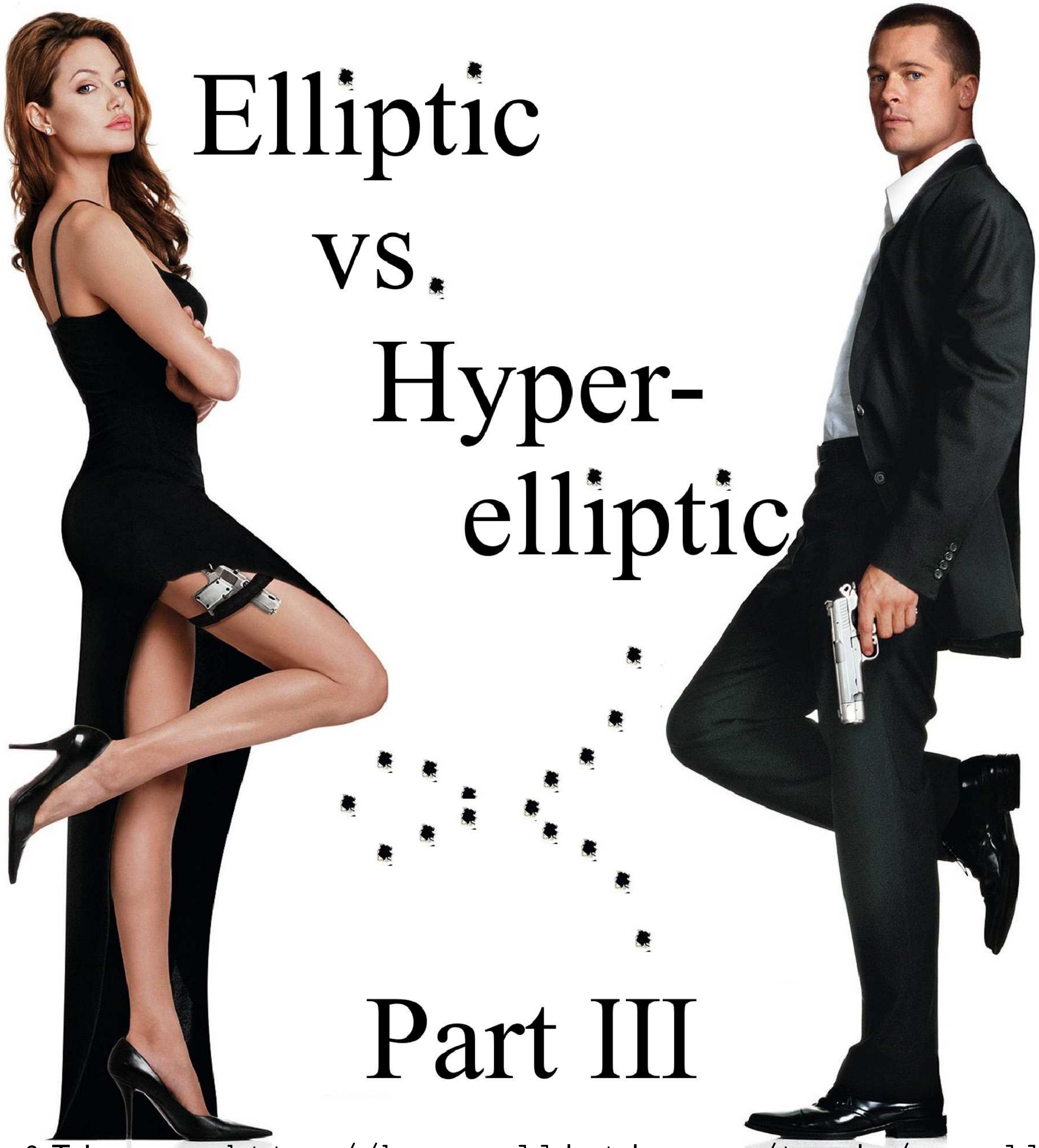
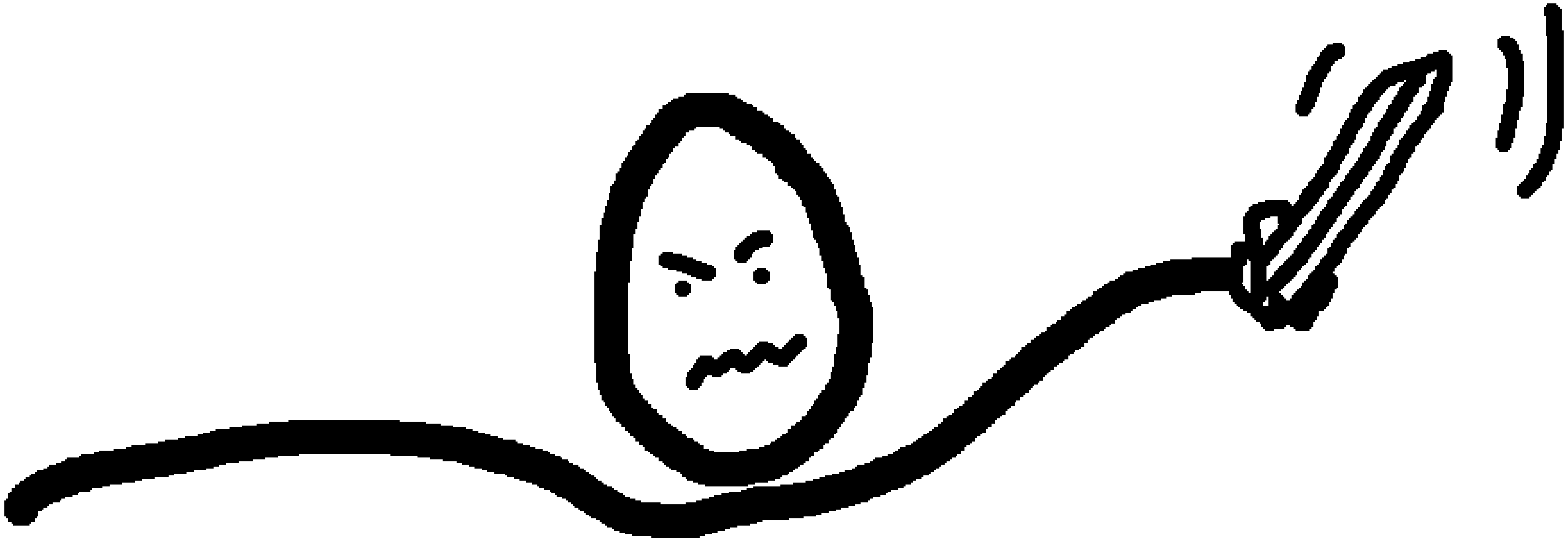


