High-speed cryptography, part 1: elliptic-curve formulas

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

Crypto performance problems often lead users to reduce cryptographic security levels or give up on cryptography.

Example 1 (according to Firefox on Linux, 2013.06.24): Google SSL uses RSA-1024.

Security note:
Analyses in 2003 concluded that RSA-1024 was breakable; e.g., 2003 Shamir–Tromer estimated 1 year, $\approx 10^7$ USD.
RSA Labs and NIST response:
Move to RSA-2048 by 2010.

eed cryptography,

curve formulas

. Bernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

Crypto performance problems often lead users to reduce cryptographic security levels or give up on cryptography.

Example 1 (according to Firefox on Linux, 2013.06.24): Google SSL uses RSA-1024.

Security note:
Analyses in 2003 concluded that RSA-1024 was breakable; e.g., 2003 Shamir–Tromer estimated 1 year, $\approx 10^7$ USD. RSA Labs and NIST response: Move to RSA-2048 by 2010.

Example

Example
1024: "t
risk of k
performa

Example
AES loa

Example
https://
is protec
https://
redirects
http://s
turning

graphy,

ulas

n

is at Chicago &

siteit Eindhoven

Crypto performance problems often lead users to reduce cryptographic security levels or give up on cryptography.

Example 1 (according to Firefox on Linux, 2013.06.24): Google SSL uses RSA-1024.

Security note:
Analyses in 2003 concluded that RSA-1024 was breakable; e.g., 2003 Shamir–Tromer estimated 1 year, $\approx 10^7$ USD.
RSA Labs and NIST response: Move to RSA-2048 by 2010.

Example 2: Tor us

Example 3: DNSS
1024: "tradeoff be
risk of key compro
performance. . . "

Example 4: OpenS
AES load addresse

Example 5:
https://sourcefo
is protected by SS
https://sourcefo
redirects browser t
http://sourcefor
turning off the cry

ago &
hoven

Crypto performance problems often lead users to reduce cryptographic security levels or give up on cryptography.

Example 1 (according to Firefox on Linux, 2013.06.24): Google SSL uses RSA-1024.

Security note:
Analyses in 2003 concluded that RSA-1024 was breakable; e.g., 2003 Shamir–Tromer estimated 1 year, $\approx 10^7$ USD.
RSA Labs and NIST response: Move to RSA-2048 by 2010.

Example 2: Tor uses RSA-1

Example 3: DNSSEC uses R
1024: "tradeoff between the
risk of key compromise and
performance. . . "

Example 4: OpenSSL uses s
AES load addresses; danger

Example 5:
https://sourceforge.net/a
is protected by SSL but
https://sourceforge.net/d
redirects browser to
http://sourceforge.net/de
turning off the cryptography

Crypto performance problems often lead users to reduce cryptographic security levels or give up on cryptography.

Example 1 (according to Firefox on Linux, 2013.06.24): Google SSL uses RSA-1024.

Security note:
Analyses in 2003 concluded that RSA-1024 was breakable; e.g., 2003 Shamir–Tromer estimated 1 year, $\approx 10^7$ USD.
RSA Labs and NIST response: Move to RSA-2048 by 2010.

Example 2: Tor uses RSA-1024.

Example 3: DNSSEC uses RSA-1024: "tradeoff between the risk of key compromise and performance. . . "

Example 4: OpenSSL uses secret AES load addresses; dangerous!

Example 5:
`https://sourceforge.net/account` is protected by SSL but `https://sourceforge.net/develop` redirects browser to `http://sourceforge.net/develop`, turning off the cryptography.

performance problems
ad users to reduce
aphic security levels
up on cryptography.

e 1 (according to
on Linux, 2013.06.24):
SSL uses RSA-1024.

note:
s in 2003 concluded
A-1024 was breakable;
03 Shamir–Tromer
ed 1 year, $\approx 10^7$ USD.
os and NIST response:
RSA-2048 by 2010.

Example 2: Tor uses RSA-1024.

Example 3: DNSSEC uses RSA-1024: "tradeoff between the risk of key compromise and performance. . ."

Example 4: OpenSSL uses secret AES load addresses; dangerous!

Example 5:
`https://sourceforge.net/account`
is protected by SSL but
`https://sourceforge.net/develop`
redirects browser to
`http://sourceforge.net/develop`,
turning off the cryptography.

Extensiv
⇒ fast h
Example
460200
332304
182632

Requires
and opti
Not just
not just

My topic
decompo
operatio

ce problems
o reduce
urity levels
tography.

ding to
2013.06.24):
RSA-1024.

concluded
ns breakable;
-Tromer
$\approx 10^7$ USD.
ST response:
8 by 2010.

Example 2: Tor uses RSA-1024.

Example 3: DNSSEC uses RSA-1024: "tradeoff between the risk of key compromise and performance. . . "

Example 4: OpenSSL uses secret AES load addresses; dangerous!

Example 5:
https://sourceforge.net/account
is protected by SSL but
https://sourceforge.net/develop
redirects browser to
http://sourceforge.net/develop,
turning off the cryptography.

Extensive work on
⇒ fast high-securi
Example: Curve25
460200 Cortex A8
332304 Snapdrago
182632 Ivy Bridge

Requires serious a
and optimization o
Not just "polynom
not just "quadrati

My topic today:
decomposing ellipt
operations into fie

ns

4):

le;

).
se:
.

Example 2: Tor uses RSA-1024.

Example 3: DNSSEC uses RSA-1024: "tradeoff between the risk of key compromise and performance. . . "

Example 4: OpenSSL uses secret AES load addresses; dangerous!

Example 5:
`https://sourceforge.net/account`
is protected by SSL but
`https://sourceforge.net/develop`
redirects browser to
`http://sourceforge.net/develop`,
turning off the cryptography.

Extensive work on ECC spee
⇒ fast high-security ECC.
Example: Curve25519 ECDI
460200 Cortex A8 cycles;
332304 Snapdragon S4 cycle
182632 Ivy Bridge cycles.

Requires serious analysis
and optimization of algorith
Not just "polynomial time";
not just "quadratic time".

My topic today:
decomposing elliptic-curve
operations into field operatio

Example 2: Tor uses RSA-1024.

Example 3: DNSSEC uses RSA-1024: "tradeoff between the risk of key compromise and performance. . . "

Example 4: OpenSSL uses secret AES load addresses; dangerous!

Example 5:
https://sourceforge.net/account
is protected by SSL but
https://sourceforge.net/develop
redirects browser to
http://sourceforge.net/develop,
turning off the cryptography.

Extensive work on ECC speed
$\Rightarrow$ fast high-security ECC.
Example: Curve25519 ECDH in
460200 Cortex A8 cycles;
332304 Snapdragon S4 cycles;
182632 Ivy Bridge cycles.

Requires serious analysis and optimization of algorithms. Not just "polynomial time"; not just "quadratic time".

My topic today:
decomposing elliptic-curve operations into field operations.

e 2: Tor uses RSA-1024.

e 3: DNSSEC uses RSA-
tradeoff between the
ey compromise and
ance. . . ”

e 4: OpenSSL uses secret
d addresses; dangerous!

e 5:
/sourceforge.net/account
cted by SSL but
/sourceforge.net/develop
s browser to
sourceforge.net/develop,
off the cryptography.

Extensive work on ECC speed
⇒ fast high-security ECC.
Example: Curve25519 ECDH in
460200 Cortex A8 cycles;
332304 Snapdragon S4 cycles;
182632 Ivy Bridge cycles.

Requires serious analysis
and optimization of algorithms.
Not just “polynomial time”;
not just “quadratic time”.

My topic today:
decomposing elliptic-curve
operations into field operations.

Eliminat

Typical
$P \mapsto nP$

Decomp
$P, Q \mapsto$

Addition
$((x_1 y_2 +$
$(y_1 y_2 -$
uses exp

Better:
and work
Represen
$(X : Y$
$y = Y/Z$

ses RSA-1024.

SEC uses RSA-
etween the
omise and

SSL uses secret
es; dangerous!

rge.net/account
L but
rge.net/develop
to
ge.net/develop,
yptography.

Extensive work on ECC speed
$\Rightarrow$ fast high-security ECC.
Example: Curve25519 ECDH in
460200 Cortex A8 cycles;
332304 Snapdragon S4 cycles;
182632 Ivy Bridge cycles.

Requires serious analysis
and optimization of algorithms.
Not just "polynomial time";
not just "quadratic time".

My topic today:
decomposing elliptic-curve
operations into field operations.

Eliminating divisio

Typical computati
$P \mapsto nP$.

Decompose into a
$P, Q \mapsto P + Q$.

Addition (x_1, y_1) -
$((x_1 y_2 + y_1 x_2)/(1$
$(y_1 y_2 - x_1 x_2)/(1$
uses expensive div

Better: postpone
and work with frac
Represent (x, y) a
$(X : Y : Z)$ with
$y = Y/Z$ for $Z \neq$

024.

RSA-

e

secret

ous!

`ccount`

`evelop`

`evelop`,

y.

Extensive work on ECC speed
$\Rightarrow$ fast high-security ECC.
Example: Curve25519 ECDH in
460200 Cortex A8 cycles;
332304 Snapdragon S4 cycles;
182632 Ivy Bridge cycles.

Requires serious analysis
and optimization of algorithms.
Not just "polynomial time";
not just "quadratic time".

My topic today:
decomposing elliptic-curve
operations into field operations.

Eliminating divisions

Typical computation:
$P \mapsto nP$.

Decompose into additions:
$P, Q \mapsto P + Q$.

Addition $(x_1, y_1) + (x_2, y_2)$
$((x_1y_2 + y_1x_2)/(1 + dx_1x_2$
$(y_1y_2 - x_1x_2)/(1 - dx_1x_2$
uses expensive divisions.

Better: postpone divisions
and work with fractions.
Represent (x, y) as
$(X : Y : Z)$ with $x = X/Z$
$y = Y/Z$ for $Z \neq 0$.

Extensive work on ECC speed
$\Rightarrow$ fast high-security ECC.
Example: Curve25519 ECDH in
460200 Cortex A8 cycles;
332304 Snapdragon S4 cycles;
182632 Ivy Bridge cycles.

Requires serious analysis
and optimization of algorithms.
Not just "polynomial time";
not just "quadratic time".

My topic today:
decomposing elliptic-curve
operations into field operations.

Eliminating divisions

Typical computation:
$P \mapsto nP$.

Decompose into additions:
$P, Q \mapsto P + Q$.

Addition $(x_1, y_1) + (x_2, y_2) =$
$((x_1 y_2 + y_1 x_2)/(1 + d x_1 x_2 y_1 y_2),$
$(y_1 y_2 - x_1 x_2)/(1 - d x_1 x_2 y_1 y_2))$
uses expensive divisions.

Better: postpone divisions
and work with fractions.
Represent (x, y) as
$(X : Y : Z)$ with $x = X/Z$ and
$y = Y/Z$ for $Z \neq 0$.

e work on ECC speed
high-security ECC.
e: Curve25519 ECDH in
Cortex A8 cycles;
Snapdragon S4 cycles;
Ivy Bridge cycles.

s serious analysis
mization of algorithms.
“polynomial time”;
“quadratic time”.

c today:
osing elliptic-curve
ns into field operations.

Eliminating divisions

Typical computation:
$P \mapsto nP$.

Decompose into additions:
$P, Q \mapsto P + Q$.

Addition $(x_1, y_1) + (x_2, y_2) =$
$((x_1 y_2 + y_1 x_2)/(1 + d x_1 x_2 y_1 y_2),$
$(y_1 y_2 - x_1 x_2)/(1 - d x_1 x_2 y_1 y_2))$
uses expensive divisions.

Better: postpone divisions
and work with fractions.
Represent (x, y) as
$(X : Y : Z)$ with $x = X/Z$ and
$y = Y/Z$ for $Z \neq 0$.

Addition
handle f

$\left(\frac{X_1}{Z_1}, \frac{Y}{Z}\right.$

$\left(\frac{\frac{X_1}{Z_1}\frac{Y}{Z}}{1 + d}\right.$

$\frac{\frac{Y_1}{Z_1}\frac{Y}{Z}}{1 - d}$

$\left(\frac{Z_1 Z_2(}{Z_1^2 Z_2^2}\right.$

$\frac{Z_1 Z_2(}{Z_1^2 Z_2^2}$

ECC speed
ity ECC.
5519 ECDH in
cycles;
on S4 cycles;
cycles.

nalysis
of algorithms.
nial time";
c time".

tic-curve
ld operations.

Eliminating divisions

Typical computation:
$P \mapsto nP$.

Decompose into additions:
$P, Q \mapsto P + Q$.

Addition $(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2 + y_1x_2)/(1 + dx_1x_2y_1y_2),$
$(y_1y_2 - x_1x_2)/(1 - dx_1x_2y_1y_2))$
uses expensive divisions.

Better: postpone divisions
and work with fractions.
Represent (x, y) as
$(X : Y : Z)$ with $x = X/Z$ and
$y = Y/Z$ for $Z \neq 0$.

Addition now has
handle fractions as

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X}{Z}\right.$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z}}\right.$$

$$\frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z}}$$

$$\left(\frac{Z_1Z_2(X_1Y_2 + Y}{Z_1^2Z_2^2 + dX_1X_2}\right.$$

$$\frac{Z_1Z_2(Y_1Y_2 - X}{Z_1^2Z_2^2 - dX_1X_2}$$

ed

H in

es;

ms.

ons.

Eliminating divisions

Typical computation:
$P \mapsto nP$.

Decompose into additions:
$P, Q \mapsto P + Q$.

Addition $(x_1, y_1) + (x_2, y_2) =$
$((x_1 y_2 + y_1 x_2)/(1 + d x_1 x_2 y_1 y_2),$
$(y_1 y_2 - x_1 x_2)/(1 - d x_1 x_2 y_1 y_2))$
uses expensive divisions.

Better: postpone divisions and work with fractions.
Represent (x, y) as $(X : Y : Z)$ with $x = X/Z$ and $y = Y/Z$ for $Z \neq 0$.

Addition now has to handle fractions as input:

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}, \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) =$$

$$\left(\frac{Z_1 Z_2 (X_1 Y_2 + Y_1 X_2)}{Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2}, \frac{Z_1 Z_2 (Y_1 Y_2 - X_1 X_2)}{Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2}\right)$$

Eliminating divisions

Typical computation:
$P \mapsto nP$.

Decompose into additions:
$P, Q \mapsto P + Q$.

Addition $(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2 + y_1x_2)/(1 + dx_1x_2y_1y_2),$
$(y_1y_2 - x_1x_2)/(1 - dx_1x_2y_1y_2))$
uses expensive divisions.

Better: postpone divisions
and work with fractions.
Represent (x, y) as
$(X : Y : Z)$ with $x = X/Z$ and
$y = Y/Z$ for $Z \neq 0$.

Addition now has to
handle fractions as input:

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}, \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) =$$

$$\left(\frac{Z_1Z_2(X_1Y_2 + Y_1X_2)}{Z_1^2Z_2^2 + dX_1X_2Y_1Y_2}, \frac{Z_1Z_2(Y_1Y_2 - X_1X_2)}{Z_1^2Z_2^2 - dX_1X_2Y_1Y_2}\right)$$

ing divisions

computation:

P.

ose into additions:

$P + Q$.

n $(x_1, y_1) + (x_2, y_2) =$

$- y_1 x_2)/(1 + d x_1 x_2 y_1 y_2)$,

$- x_1 x_2)/(1 - d x_1 x_2 y_1 y_2))$

pensive divisions.

postpone divisions

k with fractions.

nt (x, y) as

: Z) with $x = X/Z$ and

Z for $Z \neq 0$.

Addition now has to handle fractions as input:

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}, \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) =$$

$$\left(\frac{Z_1 Z_2 (X_1 Y_2 + Y_1 X_2)}{Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2}, \frac{Z_1 Z_2 (Y_1 Y_2 - X_1 X_2)}{Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2}\right)$$

i.e. $\Big(\frac{X_1}{Z_1}$

$= \Big(\frac{X_3}{Z_3},$

where

$F = Z_1^2$

$G = Z_1^2$

$X_3 = Z_1$

$Y_3 = Z_1$

$Z_3 = F$

Input to

$X_1, Y_1,$

Output

$X_3, Y_3,$

ons

on:

dditions:

$+ (x_2, y_2) =$

$+ dx_1 x_2 y_1 y_2),$

$- dx_1 x_2 y_1 y_2))$

isions.

divisions

ctions.

s

$x = X/Z$ and

0.

Addition now has to handle fractions as input:

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}, \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) =$$

$$\left(\frac{Z_1 Z_2 (X_1 Y_2 + Y_1 X_2)}{Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2}, \frac{Z_1 Z_2 (Y_1 Y_2 - X_1 X_2)}{Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2}\right)$$

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) +$

$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$

where

$F = Z_1^2 Z_2^2 - d X_1$

$G = Z_1^2 Z_2^2 + d X_1$

$X_3 = Z_1 Z_2 (X_1 Y_2$

$Y_3 = Z_1 Z_2 (Y_1 Y_2 -$

$Z_3 = FG.$

Input to addition a

$X_1, Y_1, Z_1, X_2, Y_2,$

Output from addit

X_3, Y_3, Z_3. No div

$=$

$y_1y_2)$,

$y_1y_2))$

and

Addition now has to handle fractions as input:

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}, \right.$$

$$\left. \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) =$$

$$\left(\frac{Z_1Z_2(X_1Y_2 + Y_1X_2)}{Z_1^2Z_2^2 + dX_1X_2Y_1Y_2}, \right.$$

$$\left. \frac{Z_1Z_2(Y_1Y_2 - X_1X_2)}{Z_1^2Z_2^2 - dX_1X_2Y_1Y_2}\right)$$

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right.$

$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$

where

$F = Z_1^2Z_2^2 - dX_1X_2Y_1Y_2$,
$G = Z_1^2Z_2^2 + dX_1X_2Y_1Y_2$,
$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2)F$
$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)G$,
$Z_3 = FG$.

Input to addition algorithm:
$X_1, Y_1, Z_1, X_2, Y_2, Z_2$.
Output from addition algorit
X_3, Y_3, Z_3. No divisions nee

Addition now has to handle fractions as input:

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}},\right.$$

$$\left.\frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) =$$

$$\left(\frac{Z_1 Z_2(X_1 Y_2 + Y_1 X_2)}{Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2},\right.$$

$$\left.\frac{Z_1 Z_2(Y_1 Y_2 - X_1 X_2)}{Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2}\right)$$

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$

$$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$$

where

$F = Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2$,
$G = Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2$,
$X_3 = Z_1 Z_2 (X_1 Y_2 + Y_1 X_2) F$,
$Y_3 = Z_1 Z_2 (Y_1 Y_2 - X_1 X_2) G$,
$Z_3 = FG$.

Input to addition algorithm:
$X_1, Y_1, Z_1, X_2, Y_2, Z_2$.
Output from addition algorithm:
X_3, Y_3, Z_3. No divisions needed!

n now has to

ractions as input:

$$\ldots 1\Big) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) =$$

$$\ldots \frac{\ldots_2 + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{\ldots \frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}},$$

$$\ldots \frac{\ldots_2 - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{\ldots \frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\Bigg) =$$

$$\ldots \frac{(X_1Y_2 + Y_1X_2)}{\ldots + dX_1X_2Y_1Y_2},$$

$$\ldots \frac{(Y_1Y_2 - X_1X_2)}{\ldots - dX_1X_2Y_1Y_2}\Bigg)$$

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$

$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$

where

$F = Z_1^2 Z_2^2 - dX_1X_2Y_1Y_2,$
$G = Z_1^2 Z_2^2 + dX_1X_2Y_1Y_2,$
$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2)F,$
$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)G,$
$Z_3 = FG.$

Input to addition algorithm:
$X_1, Y_1, Z_1, X_2, Y_2, Z_2$.
Output from addition algorithm:
X_3, Y_3, Z_3. No divisions needed!

Save mu

eliminati

subexpre

$A = Z_1$
$C = X_1$
$D = Y_1 \cdot$
$E = d \cdot$
$F = B -$
$X_3 = A$
$Y_3 = A \cdot$
$Z_3 = F$

Cost: 11

Can do

to

s input:

$$\frac{\ }{\ 2}, \frac{Y_2}{Z_2}\right) =$$

$$\frac{\ }{\ 2},$$

$$\frac{\ }{\ 2}\right) =$$

$$\frac{{}_1X_2)}{Y_1Y_2},$$

$$\frac{{}_1X_2)}{Y_1Y_2}\right)$$

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$

$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$

where

$$F = Z_1^2 Z_2^2 - dX_1X_2Y_1Y_2,$$
$$G = Z_1^2 Z_2^2 + dX_1X_2Y_1Y_2,$$
$$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2)F,$$
$$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)G,$$
$$Z_3 = FG.$$

Input to addition algorithm:
$X_1, Y_1, Z_1, X_2, Y_2, Z_2$.
Output from addition algorithm:
X_3, Y_3, Z_3. No divisions needed!

Save multiplicatio
eliminating comm
subexpressions:

$A = Z_1 \cdot Z_2$; $B =$
$C = X_1 \cdot X_2$;
$D = Y_1 \cdot Y_2$;
$E = d \cdot C \cdot D$;
$F = B - E$; $G =$
$X_3 = A \cdot F \cdot (X_1 \cdot$
$Y_3 = A \cdot G \cdot (D -$
$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} +$
Can do better: 10

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$

$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$

where

$F = Z_1^2 Z_2^2 - dX_1X_2Y_1Y_2,$
$G = Z_1^2 Z_2^2 + dX_1X_2Y_1Y_2,$
$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2)F,$
$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)G,$
$Z_3 = FG.$

Input to addition algorithm:
$X_1, Y_1, Z_1, X_2, Y_2, Z_2$.
Output from addition algorithm:
X_3, Y_3, Z_3. No divisions needed!

Save multiplications by eliminating common subexpressions:

$A = Z_1 \cdot Z_2$; $B = A^2$;
$C = X_1 \cdot X_2$;
$D = Y_1 \cdot Y_2$;
$E = d \cdot C \cdot D$;
$F = B - E$; $G = B + E$;
$X_3 = A \cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot$
$Y_3 = A \cdot G \cdot (D - C)$;
$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.
Can do better: $10\mathbf{M} + 1\mathbf{S} +$

i.e. $\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$

$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$

where

$F = Z_1^2 Z_2^2 - dX_1X_2Y_1Y_2$,

$G = Z_1^2 Z_2^2 + dX_1X_2Y_1Y_2$,

$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2)F$,

$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)G$,

$Z_3 = FG$.

Input to addition algorithm:

$X_1, Y_1, Z_1, X_2, Y_2, Z_2$.

Output from addition algorithm:

X_3, Y_3, Z_3. No divisions needed!

Save multiplications by eliminating common subexpressions:

$A = Z_1 \cdot Z_2$; $B = A^2$;

$C = X_1 \cdot X_2$;

$D = Y_1 \cdot Y_2$;

$E = d \cdot C \cdot D$;

$F = B - E$; $G = B + E$;

$X_3 = A \cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot X_2)$;

$Y_3 = A \cdot G \cdot (D - C)$;

$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

Can do better: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

$$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) + \left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$$

$$= \left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right)$$

$F = Z_1^2 Z_2^2 - dX_1X_2Y_1Y_2$,

$G = Z_1^2 Z_2^2 + dX_1X_2Y_1Y_2$,

$X_3 = Z_1Z_2(X_1Y_2 + Y_1X_2)F$,

$Y_3 = Z_1Z_2(Y_1Y_2 - X_1X_2)G$,

$Z_3 = FG$.

Input to addition algorithm: $X_1, Y_1, Z_1, X_2, Y_2, Z_2$.

Output from addition algorithm: X_3, Y_3, Z_3. No divisions needed!

Save multiplications by eliminating common subexpressions:

$A = Z_1 \cdot Z_2$; $B = A^2$;
$C = X_1 \cdot X_2$;
$D = Y_1 \cdot Y_2$;
$E = d \cdot C \cdot D$;
$F = B - E$; $G = B + E$;
$X_3 = A \cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot X_2)$;
$Y_3 = A \cdot G \cdot (D - C)$;
$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.
Can do better: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

Faster d

(x_1, y_1)
$((x_1y_1+$
$(y_1y_1-$
$((2x_1y_1)$
$(y_1^2-x_1^2$

$x_1^2 + y_1^2$
(x_1, y_1)
$((2x_1y_1)$
$(y_1^2-x_1^2$

Again el
using $\mathbf{P}^2$
Much fa
Useful:

$\left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right)$

$X_2 Y_1 Y_2,$

$X_2 Y_1 Y_2,$

$+ Y_1 X_2) F,$

$- X_1 X_2) G,$

algorithm:

$Z_2.$

tion algorithm:

visions needed!

Save multiplications by eliminating common subexpressions:

$A = Z_1 \cdot Z_2$; $B = A^2$;

$C = X_1 \cdot X_2$;

$D = Y_1 \cdot Y_2$;

$E = d \cdot C \cdot D$;

$F = B - E$; $G = B + E$;

$X_3 = A \cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot X_2)$;

$Y_3 = A \cdot G \cdot (D - C)$;

$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

Can do better: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

<u>Faster doubling</u>

$(x_1, y_1) + (x_1, y_1)$

$((x_1 y_1 + y_1 x_1)/(1$

$(y_1 y_1 - x_1 x_1)/(1$

$((2 x_1 y_1)/(1 + d x_1^2$

$(y_1^2 - x_1^2)/(1 - d x$

$x_1^2 + y_1^2 = 1 + d x_1^2$

$(x_1, y_1) + (x_1, y_1)$

$((2 x_1 y_1)/(x_1^2 + y_1^2$

$(y_1^2 - x_1^2)/(2 - x_1^2$

Again eliminate di

using $\mathbf{P}^2$: only $3\mathbf{M}$

Much faster than

Useful: many doul

thm:

ded!

Save multiplications by eliminating common subexpressions:

$A = Z_1 \cdot Z_2$; $B = A^2$;
$C = X_1 \cdot X_2$;
$D = Y_1 \cdot Y_2$;
$E = d \cdot C \cdot D$;
$F = B - E$; $G = B + E$;
$X_3 = A \cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot X_2)$;
$Y_3 = A \cdot G \cdot (D - C)$;
$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.
Can do better: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

<u>Faster doubling</u>

$(x_1, y_1) + (x_1, y_1) =$
$((x_1y_1 + y_1x_1)/(1 + dx_1x_1y_1$
$(y_1y_1 - x_1x_1)/(1 - dx_1x_1y_1$
$((2x_1y_1)/(1 + dx_1^2y_1^2),$
$(y_1^2 - x_1^2)/(1 - dx_1^2y_1^2)).$

$x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ so
$(x_1, y_1) + (x_1, y_1) =$
$((2x_1y_1)/(x_1^2 + y_1^2),$
$(y_1^2 - x_1^2)/(2 - x_1^2 - y_1^2)).$

Again eliminate divisions using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in E

Save multiplications by eliminating common subexpressions:

$A = Z_1 \cdot Z_2$; $B = A^2$;
$C = X_1 \cdot X_2$;
$D = Y_1 \cdot Y_2$;
$E = d \cdot C \cdot D$;
$F = B - E$; $G = B + E$;
$X_3 = A \cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot X_2)$;
$Y_3 = A \cdot G \cdot (D - C)$;
$Z_3 = F \cdot G$.

Cost: $11\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.
Can do better: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

<u>Faster doubling</u>

$(x_1, y_1) + (x_1, y_1) =$
$((x_1 y_1 + y_1 x_1)/(1 + d x_1 x_1 y_1 y_1),$
$(y_1 y_1 - x_1 x_1)/(1 - d x_1 x_1 y_1 y_1)) =$
$((2 x_1 y_1)/(1 + d x_1^2 y_1^2),$
$(y_1^2 - x_1^2)/(1 - d x_1^2 y_1^2))$.

$x_1^2 + y_1^2 = 1 + d x_1^2 y_1^2$ so
$(x_1, y_1) + (x_1, y_1) =$
$((2 x_1 y_1)/(x_1^2 + y_1^2),$
$(y_1^2 - x_1^2)/(2 - x_1^2 - y_1^2))$.

Again eliminate divisions using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in ECC.

ltiplications by
ing common
essions:

$\cdot Z_2$; $B = A^2$;

$\cdot X_2$;

$\cdot Y_2$;

$C \cdot D$;

$- E$; $G = B + E$;

$\cdot F \cdot (X_1 \cdot Y_2 + Y_1 \cdot X_2)$;

$G \cdot (D - C)$;

$\cdot G$.

$1\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

better: $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

Faster doubling

$$(x_1, y_1) + (x_1, y_1) = \\ ((x_1y_1 + y_1x_1)/(1 + dx_1x_1y_1y_1), \\ (y_1y_1 - x_1x_1)/(1 - dx_1x_1y_1y_1)) = \\ ((2x_1y_1)/(1 + dx_1^2y_1^2), \\ (y_1^2 - x_1^2)/(1 - dx_1^2y_1^2)).$$

$x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ so

$$(x_1, y_1) + (x_1, y_1) = \\ ((2x_1y_1)/(x_1^2 + y_1^2), \\ (y_1^2 - x_1^2)/(2 - x_1^2 - y_1^2)).$$

Again eliminate divisions
using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in ECC.

More ad

Dual ad

(x_1, y_1)

$((x_1y_1 +$

$(x_1y_1 -$

Low deg

Warning

Is this re

Most EC

ns by

on

A^2;

$B + E$;

$Y_2 + Y_1 \cdot X_2$);

C);

$+ 1\mathbf{D}$.

$\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

Faster doubling

$(x_1, y_1) + (x_1, y_1) =$
$((x_1y_1{+}y_1x_1)/(1{+}dx_1x_1y_1y_1),$
$(y_1y_1{-}x_1x_1)/(1{-}dx_1x_1y_1y_1)) =$
$((2x_1y_1)/(1 + dx_1^2y_1^2),$
$(y_1^2{-}x_1^2)/(1 - dx_1^2y_1^2)).$

$x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ so
$(x_1, y_1) + (x_1, y_1) =$
$((2x_1y_1)/(x_1^2 + y_1^2),$
$(y_1^2{-}x_1^2)/(2 - x_1^2 - y_1^2)).$

Again eliminate divisions
using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in ECC.

More addition stra

Dual addition form
$(x_1, y_1) + (x_2, y_2)$
$((x_1y_1 + x_2y_2)/(x$
$(x_1y_1 - x_2y_2)/(x$
Low degree, no ne

Warning: fails for
Is this really "addi
Most EC formulas

X_2);

$+ 1\mathbf{D}$.

Faster doubling

$(x_1, y_1) + (x_1, y_1) =$
$((x_1y_1{+}y_1x_1)/(1{+}dx_1x_1y_1y_1),$
$(y_1y_1{-}x_1x_1)/(1{-}dx_1x_1y_1y_1)) =$
$((2x_1y_1)/(1 + dx_1^2y_1^2),$
$(y_1^2{-}x_1^2)/(1 - dx_1^2y_1^2))$.

$x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ so
$(x_1, y_1) + (x_1, y_1) =$
$((2x_1y_1)/(x_1^2 + y_1^2),$
$(y_1^2{-}x_1^2)/(2 - x_1^2 - y_1^2))$.

Again eliminate divisions
using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in ECC.

More addition strategies

Dual addition formula:
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y$
$(x_1y_1 - x_2y_2)/(x_1y_2 - x_2y$
Low degree, no need for d.

Warning: fails for doubling!
Is this really "addition"?
Most EC formulas have failu

Faster doubling

$(x_1, y_1) + (x_1, y_1) =$
$((x_1 y_1 + y_1 x_1)/(1 + d x_1 x_1 y_1 y_1),$
$(y_1 y_1 - x_1 x_1)/(1 - d x_1 x_1 y_1 y_1)) =$
$((2 x_1 y_1)/(1 + d x_1^2 y_1^2),$
$(y_1^2 - x_1^2)/(1 - d x_1^2 y_1^2)).$

$x_1^2 + y_1^2 = 1 + d x_1^2 y_1^2$ so
$(x_1, y_1) + (x_1, y_1) =$
$((2 x_1 y_1)/(x_1^2 + y_1^2),$
$(y_1^2 - x_1^2)/(2 - x_1^2 - y_1^2)).$

Again eliminate divisions
using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in ECC.

More addition strategies

Dual addition formula:
$(x_1, y_1) + (x_2, y_2) =$
$((x_1 y_1 + x_2 y_2)/(x_1 x_2 + y_1 y_2),$
$(x_1 y_1 - x_2 y_2)/(x_1 y_2 - x_2 y_1)).$
Low degree, no need for d.

Warning: fails for doubling!
Is this really "addition"?
Most EC formulas have failures.

Faster doubling

$(x_1, y_1) + (x_1, y_1) =$
$((x_1y_1 + y_1x_1)/(1 + dx_1x_1y_1y_1),$
$(y_1y_1 - x_1x_1)/(1 - dx_1x_1y_1y_1)) =$
$((2x_1y_1)/(1 + dx_1^2y_1^2),$
$(y_1^2 - x_1^2)/(1 - dx_1^2y_1^2)).$

$x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ so
$(x_1, y_1) + (x_1, y_1) =$
$((2x_1y_1)/(x_1^2 + y_1^2),$
$(y_1^2 - x_1^2)/(2 - x_1^2 - y_1^2)).$

Again eliminate divisions
using $\mathbf{P}^2$: only $3\mathbf{M} + 4\mathbf{S}$.
Much faster than addition.
Useful: many doublings in ECC.

More addition strategies

Dual addition formula:
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2),$
$(x_1y_1 - x_2y_2)/(x_1y_2 - x_2y_1)).$
Low degree, no need for d.

Warning: fails for doubling!
Is this really "addition"?
Most EC formulas have failures.

More coordinate systems:
Inverted: $x = Z/X$, $y = Z/Y$.
Extended: $x = X/Z$, $y = Y/T$.
Completed: $x = X/Z$, $y = Y/Z$,
$xy = T/Z$.

oubling

$+ (x_1, y_1) =$

$y_1 x_1)/(1{+}dx_1 x_1 y_1 y_1),$

$x_1 x_1)/(1{-}dx_1 x_1 y_1 y_1)) =$

$)/(1 + dx_1^2 y_1^2),$

$)/(1 - dx_1^2 y_1^2)).$

$= 1 + dx_1^2 y_1^2$ so

$+ (x_1, y_1) =$

$)/(x_1^2 + y_1^2),$

$)/(2 - x_1^2 - y_1^2)).$

iminate divisions

: only $3\mathbf{M} + 4\mathbf{S}$.

ster than addition.

many doublings in ECC.

More addition strategies

Dual addition formula:

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

$((x_1 y_1 + x_2 y_2)/(x_1 x_2 + y_1 y_2),$

$(x_1 y_1 - x_2 y_2)/(x_1 y_2 - x_2 y_1)).$

Low degree, no need for d.

Warning: fails for doubling!

Is this really "addition"?

Most EC formulas have failures.

More coordinate systems:

Inverted: $x = Z/X$, $y = Z/Y$.

Extended: $x = X/Z$, $y = Y/T$.

Completed: $x = X/Z$, $y = Y/Z$, $xy = T/Z$.

More ell

Edwards

Easiest v

elliptic c

Geometr

are Edwa

Algebrai

more elli

Every oc

expresse

$v^2 = u^3$

Warning

different

$=$
$+dx_1x_1y_1y_1)$,
$-dx_1x_1y_1y_1)) =$
${}_1^2y_1^2)$,
${}_1^2y_1^2))$.
${}_1^2y_1^2$ so
$=$
${}^2)$,
$- y_1^2))$.
visions
$\mathbf{M} + 4\mathbf{S}$.
addition.
blings in ECC.

More addition strategies

Dual addition formula:
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2),$
$(x_1y_1 - x_2y_2)/(x_1y_2 - x_2y_1))$.
Low degree, no need for d.

Warning: fails for doubling!
Is this really "addition"?
Most EC formulas have failures.

More coordinate systems:
Inverted: $x = Z/X$, $y = Z/Y$.
Extended: $x = X/Z$, $y = Y/T$.
Completed: $x = X/Z$, $y = Y/Z$, $xy = T/Z$.

More elliptic curve

Edwards curves ar
Easiest way to unc
elliptic curves is E

Geometrically, all
are Edwards curve

Algebraically,
more elliptic curve

Every odd-char cu
expressed as Weie
$v^2 = u^3 + a_2u^2 +$

Warning: "Weiers
different meaning

$y_1)$,

$y_1)) =$

ECC.

More addition strategies

Dual addition formula:

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

$((x_1 y_1 + x_2 y_2)/(x_1 x_2 + y_1 y_2),$

$(x_1 y_1 - x_2 y_2)/(x_1 y_2 - x_2 y_1))$.

Low degree, no need for d.

Warning: fails for doubling!

Is this really "addition"?

Most EC formulas have failures.

More coordinate systems:

Inverted: $x = Z/X$, $y = Z/Y$.

Extended: $x = X/Z$, $y = Y/T$.

Completed: $x = X/Z$, $y = Y/Z$, $xy = T/Z$.

More elliptic curves

Edwards curves are elliptic.

Easiest way to understand elliptic curves is Edwards.

Geometrically, all elliptic cur are Edwards curves.

Algebraically, more elliptic curves exist.

Every odd-char curve can be expressed as Weierstrass cur

$v^2 = u^3 + a_2 u^2 + a_4 u + a_6$

Warning: "Weierstrass" has different meaning in char 2.

More addition strategies

Dual addition formula:
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2),$
$(x_1y_1 - x_2y_2)/(x_1y_2 - x_2y_1)).$
Low degree, no need for d.

Warning: fails for doubling!
Is this really "addition"?
Most EC formulas have failures.

More coordinate systems:
Inverted: $x = Z/X$, $y = Z/Y$.
Extended: $x = X/Z$, $y = Y/T$.
Completed: $x = X/Z$, $y = Y/Z$,
$xy = T/Z$.

More elliptic curves

Edwards curves are elliptic.
Easiest way to understand
elliptic curves is Edwards.

Geometrically, all elliptic curves
are Edwards curves.

Algebraically,
more elliptic curves exist.

Every odd-char curve can be
expressed as Weierstrass curve
$v^2 = u^3 + a_2u^2 + a_4u + a_6$.

Warning: "Weierstrass" has
different meaning in char 2.

dition strategies

dition formula:

$+ (x_2, y_2) =$

$- x_2y_2)/(x_1x_2 + y_1y_2),$

$- x_2y_2)/(x_1y_2 - x_2y_1)).$

gree, no need for d.

: fails for doubling!

eally "addition"?

C formulas have failures.

ordinate systems:

: $x = Z/X$, $y = Z/Y$.

d: $x = X/Z$, $y = Y/T$.

ed: $x = X/Z$, $y = Y/Z$,

$/Z$.

More elliptic curves

Edwards curves are elliptic.
Easiest way to understand
elliptic curves is Edwards.

Geometrically, all elliptic curves
are Edwards curves.

Algebraically,
more elliptic curves exist.

Every odd-char curve can be
expressed as Weierstrass curve
$v^2 = u^3 + a_2u^2 + a_4u + a_6$.

Warning: "Weierstrass" has
different meaning in char 2.

Addition

$v^2 = u^3$

Slope λ

Note tha

ategies

nula:

=

$x_1x_2 + y_1y_2)$,

$x_1y_2 - x_2y_1))$.

eed for d.

doubling!

tion"?

have failures.

ystems:

X, $y = Z/Y$.

$/Z$, $y = Y/T$.

X/Z, $y = Y/Z$,

More elliptic curves

Edwards curves are elliptic.
Easiest way to understand
elliptic curves is Edwards.

Geometrically, all elliptic curves
are Edwards curves.

