INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.770/16

ADVANCED WORKSHOP ON ALGEBRAIC GEOMETRY

(15 - 26 August 1994)

Elliptic moduli curves and Poncelet polygons

W.P. Barth

Mathematisches Institut
Universität Erlangen-Nürnberg
Bismarkstrasse 1 1/2
D-91054 Erlangen
Germany

These are preliminary lecture notes, intended only for distribution to participants

Elliptic moduli curves and Poncelet polygons

W.Barth

August 15, 1994

Mathematisches Institut der Univ., Bismarckstr. 1 1/2, D - 91054 Erlangen

Contents

In the sequel the base field always will be $\mathbb{C}$.

An elliptic curve is a smooth curve of genus one. Only after specifying an origin, it carries a group structure.

Elliptic curves are classified by their modular curve, which is rational. By an elliptic modular curve I mean a curve classifying elliptic curves with additional structure (e.g. level-structure, distinguished torsion subgroup, distinguished torsion element).

1 Elliptic curves as double covers of the line

Here we shall consider elliptic curves E as double covers of the projective line $\mathbb{P}_1$ with four branch points. Let us describe first the affine part of such a curve E. It is defined by a quadruplet a_1, a_2, a_3, a_4 of *distinct* points $a_i \in \mathbb{C}$, as the Riemann surface of the square-root function

$$w = \sqrt{(z-a_1)(z-a_2)(z-a_3)(z-a_4)}.$$

This square–root function has two branches $\pm w$ differing by their sign.

To extend the curve over ∞ we have to pass to another coordinate $z' = 1/z$. The function w then is

$$\sqrt{(\frac{1}{z'} - a_1) \cdot \ldots \cdot (\frac{1}{z'} - a_4)} = \frac{1}{z'^2} \cdot \sqrt{(1 - a_1 z') \cdot \ldots \cdot (1 - a_4 z')}.$$

If we use $w' = z'^2 \cdot w$ in place of w, then we can define the curve E near ∞ as the Riemann surface of

$$w' = \sqrt{(1 - a_1 z') \cdot \ldots \cdot (1 - a_4 z')}$$

and complete E in this way near ∞ to a smooth, complete curve.

Notice, that it is inevitable, to pass from w to $w' = z'^2 w$. In other words: The curve E is not a subset of the product space $\mathbb{C} \times \mathbb{P}_1$, but of a *locally trivial fibre bundle* obtained from two copies of $\mathbb{C}^2$ with coordinates (z, w) and (z', w') by glueing via

$$z' = \frac{1}{z}, \quad w' = \frac{1}{z^2} w.$$

Then E is a subset in this bundle. This bundle usually is denoted by $\mathcal{O}_{\mathbb{P}_1}(2)$.

Instead of two affine coordinates z and z' we could use one pair of homogeneous coordinates $(\lambda : \mu)$ on $\mathbb{P}_1$. If we transform $z = \lambda/\mu$, then we find that the curve E is defined by the equation

$$w^2 = (\lambda - a_1\mu)(\lambda - a_2\mu)(\lambda - a_3\mu)(\lambda - a_4\mu).$$

Notice, that in this homogeneous form, we may without problems include the case that one root, say a_4 is infinity. We just replace the factor $(\lambda - a_4\mu)$ by μ alone. The resulting homogeneous equation

$$w^2 = (\lambda - a_1\mu)(\lambda - a_2\mu)(\lambda - a_3\mu) \cdot \mu$$

has the affine form (put $\mu = 1, \lambda = z$)

$$w^2 = (z - a_1)(z - a_2)(z - a_3),$$

a polynomial of degree three!

Of course, being here on a conference devoted to the study moduli, we want to understand the moduli of the curve E. These moduli are encoded in the four points $a_1, \ldots, a_4$. The standard procedure would be to quotient out the set of ordered quadruplets $(a_1, \ldots, a_4)$ by the action of the projective group $PGL(2, \mathbb{C})$. Let us not use this standard procedure, but simplify life a little bit: We consider only special quadruplets

$$(a_1, a_2, a_3, a_4) = (p, -p, \frac{1}{p}, -\frac{1}{p}).$$

Of course, we must make sure, that in this way we don't miss any quadruplets of points. But two quadruplets are equivalent under the group $PGL(2, \mathbb{C})$ if and only if they have the same cross–ratio. (This is sometimes called the 'Main Theorem of projective geometry').

