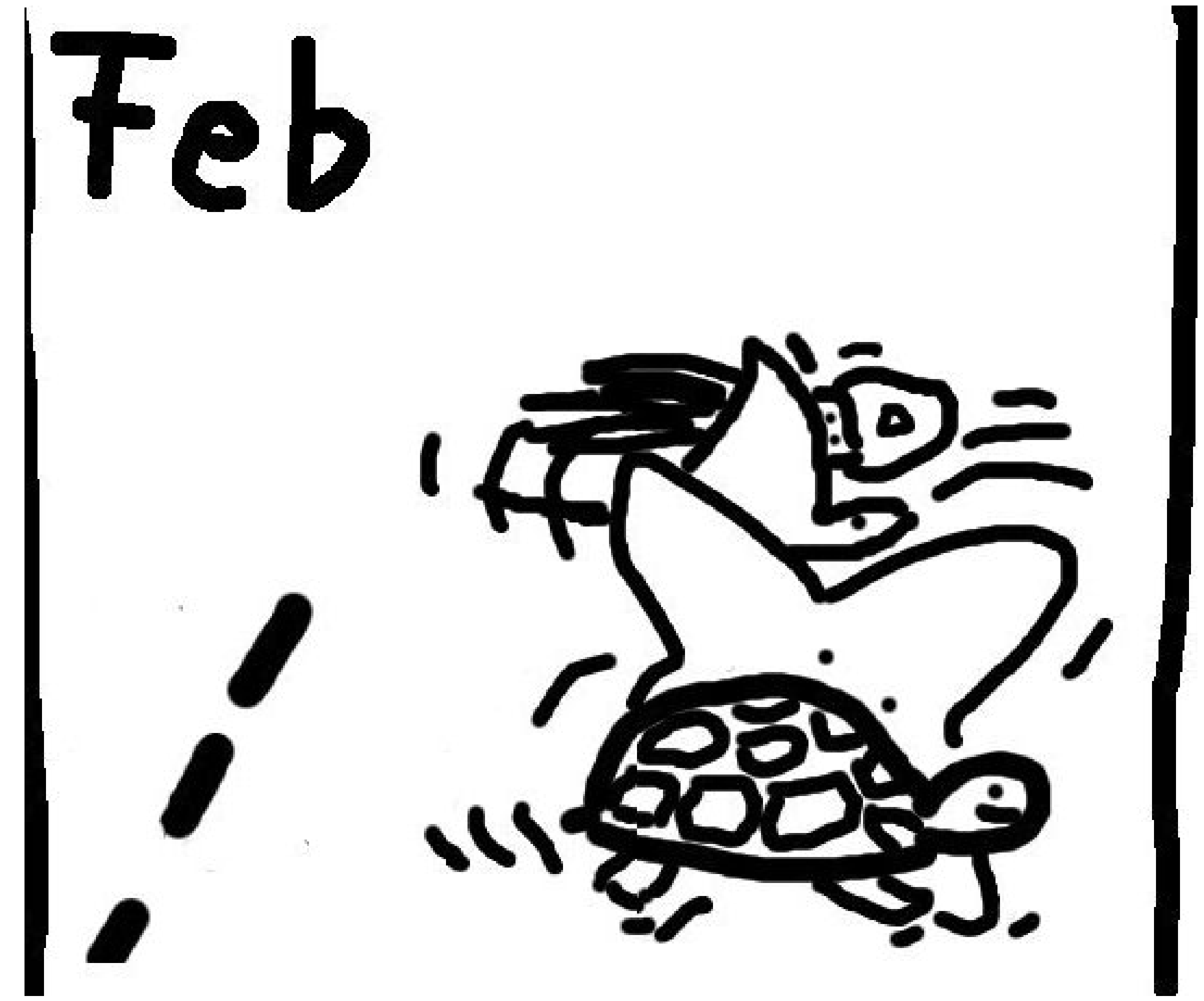

Feb

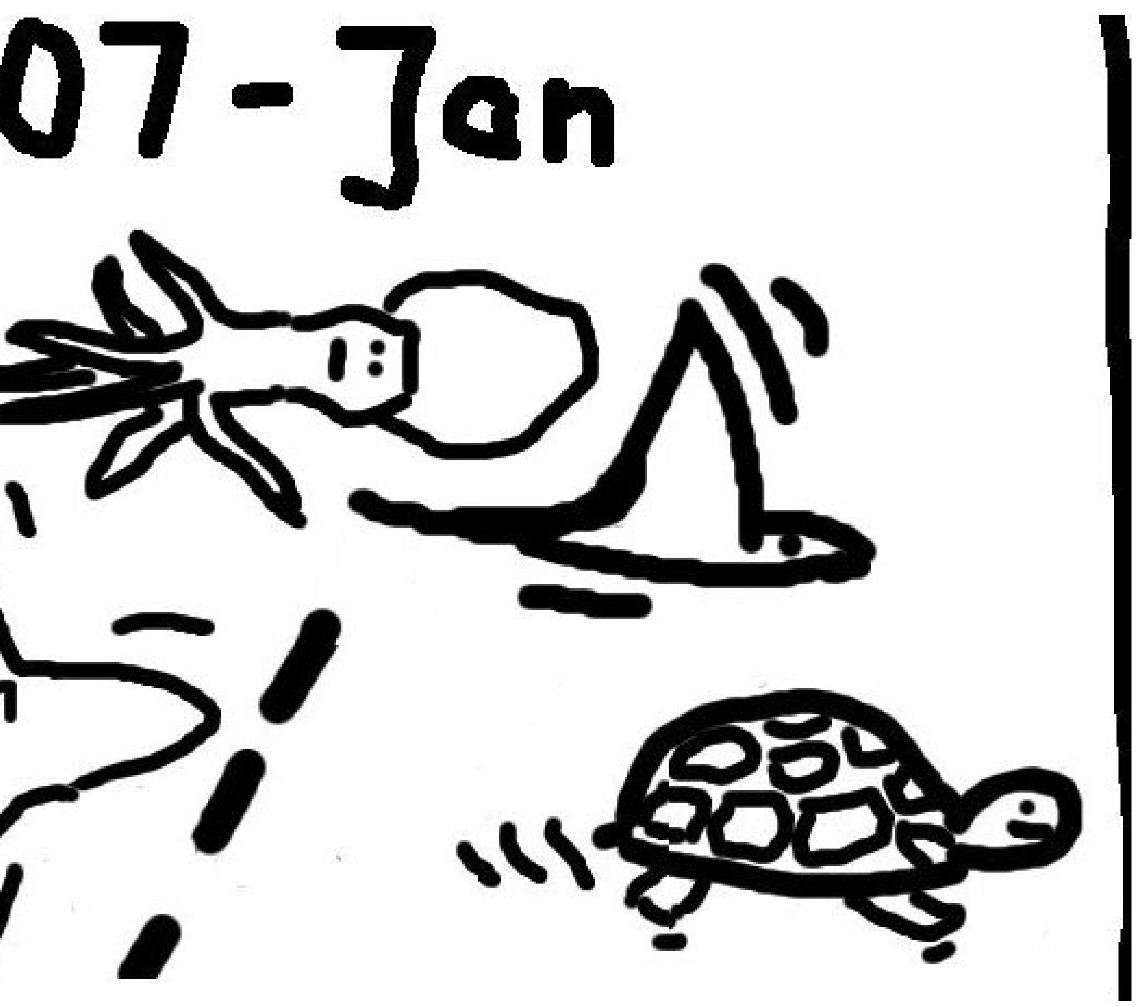


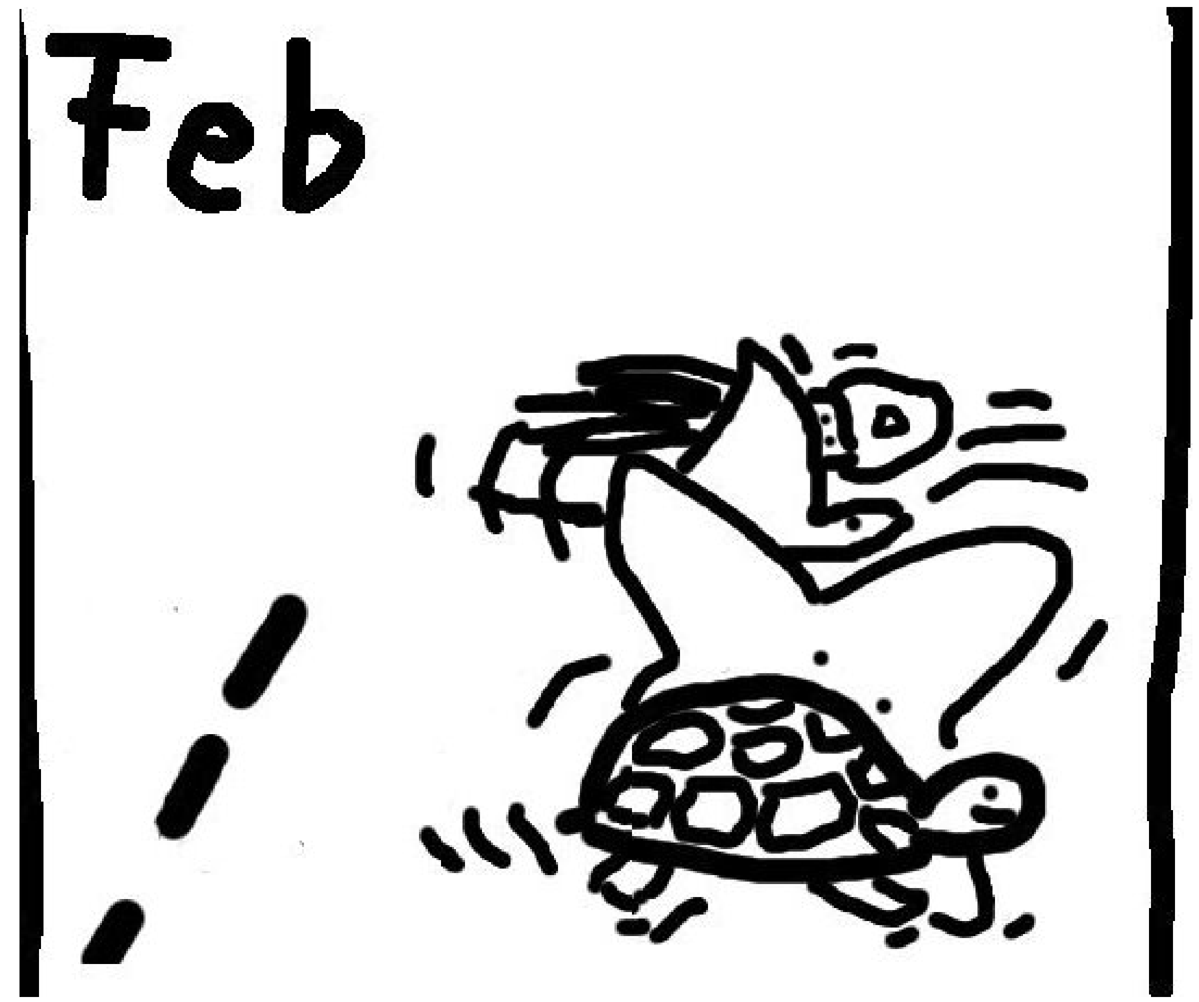

2007 - Jan

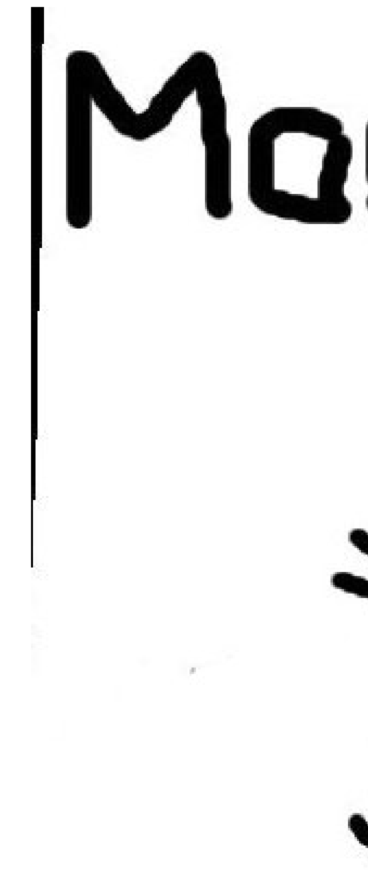

Feb

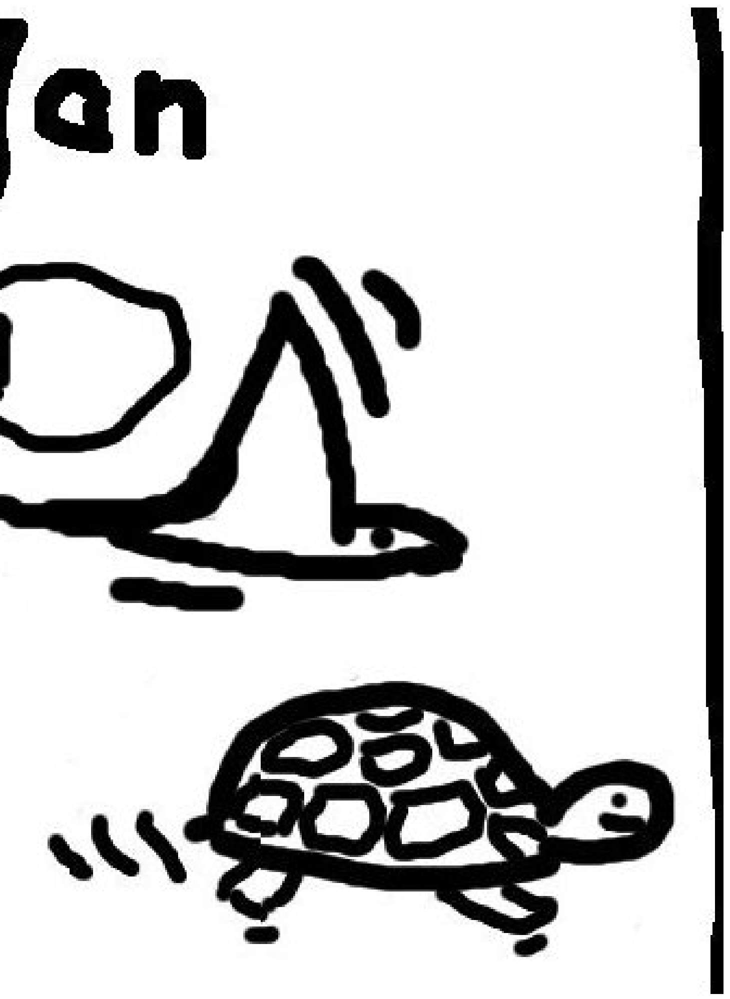

2007-Jan

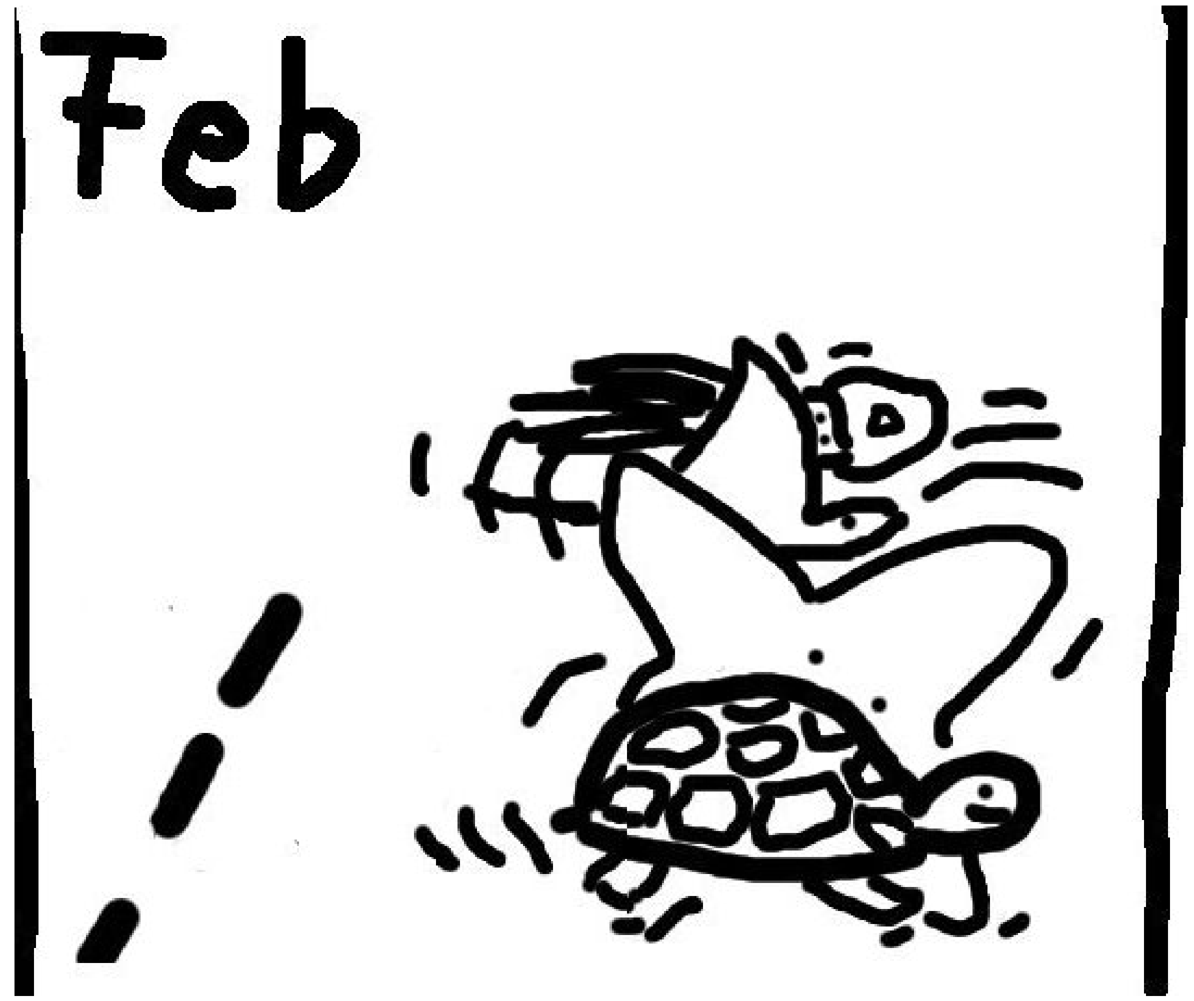

Feb


07 - Jan

