ON CAYLEY'S EXPLICIT SOLUTION TO PONCELET'S PORISM

Autor(en): **Griffiths, Phillip / Harris, Joseph**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **24 (1978)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-49688

ON CAYLEY'S EXPLICIT SOLUTION TO PONCELET'S PORISM [1]

by Phillip GRIFFITHS [2] and Joseph HARRIS [3]

Let C and D be two smooth conics generally situated in the projective plane. The classical problem of Poncelet is to determine if there is a closed polygon inscribed in C and circumscribed about D. His beautiful result is that there is one such if, and only if, there are infinitely many. More precisely, if we let x denote a point of C and ξ a tangent line to D, and if we make the construction

$$(x, \xi) \to (x', \xi) \to (x', \xi')$$

as depicted by Figure 1

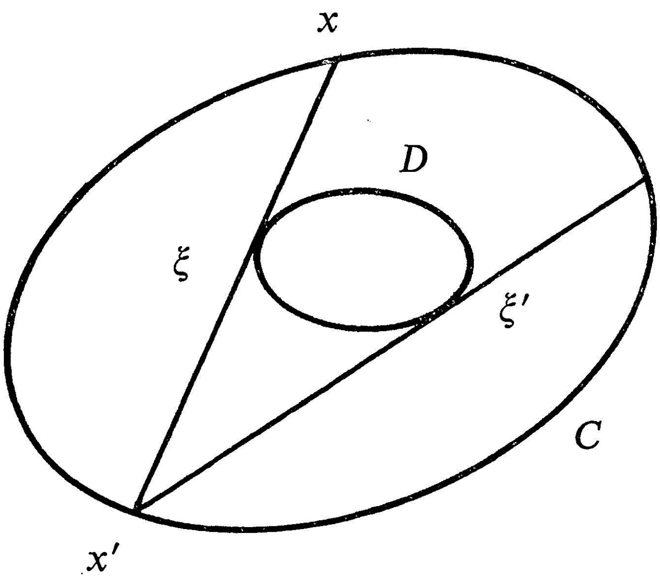

Figure 1

then Poncelet's theorem states: *The requirement that the* n^{th} *iterate of this construction give us back* (x, ξ) *is independent of the initial data.*

Following Poncelet's original synthetic proof, Jacobi gave in 1835 an analytic argument based on (to us) elaborate formulae from the theory of

---

[1]) Presented at the Colloquium on Topology and Algebra, April 1977, Zurich.
[2]) Research partially supported by NSF Grant MCS 72-05154
[3]) NSF Predoctoral Fellow.

elliptic functions. In a recent paper [1]) we gave a "modern" algebro-geometric version of Jacobi's proof together with an extension of the Poncelet theorem to 3-space. In that paper we stated that it seemed (to us) difficult to find the explicit conditions for Poncelet's porism [2]) to hold. In the interim Marcel Berger called to our attention a series of papers by Cayley [3]) on exactly this question. Cayley's method was again based on complicated identities from elliptic functions, but his final result was quite simple. So in this paper we shall give an algebro-geometric proof of Cayley's theorem, one which yields a rather elegant explicit formula that a point on an elliptic curve be of finite order n (c.f. the end of §1 below). When applied to the Poncelet problem the result is this:

Let $C(x) = 0, D(x) = 0$ *be the quadratic equations in* $x = [x_0, x_1, x_2]$ *which define* C, D *respectively, and consider the expansion*

$$\sqrt{\det(t\,C + D)} = A_0 + A_1 t + A_2 t^2 + \ldots$$

of the square root of the determinant of the quadratic form $t\,C(x) + D(x)$. *Then the Poncelet construction yields a finite polygon of* n *sides (with arbitrary starting data) if, and only if,*

$$\begin{vmatrix} A_2 & \cdots & A_{m+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ A_{m+1} & \cdots & A_{2m} \end{vmatrix} = 0 \qquad n = 2m+1\,, \text{ or}$$

$$\begin{vmatrix} A_3 & \cdots & A_{m+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ A_{m+1} & \cdots & A_{2m} \end{vmatrix} = 0 \qquad n = 2m\,.$$

It is our pleasure to thank Marcel Berger for pointing out to us the Cayley references, which he found discussed extensively in the book "Les Coniques" by Henri Lebesgue.

