Models of Elliptic Curves

Daniel J. Bernstein
University of Illinois at Chicago
djb@cr.yp.to

and

Tanja Lange
Technische Universiteit Eindhoven
tanja@hyperelliptic.org

26.03.2009

Elliptic curves I

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

How to turn this into an equation?
How to use this definition for computations involving elliptic curves?

Elliptic curves I

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

How to turn this into an equation?
How to use this definition for computations involving elliptic curves?

Use Riemann-Roch theorem! This implies

$$\ell(D) \geq \deg(D) - g + 1,$$

with equality if $\deg(D) > 2g - 2$
where $L(D) = \{f \in K(C) | \operatorname{div}(f) \geq -D\}$, $\ell(D) = \dim(L(D))$
and C/K is a curve of genus g.

Elliptic curves I

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

How to turn this into an equation?
How to use this definition for computations involving elliptic curves?

Use Riemann-Roch theorem! This implies

$$\ell(D) \geq \deg(D) - g + 1,$$

with equality if $\deg(D) > 2g - 2 = 2 \cdot 1 - 2 = 0$
where $L(D) = \{f \in K(C) | \mathrm{div}(f) \geq -D\}$, $\ell(D) = \dim(L(D))$
and C/K is a curve of genus g.

Elliptic curves II

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

Call this point P_∞.

Riemann-Roch theorem for $g = 1$ gives equality for $\deg(D) > 0$, i.e. $\ell(D) = \deg(D) - g + 1$, and thus

$$\ell(P_\infty) \;=\; \deg(P_\infty) - 1 + 1 = 1,$$

Elliptic curves II

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

Call this point P_∞.

Riemann-Roch theorem for $g = 1$ gives equality for $\deg(D) > 0$, i.e. $\ell(D) = \deg(D) - g + 1$, and thus

$$\begin{aligned} \ell(P_\infty) &= \deg(P_\infty) - 1 + 1 = 1, \\ \ell(2P_\infty) &= \deg(2P_\infty) - 1 + 1 = 2, \Rightarrow \exists x \in L(2P_\infty)\backslash K, \end{aligned}$$

Elliptic curves II

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

Call this point P_∞.

Riemann-Roch theorem for $g = 1$ gives equality for $\deg(D) > 0$, i.e. $\ell(D) = \deg(D) - g + 1$, and thus

$$
\begin{aligned}
\ell(P_\infty) &= \deg(P_\infty) - 1 + 1 = 1, \\
\ell(2P_\infty) &= \deg(2P_\infty) - 1 + 1 = 2, \Rightarrow \exists x \in L(2P_\infty) \backslash K, \\
\ell(3P_\infty) &= \deg(3P_\infty) - 1 + 1 = 3, \Rightarrow \exists y \in L(3P_\infty) \backslash L(2P_\infty),
\end{aligned}
$$

Elliptic curves II

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

Call this point P_∞.

Riemann-Roch theorem for $g = 1$ gives equality for $\deg(D) > 0$, i.e. $\ell(D) = \deg(D) - g + 1$, and thus

$$
\begin{aligned}
\ell(P_\infty) &= \deg(P_\infty) - 1 + 1 = 1, \\
\ell(2P_\infty) &= \deg(2P_\infty) - 1 + 1 = 2, \Rightarrow \exists x \in L(2P_\infty) \backslash K, \\
\ell(3P_\infty) &= \deg(3P_\infty) - 1 + 1 = 3, \Rightarrow \exists y \in L(3P_\infty) \backslash L(2P_\infty), \\
\ell(4P_\infty) &= 4, \; L(4P_\infty) = \langle 1, x, y, x^2 \rangle,
\end{aligned}
$$

Elliptic curves II

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

Call this point P_∞.

Riemann-Roch theorem for $g = 1$ gives equality for $\deg(D) > 0$, i.e. $\ell(D) = \deg(D) - g + 1$, and thus

$$\begin{aligned}
\ell(P_\infty) &= \deg(P_\infty) - 1 + 1 = 1, \\
\ell(2P_\infty) &= \deg(2P_\infty) - 1 + 1 = 2, \Rightarrow \exists x \in L(2P_\infty)\backslash K, \\
\ell(3P_\infty) &= \deg(3P_\infty) - 1 + 1 = 3, \Rightarrow \exists y \in L(3P_\infty)\backslash L(2P_\infty), \\
\ell(4P_\infty) &= 4,\ L(4P_\infty) = \langle 1, x, y, x^2 \rangle, \\
\ell(5P_\infty) &= 5,\ L(5P_\infty) = \langle 1, x, y, x^2, xy \rangle,
\end{aligned}$$

Elliptic curves II

Geometric definition:
An elliptic curve E/K is a smooth, projective curve of genus 1 with a K-rational point.

Call this point P_∞.

Riemann-Roch theorem for $g = 1$ gives equality for $\deg(D) > 0$, i.e. $\ell(D) = \deg(D) - g + 1$, and thus

$$\begin{aligned}
\ell(P_\infty) &= \deg(P_\infty) - 1 + 1 = 1,\\
\ell(2P_\infty) &= \deg(2P_\infty) - 1 + 1 = 2, \Rightarrow \exists x \in L(2P_\infty) \backslash K,\\
\ell(3P_\infty) &= \deg(3P_\infty) - 1 + 1 = 3, \Rightarrow \exists y \in L(3P_\infty) \backslash L(2P_\infty),\\
\ell(4P_\infty) &= 4,\ L(4P_\infty) = \langle 1, x, y, x^2 \rangle,\\
\ell(5P_\infty) &= 5,\ L(5P_\infty) = \langle 1, x, y, x^2, xy \rangle,\\
\ell(6P_\infty) &= 6,\ \{1, x, y, x^2, xy, x^3, y^2\} \text{ are linearly dependent.}
\end{aligned}$$

Weierstrass form

$\ell(6P_\infty) = 6,\ \{1, x, y, x^2, xy, x^3, y^2\}$ are linearly dependent,

i.e. there exist $a_1, a_2, a_3, a_4, a_6 \in K$ with

$$E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$$

so that the equation is nonsingular. (Can make equation monic in y^2 and x^3.)

This form is called Weierstrass form and is the standard normal form of elliptic curves.

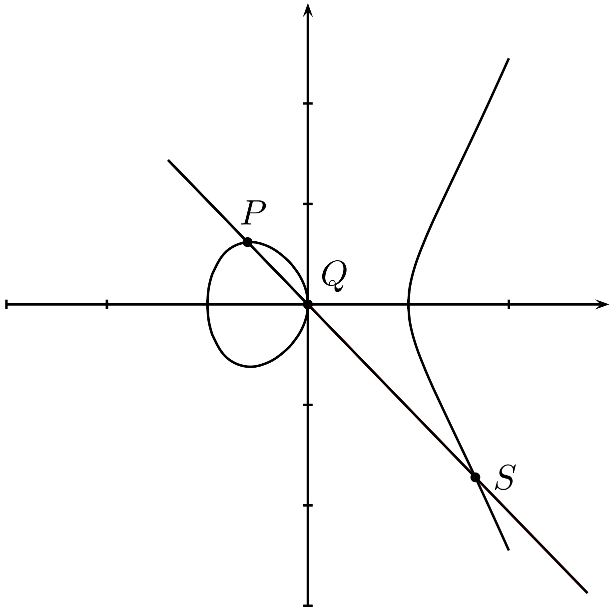
Applications in cryptography, the elliptic curve method of factorization, elliptic curve primality proving, etc. use that points on curve form a group.

Arithmetic on Weierstrass curves

- Divisor class group (of degree 0), i.e. divisors of degree 0 modulo principal divisors, is way to define a group from a given curve.
- Divisors are equivalent if they differ by a principal divisor.
- Turn the curve into an abelian group by using isomorphism between divisor class group and points.
- Each divisor class has representative $P - P_\infty$ or 0; assign point $D + P_\infty$, i.e. $P - P_\infty + P_\infty = P$ or $0 + P_\infty = P_\infty$.
- Divisor class arithmetic translates to well-known geometric addition formulas.