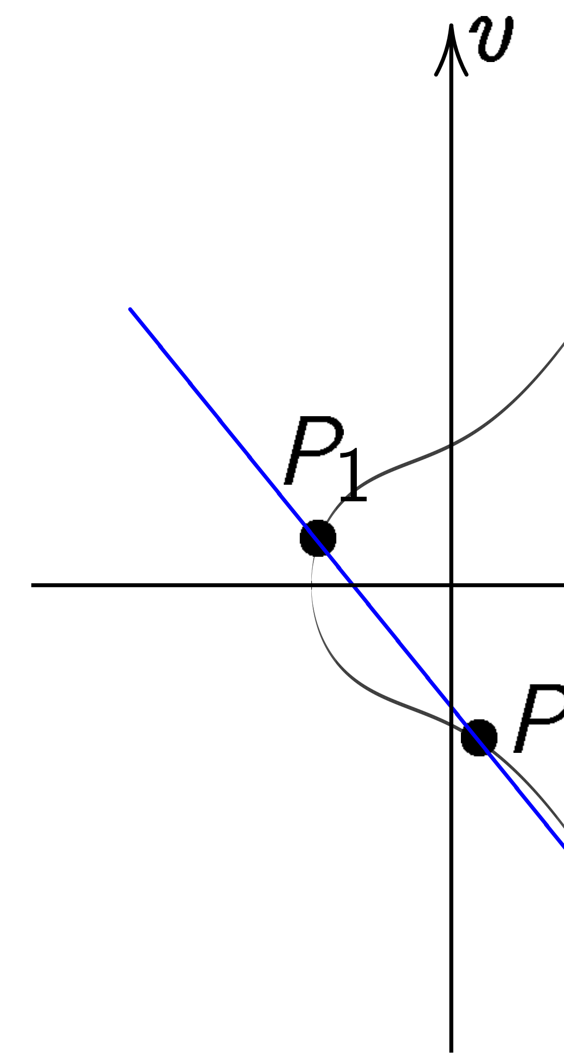
Algebraically,
more elliptic curves exist.

Every odd-char curve can be
expressed as Weierstrass curve
$v^2 = u^3 + a_2u^2 + a_4u + a_6$.

Warning: "Weierstrass" has
different meaning in char 2.

Addition on Weier

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



Slope $\lambda = (v_2 - v$

Note that $u_1 \neq u_2$

$y_2)$,
$y_1))$.

ures.

Y.
$/T$.
Y/Z,

More elliptic curves

Edwards curves are elliptic.
Easiest way to understand elliptic curves is Edwards.

Geometrically, all elliptic curves are Edwards curves.

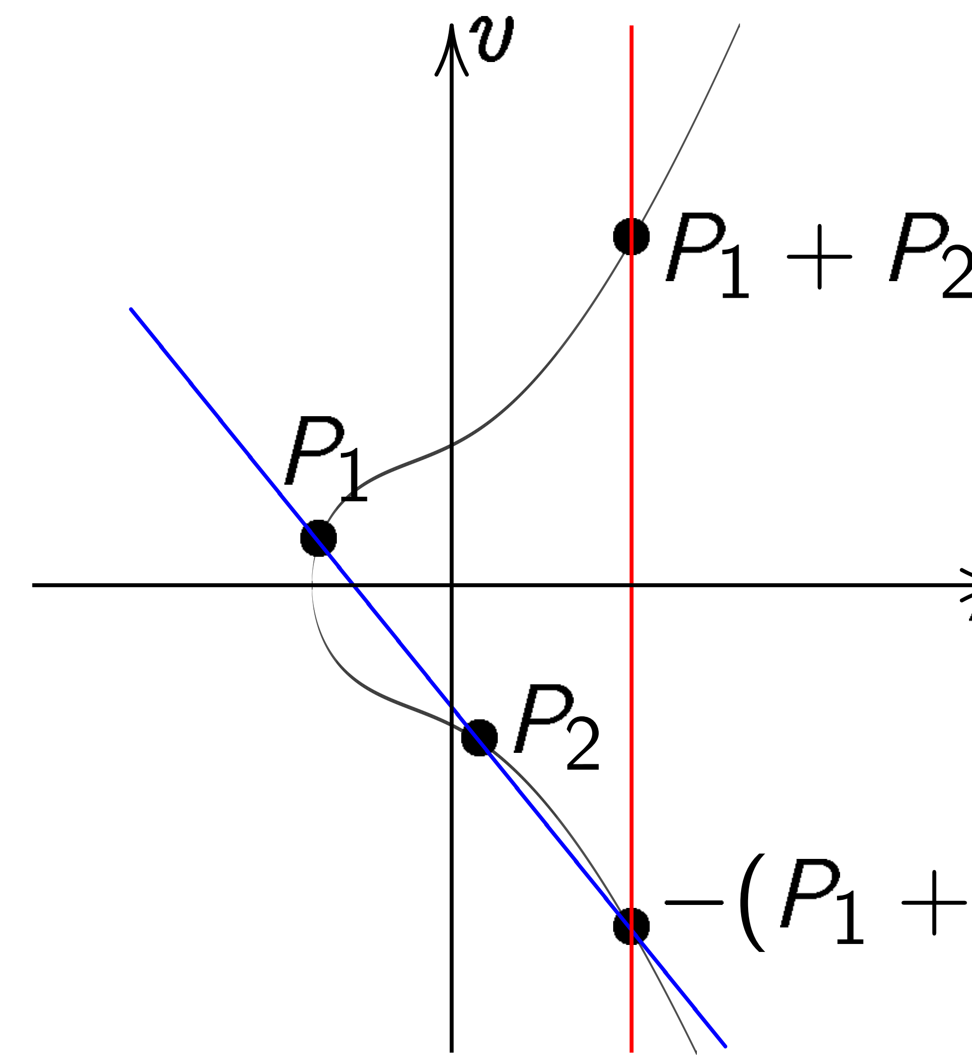
Algebraically, more elliptic curves exist.

Every odd-char curve can be expressed as Weierstrass curve $v^2 = u^3 + a_2u^2 + a_4u + a_6$.

Warning: "Weierstrass" has different meaning in char 2.

Addition on Weierstrass curv

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



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

More elliptic curves

Edwards curves are elliptic.
Easiest way to understand elliptic curves is Edwards.

Geometrically, all elliptic curves are Edwards curves.

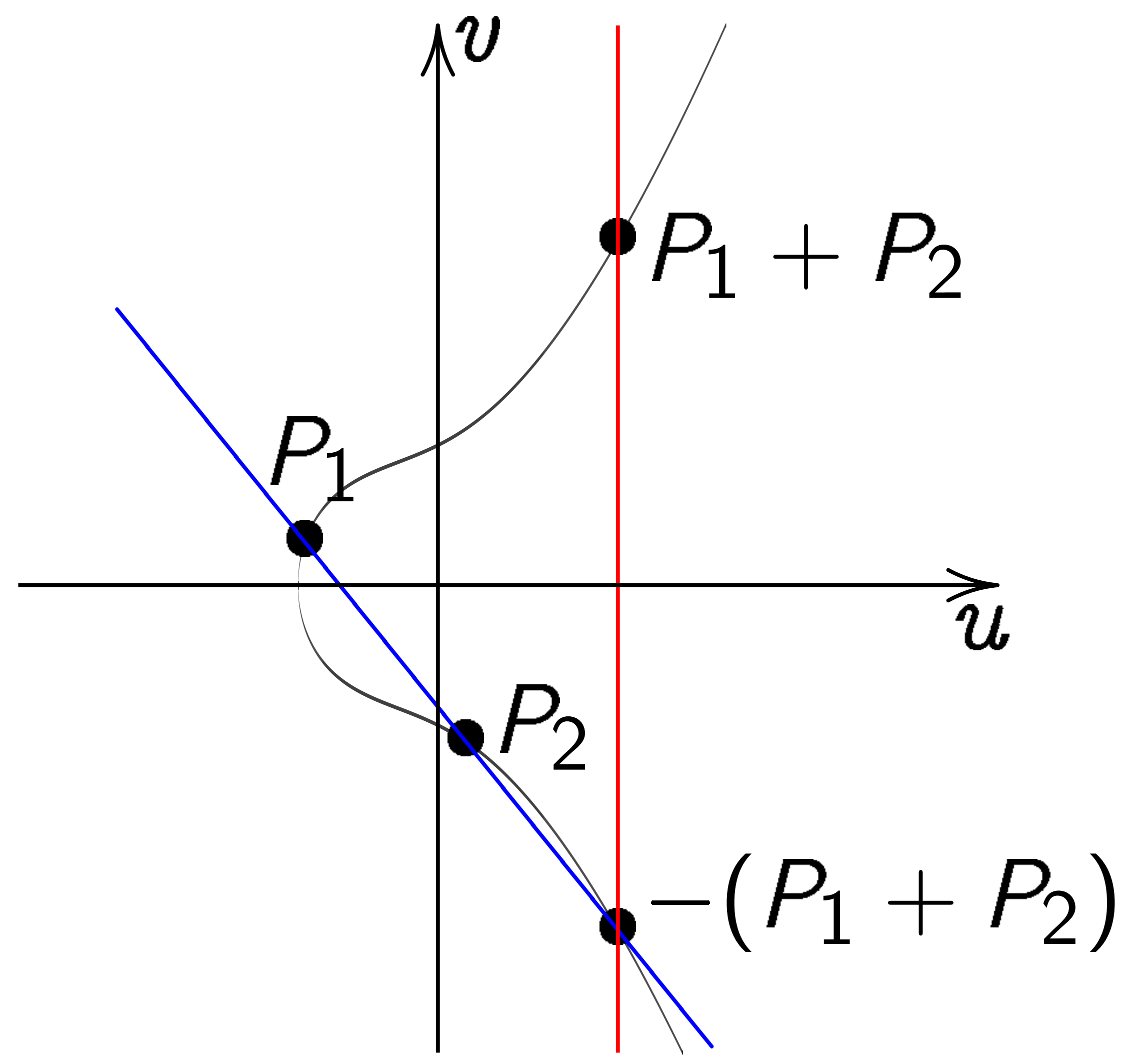
Algebraically,
more elliptic curves exist.

Every odd-char curve can be expressed as Weierstrass curve $v^2 = u^3 + a_2u^2 + a_4u + a_6$.

Warning: "Weierstrass" has different meaning in char 2.

Addition on Weierstrass curve

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



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

iptic curves

curves are elliptic.
way to understand
curves is Edwards.

rically, all elliptic curves
ards curves.

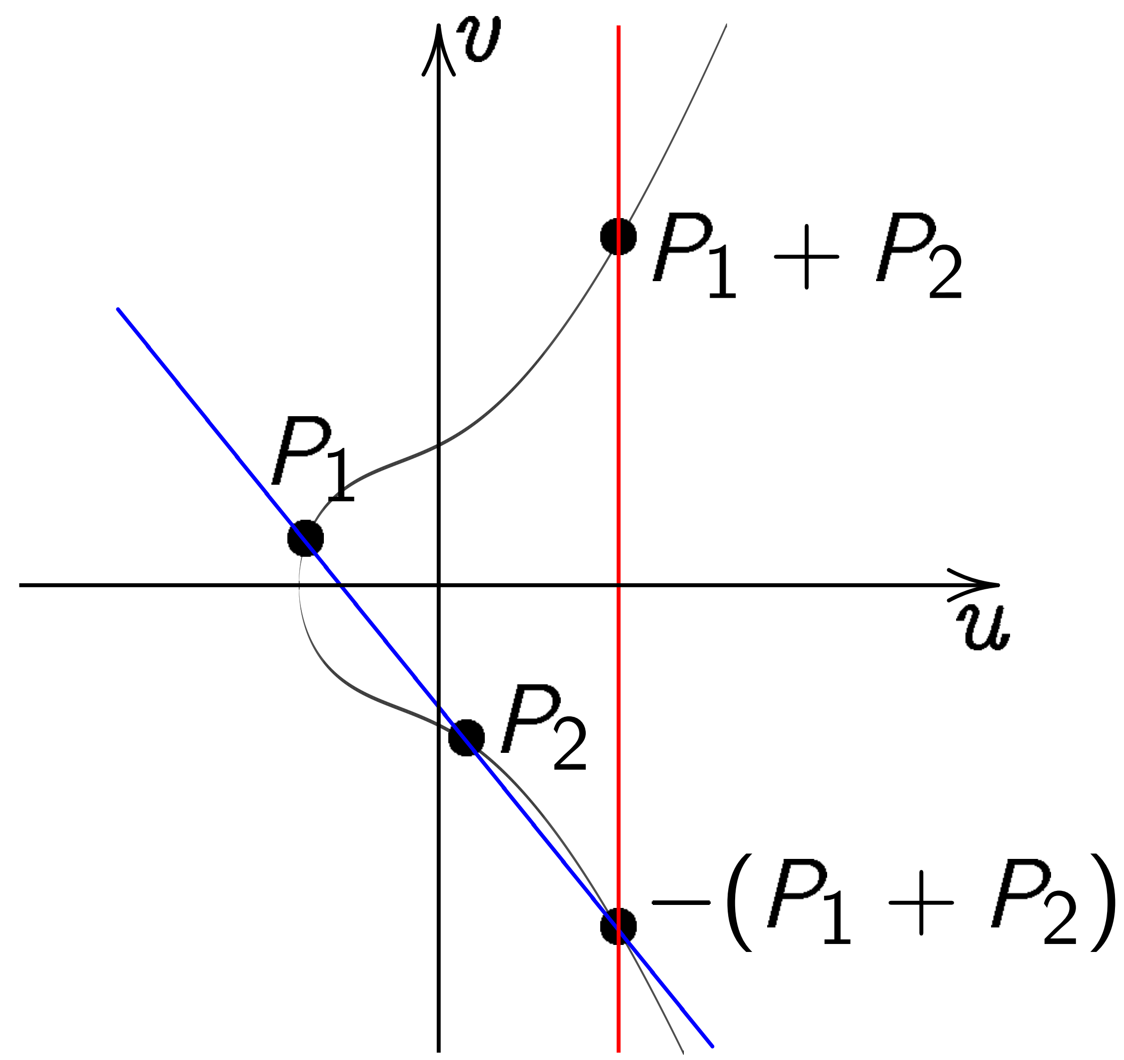
cally,
iptic curves exist.

dd-char curve can be
d as Weierstrass curve
$+ a_2u^2 + a_4u + a_6$.

: “Weierstrass” has
meaning in char 2.

Addition on Weierstrass curve

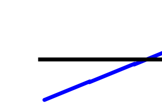
$v^2 = u^3 + u^2 + u + 1$



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

Doubling

$v^2 = u^3$



Slope λ

es

e elliptic.

derstand

dwards.

elliptic curves

s.

es exist.

rve can be

rstrass curve

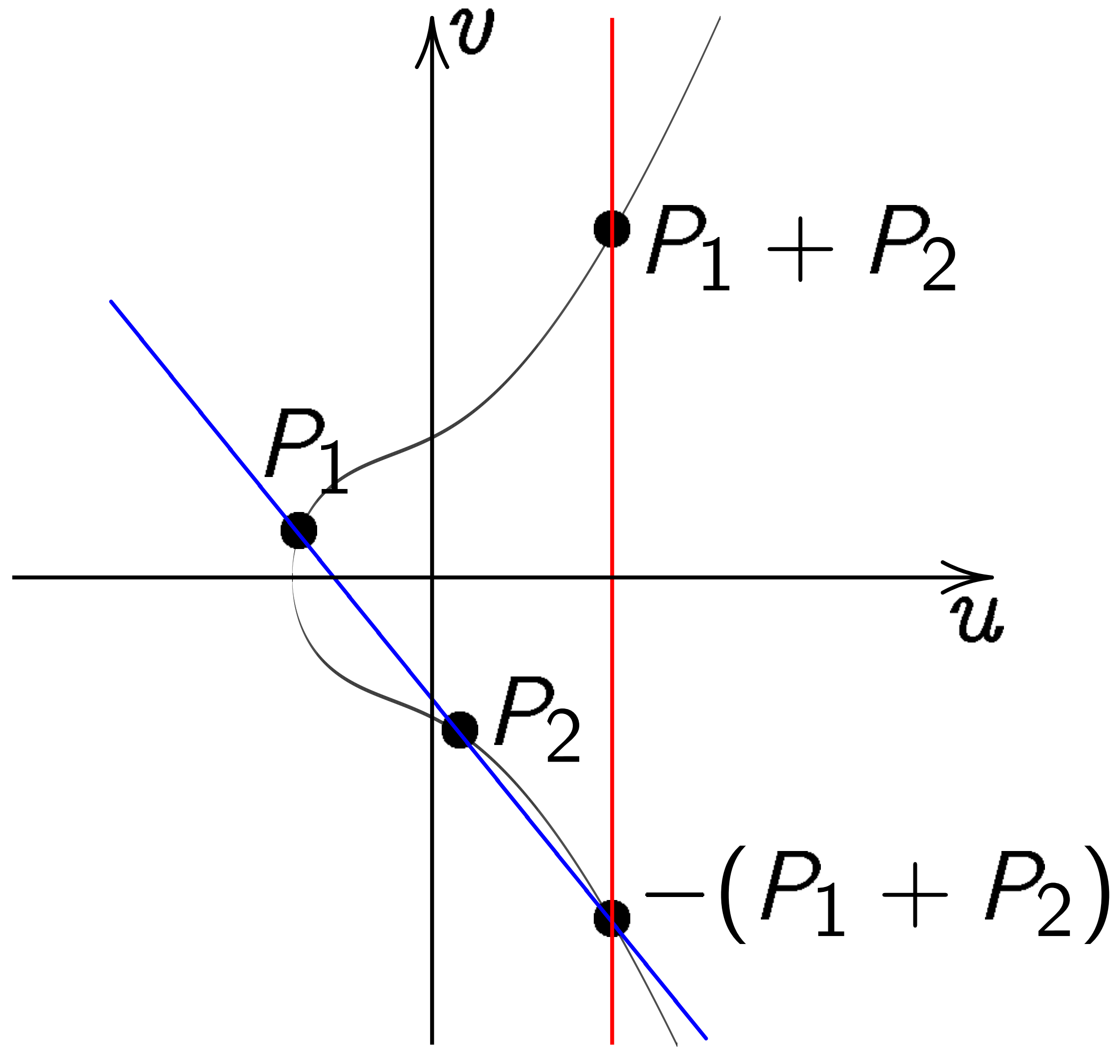
$+ a_4 u + a_6$.

trass" has

in char 2.

Addition on Weierstrass curve

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

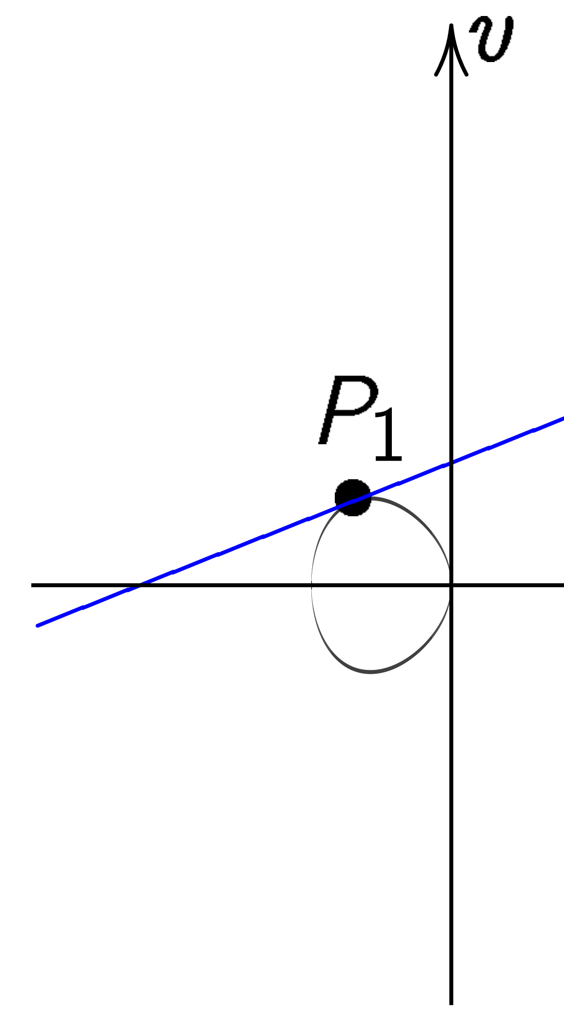


Slope $\lambda = (v_2 - v_1)/(u_2 - u_1)$.

Note that $u_1 \neq u_2$.

Doubling on Weier

$$v^2 = u^3 - u$$



Slope $\lambda = (3u_1^2 -$

rves

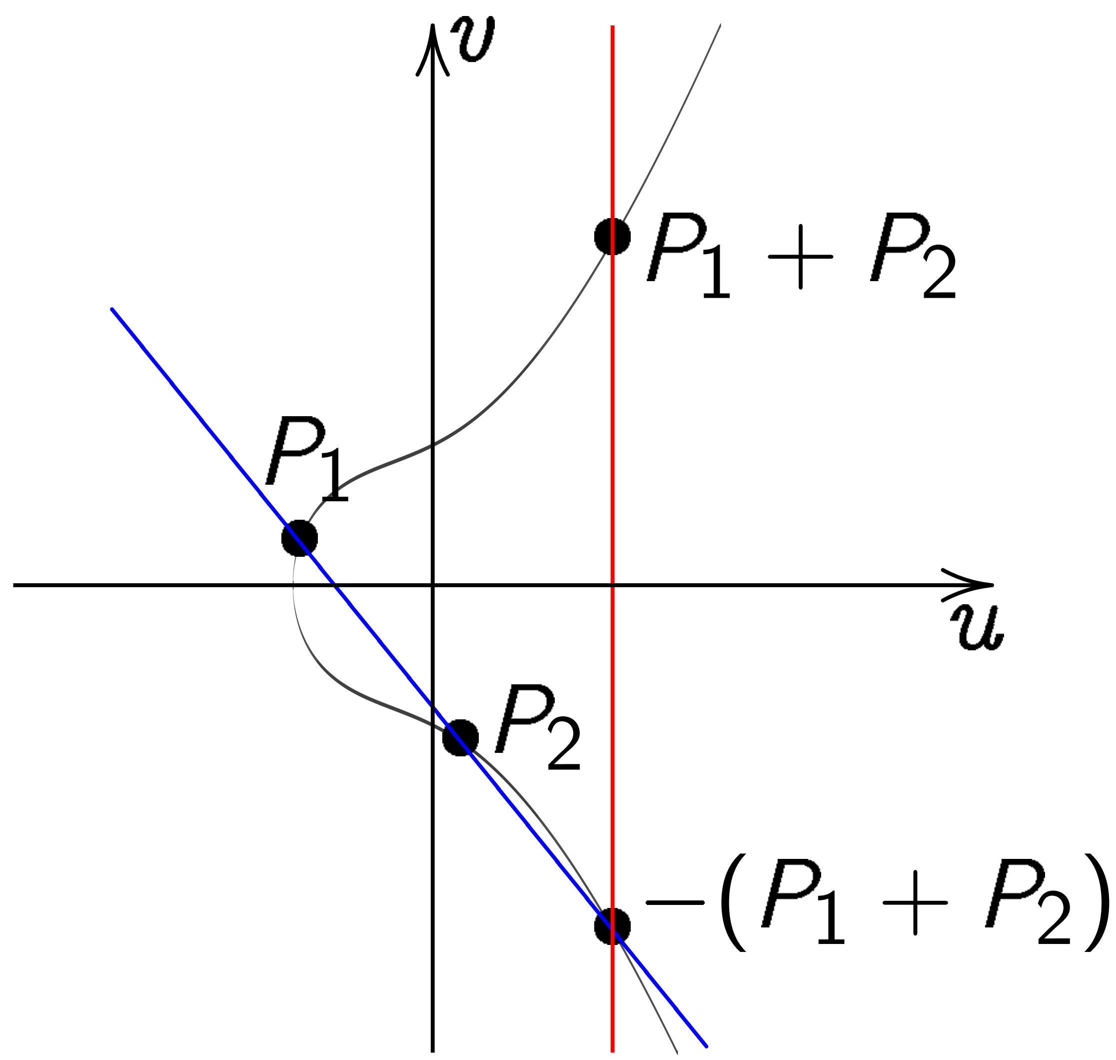
e

rve

.

Addition on Weierstrass curve

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

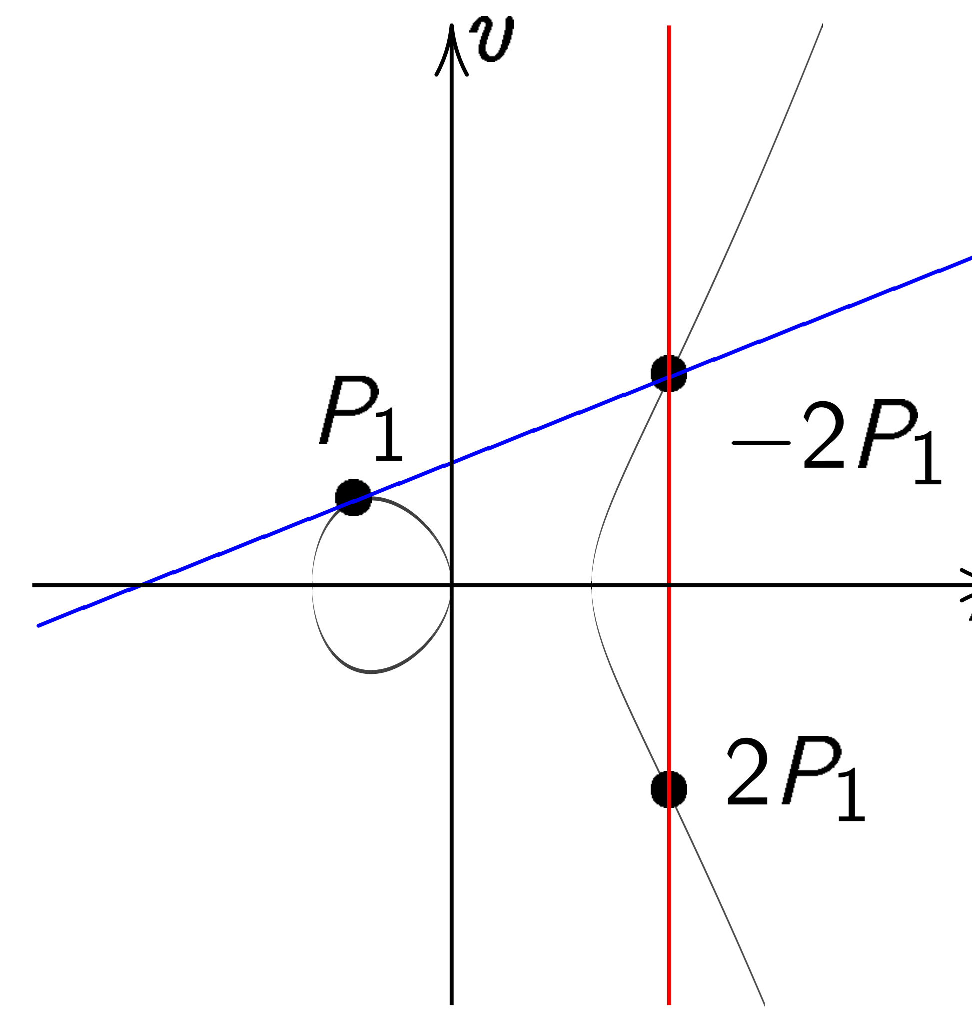


Slope $\lambda = (v_2 - v_1)/(u_2 - u_1)$.

Note that $u_1 \neq u_2$.

Doubling on Weierstrass cur

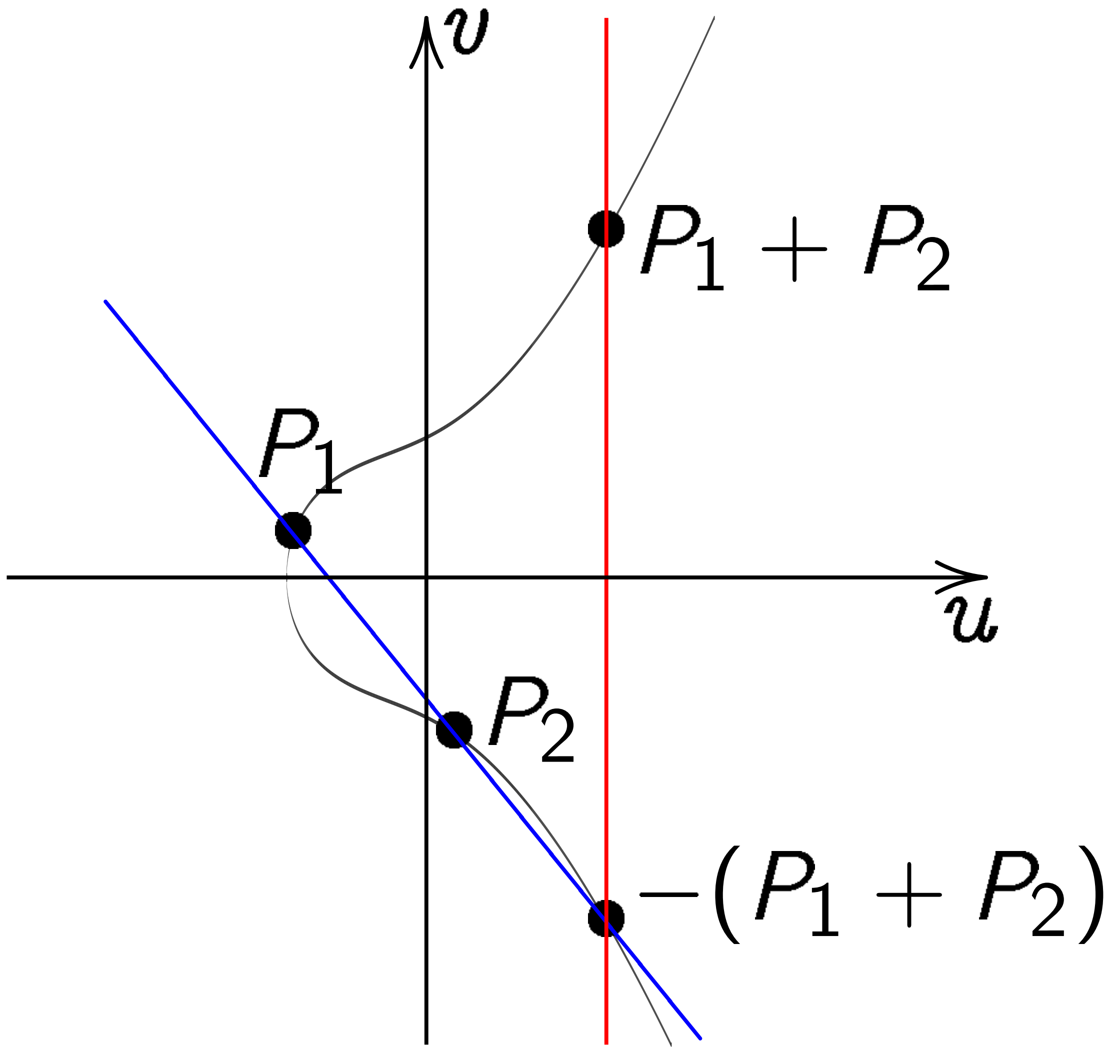
$v^2 = u^3 - u$



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

Addition on Weierstrass curve

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

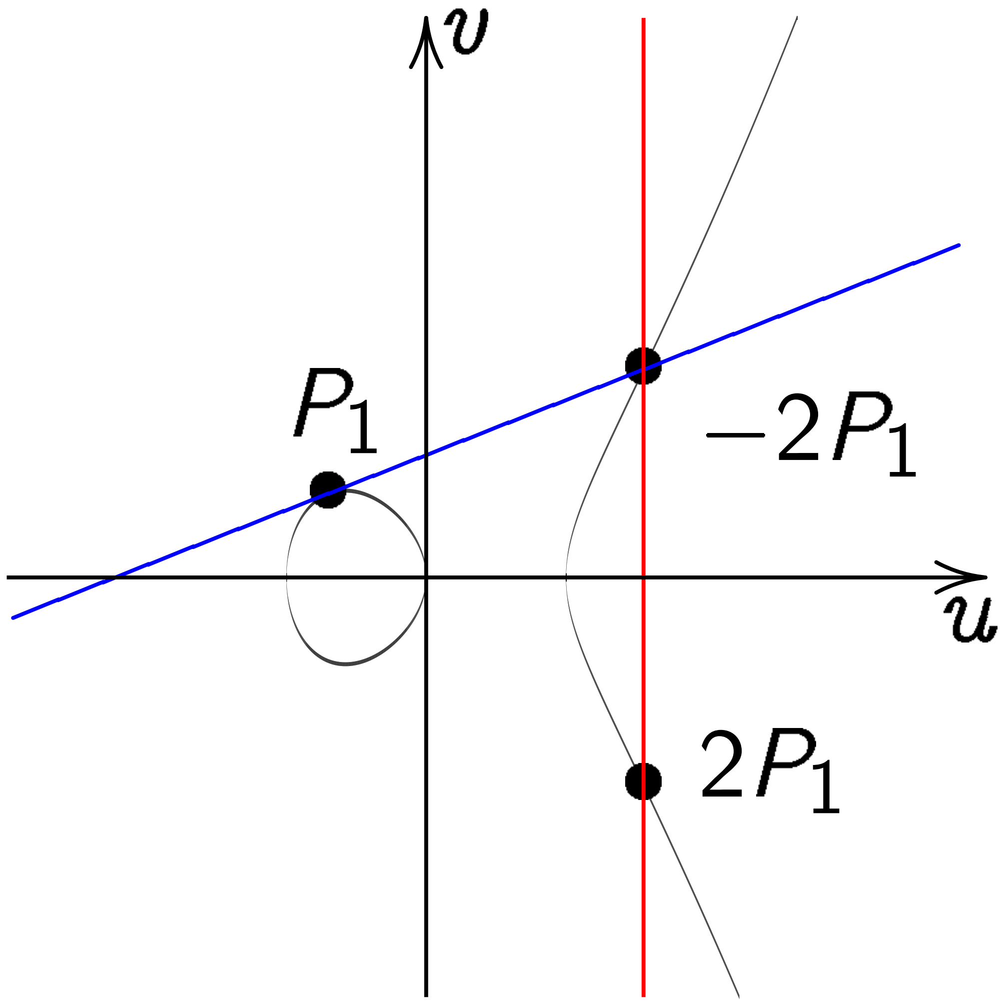


Slope $\lambda = (v_2 - v_1)/(u_2 - u_1)$.

Note that $u_1 \neq u_2$.

Doubling on Weierstrass curve

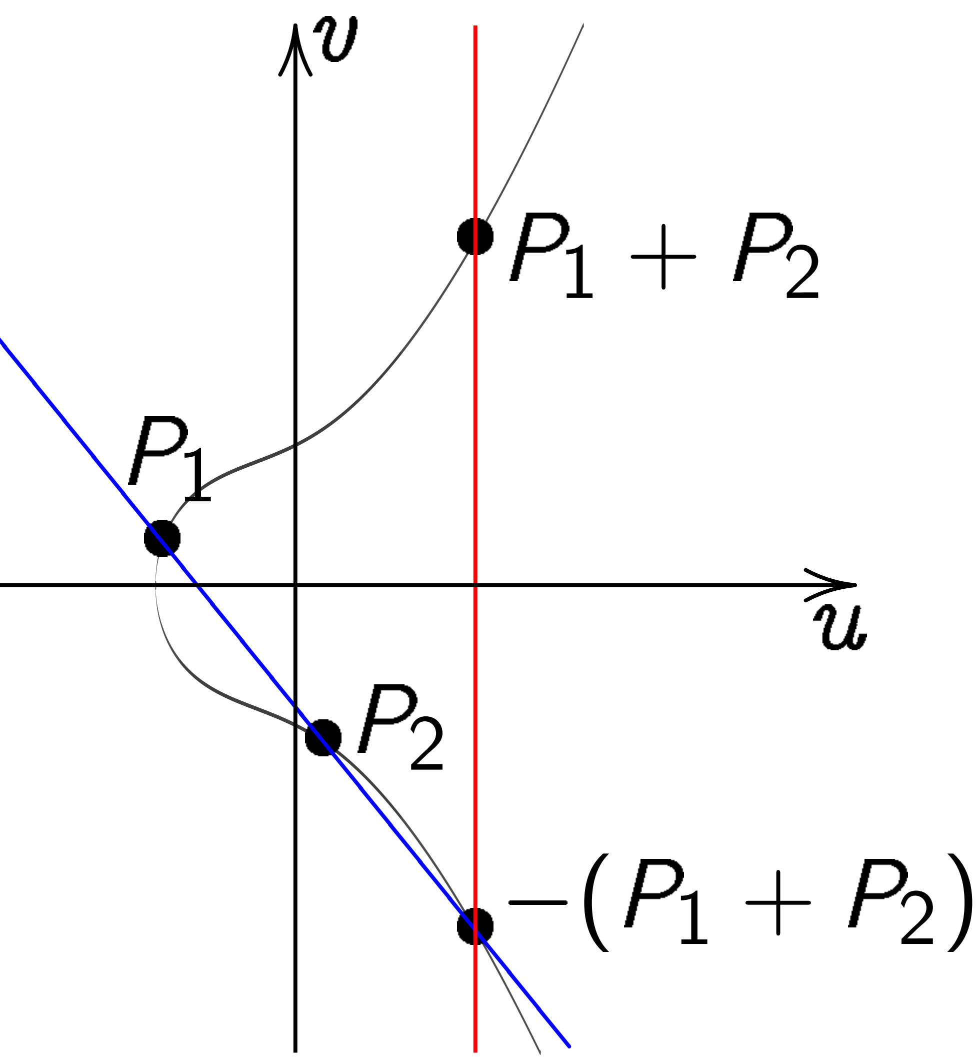
$v^2 = u^3 - u$



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

n on Weierstrass curve

$$+ u^2 + u + 1$$

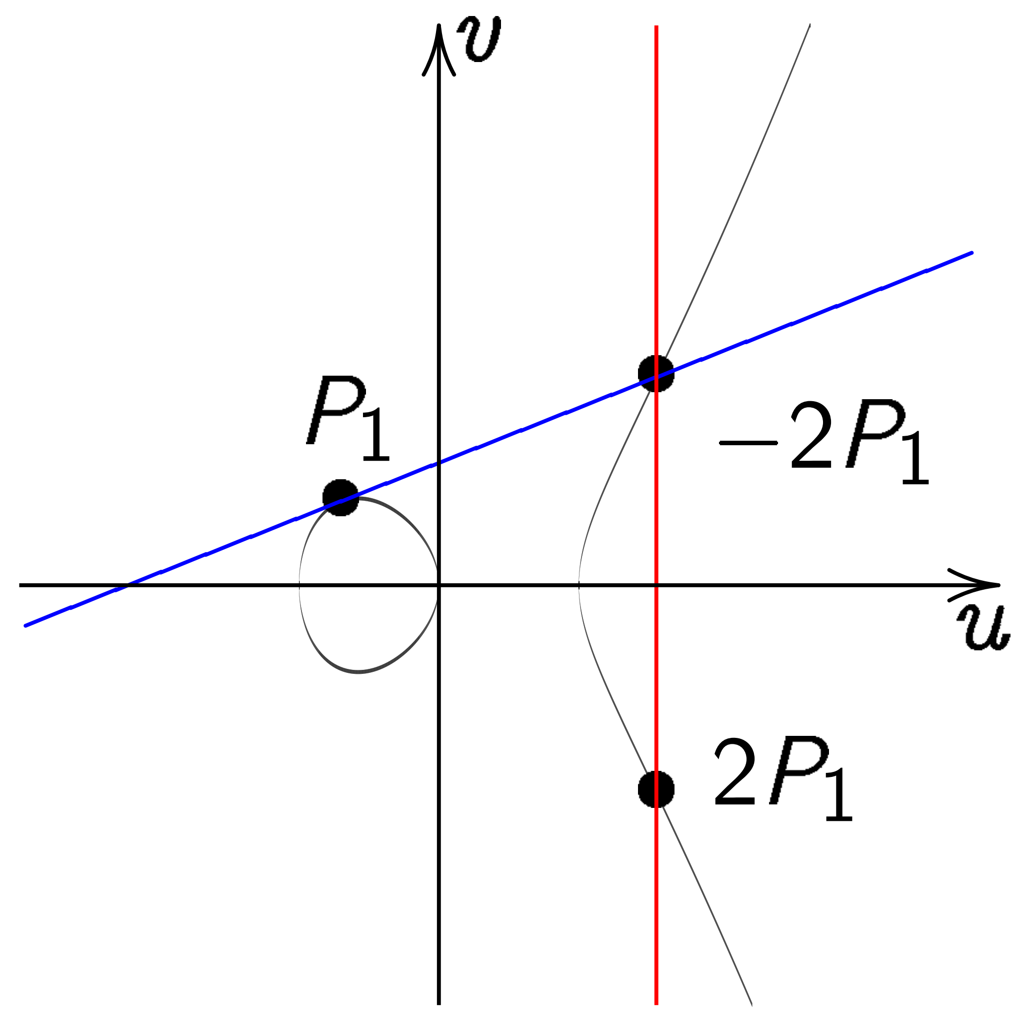


$= (v_2 - v_1)/(u_2 - u_1)$.

at $u_1 \neq u_2$.