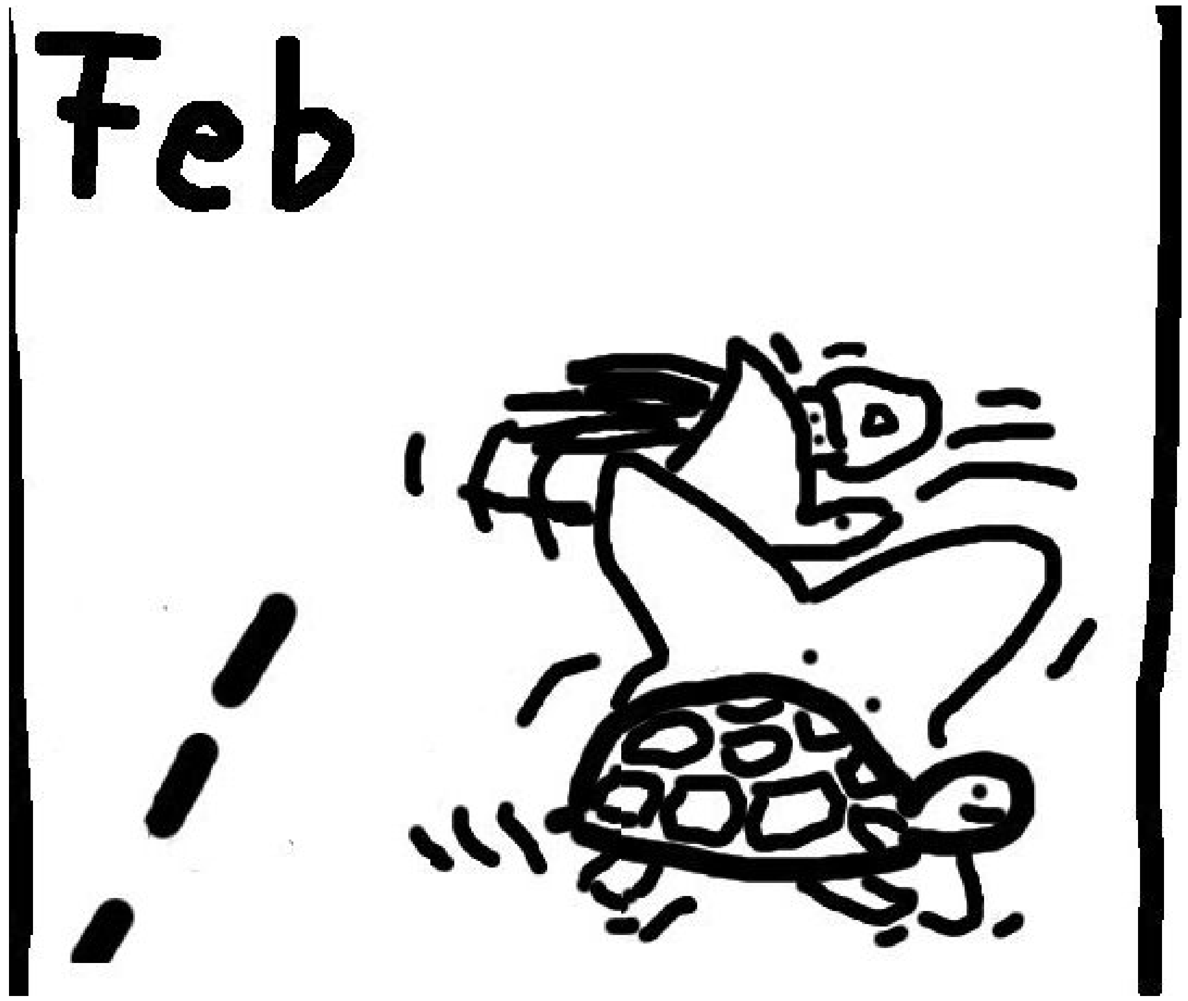

Feb

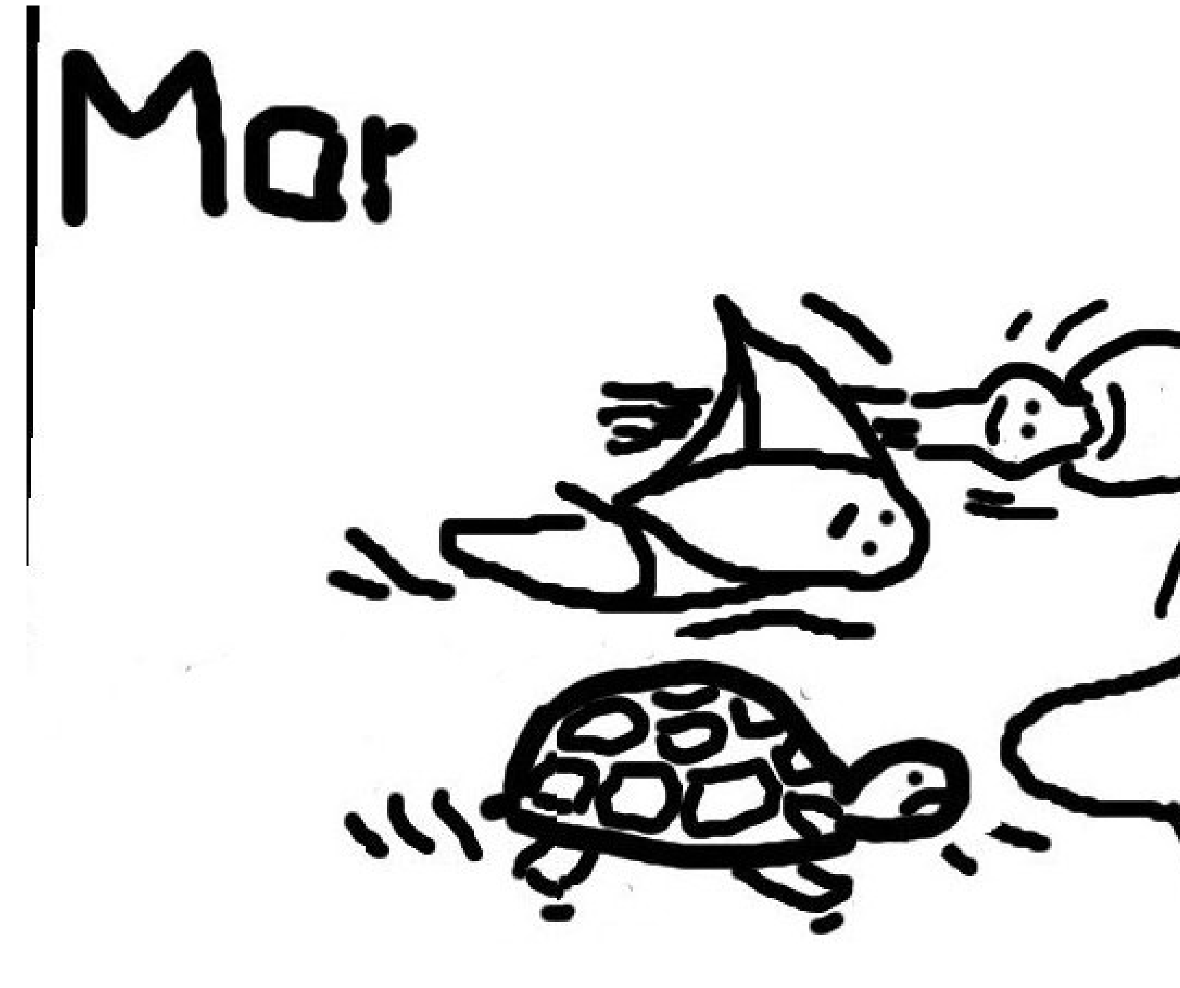


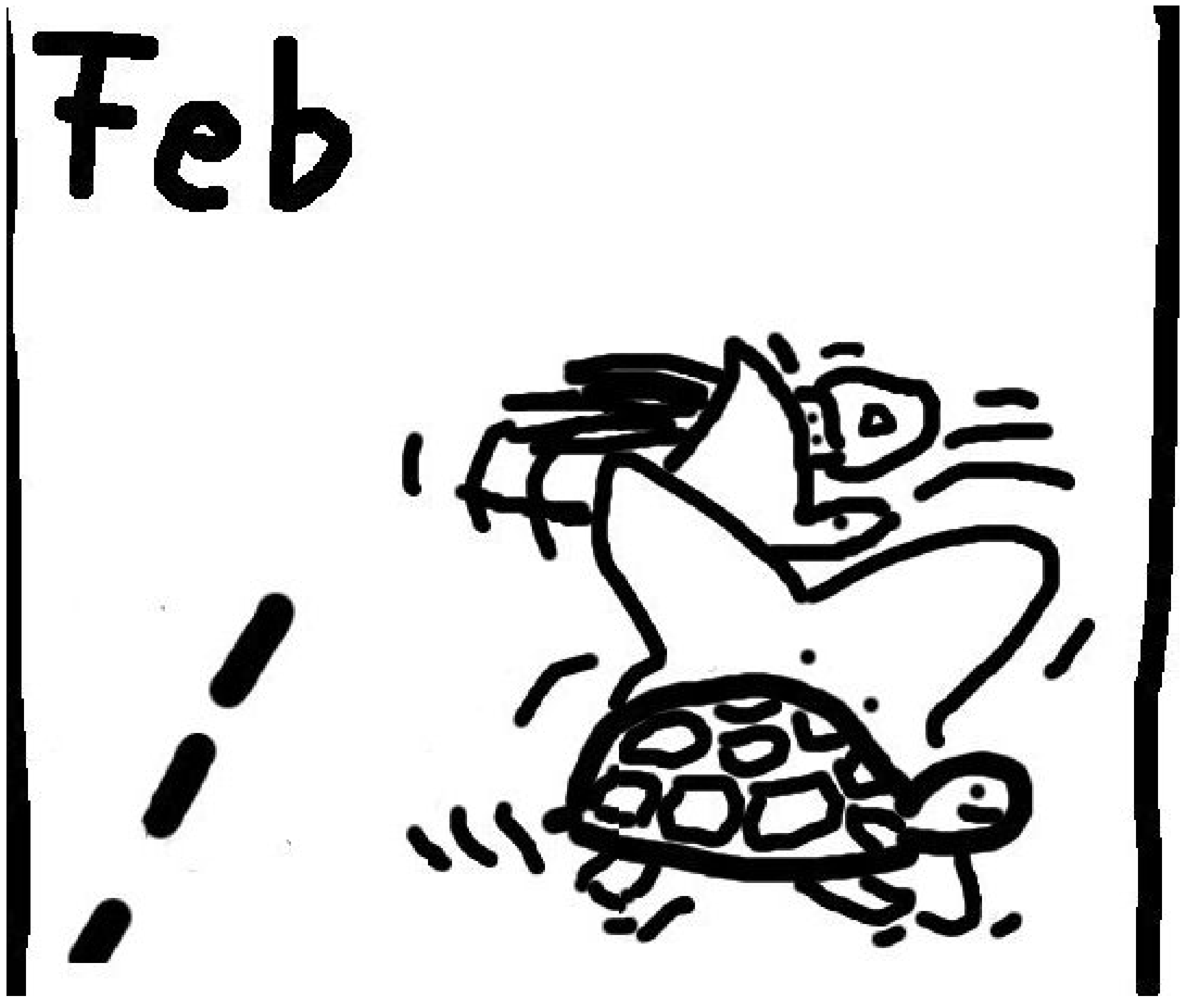

Jan

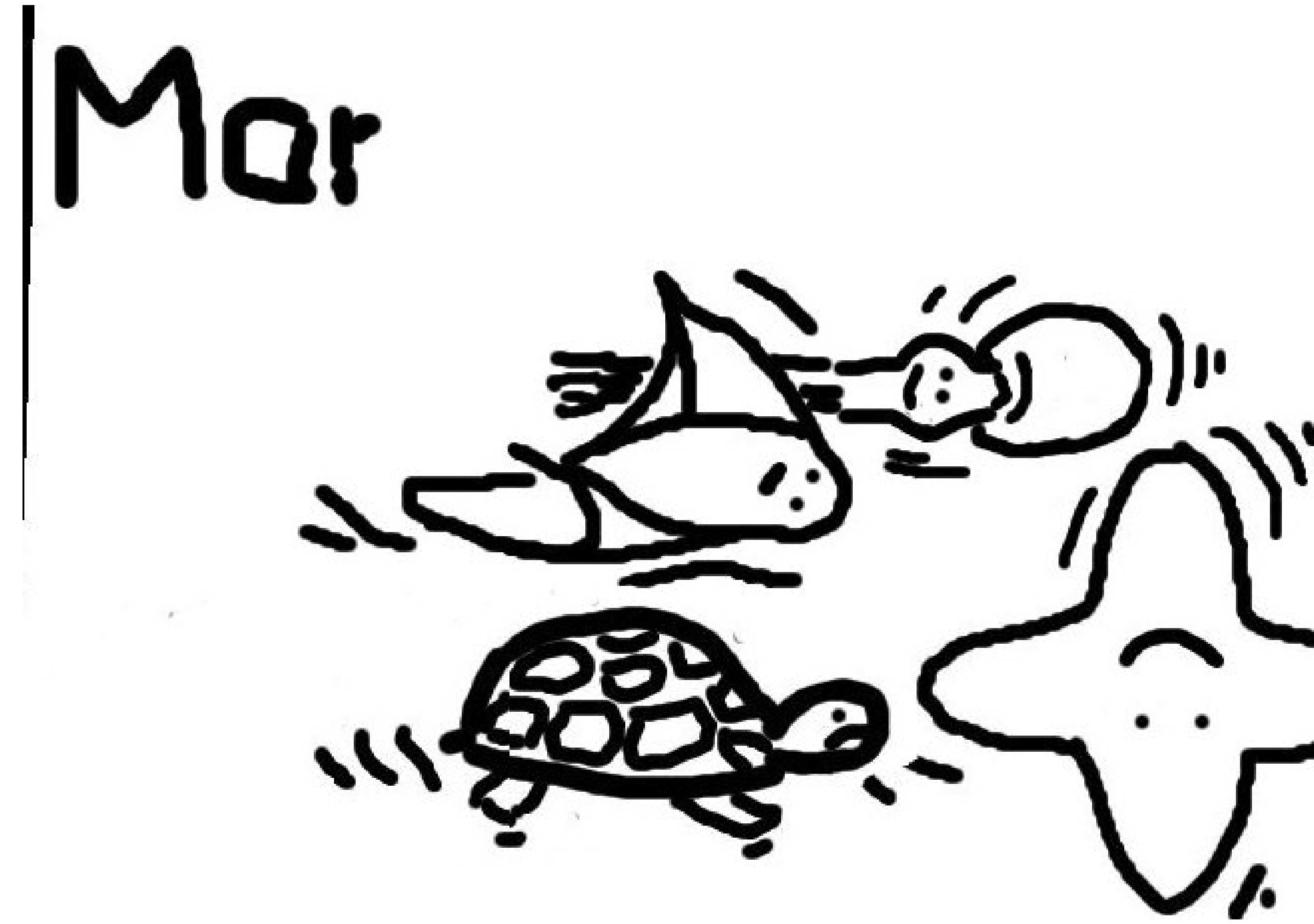

Feb


Mar

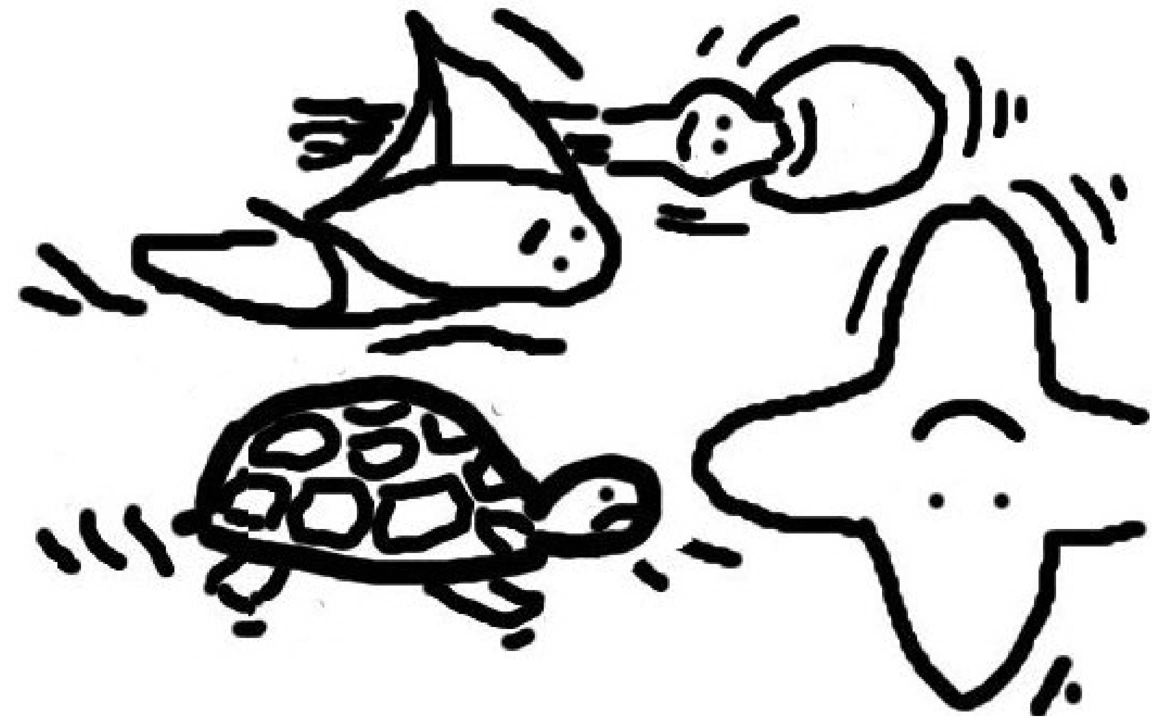

Feb


Mar


Feb

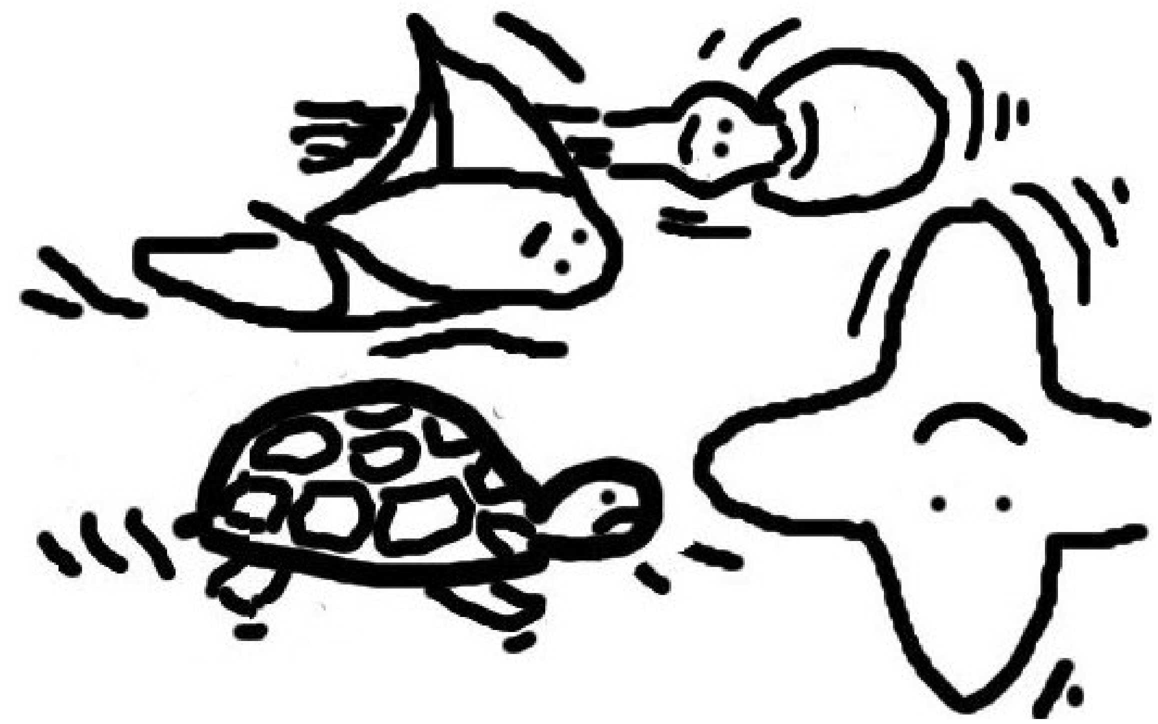

Mar

Mar



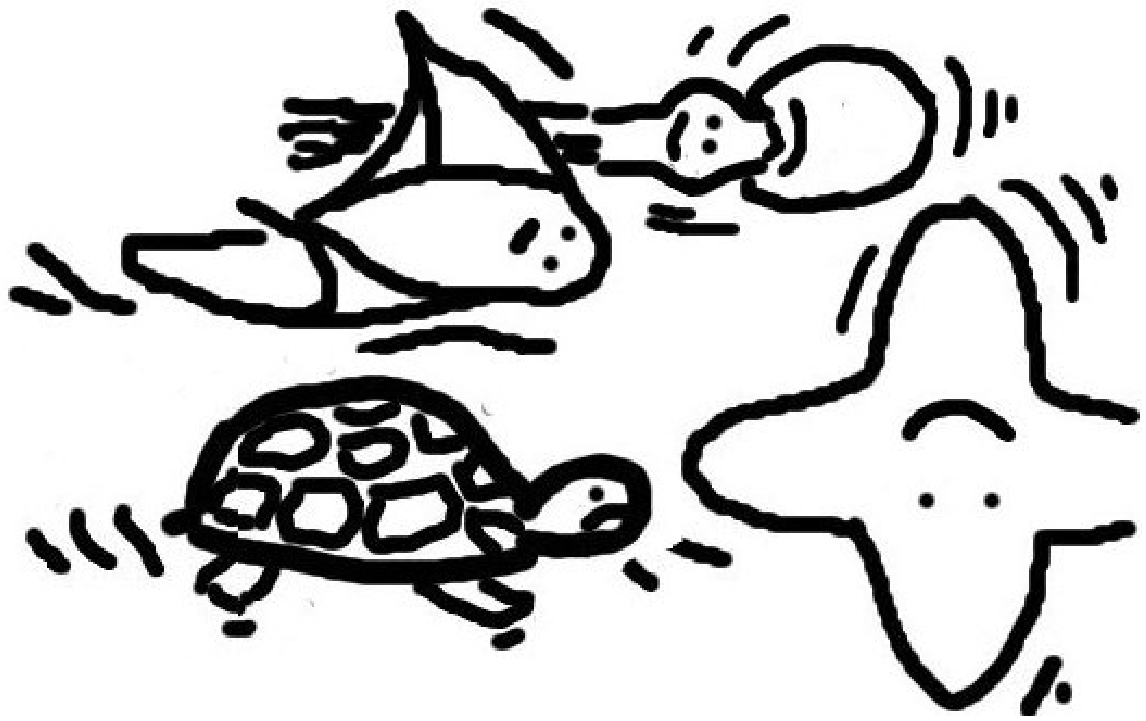