Chord-and-tangent method

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Line $y = \lambda x + \mu$ has slope

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}.$$

Equating gives

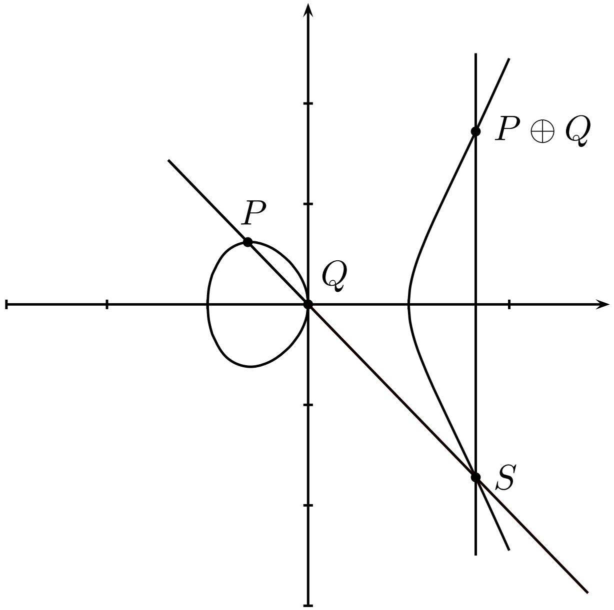
$$(\lambda x + \mu)^2 = x^3 + a_4 x + a_6.$$

This equation has 3 solutions, the x-coordinates of P, Q and S, thus

$$\begin{aligned}(x - x_P)(x - x_Q)(x - x_S) &= x^3 - \lambda^2 x^2 + (a_4 - 2\lambda\mu)x + a_6 - \mu^2 \\ x_S &= \lambda^2 - x_P - x_Q\end{aligned}$$

Chord-and-tangent method

$$E: y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Point P is on line, thus

$y_P = \lambda x_P + \mu$, i.e.
$\mu = y_P - \lambda x_P$,

and

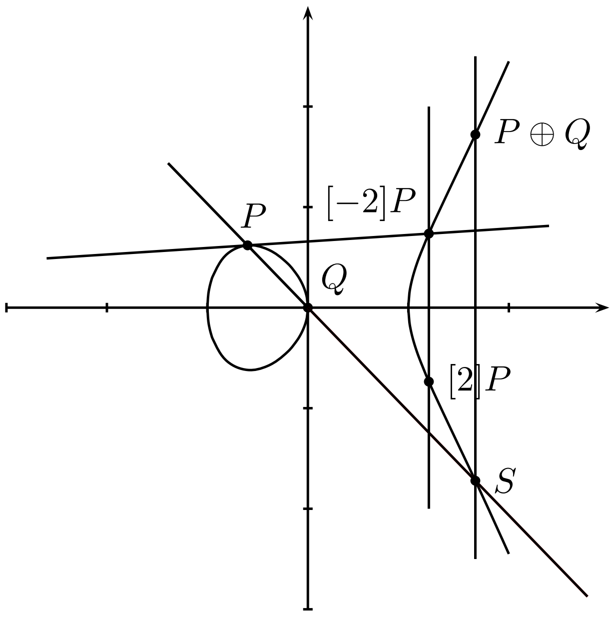
$$\begin{aligned} y_S &= \lambda x_S + \mu \\ &= \lambda x_S + y_P - \lambda x_P \\ &= \lambda(x_S - x_P) + y_P \end{aligned}$$

Point $P \oplus Q$ has the same x-coordinate as S but negative y-coordinate:

$$x_{P\oplus Q} = \lambda^2 - x_P - x_Q, \quad y_{P\oplus Q} = \lambda(x_P - x_{P\oplus Q}) - y_P$$

Chord-and-tangent method

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



When doubling, use tangent at P. Compute slope λ via partial derivatives of curve equation:

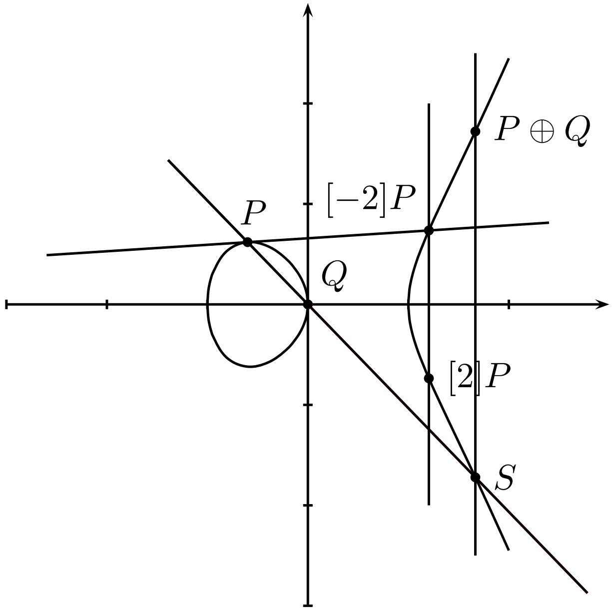
$$\lambda = \frac{3x_P^2 + a_4}{2y_P}.$$

Remaining computation identical to addition.

$$x_{[2]P} = \lambda^2 - 2x_P, \quad y_{[2]P} = \lambda(x_P - x_{[2]P}) - y_P$$

Chord-and-tangent method

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Tangent at Q is vertical $x = x_Q$.
When adding $P \oplus Q$ and S, connecting line is vertical.

Third point online is P_∞, a point infinitely far up on the y-axis:

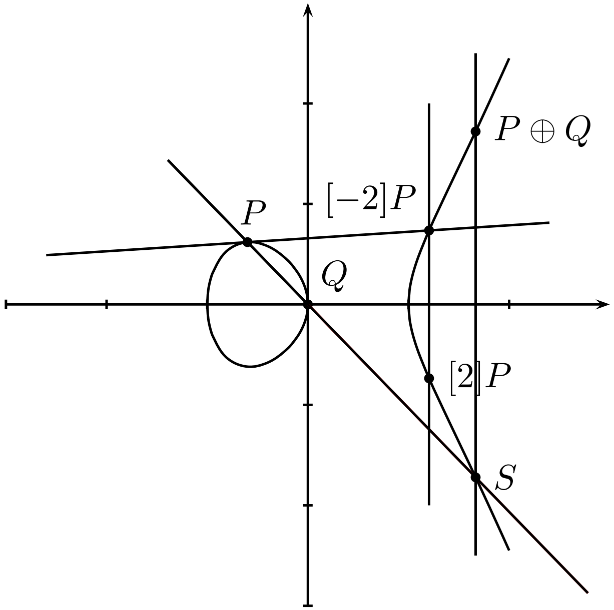
$$[2]Q = P_\infty; (P \oplus Q) \oplus S = P_\infty.$$

$$P \oplus P_\infty = P; P_\infty \oplus P_\infty = P_\infty.$$

P_∞ is neutral element; $-(x_1, y_1) = (x_1, -y_1)$.

Chord-and-tangent method

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



In general, for $(x_P, y_P) \neq (x_Q, -y_Q)$:

$$\begin{aligned}(x_P, y_P) \oplus (x_Q, y_Q) &= \\ &= (x_{P\oplus Q}, y_{P\oplus Q}) = \\ &= (\lambda^2 - x_P - x_Q, \lambda(x_P - x_{P\oplus Q}) - y_P),\end{aligned}$$

where

$$\lambda = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & \text{if } x_P \neq x_Q, \\ (3x_P^2 + a_4)/(2y_P) & \text{if } P = Q \end{cases}$$

…and all the other cases …

$P + P_\infty = P;\ P_\infty + P = P;\ P_\infty + P_\infty = P_\infty;\ P + (-P) = P_\infty$.

Total of 6 different cases. Not much better in projective coordinates.

Other curve shapes

Jacobi quartic

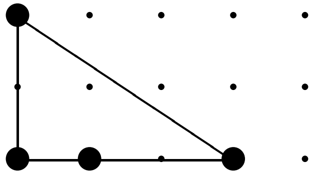
$$C : Y^2Z^2 = X^4 + 2aX^2Z^2 + Z^4$$

```
sage: x,y,z = PolynomialRing(QQ, 3, names='x,y,z').gens()
sage: C = Curve(y^2*z^2-(x^4-4*x^2*z^2+z^4))
sage: C.geometric_genus()
 1
sage: C.arithmetic_genus()
 3
```

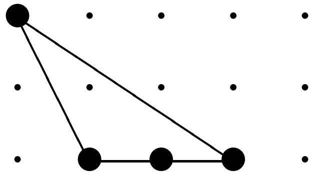
Point $(0 : 1 : 1) \in C(K)$, so C birationally equivalent to elliptic curve.

- Affine part is nonsingular but point at infinity is singular.
- With (x, y) also $(\pm x, \pm y)$ on curve; nontrivial map.
- How to define group law?
- What other shapes are there?

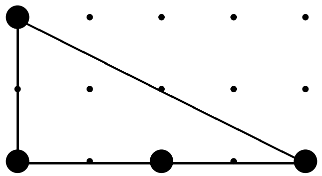
Newton Polygons, odd characteristic



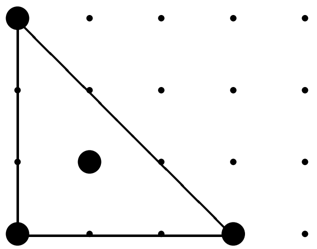
Short Weierstrass
$y^2 = x^3 + ax + b$



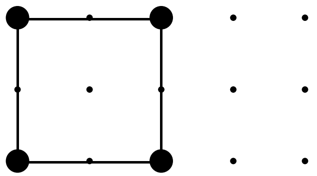
Montgomery
$by^2 = x^3 + ax^2 + x$



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



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



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

Number of integer points inside convex hull spanned by the exponents of the monomials gives the genus of the curve.