Doubling on Weierstrass curve

$$v^2 = u^3 - u$$



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

In most

(u_1, v_1)

(u_3, v_3)

$(\lambda^2 - u_1$

$u_1 \neq u_2$

$\lambda = (v_2$

Total co

(u_1, v_1)

"doublin

$\lambda = (3u$

Total co

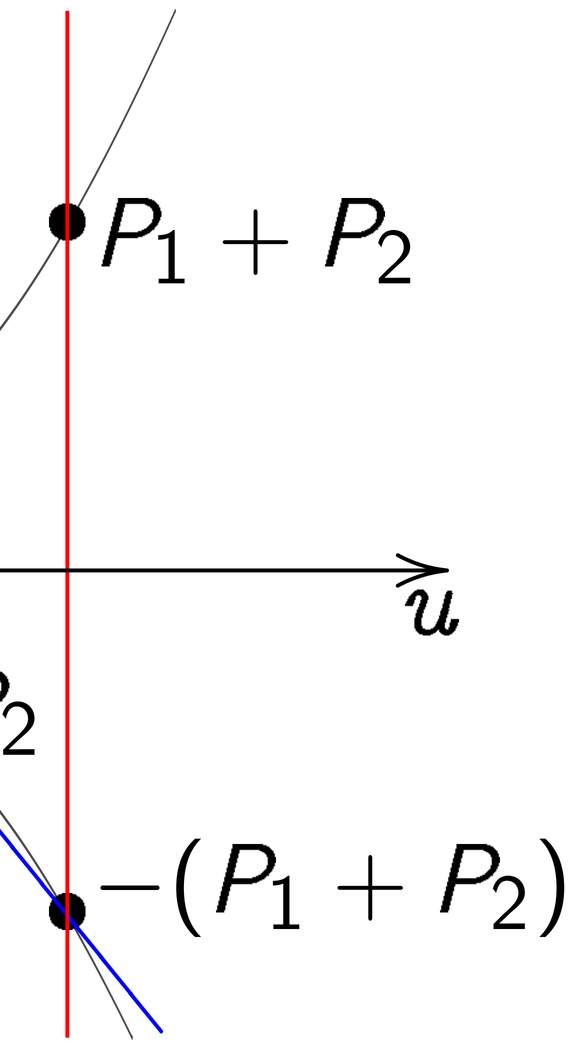
Also har

(u_1, v_1)

inputs a

rstrass curve

$+ 1$

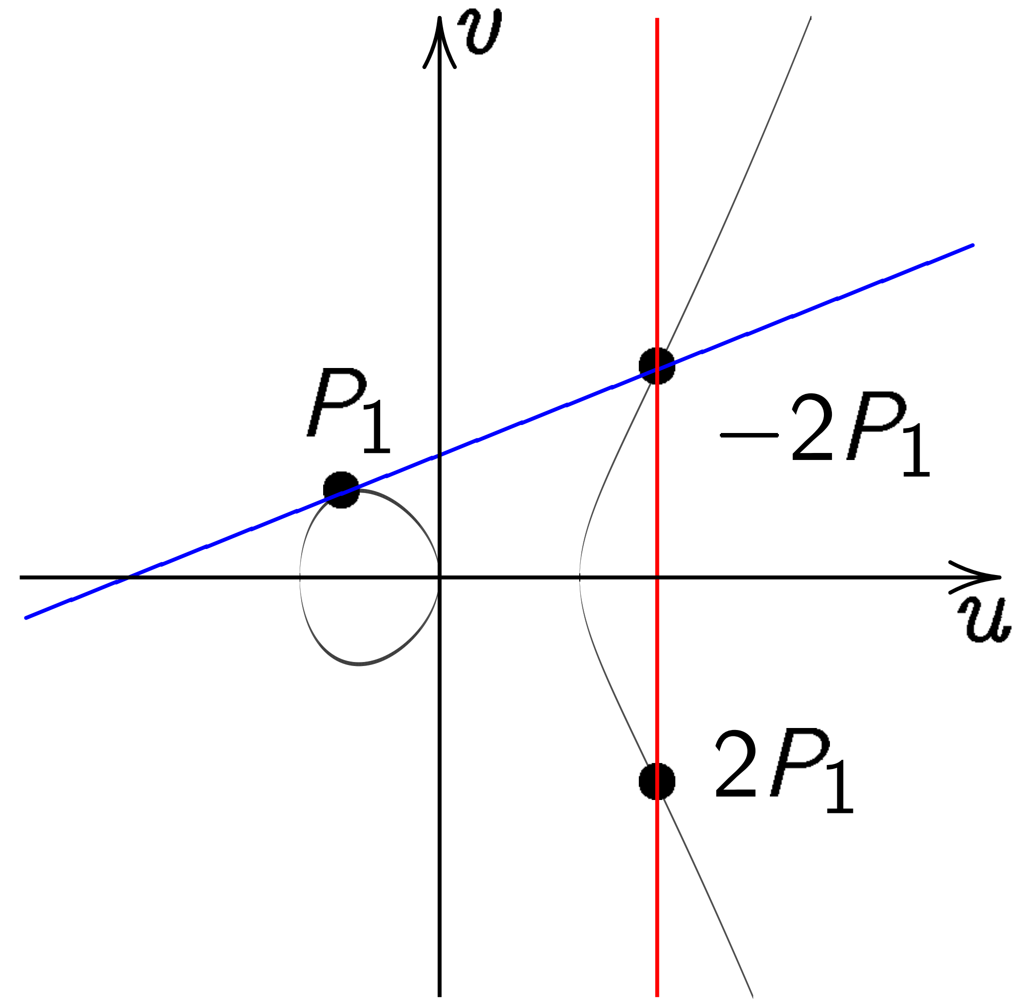


$_1)/(u_2 - u_1)$.

$_2$.

Doubling on Weierstrass curve

$v^2 = u^3 - u$



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

In most cases

$(u_1, v_1) + (u_2, v_2$

(u_3, v_3) where $(u_3$

$(\lambda^2 - u_1 - u_2, \lambda(u_1$

$u_1 \neq u_2$, "additio

$\lambda = (v_2 - v_1)/(u_2$

Total cost $1\mathbf{I} + 2\mathbf{N}$

$(u_1, v_1) = (u_2, v_2$

"doubling" (alert!

$\lambda = (3u_1^2 + 2a_2u_1$

Total cost $1\mathbf{I} + 2\mathbf{N}$

Also handle some

$(u_1, v_1) = (u_2, -v$

inputs at ∞.

ve

2

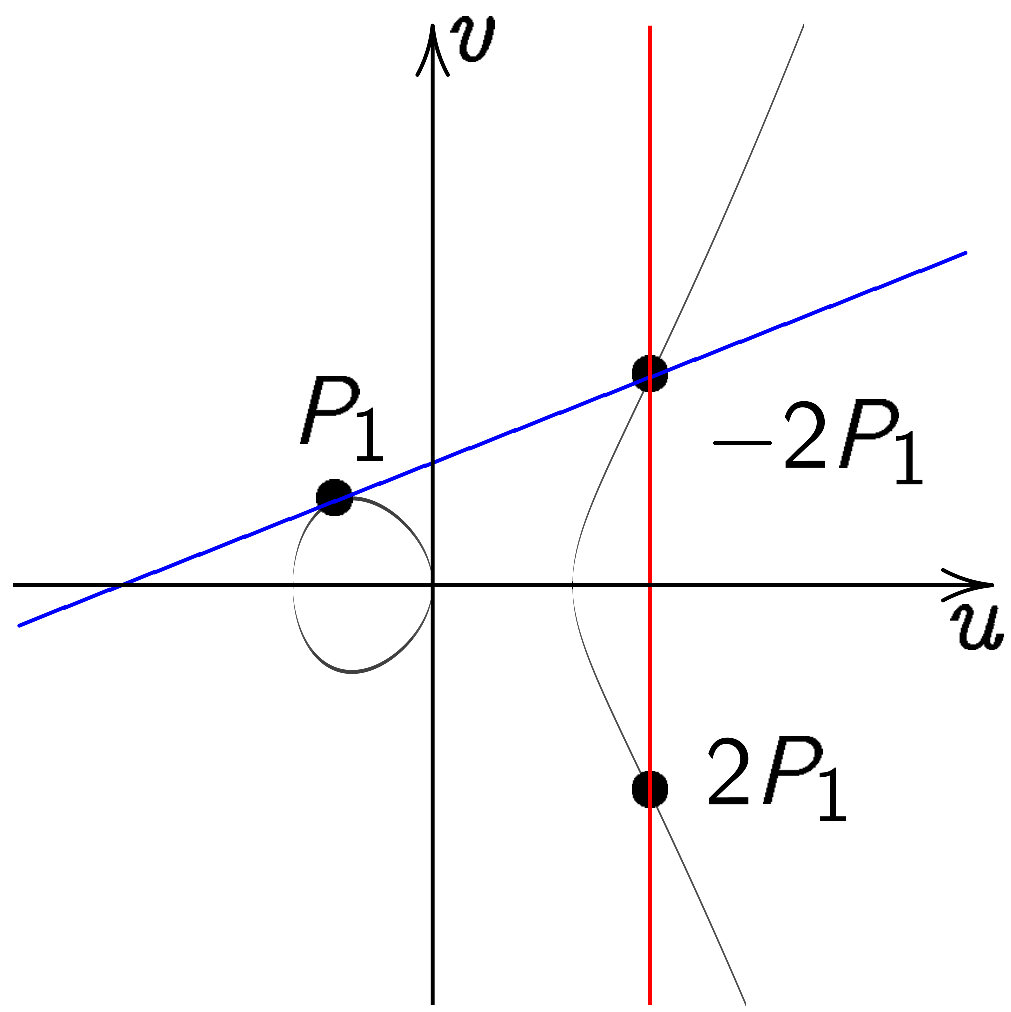
u

$P_2)$

$u_1)$.

Doubling on Weierstrass curve

$v^2 = u^3 - u$



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

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

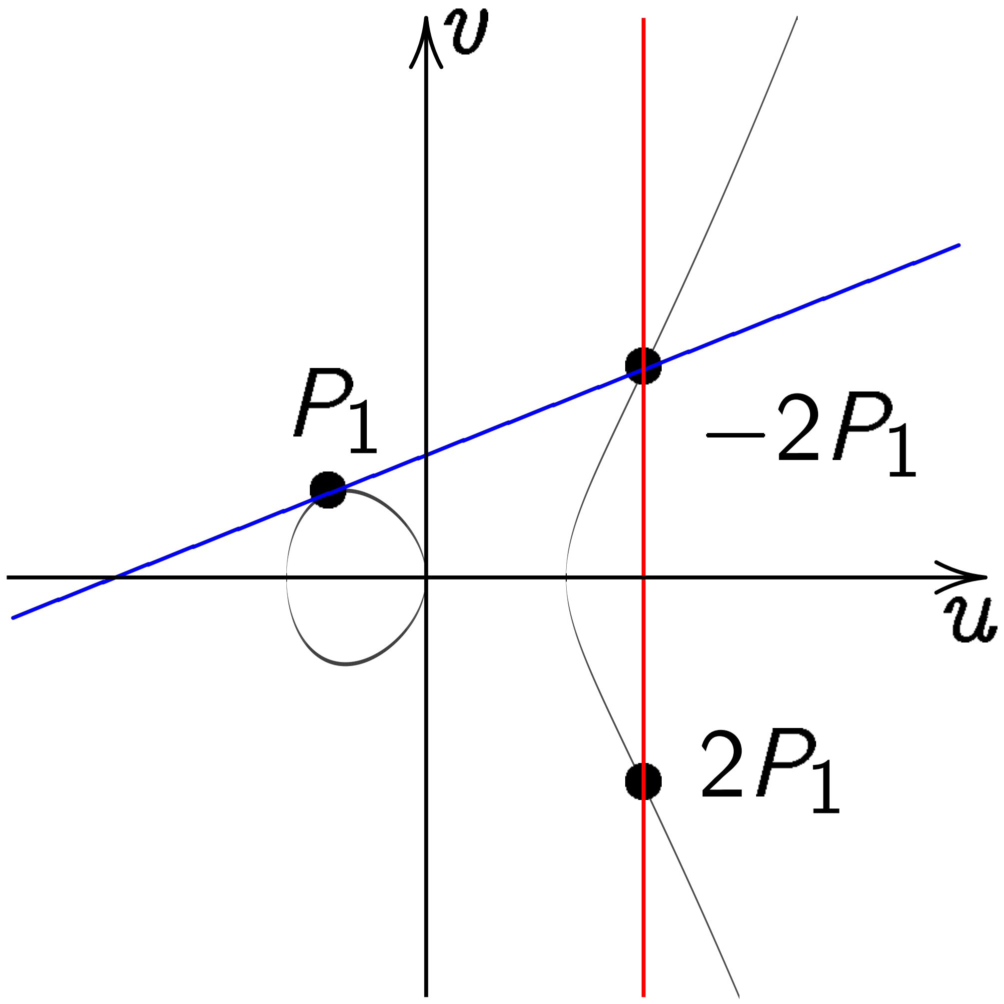
$u_1 \neq u_2$, "addition" (alert!)
$\lambda = (v_2 - v_1)/(u_2 - u_1)$.
Total cost $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}$.

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

Also handle some exceptions
$(u_1, v_1) = (u_2, -v_2)$;
inputs at ∞.

Doubling on Weierstrass curve

$v^2 = u^3 - u$



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

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

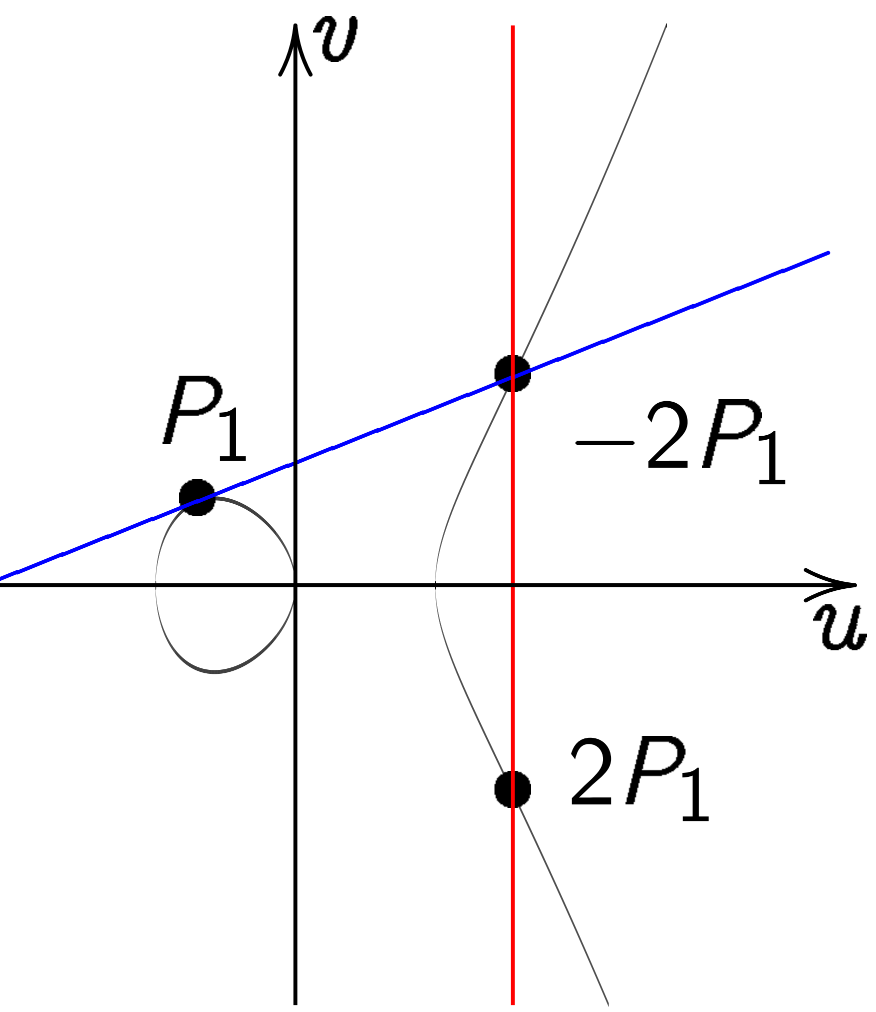
$u_1 \neq u_2$, “addition” (alert!): $\lambda = (v_2 - v_1)/(u_2 - u_1)$. Total cost $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}$.

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

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

g on Weierstrass curve

$- u$



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

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

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

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

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

Biration

Starting
on $x^2 +$

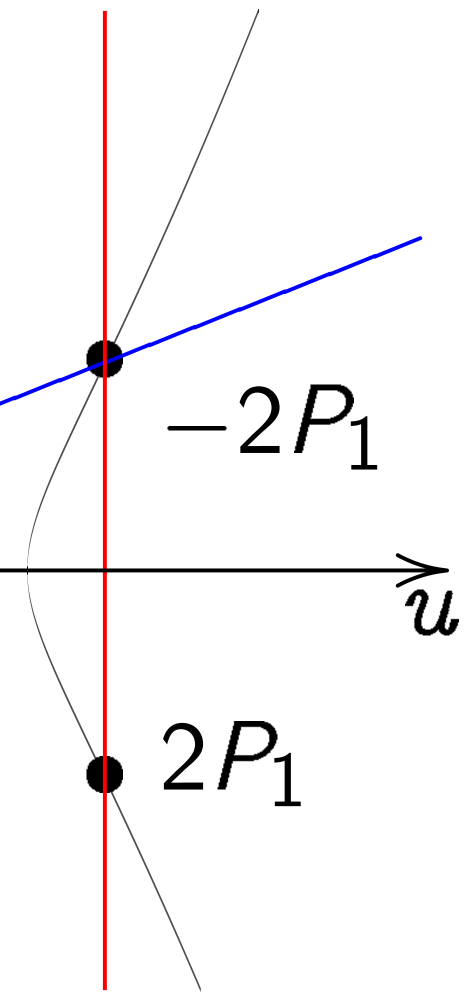
Define A
$B = 4/($
$u = (1 -$
$v = u/x$
(Skip a

$v^2 = u^3$

Maps Ec
Compati

Easily in
$x = u/v$

rstrass curve



$1)/(2v_1)$.

In most cases

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

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

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

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

Birational equivale

Starting from poin
on $x^2 + y^2 = 1 +$

Define $A = 2(1 +$
$B = 4/(1 - d)$;
$u = (1 + y)/(B(1$
$v = u/x = (1 + y$
(Skip a few except

$v^2 = u^3 + (A/B)u$

Maps Edwards to
Compatible with p

Easily invert this n
$x = u/v$, $y = (Bu$

rve

u

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

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

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

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

Birational equivalence

Starting from point (x, y)
on $x^2 + y^2 = 1 + dx^2y^2$:

Define $A = 2(1 + d)/(1 - d$
$B = 4/(1 - d)$;
$u = (1 + y)/(B(1 - y))$,
$v = u/x = (1 + y)/(Bx(1 -$
(Skip a few exceptional poin

$v^2 = u^3 + (A/B)u^2 + (1/B$

Maps Edwards to Weierstras
Compatible with point addit

Easily invert this map:
$x = u/v$, $y = (Bu - 1)/(B$

In most cases

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

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

$(u_1, v_1) = (u_2, v_2)$ and $v_1 \neq 0$,
"doubling" (alert!):
$\lambda = (3u_1^2 + 2a_2 u_1 + a_4)/(2v_1)$.
Total cost $1\mathbf{I} + 2\mathbf{M} + 2\mathbf{S}$.

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

<u>Birational equivalence</u>

Starting from point (x, y)
on $x^2 + y^2 = 1 + dx^2y^2$:

Define $A = 2(1 + d)/(1 - d)$,
$B = 4/(1 - d)$;
$u = (1 + y)/(B(1 - y))$,
$v = u/x = (1 + y)/(Bx(1 - y))$.
(Skip a few exceptional points.)

$v^2 = u^3 + (A/B)u^2 + (1/B^2)u$.

Maps Edwards to Weierstrass.
Compatible with point addition!

Easily invert this map:
$x = u/v$, $y = (Bu - 1)/(Bu + 1)$.

cases

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

, "addition" (alert!):
$- v_1)/(u_2 - u_1)$.
st $1\mathbf{I} + 2\mathbf{M} + 1\mathbf{S}$.

$= (u_2, v_2)$ and $v_1 \neq 0$,
ng" (alert!):
$_1^2 + 2a_2 u_1 + a_4)/(2v_1)$.
st $1\mathbf{I} + 2\mathbf{M} + 2\mathbf{S}$.

ndle some exceptions:
$= (u_2, -v_2)$;
t ∞.

Birational equivalence

Starting from point (x, y)
on $x^2 + y^2 = 1 + dx^2y^2$:

Define $A = 2(1 + d)/(1 - d)$,
$B = 4/(1 - d)$;
$u = (1 + y)/(B(1 - y))$,
$v = u/x = (1 + y)/(Bx(1 - y))$.
(Skip a few exceptional points.)

$$v^2 = u^3 + (A/B)u^2 + (1/B^2)u.$$

Maps Edwards to Weierstrass.
Compatible with point addition!

Easily invert this map:
$x = u/v$, $y = (Bu - 1)/(Bu + 1)$.

Some hi

There ar
elliptic-c

1984 (pu
ECM, th
of factor

1984 (pu
and inde
1984 (pu
Elliptic-c

Bosma,
Chudnov
elliptic-c

$) =$

$_3, v_3) =$

$-u_3)-v_1)$.

n" (alert!):

$_2 - u_1)$.

$\mathbf{M} + 1\mathbf{S}$.

$)$ and $v_1 \neq 0$,

$)$:

$+ a_4)/(2v_1)$.

$\mathbf{M} + 2\mathbf{S}$.

exceptions:

$_2)$;

Birational equivalence

Starting from point (x, y)
on $x^2 + y^2 = 1 + dx^2y^2$:

Define $A = 2(1 + d)/(1 - d)$,
$B = 4/(1 - d)$;
$u = (1 + y)/(B(1 - y))$,
$v = u/x = (1 + y)/(Bx(1 - y))$.
(Skip a few exceptional points.)

$$v^2 = u^3 + (A/B)u^2 + (1/B^2)u.$$

Maps Edwards to Weierstrass.
Compatible with point addition!

Easily invert this map:
$x = u/v$, $y = (Bu - 1)/(Bu + 1)$.

Some history

There are many p
elliptic-curve comp

1984 (published 1
ECM, the elliptic-
of factoring intege

1984 (published 1
and independently
1984 (published 1
Elliptic-curve cryp

Bosma, Goldwass
Chudnovsky–Chud
elliptic-curve prim

).

:

$\neq 0$,

v_1).

s:

Birational equivalence

Starting from point (x, y) on $x^2 + y^2 = 1 + dx^2y^2$:

Define $A = 2(1 + d)/(1 - d)$, $B = 4/(1 - d)$; $u = (1 + y)/(B(1 - y))$, $v = u/x = (1 + y)/(Bx(1 - y))$. (Skip a few exceptional points.)

$$v^2 = u^3 + (A/B)u^2 + (1/B^2)u.$$

Maps Edwards to Weierstrass. Compatible with point addition!

Easily invert this map: $x = u/v$, $y = (Bu - 1)/(Bu + 1)$.

Some history

There are many perspective
elliptic-curve computations.

1984 (published 1987) Lens
ECM, the elliptic-curve met
of factoring integers.

1984 (published 1985) Mille
and independently
1984 (published 1987) Kobl
Elliptic-curve cryptography.

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

Birational equivalence

Starting from point (x, y)
on $x^2 + y^2 = 1 + dx^2y^2$:

Define $A = 2(1 + d)/(1 - d)$,
$B = 4/(1 - d)$;
$u = (1 + y)/(B(1 - y))$,
$v = u/x = (1 + y)/(Bx(1 - y))$.
(Skip a few exceptional points.)

$v^2 = u^3 + (A/B)u^2 + (1/B^2)u$.

Maps Edwards to Weierstrass.
Compatible with point addition!

Easily invert this map:
$x = u/v$, $y = (Bu - 1)/(Bu + 1)$.

Some history

There are many perspectives on elliptic-curve computations.

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

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

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

al equivalence

from point (x, y)
$y^2 = 1 + dx^2y^2$:

$A = 2(1 + d)/(1 - d)$,
$1 - d)$;
$+ y)/(B(1 - y))$,
$= (1 + y)/(Bx(1 - y))$.
few exceptional points.)

$+ (A/B)u^2 + (1/B^2)u$.

dwards to Weierstrass.
ible with point addition!

vert this map:
$, y = (Bu - 1)/(Bu + 1)$.

Some history

There are many perspectives on elliptic-curve computations.

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

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

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

The Edw

1761 Eu
introduc
for $x^2 +$
the “lem

2007 Ed
many cu
Theorem
all ellipti

2007 Be
Edwards
for $x^2 +$
and give

ence

nt (x, y)

dx^2y^2:

$d)/(1-d)$,

$-y))$,

$)/(Bx(1-y))$.

tional points.)

$u^2 + (1/B^2)u$.

Weierstrass.

oint addition!

map:

$u-1)/(Bu+1)$.

Some history

There are many perspectives on elliptic-curve computations.

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

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

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

The Edwards pers

1761 Euler, 1866
introduced an add
for $x^2 + y^2 = 1 -$
the “lemniscatic e

2007 Edwards gen
many curves $x^2 +$
Theorem: have no
all elliptic curves o

2007 Bernstein–La
Edwards addition
for $x^2 + y^2 = 1 +$
and gives new EC

),

$- y))$.

nts.)

$^2)u$.

ss.

tion!

$u + 1)$.

Some history

There are many perspectives on elliptic-curve computations.

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

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

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

The Edwards perspective is

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curv

2007 Edwards generalized to
many curves $x^2 + y^2 = 1 + c$
Theorem: have now obtaine
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is com
for $x^2 + y^2 = 1 + dx^2y^2$ if d
and gives new ECC speed re

Some history

There are many perspectives on elliptic-curve computations.

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

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

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

The Edwards perspective is new!

1761 Euler, 1866 Gauss introduced an addition law for $x^2 + y^2 = 1 - x^2y^2$, the “lemniscatic elliptic curve.”

2007 Edwards generalized to many curves $x^2 + y^2 = 1 + c^4x^2y^2$.
Theorem: have now obtained all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \blacksquare$; and gives new ECC speed records.

story

re many perspectives on
curve computations.

ublished 1987) Lenstra:
he elliptic-curve method
ring integers.

ublished 1985) Miller,
ependently
ublished 1987) Koblitz:
curve cryptography.

Goldwasser–Kilian,
vsky–Chudnovsky, Atkin:
curve primality proving.

The Edwards perspective is new!

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the “lemniscatic elliptic curve.”

2007 Edwards generalized to
many curves $x^2+y^2 = 1+c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \blacksquare$;
and gives new ECC speed records.

Represen

Crypto 1
elliptic c

Given n
division-
compute
“in 26 lo
but can

“It appe
represen
in the fo
Each po
triple (x
to the p

erspectives on
utations.

987) Lenstra:
curve method
ers.

985) Miller,
.

987) Koblitz:
tography.

er–Kilian,
lnovsky, Atkin:
ality proving.

The Edwards perspective is new!

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curve."

2007 Edwards generalized to
many curves $x^2 + y^2 = 1 + c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \blacksquare$;
and gives new ECC speed records.

Representing curve

Crypto 1985, Mille
elliptic curves in c

Given $n \in \mathbf{Z}$, $P \in$
division-polynomia
computes $nP \in E$
"in $26 \log_2 n$ mult
but can do better!

"It appears to be
represent the poin
in the following fo
Each point is repre
triple (x, y, z) whi
to the point $(x/z^2$

s on

tra:
hod

r,

itz:

tkin:
ng.

The Edwards perspective is new!

1761 Euler, 1866 Gauss introduced an addition law for $x^2 + y^2 = 1 - x^2y^2$, the "lemniscatic elliptic curve."

2007 Edwards generalized to many curves $x^2 + y^2 = 1 + c^4x^2y^2$. Theorem: have now obtained all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange: Edwards addition law is complete for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \blacksquare$; and gives new ECC speed records.

<u>Representing curve points</u>

Crypto 1985, Miller, "Use of elliptic curves in cryptograph

Given $n \in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$, division-polynomial recurrenc 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 in the following form: Each point is represented by triple (x, y, z) which corresp to the point $(x/z^2, y/z^3)$."

The Edwards perspective is new!

1761 Euler, 1866 Gauss introduced an addition law for $x^2 + y^2 = 1 - x^2y^2$, the "lemniscatic elliptic curve."

2007 Edwards generalized to many curves $x^2 + y^2 = 1 + c^4x^2y^2$. Theorem: have now obtained all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange: Edwards addition law is complete for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \blacksquare$; and gives new ECC speed records.

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 $(x/z^2, y/z^3)$."

wards perspective is new!

ler, 1866 Gauss
ed an addition law
$y^2 = 1 - x^2y^2$,
nniscatic elliptic curve.”

wards generalized to
urves $x^2+y^2 = 1+c^4x^2y^2$.
n: have now obtained
ic curves over $\overline{\mathbf{Q}}$.

rnstein–Lange:
addition law is complete
$y^2 = 1 + dx^2y^2$ if $d \neq \blacksquare$;
es new ECC speed records.

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 $(x/z^2, y/z^3)$.”

1986 Ch
“Sequen
generate
in forma
and new
and fact

“The cru
the choi
of an alg
where co
are the l

Most im
ADD is
DBL is

pective is new!

Gauss

ition law

x^2y^2,

lliptic curve."

eralized to

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

ow obtained

over $\overline{\mathbf{Q}}$.

ange:

law is complete

dx^2y^2 if $d \neq \blacksquare$;

C speed records.

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 $(x/z^2, y/z^3)$."

1986 Chudnovsky-

"Sequences of nur

generated by addit

in formal groups

and new primality

and factorization t

"The crucial probl

the choice of the r

of an algebraic gro

where computation

are the least time

Most important co

ADD is $P, Q \mapsto P$

DBL is $P \mapsto 2P$.

new!

ve.”

o

$^4x^2y^2$.

d

nplete

$d \neq \blacksquare$;

ecords.

<u>Representing curve points</u>

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 $(x/z^2, y/z^3)$.”

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

“The crucial problem becom
the choice of the model
of an algebraic group variety
where computations mod p
are the least time consumin

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

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 $(x/z^2, y/z^3)$."

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 $P \mapsto 2P$.

nting curve points

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

$\in \mathbf{Z}$, $P \in E(\mathbf{F}_q)$,
polynomial recurrence
es $nP \in E(\mathbf{F}_q)$
$\mathrm{g}_2\, n$ multiplications";
do better!

ars to be best to
t the points on the curve
ollowing form:
int is represented by the
$, y, z)$ which corresponds
oint $(x/z^2, y/z^3)$."

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:

e points

er, "Use of
ryptography":

$E(\mathbf{F}_q)$,
l recurrence
$(\mathbf{F}_q)$
iplications";

best to
ts on the curve
rm:
esented by the
ch corresponds
$^2, y/z^3)$."

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 c
lying in low-dimen
for otherwise the n
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: $x^3 + y^3 +$

f
ny":
ce
";
curve
the
onds

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

Optimizi

For "tra
on $y^2 =$
1986 Ch
state exp
10**M** for

Consequ
$\approx \Big(10\,\mathrm{lg}$

to comp
using sli
of scalar

Notation

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

Optimizing Jacobi

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

Consequence:
$\approx \left(10 \lg n + 16 \frac{\text{l}}{\text{lg}}\right.$
to compute n, $P \mapsto$
using sliding-windo
of scalar multiplica

Notation: lg = log

sky,

nes

y,

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

<u>Optimizing Jacobian coordin</u>

For “traditional” $(X/Z^2, Y/$
on $y^2 = x^3 + ax + b$:
1986 Chudnovsky–Chudnovs
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 metho
of scalar multiplication.

Notation: $\lg = \log_2$.

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

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: $\lg = \log_2$.

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.”

Veierstrass:
$+ ax + b$.

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

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

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

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

Here are
$S = 4$
$M = 3$
$T = M$
$X_3 =$
$Y_3 =$
$Z_3 =$

Total co
S is the
D is the

The squ
$X_1^2, Y_1^2,$

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

n:

$- d^2 = 1.$

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

$+ 1 = 3dxy.$

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

Here are the DBL

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

$M = 3X_1^2 + aZ$

$T = M^2 - 2S;$

$X_3 = T;$

$Y_3 = M \cdot (S - T$

$Z_3 = 2Y_1 \cdot Z_1.$

Total cost 3**M** + 6

S is the cost of sq

D is the cost of m

The squarings pro

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

ces,

s

. to

rves."

x^2+1.

y.

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

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

ing Jacobian coordinates

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

$x^3 + ax + b$:

udnovsky–Chudnovsky

plicit formulas using

DBL; 16**M** for ADD.

uence:

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

ute $n, P \mapsto nP$

ding-windows method

multiplication.

n: $\lg = \log_2$.

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 EC

curves th

Curve-ch

1986 Ch

Can elim

by choos

But "it i

to choos

If $a = -$

$= 3(X_1$

Replace

Now DB

an coordinates

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

$+ b$:

-Chudnovsky

ulas using

M for ADD.

$\text{g}\, n$

$\lg n \Big)$ **M**

$\to nP$

ows method

ation.

$_2$.

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 standar

curves that make

Curve-choice advic

1986 Chudnovsky-

Can eliminate the

by choosing curve

But "it is even sm

to choose curve w

If $a = -3$ then M

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

Replace 2**S** with 1

Now DBL costs 4

nates

$Z^3)$

sky

D.

od

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 fa

Curve-choice advice from 1986 Chudnovsky–Chudnovs

Can eliminate the $1\mathbf{D}$ 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 $2\mathbf{S}$ with $1\mathbf{M}$.

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 $1\mathbf{D}$ 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 $4\mathbf{M} + 4\mathbf{S}$.

g is faster than **M**.

e the DBL formulas:

$X_1 \cdot Y_1^2$;

$3X_1^2 + aZ_1^4$;

$M^2 - 2S$;

T;

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

$2Y_1 \cdot Z_1$.

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

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

cost of multiplying by a.

arings 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 Be

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

$11\mathbf{M} + 5$

How? E

instead c

compute

DBL for

computi

Same ide

but have

to elimin

than **M**.

formulas:

$_1^4$;

$T) - 8Y_1^4$;

$6\mathbf{S} + 1\mathbf{D}$ where

uaring in $\mathbf{F}_q$,

ultiplying by a.

duce

^{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 DBL

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

How? Easy $\mathbf{S} - \mathbf{M}$

instead of comput

compute $(Y_1 + Z_1$

DBL formulas wer

computing Y_1^2 and

Same idea for the

but have to scale

to eliminate divisio

where

$\mathbf{F}_q$,

by a.

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 DBL.
$11\mathbf{M} + 5\mathbf{S}$ for ADD.

How? Easy $\mathbf{S} - \mathbf{M}$ tradeoff:
instead of computing $2Y_1 \cdot Z$
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 form
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.

CC standards choose
hat make formulas faster.

hoice advice from
udnovsky–Chudnovsky:

ninate the 1**D**
sing curve with $a = 1$.

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

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

BL costs 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
$U_1 = X_1$
$S_1 = Y_1$
many m

1986 Ch
"We sug
addition
$(X, Y, Z,$

Disadva
Allocate
Pay 1**S**

Advanta
Save 2**S**
Save 1**S**

rds choose
formulas faster.

ce from
-Chudnovsky:

$1\mathbf{D}$
with $a = 1$.

arter"
ith $a = -3$.

$= 3(X_1^2 - Z_1^4)$
$X_1 + Z_1^2)$.
$\mathbf{M}$.

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

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 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 compu

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

Disadvantages:
Allocate space for
Pay $1\mathbf{S} + 1\mathbf{M}$ in A

Advantages:
Save $2\mathbf{S} + 2\mathbf{M}$ at
Save $1\mathbf{S}$ at start o

aster.

sky:

1.

3.

$- Z_1^4)$

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

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

Disadvantages:
Allocate space for Z^2, Z^3.
Pay 1**S**+1**M** in ADD and ir

Advantages:
Save 2**S** + 2**M** at start of A
Save 1**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.

rnstein:

S for DBL.

5S for ADD.

asy $\mathbf{S} - \mathbf{M}$ tradeoff:

of computing $2Y_1 \cdot Z_1$,

e $(Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$.

mulas were already

ng Y_1^2 and Z_1^2.

ea for the ADD formulas,

e to scale X, Y, Z

nate 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 Co

Store po

If point

also cacl

No cost,

If point

reuse Z^2

Best Jac

including

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

$11\mathbf{M} + 5$

$10\mathbf{M} + 4$

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

.

D.

M tradeoff:

ing $2Y_1 \cdot Z_1$,

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

e already

Z_1^2.

ADD formulas,

X, Y, Z

ons 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–Miya

Store point as $(X$

If point is input to

also cache Z^2 and

No cost, aside fro

If point is input to

reuse Z^2, Z^3. Sav

Best Jacobian spe

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

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

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

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

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

Z_1,

Z_1^2.

nulas,

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 A
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

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. $Z_2 = 1$).

r $y^2 = x^3 + ax + b$:
$_1 Z_2^2$, $U_2 = X_2 Z_1^2$,
Z_2^3, $S_2 = Y_2 Z_1^3$,
ore computations.

udnovsky–Chudnovsky:
ggest to write
formulas involving
, Z^2, Z^3)."

ntages:
space for Z^2, Z^3.
$+ 1$**M** in ADD and in DBL.

ges:
$+ 2$**M** at start of ADD.
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. $Z_2 = 1$).

Compare
curves x
in projec
(2007 B
$3\mathbf{M} + 4\mathbf{S}$
$10\mathbf{M} + 1$
$9\mathbf{M} + 1\mathbf{S}$

Inverted
(2007 B
$3\mathbf{M} + 4\mathbf{S}$
$9\mathbf{M} + 1\mathbf{S}$
$8\mathbf{M} + 1\mathbf{S}$

Even be
extended
(2008 Hi

$+ ax + b$:

$X_2 Z_1^2$,

$Y_2 Z_1^3$,

utations.

-Chudnovsky:

rite

involving

Z^2, Z^3.

DD and in DBL.

start of ADD.

f 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 speed
curves $x^2 + y^2 =$
in projective coord
(2007 Bernstein–L
$3\mathbf{M} + 4\mathbf{S}$ for DBL
$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ f
$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ fo

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

Even better speed
extended/complet
(2008 Hisil–Wong–

sky:

n DBL.

DD.

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 Edwa
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 coordinate
(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.

Even better speeds from
extended/completed coordin
(2008 Hisil–Wong–Carter–Da

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.