Zoo

Mar

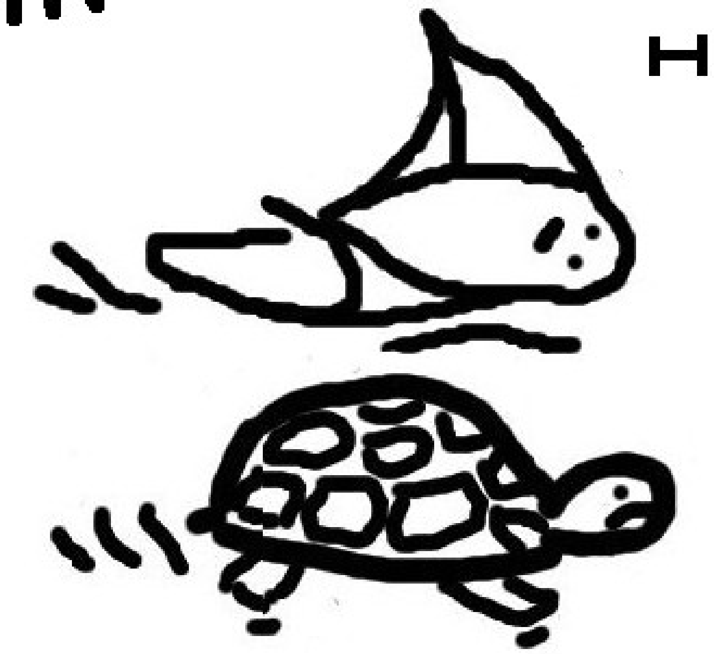


Zoom

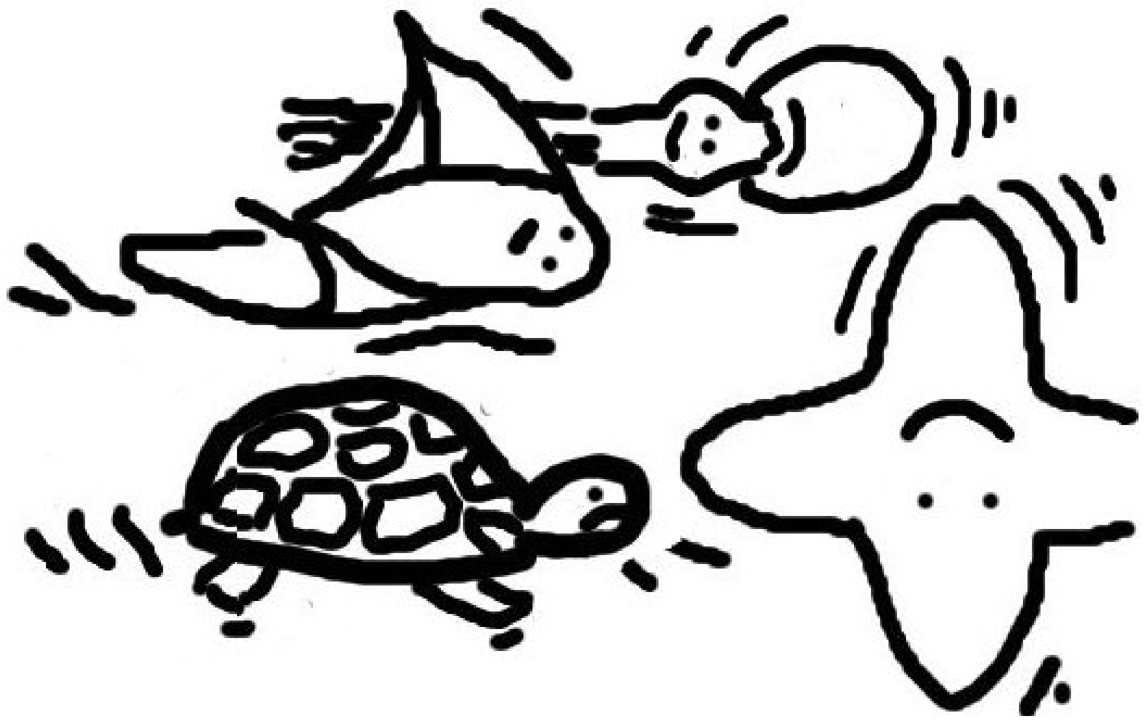
Mar



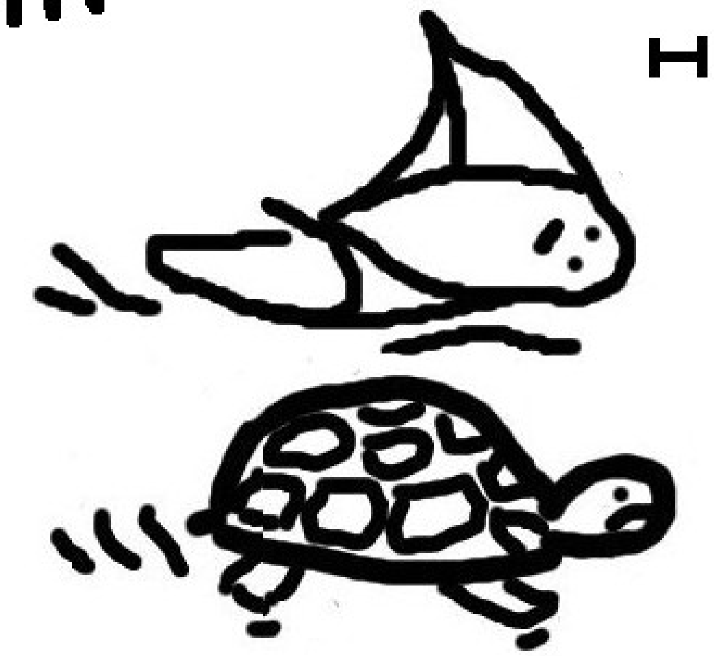
Zoom



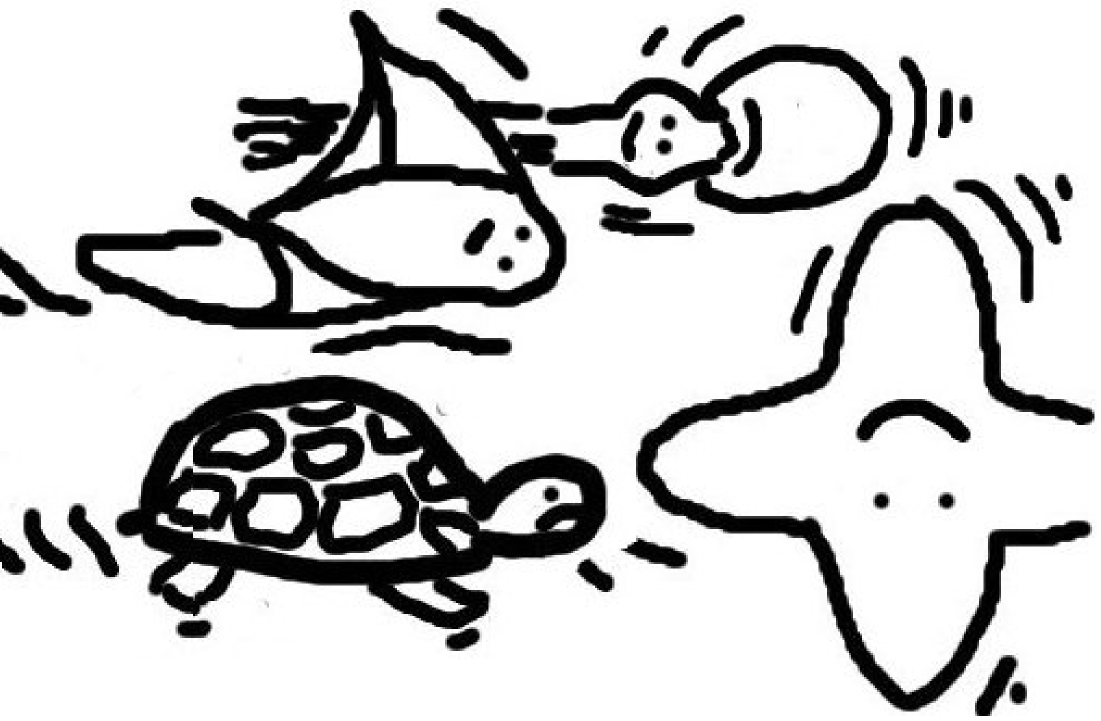
Mar



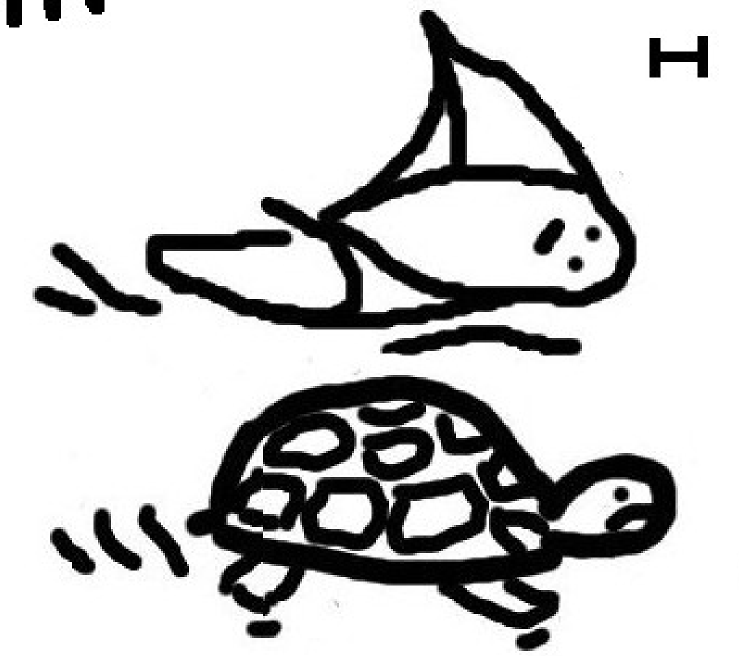
Zoom



r



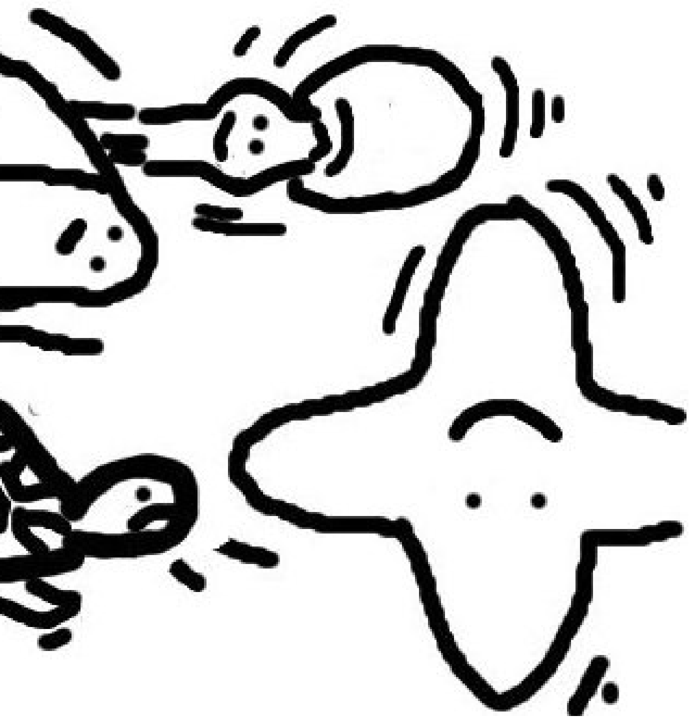
Zoom

