Rational Poncelet

Johan Los†, Tiemar Mepschen‡ and Jaap Top§
Johan Bernoulli Institute for Mathematics and Computer Science
University of Groningen, Nijenborgh 9, 9747 AG Groningen, Netherlands
†J.Los@tudelft.nl
‡sjoontimo@gmail.com
§j.top@rug.nl

Received 12 January 2018
Accepted 25 April 2018
Published 5 July 2018

We construct rational Poncelet configurations, which means finite sets of pairwise distinct $K$-rational points $P_1, \ldots, P_n$ in the plane such that all $P_i$ are on a fixed conic section defined over $K$, and moreover the lines $P_1P_2, P_2P_3, \ldots, P_{n-1}P_n, P_nP_1$ are all tangent to some other fixed conic section defined over $K$. This is done for $K = \mathbb{Q}$ in which case only $1 < n < 11$ and $n = 12$ are possible, and for certain real quadratic number fields $K$; here moreover $n = 11$ and $12 < n < 17$ and $n = 18$ occur, but no further new values of $n$. In fact, for every pair $(K, n)$ presented here, we show that infinitely many such tuples $(P_1, \ldots, P_n)$ exist.

The construction uses elliptic curves $E$ over $K$ such that the group $E(K)$ is infinite and moreover contains a point of exact order $n$. As an aside, a formulation of Mazur’s theorem/Ogg’s conjecture in terms of arbitrary genus one curves over the rational numbers (so not necessarily containing any rational point) is presented, since this occurs naturally in the context of Poncelet configurations.

Keywords: Poncelet closure theorem; elliptic curve; torsion point.

Mathematics Subject Classification 2010: 11G05, 14H52, 51N35

1. Introduction

Poncelet’s closure theorem, stated and proven originally by Jean-Victor Poncelet (1788–1867) while he was imprisoned as a prisoner of war in Saratov (Russia), is the following. Suppose $C \neq D$ are two reduced and irreducible conic sections in the plane. Let $P = P_1 \in C$ and let $\ell = \ell_1$ be a line containing $P$, such that $\ell$ is tangent to $D$. One now defines inductively, for $n = 1, 2, \ldots$ the point $P_{n+1} \in C$ as the second point of intersection of $C$ and $\ell_n$, and the line $\ell_{n+1}$ as the second line containing $P_{n+1}$ and tangent to $D$ (note that $\ell_n$ also has this property).

*Parts of this paper originated from Johan’s bachelor’s thesis (2013) at Groningen University and Tiemar’s bachelor’s thesis (2017) at Groningen University.
In this way, one obtains a sequence

\[(P_1, \ell_1), (P_2, \ell_2), \ldots, (P_n, \ell_n), \ldots\]

The special cases where either \(P_j \in C \cap D\) for some \(j\), or \(\ell_j\) is tangent to both \(C\) and \(D\) for some \(j\), both trivially result in a periodic sequence; these cases we will call “trivial periodic Poncelet sequences”, see also [2, 7.6–7.9]. Poncelet’s result states that if for some pair \((P, \ell)\) and obtains a nontrivial periodic sequence with period \(n\), then in fact one obtains an \(n\)-periodic sequence for all starting points \((Q, m)\) with \(Q \in C\) and \(m\) a line tangent to \(D\) and \(Q \in m\).

We refer to [1] for a brief history of the result and to [2] for a more extensive exposition; in fact, the first generally accepted proof of Poncelet’s theorem was given by Jacobi [10] in 1828.

We note that recently a renewed interest in the theorem arose from its relevance to billiard trajectories inside an ellipse, integrable systems, and QRT maps; see, for example, [4, 19, 14, 18, 9, 8].

In the present note, some arithmetical aspects of the closure theorem will be discussed. We first very briefly describe the modern algebraic geometric view on the result, since this will lead to the constructions below.