Even better speeds from
extended/completed coordinates
(2008 Hisil–Wong–Carter–Dawson).

hen–Miyaji–Ono:

int as $(X : Y : Z)$.

is input to ADD,

he Z^2 and Z^3.

aside from space.

is input to another ADD,

$^2, Z^3$. Save $1\mathbf{S} + 1\mathbf{M}$!

cobian speeds today,

g $\mathbf{S} - \mathbf{M}$ tradeoffs:

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

$5\mathbf{S}$ for ADD.

$4\mathbf{S}$ for reADD.

$\mathbf{S}$ 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.

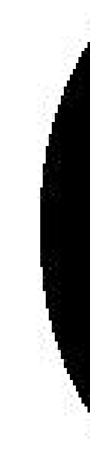
Inverted Edwards coordinates (2007 Bernstein–Lange):

$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.

$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.

$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Even better speeds from extended/completed coordinates (2008 Hisil–Wong–Carter–Dawson).



$y^2 = x^3$

ji–Ono:

$: Y : Z)$.

ADD,

Z^3.

m space.

another ADD,

e $1\mathbf{S} + 1\mathbf{M}$!

eds today,

radeoffs:

if $a = -3$.

D.

DD.

D (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.

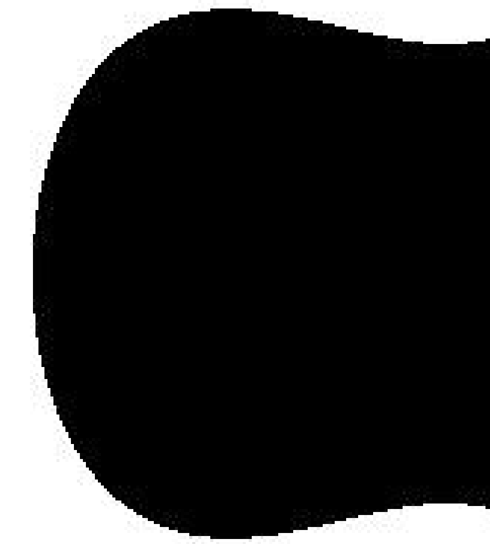
Inverted Edwards coordinates (2007 Bernstein–Lange):

$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.

$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.

$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Even better speeds from extended/completed coordinates (2008 Hisil–Wong–Carter–Dawson).



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

ADD,

M!

3.

$_2 = 1$).

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.

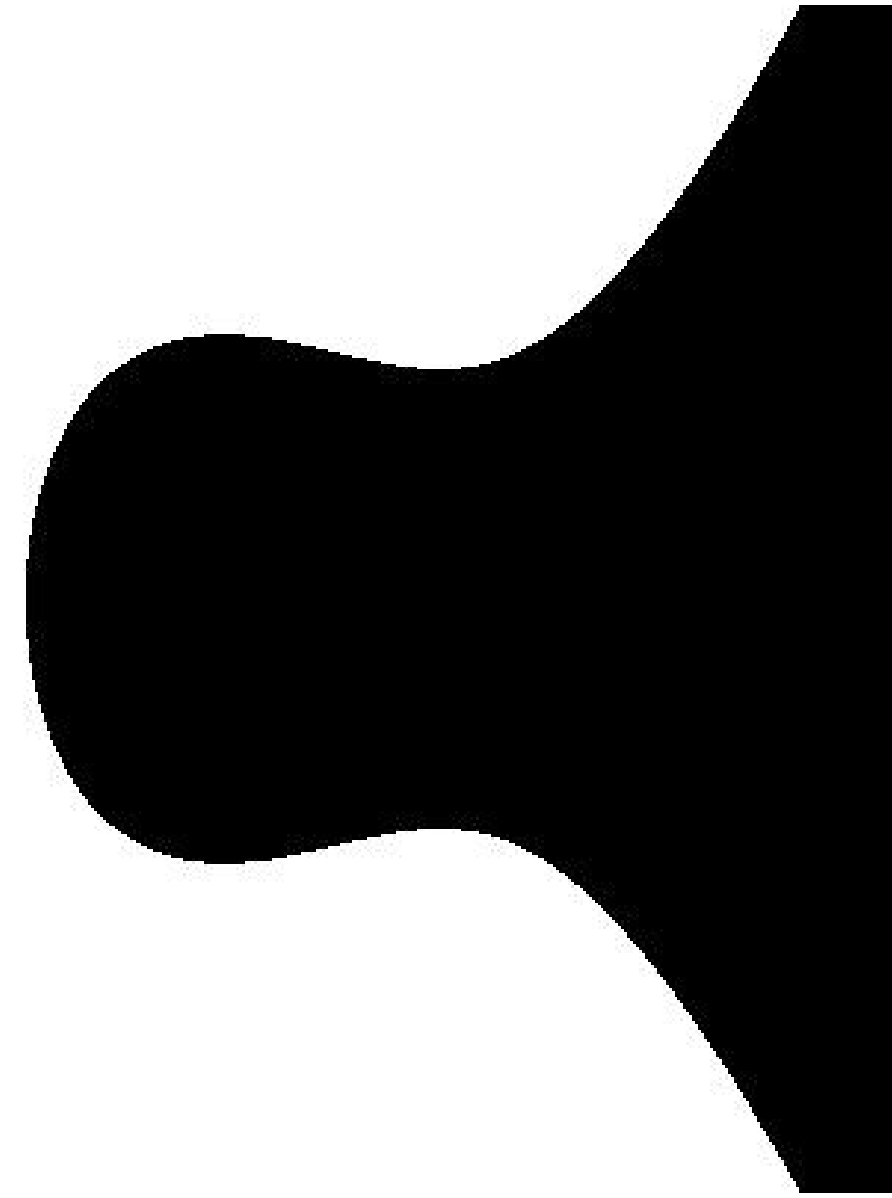
Inverted Edwards coordinates (2007 Bernstein–Lange):

$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ for DBL.

$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for ADD.

$8\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ for mADD.

Even better speeds from extended/completed coordinates (2008 Hisil–Wong–Carter–Dawson).



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

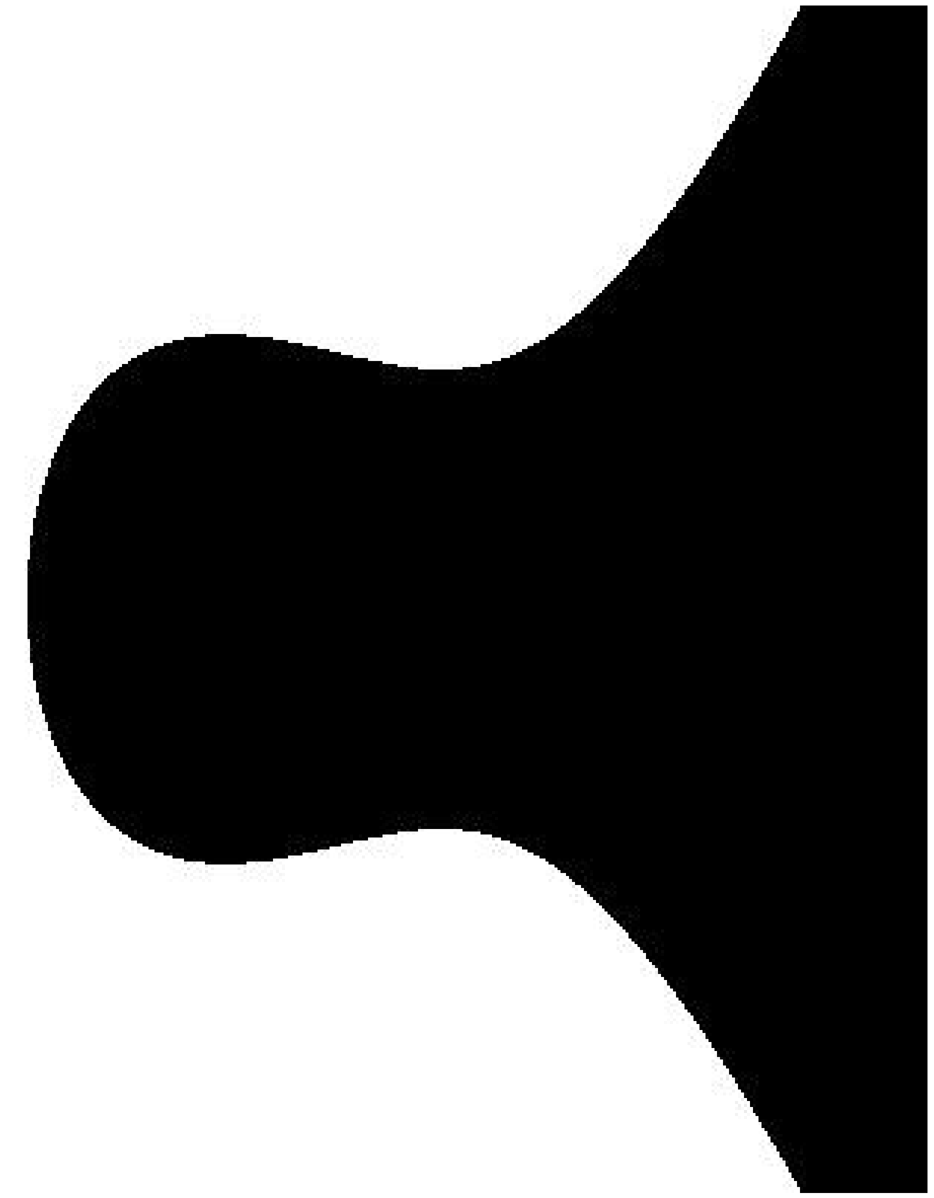
Compare to speeds for Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ in projective coordinates (2007 Bernstein–Lange):

$3\mathbf{M} + 4\mathbf{S}$ 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.

Even better speeds from extended/completed coordinates (2008 Hisil–Wong–Carter–Dawson).



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

e to speeds for Edwards

$^2 + y^2 = 1 + dx^2y^2$

ctive coordinates

ernstein–Lange):

S for DBL.

1**S** + 1**D** for ADD.

S + 1**D** for mADD.

Edwards coordinates

ernstein–Lange):

S + 1**D** for DBL.

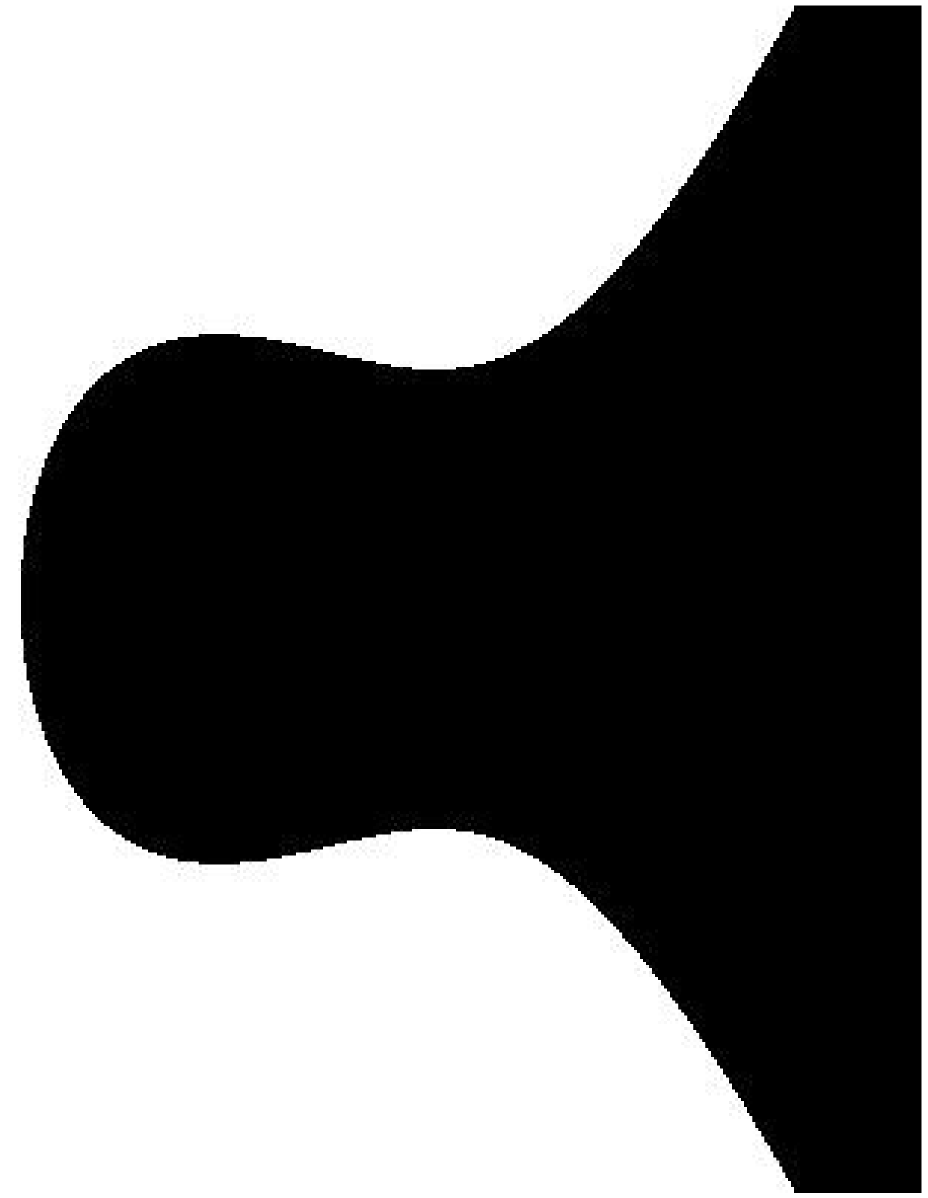
S + 1**D** for ADD.

S + 1**D** for mADD.

tter speeds from

d/completed coordinates

sil–Wong–Carter–Dawson).



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

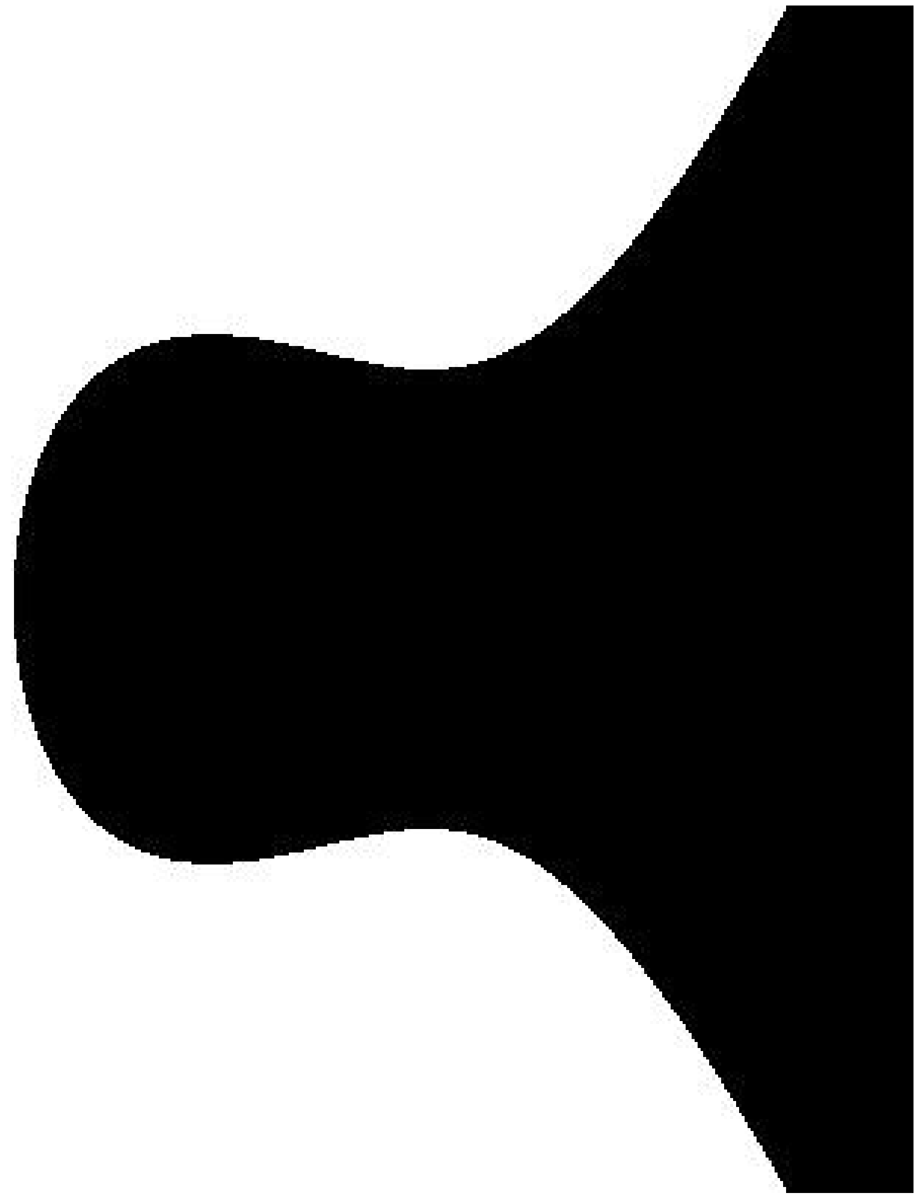
The We

turtle: o

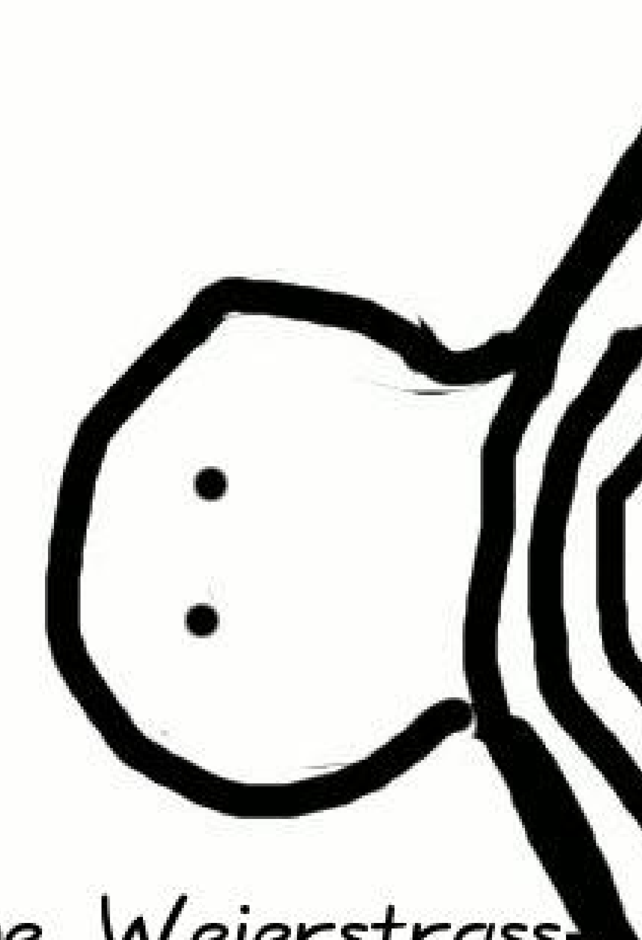
and slow

(picture)

s for Edwards
$1 + dx^2y^2$
linates
ange):
.
or ADD.
r mADD.
coordinates
ange):
r DBL.
r ADD.
r mADD.
s from
ed coordinates
-Carter–Dawson).



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



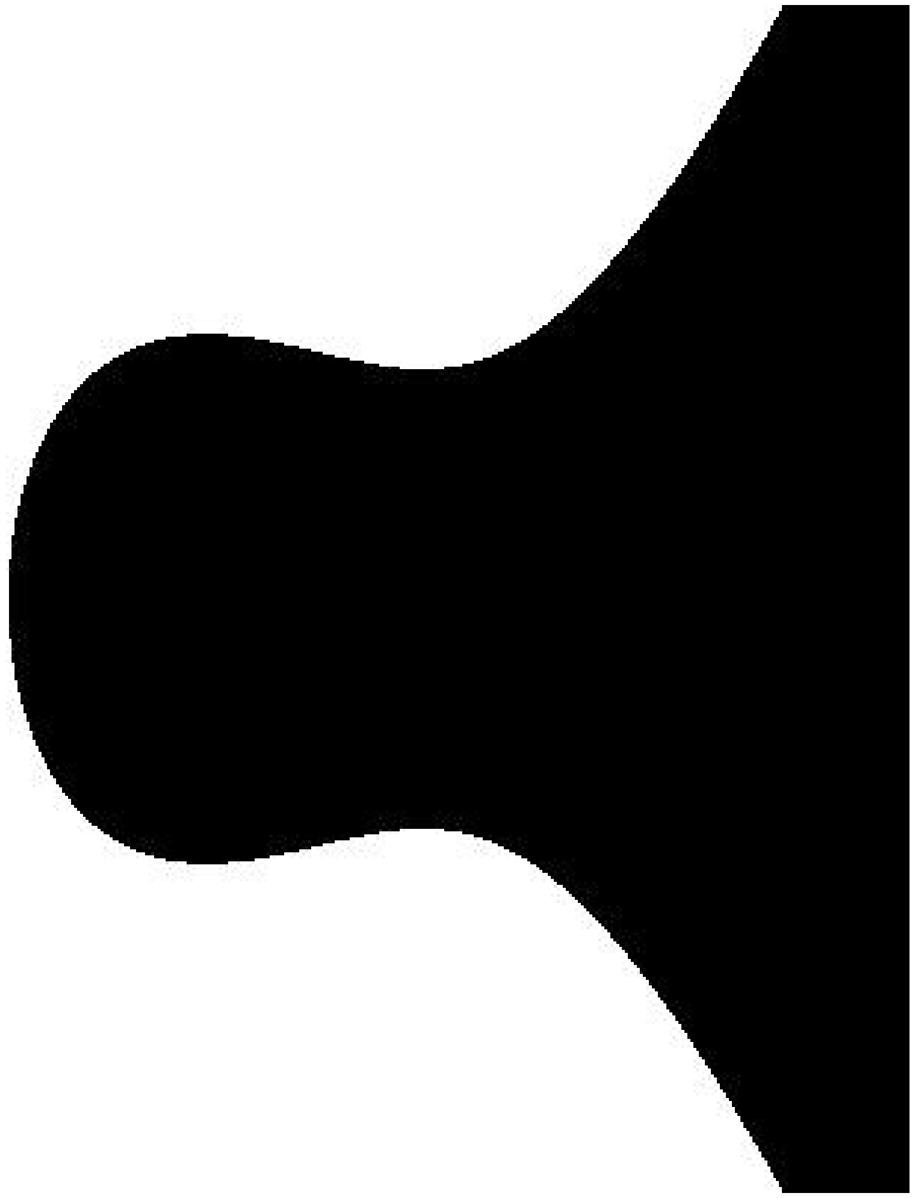
The Weierstrass-
turtle: old, trusted
and slow. Warning
(picture) incomplet

ards

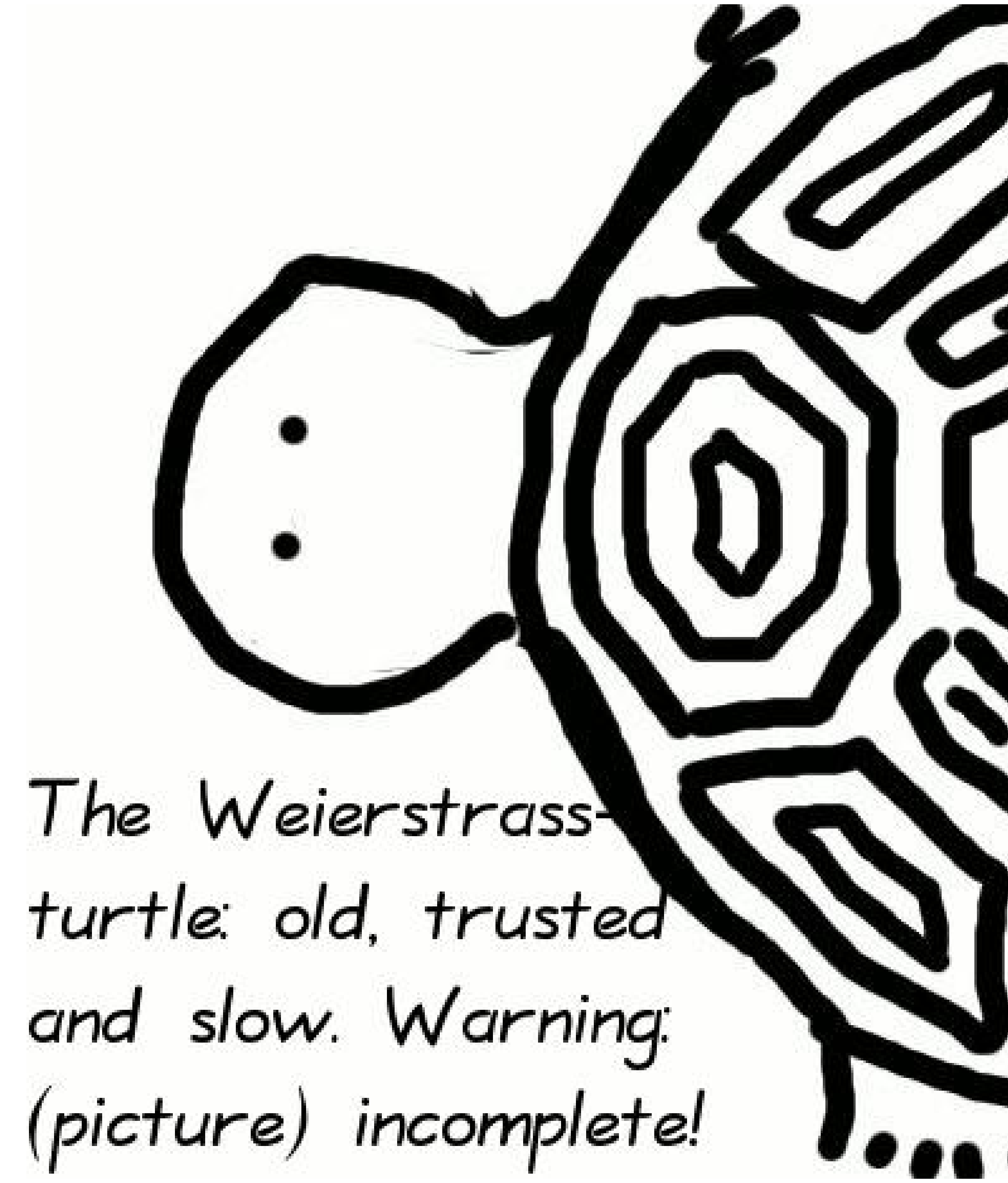
es

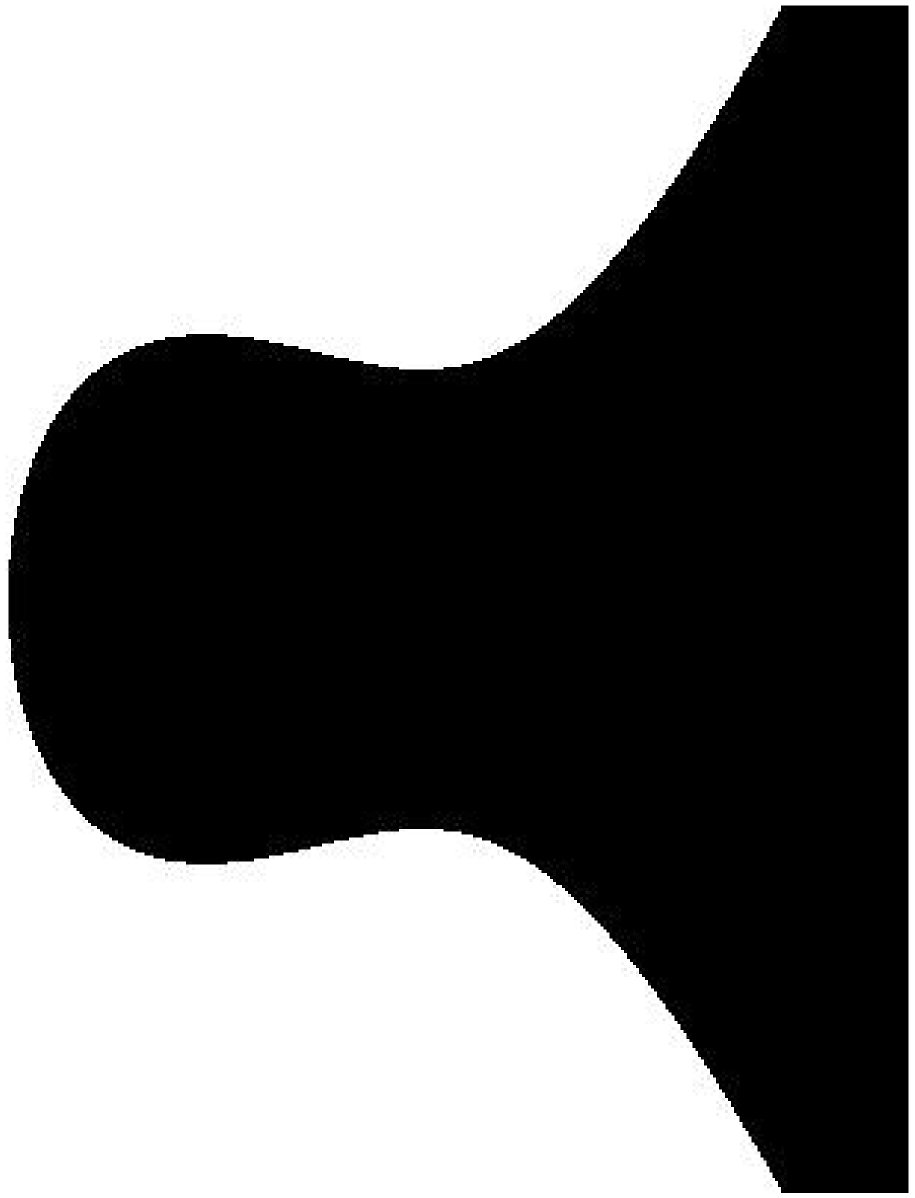
nates

awson).