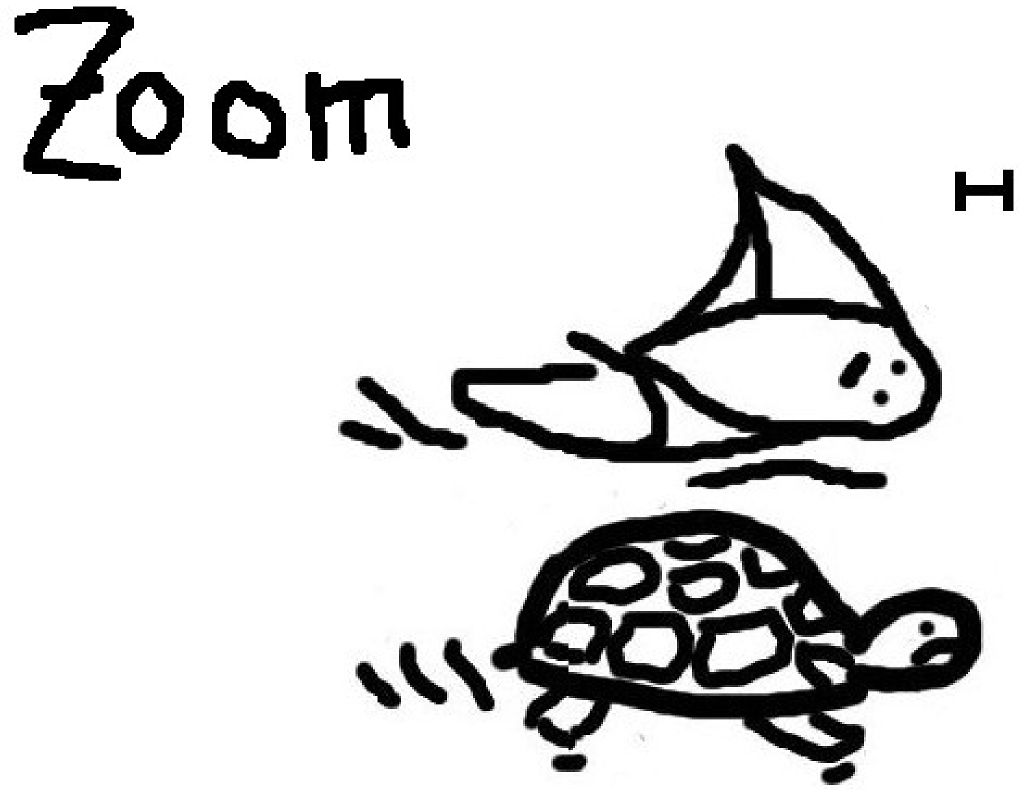


Faster H

2007 His

7.8**M** fo

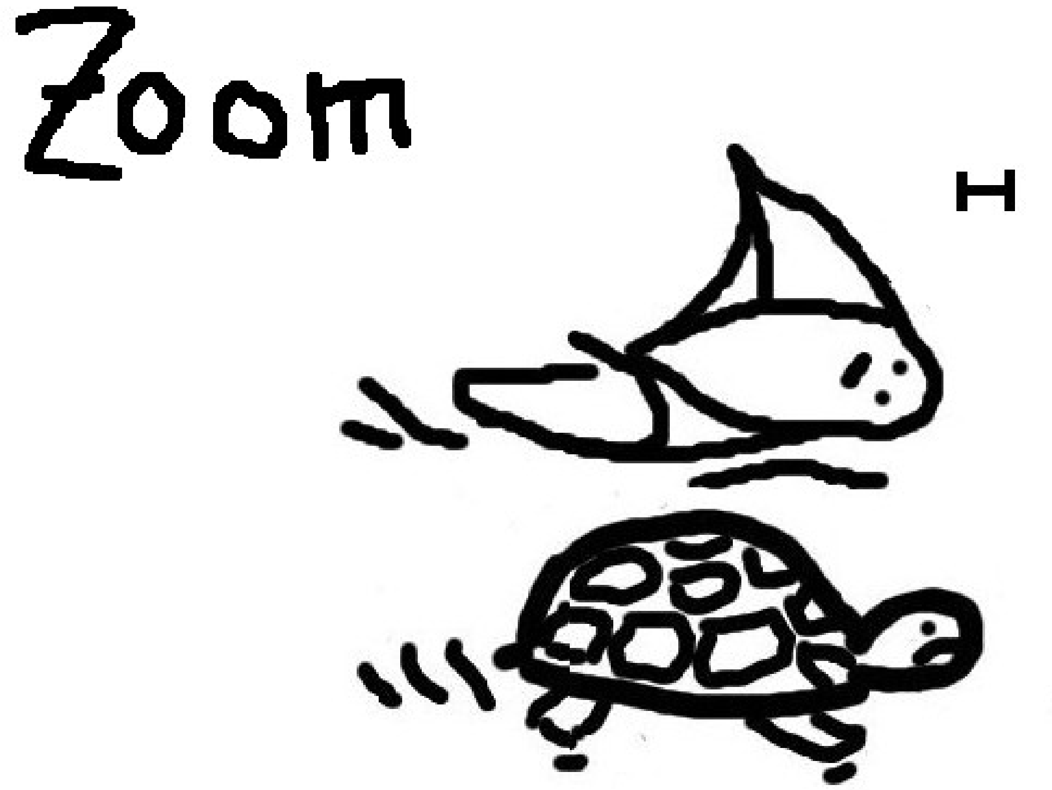




Faster Hessian arit

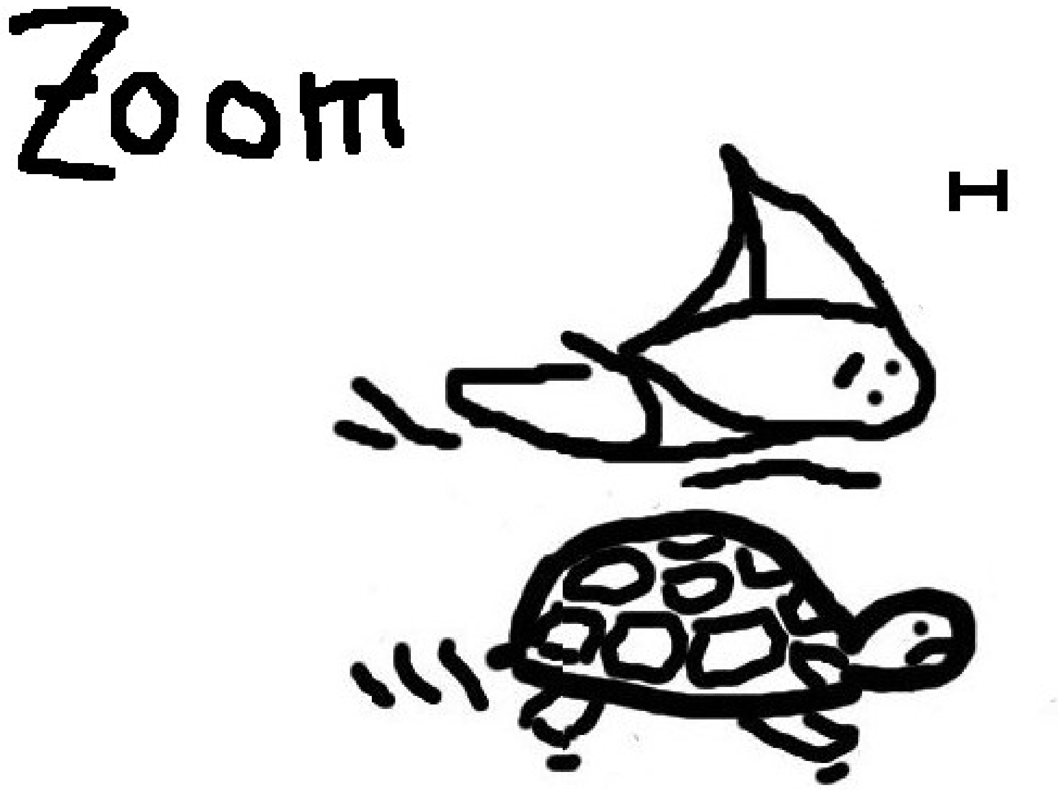
2007 Hisil–Carter–

7.8**M** for DBL.



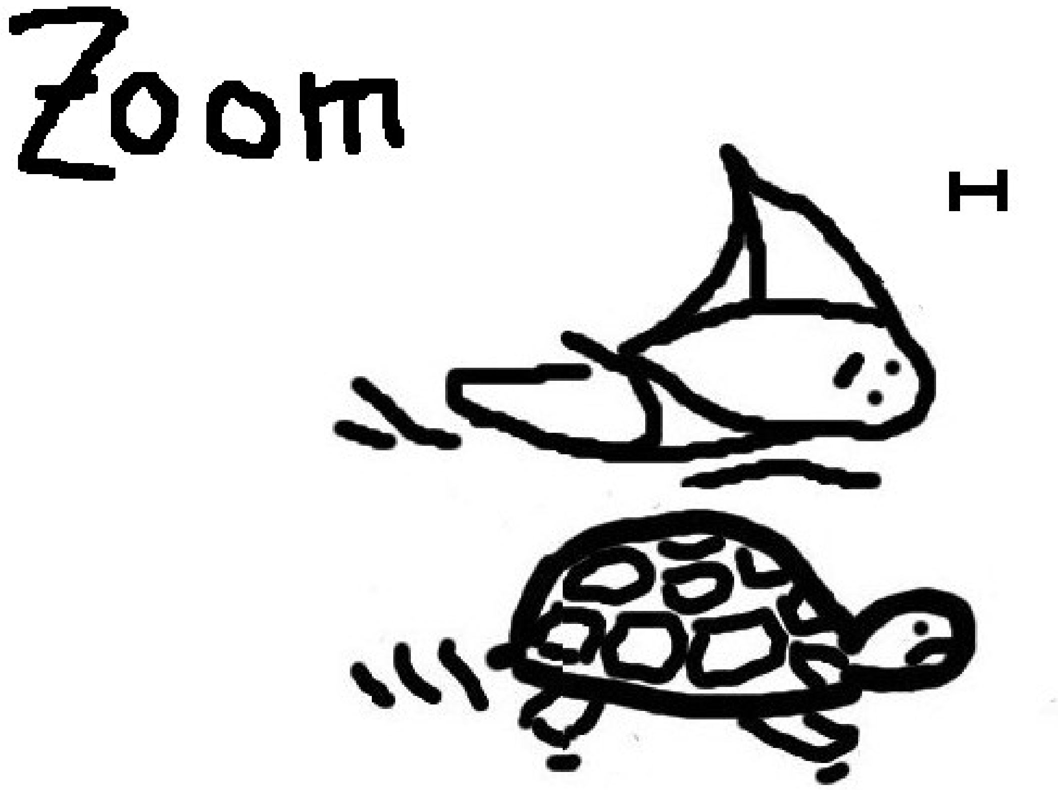
Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.



