How old and known are the Edwards curves

Edouard Cu(r)velier
Alphonse Magnus
Jean-Jacques Quisquater

UCLouvain – Louvain-la-Neuve - Belgium

The project

- Master thesis: is it possible to teach Edwards curves before general elliptic curves?

- Including the history of such curves.

- Surprise!

UCL
Université catholique de Louvain

Faculté des Sciences

Courbes Elliptiques d'Edwards.

Cuvelier Édouard

Année académique 2009-2010

Promoteur : Professeur Jean-Jacques Quisquater
Lecteurs : Professeur François Koeune
Professeur Alphonse Magnus

Mémoire présenté en vue de l'obtention
du master en sciences mathématiques
par **Édouard Cuvelier**.

Edwards (AMS-2007)

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 44, Number 3, July 2007, Pages 393–422
S 0273-0979(07)01153-6
Article electronically published on April 9, 2007

A NORMAL FORM FOR ELLIPTIC CURVES

HAROLD M. EDWARDS

ABSTRACT. The normal form $x^2+y^2=a^2+a^2x^2y^2$ for elliptic curves simplifies formulas in the theory of elliptic curves and functions. Its principal advantage is that it allows the *addition law*, the group law on the elliptic curve, to be stated explicitly

$$X = \frac{1}{a}\cdot\frac{xy'+x'y}{1+xyx'y'}, \quad Y = \frac{1}{a}\cdot\frac{yy'-xx'}{1-xyx'y'}.$$

The j-invariant of an elliptic curve determines 24 values of a for which the curve is equivalent to $x^2+y^2=a^2+a^2x^2y^2$, namely, the roots of $(x^8+14x^4+1)^3-\frac{j}{16}(x^5-x)^4$. The symmetry in x and y implies that the two transcendental functions $x(t)$ and $y(t)$ that parameterize $x^2+y^2=a^2+a^2x^2y^2$ in a natural way are essentially the same function, just as the parameterizing functions $\sin t$ and $\cos t$ of the circle are essentially the same function. Such a parameterizing function is given explicitly by a quotient of two simple theta series depending on a parameter τ in the upper half plane.