All these curves generically have genus 1.

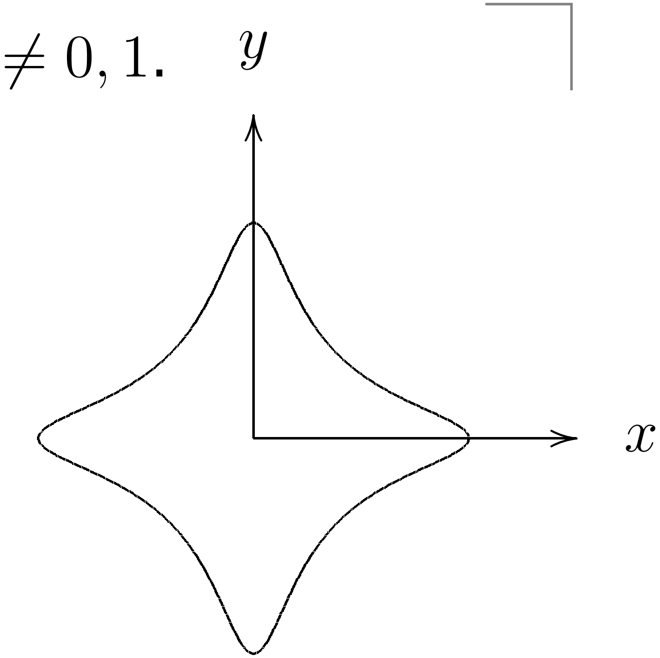
Edwards curves – because shape does matter

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$

Generalization covers more curves over k.

Associative operation on most points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law



$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order 2; $(1, 0)$ and $(-1, 0)$ have order 4.

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0,0)$. Then Weierstrass form:
$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$
- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.
- Addition on Edwards and Weierstrass corresponds.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\dfrac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \dfrac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $$P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$$
- $$[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\dfrac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \dfrac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Having addition law work for doubling removes some checks from the code.

Complete addition law

- Points at infinity blow up minimally over $k(\sqrt{d})$, so if d is not a square in k, then there are no points at infinity.
- If d is not a square, the only exceptional points of the birational equivalence are P_∞ corresponding to $(0,1)$ and $(0,0)$ corresponding to $(0,-1)$.
- If d is not a square the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.

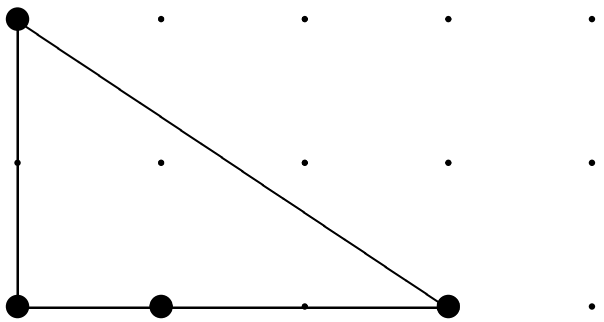
Fast addition law

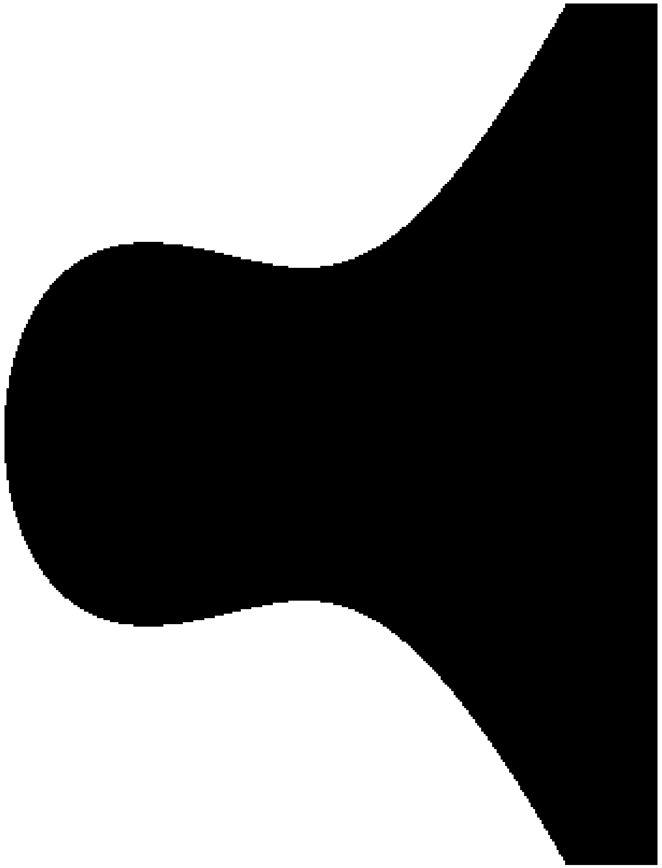
- Very fast point addition 10M + 1S + 1D. Even faster with Extended Edwards coordinates (Hisil et al.).
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature.
- For comparison: IEEE standard P1363 provides “the fastest arithmetic on elliptic curves” by using Jacobian coordinates on Weierstrass curves.
  - Point addition 12M + 4S.
  - Doubling formulas need only 4M + 4S.
- For more curve shapes, better algorithms (even for Weierstrass curves) and many more operations (mixed addition, re-addition, tripling, scaling,. . .) see
  `www.hyperelliptic.org/EFD`
  and the following competition.

Starring . . .