Faster Hessian arithmetic

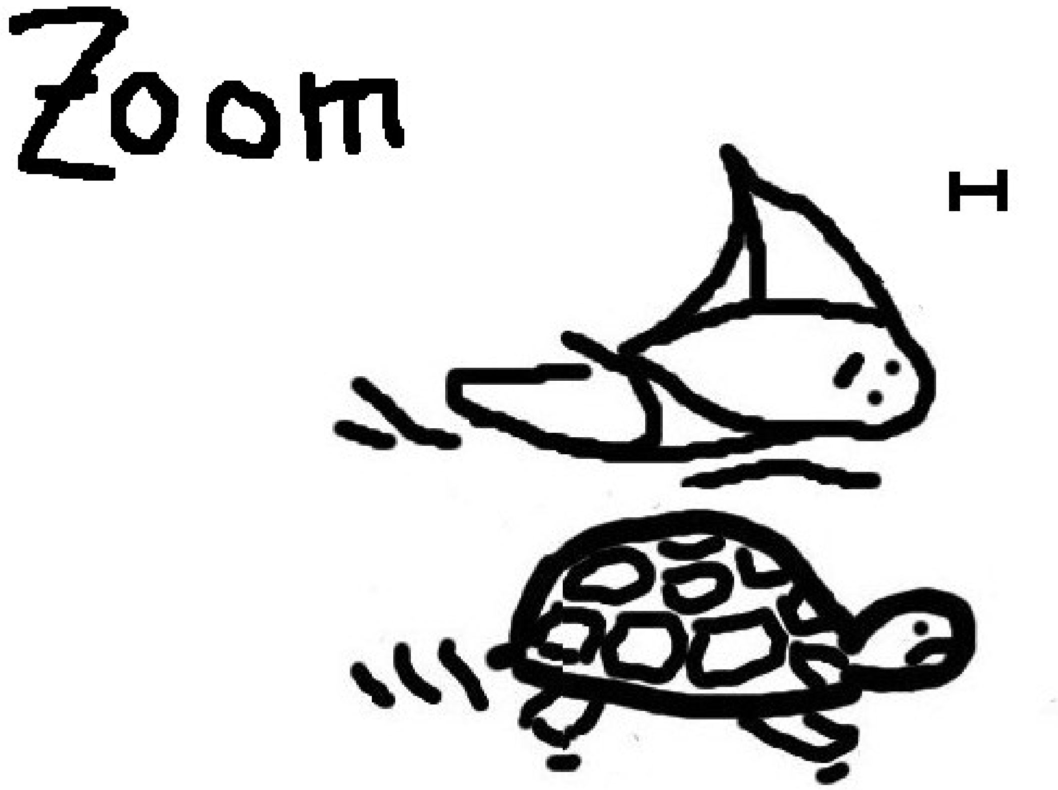
2007 Hisil–Carter–Dawson:
7.8**M** for DBL.



Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.



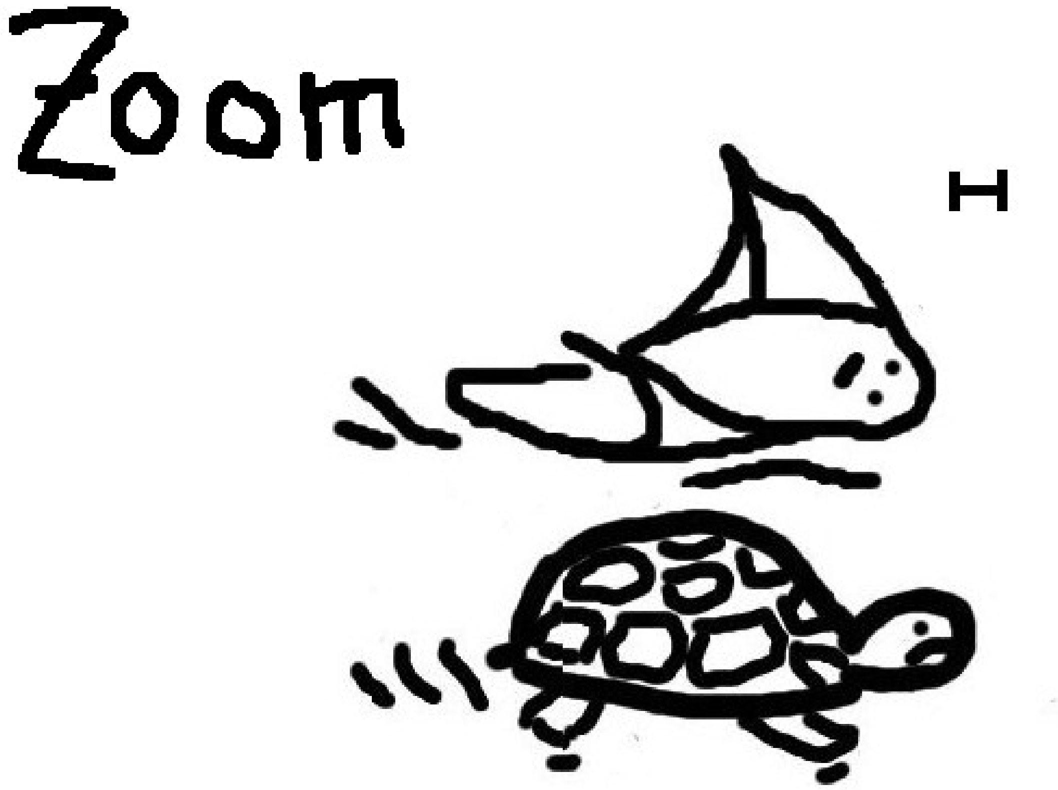
Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer: analyze exact **S**/**M**, overhead for checking for special cases, extra DBL, extra ADD, etc.



Faster Hessian arithmetic

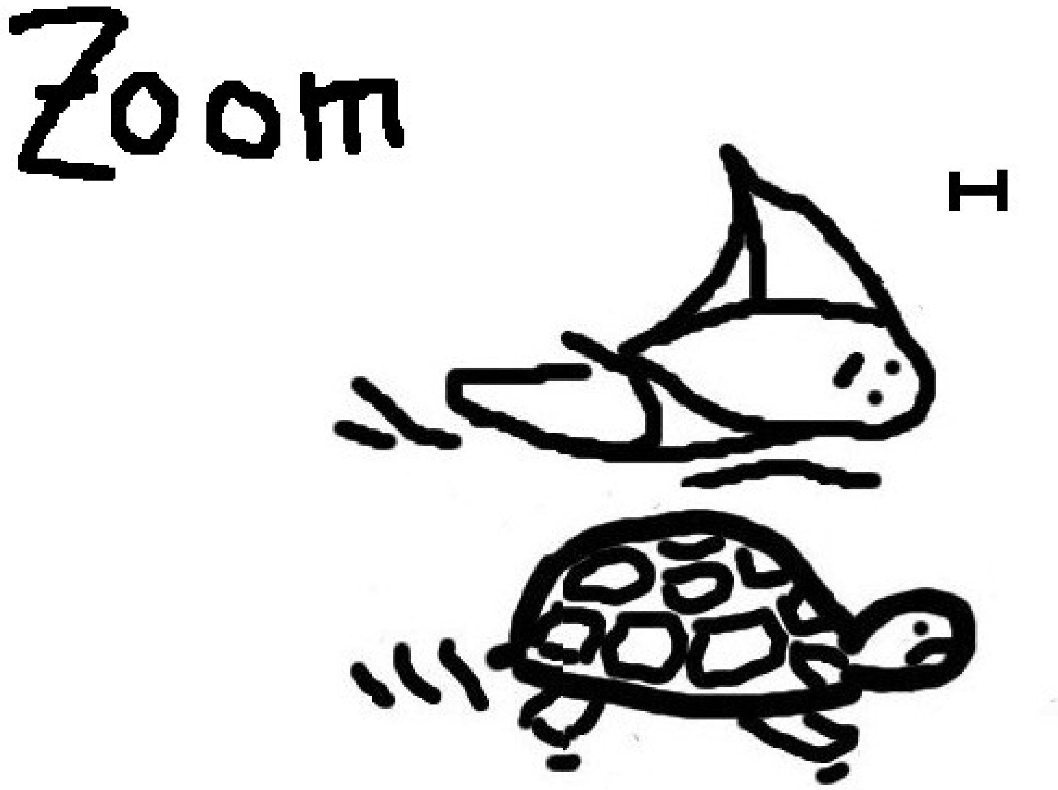
2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer:
analyze exact **S**/**M**, overhead for checking for special cases, extra DBL, extra ADD, etc.

Or speed up Hessian more.



Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for
DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer:
analyze exact **S**/**M**, overhead
for checking for special cases,
extra DBL, extra ADD, etc.

Or speed up Hessian more.

New: 7.6**M** for DBL.

Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer: analyze exact **S**/**M**, overhead for checking for special cases, extra DBL, extra ADD, etc.

Or speed up Hessian more.

New: 7.6**M** for DBL.

New (an

Generali
twisted
$aX^3 + Y$
with $a(2$

2007 7.8
2010 11
new 7.6

Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for
DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer:
analyze exact **S**/**M**, overhead
for checking for special cases,
extra DBL, extra ADD, etc.

Or speed up Hessian more.

New: 7.6**M** for DBL.

New (announced J

Generalize to more
twisted Hessian c
$aX^3 + Y^3 + Z^3 =$
with $a(27a - d^3)$

2007 7.8**M** DBL id
2010 11**M** ADD g
new 7.6**M** DBL ge

Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer: analyze exact **S**/**M**, overhead for checking for special cases, extra DBL, extra ADD, etc.

Or speed up Hessian more.

New: 7.6**M** for DBL.

New (announced July 2009)

Generalize to more curves: **twisted Hessian curves** $aX^3 + Y^3 + Z^3 = dXYZ$ with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, b
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer: analyze exact **S**/**M**, overhead for checking for special cases, extra DBL, extra ADD, etc.

Or speed up Hessian more.

New: 7.6**M** for DBL.

New (announced July 2009):

Generalize to more curves:
twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but 2010 11**M** ADD generalizes, new 7.6**M** DBL generalizes.

Faster Hessian arithmetic

2007 Hisil–Carter–Dawson:
7.8**M** for DBL.

2010 Hisil: 11**M** for ADD.

Hessian tied with Weierstrass for
DBL-DBL-DBL-DBL-DBL-ADD.

Need to zoom in closer:
analyze exact **S**/**M**, overhead
for checking for special cases,
extra DBL, extra ADD, etc.

Or speed up Hessian more.

New: 7.6**M** for DBL.

New (announced July 2009):

Generalize to more curves:
twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Rotate addition law
so that it also works for DBL;
complete if a is not a cube.
Eliminates special-case overhead,
helps stop side-channel attacks.

lessian arithmetic

sil–Carter–Dawson:
r DBL.

sil: 11**M** for ADD.

tied with Weierstrass for
BL-DBL-DBL-DBL-ADD.

zoom in closer:
exact **S**/**M**, overhead
king for special cases,
BL, extra ADD, etc.

d up Hessian more.

6**M** for DBL.

New (announced July 2009):

Generalize to more curves:
twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Rotate addition law
so that it also works for DBL;
complete if a is not a cube.
Eliminates special-case overhead,
helps stop side-channel attacks.

Triplings

TPL is *I*

2007 His
12.8**M** f

Generali

thmetic

-Dawson:

or ADD.

Weierstrass for
BL-DBL-ADD.

closer:
M, overhead
pecial cases,
ADD, etc.

an more.

BL.

New (announced July 2009):

Generalize to more curves:
twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Rotate addition law
so that it also works for DBL;
complete if a is not a cube.
Eliminates special-case overhead,
helps stop side-channel attacks.

Triplings (assumin

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–
12.8**M** for Hessian

Generalizes to twis

ss for
ADD.

d
s,

New (announced July 2009):

Generalize to more curves:
twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Rotate addition law
so that it also works for DBL;
complete if a is not a cube.
Eliminates special-case overhead,
helps stop side-channel attacks.

Triplings (assuming $d \neq 0$)

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson:
12.8**M** for Hessian TPL.

Generalizes to twisted Hessia

New (announced July 2009):

Generalize to more curves:

twisted Hessian curves

$aX^3 + Y^3 + Z^3 = dXYZ$

with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but

2010 11**M** ADD generalizes,

new 7.6**M** DBL generalizes.

Rotate addition law

so that it also works for DBL;

complete if a is not a cube.

Eliminates special-case overhead,

helps stop side-channel attacks.

<u>Triplings (assuming $d \neq 0$)</u>

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson:

12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

New (announced July 2009):

Generalize to more curves:

twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Rotate addition law
so that it also works for DBL;
complete if a is not a cube.
Eliminates special-case overhead,
helps stop side-channel attacks.

Triplings (assuming $d \neq 0$)

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson:
12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

2015 Kohel: 11.2**M**.

New (announced July 2009):

Generalize to more curves:
twisted Hessian curves
$aX^3 + Y^3 + Z^3 = dXYZ$
with $a(27a - d^3) \neq 0$.

2007 7.8**M** DBL idea fails, but
2010 11**M** ADD generalizes,
new 7.6**M** DBL generalizes.

Rotate addition law
so that it also works for DBL;
complete if a is not a cube.
Eliminates special-case overhead,
helps stop side-channel attacks.

Triplings (assuming $d \neq 0$)

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson:
12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

2015 Kohel: 11.2**M**.

New: 10.8**M** assuming
field with fast primitive $\sqrt[3]{1}$;
e.g., $\mathbf{F}_q[\omega]/(\omega^2 + \omega + 1)$, or
$\mathbf{F}_p$ with $7p = 2^{298} + 2^{149} + 1$.

(More history in small char.
See paper for details.)

nnounced July 2009):

ze to more curves:

Hessian curves

$Y^3 + Z^3 = dXYZ$

$27a - d^3) \neq 0$.

3**M** DBL idea fails, but

M ADD generalizes,

M DBL generalizes.

addition law

't also works for DBL;

te if a is not a cube.

es special-case overhead,

op side-channel attacks.

<u>Triplings (assuming $d \neq 0$)</u>

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson: 12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

2015 Kohel: 11.2**M**.

New: 10.8**M** assuming field with fast primitive $\sqrt[3]{1}$; e.g., $\mathbf{F}_q[\omega]/(\omega^2 + \omega + 1)$, or $\mathbf{F}_p$ with $7p = 2^{298} + 2^{149} + 1$.

(More history in small char. See paper for details.)

If $aX^3 +$

then VW

where

$U = -X$

If $VW(V$

then aX

where Q

$S = -(V$

$dX_3 = F$

$Y_3 = RS$

$Z_3 = RV$

Compose

$(X_3 : Y_3$

July 2009):

e curves:

curves

$= dXYZ$

$\neq 0$.

dea fails, but

eneralizes,

eneralizes.

aw

ks for DBL;

not a cube.