---

[1]) *A Poncelet Theorem in Space*, to appear in Comment. Math. Helvitici.

[2]) This word appears in the classical literature on the Poncelet theorem. According to the Random House Dictionary, a porism is "a proposition affirming the possibility of finding such conditions as will render a certain problem indeterminate, or capable of innumerable solutions".

[3]) The references to Cayley are given in a footnote to our paper [1]).

1. Points of finite order on elliptic curves

Let E be an elliptic curve over the complex numbers with origin $\mathfrak{o}$. In practice E will have various realizations as an algebraic curve defined by polynomial equations in projective space; e.g., as a plane cubic, the intersection of two quadrics in $\mathbf{P}^3$, etc. All of these projective models are birationally isomorphic to the given curve E. It is well known that E admits a commutative group law with $\mathfrak{o}$ being the identity, and we are interested in the points p of finite order n defined by

$$np = \mathfrak{o}$$

where $np = p + \dots + p$ (n times). Specifically, we pose the question of finding a projective model of E relative to which these points have a simple explicit description.

From a complex-analytic point of view we may realize E as the Riemann surface

$$E = \mathbf{C}/\Lambda$$

obtained by factoring the complex u-plane by a lattice Λ with $u = 0$ projecting onto the origin $\mathfrak{o}$; this is a consequence of Abel's theorem [1]). The group law on E is obtained from the additive structure on $\mathbf{C}$, and so if $u_0 \in \mathbf{C}$ projects onto $p \in E$ the finite order condition is

(1) $$nu_0 \equiv 0 \text{ modulo } \Lambda .$$

In particular there are n^2 points of finite order n on E corresponding to the points of

$$\frac{1}{n}\Lambda.$$

Our problem may be generalized to that of giving projective meaning to the equation

(2) $$u_1 + \dots + u_n \equiv 0 \text{ modulo } \Lambda ,$$

which specializes to (1) when the u_i tend together. Here again the basic step is the following variant of *Abel's theorem* [2]) *: Given* $u_i, v_i \in \mathbf{C}$ $(i = 1, \dots, n)$

---

[1]) This is the classical version of Abel's theorem used in [1]).
[2]) C.f. L. Ahlfors, *Complex Analysis*, McGraw-Hill (New York), Exercise 2 on page 267. This may be thought of as providing a converse to the classical Abel's theorem.

there is an entire meromorphic function $f(u)$ *with period lattice* Λ *and having zeroes at* $u_i + \Lambda$ *and poles at* $v_i + \Lambda$ *if, and only if,*

$$u_1 + \ldots + u_n \equiv v_1 + \ldots + v_n \text{ modulo } \Lambda\,.$$

It follows that the vector space $H^0\left(\mathcal{O}_E([n\mathfrak{o}])\right)$ of rational functions on E having a pole of order at most n at $\mathfrak{o}$, or equivalently the entire meromorphic functions $f(u)$ which have period lattice Λ and a pole of order at most n at $u = 0$, has dimension n. If we choose a basis $f_1, \ldots, f_n$ for this vector space, then for $n \geqq 3$ the mapping

$$F(u) = [f_1(u), \ldots, f_n(u)]$$

induces a projective embedding

$$E \to \mathbf{P}^{n-1}$$

whose image is easily proved to be a smooth algebraic curve of degree n. Thus, for $n = 3$ we have a plane cubic, for $n = 4$ the intersection of two quadrics in $\mathbf{P}^3$, etc. In general we shall call the image the *normal elliptic curve of degree* n. According to Abel's theorem the hyperplane sections of this curve, which are just the zeroes of functions $f \in H^0\left(\mathcal{O}_E([n\mathfrak{o}])\right)$, are characterized by $u_1 + \ldots + u_n \equiv 0$ modulo Λ. Put differently, the condition (2) is equivalent to