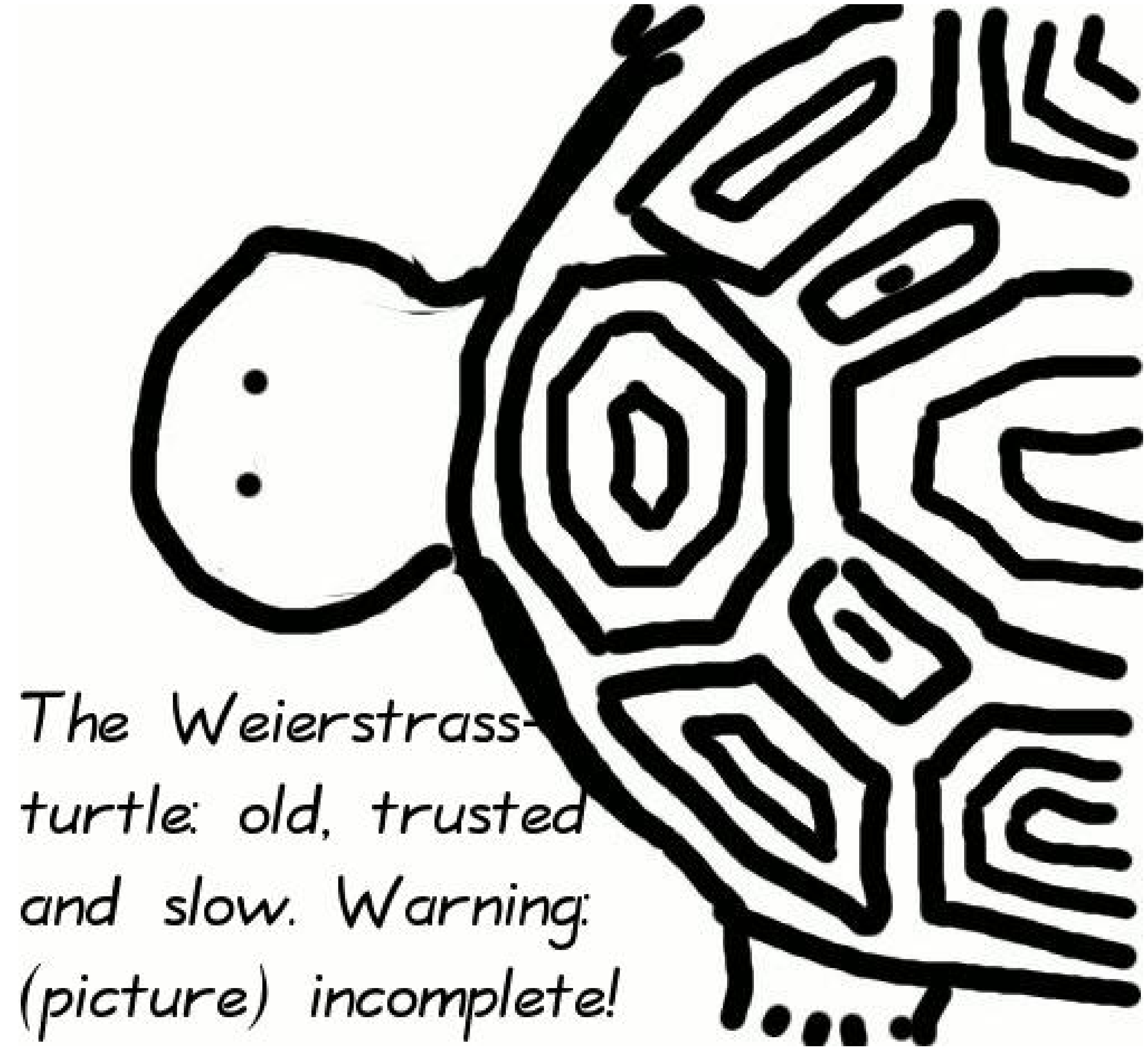


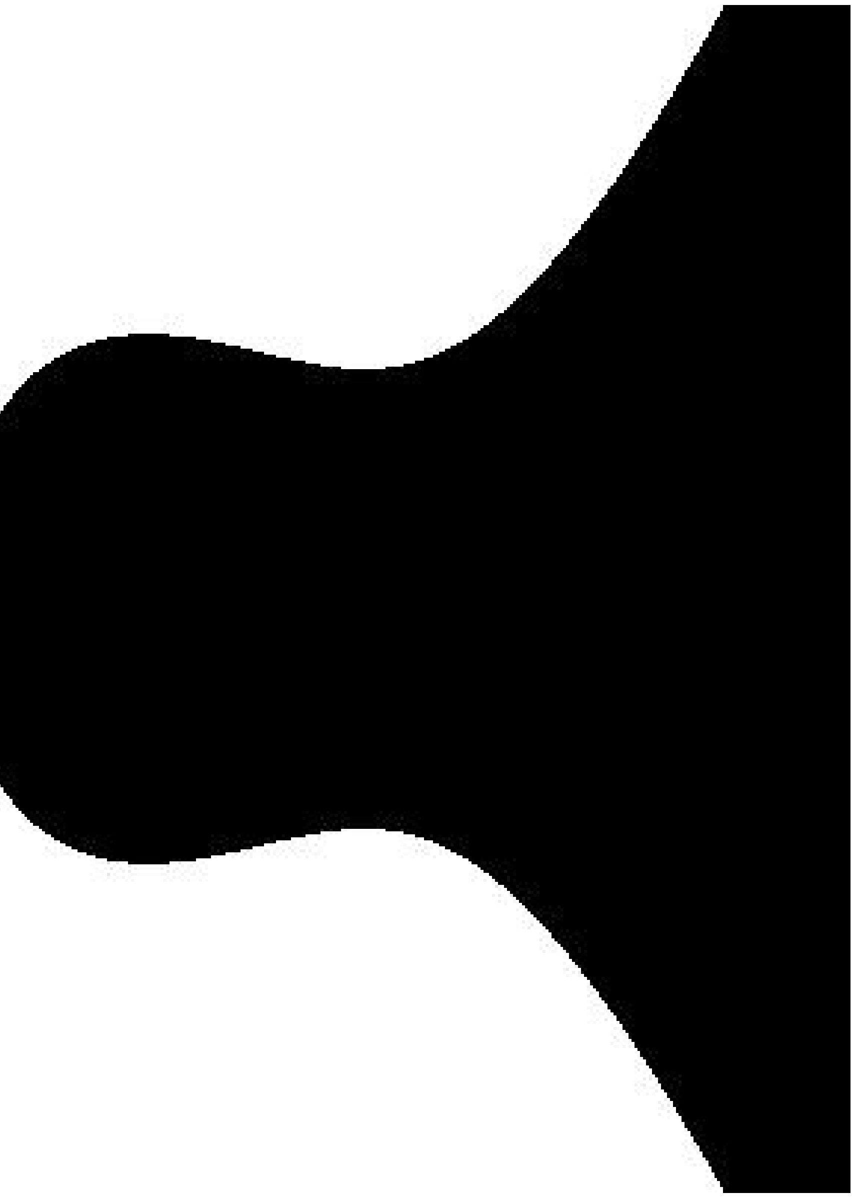
$y^2 = x^3 - 0.4x + 0.7$



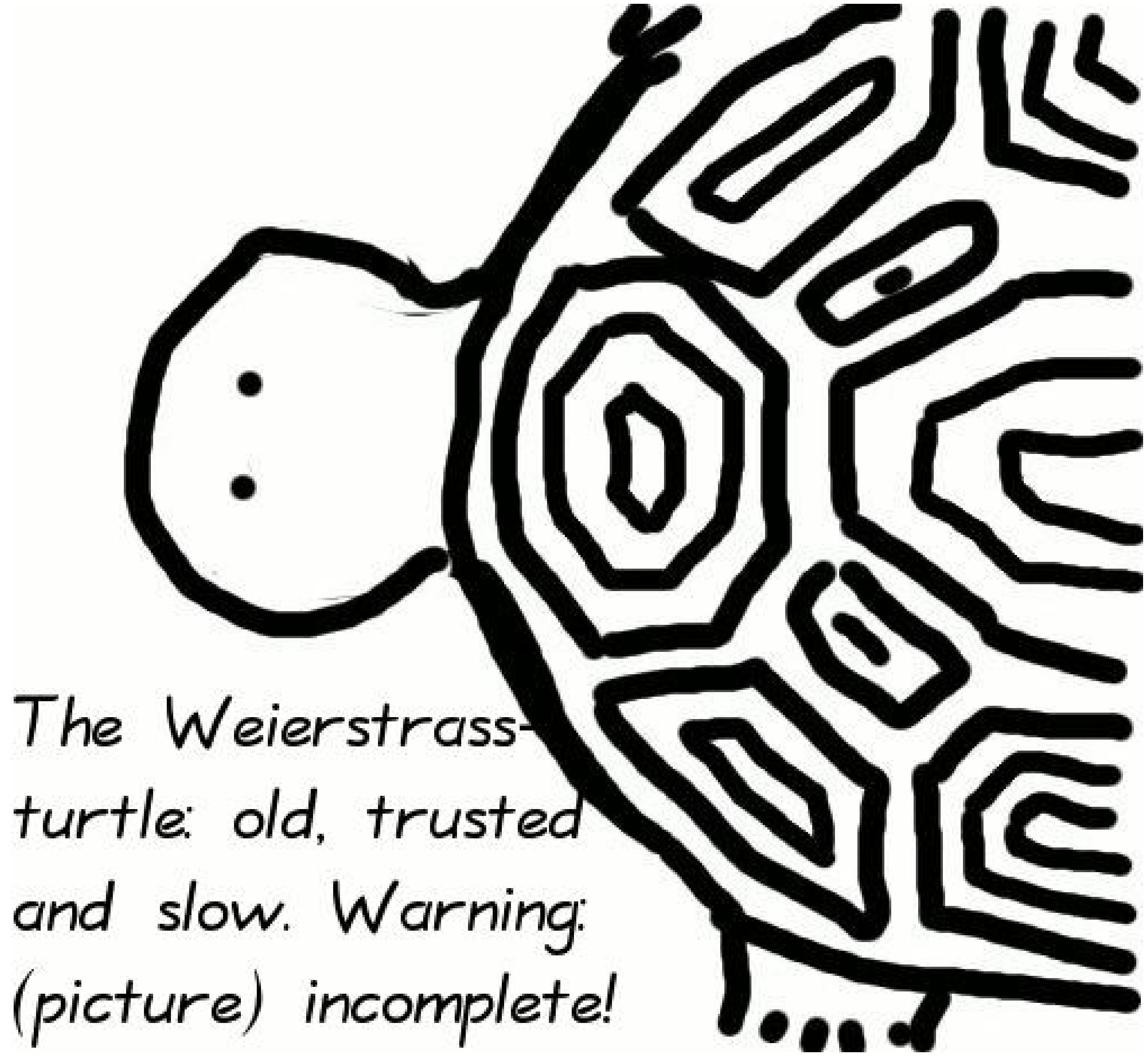


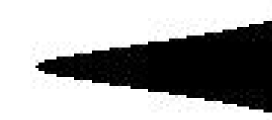
$$y^2 = x^3 - 0.4x + 0.7$$


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

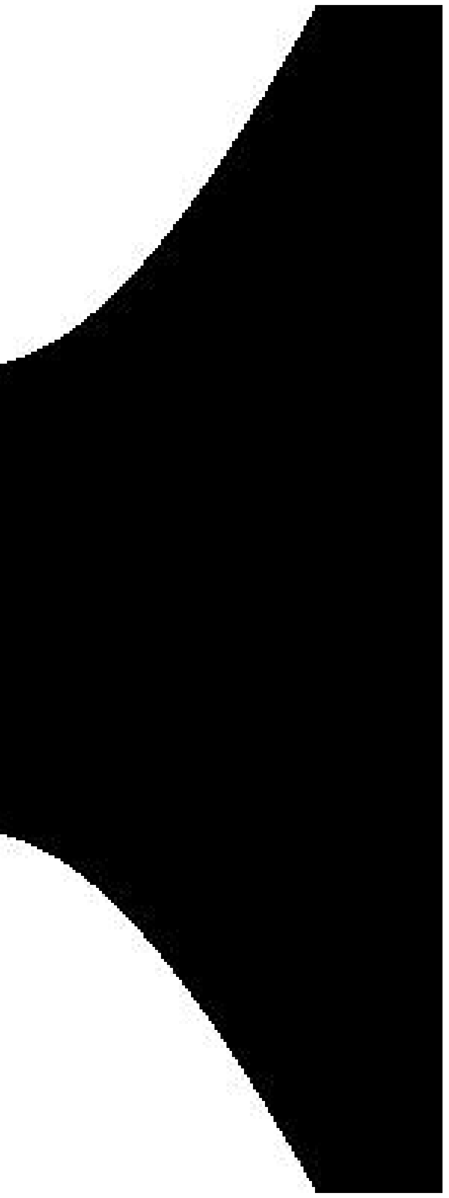


$- 0.4x + 0.7$

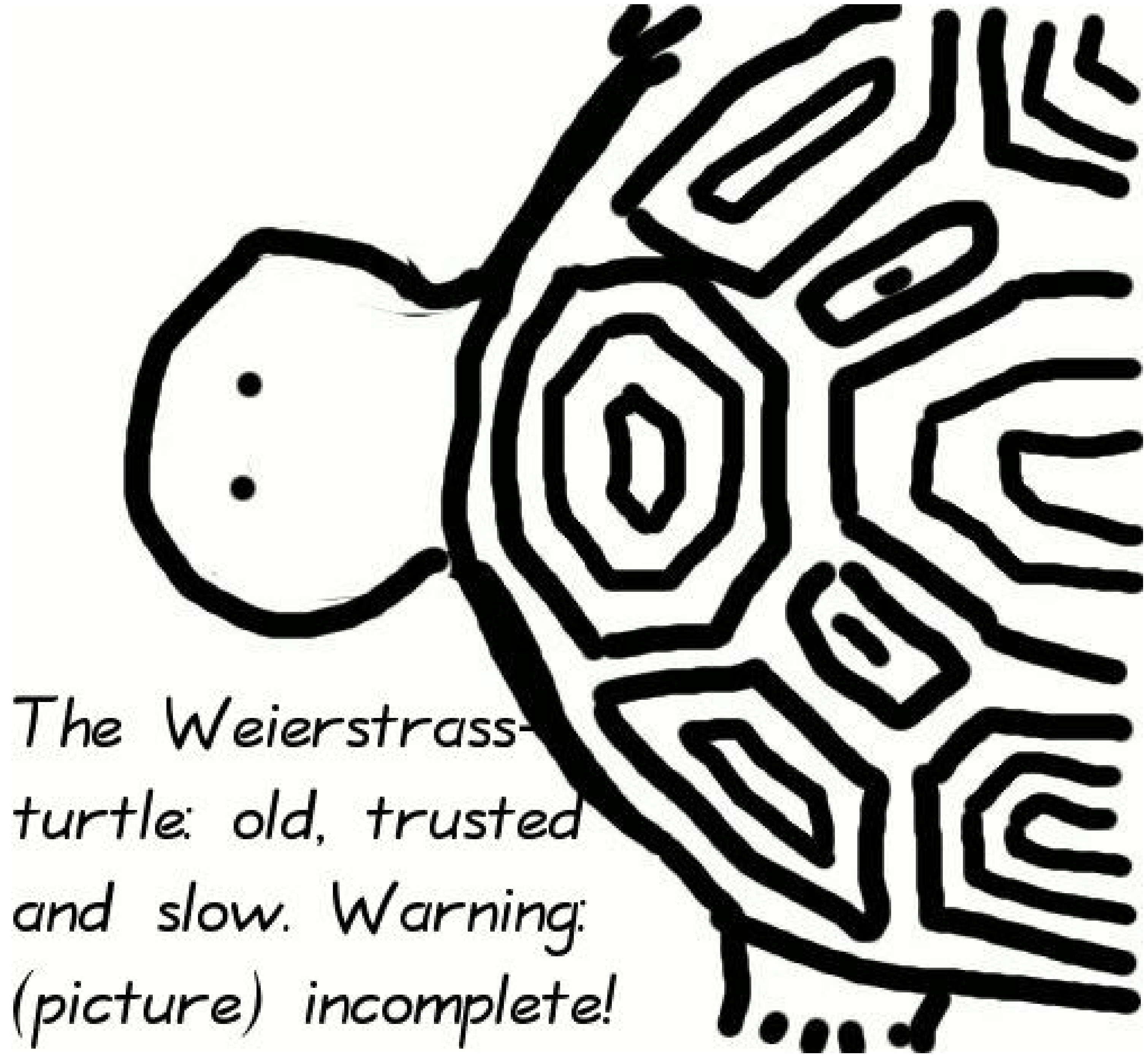

The Weierstrass-
turtle: old, trusted
and slow. Warning:
(picture) incomplete!