Elliptic vs. Hyper-elliptic

Part III

Elliptic strikes back

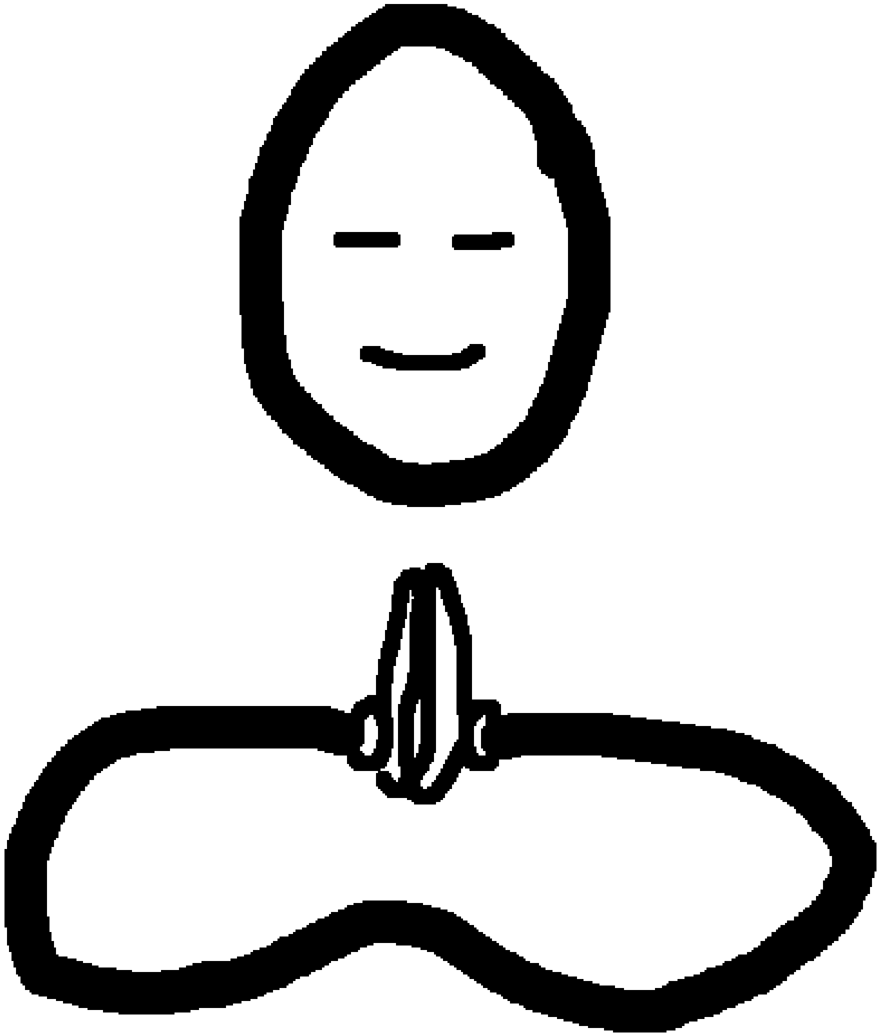


To face the challenge, to take the competition to a completely new level . . .