$$\det \left\| f_i(u_j) \right\| = 0 \tag{3}$$

expressing the failure of the points $F(u_1), \ldots, F(u_n)$ to be in general position. If we denote by

$$WF(u) = \begin{vmatrix} f_1(u) & \ldots & f_n(u) \\ f_1'(u) & & f_n'(u) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ f_1^{(n-1)}(u) & \ldots & f_n^{(n-1)}(u) \end{vmatrix}$$

the Wronskian of the functions $f_i(u)$, then by letting the u_i tend together the condition (3) specializes to the equation

$$WF(u) = 0 \tag{4}$$

characterizing the solutions to (1). Points satisfying (4) will be called *hyperflexes*, and what we have shown is that:

The points of order n *on an elliptic curve are precisely the hyperflexes of the normal elliptic curve of degree* n.

Now we observe that the equation (4) is independent of the selection of basis $\{f_i\}$ and local coordinate u on E. To see therefore whether or not a given point p is of finite order n we will make convenient choices. Namely, we may choose a basis $\{1, f(u)\}$ for $H^0(\mathcal{O}_E([2\mathfrak{o}]))$ such that $f(p) = 0$. In other words, the function f induces a 2-to-1 map

$$f : E \to \mathbf{P}^1 \tag{5}$$

with $p \in f^{-1}(0)$. It is well-known that the representation (5) has four branch points, one of which is the point at infinity with $f^{-1}(\infty) = \mathfrak{o}$. If we let x be the coordinate on $\mathbf{P}^1$ and a, b, c the finite branch points, then E is conformally represented as the Riemann surface of the algebraic function $\sqrt{(x-a)(x-b)(x-c)}$.

Put another way, the plane cubic curve with affine equation

$$y^2 = (x-a)(x-b)(x-c) \tag{6}$$

gives a projective model of E. Setting $x = f(u)$, since the holomorphic differential du is a constant multiple of dx/y it follows that, with a suitable normalization, $2y = f'(u) = \dfrac{df(u)}{du}$. Consequently the projective model (6) of E is given by the mapping $E \to \mathbf{P}^2$ associated to the basis $\{1, f(u), f'(u)\}$ of $H^0(\mathcal{O}_E([3\mathfrak{o}]))$. Of course, $f(u)$ and $f'(u)$ are essentially the Weierstrass functions. We recall that that their Laurent series around $u = 0$ are

$$\left\{\begin{aligned} f(u) &= \frac{1}{u^2} + \cdots \\ f'(u) &= \frac{-2}{u^3} + \cdots \\ &\ \ \vdots \\ f^{(k)}(u) &= \frac{(-1)^k (k+1)!}{u^{k+2}} + \cdots \end{aligned}\right. \tag{7}$$

Returning to our question of whether $p \in f^{-1}(0)$ is of finite order n, we will use $x = f(u)$ as local coordinate around p and choose the functions

$$
(8) \qquad \begin{cases} 1, x, \ldots, x^m; y, xy, \ldots, x^{m-1}y & n = 2m+1 \\ 1, x, \ldots, x^m; y, xy, \ldots, x^{m-2}y & n = 2m \end{cases}
$$

as basis for $H^0(\mathcal{O}_E([n\mathfrak{o}]))$. That this choice gives a basis follows from the Laurent series (7). It is now an easy matter to express the Wronskian equation (4) at $x = 0$.