Now the cross-ratio of our special quadruplet is

$$\begin{aligned} CR(p, -p, \frac{1}{p}, -\frac{1}{p}) &= \frac{p - \frac{1}{p}}{p + \frac{1}{p}} : \frac{-p - \frac{1}{p}}{-p + \frac{1}{p}} \\ &= \frac{-(p - \frac{1}{p})^2}{-(p + \frac{1}{p})^2} \\ &= \frac{(p^2 - 1)^2}{(p^2 + 1)^2}. \end{aligned}$$

This function $\phi = (p^2-1)^2/(p^2+1)^2)$ is a rational function on $\mathbb{P}_1$ and defines a morphism

$$\phi : \mathbb{P}_1 \ni (p:q) \rightarrow (p^2-q^2)^2 : (p^2+q^2)^2 \in \mathbb{P}_1$$

of degree four. In particular, this morphism is surjective. And this means, by proper choice of p, we get all possible cross-ratios.

So we found: Associating to p the elliptic curve with the four branch points $\pm p, \pm\frac{1}{p}$ we obtain all possible elliptic curves. But we do get the same elliptic curves *more than once*! There are two reasons for this, an obvious one, and a less obvious on.

The obvious reason: Obviously, each of the four points $p' \in \{\pm p, \pm\frac{1}{p}\}$ defines the same quadruplet

$$\{\pm p', \pm\frac{1}{p'}\} = \{\pm p, \pm\frac{1}{p}\},$$

just in another order. As the function $(z-z_1)\cdot\ldots\cdot(z-z_4)$ is invariant under permutations of the branch points z_i, such a reordering gives the same elliptic curve $E = E_{p'} = E_p$.

Let us have a closer look at these reorderings: The quadruplets $\pm p, \pm\frac{1}{p}$ are *orbits of a group action* on $\mathbb{P}_1$, namely of an action of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. If we denote the two generators of this group by σ and τ, this action is

$$\sigma : p \rightarrow -p, \quad \tau : p \rightarrow \frac{1}{p}.$$

The reordering of a quadruplet is nothing but the group action in an orbit.

Now this group is very small, and its action very simple, but nevertheless very beautiful: The general orbit has length four, but there are three special orbits

$$\{\pm 1\}, \quad \{\pm i\}, \quad \{0, \infty\}$$

of length two. The six points in these three orbits can be thought of as the six vertices of a regular octahedron, inscribed in the Riemann sphere $\mathbb{P}_1$. An orbit consists then just of the a pair of opposite vertices.

If you are classically minded, you recognize the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ as the *four group V of Felix Klein.* He studied this group as a subgroup of the full symmetry group of the octahedron [K, p.16]. V is a normal subgroup in the full rotation group of the octahedron, which is isomorphic to the symmetric group S_4. Everybody knows the exact sequence of groups

$$1 \rightarrow V \rightarrow S_4 \rightarrow S_3 \rightarrow 1,$$

the morphism $S_4 \rightarrow S_3$ being given by the action of S_4 on the three diagonals of the octahedron, which connect the three pairs of opposite vertices.

The nonobvious reason: Each symmetry $\nu \in S_4$ of the icosahedron transforms an orbit $\pm p, \pm\frac{1}{p}$ of V into another such orbit, because V is normal in S_4. For example the symmetry

$$\nu : z \mapsto i \cdot z$$

transforms the orbit $\pm p, \pm\frac{1}{p}$ to the orbit $\pm i \cdot p, \pm\frac{1}{i \cdot p}$ with cross-ratio

$$CR(i\cdot p, -i\cdot p, \frac{1}{i\cdot p}, -\frac{1}{i\cdot p}) \quad = \quad \left(\frac{(i\cdot p)^2-1}{(i\cdot p)^2+1}\right)^2$$

$$
\begin{aligned}
&= \left(\frac{-p^2-1}{-p^2+1}\right)^2 \\
&= \left(\frac{p^2+1}{p^2-1}\right)^2 \\
&= 1/CR(p,-p,\frac{1}{p},-\frac{1}{p}) \\
&= CR(p,-p,-\frac{1}{p},\frac{1}{p}).
\end{aligned}
$$

The cross-ratio is different, but it is one of the six cross-ratios

$$CR, \quad \frac{1}{CR}, \quad 1-CR, \quad 1-\frac{1}{CR}, \quad \frac{1}{1-CR}, \quad \frac{CR}{CR-1}$$

obtained from the original quadruplet by reordering it under permutations, which do *not belong* to Klein's four group V.