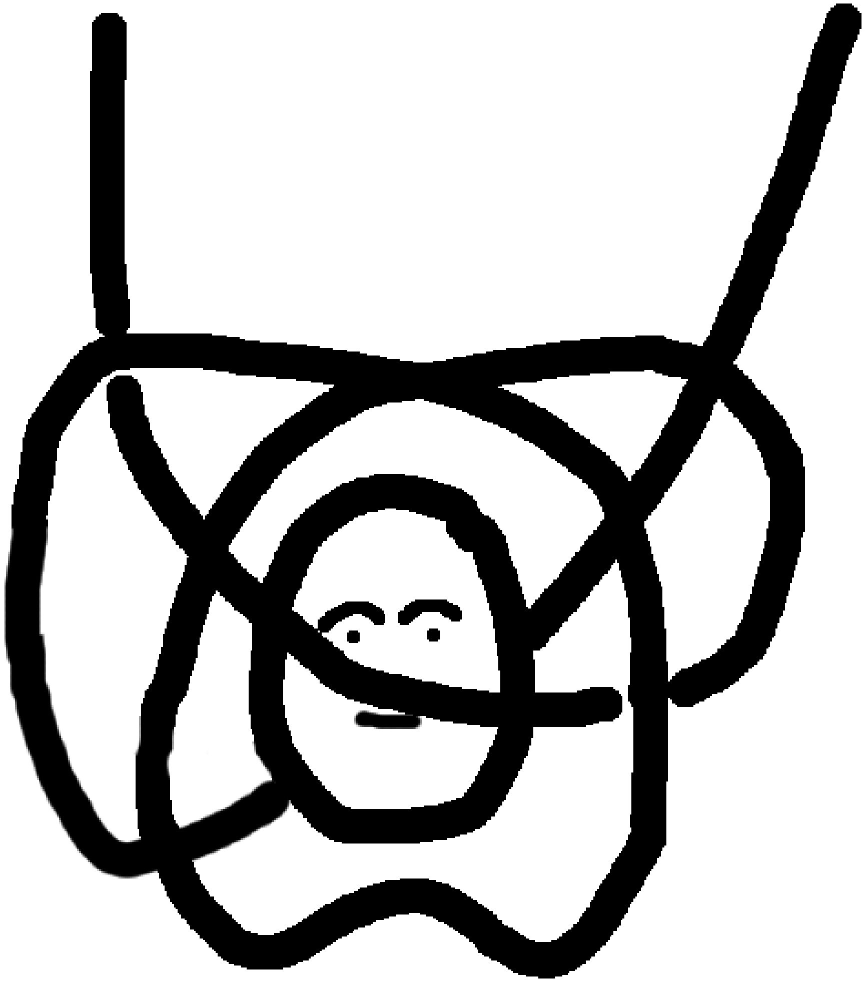
$$y^2 = x^3 + ax + b$$

…elliptic has to reconsider its form …

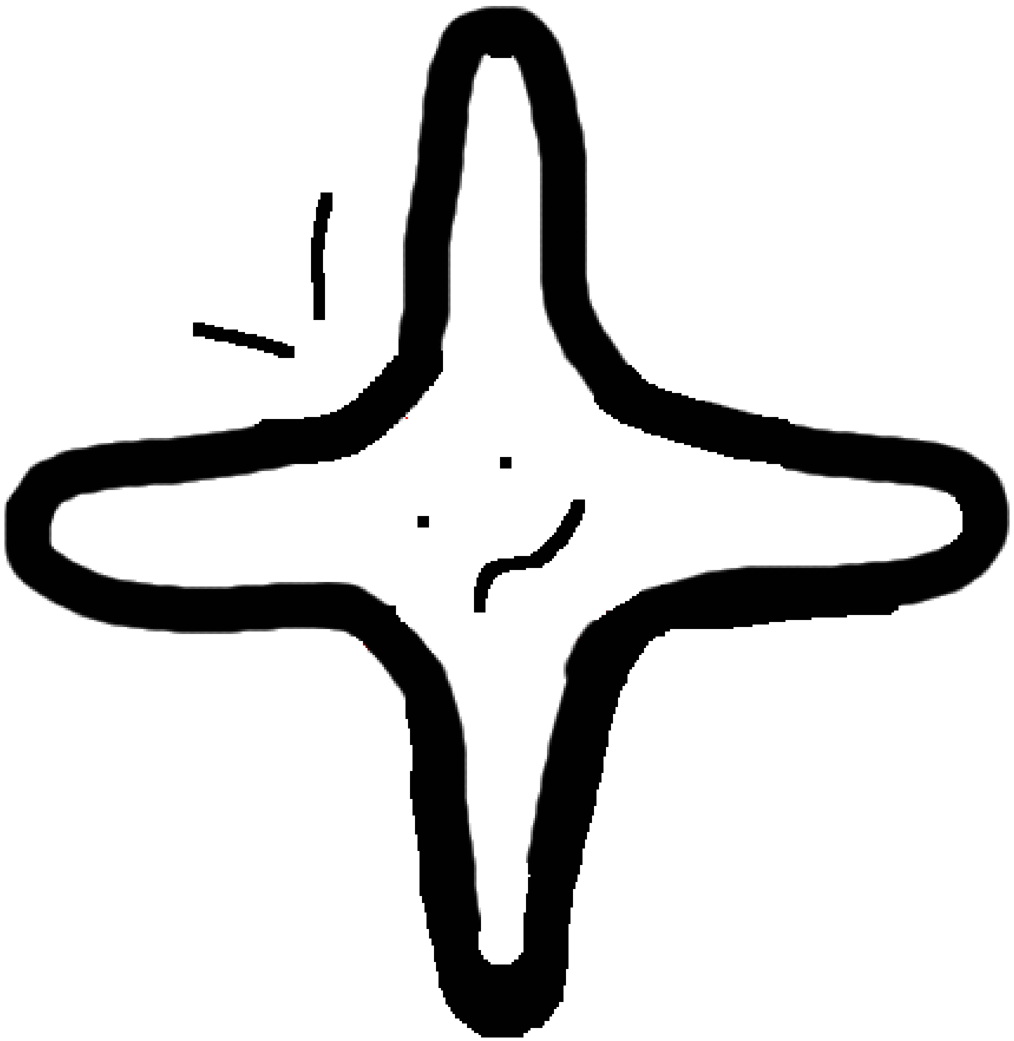
...has to abstract from its Weierstrass form ...