We consider the case $n = 2m + 1$ and let $\dfrac{dg(x)}{dx}$ be the derivative of $g(x)$ *evaluated at* $x = 0$. The choice of basis (8) facilitates the evaluation of the Wronskian. For example, from $\dfrac{d^k(x^l)}{dx^k} = 0$ for $k > l$ the Wronskian has the form

$$
\left|\begin{array}{ccc|c}
1 & \ldots & 0 & \text{———} \\
. & . & . & \\
. & . & . & \text{———} \\
. & . & . & \\
0 & \ldots & m! & \text{———} \\
\hline
0 & \ldots & 0 & \text{———} \\
. & . & . & \\
. & . & . & \text{———} \\
. & . & . & \\
0 & \ldots & 0 & \text{———}
\end{array}\right| ,
$$

so that (4) is equivalent to

$$
(9) \qquad \begin{vmatrix}
\dfrac{d^{m+1}y}{dx^{m+1}} & \dfrac{d^{m+1}(xy)}{dx^{m+1}} & \ldots & \dfrac{d^{m+1}(x^{m-1}y)}{dx^{m+1}} \\
\dfrac{d^{m+2}y}{dx^{m+2}} & \dfrac{d^{m+2}(xy)}{dx^{m+2}} & \ldots & \dfrac{d^{m+2}(x^{m-1}y)}{dx^{m+2}} \\
. & . & & . \\
. & . & & . \\
. & . & & . \\
\dfrac{d^{2m}y}{dx^{2m}} & \dfrac{d^{2m}(xy)}{dx^{2m}} & \ldots & \dfrac{d^{2m}(x^{m-1}y)}{dx^{2m}}
\end{vmatrix} = 0
$$

If the series expansion of $y(x)$ is

$$y(x) = \sum_{k=0}^{\infty} A_k x^k ,$$

then (9) is

$$\begin{vmatrix} (m+1)!\ A_{m+1} & (m+1)!\ A_m & \dots & (m+1)!\ A_2 \\ (m+2)!\ A_{m+2} & (m+2)!\ A_{m+1} & \dots & (m+2)!A_3 \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ (2m)!\ A_{2m} & (2m)!\ A_{2m-1} & \dots & (2m)!\ A_{m+1} \end{vmatrix} = 0 .$$

In summary we have proved

(10) *Let E be an elliptic curve with origin $\mathfrak{o}$ and $p \in E$ a given point. Then p is of finite order $n \Leftrightarrow$ the following condition is satisfied: Choose rational functions x, y on E having poles of respective orders 2, 3 at $\mathfrak{o}$ but which are regular elsewhere and with $x(p) = 0$. Then there is an equation $y^2 = (x-a)(x-b)(x-c)$ where a, b, c are distinct and non-zero, and we write*

$$y = \sqrt{(x-a)(x-b)(x-c)} = \sum_{k=0}^{\infty} A_k x^k .$$

The finite order condition is

$$\begin{vmatrix} A_2 & A_3 & \dots & A_{m+1} \\ A_3 & A_4 & \dots & A_{m+2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ A_{m+1} & A_{m+2} & \dots & A_{2m} \end{vmatrix} = 0 , \quad n = 2m+1$$

$$\begin{vmatrix} A_3 & A_4 & \dots & A_{m+1} \\ A_4 & A_5 & \dots & A_{m+2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ A_{m+1} & A_{m+2} & \dots & A_{2m} \end{vmatrix} = 0 , \quad n = 2n .$$

2. Application to the Poncelet problem

We consider two smooth conics C and D meeting transversely at four points x_i $(i = 0, 1, 2, 3)$ of the projective plane $\mathbf{P}^2$. The dual conic $D^* \subset \mathbf{P}^{2*}$ consists of the tangent lines ξ to D, and we consider the incidence correspondence

$$E \subset C \times D^*$$

of pairs $p = (x, \xi)$ with $x \in \xi$ (c.f. Figure 1 above). E is the basic algebraic curve underlying the Poncelet construction, and we shall now examine it.