-case overhead,

annel attacks.

Triplings (assuming $d \neq 0$)

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson:
12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

2015 Kohel: 11.2**M**.

New: 10.8**M** assuming
field with fast primitive $\sqrt[3]{1}$;
e.g., $\mathbf{F}_q[\omega]/(\omega^2 + \omega + 1)$, or
$\mathbf{F}_p$ with $7p = 2^{298} + 2^{149} + 1$.

(More history in small char.
See paper for details.)

If $aX^3 + Y^3 + Z^3$
then $VW(V + dU$
where
$U = -XYZ$, $V =$

If $VW(V + dU +$
then $aX_3^3 + Y_3^3 +$
where $Q = dU$, R
$S = -(V + Q + R$
$dX_3 = R^3 + S^3 +$
$Y_3 = RS^2 + SV^2$
$Z_3 = RV^2 + SR^2$

Compose these 3-i
$(X_3 : Y_3 : Z_3) = 3$

:

out

,

L;

.

head,

cks.

Triplings (assuming $d \neq 0$)

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson:
12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

2015 Kohel: 11.2**M**.

New: 10.8**M** assuming
field with fast primitive $\sqrt[3]{1}$;
e.g., $\mathbf{F}_q[\omega]/(\omega^2+\omega+1)$, or
$\mathbf{F}_p$ with $7p = 2^{298}+2^{149}+1$.

(More history in small char.
See paper for details.)

If $aX^3+Y^3+Z^3=dXYZ$
then $VW(V+dU+aW)=$
where
$U=-XYZ$, $V=Y^3$, $W=$

If $VW(V+dU+aW)=U^3$
then $aX_3^3+Y_3^3+Z_3^3=dX_3$
where $Q=dU$, $R=aW$,
$S=-(V+Q+R)$,
$dX_3=R^3+S^3+V^3-3RS$
$Y_3=RS^2+SV^2+VR^2-3$
$Z_3=RV^2+SR^2+VS^2-3$

Compose these 3-isogenies:
$(X_3:Y_3:Z_3)=3(X:Y:Z$

Triplings (assuming $d \neq 0$)

TPL is $P \mapsto 3P$.

2007 Hisil–Carter–Dawson: 12.8**M** for Hessian TPL.

Generalizes to twisted Hessian.

2015 Kohel: 11.2**M**.

New: 10.8**M** assuming field with fast primitive $\sqrt[3]{1}$; e.g., $\mathbf{F}_q[\omega]/(\omega^2+\omega+1)$, or $\mathbf{F}_p$ with $7p = 2^{298}+2^{149}+1$.

(More history in small char. See paper for details.)

If $aX^3+Y^3+Z^3 = dXYZ$ then $VW(V+dU+aW) = U^3$ where $U = -XYZ$, $V = Y^3$, $W = X^3$.

If $VW(V+dU+aW) = U^3$ then $aX_3^3+Y_3^3+Z_3^3 = dX_3Y_3Z_3$ where $Q = dU$, $R = aW$,
$S = -(V+Q+R)$,
$dX_3 = R^3+S^3+V^3-3RSV$,
$Y_3 = RS^2+SV^2+VR^2-3RSV$,
$Z_3 = RV^2+SR^2+VS^2-3RSV$.

Compose these 3-isogenies: $(X_3 : Y_3 : Z_3) = 3(X : Y : Z)$.

s (assuming $d \neq 0$)

$P \mapsto 3P$.

sil–Carter–Dawson:
or Hessian TPL.

zes to twisted Hessian.

hel: 11.2**M**.

.8**M** assuming
h fast primitive $\sqrt[3]{1}$;
$\omega]/(\omega^2+\omega+1)$, or
$7p = 2^{298}+2^{149}+1$.

istory in small char.
er for details.)

If $aX^3+Y^3+Z^3 = dXYZ$
then $VW(V+dU+aW) = U^3$
where
$U = -XYZ$, $V = Y^3$, $W = X^3$.

If $VW(V+dU+aW) = U^3$
then $aX_3^3+Y_3^3+Z_3^3 = dX_3Y_3Z_3$
where $Q = dU$, $R = aW$,
$S = -(V+Q+R)$,
$dX_3 = R^3+S^3+V^3-3RSV$,
$Y_3 = RS^2+SV^2+VR^2-3RSV$,
$Z_3 = RV^2+SR^2+VS^2-3RSV$.

Compose these 3-isogenies:
$(X_3 : Y_3 : Z_3) = 3(X : Y : Z)$.

To quick

Three cu

For three
(α,β,γ)
$(\alpha R+\beta$
$(\alpha S+\beta$
$(\alpha V+\beta$
$= \alpha\beta\gamma d$
$+ (\alpha\beta^2$
$+ (\beta\alpha^2$
$+ (\alpha+\beta$

Also use
Solve for

g $d \neq 0$)

-Dawson:

n TPL.

sted Hessian.

M.

ming

nitive $\sqrt[3]{1}$;

$\omega + 1$), or

$+ 2^{149} + 1$.

mall char.

ils.)

If $aX^3 + Y^3 + Z^3 = dXYZ$
then $VW(V + dU + aW) = U^3$
where
$U = -XYZ$, $V = Y^3$, $W = X^3$.

If $VW(V + dU + aW) = U^3$
then $aX_3^3 + Y_3^3 + Z_3^3 = dX_3Y_3Z_3$
where $Q = dU$, $R = aW$,
$S = -(V + Q + R)$,
$dX_3 = R^3 + S^3 + V^3 - 3RSV$,
$Y_3 = RS^2 + SV^2 + VR^2 - 3RSV$,
$Z_3 = RV^2 + SR^2 + VS^2 - 3RSV$.

Compose these 3-isogenies:
$(X_3 : Y_3 : Z_3) = 3(X : Y : Z)$.

To quickly triple (

Three cubings for

For three choices o
(α, β, γ) compute
$(\alpha R + \beta S + \gamma V)$
$(\alpha S + \beta V + \gamma R)$
$(\alpha V + \beta R + \gamma S)$
$= \alpha\beta\gamma dX_3$
$+ (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha$
$+ (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma$
$+ (\alpha + \beta + \gamma)^3 RSV$

Also use $a(R + S +$
Solve for $dX_3, Y_3,$

an.

1.

If $aX^3 + Y^3 + Z^3 = dXYZ$
then $VW(V + dU + aW) = U^3$
where
$U = -XYZ$, $V = Y^3$, $W = X^3$.

If $VW(V + dU + aW) = U^3$
then $aX_3^3 + Y_3^3 + Z_3^3 = dX_3Y_3Z_3$
where $Q = dU$, $R = aW$,
$S = -(V + Q + R)$,
$dX_3 = R^3 + S^3 + V^3 - 3RSV$,
$Y_3 = RS^2 + SV^2 + VR^2 - 3RSV$,
$Z_3 = RV^2 + SR^2 + VS^2 - 3RSV$.

Compose these 3-isogenies:
$(X_3 : Y_3 : Z_3) = 3(X : Y : Z)$.

To quickly triple $(X : Y : Z)$

Three cubings for R, S, V.

For three choices of constan
(α, β, γ) compute
$(\alpha R + \beta S + \gamma V) \cdot$
$(\alpha S + \beta V + \gamma R) \cdot$
$(\alpha V + \beta R + \gamma S)$
$= \alpha\beta\gamma dX_3$
$+ (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2)Y_3$
$+ (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2)Z_3$
$+ (\alpha + \beta + \gamma)^3 RSV$.

Also use $a(R + S + V)^3 = d$
Solve for dX_3, Y_3, Z_3.

If $aX^3 + Y^3 + Z^3 = dXYZ$
then $VW(V + dU + aW) = U^3$
where
$U = -XYZ$, $V = Y^3$, $W = X^3$.

If $VW(V + dU + aW) = U^3$
then $aX_3^3 + Y_3^3 + Z_3^3 = dX_3Y_3Z_3$
where $Q = dU$, $R = aW$,
$S = -(V + Q + R)$,
$dX_3 = R^3 + S^3 + V^3 - 3RSV$,
$Y_3 = RS^2 + SV^2 + VR^2 - 3RSV$,
$Z_3 = RV^2 + SR^2 + VS^2 - 3RSV$.

Compose these 3-isogenies:
$(X_3 : Y_3 : Z_3) = 3(X : Y : Z)$.

To quickly triple $(X : Y : Z)$:

Three cubings for R, S, V.

For three choices of constants
(α, β, γ) compute
$(\alpha R + \beta S + \gamma V) \cdot$
$(\alpha S + \beta V + \gamma R) \cdot$
$(\alpha V + \beta R + \gamma S)$
$= \alpha\beta\gamma dX_3$
$+ (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2)Y_3$
$+ (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2)Z_3$
$+ (\alpha + \beta + \gamma)^3 RSV$.

Also use $a(R + S + V)^3 = d^3RSV$.
Solve for dX_3, Y_3, Z_3.

$-Y^3 + Z^3 = dXYZ$

$V(V + dU + aW) = U^3$

XYZ, $V = Y^3$, $W = X^3$.

$/ + dU + aW) = U^3$

$^3_3 + Y_3^3 + Z_3^3 = dX_3Y_3Z_3$

$= dU$, $R = aW$,

$/ + Q + R)$,

$R^3 + S^3 + V^3 - 3RSV$,

$S^2 + SV^2 + VR^2 - 3RSV$,

$V^2 + SR^2 + VS^2 - 3RSV$.

e these 3-isogenies:

$: Z_3) = 3(X : Y : Z)$.

To quickly triple $(X : Y : Z)$:

Three cubings for R, S, V.

For three choices of constants (α, β, γ) compute

$$(\alpha R + \beta S + \gamma V) \cdot (\alpha S + \beta V + \gamma R) \cdot (\alpha V + \beta R + \gamma S)$$
$$= \alpha\beta\gamma dX_3 + (\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)Y_3 + (\beta\alpha^2+\gamma\beta^2+\alpha\gamma^2)Z_3 + (\alpha+\beta+\gamma)^3 RSV.$$

Also use $a(R+S+V)^3 = d^3RSV$.

Solve for dX_3, Y_3, Z_3.

2015 Ko

(4 cubin

introduc

(α, β, γ)

(α, β, γ)

(α, β, γ)

$= dXYZ$

$+ aW) = U^3$

Y^3, $W = X^3$.

$aW) = U^3$

$Z_3^3 = dX_3Y_3Z_3$

$= aW$,

$R)$,

$V^3 - 3RSV$,

$+VR^2 - 3RSV$,

$+VS^2 - 3RSV$.

isogenies:

$(X : Y : Z)$.

To quickly triple $(X : Y : Z)$:

Three cubings for R, S, V.

For three choices of constants (α, β, γ) compute

$(\alpha R + \beta S + \gamma V) \cdot$
$(\alpha S + \beta V + \gamma R) \cdot$
$(\alpha V + \beta R + \gamma S)$
$= \alpha\beta\gamma dX_3$
$+ (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) Y_3$
$+ (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2) Z_3$
$+ (\alpha + \beta + \gamma)^3 RSV$.

Also use $a(R + S + V)^3 = d^3 RSV$.
Solve for dX_3, Y_3, Z_3.

2015 Kohel's 11.2

(4 cubings + 4 mu

introduced this TR

$(\alpha, \beta, \gamma) = (1, 1, 1$

$(\alpha, \beta, \gamma) = (1, -1$

$(\alpha, \beta, \gamma) = (1, 1, 0$

U^3

X^3.

3

$Y_3 Z_3$

SV,

$3RSV$,

$3RSV$.

).

To quickly triple $(X : Y : Z)$:

Three cubings for R, S, V.

For three choices of constants (α, β, γ) compute
$(\alpha R + \beta S + \gamma V) \cdot$
$(\alpha S + \beta V + \gamma R) \cdot$
$(\alpha V + \beta R + \gamma S)$
$= \alpha\beta\gamma d X_3$
$+ (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) Y_3$
$+ (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2) Z_3$
$+ (\alpha + \beta + \gamma)^3 RSV$.

Also use $a(R+S+V)^3 = d^3 RSV$.
Solve for dX_3, Y_3, Z_3.

2015 Kohel's 11.2**M**
(4 cubings + 4 mults)
introduced this TPL idea wi
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, -1, 0)$,
$(\alpha, \beta, \gamma) = (1, 1, 0)$.

To quickly triple $(X : Y : Z)$:

Three cubings for R, S, V.

For three choices of constants (α, β, γ) compute

$$(\alpha R + \beta S + \gamma V) \cdot$$
$$(\alpha S + \beta V + \gamma R) \cdot$$
$$(\alpha V + \beta R + \gamma S)$$
$$= \alpha\beta\gamma d X_3$$
$$+ (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) Y_3$$
$$+ (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2) Z_3$$
$$+ (\alpha + \beta + \gamma)^3 RSV.$$

Also use $a(R + S + V)^3 = d^3 RSV$.

Solve for dX_3, Y_3, Z_3.

2015 Kohel's 11.2**M**

(4 cubings + 4 mults)

introduced this TPL idea with

$(\alpha, \beta, \gamma) = (1, 1, 1)$,

$(\alpha, \beta, \gamma) = (1, -1, 0)$,

$(\alpha, \beta, \gamma) = (1, 1, 0)$.

To quickly triple $(X : Y : Z)$:

Three cubings for R, S, V.

For three choices of constants (α, β, γ) compute

$$(\alpha R + \beta S + \gamma V) \cdot (\alpha S + \beta V + \gamma R) \cdot (\alpha V + \beta R + \gamma S)$$
$$= \alpha\beta\gamma d X_3 + (\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) Y_3 + (\beta\alpha^2 + \gamma\beta^2 + \alpha\gamma^2) Z_3 + (\alpha + \beta + \gamma)^3 RSV.$$

Also use $a(R+S+V)^3 = d^3 RSV$.
Solve for dX_3, Y_3, Z_3.

2015 Kohel's 11.2**M** (4 cubings + 4 mults) introduced this TPL idea with
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, -1, 0)$,
$(\alpha, \beta, \gamma) = (1, 1, 0)$.

New 10.8**M** (6 cubings) makes faster choices assuming fast primitive $\omega = \sqrt[3]{1}$:
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, \omega, \omega^2)$,
$(\alpha, \beta, \gamma) = (1, \omega^2, \omega)$.

kly triple $(X : Y : Z)$:

ubings for R, S, V.

e choices of constants
) compute
$\beta S + \gamma V) \cdot$
$\beta V + \gamma R) \cdot$
$\beta R + \gamma S)$
X_3
$+\beta\gamma^2+\gamma\alpha^2)Y_3$
$+\gamma\beta^2+\alpha\gamma^2)Z_3$
$+\gamma)^3 RSV$.

$a(R+S+V)^3 = d^3 RSV$.
r dX_3, Y_3, Z_3.

2015 Kohel's 11.2**M**
(4 cubings + 4 mults)
introduced this TPL idea with
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, -1, 0)$,
$(\alpha, \beta, \gamma) = (1, 1, 0)$.

New 10.8**M** (6 cubings)
makes faster choices
assuming fast primitive $\omega = \sqrt[3]{1}$:
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, \omega, \omega^2)$,
$(\alpha, \beta, \gamma) = (1, \omega^2, \omega)$.

Are tripl

2005 Di
"double-
compute
$2^{15}3^2 P$
$+ 2$
2TPL, 1

2006 Do
generaliz
e.g., con
$2^{12}3^3 3P$
after pre
3TPL, 1

$X : Y : Z$):

R, S, V.

of constants

$^2)Y_3$

$^2)Z_3$

V.

$+V)^3 = d^3 RSV$.

Z_3.

2015 Kohel's 11.2**M** (4 cubings + 4 mults) introduced this TPL idea with
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, -1, 0)$,
$(\alpha, \beta, \gamma) = (1, 1, 0)$.