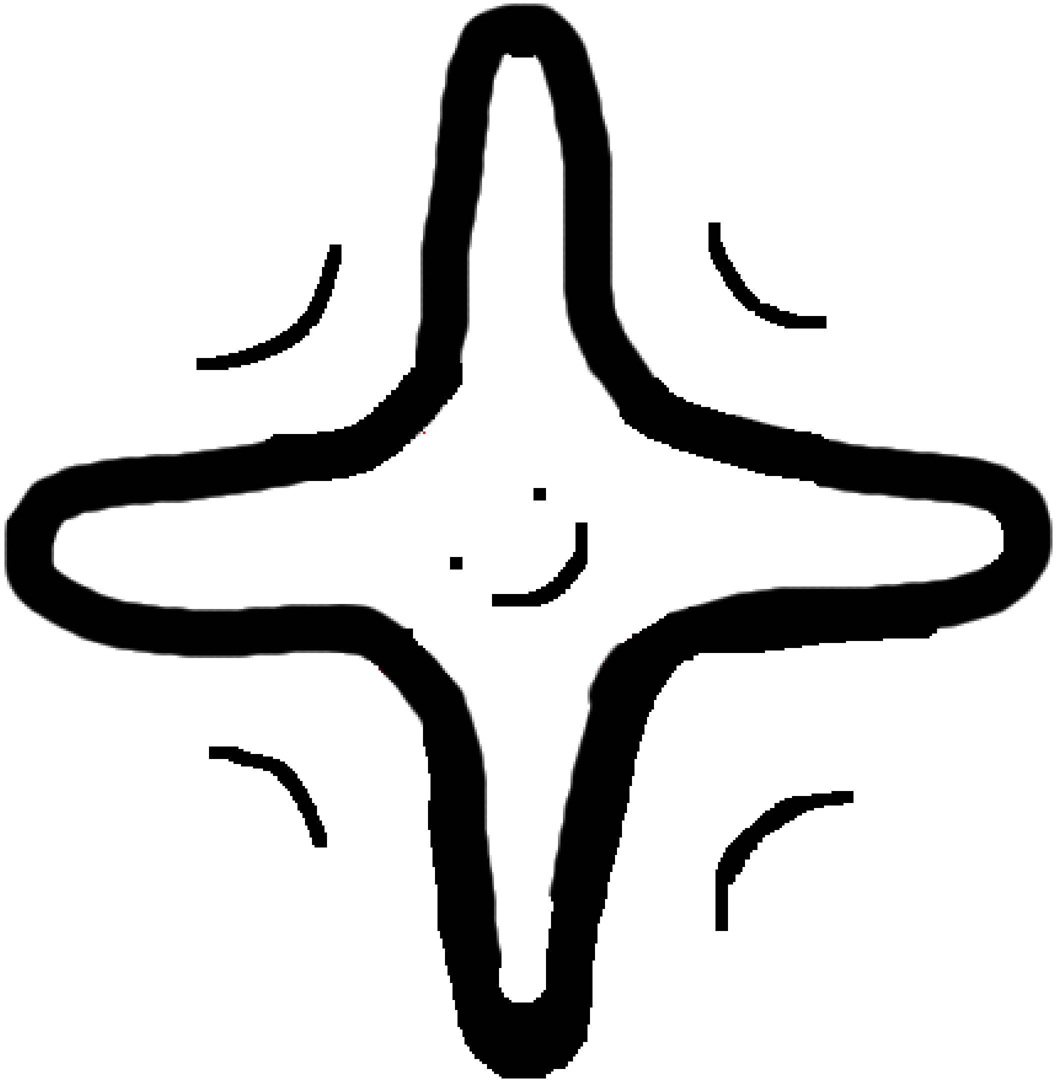
. . . has to undergo severe isomorphic transformations . . .