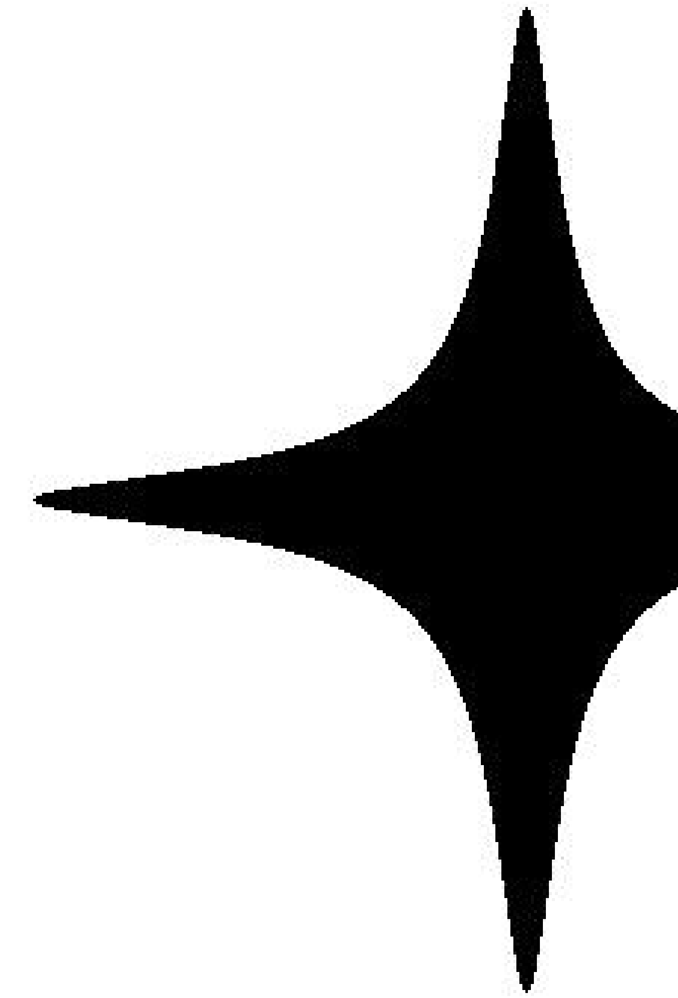


$x^2 + y^2$

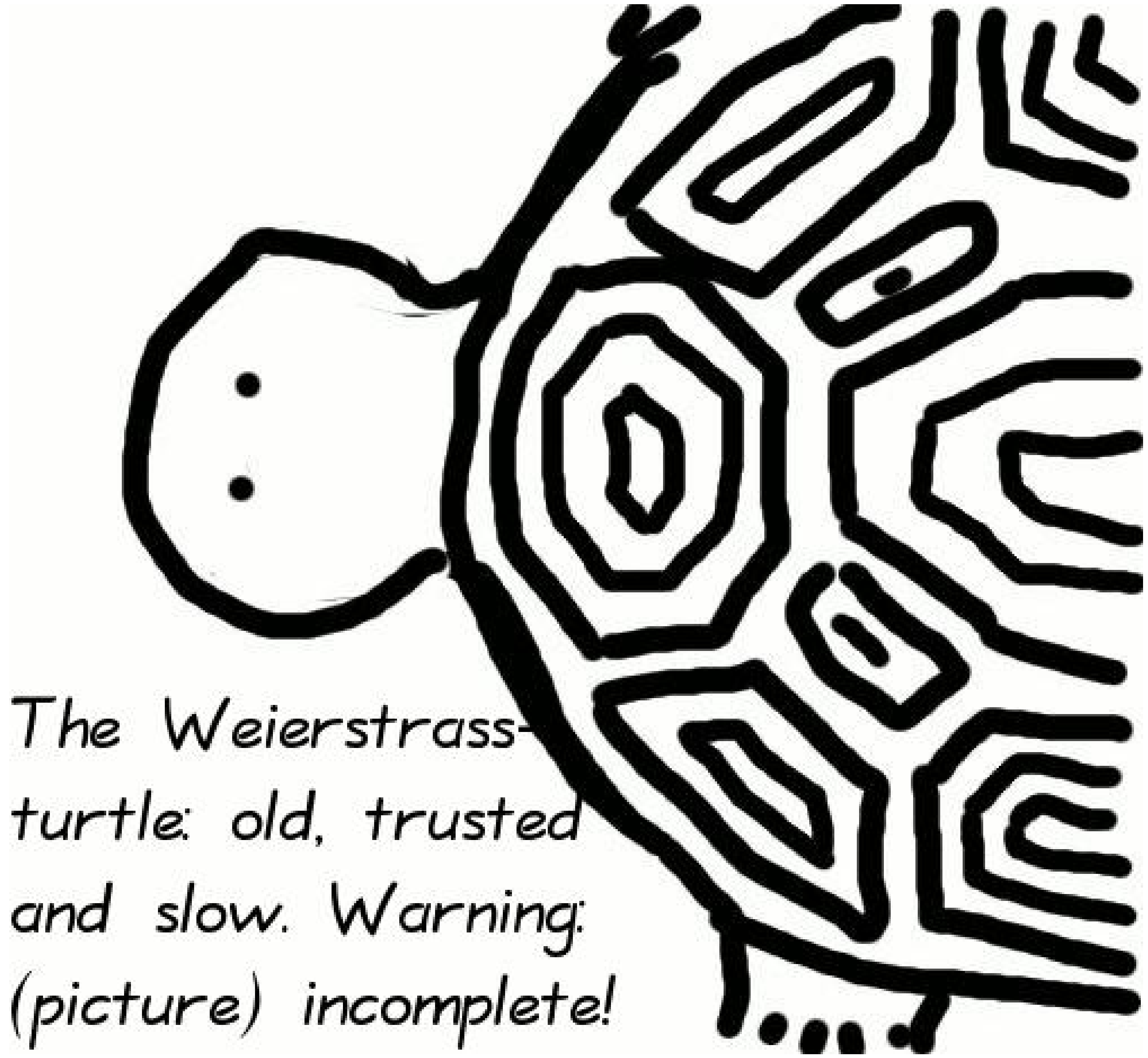


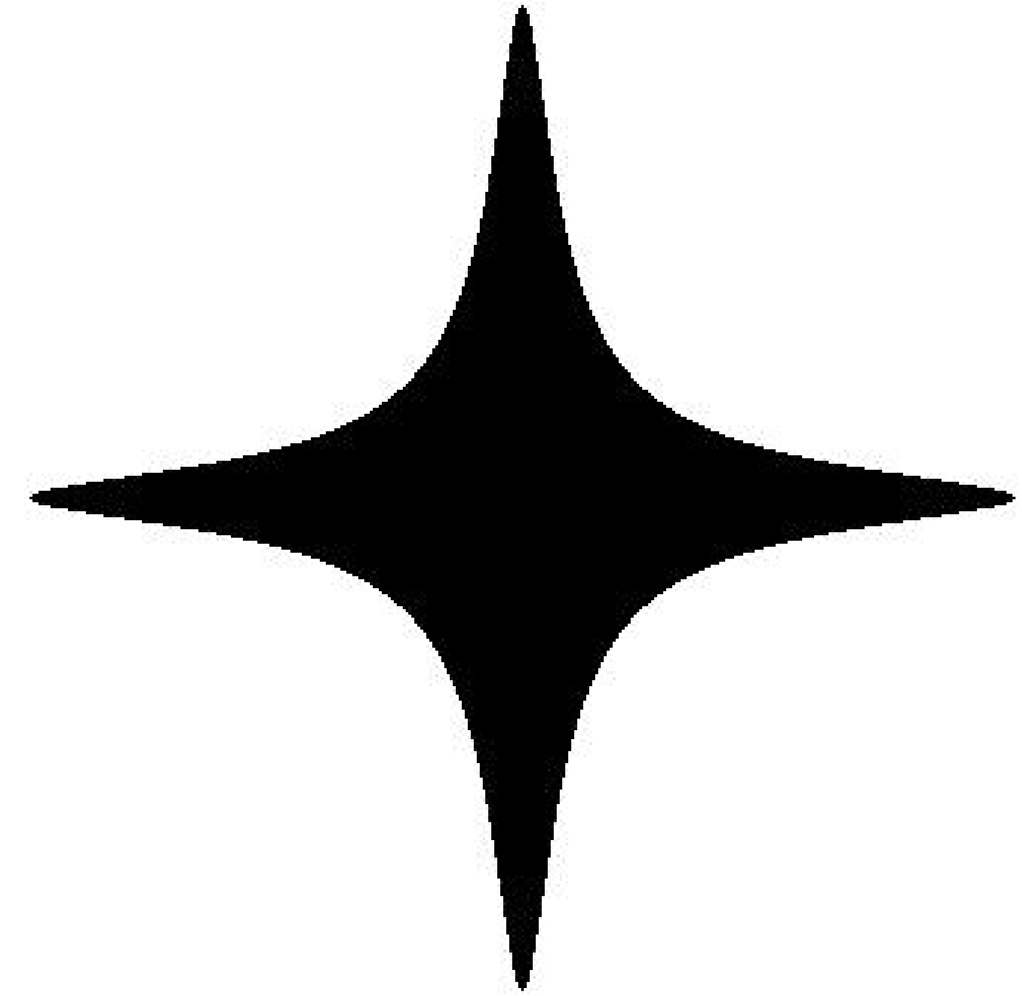
0.7


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

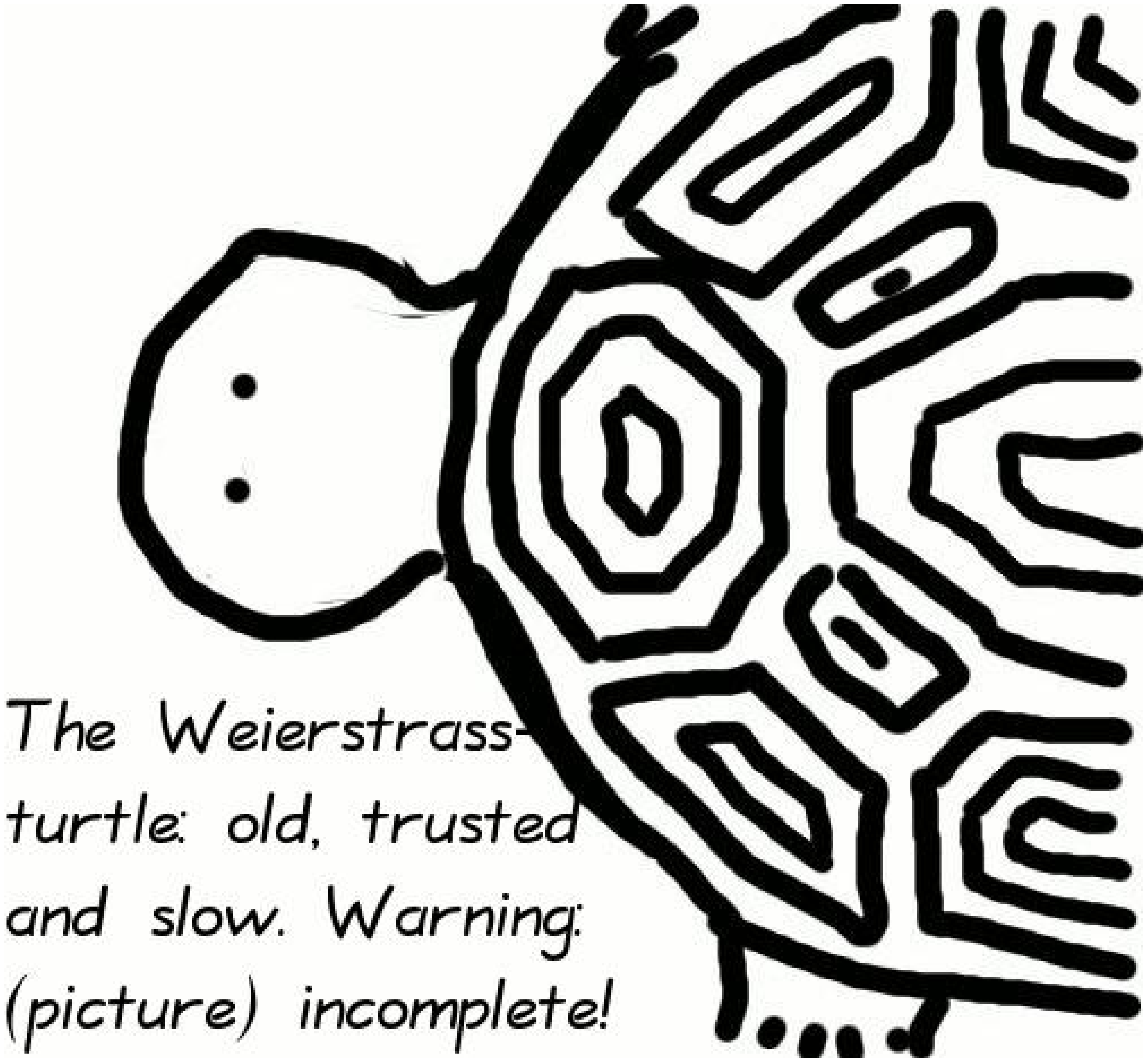


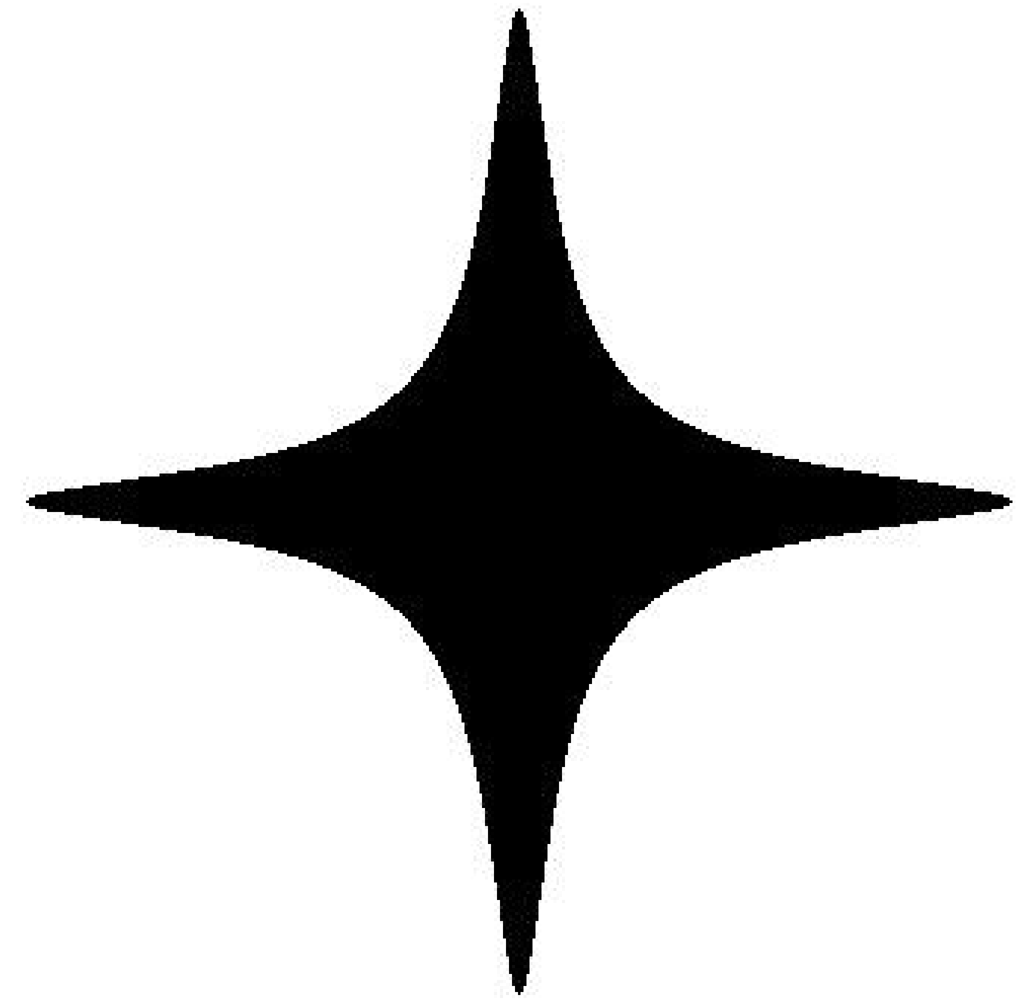
$x^2 + y^2 = 1 - 300$



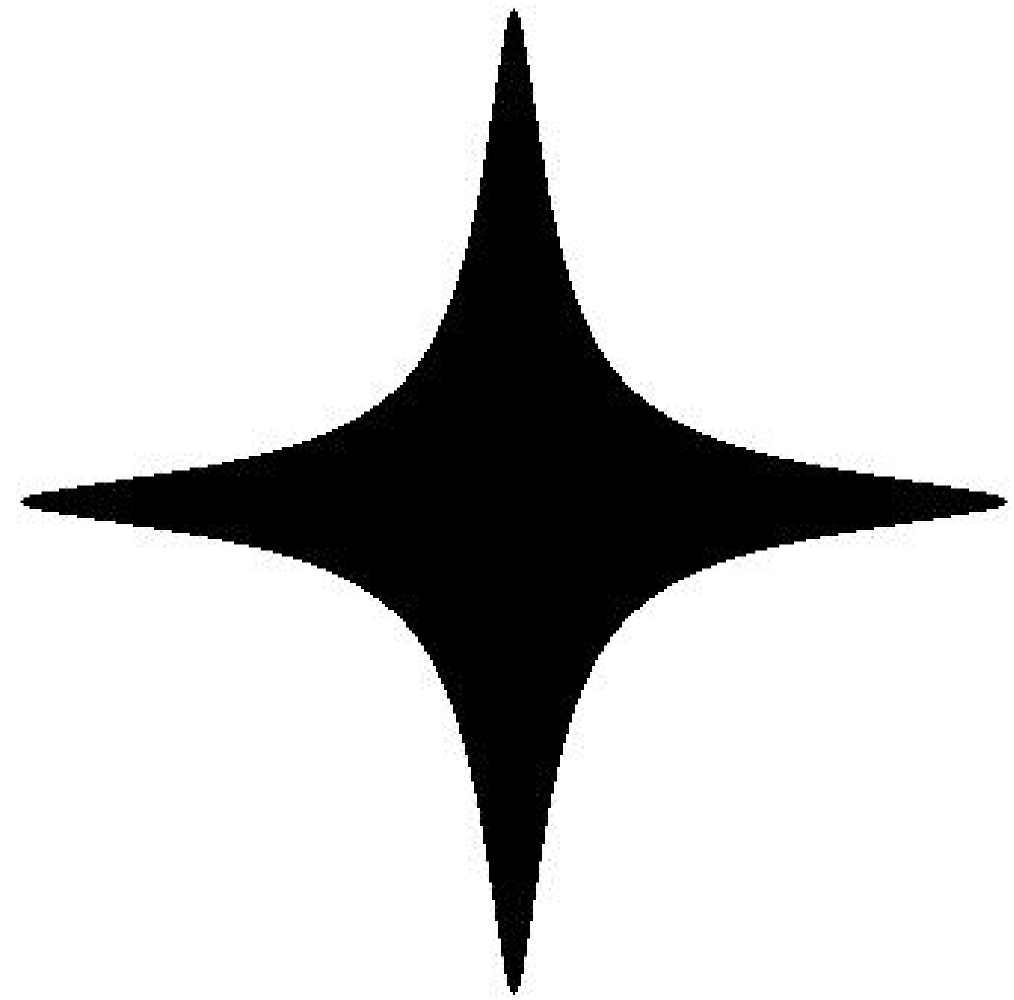


$$x^2 + y^2 = 1 - 300x^2y^2$$

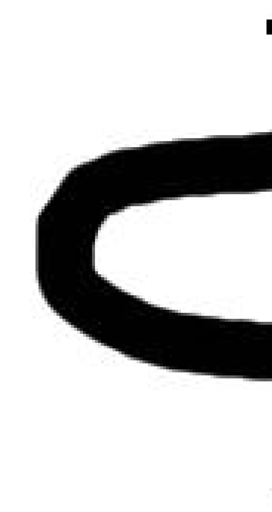




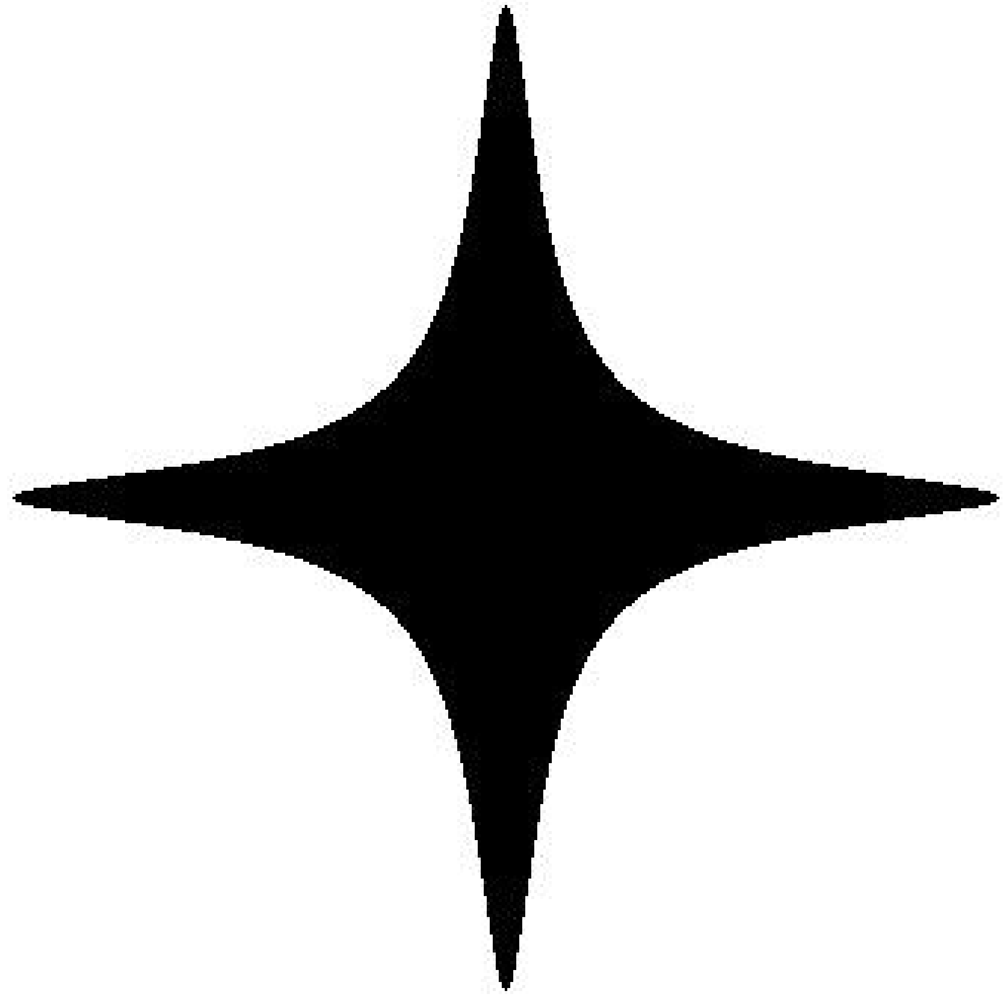
$$x^2 + y^2 = 1 - 300x^2y^2$$



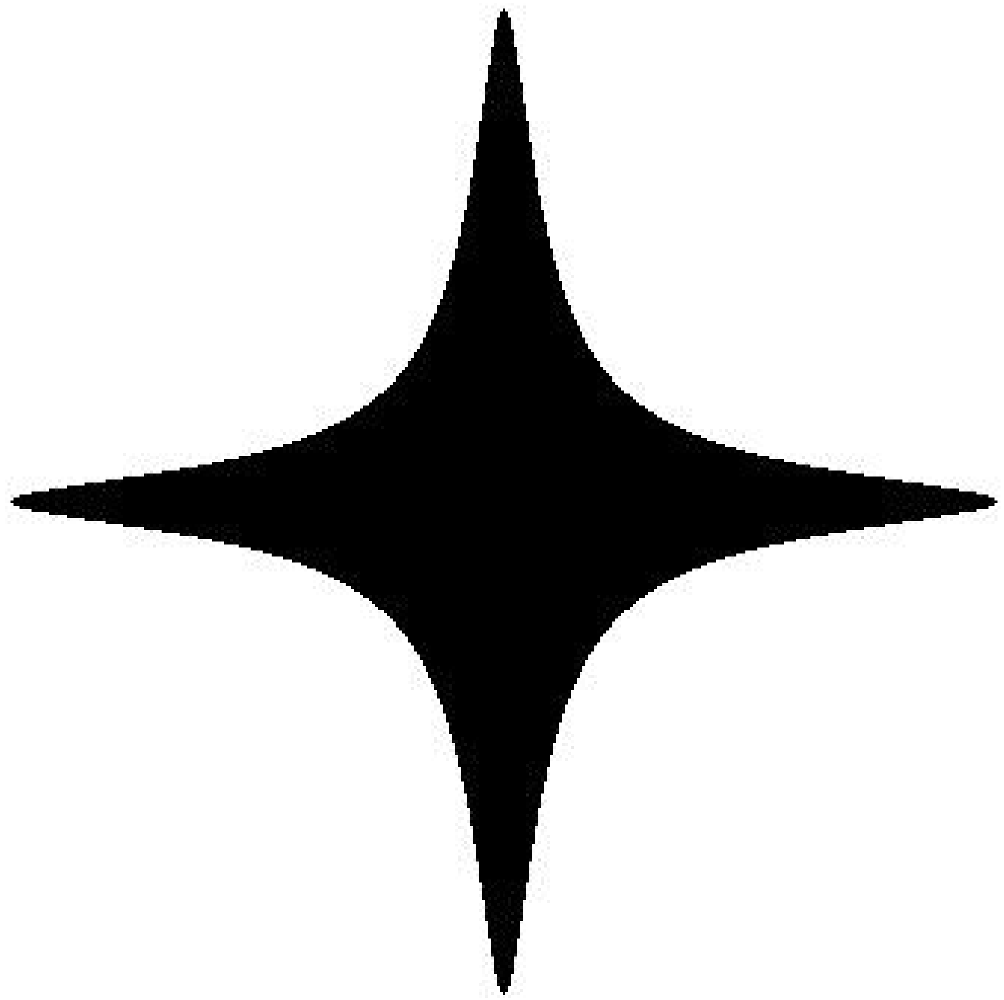
$$x^2 + y^2 = 1 - 300x^2y^2$$



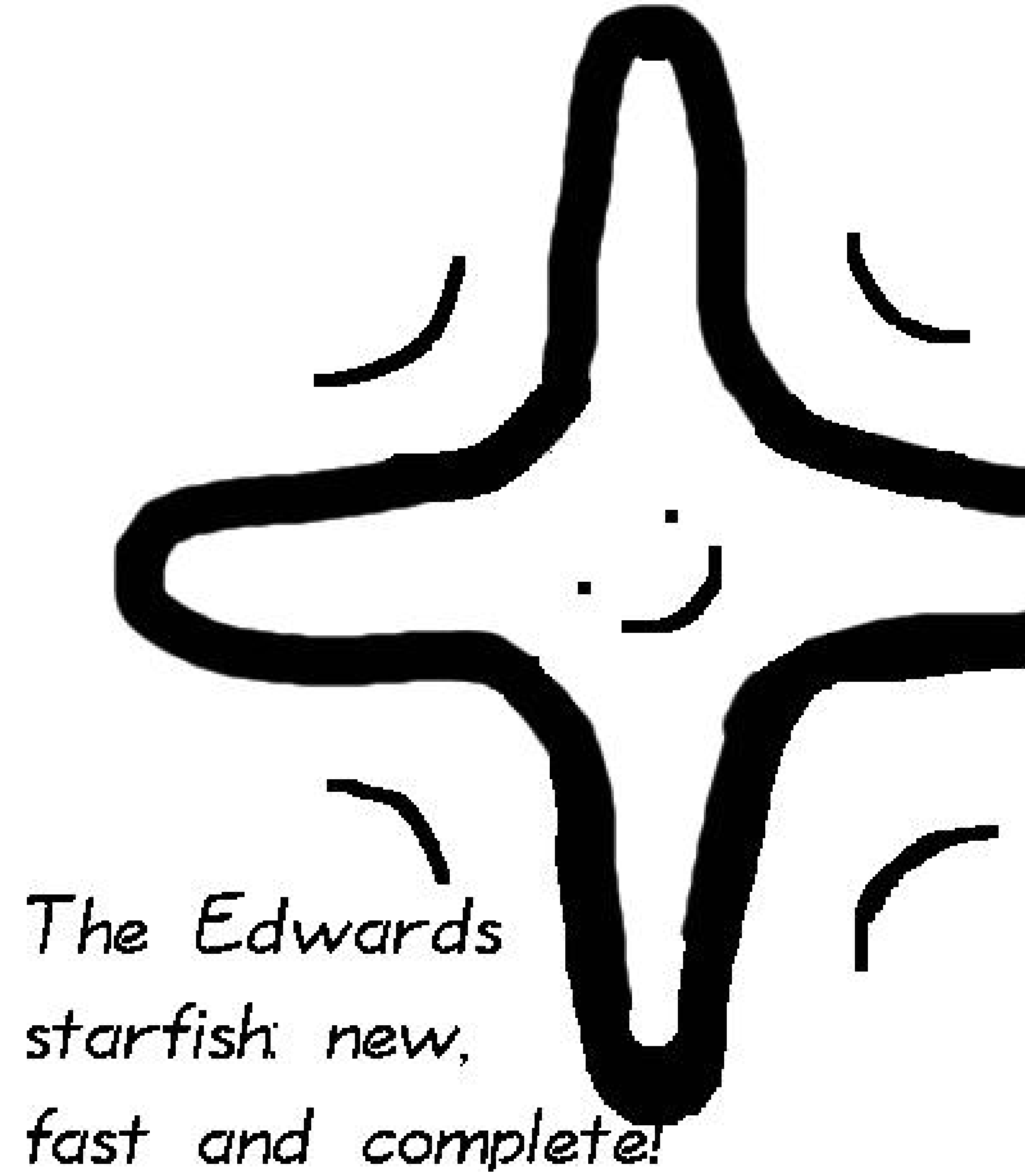
The Edv
starfish:
fast and

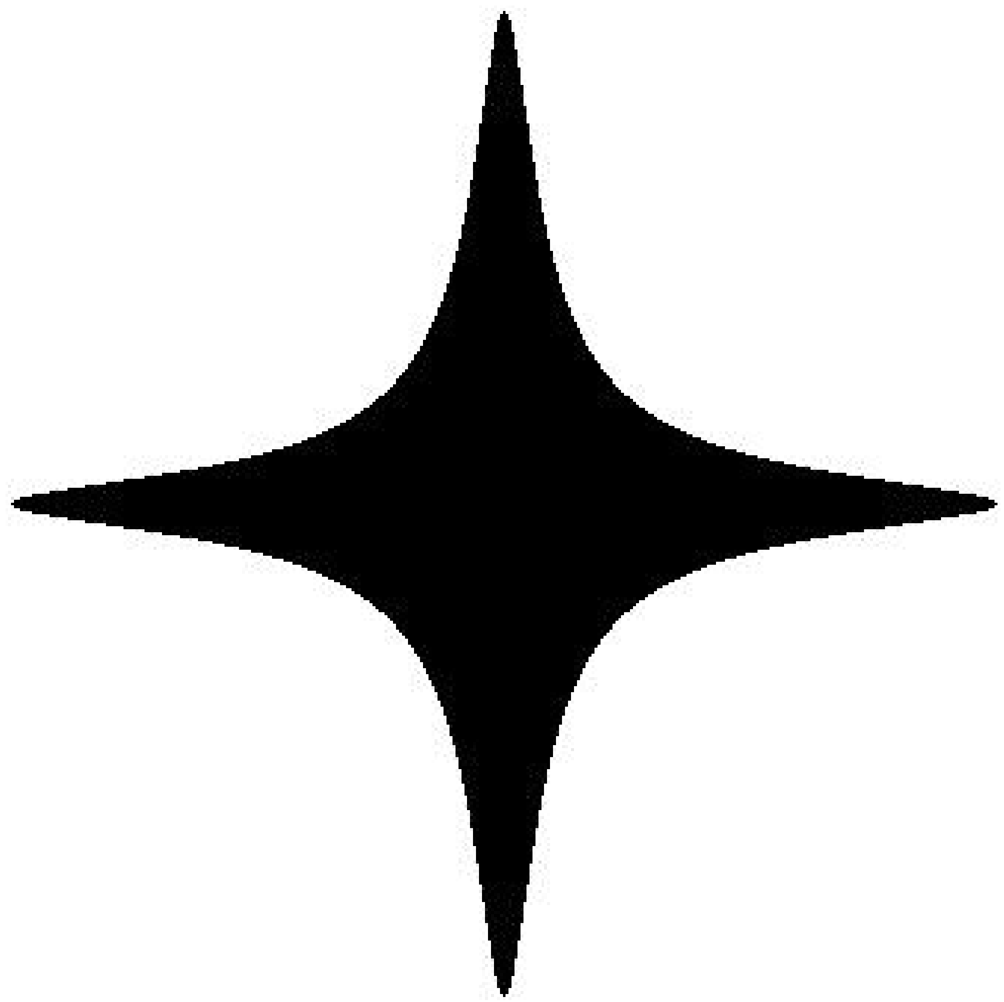


$$x^2 + y^2 = 1 - 300x^2y^2$$

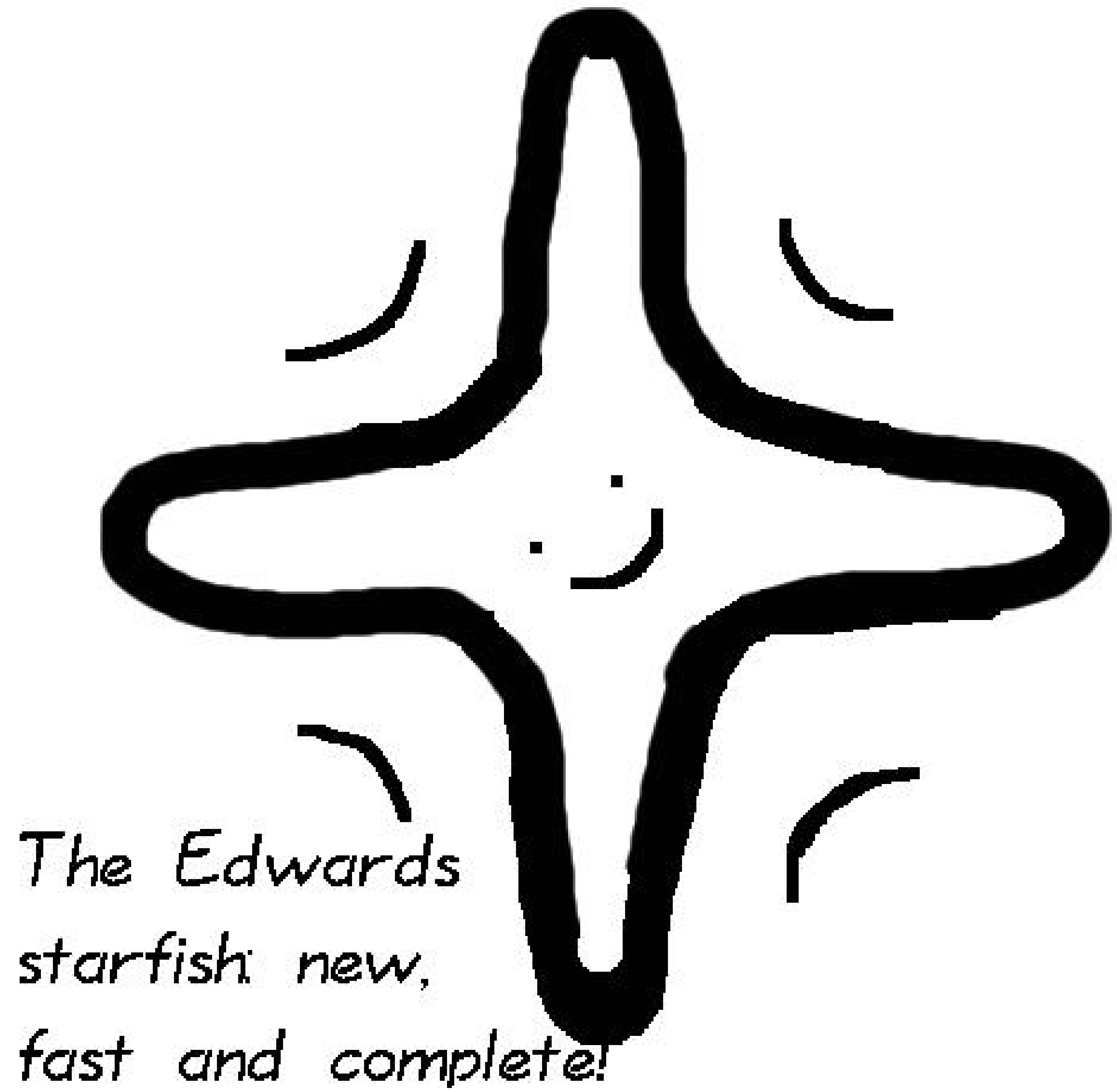


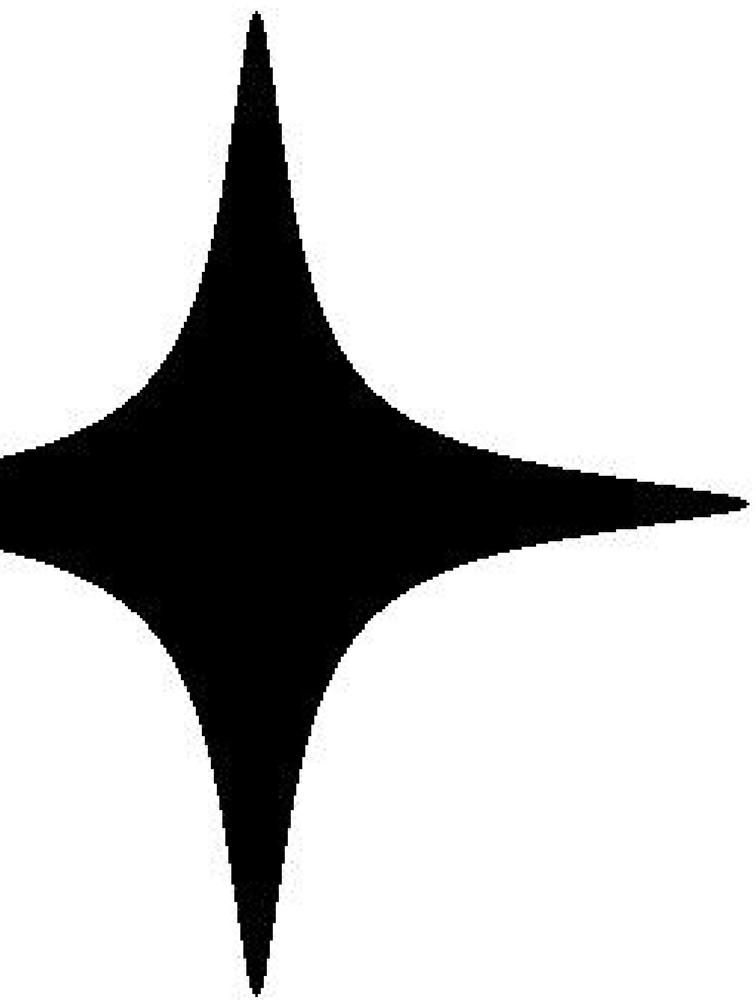
$$x^2 + y^2 = 1 - 300x^2y^2$$



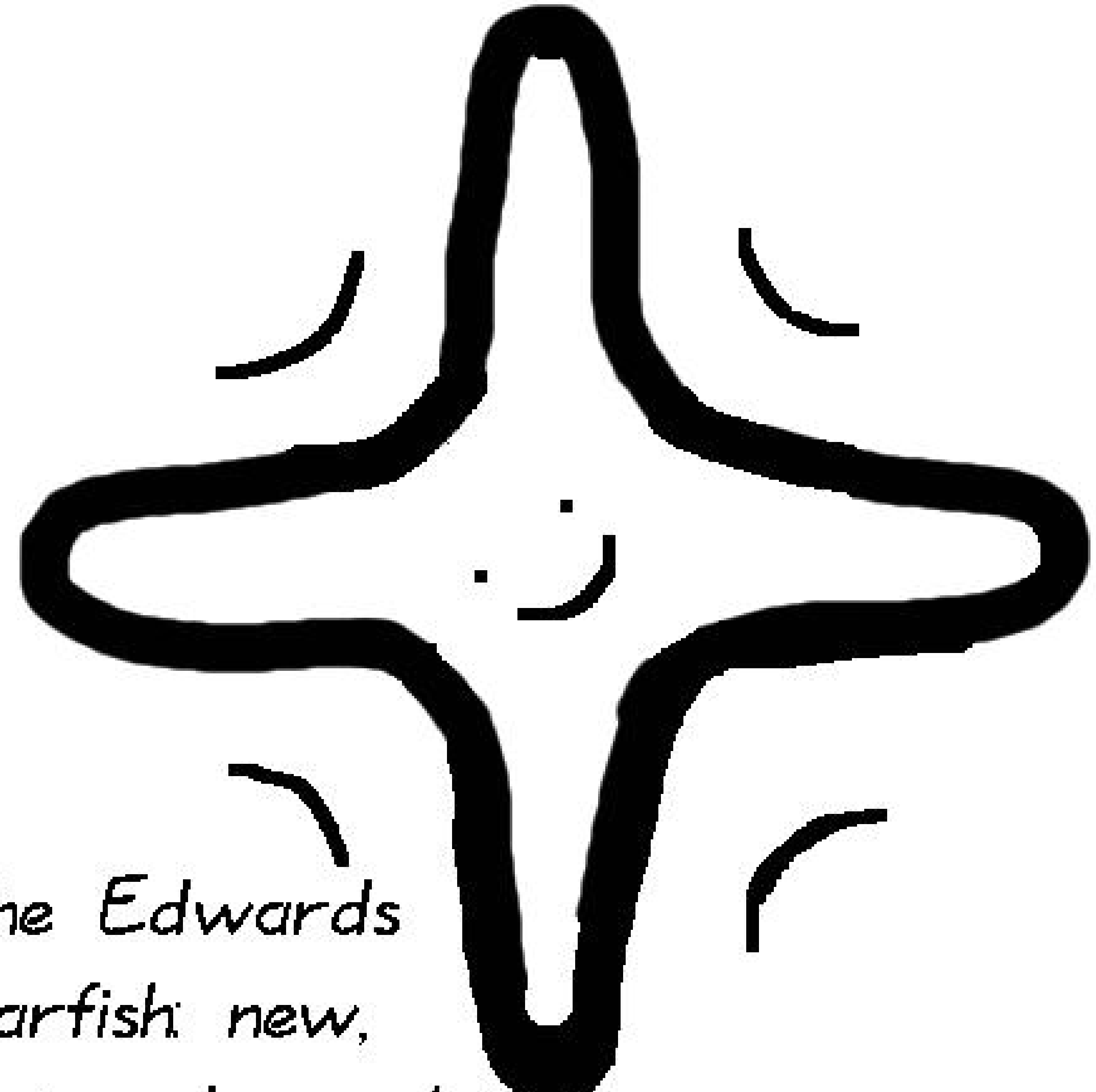


$$x^2 + y^2 = 1 - 300x^2y^2$$



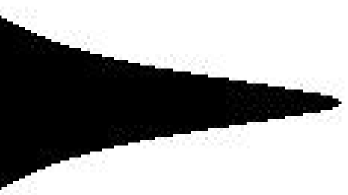


$= 1 - 300x^2y^2$

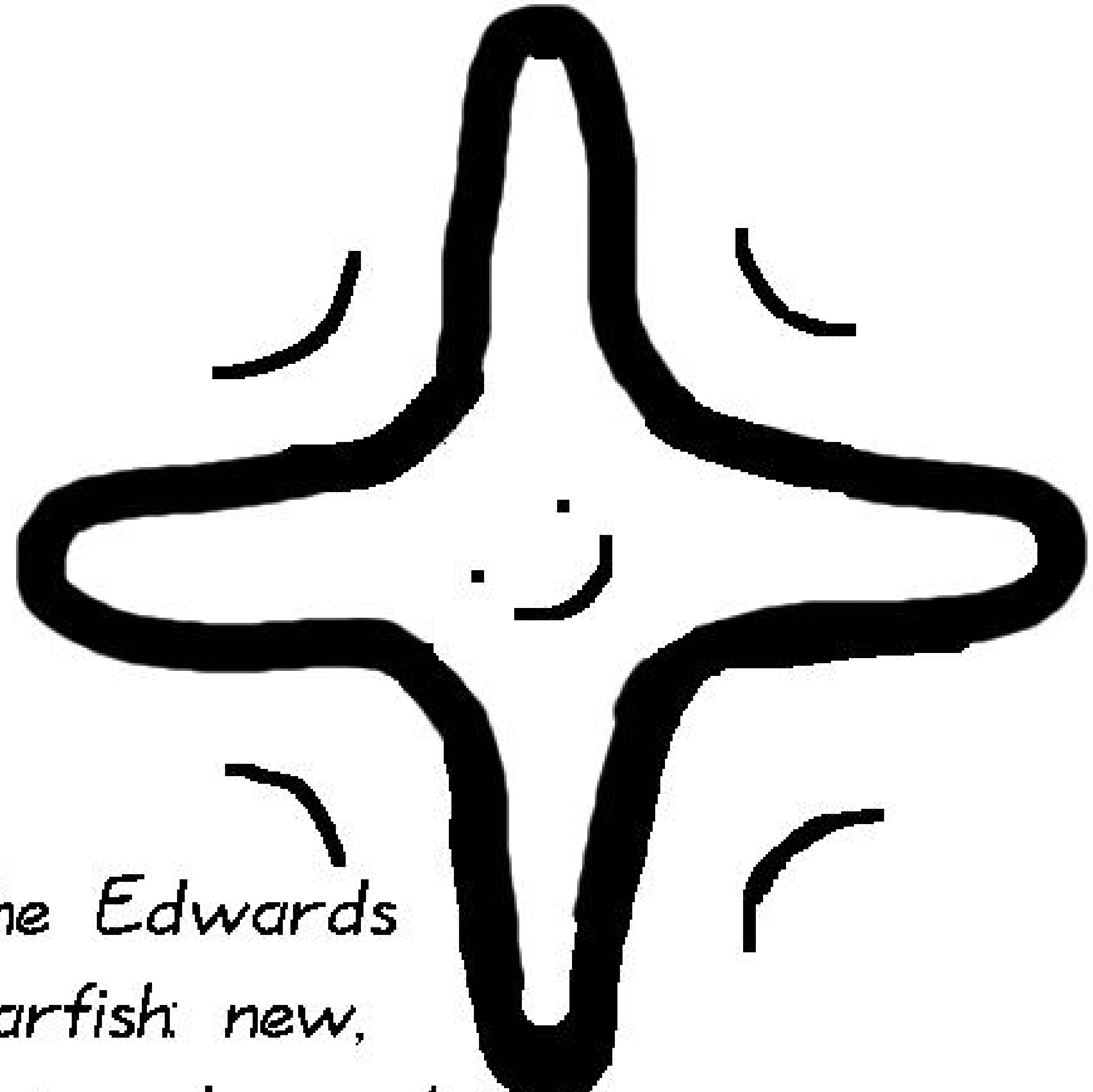


The Edwards starfish: new, fast and complete!

Start!

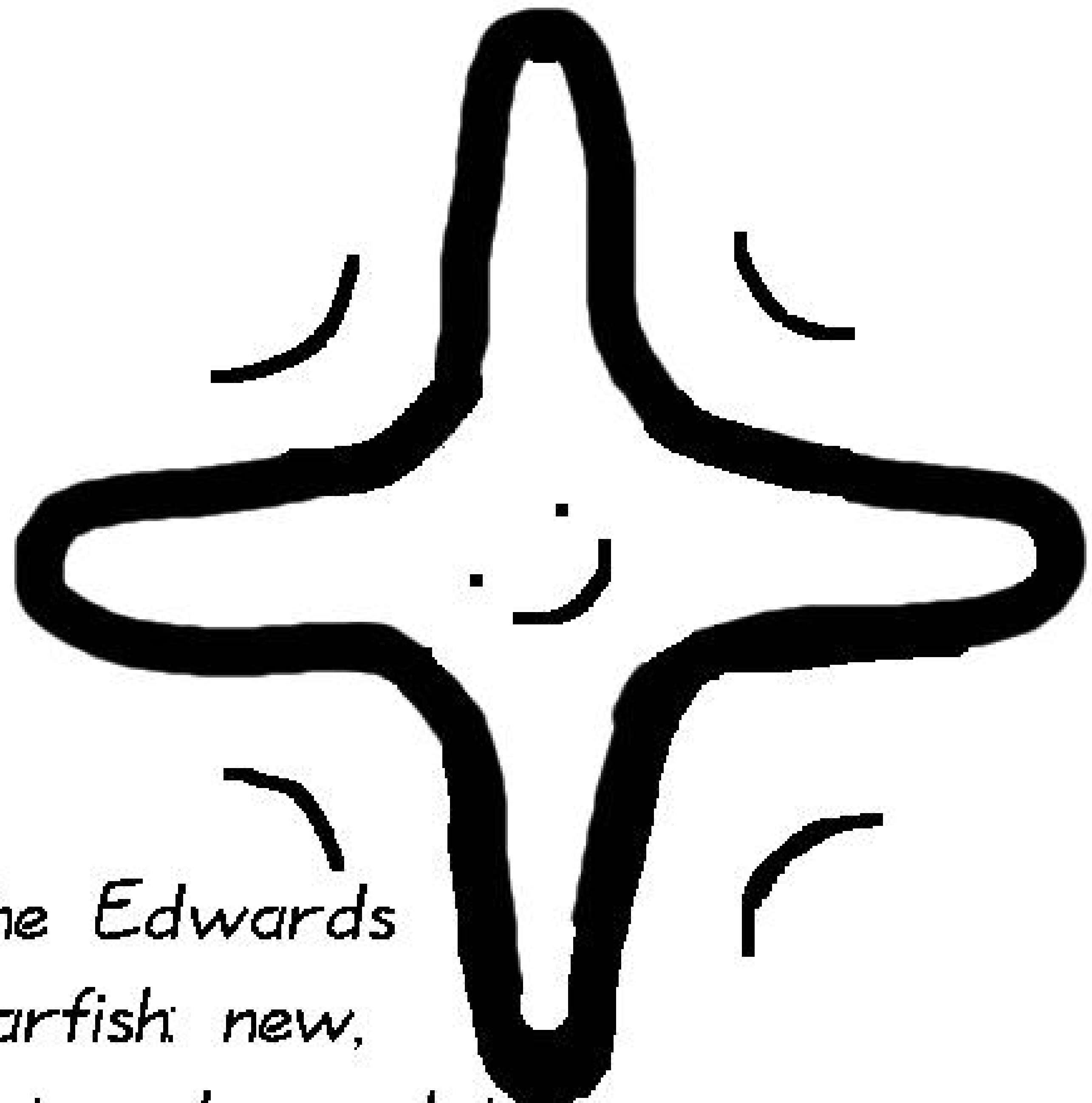


$0x^2y^2$



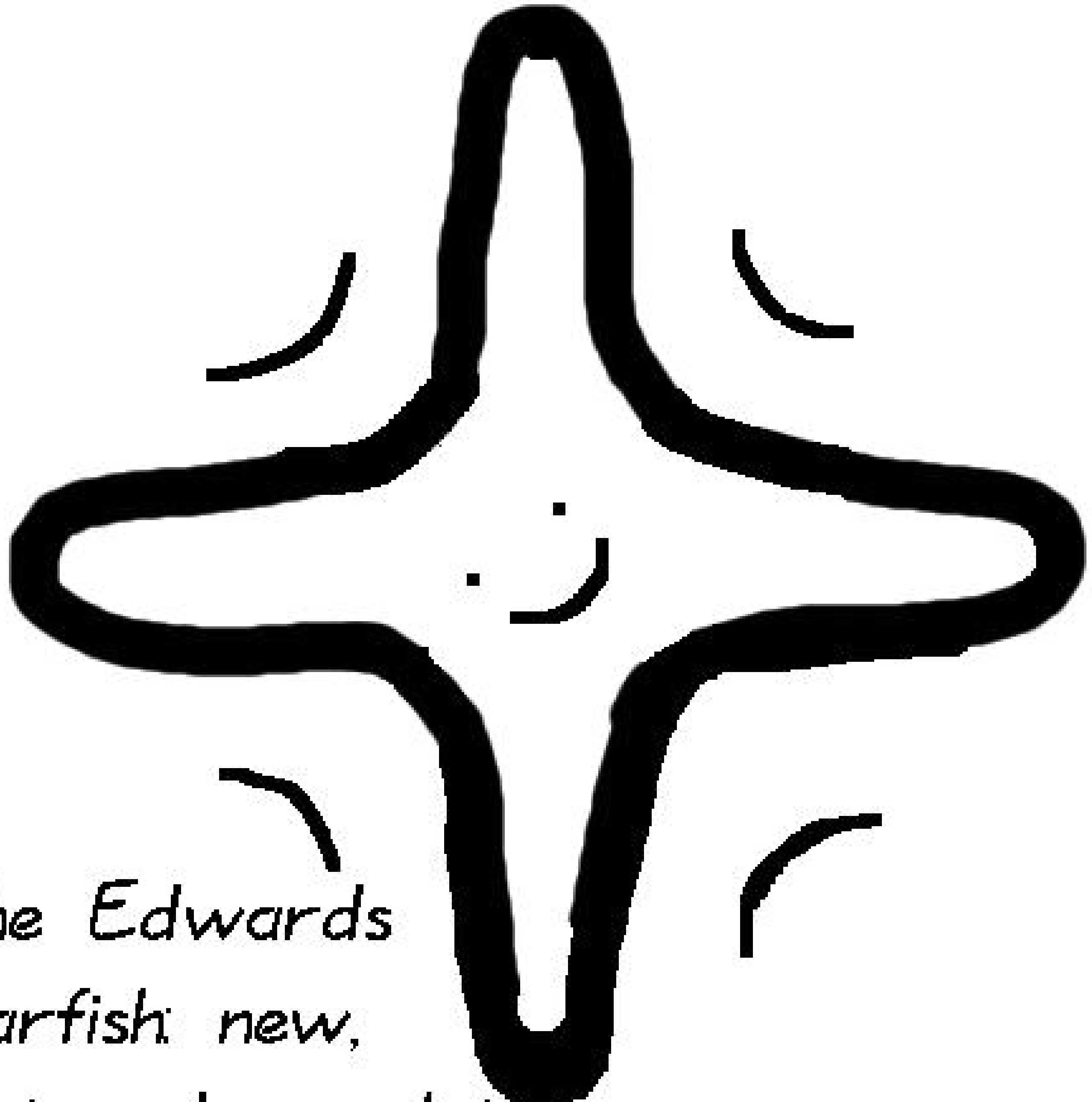
The Edwards starfish: new, fast and complete!

Start!

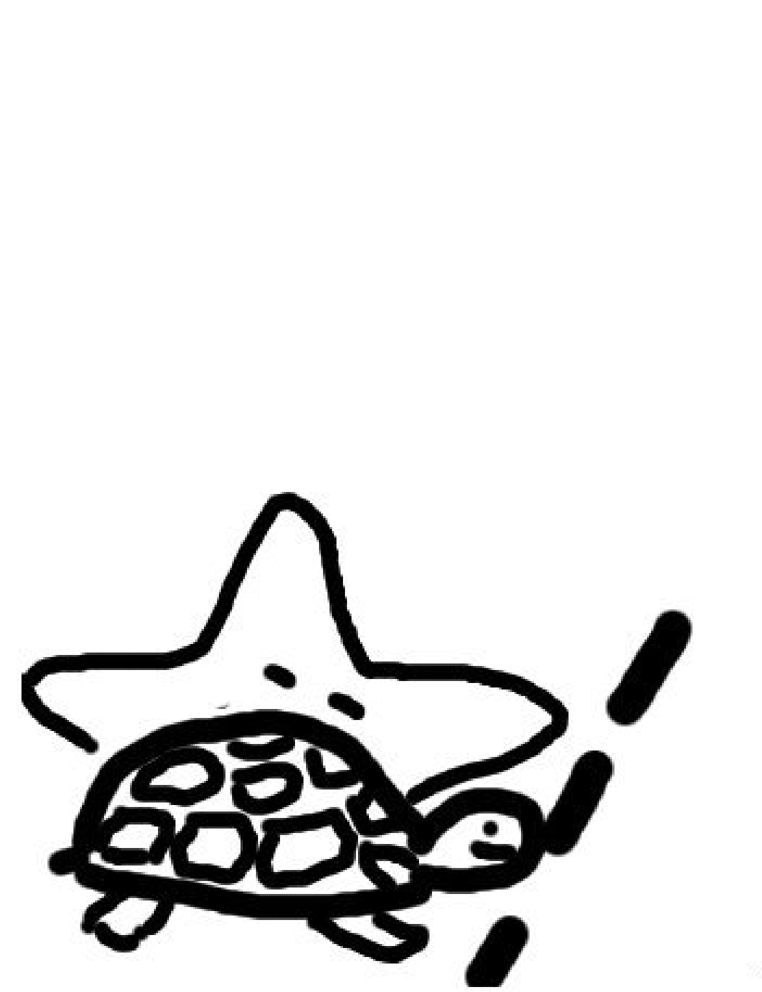


The Edwards
starfish: new,
fast and complete!

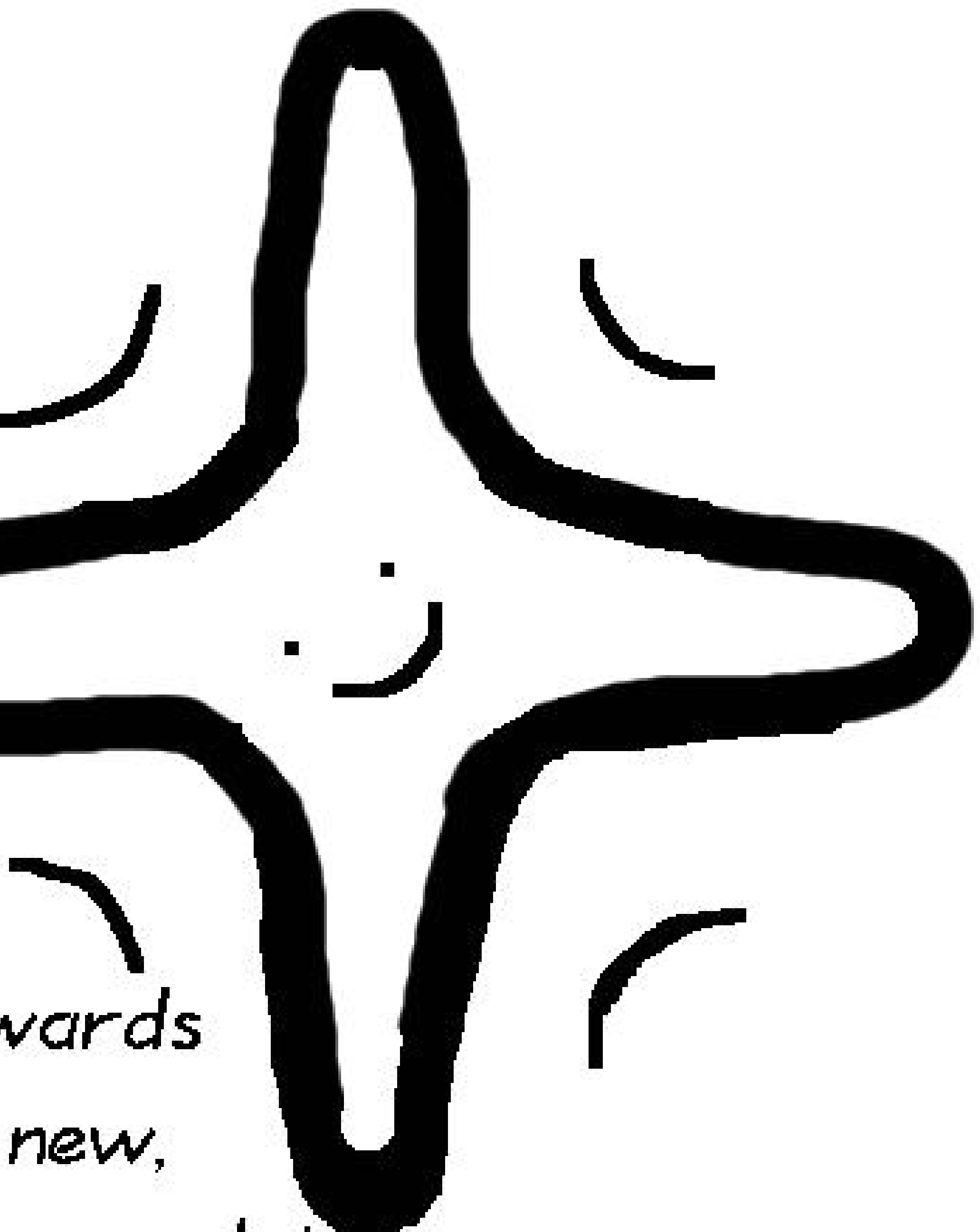
Start!



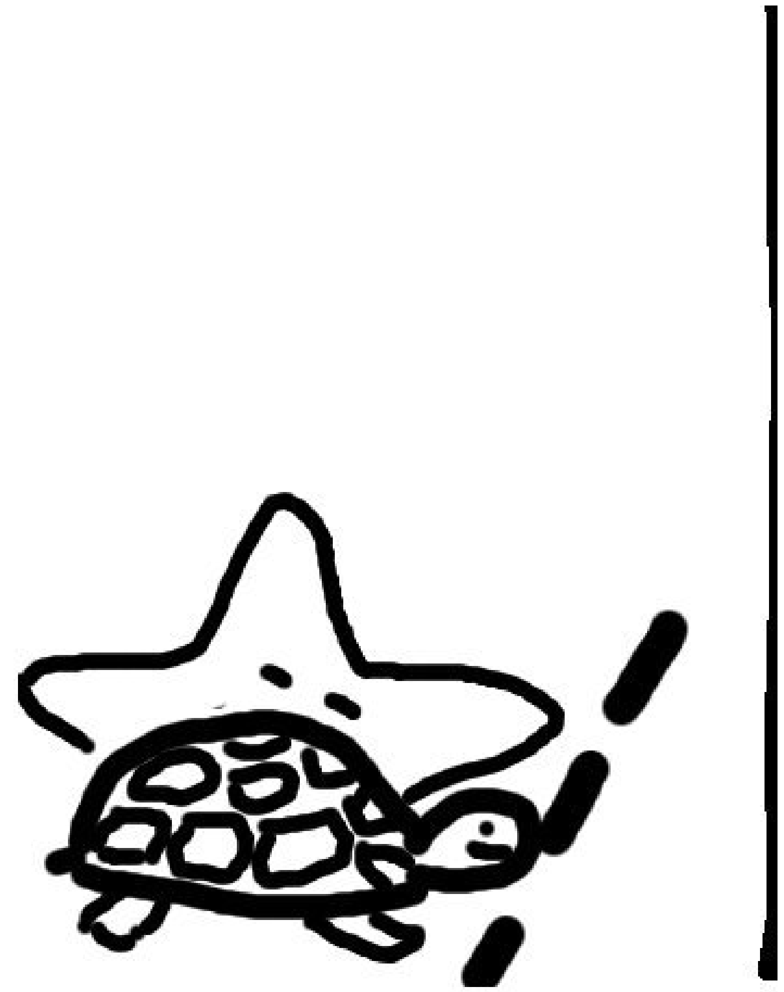
The Edwards
starfish: new,
fast and complete!



Start!

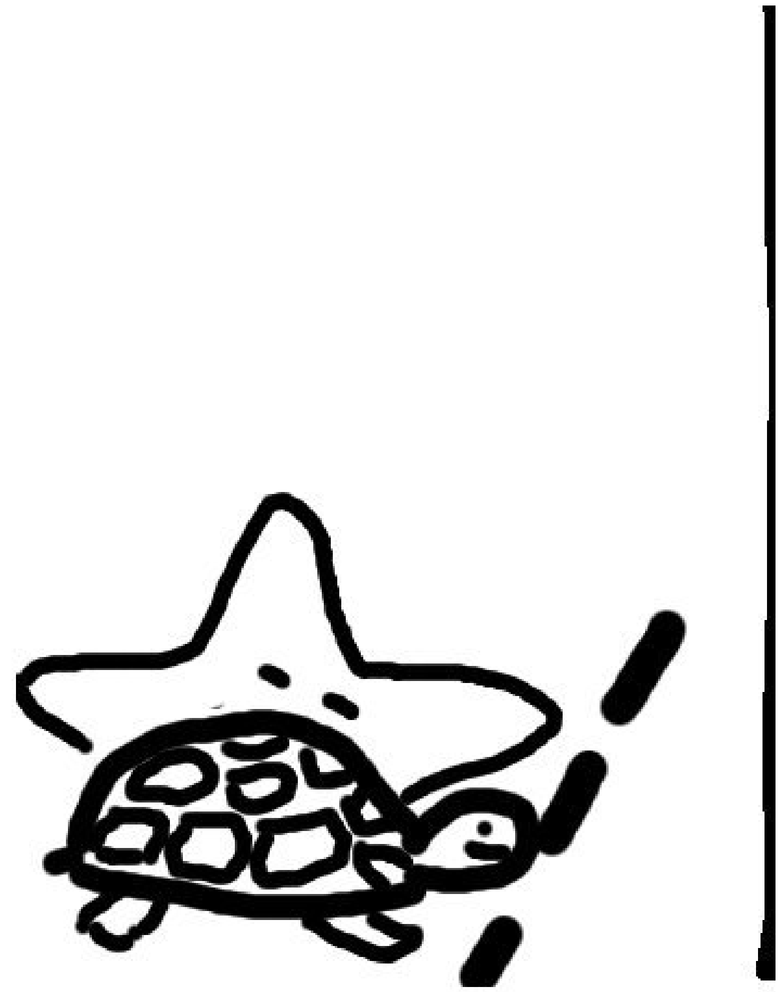


wards
new,
complete!



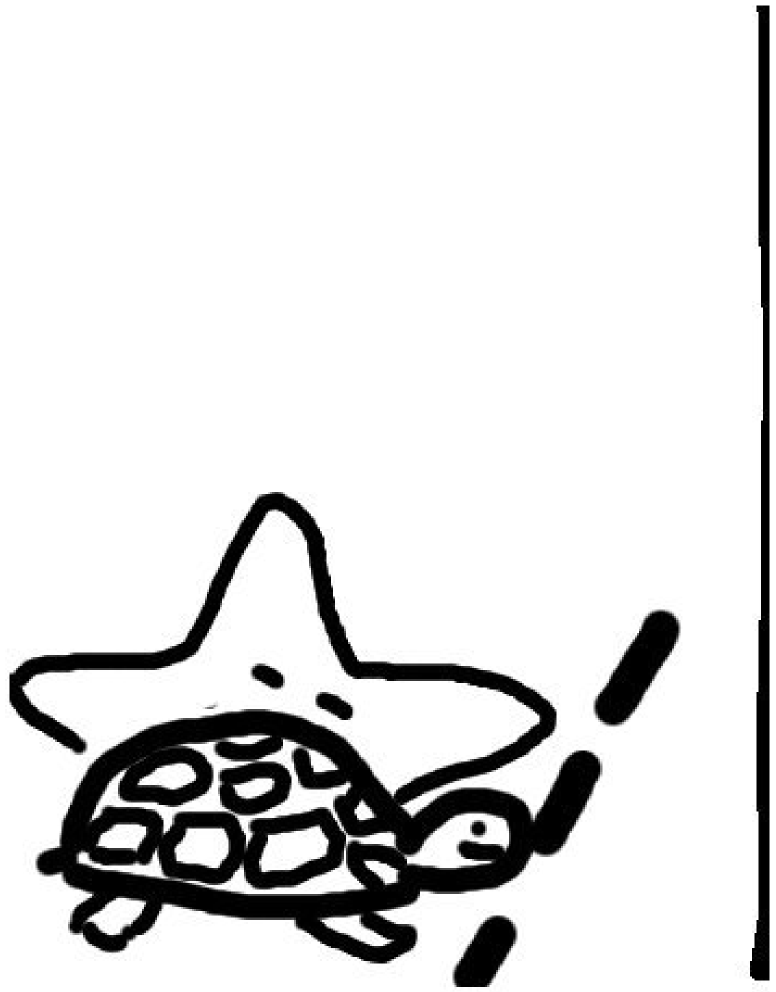
Start!

Weierstras
left behind

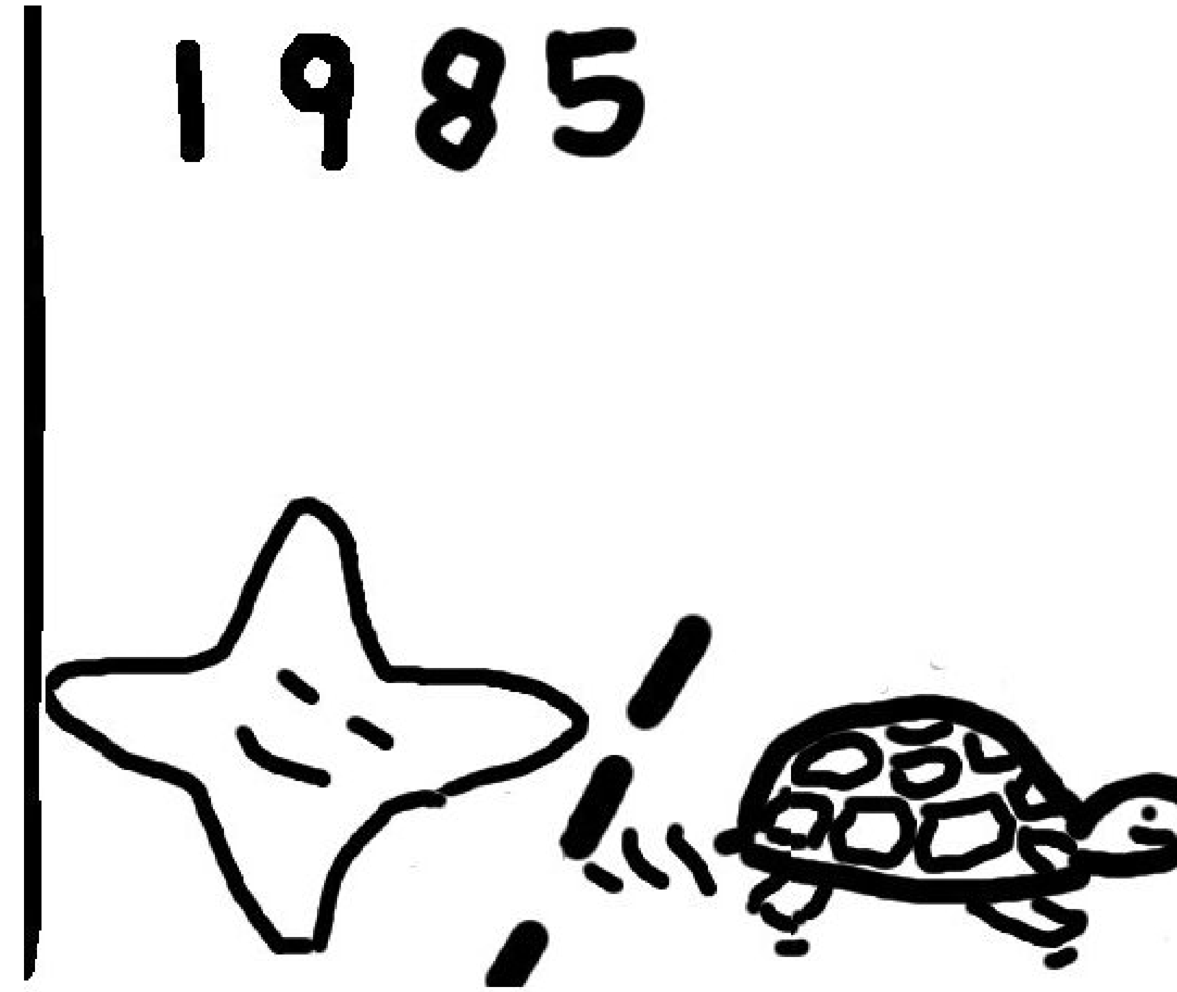


Start!