Weierstrass curve

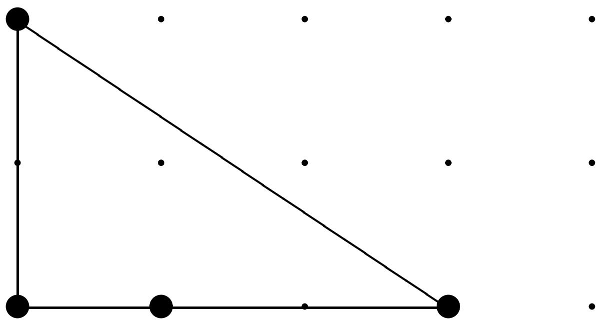
$$y^2 = x^3 - 0.4x + 0.7$$

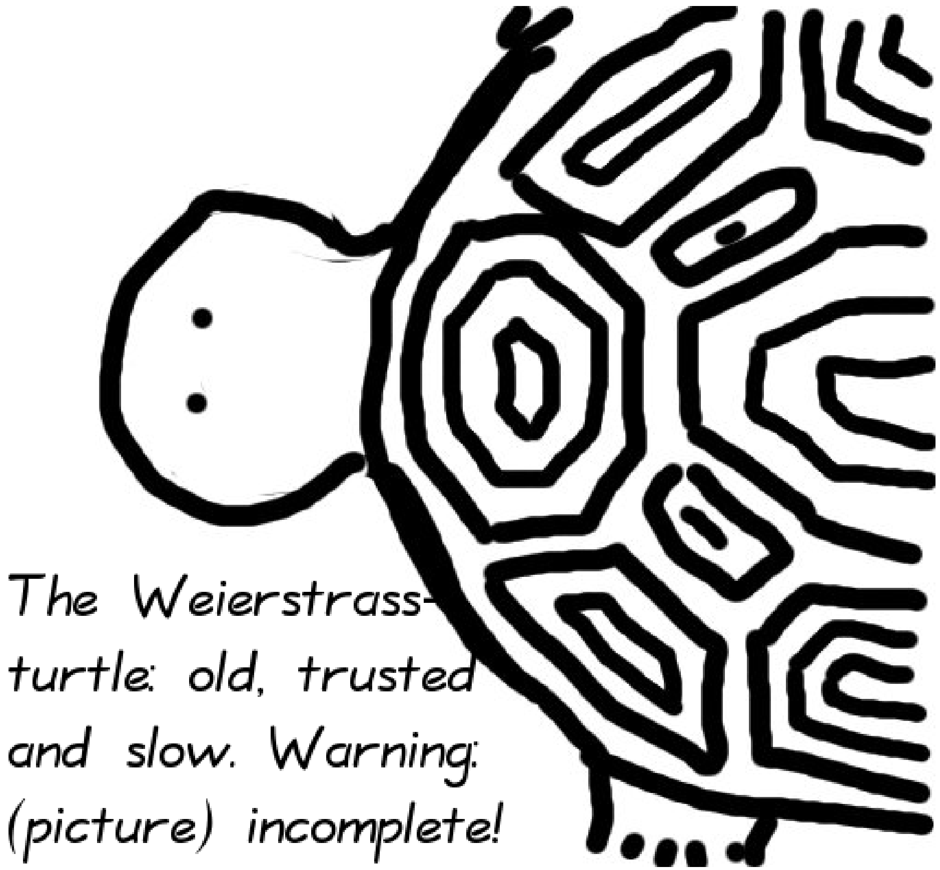




Weierstrass curve

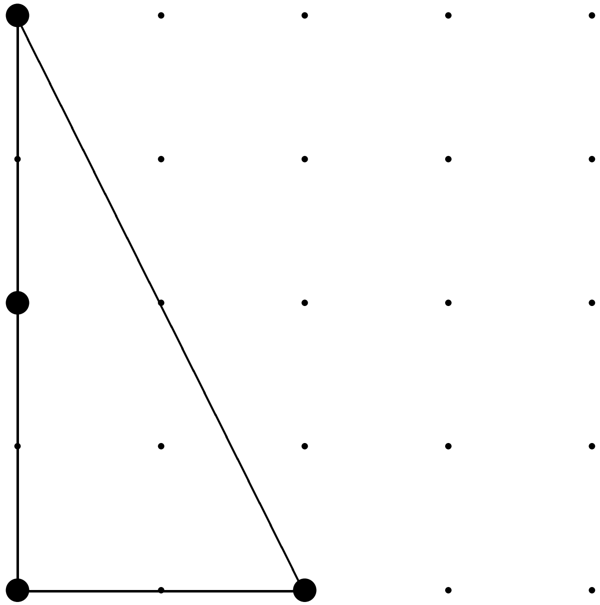
$$y^2 = x^3 - 0.4x + 0.7$$

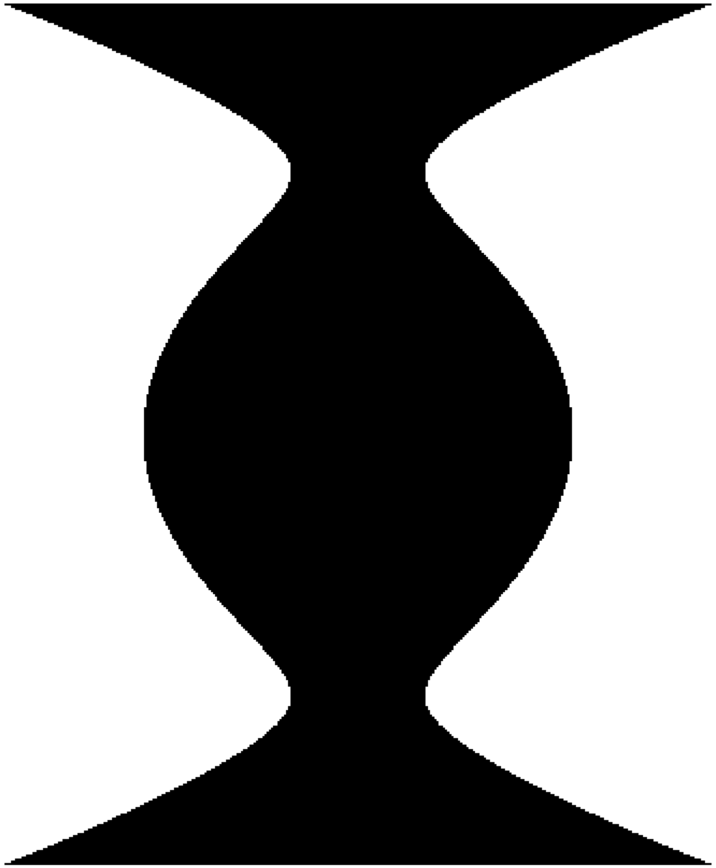




Jacobi quartic

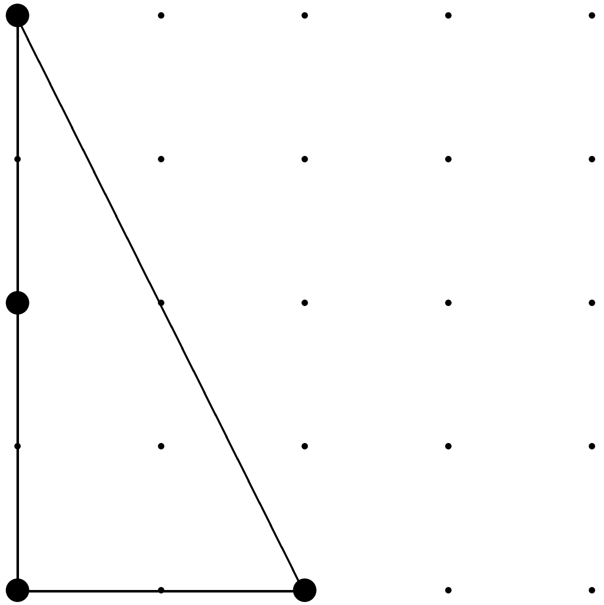
$x^2 = y^4 - 1.9y^2 + 1$