Denote by \(D^\vee\) the dual of the conic section \(D\); its points correspond to the lines in \(P^2\) which are tangent to \(D\). Note that in fact \(D^\vee\) is itself a conic section in the dual projective plane. Let

\[X := \{ (P, \ell) \in C \times D^\vee : P \in \ell \} \]

Then \(X\) is an algebraic curve. The two projections \((P, \ell) \mapsto P\) respectively, \((P, \ell) \mapsto \ell\) define morphisms \(X \to C\) and \(X \to D^\vee\) of degree 2. Hence they correspond to involutions on \(X\) we denote by \(\sigma : (P, \ell) \mapsto (P', \ell)\) and \(\tau : (P, \ell) \mapsto (P, \ell')\). In general, \(C \cap D\) consists of four distinct points (in the remaining cases, \(C\) and \(D\) share a tangent line and in fact the curve \(X\) is rational and the result is simpler).

We will assume from now on that we are in the general case. Then the involutions \(\sigma\) and \(\tau\) have precisely four fixpoints, and hence \(X\) has genus 1.

If we equip \(X\) with the structure of an elliptic curve by choosing a distinguished point on it (after all, we have points \((P, \ell)\) available), then in terms of the group law obtained in this way on \(X\), one concludes that \(\sigma, \tau\) are given by \(x \mapsto \xi_\sigma - x\) respectively, \(x \mapsto \xi_\tau - x\) (here \(x \in X\), and \(\xi_\sigma, \xi_\tau \in X\) are some given points). Hence the composition \(\tau \sigma\), which is the map \((P, \ell) \mapsto (P', \ell')\), is translation over \(\xi_\tau - \xi_\sigma \in X\). The theorem is now immediate: if the sequence of pairs is periodic then translation is done over a point of finite order, and this makes the sequence periodic regardless of the initial pair of a point and a line.

We will now reverse this reasoning, by starting from an elliptic curve \(E\) with a point on it, and next write the translation over that point as composition of two involutions without fixed points. The quotient by each of these involutions yields a map \(E \to \mathbb{P}^1\) and hence an embedding of \(E\) as a curve of bidegree \((2, 2)\) in \(\mathbb{P}^1 \times \mathbb{P}^1\). With a choice of an isomorphism between the first \(\mathbb{P}^1\) here and any conic section \(C\),
it turns out there is a unique conic section $D$ such that the bihomogeneous equation for $E$ obtained here corresponds to the relation “$P \in \ell$” for points $P \in C$ and lines $\ell \in D$.

So one ends up in the situation of Poncelet’s theorem by choosing the point on $E$ to be a torsion point. Moreover, one obtains situations with all lines and points and conic sections defined over some field $K$ by demanding all points and maps used here to be defined over $K$. We summarize the discussion presented here in the next result.

**Theorem 1.1.** Let $K$ be a number field and $n \in \mathbb{Z}_{\geq 3}$. Conic sections $C \neq D$ over $K$ with $\#(C \cap D) = 4$ exist admitting infinitely many $K$-rational periodic Poncelet sequences of exact period $n$ if and only if an elliptic curve $E/K$ exists with $E(K)$ infinite and containing a point of order $n$.

The proof of this result presented below is constructive, so in particular it allows one to present explicit $K$-rational examples of Poncelet’s closure theorem whenever an elliptic curve with the required properties exists over $K$. In case $K = \mathbb{Q}$ this happens for $n \in \{3, 4, 5, 6, 7, 8, 9, 10, 12\}$, and for suitable real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ one can add all $n \in \{11, 13, 14, 15, 16, 18\}$ to this list. However restricting to these two types of fields, no other values of $n$ are possible.