Referring again to Figure 1, there are on E a pair of involutions defined by

$$\begin{cases} i\,(x, \xi) = (x', \xi) \\ i'\,(x', \xi) = (x', \xi') \end{cases}$$

whose composition $j = i' \circ i$ is given by $j\,(x, \xi) = (x', \xi')$. It follows that Poncelet's construction beginning at $p = (x, \xi)$ gives a closed polygon of n sides if, and only if,

$$j^n(p) = p\,.$$

The mapping

$$(x, \xi) \to x$$

represents $E \to C$ as a two-sheeted branched covering whose branch points are just the points $x_i \in C \cap D$ $(i = 0, 1, 2, 3)$, and the involution i' interchanges the sheets of this mapping (c.f. Figure 2 below). Similarly, i interchanges the two sheets of the mapping $E \to D^*$ given by $(x, \xi) \to \xi$ whose branch points are the four bitangents to the pair of conics. It follows that if we choose the origin to be $\mathfrak{o} = (x_0, \xi_0)$ in Figure 2 below

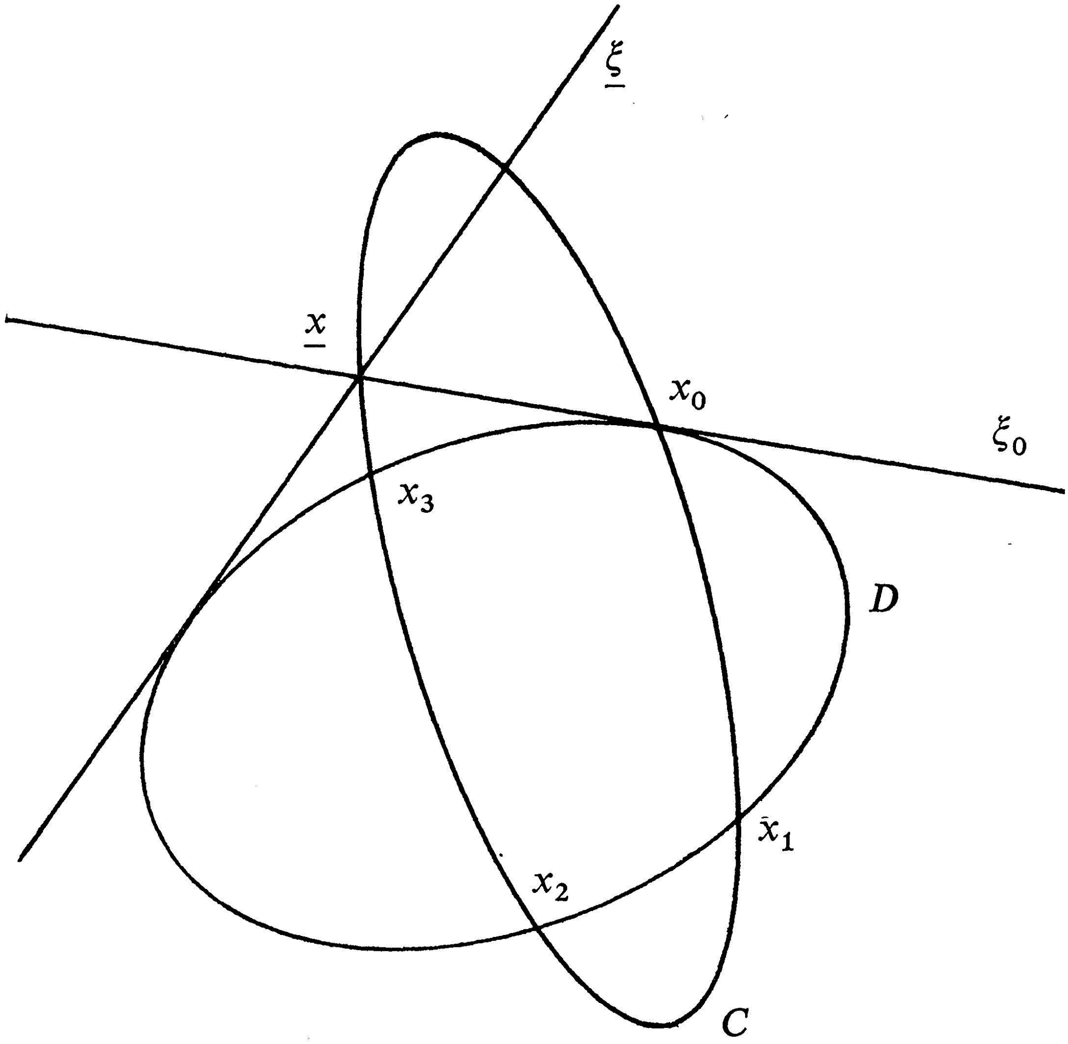

Figure 2

then E is an elliptic curve; i.e. a smooth algebraic curve of genus one with a marked point chosen as the identity for the group law. If we let $p = (\underline{x}, \underline{\xi})$ in Figure 2, then the Poncelet theorem is:

The Poncelet construction gives a closed polygon of n *sides with arbitrary initial data* $q = (x, \xi) \in E$ *if, and only if,*

$$np = \mathfrak{o} \tag{11}$$

on the elliptic curve E.

Proof. We want to show that (11) is equivalent to

$$j^n(q) = q$$

for an arbitrary point $q \in E$. On the universal covering $\mathbf{C}$ of E any involution i_1 having at least one fixed point lifts to

$$\tilde{i}_1(u) \equiv -u + v \text{ modulo } \Lambda ,$$

and $i_1(\mathfrak{o}) = \mathfrak{o}$ is equivalent to $v \in \Lambda$. It follows that