So the action of the octahedral group S_4 transforms the original quadruplet $\pm p, \pm\frac{1}{p}$ into six different orbits of V, which all give isomorphic elliptic curves E.

Since the cross-ratio map has degree four, the four points in one V-orbit are exactly those points $p \in \mathbb{P}_1$, for which the cross-ratio $CR(p,-p,\frac{1}{p},-\frac{1}{p})$ is the same. The 24 points in the six V-orbits equivalent under the octahedral group S_4 then are exactly those points $p \in \mathbb{P}_1$, for which the V-orbit gives the same elliptic curve. Therefore, the moduli space for elliptic curves is the quotient of $\mathbb{P}_1$ by the octahedral group S_4.

The quotient map

$$\underbrace{\mathbb{P}_1 \xrightarrow{mod\ V} \mathbb{P}_1 \xrightarrow{mod\ S_3} \mathbb{P}_1}_{mod\ \ S_4}$$

can be written down explicitly in terms of the *invariants of the octahedral group* [K, p.54]:

$$
\begin{aligned}
t &:= pq(p^4-q^4) \\
w &:= p^8+14p^4q^4+q^8
\end{aligned}
$$

The quotient map by S_4 is

$$(p:q) \to (16w^3 : t^4)$$

or in affine form

$$j(p) := 16\frac{w^3}{t^4}.$$

Exercise: Compute the points $(p:q) \in \mathbb{P}_1$, for which the S_4-orbit has length < 24. Apart from the vertices of the octahedron (orbit length $= 6$) these are the points corresponding to mid-points of the edges (orbit length $= 12$) and to the centers of the faces (orbit length $= 8$). They correspond to special elliptic curves:

points	curve
vertices	degenerate
mid points	$\mathbb{Z}_4$-symmetry
centers	$\mathbb{Z}_6$-symmetry

Compute the j–invariants for these points.

The *moduli curve* $\mathbb{P}_1/S_4$ parametrizing isomorphism classes of elliptic curves is just another copy of the projective line $\mathbb{P}_1$. The same holds for the quotient $\mathbb{P}_1/V$. This curve contains six distinct points for each elliptic curve E (resp. one, if E is degenerate, two, if E has $\mathbb{Z}_6$–symmetry, or three, if E has $\mathbb{Z}_4$–symmetry). The points in $\mathbb{P}_1/V$ also have some meaning in terms of moduli: Even, if the elliptic curves E are isomorphic, the V–action on their quadruplet of branch points differs. As the four branch points can be thought of as the images of the four half–periods on E (if one chooses an origine for E over one of these branch points) this is a $\mathbb{Z}_2 \times \mathbb{Z}_2$–action on the half–periods of E. Such an action is called a *level-2-structure* on the elliptic curve E. The quotient $\mathbb{P}_1/V$ therefore is a moduli curve parametrizing *elliptic curves with level-2-structures.*

One can construct a kind of universal family of elliptic curves, parametrized by the first copy of $\mathbb{P}_1$. To do this, consider in

$$\mathbb{P}_1(p,q) \times \mathbb{P}_1(\lambda,\mu)$$

the curve consisting of the four components

$$\begin{aligned} C_1 &: (\lambda:\mu) = (p:q) \\ C_2 &: (\lambda:\mu) = (-p:q) \\ C_3 &: (\lambda:\mu) = (q:p) \\ C_4 &: (\lambda:\mu) = (-q:p) \end{aligned}$$

There exists a double cover $\pi : X \to \mathbb{P}_1 \times \mathbb{P}_1$ branched exactly over this curve. For each $(p:q) \in \mathbb{P}_1$ the curve $E_{(p:q)} = \pi^{-1}(\{(p:q)\} \times \mathbb{P}_1)$ is the elliptic curve belonging to the point $(p:q)$. So X is family of elliptic curves containing a copy of each curve. However it contains each curve E (if it is general) exactly 24 times. So it does not parametrize these curves effectively.

It is natural to ask, whether a quotient of X by the action of S_4 on $\mathbb{P}_1(p:q)$ exists. This quotient would be a universal family of elliptic curves. Now, analyzing precisely the line bundle needed to form the double cover, one even checks that already the quotient X/V does not exist as a family of elliptic curves: *there is no universal family of elliptic curves with level-2-structure, nor of elliptic curves themselves.*

Exercise: Prove this!