... until it finds ...



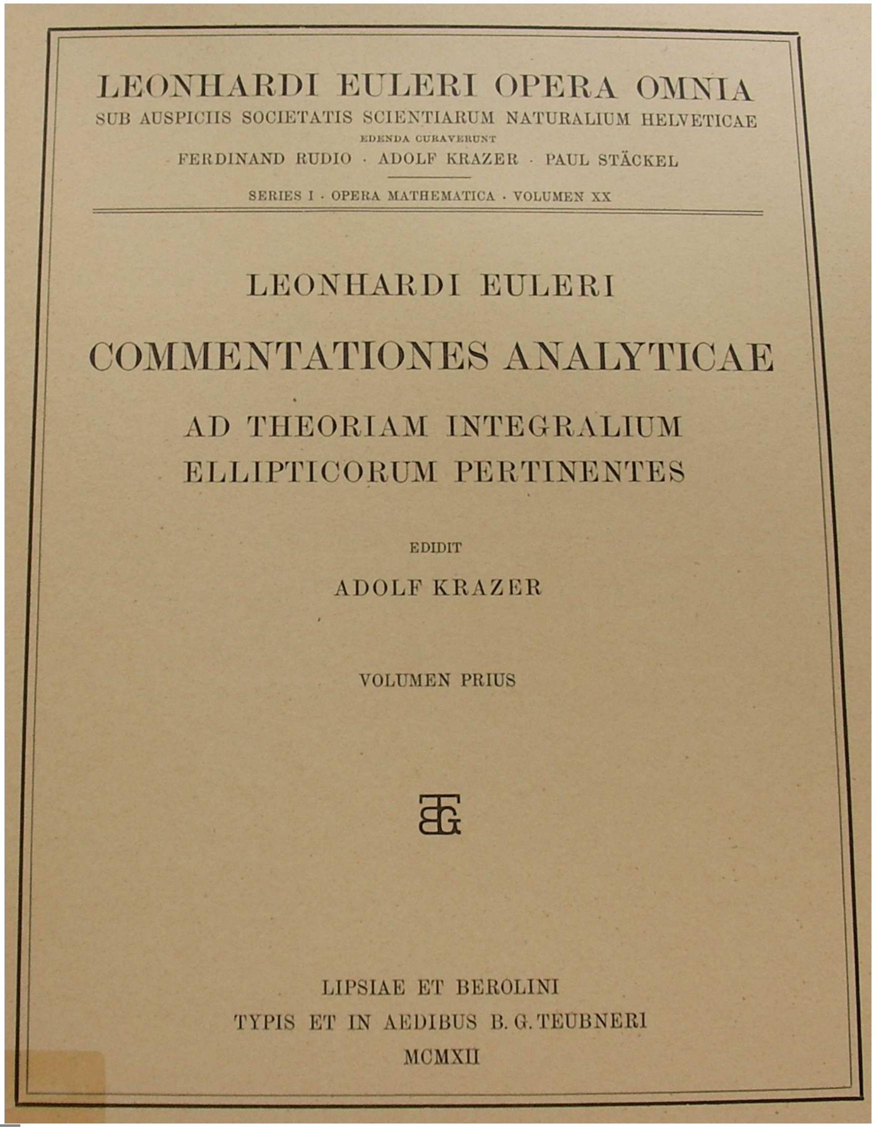
. . . its true . . .