$$\begin{cases} \tilde{i}(u) \equiv -u - w \text{ modulo } \Lambda \\ \tilde{i}'(u) \equiv -u \qquad \text{ modulo } \Lambda, \end{cases}$$

so that

$$\tilde{j}(u) \equiv u + w \text{ modulo } \Lambda,$$

and consequently

$$j^n(q) = q \Leftrightarrow nw \equiv 0 \text{ modulo } \Lambda.$$

Taking p to be the image of w in $E = \mathbf{C}/\Lambda$, we have

$$p = j(\mathfrak{o}) = (\underline{x}, \underline{\xi})$$

in Figure 2, which proves our assertion. Q.E.D.

To complete our story we want to combine this result with the explicit formula (10). As in the introduction we consider the pencil of conics

$$D_t = \{ t\, C(x) + D(x) = 0 \}$$

passing through the four base points x_i. The determinant $\det\big(t\, C(x) + D(x)\big)$ is a cubic polynomial in t with non-zero roots t_i $(i = 1, 2, 3)$. For $t \neq t_i$ we draw the tangent line to D_t through x_0 meeting C in a unique residual point $x(t)$. It is easy to see that $t = t_i$ is mapped into x_i (with suitable indexing), and since $D_\infty = C$ the value $t = \infty$ is mapped to x_0. Taking $t = 0$ we see that $t = 0$ corresponds to x, so that in summary:

The elliptic curve E *is birationally equivalent to the Riemann surface of the algebraic function* $\sqrt{\det\big(t\, C(x) + D(x)\big)}$ *with the origin* $\mathfrak{o}$ *corresponding to* $t = \infty$ *and the point* $p = (\underline{x}, \underline{\xi})$ *to one of the two points lying over* $t = 0$.

Combining this with (10) gives Cayley's result stated in the introduction.

(Reçu le 27 juin 1977)

Phillip Griffiths
Joseph Harris

Department of Mathematics
Harvard University
Cambridge, Mass. 02138

Department of Mathematics
Massachusetts Institute
of Technology
Cambridge, Mass. 02138