2 The group structure on elliptic curves

Everybody knows that an elliptic curve E over $\mathbb{C}$ carries the structure of a compact, commutative complex Lie group of dimension one. That is, as a complex manifold E is a group quotient $\mathbb{C}/\Gamma$, where $\Gamma \subset \mathbb{C}$ is a lattice. However, this information is transcendental! It is usually very hard, to describe the group structure algebraically, i.e. geometrically. The simplest way to do this is on the model of E as a plane cubic curve. But I don't know of any way to describe the group structure on E in terms of the double cover representation studied so far.

Perhaps, since everybody knows it anyhow, I may just use this group structure without further reasoning. So in this section, I mean by an elliptic curve E a quotient $\mathbb{C}/\Gamma$. We shall denote the group operation by addition '+' and the inverse of an element $x \in E$ by $-x$. We only need two simple facts:

1. Involutions with fixed points. The group E admits the standard involution

$$i : E \ni x \mapsto -x \in E.$$

The origin $e_0 \in E$ is an isolated fixed point for i. There are three more fixed points, the non-trivial elements $e_1, e_2, e_3 \in E$ of order two. The quotient E/i is a copy of the projective line $\mathbb{P}_1$. The quotient map obviously is of order two with four branch points $e_0, ..., e_3$. In this way we recover E as a double cover of $\mathbb{P}_1$, branched over the images of the four half-periods.

In section 1 we defined a level-2-structure on E as an action of the Klein four group V on the four branch points, permuting them in pairs. Now, the half-periods themselves form a group, acting on themselves in this, unique, way. So a level-2-structure is the same as *an isomorphism of the group* $\mathbb{Z}_2 \times \mathbb{Z}_2$ with the half-period subgroup.

Any element $x_0 \in E$ defines an involution

$$i_0 : E \ni x \to x_0 - x \in E.$$

An element $x \in E$ is a fixed point for i_0, if $x = x_0 - x$, i.e. if $2x = x_0$. There are, of course, four such points x differring by half-periods. We need the converse: *Given an involution $j : E \to E$ with fixed points, then there is an $x_0 \in E$ with $j = i_0$.*

Proof. Let $y \in E$ be a fixed point for j. Consider the map $j' : x \to j(x + y) - y$. Clearly

$$j'(j'(x)) = j(j(x + y) - y + y) - y = j(j(x + y)) - y = x + y - y = x,$$

hence j' is a nontrivial involution with the origin e_0 as fixed point. All automorphisms of E leaving e_0 fixed, are induced by multiplying in $\mathbb{C}$ with a complex number, which in the case of j' must be -1. This implies $j' = i$, i.e. for all $x \in E$:

$$\begin{aligned} j(x + y) - y &= -x \\ j(x + y) &= -x + y \\ j(x) &= j((x - y) + y) \\ &= 2y - x \end{aligned}$$

and j is the involution $x \to 2y - x$. □

As a consequence we notice: Given two involutions $j_1(x) = x_1 - x$ and $j_2(x) = x_2 - x$ with fixed points, then their product

$$j_2(j_1(x)) = x_2 - (j_1(x)) = x_2 - x_1 + x$$

is a *translation* by the element $x_2 - x_1 \in E$. And the product $j_1 j_2$ is the inverse translation, by $x_1 - x_2$.

2. *Torsion elements.* For each $n \in \mathbb{N}$, the n-torsion subgroup $E^{(n)} \subset E$ consists of the elements with $n \cdot x = 0$, which are n^2 in number. We met already the half-period subgroup $E^{(2)}$. Of course, this group contains the origin, and if n is not a prime, also other improper n-torsion elements.

There is an explicit characterization of the elements of order n on E, due to Cayley [C,GH]: Assume the curve E is given as a double cover branched over the four points $a_1, a_2, a_3 \in \mathbb{C}$ and ∞. Form the power series expansion

$$\sqrt{(z - a_1)(z - a_2)(z - a_3)} = \sum_{k=0}^{\infty} c_k z^k.$$

Then the two points on E over the origin are n-torsion if and only if the symmetric determinant d_n vanishes, where

$$d_n = \begin{pmatrix} c_2 & c_3 & \cdots & c_{m+1} \\ c_3 & c_4 & \cdots & c_{m+2} \\ \vdots & \vdots & & \vdots \\ c_{m+1} & c_{m+2} & \cdots & c_{2m} \end{pmatrix} \qquad \text{for } n = 2m + 1$$

and

$$d_n = \begin{pmatrix} c_3 & c_4 & \dots & c_{m+1} \\ c_4 & c_5 & \dots & c_{m+2} \\ \vdots & \vdots & & \vdots \\ c_{m+1} & c_{m+2} & \dots & c_{2m-1} \end{pmatrix} \quad \text{for } n = 2m.$$

3 Poncelet Polygons

A polygon is a cyclically ordered set $L_0, L_1, ..., L_{n-1}$ of distinct lines $L_i \subset \mathbb{P}_2$. We use the convention $L_n = L_0$. The vertices of this polygon are the n points $P_i = L_i \cap L_{i+1}$. We assume that they are all distinct too.