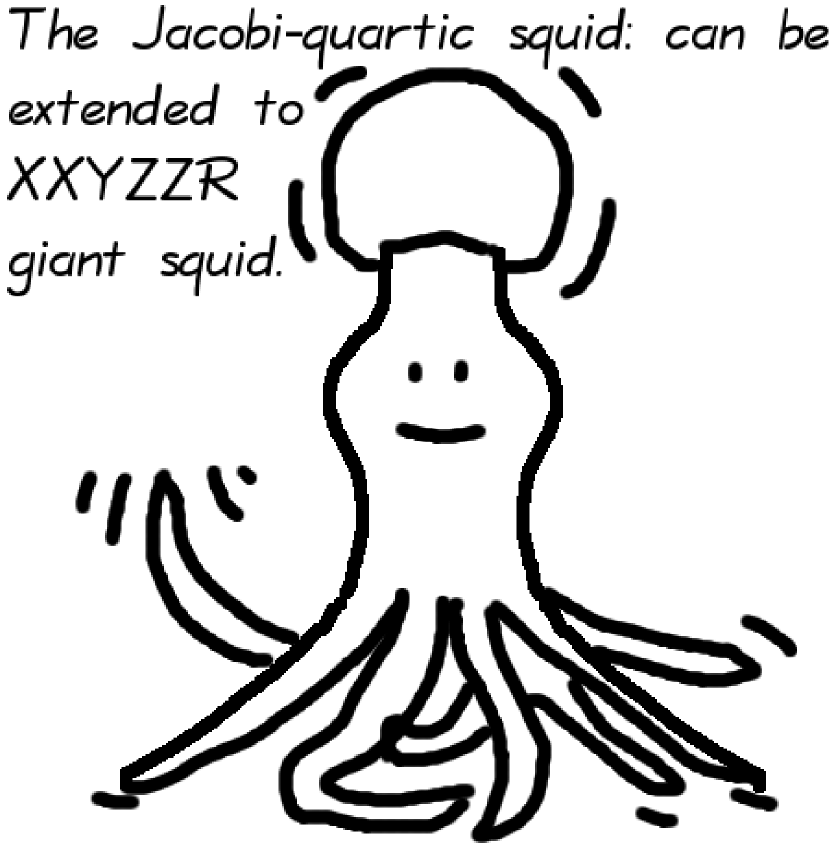




Jacobi quartic

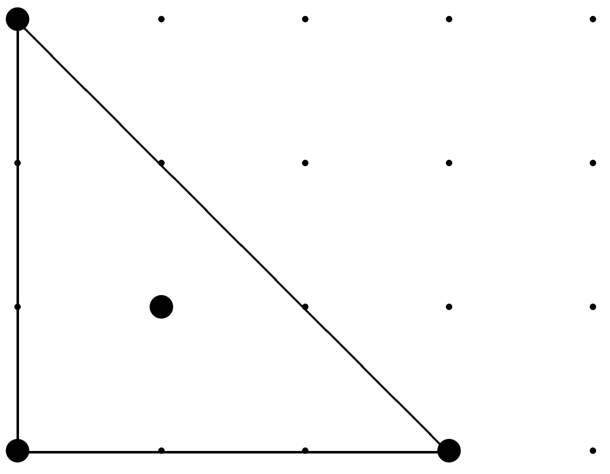
$$x^2 = y^4 - 1.9y^2 + 1$$

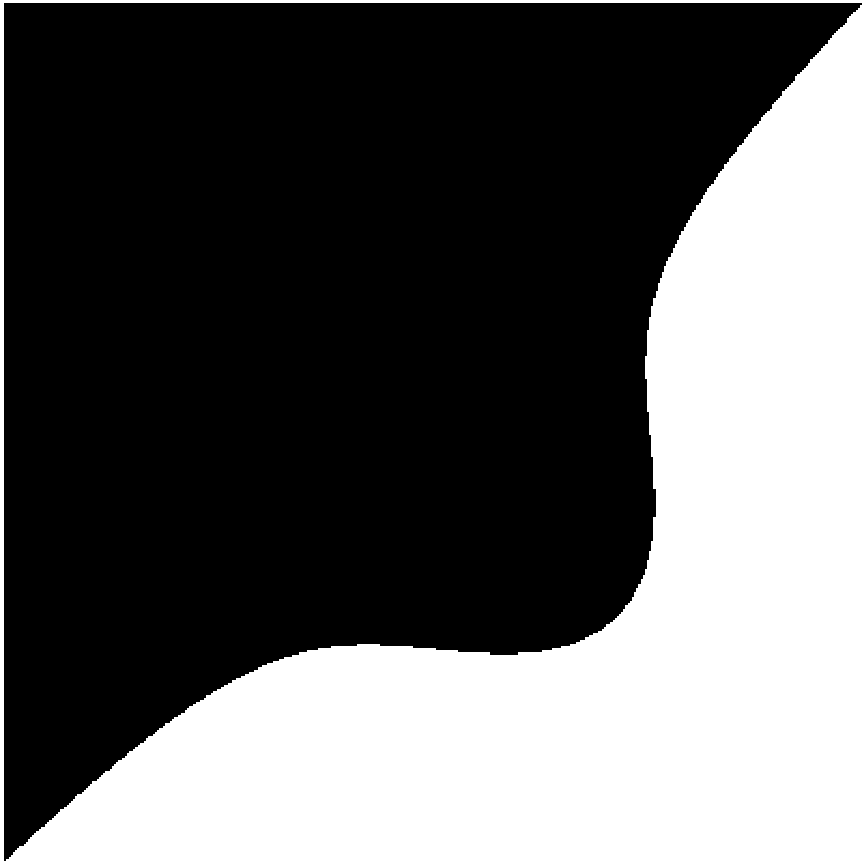




Hessian curve

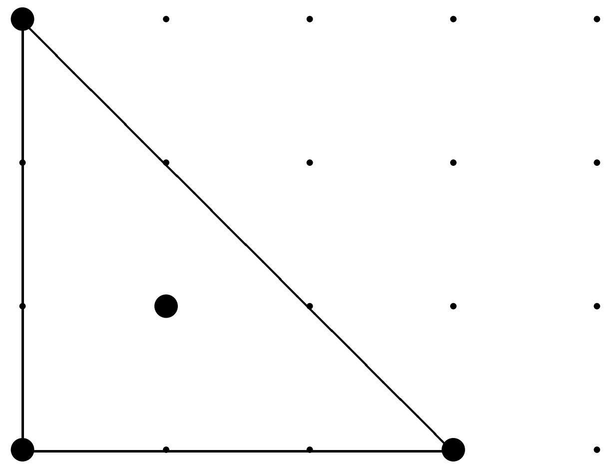
$$x^3 - y^3 + 1 = 0.3xy$$





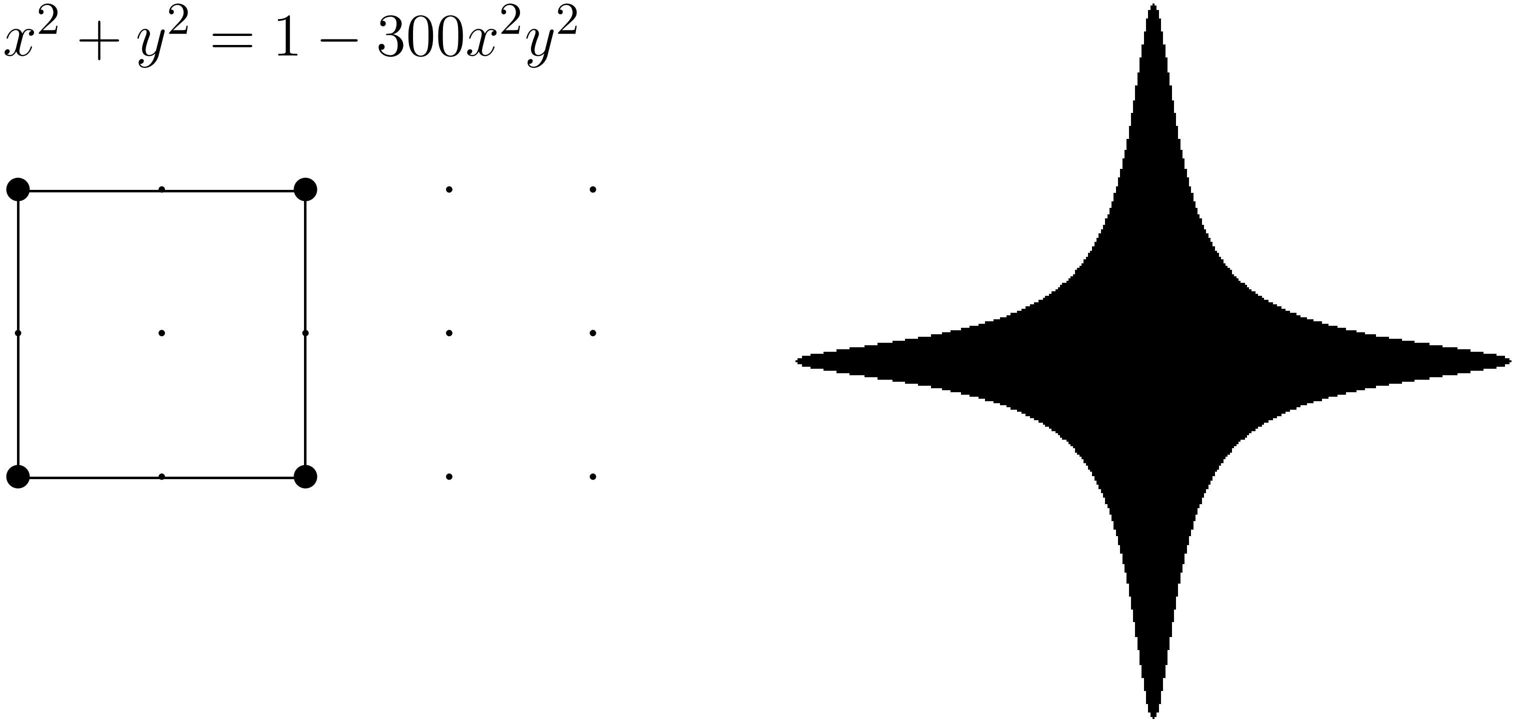
Hessian curve

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