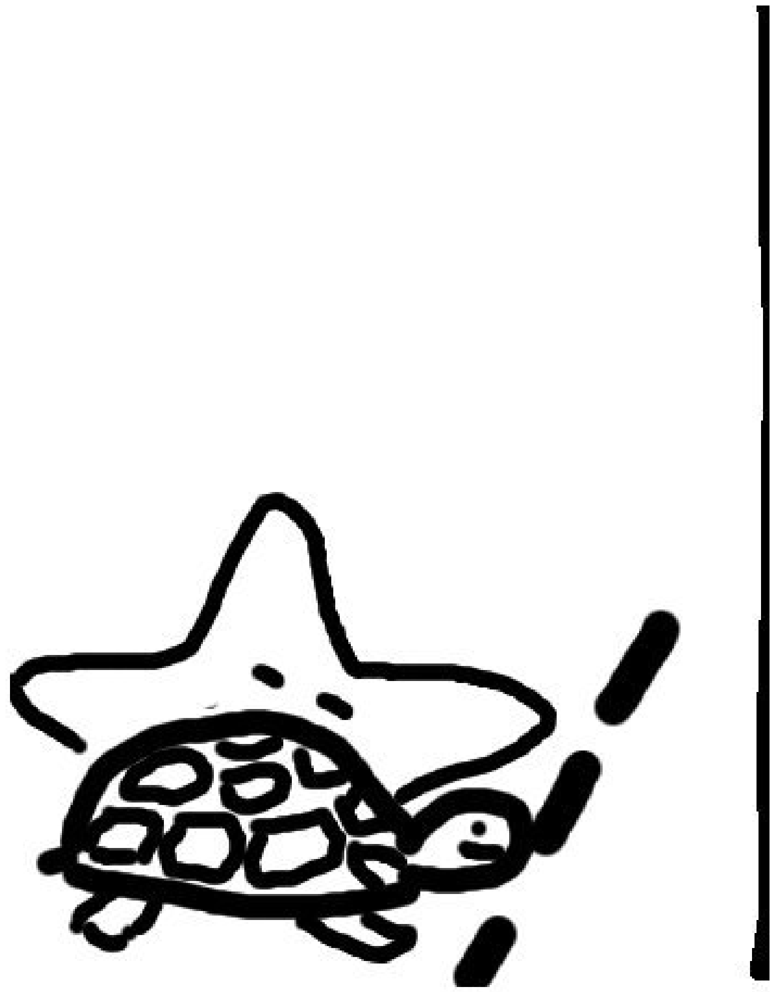
Weierstrass sets off; Ed
left behind sleeping



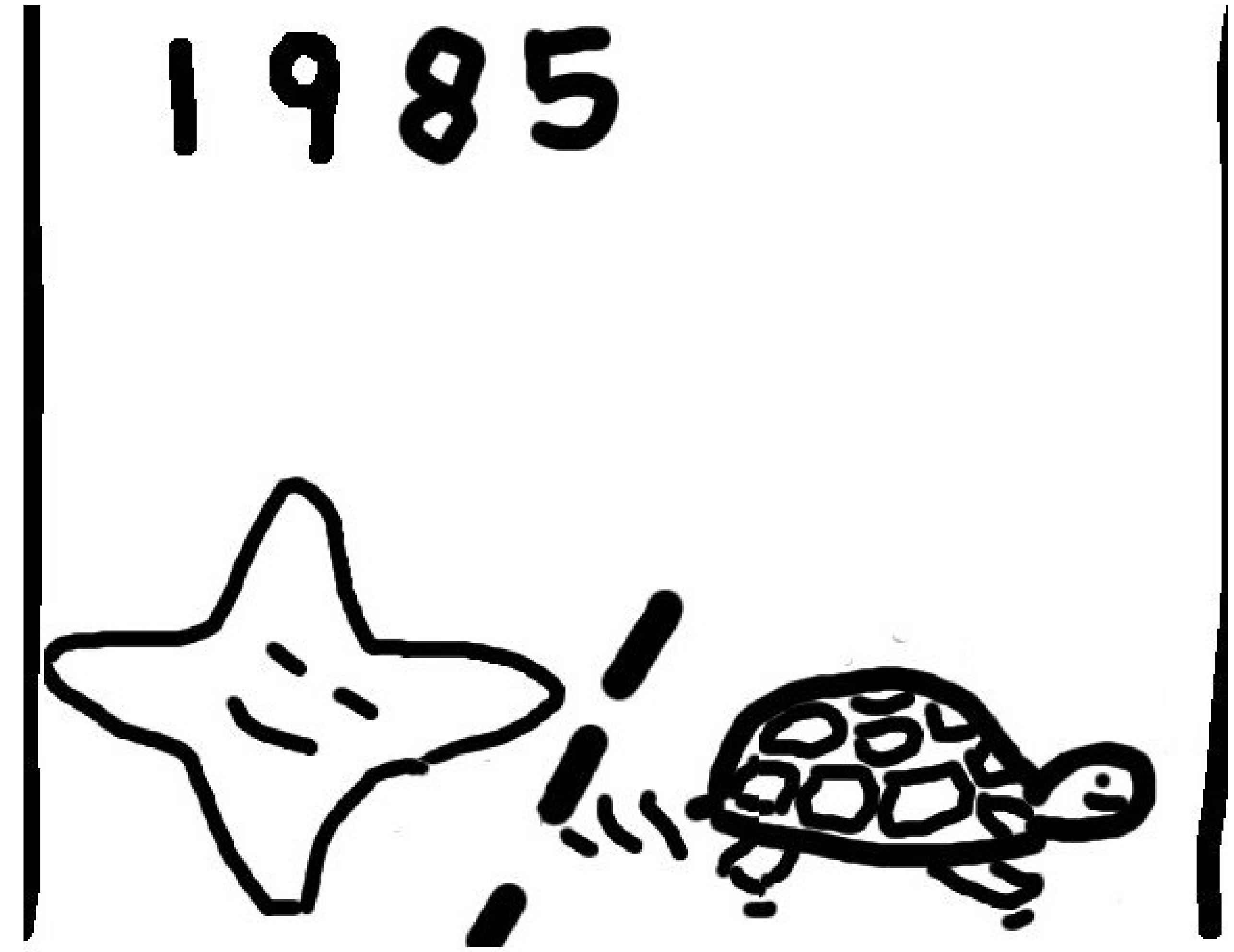
Start!



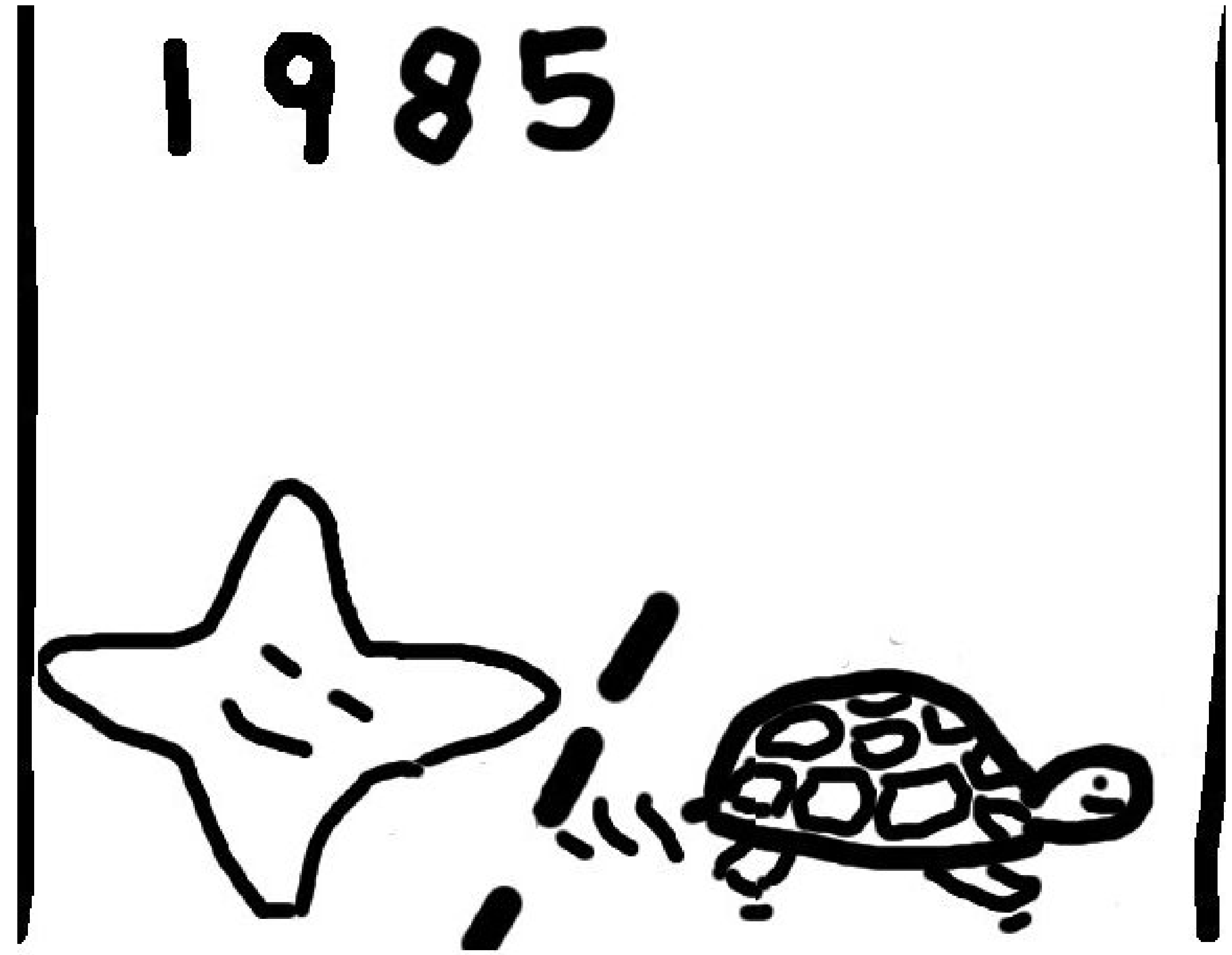
Weierstrass sets off, Edwards
left behind sleeping



Start!

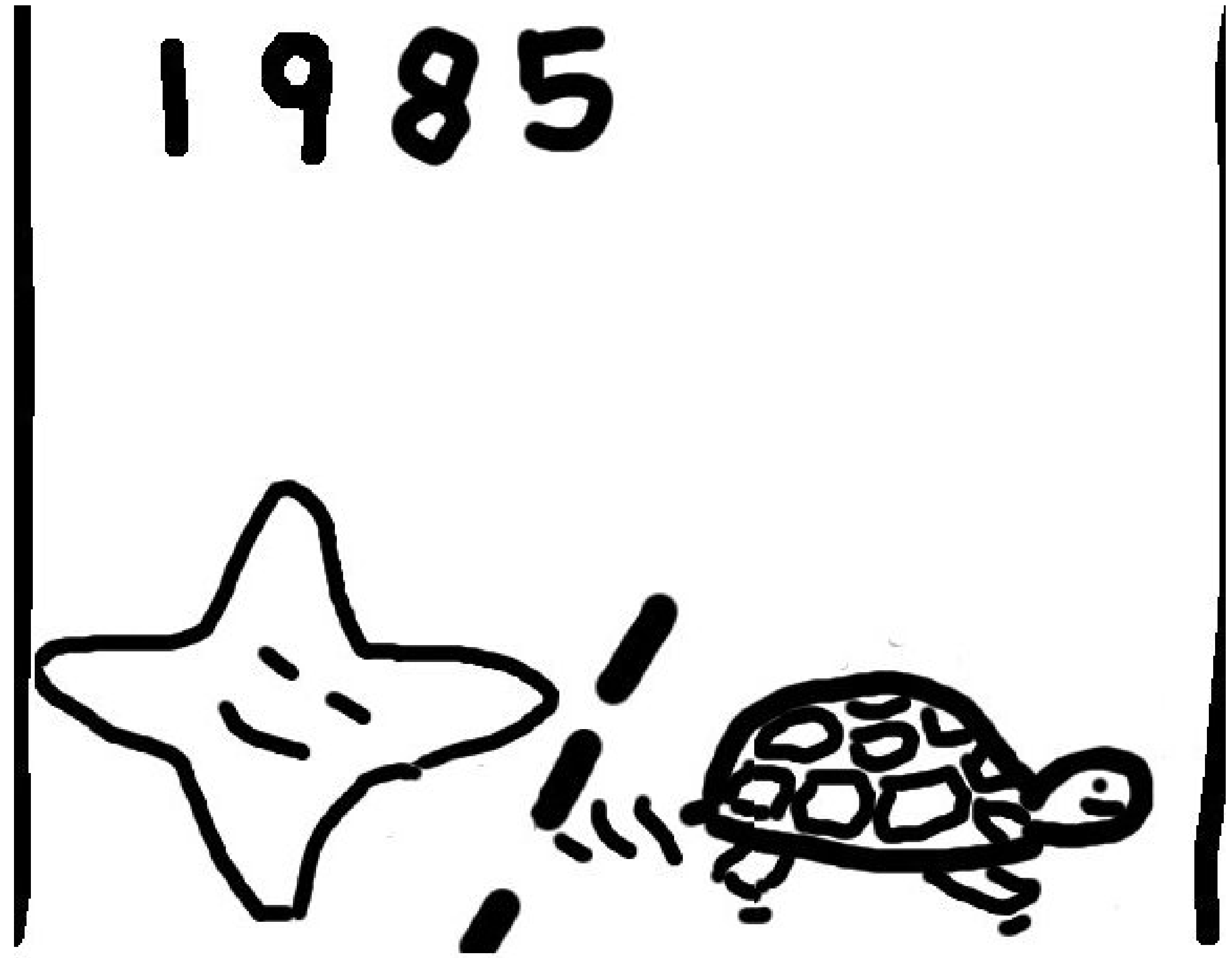


Weierstrass sets off, Edwards
left behind sleeping



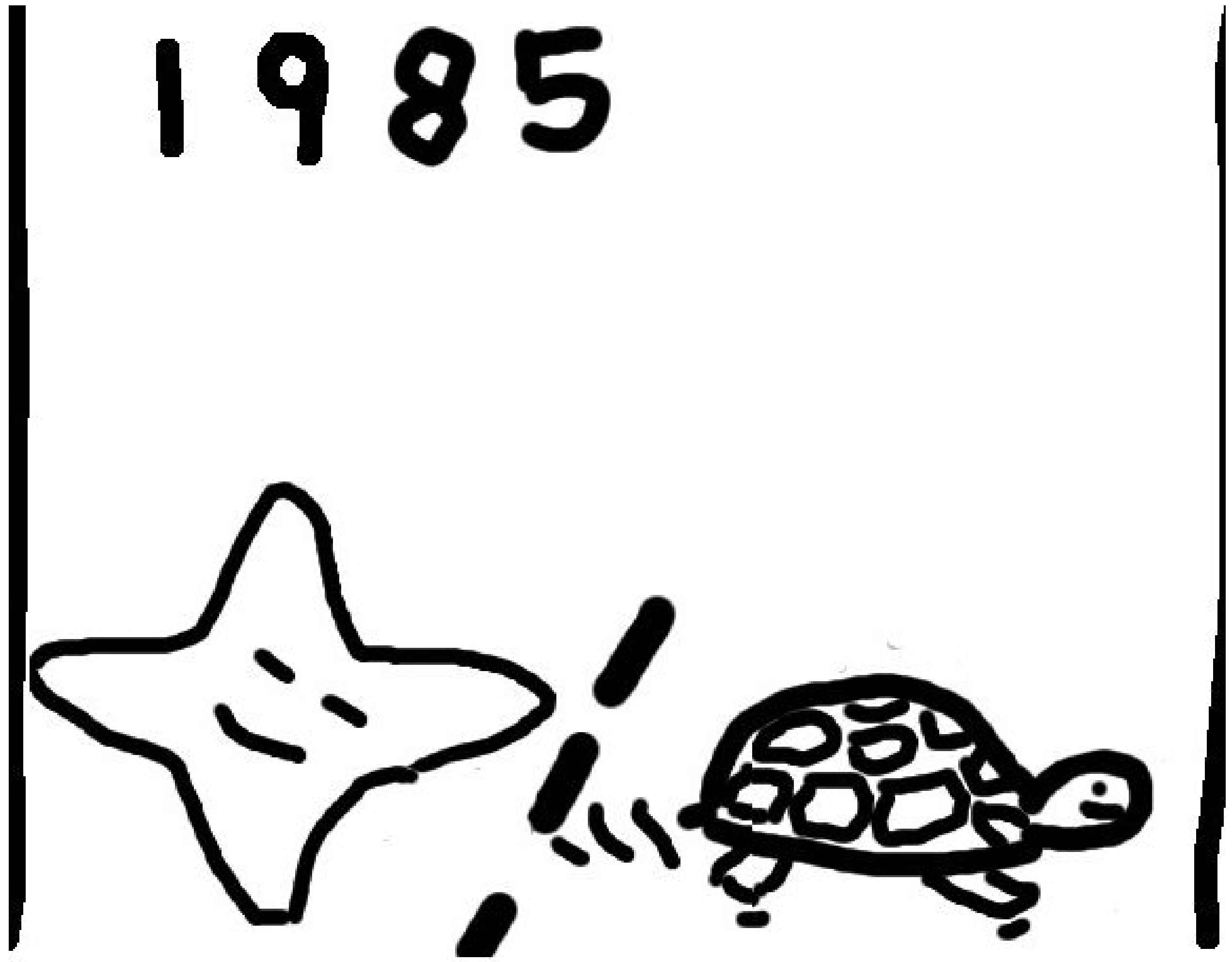
Weierstrass sets off, Edwards
left behind sleeping

Weierstras
finally Edw



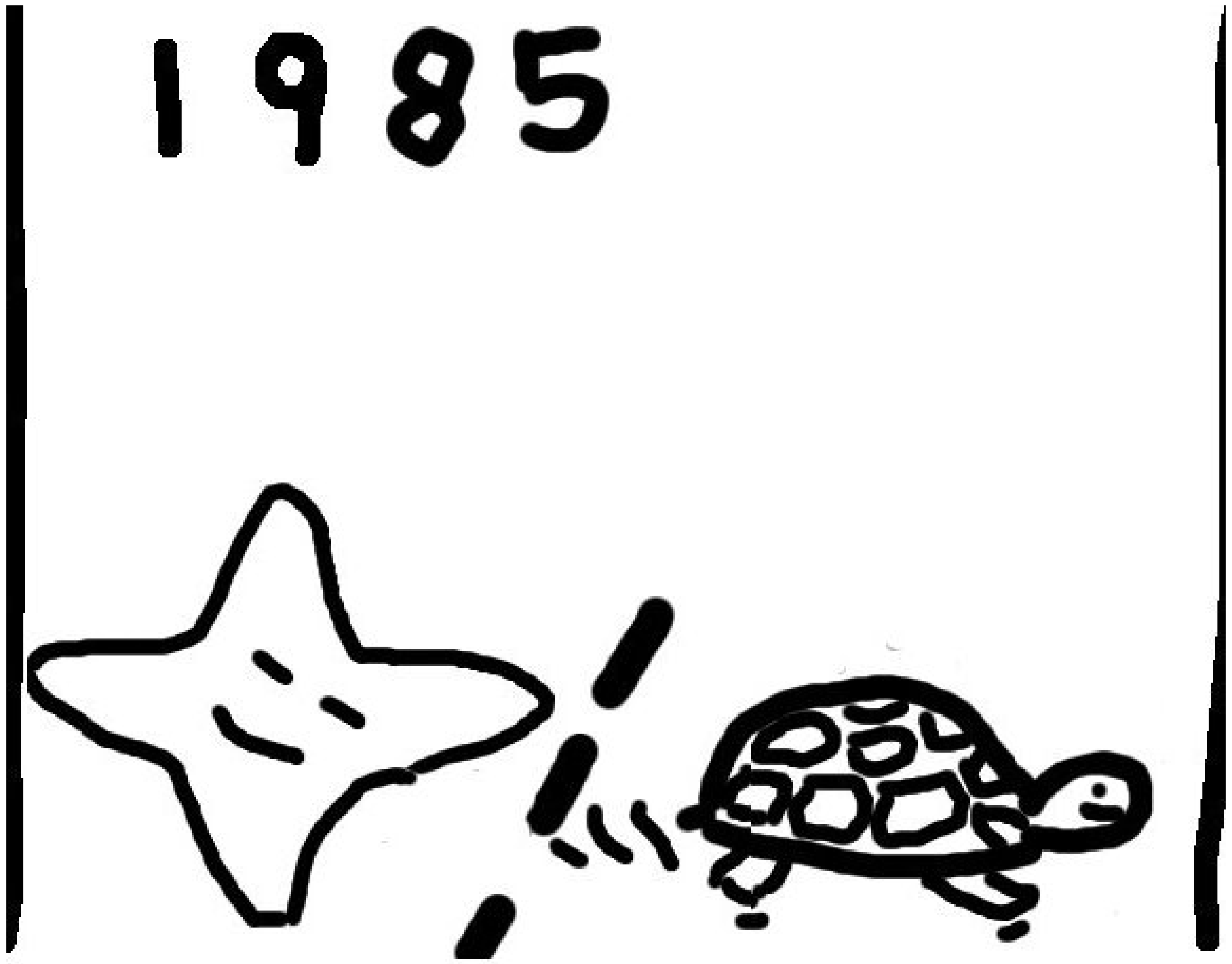
Weierstrass sets off. Edwards
left behind sleeping

Weierstrass has made sc
finally Edwards wakes u

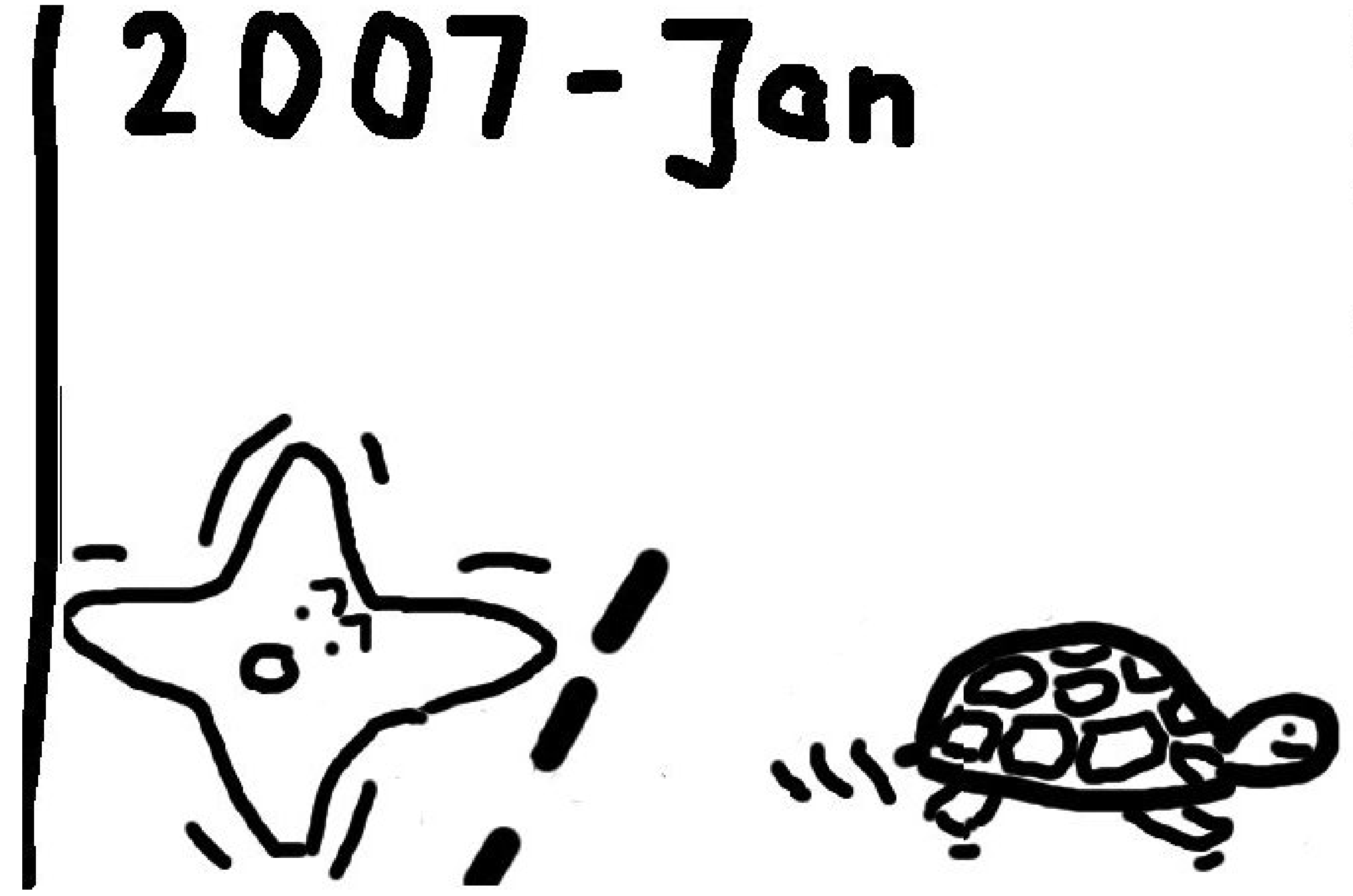


Weierstrass sets off, Edwards left behind sleeping

Weierstrass has made some progress
finally Edwards wakes up.

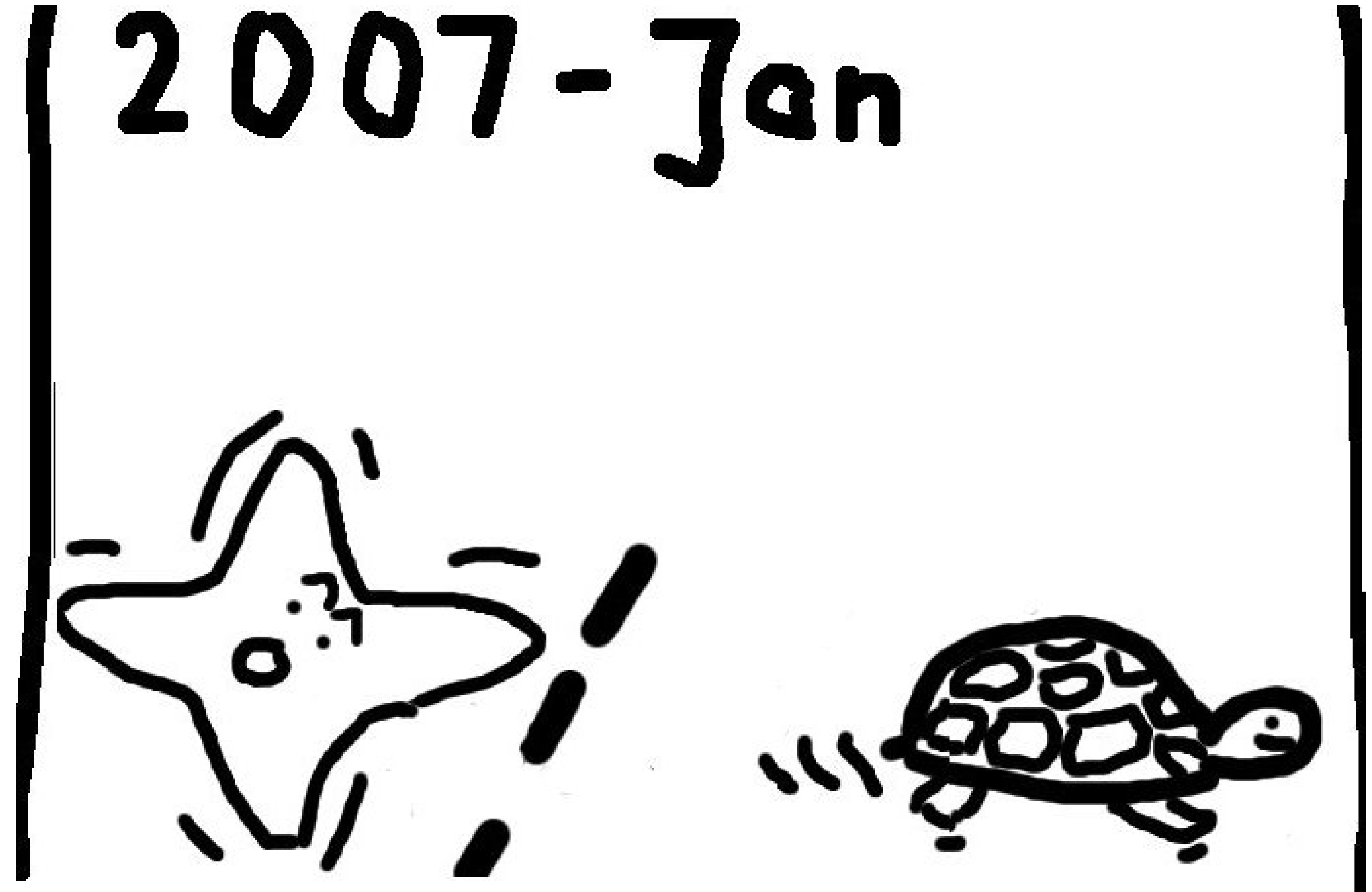


Weierstrass sets off, Edwards
left behind sleeping

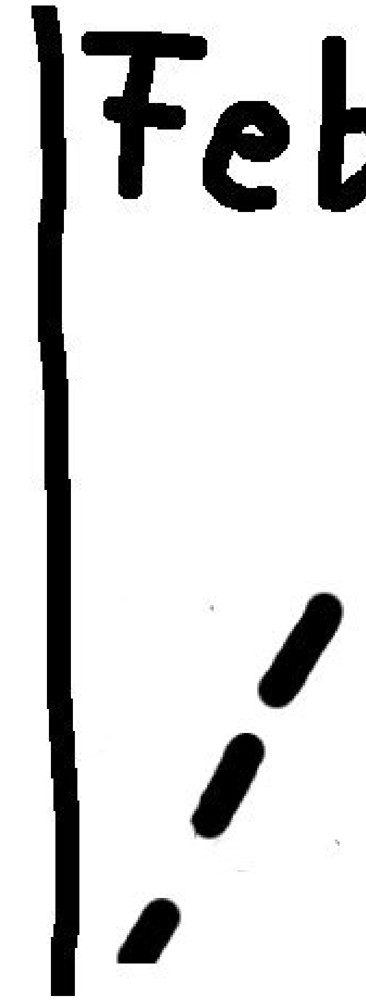


Weierstrass has made some progress –
finally Edwards wakes up.

s sets off. Edwards
sleeping

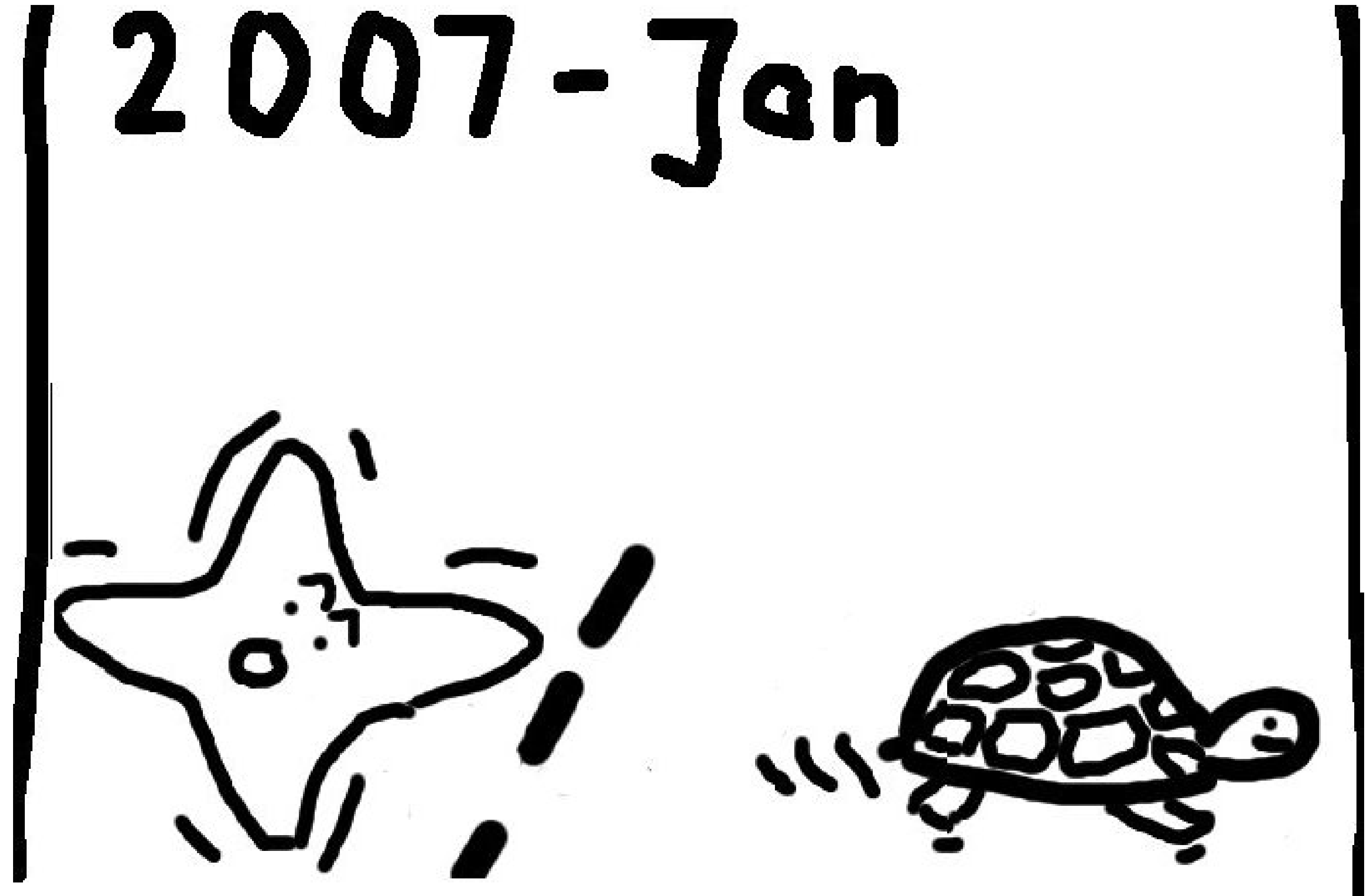


Weierstrass has made some progress - finally Edwards wakes up.



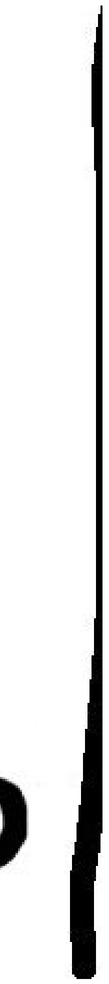
Exciting p
about to

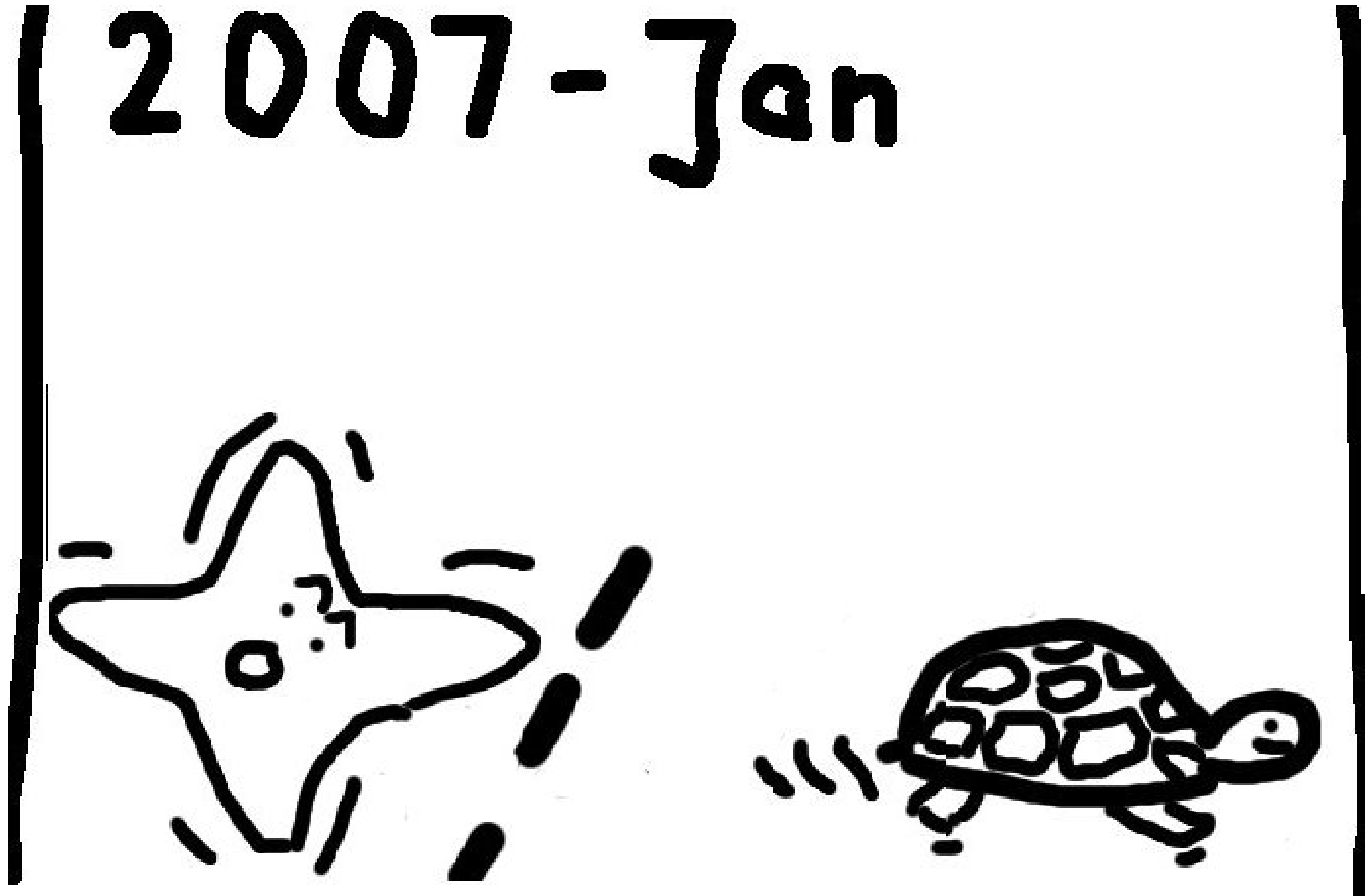
wards



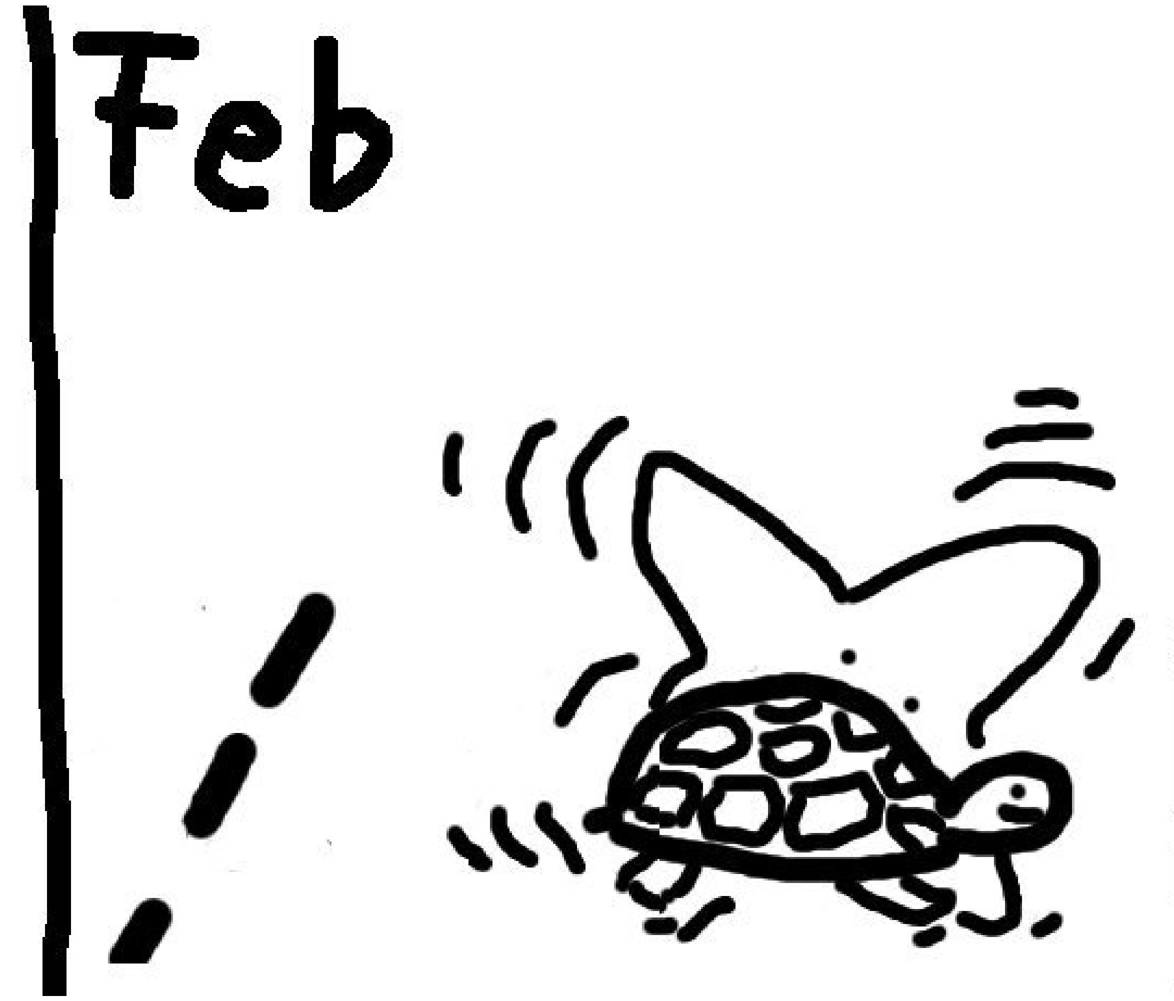
Weierstrass has made some progress -
finally Edwards wakes up.