2. THE ADDITION FORMULA FOR $x^2+y^2+x^2y^2=1$

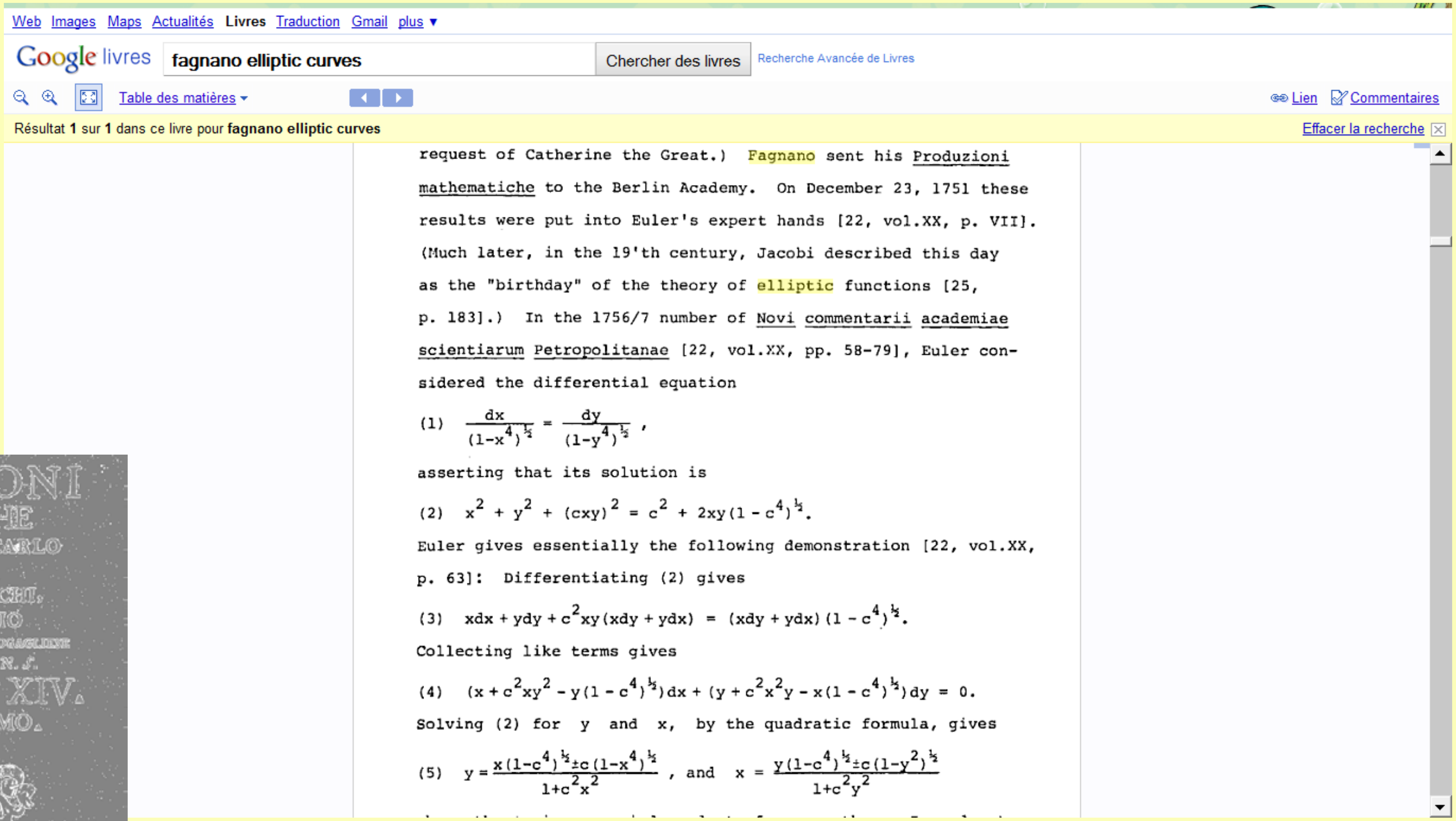
Euler's very first paper [5] on the theory of elliptic functions contains formulas that strongly suggest[1] an explicit "addition formula" in the special case of the elliptic curve $x^2+y^2+x^2y^2=1$. This curve, which becomes $z^2=1-x^4$ when one sets $z=y(1+x^2)$, was of great interest to Gauss; the last entry of his famous *Tagebuch* relates to it, as does his reference to "the transcendental functions which depend on the integral $\int\frac{dx}{\sqrt{1-x^4}}$" in Article 335 of the *Disquisitiones Arithmeticae*. In notes published posthumously in his *Werke* [6], Gauss stated explicitly the formulas Euler had hinted at decades earlier, putting them in the form

$$S=\frac{sc'+s'c}{1-ss'cc'}, \qquad C=\frac{cc'-ss'}{1+ss'cc'}. \tag{2.1}$$

Gauss's choice of the letters s and c brings out the analogy with the addition laws for sines and cosines. (The numerators *are* the addition laws for sines and cosines.) He in fact defines two transcendental functions $s(t)$ and $c(t)$ with the property that (2.1) expresses $(S,C)=(s(t+t'),c(t+t'))$ in terms of $(s,c)=(s(t),c(t))$ and $(s',c')=(s(t'),c(t'))$. The definition of $s(t)$ takes the implicit form $t=\int_0^{s(t)}\frac{dx}{\sqrt{1-x^4}}$ analogous to $t=\int_0^{\sin t}\frac{dx}{\sqrt{1-x^2}}$, while $c(t)=\sqrt{\frac{1-s(t)^2}{1+s(t)^2}}$ (with $c(0)=1$) is analogous to $\cos t=\sqrt{1-\sin^2 t}$ (with $\cos 0=1$).

These remarkable Euler-Gauss formulas apply only to the specific curve $s^2+c^2+s^2c^2=1$, but they are a special case of a formula that describes the group law of an arbitrary elliptic curve.

Giulio Carlo Fagnano (1751)



request of Catherine the Great.) Fagnano sent his Produzioni mathematiche to the Berlin Academy. On December 23, 1751 these results were put into Euler's expert hands [22, vol.XX, p. VII]. (Much later, in the 19'th century, Jacobi described this day as the "birthday" of the theory of elliptic functions [25, p. 183].) In the 1756/7 number of Novi commentarii academiae scientiarum Petropolitanae [22, vol.XX, pp. 58-79], Euler considered the differential equation

(1) $$\frac{dx}{(1-x^4)^{\frac{1}{2}}} = \frac{dy}{(1-y^4)^{\frac{1}{2}}},$$

asserting that its solution is

(2) $$x^2 + y^2 + (cxy)^2 = c^2 + 2xy(1-c^4)^{\frac{1}{2}}.$$

Euler gives essentially the following demonstration [22, vol.XX, p. 63]: Differentiating (2) gives