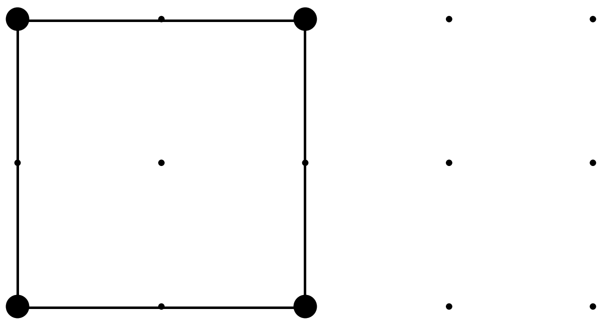
Edwards curve

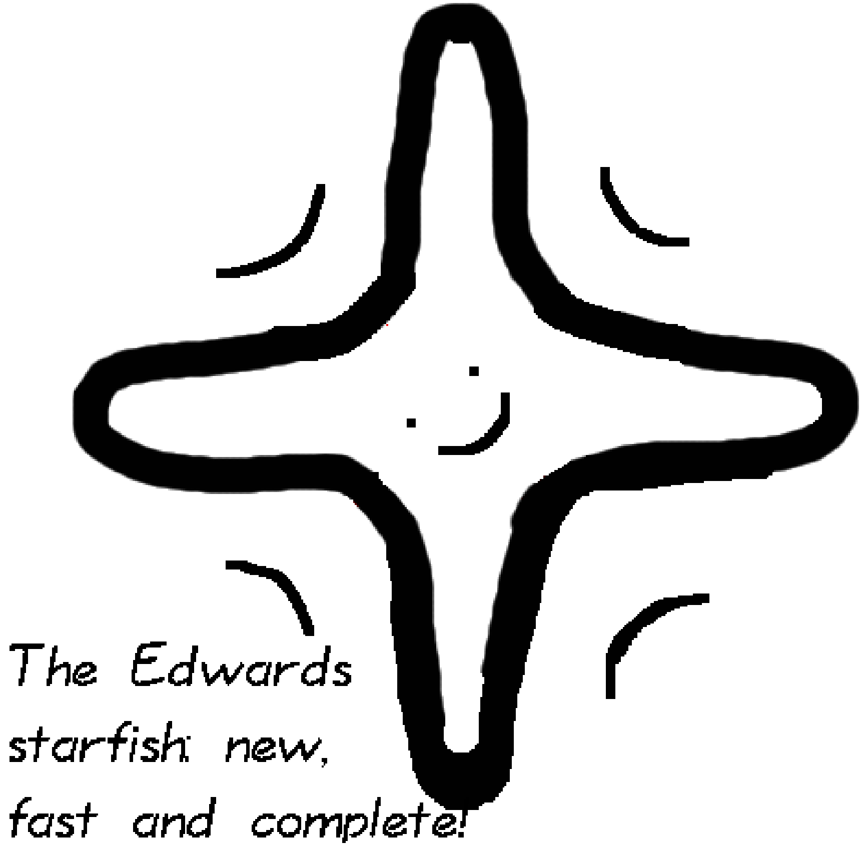
$x^2 + y^2 = 1 - 300x^2y^2$



Edwards curve

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

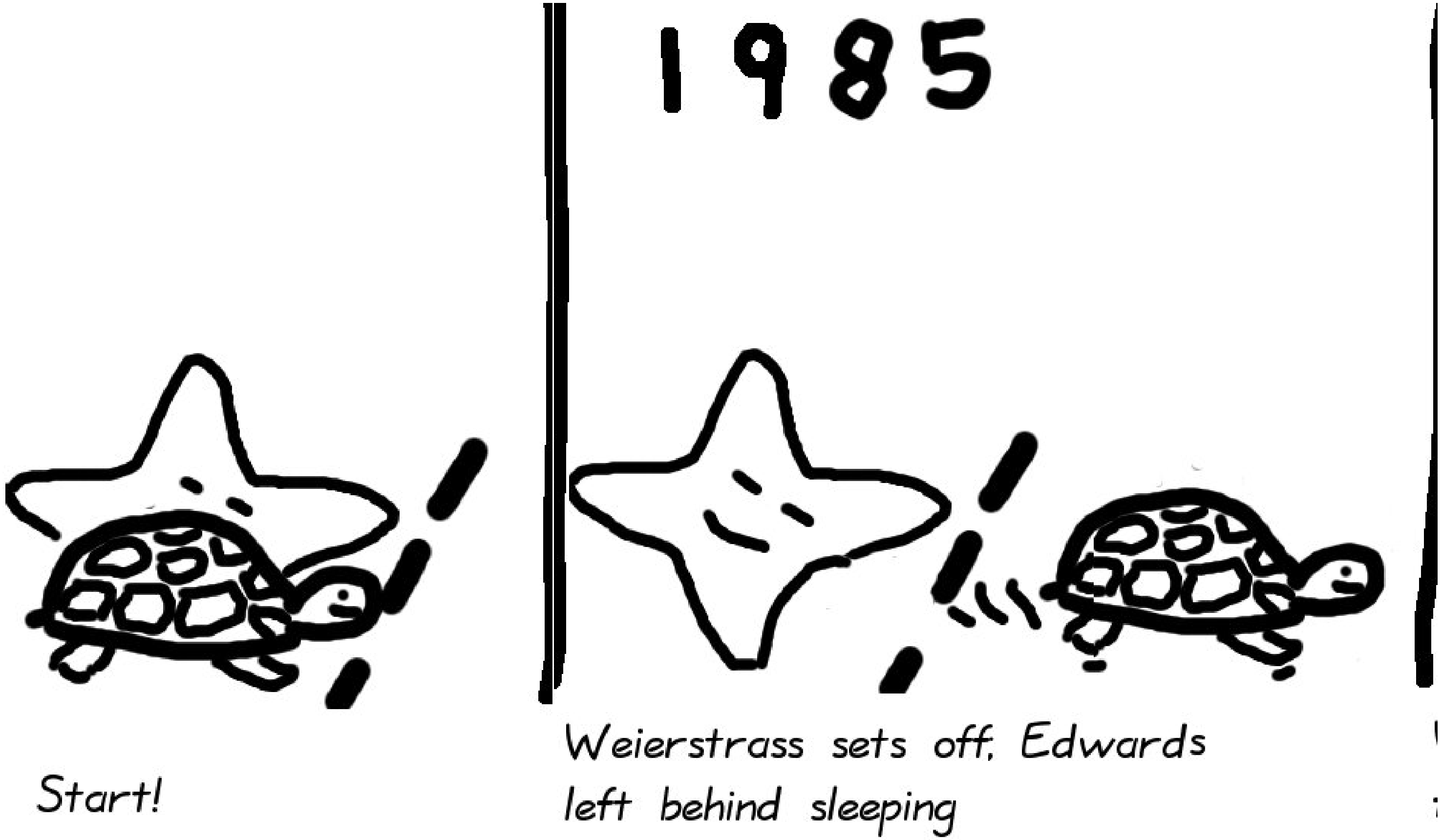




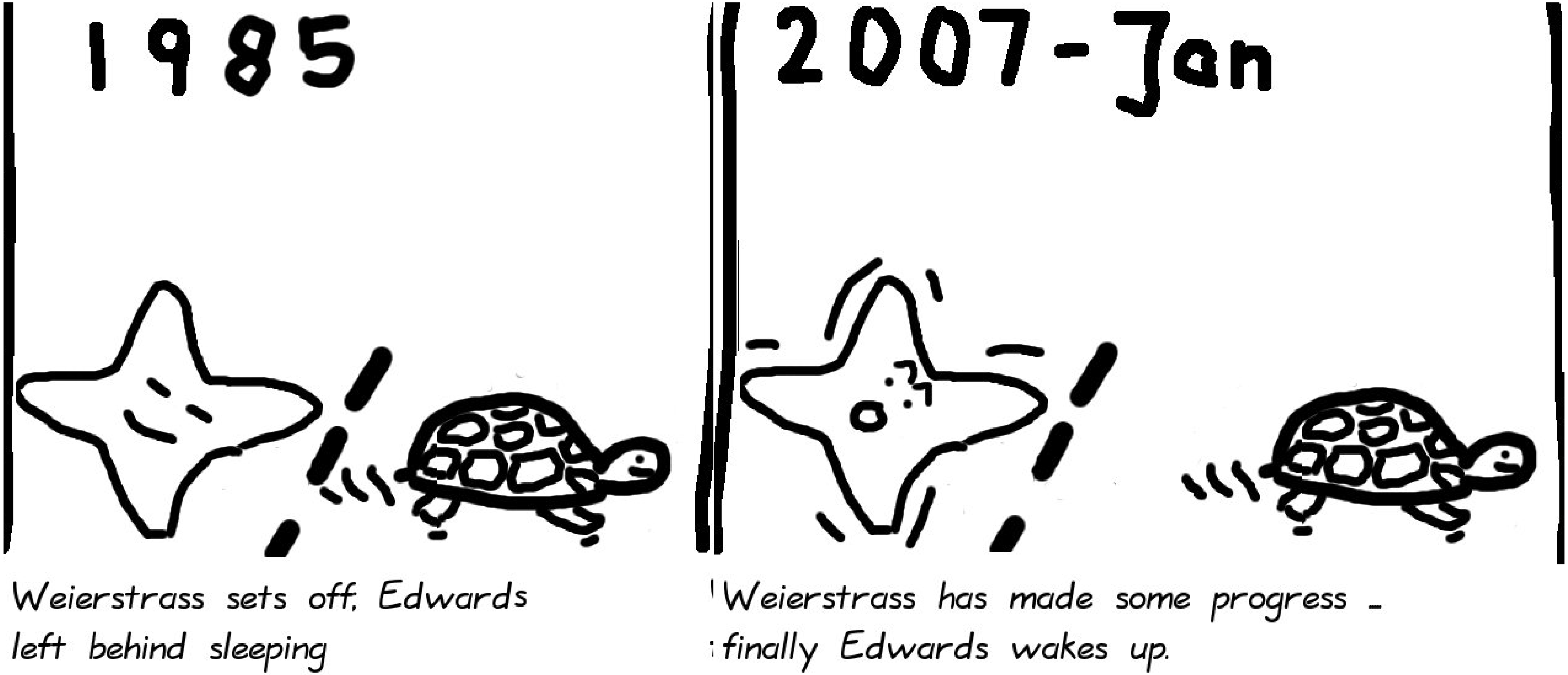
The race – zoom on Weierstrass and Edwards