New 10.8**M** (6 cubings) makes faster choices assuming fast primitive $\omega = \sqrt[3]{1}$:
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, \omega, \omega^2)$,
$(\alpha, \beta, \gamma) = (1, \omega^2, \omega)$.

Are triplings usefu

2005 Dimitrov–Im
"double-base chai
compute 314159P
$2^{15}3^2P + 2^{11}3^2P$
$+ 2^4 3^1 P - 2$
2TPL, 15DBL, 4A

2006 Doche–Imbe
generalized double
e.g., compute 314
$2^{12}3^3 3P - 2^7 3^3 5P$
after precomputin
3TPL, 13DBL, 6A

):

ts

^3RSV.

2015 Kohel's 11.2**M**
(4 cubings + 4 mults)
introduced this TPL idea with
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, -1, 0)$,
$(\alpha, \beta, \gamma) = (1, 1, 0)$.

New 10.8**M** (6 cubings)
makes faster choices
assuming fast primitive $\omega = \sqrt[3]{1}$:
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, \omega, \omega^2)$,
$(\alpha, \beta, \gamma) = (1, \omega^2, \omega)$.

Are triplings useful?

2005 Dimitrov–Imbert–Mish
"double-base chains": e.g.,
compute $314159P$ as
$$2^{15}3^2P + 2^{11}3^2P + 2^8 3^1 P$$
$$+ 2^4 3^1 P - 2^0 3^0 P.$$
2TPL, 15DBL, 4ADD.

2006 Doche–Imbert
generalized double-base chai
e.g., compute $314159P$ as
$2^{12}3^3 3P - 2^7 3^3 5P - 2^4 3^1 7P -$
after precomputing $3P, 5P, 7$
3TPL, 13DBL, 6ADD.

2015 Kohel's 11.2**M**
(4 cubings + 4 mults)
introduced this TPL idea with
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, -1, 0)$,
$(\alpha, \beta, \gamma) = (1, 1, 0)$.

New 10.8**M** (6 cubings)
makes faster choices
assuming fast primitive $\omega = \sqrt[3]{1}$:
$(\alpha, \beta, \gamma) = (1, 1, 1)$,
$(\alpha, \beta, \gamma) = (1, \omega, \omega^2)$,
$(\alpha, \beta, \gamma) = (1, \omega^2, \omega)$.

<u>Are triplings useful?</u>

2005 Dimitrov–Imbert–Mishra
"double-base chains": e.g.,
compute $314159P$ as

$$2^{15}3^2P + 2^{11}3^2P + 2^8 3^1 P + 2^4 3^1 P - 2^0 3^0 P.$$

2TPL, 15DBL, 4ADD.

2006 Doche–Imbert
generalized double-base chains:
e.g., compute $314159P$ as

$$2^{12}3^3 3P - 2^7 3^3 5P - 2^4 3^1 7P - 2^0 3^0 P$$

after precomputing $3P, 5P, 7P$.
3TPL, 13DBL, 6ADD.

hel's 11.2**M**
gs + 4 mults)
ed this TPL idea with
$) = (1, 1, 1)$,
$) = (1, -1, 0)$,
$) = (1, 1, 0)$.

8**M** (6 cubings)
aster choices
g fast primitive $\omega = \sqrt[3]{1}$:
$) = (1, 1, 1)$,
$) = (1, \omega, \omega^2)$,
$) = (1, \omega^2, \omega)$.

Are triplings useful?

2005 Dimitrov–Imbert–Mishra "double-base chains": e.g., compute $314159P$ as
$$2^{15}3^2P + 2^{11}3^2P + 2^8 3^1 P + 2^4 3^1 P - 2^0 3^0 P.$$
2TPL, 15DBL, 4ADD.

2006 Doche–Imbert generalized double-base chains: e.g., compute $314159P$ as
$$2^{12}3^3 3P - 2^7 3^3 5P - 2^4 3^1 7P - 2^0 3^0 P$$
after precomputing $3P, 5P, 7P$.
3TPL, 13DBL, 6ADD.

Not goo
Good fo
factoriza

Also nee
Good fo

M

ults)

PL idea with

),

, 0),

)).

bings)

ces

nitive $\omega = \sqrt[3]{1}$:

),

ω^2),

ω).

Are triplings useful?

2005 Dimitrov–Imbert–Mishra "double-base chains": e.g., compute $314159P$ as

$$2^{15}3^2P + 2^{11}3^2P + 2^83^1P + 2^43^1P - 2^03^0P.$$

2TPL, 15DBL, 4ADD.

2006 Doche–Imbert generalized double-base chains: e.g., compute $314159P$ as

$$2^{12}3^33P - 2^73^35P - 2^43^17P - 2^03^0P$$

after precomputing $3P, 5P, 7P$.

3TPL, 13DBL, 6ADD.

Not good for cons

Good for signature

factorization, matl

Also need time to

Good for scalars u

th

$\sqrt[3]{1}$:

Are triplings useful?

2005 Dimitrov–Imbert–Mishra "double-base chains": e.g., compute $314159P$ as
$$2^{15}3^2P + 2^{11}3^2P + 2^8 3^1 P + 2^4 3^1 P - 2^0 3^0 P.$$
2TPL, 15DBL, 4ADD.

2006 Doche–Imbert generalized double-base chains: e.g., compute $314159P$ as
$$2^{12}3^3 3P - 2^7 3^3 5P - 2^4 3^1 7P - 2^0 3^0 P$$
after precomputing $3P, 5P, 7P$.
3TPL, 13DBL, 6ADD.

Not good for constant time.
Good for signature verificati
factorization, math, etc.

Also need time to compute
Good for scalars used many

Are triplings useful?

2005 Dimitrov–Imbert–Mishra "double-base chains": e.g., compute $314159P$ as

$$2^{15}3^2P + 2^{11}3^2P + 2^8 3^1 P + 2^4 3^1 P - 2^0 3^0 P.$$

2TPL, 15DBL, 4ADD.

2006 Doche–Imbert generalized double-base chains: e.g., compute $314159P$ as

$$2^{12}3^3 3P - 2^7 3^3 5P - 2^4 3^1 7P - 2^0 3^0 P$$

after precomputing $3P, 5P, 7P$.
3TPL, 13DBL, 6ADD.

Not good for constant time.
Good for signature verification, factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Are triplings useful?

2005 Dimitrov–Imbert–Mishra "double-base chains": e.g., compute $314159P$ as

$$2^{15}3^2P + 2^{11}3^2P + 2^83^1P + 2^43^1P - 2^03^0P.$$

2TPL, 15DBL, 4ADD.

2006 Doche–Imbert generalized double-base chains: e.g., compute $314159P$ as

$$2^{12}3^33P - 2^73^35P - 2^43^17P - 2^03^0P$$

after precomputing $3P, 5P, 7P$.
3TPL, 13DBL, 6ADD.

Not good for constant time.
Good for signature verification, factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007 Bernstein–Birkner–Lange–Peters:

Double-base chains speed up Weierstrass curves slightly: 9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian: 9.65**M**/bit. Still not competitive.

ings useful?

mitrov–Imbert–Mishra
-base chains": e.g.,
e $314159P$ as
$+ 2^{11}3^2P + 2^8 3^1 P$
$2^4 3^1 P - 2^0 3^0 P$.
5DBL, 4ADD.

oche–Imbert
zed double-base chains:
mpute $314159P$ as
$-2^7 3^3 5P - 2^4 3^1 7P - 2^0 3^0 P$
ecomputing $3P, 5P, 7P$.
3DBL, 6ADD.

Not good for constant time.
Good for signature verification,
factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007
Bernstein–Birkner–Lange–Peters:

Double-base chains speed up
Weierstrass curves slightly:
9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian:
9.65**M**/bit. Still not competitive.

Revisit c
using lat
latest do

l?

bert–Mishra
ns": e.g.,
as
$+ 2^8 3^1 P$
$^0 3^0 P$.
DD.

rt
e-base chains:
$159P$ as
$-2^4 3^1 7P - 2^0 3^0 P$
g $3P, 5P, 7P$.
DD.

Not good for constant time.
Good for signature verification, factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007 Bernstein–Birkner–Lange–Peters:

Double-base chains speed up Weierstrass curves slightly: 9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian: 9.65**M**/bit. Still not competitive.

Revisit conclusions
using latest Hessia
latest double-base

ra

ins:

$-2^0 3^0 P$

P.

Not good for constant time.
Good for signature verification,
factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007
Bernstein–Birkner–Lange–Peters:

Double-base chains speed up
Weierstrass curves slightly:
9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian:
9.65**M**/bit. Still not competitive.

Revisit conclusions
using latest Hessian formula
latest double-base technique

Not good for constant time.
Good for signature verification,
factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007
Bernstein–Birkner–Lange–Peters:

Double-base chains speed up
Weierstrass curves slightly:
9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian:
9.65**M**/bit. Still not competitive.

Revisit conclusions
using latest Hessian formulas,
latest double-base techniques.

Not good for constant time.
Good for signature verification,
factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007
Bernstein–Birkner–Lange–Peters:

Double-base chains speed up
Weierstrass curves slightly:
9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian:
9.65**M**/bit. Still not competitive.

Revisit conclusions
using latest Hessian formulas,
latest double-base techniques.

New: 8.77**M**/bit for 256 bits.

Not good for constant time.
Good for signature verification, factorization, math, etc.

Also need time to compute chain.
Good for scalars used many times.

Analysis+optimization from 2007 Bernstein–Birkner–Lange–Peters:

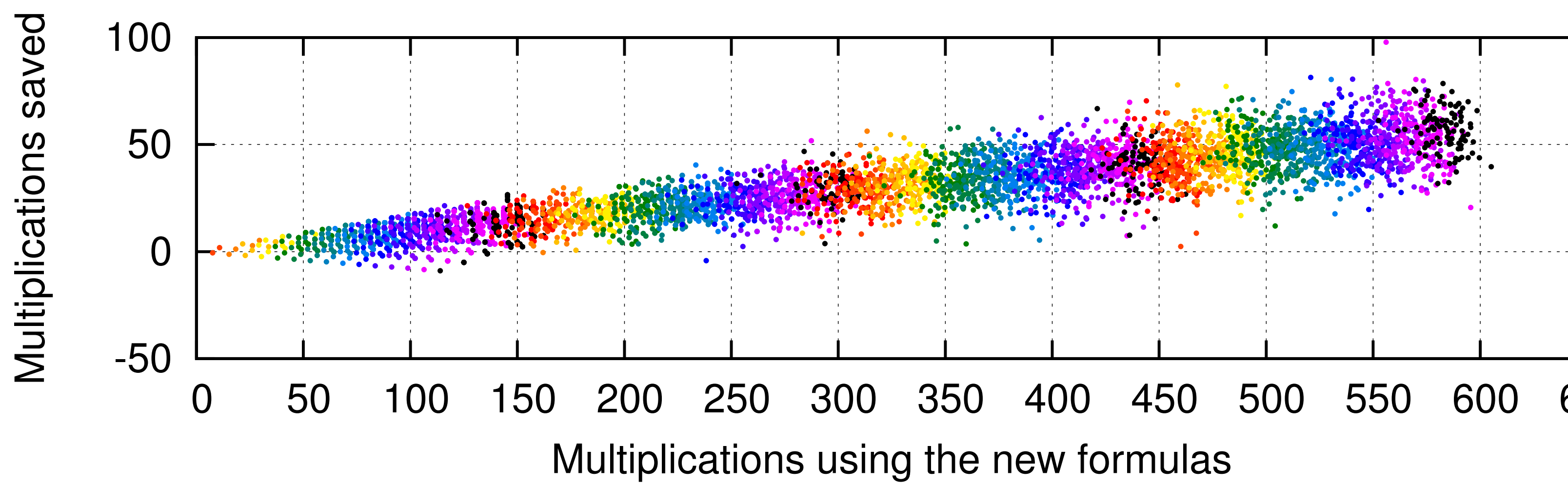
Double-base chains speed up Weierstrass curves slightly: 9.29**M**/bit for 256-bit scalars.

More savings for, e.g., Hessian: 9.65**M**/bit. Still not competitive.

Revisit conclusions using latest Hessian formulas, latest double-base techniques.

New: 8.77**M**/bit for 256 bits.

Comparison to Weierstrass for 1-bit, 2-bit, . . . , 64-bit scalars:



Uses 2008 Doche–Habsieger "tree search" and some new improvements: e.g., account for costs of ADD, DBL, TPL.

d for constant time.
r signature verification,
tion, math, etc.

ed time to compute chain.
r scalars used many times.

+optimization from 2007
n–Birkner–Lange–Peters:

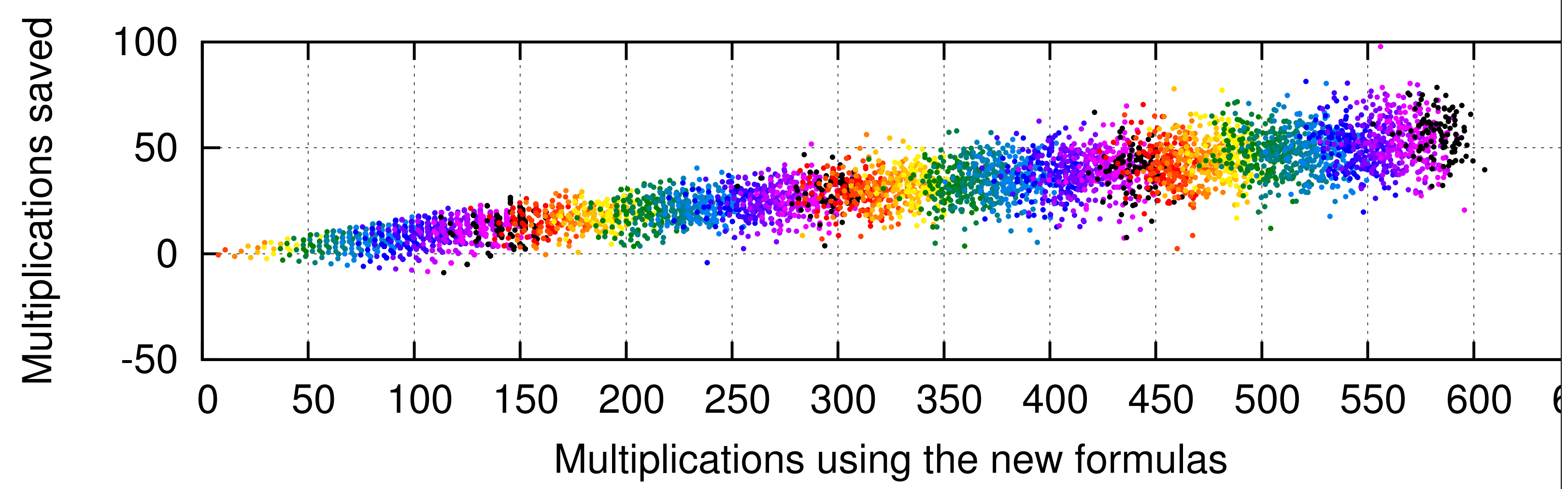
pase chains speed up
rass curves slightly:
bit for 256-bit scalars.

vings for, e.g., Hessian:
bit. Still not competitive.

Revisit conclusions
using latest Hessian formulas,
latest double-base techniques.

New: 8.77**M**/bit for 256 bits.

Comparison to Weierstrass for
1-bit, 2-bit, . . . , 64-bit scalars:



Uses 2008 Doche–Habsieger
"tree search" and some new
improvements: e.g., account for
costs of ADD, DBL, TPL.