(3) $$xdx + ydy + c^2xy(xdy + ydx) = (xdy + ydx)(1-c^4)^{\frac{1}{2}}.$$

Collecting like terms gives

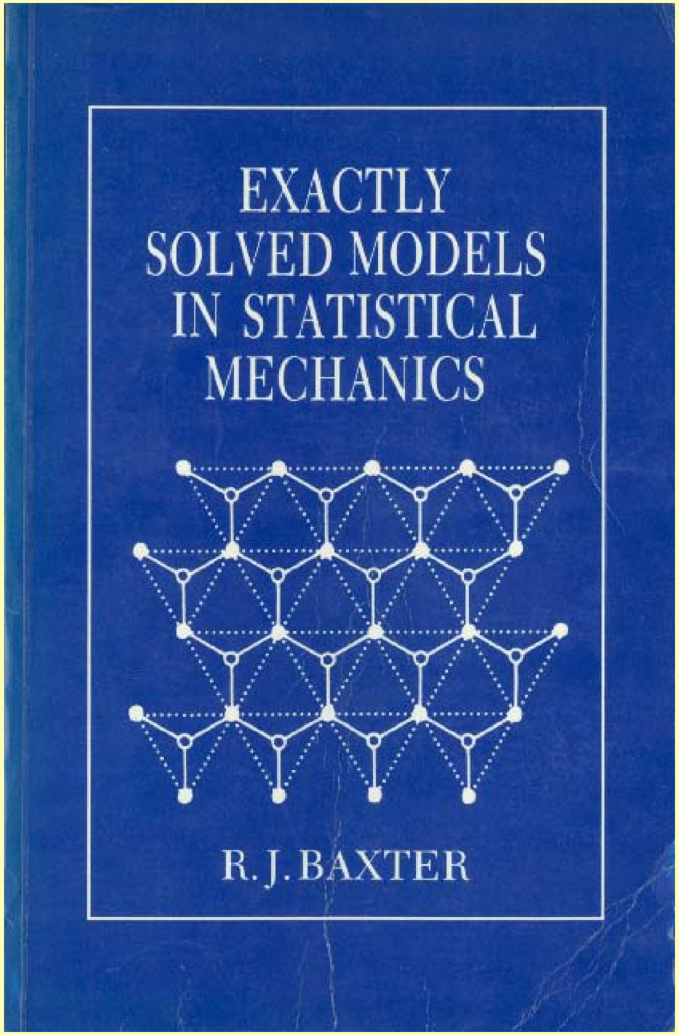
(4) $$(x + c^2xy^2 - y(1-c^4)^{\frac{1}{2}})dx + (y + c^2x^2y - x(1-c^4)^{\frac{1}{2}})dy = 0.$$

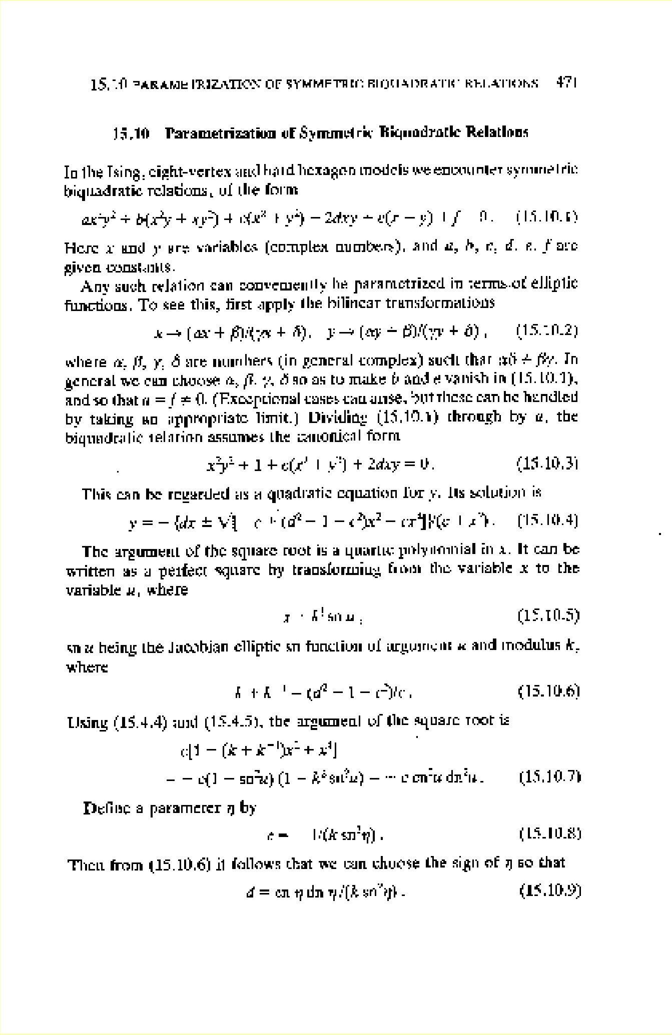
Solving (2) for y and x, by the quadratic formula, gives