Weierstrass vs. Edwards I

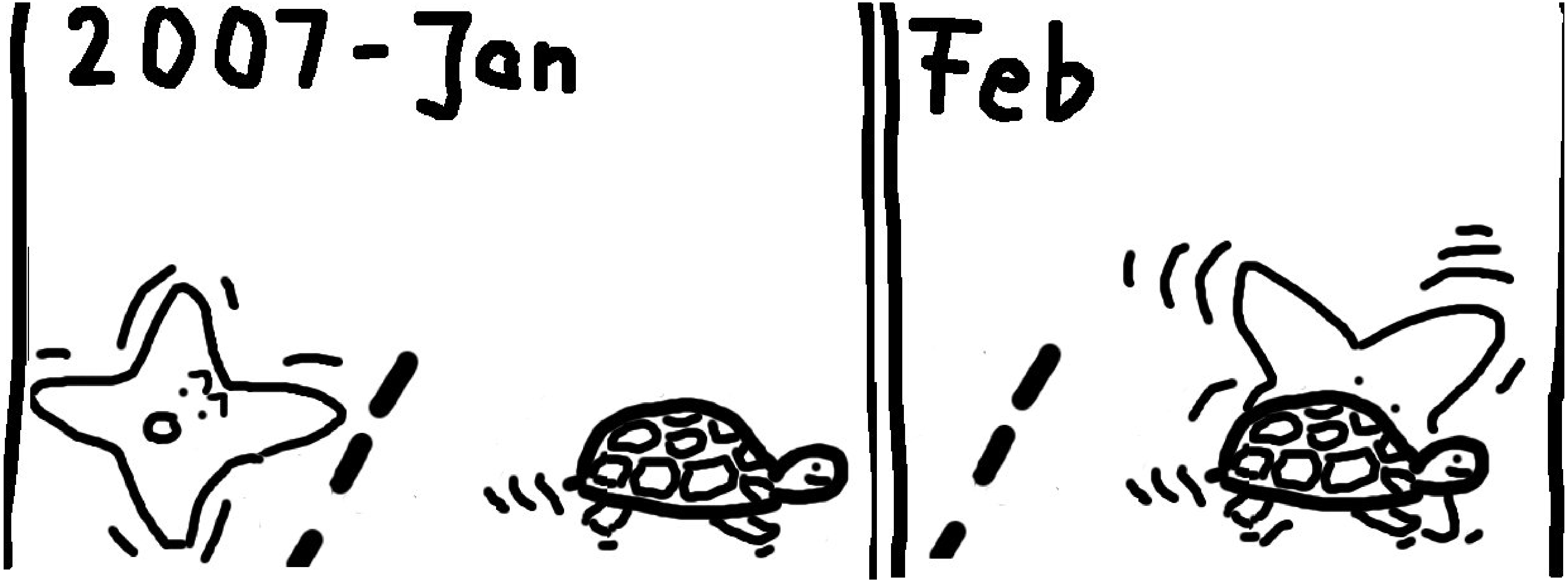
Weierstrass vs. Edwards II



Weierstrass vs. Edwards III



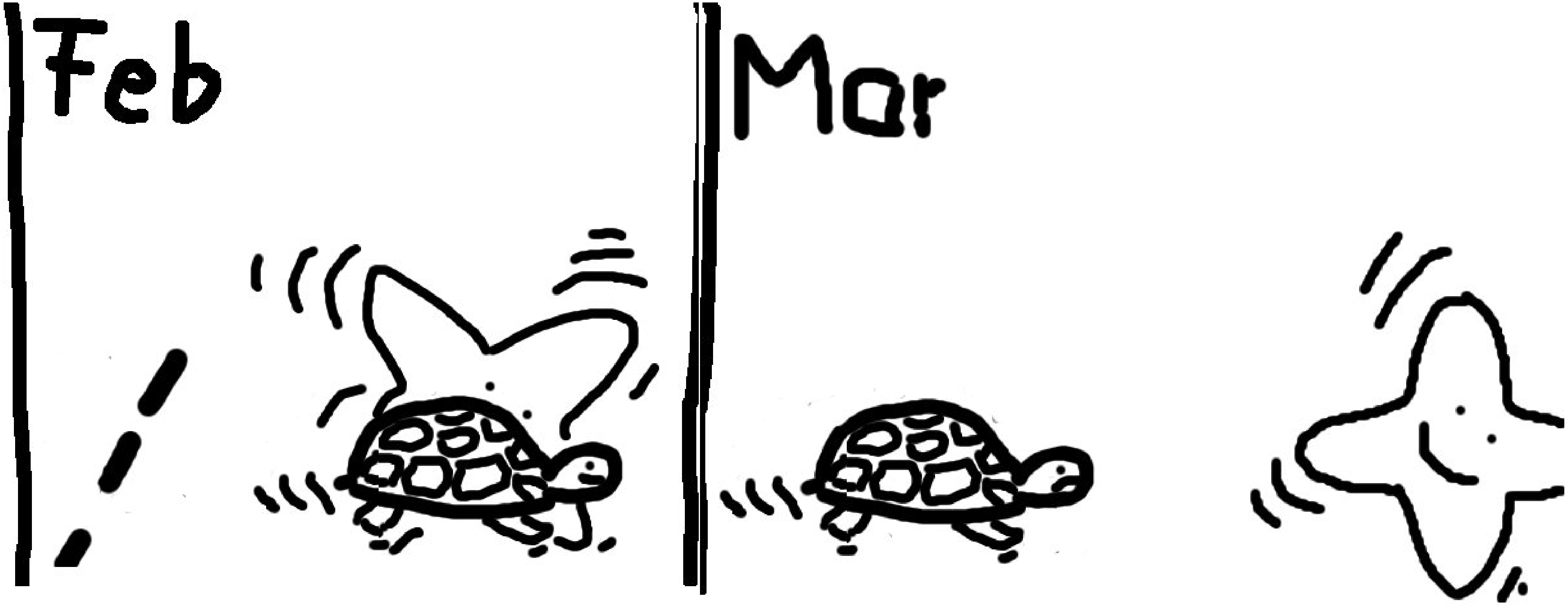
Weierstrass vs. Edwards IV



Weierstrass has made some progress – finally Edwards wakes up.

Exciting progress: Edwards about to overtake!!

Weierstrass vs. Edwards V



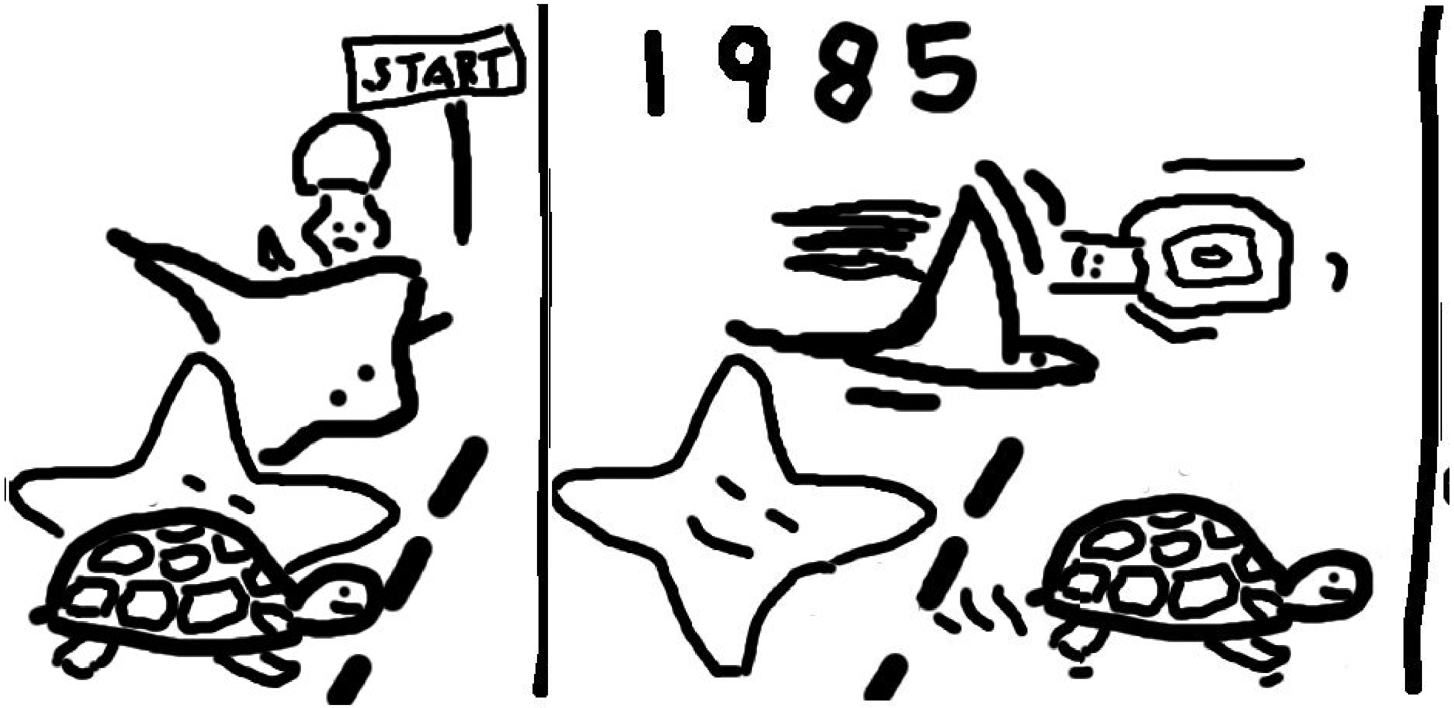
Exciting progress: Edwards about to overtake!!

And the winner is: Edwards!