Let $C, D \subset \mathbb{P}_2$ be smooth conics. We say that the polygon *is inscribed in* the conic D, if the n points P_i lie on D. We say that the polygon *is circumscribed about* the conic C, if the n lines L_i are tangent to this conic. A *Poncelet polygon for the pair* C, D of conics is a polygon simultaneously circumscribed about C and inscribed in D.

Poncelet's theorem: *If for two smooth conics $C, D \subset \mathbb{P}_2$ there is one Poncelet n-gon, then there are infinitely many such n-gons.*

A Poncelet n-gon is determined by any one of its lines: L_i determines its two intersections $P_{i-1} \neq P_i$ with D, and the point P_i determines another tangent, namely L_{i+1} to C. Repeating the construction $(L_i, P_i) \mapsto (L_{i+1}, P_{i+1})$ one obtains the whole polygon in this way. The Poncelet property is the fact, that the $n+1$-th line constructed coincides with the first one. *The polygon closes*, and Poncelet's theorem therefore often is called Poncelet's closure theorem.

The simplest case of Poncelet's theorem, easy to analyze, deals with two concentric circles, whose radii satisfy

$$\frac{r}{R} = sin(\frac{\pi}{n}).$$

Poncelet had difficulties with the proof of his theorem for conics, mainly for two reasons:

1. He introduced the use of points with complex coordinates into Geometry. At his time it was by no means clear whether this is legitimate.

2. The transcendental sin-function in the formula above must be generalized to the elliptic integral. (Recall, that the sin-function is the inverse function of the integral $\int dz/\sqrt{1-z^2}$, and that generalizing the polynomial $1-z^2$ to a polynomial of degree four leads to the elliptic integral.)

The standard proof for Poncelet's theorem nowadays does not use elliptic integrals, but their geometric counterparts: elliptic curves. (See e.g. [GH].)

Where is an elliptic curve in Poncelet's situation? Let us assume that the two conics C and D are in general position, i.e., that they intersect in four distinct points A_0, A_1, A_2, A_3. As a smooth conic is isomorphic with the projective line $\mathbb{P}_1$, we have a quadruplet $A_0, ..., A_3$ on both copies C and D of $\mathbb{P}_1$. For both quadruplets we can form the double cover of $\mathbb{P}_1$, branched over this quadruplet just as in section 1, and there are elliptic curves, even two of them.

The elliptic curve E, the covering of the conic D, naturally controls Poncelet polygons: Through each point $A \subset D$ there are two tangents L and L' to C. These two tangents coincide if and only if A is one of the four points $E_i \in C \cap D$. It is not so hard to show that all pairs (L, A) with

- $A \in D$,

- L tangent to C,
- $A \in L$,

form a curve $E \subset D \times C^*$, and that this curve is isomorphic with the elliptic curve E. The covering map $E \to D$ is given by sending a pair (L, A) to its point $A \in D$. This covering of degree two determines an involution i_D on E with four fixed points (over the quadruplet $A_0, ..., A_3$).

What about the projection $(L, A) \to L$ onto the first factor? It sends a pair (L, A) to the tangent L of C. In general, this tangent meets the conic D in two points A, so this projection $E \to C^* \simeq \mathbb{P}_1$ is of degree two also. The branch points are the pairs (L, A) such that the tangent L to C meets D in just one point, i.e., such that L is tangent to D too. There are exactly four double tangents L (touching C and D simultaneously). So also this projection of degree two determines an involution i_C on E with four fixed points.