. . . normal form!

$$x^2+y^2=c^2(1+dx^2y^2)$$

Long, long ago . . .



Euler 1761

“ Observationes de Comparatione Arcuum Curvarum Irrectificabilium”

I. DE ELLIPSI

1. Sit quadrans ellipticus ABC (Fig. 1), cuius centrum in C, eiusque semiaxes ponantur $CA = 1$ et $CB = c$; sumta ergo abscissa quacunque $CP = x$ erit applicata ei respondens $PM = y = c\sqrt{(1-xx)}$; cuius differentiale cum sit $dy = -\frac{cx\,dx}{\sqrt{(1-xx)}}$, erit abscissae $CP = x$ arcus ellipticus respondens

$$BM = \int \frac{dx\sqrt{(1-(1-cc)xx)}}{\sqrt{(1-xx)}}.$$

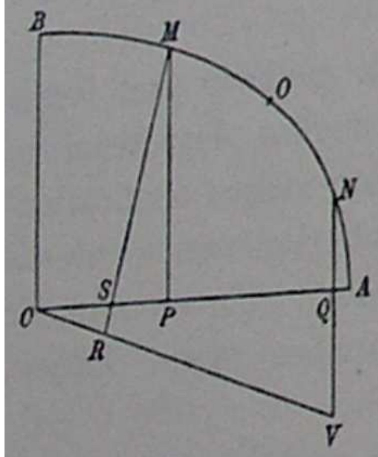


Fig. 1.

Ponatur brevitatis gratia $1 - cc = n$, ut sit arcus

$$BM = \int dx \boxed{\sqrt{\frac{1-nxx}{1-xx}}},$$

$$\frac{1}{y^2} = \frac{1-nx^2}{1-x^2} \Leftrightarrow x^2 + y^2 = 1 + nx^2y^2.$$

Euler 1761

COROLLARIUM 3

43. Inventio ergo cordarum arcuum quorumvis multiplorum una cum cordis complementi ita se habebit:

Corda arcus	Corda complementi
simpli $= a$	simpli $= A$
dupli $= b = \dfrac{2aA}{1 - aaAA}$	dupli $= \dfrac{AA - aa}{1 + aaAA} = B$
tripli $= c = \dfrac{aB + bA}{1 - abAB}$	tripli $= \dfrac{AB - ab}{1 + abAB} = C$
quadrupli $= d = \dfrac{aC + cA}{1 - acAC}$	quadrupli $= \dfrac{AC - ac}{1 + acAC} = D$
quintupli $= e = \dfrac{aD + dA}{1 - adAD}$	quintupli $= \dfrac{AD - ad}{1 + adAD} = E$
etc.	etc.

Euler gives doubling and (special) addition for (a, A) on $a^2 + A^2 = 1 - a^2A^2$.

Gauss, posthumously

ELEGANTIORES INTEGRALIS $\int \frac{dx}{\sqrt{(1-x^4)}}$ PROPRIETATES.