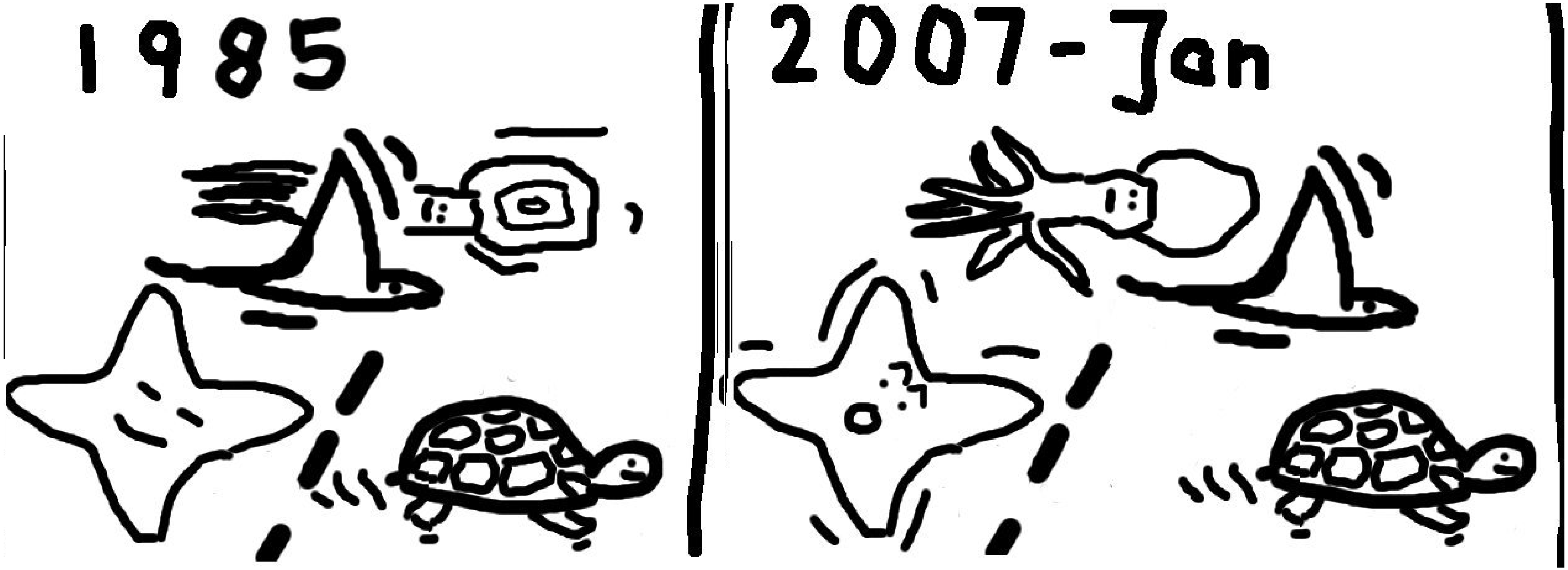
all competitors . . .

All competitors I

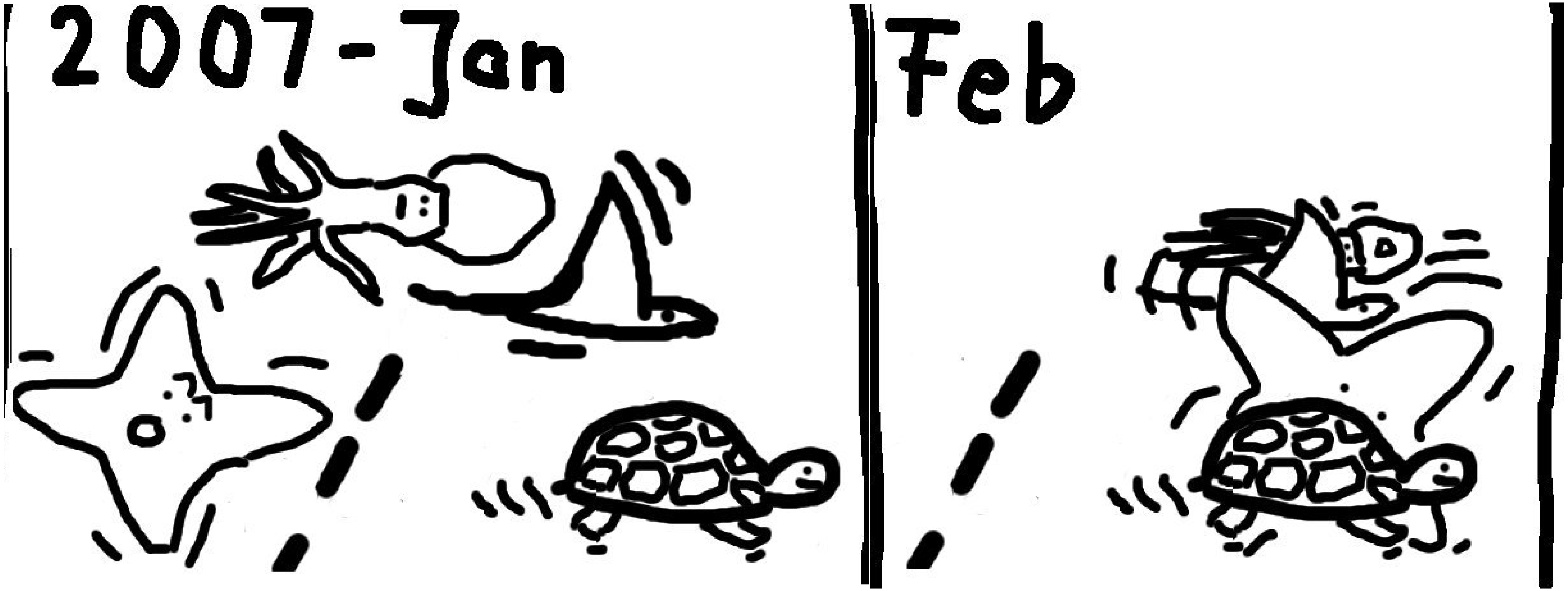
All competitors II



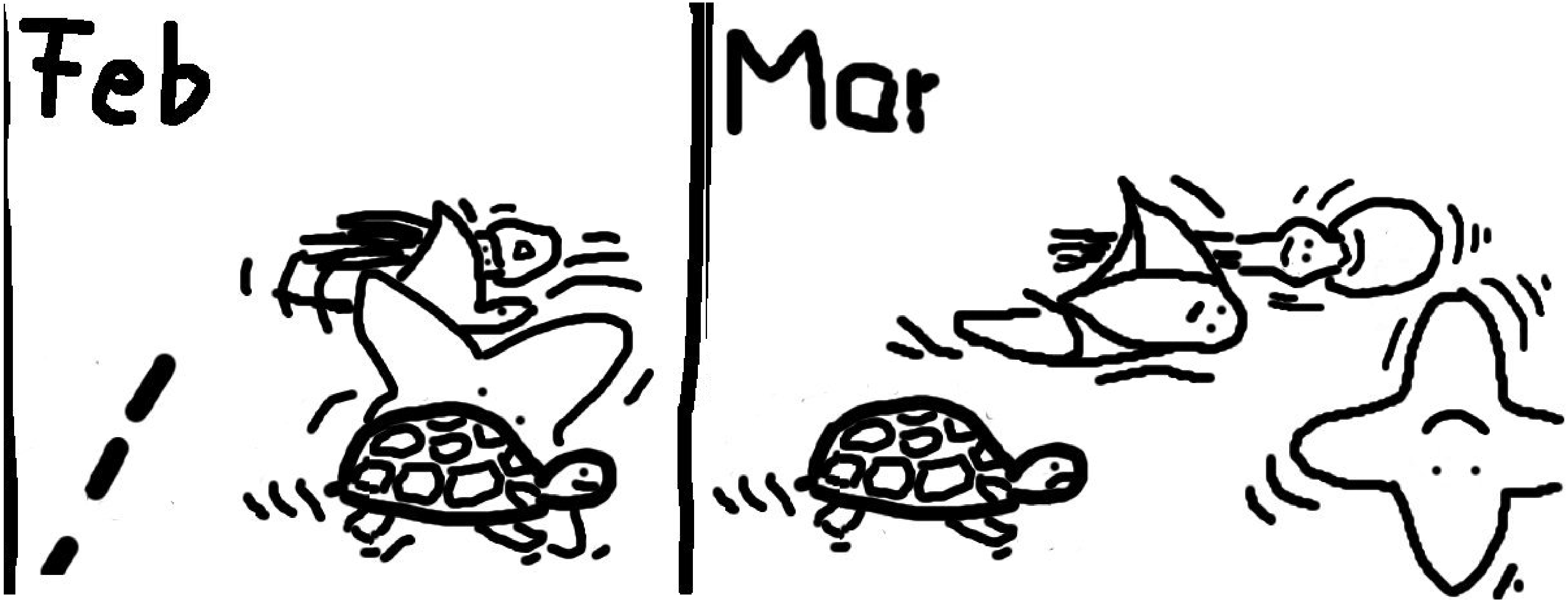
All competitors III



All competitors IV



All competitors V



Read the full story at:

`hyperelliptic.org/EFD`