Using these two involutions, one can describe the construction step $L_i \to L_{i+1}$ leading to the Poncelet polygon: Let $t : E \to E$ be the translation $i_D i_C$ and let $t' = i_C i_D$. (These are translations, inverse to each other, cf. section 2.) Then t maps a pair

$$(L_i, P_i) \mapsto i_C(L_i, P_i) = (L_{i+1}, P_i) \mapsto i_D(L_{i+1}, P_i) = (L_{i+1}, P_{i+1})$$

and t' maps

$$(L_i, P_i) \mapsto i_D(L_i, Pi) = (L_i, P_{i-1}) \mapsto i_C(L_i, P_{i-1}) = (L_{i-1}, P_{i-1}).$$

So the pair (L_i, P_i) is mapped to its successor, resp. predecessor in the polygon.

Now we can prove Poncelet's theorem: Let $C, D \subset \mathbb{P}_2$ be two smooth conics meeting in four distinct points. Define the elliptic curve $E = \{(L, A)\}$ as above with its involutions i_C and i_D. If there exists one Poncelet-n-gon circumscribet about C and inscribed in D, then there is a pair $(L, A) \in E$ with $t^n(L, A) = (L, A)$. This means that the translation t is of order n. Then $t^n(L', A') = (L', A')$ for all pairs $(L', A') \in E$, which means, each pair (L', A') can be completed to a closed Poncelet polygon

$$(L', A'), \quad t(L', A'), \quad \dots \quad , t^{n-1}(L', A'), \quad t^n(L', A') = (L', A').$$

In the next section, the last one, we shall see, that Poncelet polygons lead to explicit plane models of a series of elliptic modular curves. Before this, we have to parametrize explicitly all pairs (C, D) of smooth conics in general position.

C and D are in general position, if they meet in four distinct points. No three of them can be collinear, so there is a projective transformation mapping these four points to the four distinguished points

$$A_0 = (1 : 1 : 1) \qquad A_1 = (1 : 1 : -1)$$
$$A_2 = (1 : -1 : 1) \qquad A_3 = (-1 : 1 : 1)$$

The two conics C and D then are transformed into two conics of the pencil of conics through these four base points. In homogeneous coordinates (z_0, z_1, z_2) the equations of the conics in this pencil are

$$\alpha z_0^2 + \beta z_1^2 + \gamma z_2^2, \quad \alpha + \beta + \gamma = 0.$$

Of course, since C and D are smooth, their equations are of this form with $\alpha \cdot \beta \cdot \gamma \neq 0$.

If we want to start a Poncelet polygon for two conics C and D with the pair (L, A), where

$$L \; := \; \text{tangent line to } C \text{ in } A_0$$
$$A \; := \; A_0 \in D,$$

then the first point to construct would be the point

$$P := \text{ second intersection of } L \text{ with } D.$$

This point P determines the conics C and D uniquely:

As $C \neq D$, the line L cannot be tangent to D too and $P \neq A_0$. As C is non-degenerate, the point P does not lie on any one of the three lines B_k joining A_0 to $A_k, 1 \leq k \leq 3$. So D is the unique conic in the pencil determined by the A_k passing through P. And C is the unique conic in the pencil tangent to the line L joining P with A_0. In this way the pairs C, D of non-degenerate conics in our pencil correspond bijectively to the points $P \in \mathbb{P}_2$, not on B_1, B_2 or B_3. We call the point P *the control point* for the pair C, D.

The control point P not only determines the two conics C and D, but its position on D also decides, whether C and D are in Poncelet position. Recall that there exists a Poncelet-n-gon circumscribed about C and inscribed into D, if and only if P is the image of some n-torsion point $t \in E$, where $E \to D$ is the elliptic curve over D, branched at $A_0, ..., A_3$.

Cayley's condition for this to happen can be evaluated explicitly. To do this we map the rational curve D onto the projective line $\mathbb{P}_1$ parametrizing the pencil $\lambda C + \mu D$ of conics, in two steps:

Step 1: Map D onto the $\mathbb{P}_1$ parametrizing the lines through A_0 by projection. I.e., a point $A \in D$ is mapped onto the line joining A with A_0, and A_0 is mapped onto the tangent $T_{A_0}(D)$ of D in A_0.

Step 2: The pencil of lines through A_0 is mapped onto the pencil $\lambda C + \mu D$ by sending a line B through A_0 to the uniqe conic in the pencil, which touches B at A_0.

In this way one maps

D	$\to$	pencil of lines	$\to$	pencil of conics
A_0	$\mapsto$	$T_{A_0}(D)$	$\mapsto$	D
$A_k, k = 1,2,3$	$\mapsto$	B_k	$\mapsto$	the three degenerate conics
P	$\mapsto$	$T_{A_0}(C)$	$\mapsto$	C.