We now briefly discuss some related work on rationality issues for Poncelet’s closure theorem. The paper [15] by V. A. Malyshev discusses the problem of finding the integers $n$ such that two conic sections $C, D$ defined over $\mathbb{Q}$ exist, yielding purely periodic Poncelet sequences of exact period $n$. However, he does not demand that the points $P_j$ (and therefore the lines $\ell_j = P_jP_{j+1}$ as well) are defined over $\mathbb{Q}$, e.g., the third example he presents in his paper uses $C, D$ given by $x^2 + y^2 = 4$ and $x^2 + y^2 = 3$, respectively. Note that these intersect only at infinity, in 2 complex conjugate points so this example is not of the general type where one demands $\#(C \cap D) = 4$. Since in this example $D(\mathbb{Q}) = \emptyset$, no line defined over $\mathbb{Q}$ will have a rational intersection point with $D$. In particular (using our terminology) no $\mathbb{Q}$-rational Poncelet sequence exists in the present case. However, they exist (periodic of period 5) over many quadratic fields such as $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), \ldots$. The example Malyshev presents on the last page of [15] indeed is a purely periodic $\mathbb{Q}$-rational Poncelet sequence of exact period 5.

Rationality for Poncelet’s closure theorem was also discussed by Mirman in [17], see for example his Corollary 3.5. However, this paper again only demands the conic sections to be defined over $\mathbb{Q}$, and puts no restriction on the field of definition of the points in some purely periodic Poncelet sequence.

An important issue in both the paper of Malyshev and (although treated in a somewhat less general situation) the paper of Mirman is that curves $X$ defined over $\mathbb{Q}$ of genus 1 are used, without demanding that $X$ contains a $\mathbb{Q}$-rational point. As a consequence, it is not immediate how to use arithmetic properties of elliptic curves over $\mathbb{Q}$ in order to draw conclusions about the arithmetic of the curve $X$.

The following result presents an example of this, in fact used in the papers [15, 17].
Similarly, the automorphism corresponding to \( \sigma \tau \) is defined over \( k \) to \( \text{Jacobian of } C \) sequences. To illustrate this, consider the circle \( \sigma \tau \) have product in \( k \).

**Theorem 1.2.** Let \( k \) be a field and \( K \) a function field over \( k \) of genus 1. Suppose \( \sigma, \tau \in \text{Aut}(K) \) are \( k \)-linear involutions such that the fields of invariants \( K^{(\sigma)} \) and \( K^{(\tau)} \) both have genus 0.

If \( \sigma \tau \) has finite order \( n \), then an elliptic curve \( E \) over \( k \) exists containing a \( k \)-rational point of exact order \( n \).

**Proof.** Put \( K = k(X) \) for some curve \( X/k \) of genus 1, and let \( E := \text{Jac}(X) \) be the Jacobian of \( X \). Then \( E \) is an elliptic curve over \( k \). The maps \( \sigma \) and \( \tau \) correspond to \( k \)-rational automorphisms of \( X \) and thereby also of \( E \). These have order 2, and the automorphism corresponding to \( \sigma \tau \) has order \( n \).

Since the quotient of \( X \) and of \( E \) by the map corresponding to \( \sigma \) has genus 0 and \( \sigma \) is defined over \( k \), one obtains on \( E \) an involution \( D \mapsto \delta - D \) for some \( \delta \in \text{E}(k) \). Similarly, \( \tau \) yields \( D \mapsto \epsilon - D \) as involution on \( E \), for some \( \epsilon \in \text{E}(k) \).

As \( \sigma \tau \) has order \( n \), it follows that \( \delta - \epsilon \in \text{E}(k) \) is a point of order \( n \).

**Corollary 1.3.** If \( K \) a function field over \( \mathbb{Q} \) of genus 1 and \( \sigma, \tau \in \text{Aut}(K) \) are involutions such that the fields of invariants \( K^{(\sigma)} \) and \( K^{(\tau)} \) both have genus 0 and moreover \( \sigma \tau \) has finite order \( n \), then \( n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\} \).

**Proof.** This is a consequence of combining Theorem 1.2 with Mazur’s result 16 on torsion of elliptic curves over \( \mathbb{Q} \). 

**Example 1.4.** An example of Corollary 1.3 in which the field \( K \) is not the function field of an elliptic curve is obtained by taking \( K \) the function field over \( \mathbb{Q} \) corresponding to the curve with equation \( y^2 + x^4 = -1 \). Clearly, \( K \) has no places of degree 1 over \( \mathbb{Q} \). The involutions \( \sigma, \tau \) given by \( \sigma(x) = -x, \sigma(y) = y \) and \( \tau(x) = x, \tau(y) = -y \) have product \( \sigma \tau \) of order 2.