[2.]

$$1 = ss + cc + sscc \quad \text{sive} \quad 2 = (1+ss)(1+cc) = \left(\tfrac{1}{ss}-1\right)\left(\tfrac{1}{cc}-1\right)$$

$$s = \sqrt{\frac{1-cc}{1+cc}}, \qquad c = \sqrt{\frac{1-ss}{1+ss}}$$

$$\sin \operatorname{lemn}(a \pm b) = \frac{sc' \pm s'c}{1 \mp scs'c'}$$

$$\cos \operatorname{lemn}(a \pm b) = \frac{cc' \mp ss'}{1 \pm ss'cc'}$$

$$\sin \operatorname{lemn}(-a) = -\sin \operatorname{lemn} a, \qquad \cos \operatorname{lemn}(-a) = \cos \operatorname{lemn} a$$

$$\sin \operatorname{lemn} k\varpi = 0 \qquad \sin \operatorname{lemn}(k+\tfrac{1}{2})\varpi = \pm 1$$

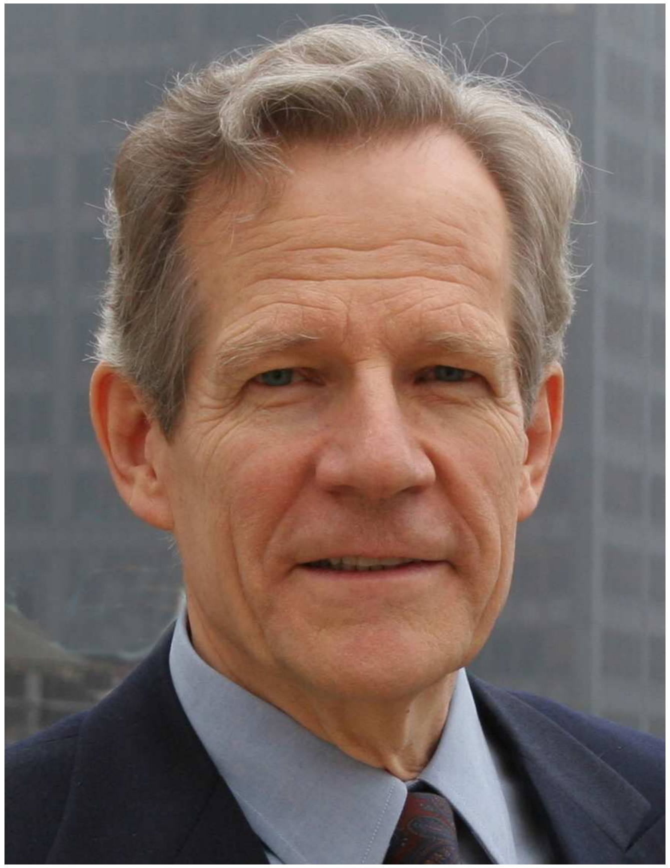
$$\cos \operatorname{lemn} k\varpi = \pm 1 \qquad \cos \operatorname{lemn}(k+\tfrac{1}{2})\varpi = 0$$

Gauss gives general addition for arbitrary points on

$$1 = s^2 + c^2 + s^2c^2.$$

Ex uno plura

- Harold M. Edwards, Bulletin of the AMS, **44**, 393–422, 2007
  $x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$
  describes an elliptic curve over field k of odd characteristic.
- Every elliptic curve can be written in this form – over some extension field.
- Ur-elliptic curve
  $$x^2 + y^2 = 1 - x^2y^2$$
  needs $\sqrt{-1} \in k$ transform.



- Edwards gives addition law for this generalized form, shows equivalence with Weierstrass form, proves addition law, gives theta parameterization . . .

Elliptic geared for crypto

Introduce further parameter d to cover more curves over k

$$x^2 + y^2 = c^2(1 + dx^2y^2), \; c, d \neq 0, dc^4 \neq 1.$$

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)}\right).$
- Neutral element is $(0, c)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.

Elliptic geared for crypto

Introduce further parameter d to cover more curves over k

$$x^2 + y^2 = c^2(1 + dx^2y^2), \; c, d \neq 0, dc^4 \neq 1.$$

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + d x_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - d x_P x_Q y_P y_Q)} \right).$
- Neutral element is $(0, c)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $[2]P = \left(\frac{x_P y_P + y_P x_P}{c(1 + d x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - d x_P x_P y_P y_P)} \right).$

Elliptic geared for crypto

Introduce further parameter d to cover more curves over k

$$x^2+y^2=c^2(1+dx^2y^2),\ c,d\neq 0, dc^4\neq 1.$$

- $P+Q=\left(\frac{x_Py_Q+y_Px_Q}{c(1+dx_Px_Qy_Py_Q)},\frac{y_Py_Q-x_Px_Q}{c(1-dx_Px_Qy_Py_Q)}\right).$
- Neutral element is $(0,c)$, this is an affine point!
- $-(x_P,y_P)=(-x_P,y_P)$.
- $[2]P=\left(\frac{x_Py_P+y_Px_P}{c(1+dx_Px_Py_Py_P)},\frac{y_Py_P-x_Px_P}{c(1-dx_Px_Py_Py_P)}\right).$
- Unified group operations!