The inhomogeneous coordinate μ/λ on the pencil of conics transforms to an affine coordinate on D vanishing on P with pole at D. [GH] observed, that the cubic polynomial under the square root in Cayley's condition, with roots at A_1, A_2, A_3 and pole at A_0 transforms into the cubic polynomial

$$det(\lambda C + \mu D),$$

the discriminant of the pencil. (Indeed, the three roots of the discriminant are the parameters for the three degenerate conics).

Assume, the control point P has coordinates $P = (p_0 : p_1 : p_2)$. Then one computes

$$\begin{aligned}
C &: (p_1 - p_2)z_0^2 + (p_2 - p_0)z_1^2 + (p_0 - p_1)z_2^2 = 0 \\
D &: (p_1^2 - p_2^2)z_0^2 + (p_2^2 - p_0^2)z_1^2 + (p_0^2 - p_1^2)z_2^2 = 0 \\
det(\lambda C + \mu D) &= \lambda^3 \cdot det(C) + \\
&\quad \lambda^2\mu \cdot det(C) \cdot \{(p_0 + p_1) + (p_1 + p_2) + (p_2 + p_0)\} + \\
&\quad \lambda\mu^2 \cdot \det(C) \cdot \{(p_0 + p_1)(p_1 + p_2) + (p_1 + p_2)(p_2 + p_0) + (p_2 + p_0)(p_0 + p_1)\} + \\
&\quad \mu^3 \cdot det(C) \cdot \{(p_0 + p_1)(p_1 + p_2)(p_2 + p_0)\} \\
&= det(C) \cdot \left(\lambda^3 + \lambda^2\mu \cdot 2s_1 + \lambda\mu^2 \cdot (s_1^2 + s_2) + \mu^3 \cdot (s_1 s_2 - s_3)\right)
\end{aligned}$$

with the symmetric functions

$$s_1 := p_0 + p_1 + p_2, \quad s_2 := p_0p_1 + p_1p_2 + p_2p_0, \quad s_3 := p_0p_1p_2.$$

The Taylor coefficients c_k are, up to the common constant factor $\sqrt{det(C)}$,

$$\begin{aligned} c_1 &= s_1 \\ c_2 &= \frac{1}{2}s_2 \\ c_3 &= -\frac{1}{2}s_3 \\ c_4 &= \frac{1}{2}s_1s_3 - \frac{1}{8}s_2^2 \\ &\vdots \end{aligned}$$

4 More elliptic modular curves

The four points $A_0, ..., A_3$ come with a natural $\mathbb{Z}_2\times\mathbb{Z}_2$–action: Let the first generator $\mu = (1,0) \in \mathbb{Z}_2\times\mathbb{Z}_2$ change the sign of the coordinate x_1 and the second generator $\tau = (0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ change the sign of the coordinate x_2. In this way the double cover E of D carries naturally a level–2–structure. We claim: Moving D in the pencil of conics with base points $A_0, ..., A_3$, we find in this way all possible elliptic covering curves, with all possible level–2–structures.

Proof of this claim: The curve E with its level–2–structure is uniquely determined by the cross–ratio of the four branch points on $\mathbb{P}_1 = D$. So we have to show, that all possible cross–ratios arise in the pencil. We project the conic

$$D: \quad \alpha x_0^2 + \beta x_1^2 + \gamma x_2^2 = 0, \quad \alpha + \beta + \gamma = 0$$

from the point A_0 onto the line $z_0 = 0$ to find

$$\begin{aligned} A_1 &\to (0:0:-2) = (0:0:1) \\ A_2 &\to (0:1:0), \\ A_3 &\to (0:1:1), \\ A_0 &\to \text{intersection of the tangent } \alpha x_0 + \beta x_1 + \gamma x_2 = 0 \\ &\quad\ \text{with the line } x_0 = 0 \\ &= (0:\gamma:-\beta). \end{aligned}$$

The cross–ratio of these four points is

$$\begin{aligned} CR(-\frac{\beta}{\gamma}, \infty, 0, 1) &= \frac{-\beta/\gamma - 0}{-\beta/\gamma - 1} : \frac{\infty - 0}{\infty - 1} \\ &= \frac{1}{1 + \gamma/\beta}. \end{aligned}$$

This crossration takes indeed all complex values, except for 1, and it takes it just once! □

We can reformulate this observation as follows: Let be given an elliptic curve E with a level-2-structure, determined by an ordering e_0, e_1, e_2, e_3 of the half-periods on E. Then there is a unique smooth conic D in our pencil, and a unique double cover $E \to D$ sending e_k to A_k for $k = 0, ..., 3$.