Other examples may for instance be constructed using the geometry of Poncelet sequences. To illustrate this, consider the circle \( C \) given by \( x^2 + y^2 = 6 \). Then \( C(\mathbb{Q}) = \emptyset \). Take the (Galois invariant) set of four points \( (\pm \sqrt[3]{3}, \pm \sqrt[3]{3}) \) on \( C \) and the four lines given by \( (x^2 - 3)(y^2 - 3) = 0 \) which form a square having the four points as vertices. The conic section \( D \) given by \( x^2 + xy + y^2 = 9/4 \) has the four given lines as tangent lines. Moreover, \( C \cap D \) consists of four distinct complex points. Therefore, the curve \( X \subset C \times D^\times \) as introduced in this section has genus 1. It is defined over \( \mathbb{Q} \) and by construction it contains no rational points over \( \mathbb{Q} \). The involutions \( \sigma, \tau \) of \( X \) satisfy the conditions of Corollary 1.3 and their product has order 4 in the present case. To make this even more explicit, an affine open part of \( X \) can be described by 4-tuples \((a, b, c, d)\), as follows. The pair \((a, b)\) describes a point \( P \in C \), so \( a^2 + b^2 = 6 \). The pair \((c, d)\) describes the line \( \ell \) with equation \( y = cx + d \). Then \( P \in \ell \) corresponds to the relation \( b = ac + d \) and \( \ell \) being tangent.
to $D$ is described by the equality $d^2 = 3c^2 + 3c + 3$. So $Q(X) = Q(a, b, c, d)$ with relations

$$\begin{align*}
    d^2 &= 3c^2 + 3c + 3, \\
    6 &= a^2 + b^2, \\
    b &= ac + d.
\end{align*}$$

The involution $\sigma$ is here given by

$$\sigma(a, b, c, d) = \left(-a - \frac{2cd}{1 + c^2}, -ac + d - \frac{2c^2d}{1 + c^2}, c, d\right)$$

and similarly

$$\tau(a, b, c, d) = \left(a, b, -c + \frac{2ab + 3}{a^2 - 3}, b + ac - \frac{2a^2b + 3a}{a^2 - 3}\right).$$

2. From Elliptic Curves to Poncelet Sequences

Let $E/K$ be an elliptic curve given by a Weierstrass equation. Suppose $T \in E(K)$ and $T \neq O = (0 : 1 : 0)$. Without loss of generality, we may and will assume $T = (0, 0)$, so $E$ is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x.$$ 

The point $T$ will have order 2 precisely when $a_3 = 0$, and from now on we assume this is not the case. The tangent line to $E$ at $T$ is given by $a_3y = a_4x$, and after a linear change of variables, we can assume this tangent line to be $y = 0$, which brings the equation in the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$ 

Now, the point $T$ will have order 3 precisely when $a_2 = 0$. We will assume $a_2 \neq 0$ so that the order of $T$ is at least 4. Then finally, scaling $(x, y) \rightarrow (\lambda^2x, \lambda^3y)$ for a suitable $\lambda$ we arrive at an equation

$$y^2 + uxy + vy = x^3 + vx^2$$

which, for $v \neq 0$ and $u^4 - u^3 + 8u^2v - 36uv + 16v^2 + 27v \neq 0$ defines an elliptic curve $E$ with point $T = (0, 0)$ not of order 2 or 3, and tangent line a $T$ given by y = 0. Compare the first part of [22, Exercise VIII.8.13] where the same special form is described.