Exciting progress: Edwa
about to overtake!!

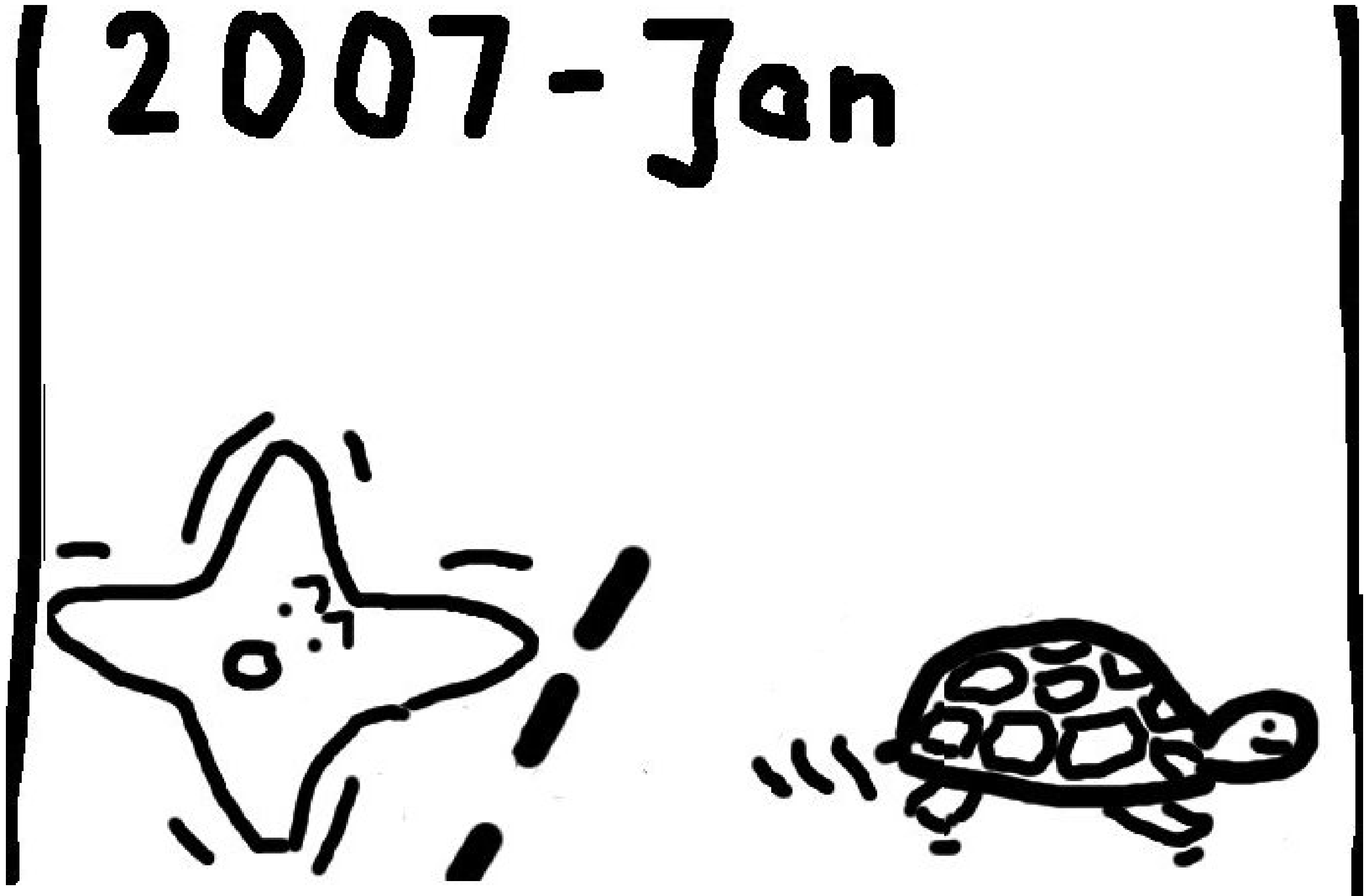




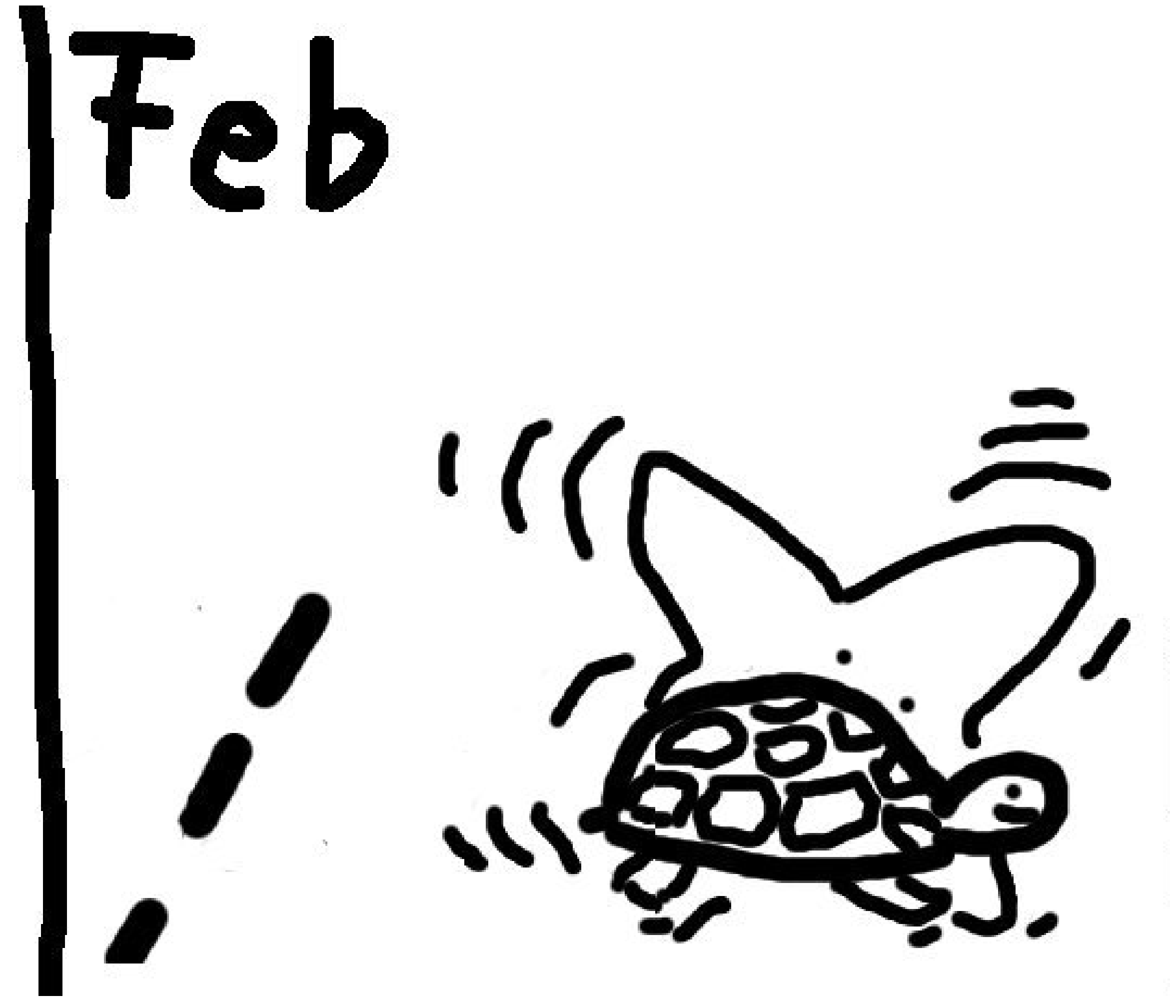
Weierstrass has made some progress – finally Edwards wakes up.



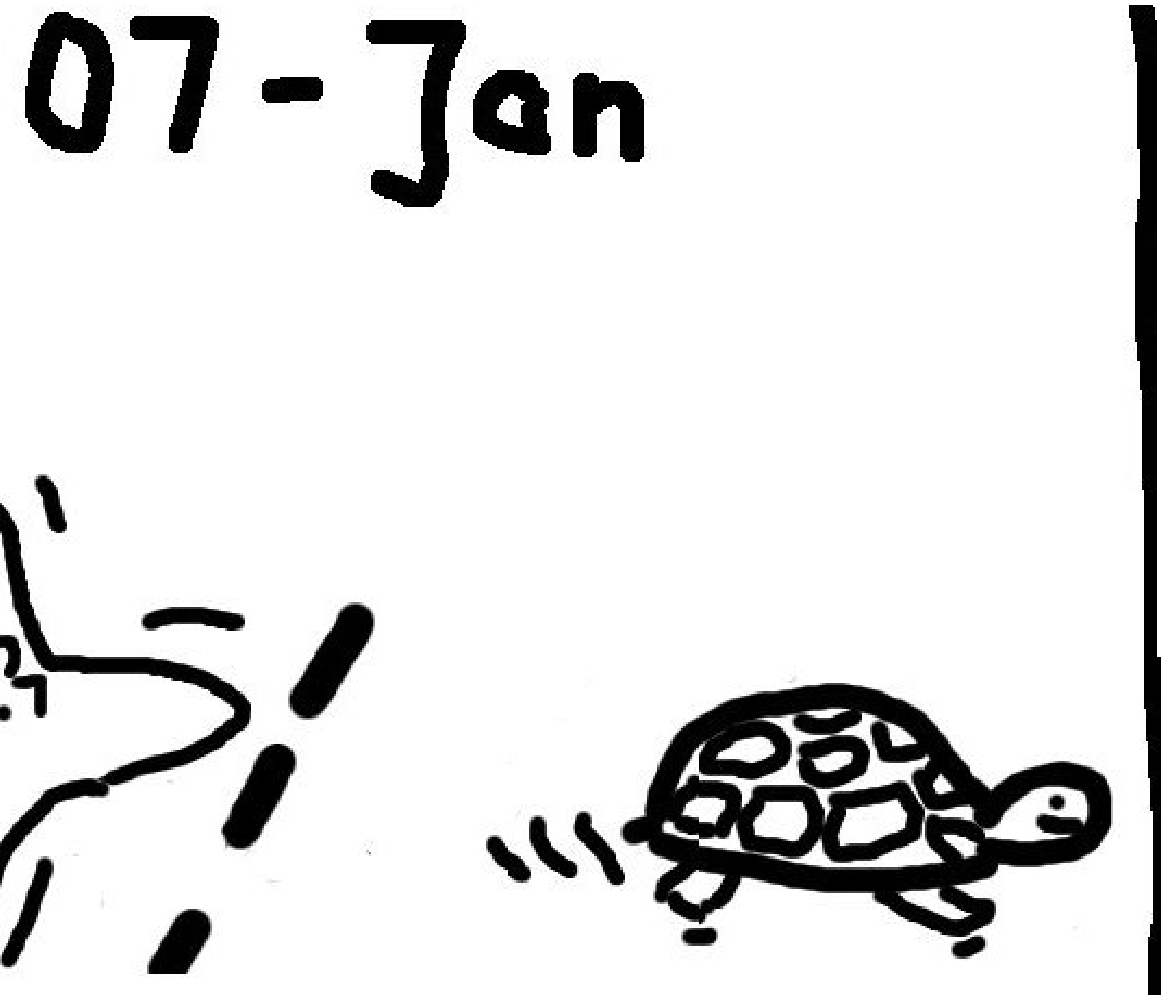
Exciting progress: Edwards about to overtake!!



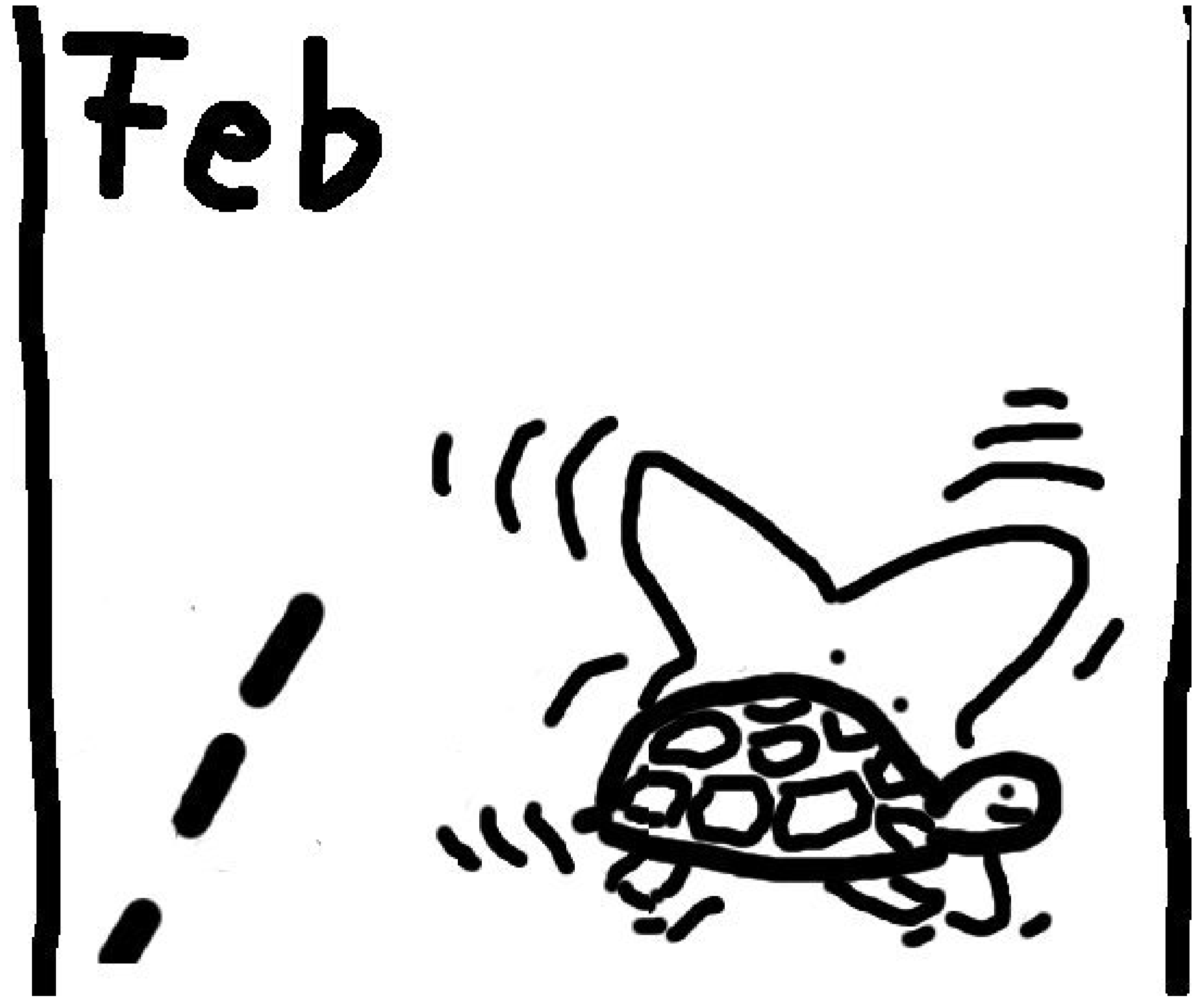
Weierstrass has made some progress -
finally Edwards wakes up.



Exciting progress: Edwards
about to overtake!!

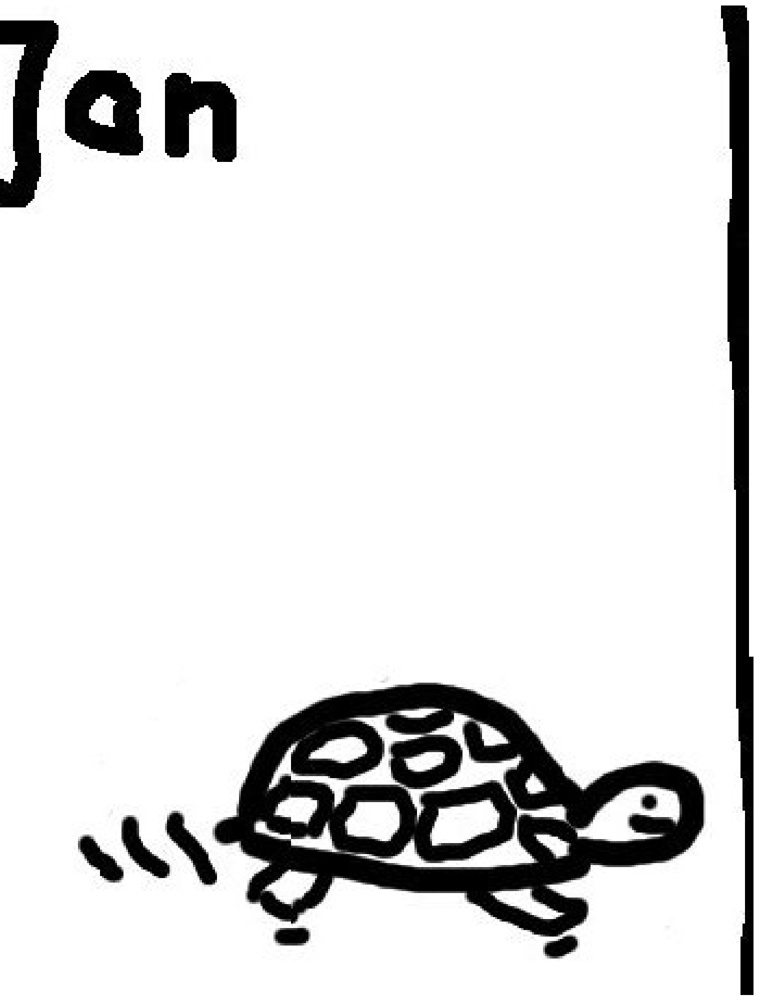


s has made some progress -
vards wakes up.

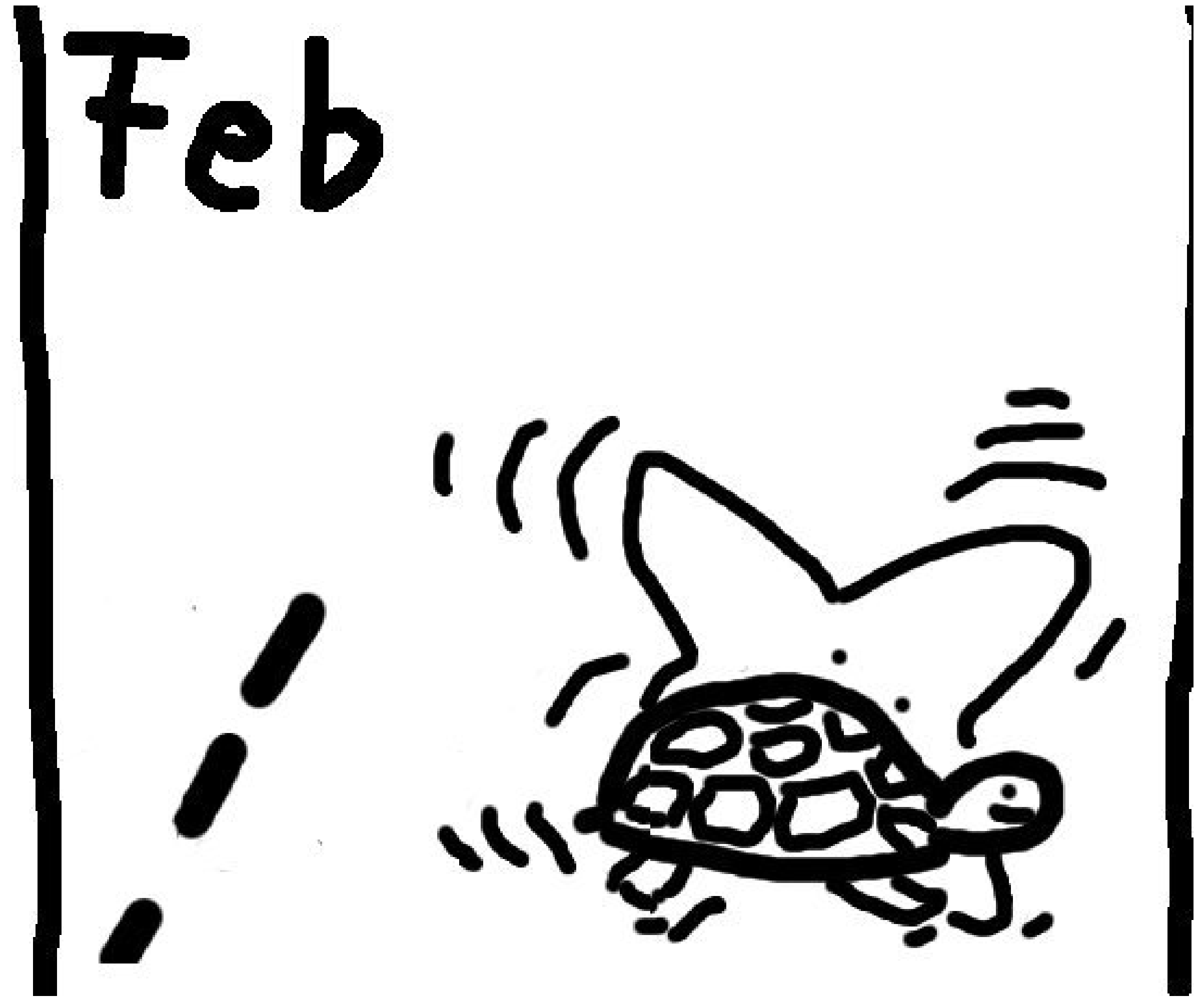


Exciting progress: Edwards
about to overtake!!

And the w

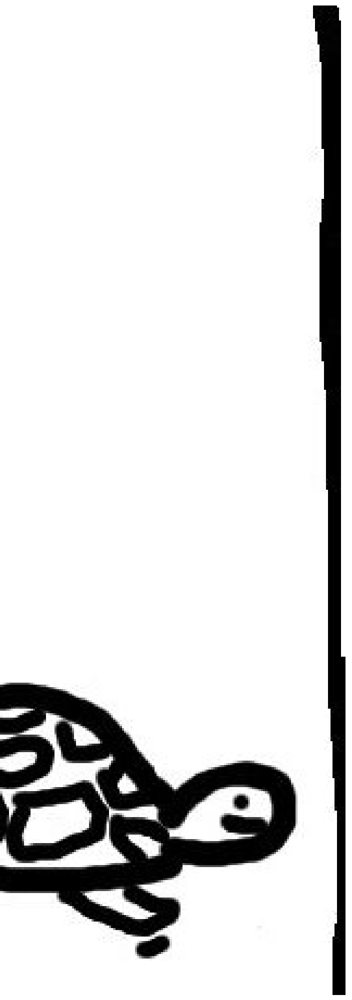


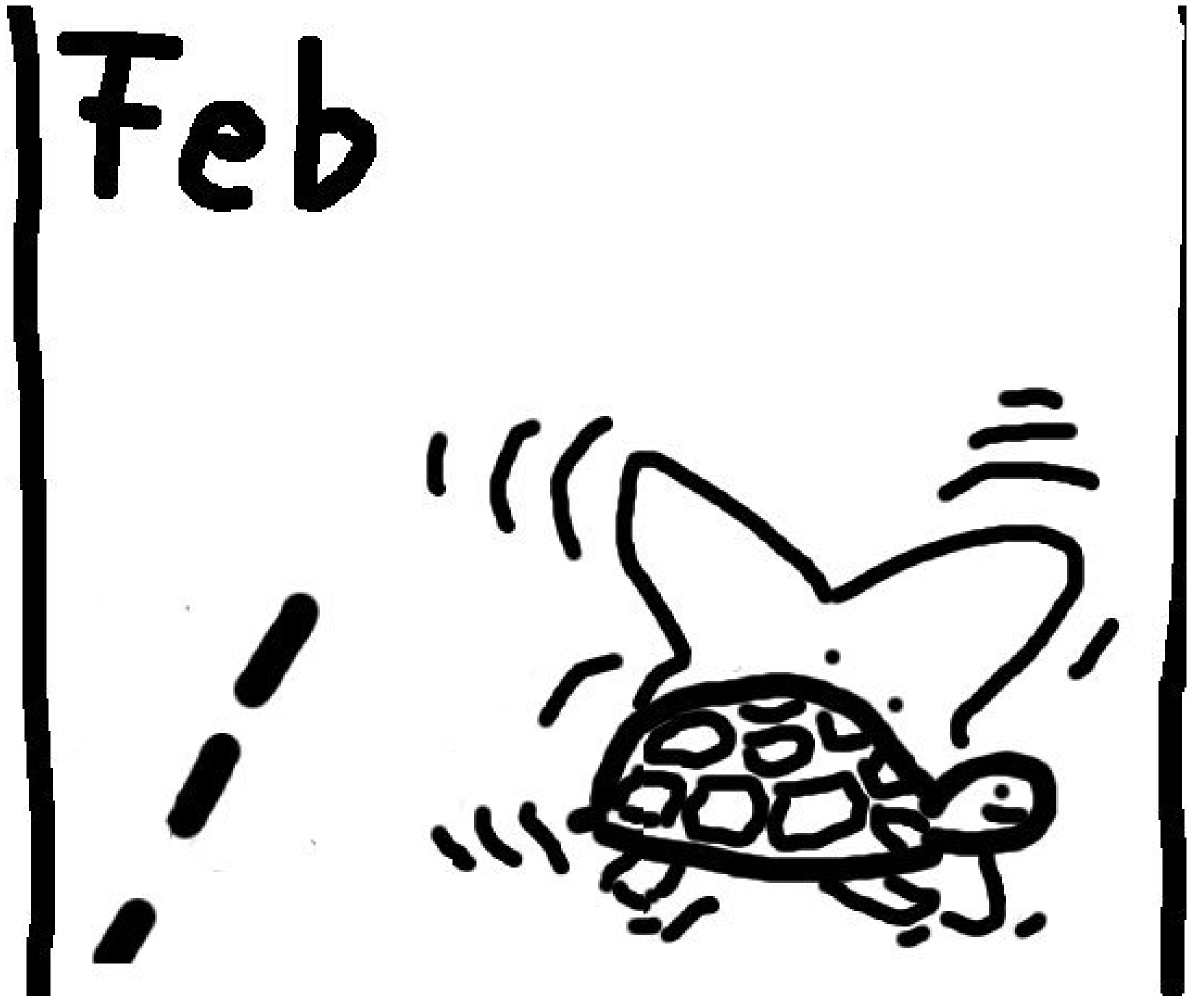
ome progress -
up.



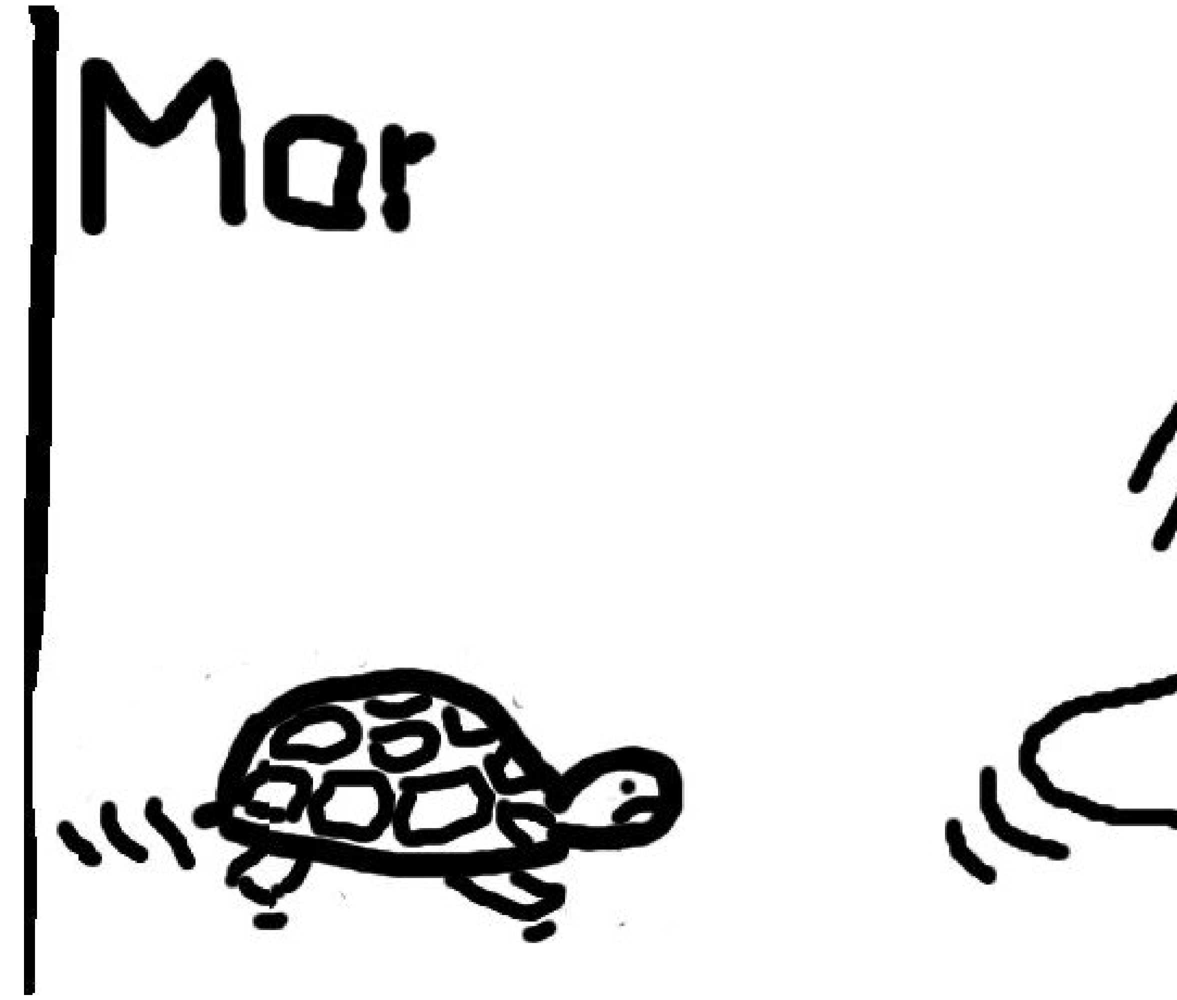
Exciting progress: Edwards about to overtake!!

And the winner is: Edw

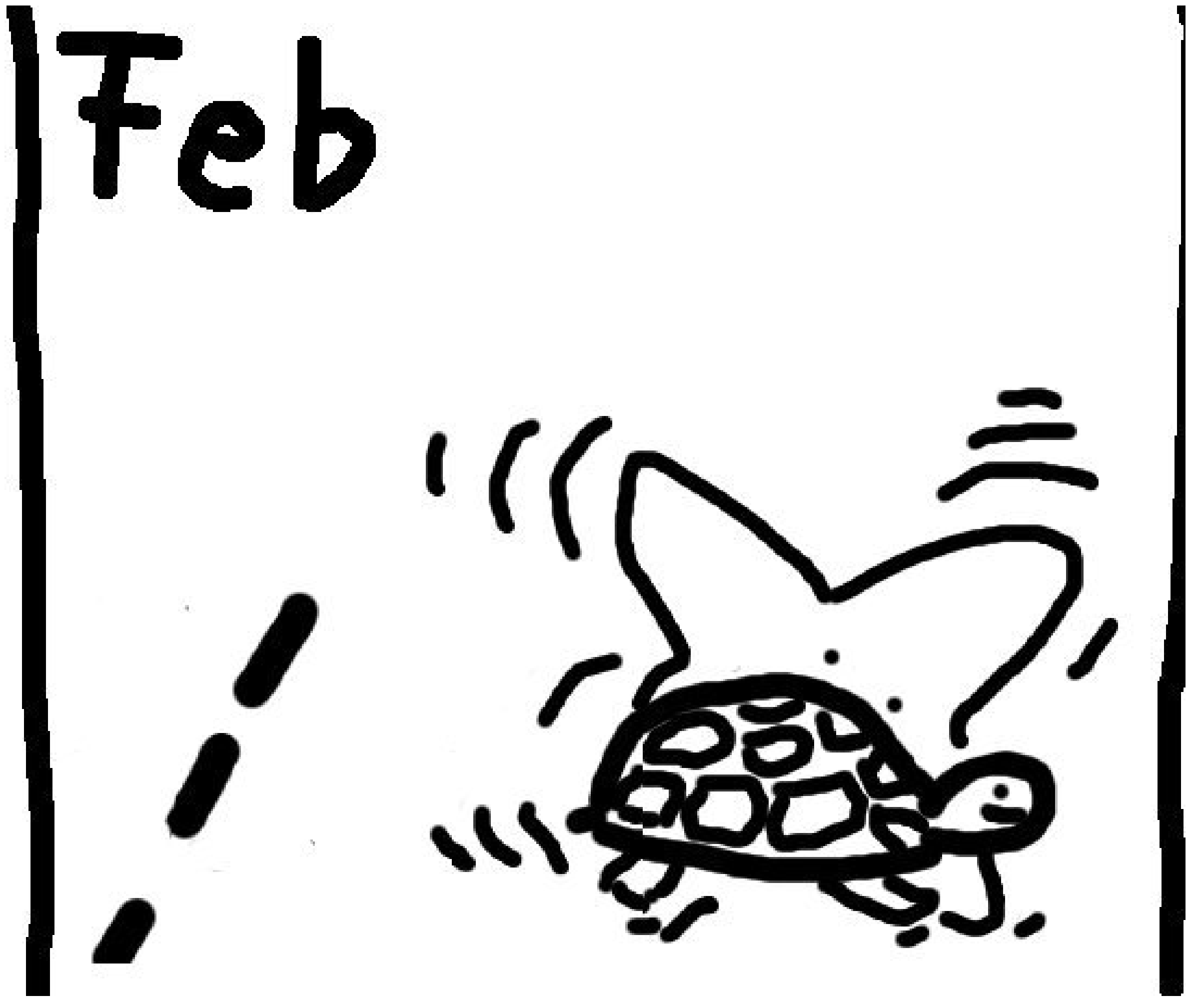




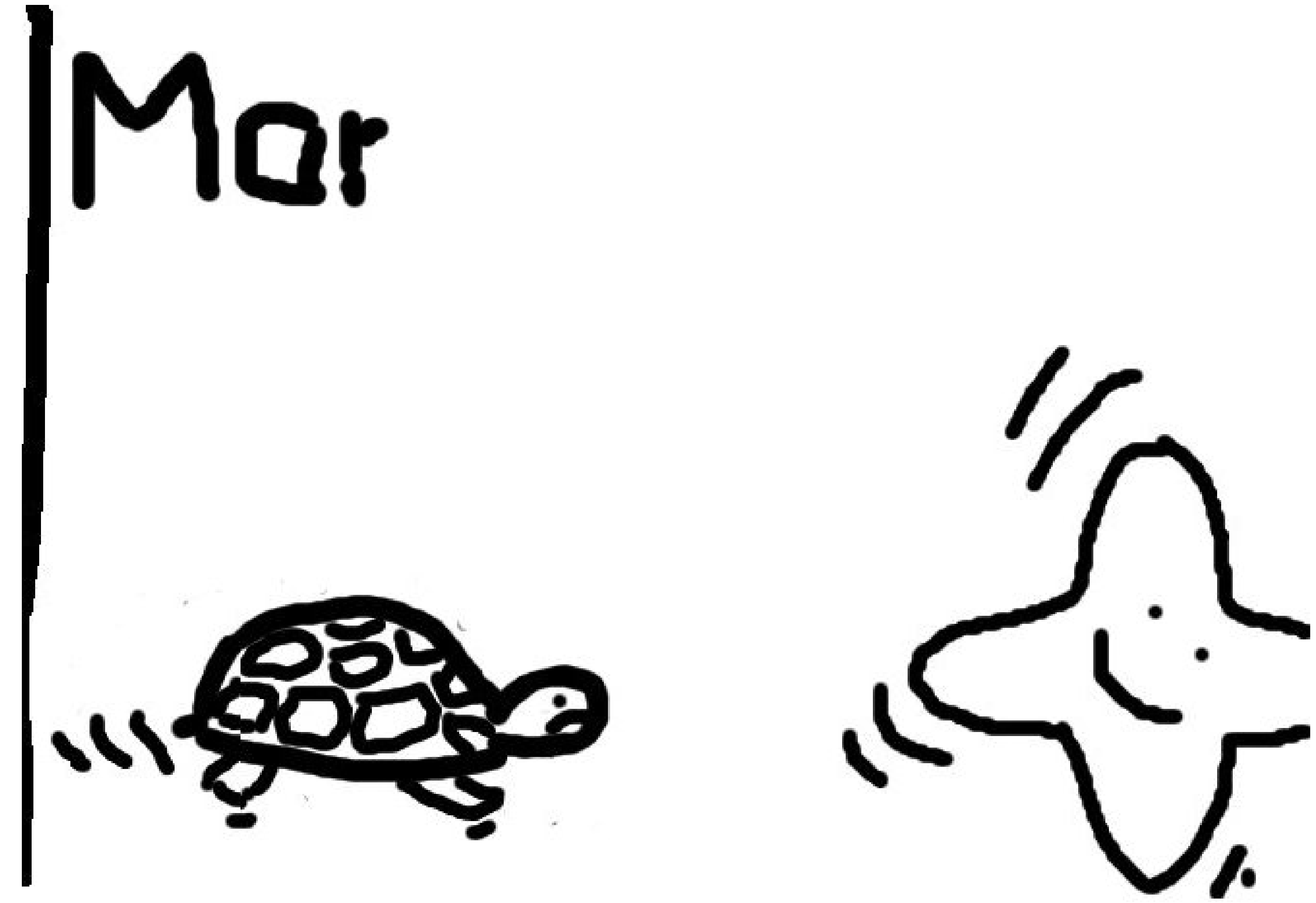
Exciting progress: Edwards about to overtake!!



And the winner is: Edwards!



Exciting progress: Edwards about to overtake!!



And the winner is: Edwards!