Elliptic geared for crypto

Introduce further parameter d to cover more curves over k

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0, dc^4 \neq 1.$$

- $$P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)}\right).$$

$$\begin{aligned}
A &= Z_P \cdot Z_Q;\ B = A^2;\ C = X_P \cdot X_Q;\ D = Y_P \cdot Y_Q;\\
E &= d \cdot C \cdot D;\ F = B - E; G = B + E;\\
X_{P+Q} &= A \cdot F \cdot ((X_P + Y_P) \cdot (X_Q + Y_Q) - C - D);\\
Y_{P+Q} &= A \cdot G \cdot (D - C);\ Z_{P+Q} = c \cdot F \cdot G.
\end{aligned}$$

Elliptic geared for crypto

Introduce further parameter d to cover more curves over k

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0, dc^4 \neq 1.$$

- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)}\right).$

$$\begin{aligned}
A &= Z_P \cdot Z_Q;\ B = A^2;\ C = X_P \cdot X_Q;\ D = Y_P \cdot Y_Q; \\
E &= d \cdot C \cdot D;\ F = B - E; G = B + E; \\
X_{P+Q} &= A \cdot F \cdot ((X_P + Y_P) \cdot (X_Q + Y_Q) - C - D); \\
Y_{P+Q} &= A \cdot G \cdot (D - C);\ Z_{P+Q} = c \cdot F \cdot G.
\end{aligned}$$

Needs 10M + 1S + 1C + 1D + 7A.

- At least one of c, d small: $x^2 + y^2 = c^2(1 + dx^2y^2)$ and $x^2 + y^2 = \bar{c}^2(1 + \bar{d}x^2y^2)$ isomorphic if $c^4 d = \bar{c}^4\bar{d}$.
- $\bar{c}^4\bar{d} = (c^4 d)^{-1}$ gives quadratic twist.

Unified? Unified!

- No exceptional cases? What if a denominator is zero?
- If d is not a square then Edwards addition law is complete: For $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$ always $dx_1x_2y_1y_2 \neq \pm 1$.
  Outline of proof:
  If $(dx_1x_2y_1y_2)^2 = 1$ then $(x_1 + dx_1x_2y_1y_2y_1)^2 = dx_1^2y_1^2(x_2 + y_2)^2$. Conclude that d is a square. But d is not a square!
- If d is not a square then there is exactly one point of order 2 and two of order 4. Otherwise the full 2-torsion group is k-rational.
- Plane curve has 2 singular points at infinity; their blow-ups are defined over $k(\sqrt{d})$ and have order 2.

Fastest unified addition-or-doubling formulae

System	Cost of unified addition-or-doubling
Projective	11M+6S+1D; see Brier/Joye ’03
Projective if $a_4 = -1$	13M+3S; see Brier/Joye ’02
Jacobi intersection	13M+2S+1D; see Liardet/Smart ’01
Jacobi quartic	10M+3S+1D; see Billet/Joye ’01
Hessian	12M; see Joye/Quisquater ’01
Edwards ($c = 1$)	10M+1S+1D

- Exactly the same formulae for doubling (no re-arrangement like in Hessian where
  $$2(X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) + (Y_1 : Z_1 : X_1);$$
  no if-else)
- No exceptional cases if d is not a square. Formulae correct for all affine inputs (incl. $(0, c), P + (-P)$).

Spotlight on the transformation

Curve $x^2 + y^2 = c^2(1 + dx^2y^2)$ in Edwards form is birationally equivalent to curve

$$E : (1/e)v^2 = u^3 + (4/e - 2)u^2 + u$$

in Montgomery form, where $e = 1 - dc^4$.
Let $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ on Edwards curve. Put

- $P_i = \infty$ if $(x_i, y_i) = (0, c)$;
- $P_i = (0, 0)$ if $(x_i, y_i) = (0, -c)$;
- $P_i = (u_i, v_i)$ if $x_i \neq 0$, where $u_i = (c + y_i)/(c - y_i)$ and $v_i = 2c(c + y_i)/(c - y_i)x_i$.

Then $P_i \in E(k)$ and $P_1 + P_2 = P_3$.