(5) $$y = \frac{x(1-c^4)^{\frac{1}{2}} \pm c(1-x^4)^{\frac{1}{2}}}{1+c^2x^2}, \text{ and } x = \frac{y(1-c^4)^{\frac{1}{2}} \pm c(1-y^2)^{\frac{1}{2}}}{1+c^2y^2}$$


PRODUZIONI
MATEMATICHE
DEL CONTE GIULIO CARLO
DI FAGNANO,
MARCHESE DE' TOSCHI,
E DI SANT' ONORIO
NOBILE ROMANO, E PATRIZIO SENOGAGLIESE
ALLA SANTITÀ DI N. S.
BENEDETTO XIV.
PONTEFICE MASSIMO.
TOMO SECONDO.
IN PESARO
L' ANNO DEL GIUBBILEO M. DCC. L.
NELLA STAMPERIA GAVELLIANA
CON LICENZA DE' SUPERIORI.

Baxter, 1982, Academic Press





15.10 Parametrization of Symmetric Biquadratic Relations

In the Ising, eight-vertex and hard hexagon models we encounter symmetric biquadratic relations, of the form

$$ax^2y^2 + b(x^2y + xy^2) + c(x^2 + y^2) + 2dxy + e(x + y) + f = 0 . \qquad (15.10.1)$$

Here x and y are variables (complex numbers), and a, b, c, d, e, f are given constants.

Any such relation can conveniently be parametrized in terms of elliptic functions. To see this, first apply the bilinear transformations

$$x \to (\alpha x + \beta)/(\gamma x + \delta) , \quad y \to (\alpha y + \beta)/(\gamma y + \delta) , \qquad (15.10.2)$$

where $\alpha, \beta, \gamma, \delta$ are numbers (in general complex) such that $\alpha\delta \neq \beta\gamma$. In general we can choose $\alpha, \beta, \gamma, \delta$ so as to make b and e vanish in (15.10.1), and so that $a = f \neq 0$. (Exceptional cases can arise, but these can be handled by taking an appropriate limit.) Dividing (15.10.1) through by a, the biquadratic relation assumes the canonical form

$$x^2y^2 + 1 + c(x^2 + y^2) + 2dxy = 0 . \qquad (15.10.3)$$

This can be regarded as a quadratic equation for y. Its solution is

$$y = -\{dx \pm \sqrt{[c + (d^2 - 1 - c^2)x^2 - cx^4]}\}/(c + x^2) . \qquad (15.10.4)$$

The argument of the square root is a quartic polynomial in x. It can be written as a perfect square by transforming from the variable x to the variable u, where

$$x = k^{1/2} \operatorname{sn} u , \qquad (15.10.5)$$

$\operatorname{sn} u$ being the Jacobian elliptic sn function of argument u and modulus k, where

$$k + k^{-1} = (d^2 - 1 - c^2)/c . \qquad (15.10.6)$$

Using (15.4.4) and (15.4.5), the argument of the square root is

$$c[1 - (k + k^{-1})x^2 + x^4] = c(1 - \operatorname{sn}^2 u)(1 - k^2 \operatorname{sn}^2 u) = c \operatorname{cn}^2 u \operatorname{dn}^2 u . \qquad (15.10.7)$$

Define a parameter η by

$$c = -1/(k \operatorname{sn}^2 \eta) . \qquad (15.10.8)$$

Then from (15.10.6) it follows that we can choose the sign of η so that

$$d = \operatorname{cn} \eta \operatorname{dn} \eta/(k \operatorname{sn}^2 \eta) . \qquad (15.10.9)$$

Lessons

1) Read what you cite ☺

2) Read papers and books from other fields