Mo

Summar
Twisted
solidly b

Chuengs
even bet
from sho
and also

tant time.
e verification,
n, etc.

compute chain.
sed many times.

ation from 2007
–Lange–Peters:

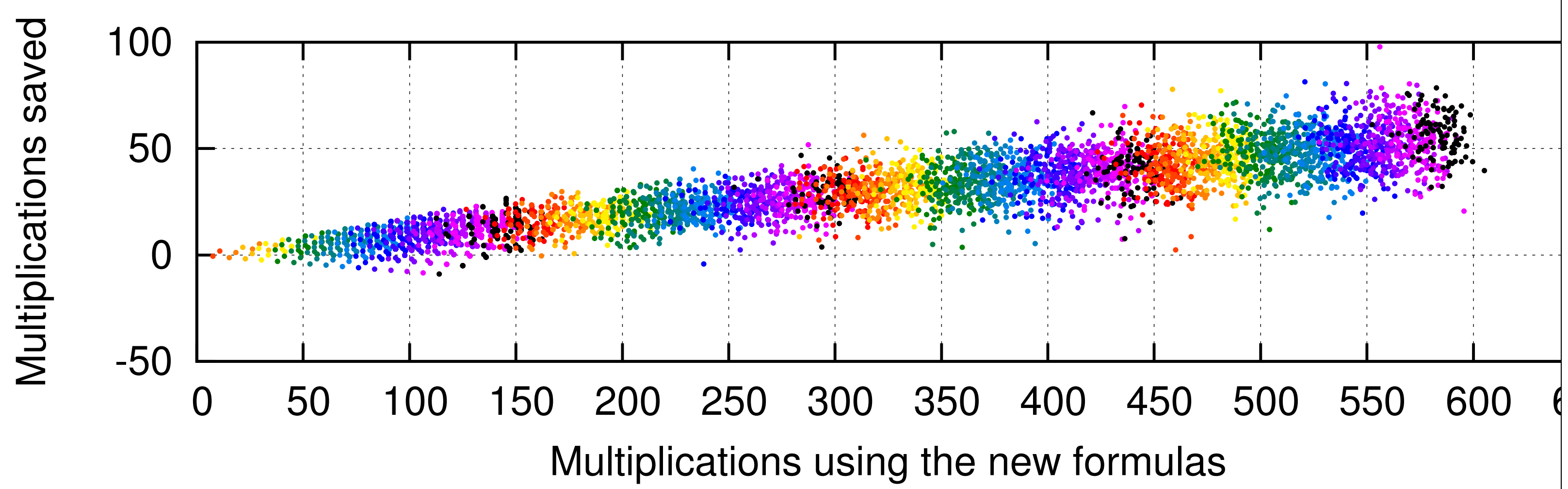
s speed up
s slightly:
-bit scalars.

e.g., Hessian:
ot competitive.

Revisit conclusions
using latest Hessian formulas,
latest double-base techniques.

New: 8.77**M**/bit for 256 bits.

Comparison to Weierstrass for
1-bit, 2-bit, . . . , 64-bit scalars:



Uses 2008 Doche–Habsieger
"tree search" and some new
improvements: e.g., account for
costs of ADD, DBL, TPL.

Mar2015

Summary:
Twisted Hessian c
solidly beat Weiers

Chuengsatiansup t
even better double
from shortest path
and also new Edw

on,

chain.
times.

2007
eters:

p

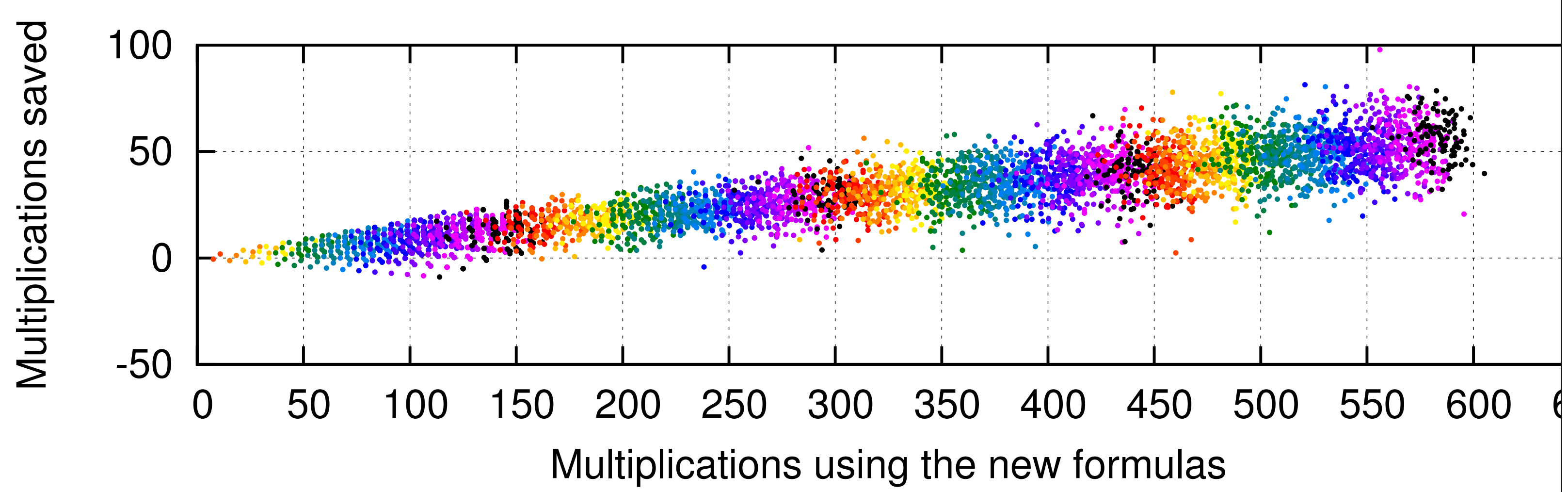
s.

an:
itive.

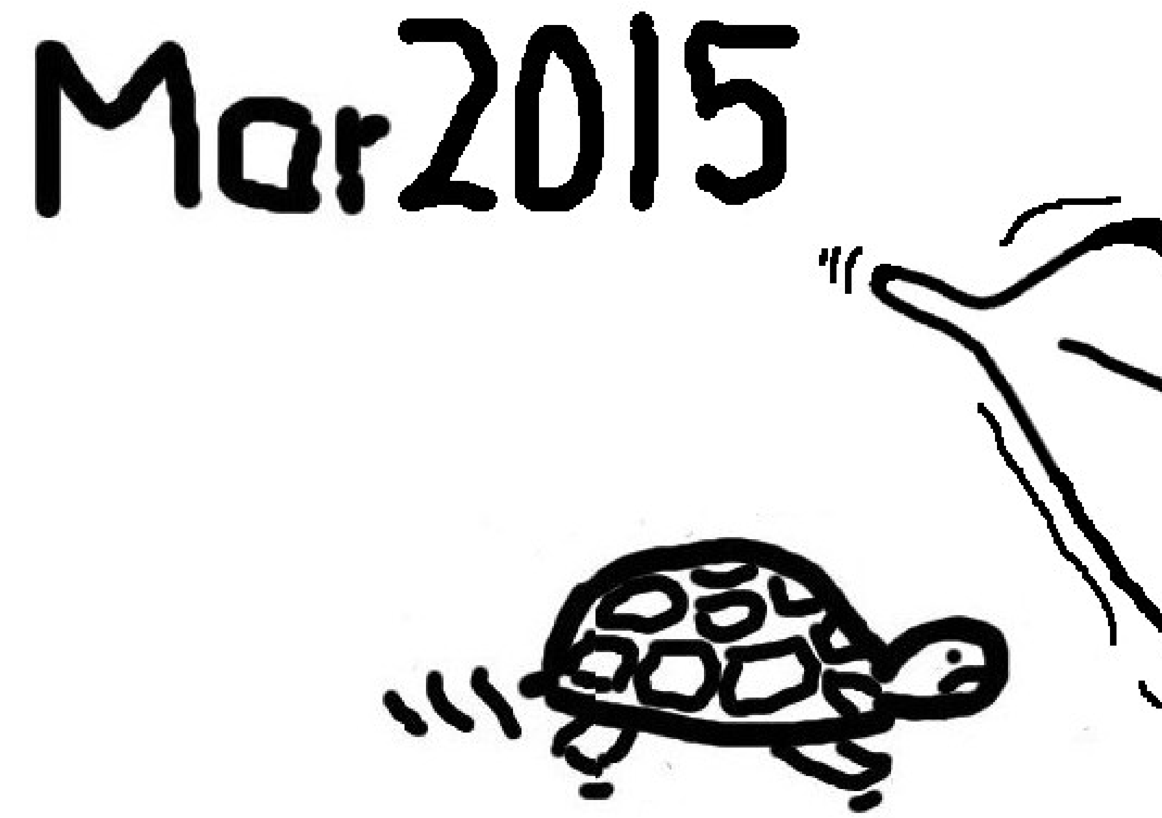
Revisit conclusions
using latest Hessian formulas,
latest double-base techniques.

New: 8.77**M**/bit for 256 bits.

Comparison to Weierstrass for
1-bit, 2-bit, . . . , 64-bit scalars:



Uses 2008 Doche–Habsieger
"tree search" and some new
improvements: e.g., account for
costs of ADD, DBL, TPL.



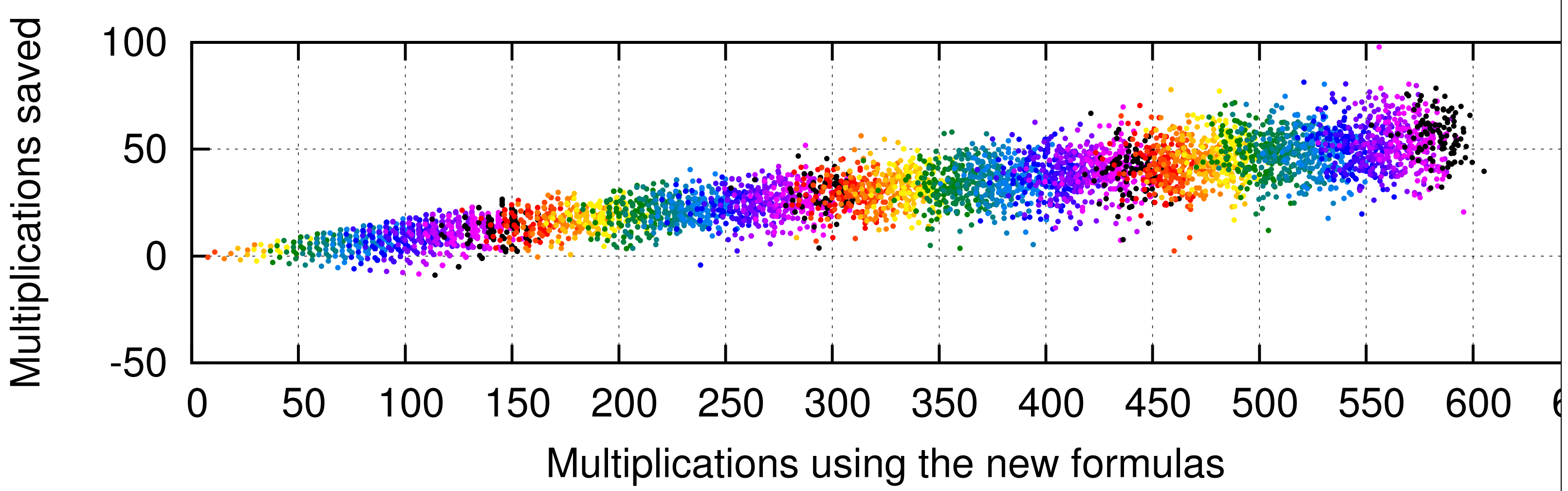
Summary:
Twisted Hessian curves
solidly beat Weierstrass.

Chuengsatiansup talk tomor
even better double-base cha
from shortest paths in DAG-
and also new Edwards speed

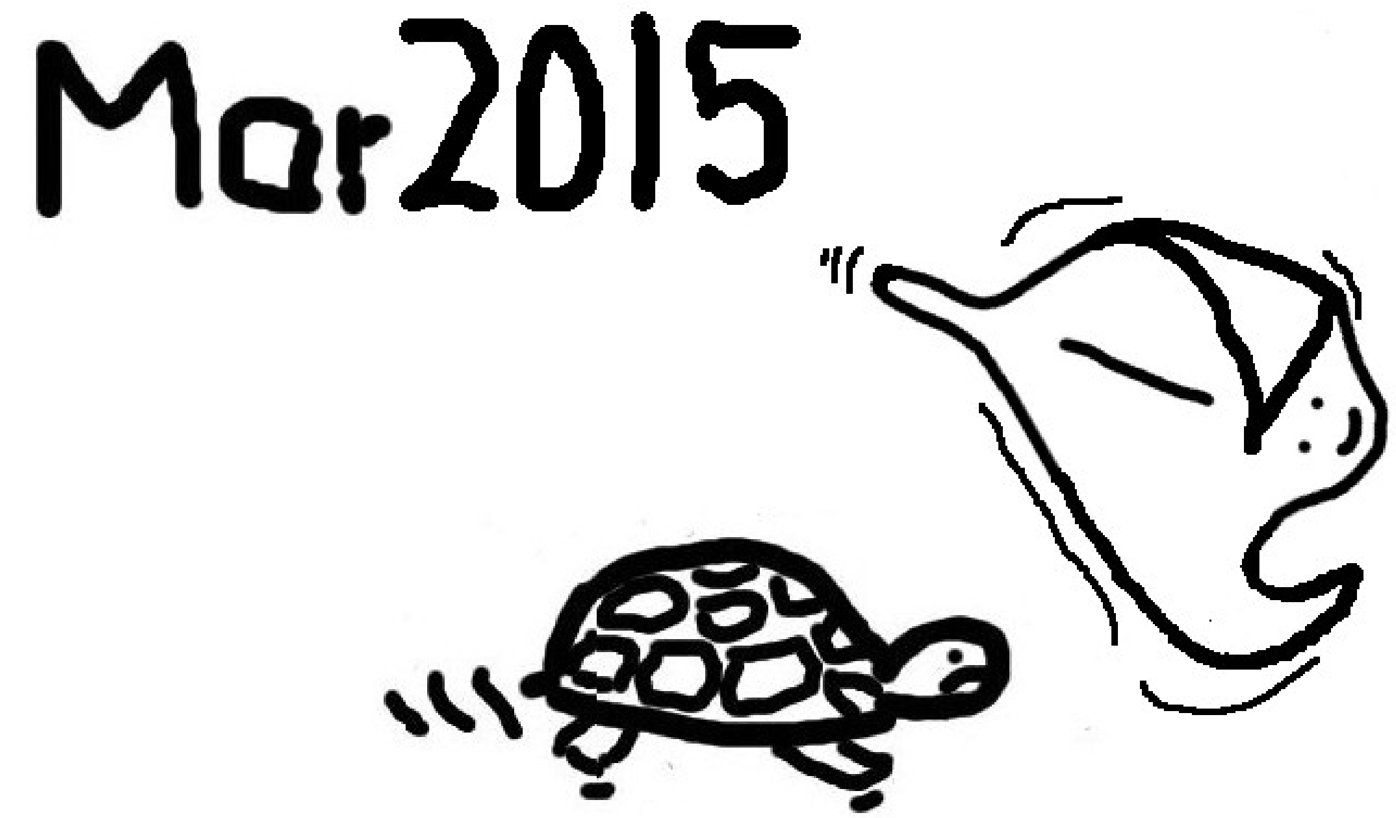
Revisit conclusions
using latest Hessian formulas,
latest double-base techniques.

New: 8.77**M**/bit for 256 bits.

Comparison to Weierstrass for
1-bit, 2-bit, . . . , 64-bit scalars:



Uses 2008 Doche–Habsieger
"tree search" and some new
improvements: e.g., account for
costs of ADD, DBL, TPL.



Summary:
Twisted Hessian curves
solidly beat Weierstrass.

Chuengsatiansup talk tomorrow:
even better double-base chains
from shortest paths in DAG—
and also new Edwards speeds!