A control point $P \in \mathbb{P}_2$ as in section 3 determines two conics C and D. There exists a Poncelet-n-gon for them, if and only if the point $P \in D$ is the image of some n-torsion point $t \in E$, where E is the double cover of D. If e.g. n is an odd prime, then E contains $n^2 - 1$ points t of order n. Since t and $-t$ have the same image in D, there are precisely $(n^2 - 1)/2$ control points on D leading to a Poncelet n-gon, inscribed into D.

Now, moving D, for each natural number $n \geq 3$ we obtain a one-parameter family of such control points. They sweep a curve in $\mathbb{P}_2$. It is not hard to show, that this plane curve is (a Zariski-open part of) an algebraic plane curve $\Pi_n \subset \mathbb{P}_2$. In fact, Cayley's explicit formula, together with the elemetary computations of the last section, gives equations for these curves in form of symmetric determinants. They can be evaluated with a computer, but there are also more theoretical ways to compute the equation of Π_n for the first few n [BM]. Here are some results, given in terms of the symmetric functions s_1, s_2 and s_3, and in terms of the symmetric functions

$$\sigma_1 := p_0^2 + p_1^2 + p_2^2, \quad \sigma_2 := p_0^2p_1^2 + p_1^2p_2^2 + p_2^2p_0^2, \quad \sigma_3 := p_0^2p_1^2p_2^2$$

of the squares of the coordinates:

n	equation fo Π_n
3	s_2
4	s_3
5	$-4s_1s_2s_3 + s_2^3 + 4s_3^2$
6	$\sigma_2^2 - 4\sigma_1\sigma_3$
7	$-4s_1s_2^4s_3 + 16s_1s_2s_3^3 + s_2^6 + 4s_2^3s_3^2 - 16s_3^4$
8	$s_3(-4\sigma_1\sigma_2\sigma_3 + \sigma_2^3 + 8\sigma_3^2)$

The classification of control points $P \in \Pi_n$, i.e. the description of the plane curve Π_n is the problem, to classify all n-torsion points $\pm t$ on all possible elliptic curves with a level-2-structure. There are three moduli problems combined in this question:

1. The classification of all elliptic curves with level-2-structure. This was done in section 1. The resulting moduli curve is rational.

2. The classification of all pairs $\pm t$ of points of order n on all elliptic curves. This is the problem to classify *isomorphism classes of pairs* E, t, since the pair E, t is isomorphic with the pair $E, -t$ under $i : E \to E$. (Let us not worry too much here about the two elliptic curves with more automorphisms.) There is a moduli curve, called $X_{00}(n)$, for this moduli problem, and one knows precisely its genus in terms of the number n. The curve is connected and if e.g. $n = p$, an odd prime then the genus of $X_{00}(n)$ equals

$$\frac{1}{3}(p-1)(p-2).$$

3. The classification of isomorphism classes of

   – elliptic curves E with

- a level-2-structure and
- a point of order n.

This moduli problem is solved by a moduli curve

$$X_{00}(n,2) := X_{00}(n) \times_{\mathbb{P}_1} X(2).$$

Here the fibre product is formed with respect to the j-function maps

$$j : X_{00}(n) \to \mathbb{P}_1, \quad j : X(2) \to \mathbb{P}_1.$$

The curve $X_{00}(n,2)$ is connected for odd n. Its genus can be computed and one finds e.g. for odd primes p

$$g(X_{00}(n,2)) = \frac{1}{4}(p-3)^2.$$

Now the plane curves Π_n defined above are birational models of the elliptic modular curves $X_{00}(n,2)$. It is quite remarkable, that these modular curves have such a series of plane models, that their equations can be given explicitly, and that all this is related to Poncelet's theorem.

5 References

BM Barth, W., Michel, J.: Modular curves and Poncelet polygons. Math. Ann. 295, 25-49 (1993)

C Cayley, A.: Phil. Trans. Royal Soc. London, vol. CLI, 225-239 (1861)

GH Griffiths, Ph., Harris, J.: On Cayley's explicit solution to Poncelet's Porism. Enseign. Math., II Ser. 24, 31-40 (1978)

K Klein, F.: Vorlesungen über das Ikosaeder, 2. Auflage, Birkhäuser, 1993