We now decompose the translation over $T$ as a composition of two involutions

$$\begin{array}{c}
    E \xrightarrow{p \mapsto p + T} E \\
    \sigma \quad \tau
\end{array}$$

as follows. For $\sigma$, we take the $-1$ map $\sigma(p) = -p$. Then necessarily $\tau$ is given by $\tau(p) = T - p$. Next, the two projections to $C$ respectively, $D^\nu$ of the curve
$X \subset C \times D \times \mathbb{C}$ described in the introduction will be mimicked in the present situation. To achieve this, one observes that $X \to C$ is a degree 2 cover with Galois group generated by $\tau : (P, \ell) \mapsto (P, \ell')$. In the present situation, we therefore consider the quotient of $E$ by the involution given by $\tau(p) = T - p$, which in coordinates looks like

$$\tau(x, y) = \left(\frac{uvx + vy + v^2}{x^2}, \frac{uv^2x + v^2x^2 + v^3y + v^4}{x^3}\right).$$

Although probably well known, for lack of a proper reference, we now describe the corresponding quotient map in the following lemma.

**Lemma 2.1.** Let $(E, O)$ be an elliptic curve over a field $k$, $T \in E(k)$, and let $\tau : E \to E$ be the involution given by $\tau(p) = T - p$, which induces the involution $\tau^#$ on the function field $k(E)$.

Then the subfield of $k(E)$ consisting of all invariants under $\tau^#$ equals $k(b)$, with $b$ any nonconstant function in the $k$-vector space $L(O + T)$ (the Riemann–Roch space over $k$ associated to the divisor $O + T$).

**Proof.** Since $\tau$ has at least one fixpoint (possibly defined over some finite extension of $k$), the field of invariants of $\tau^#$ has genus 0. Moreover, $E$ and therefore the quotient by $\tau$ as well contain a $k$-rational point, hence the field of invariants is of the form $k(b)$ for some invariant function $b \in k(E)$. Applying a fractional linear transformation to $b$ if necessary, we may (and will) assume that $b$ has a pole at the zero point $O \in E$.

As $\tau$ has order 2, the extension $k(b) \subset k(E)$ has degree 2, which implies that the divisor of poles of $b$ has degree 2. This divisor contains the point $O$, and since $b$ is invariant under $\tau^#$ it contains $\tau(O) = T$ as well. It follows that the divisor of poles of $b$ equals $T + O$ (this is also true in the special case $T = O$, with a slightly adapted reasoning).

So indeed $b \in L(O + T)$. By the Riemann–Roch theorem, the latter vector space has dimension 2 over $k$. It contains the constant functions, so 1 and $b$ form a basis and any element of it can be written uniquely as $\lambda + \mu b$ for some $\lambda, \mu \in k$. Clearly, the nonconstant elements among those are the ones with $\mu \neq 0$, and as $b$ generates $k(b)$ over $k$, so does every such $\lambda + \mu b$.

In the situation at hand, $\tau(p) = T - p$, the quotient map is given by a function $b : E \to \mathbb{P}^1$ where for $b$ we may (by Lemma 2.1) choose any nonconstant element of the Riemann–Roch space $L(O + T)$. We take

$$b := \frac{y + v}{x}.$$

Similarly, the map $c = x : E \to \mathbb{P}^1$ sending a point to its $x$-coordinate has degree 2 and the corresponding Galois group is generated by $\sigma$.

Combining this, one obtains an embedding

$$(b, c) : E \to \mathbb{P}^1 \times \mathbb{P}^1.$$
which in fact yields an isomorphism from $E$ to the curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined by
\[ b^2 c + ubc - vb - c^2 - vc - uv = 0 \]
which by construction is of bidegree $(2, 2)$.

As described in the introduction, the next task is to identify the two $\mathbb{P}^1$'s with a suitable conic section $C$ respectively dual of a conic section $D$. The choice of $C$ is in fact arbitrary; however to make the construction completely explicit, we choose
\[ C : x^2 + y^2 = 1. \]

A well-known identification $\mathbb{P}^1 \cong C$ is given by
\[ b \mapsto P_b := \left( \frac{b^2 - 1}{b^2 + 1}, \frac{2b}{b^2 + 1} \right). \]

Next, the conic section $D$ needs to be constructed. Here, the basic observation is that the variable/function $c$ we have should parametrize a family of lines $\ell_c : y = \alpha(c)x + \beta(c)$. This family is required to have two properties:

1. All lines $\ell_c$ are tangent to some given conic $D$.
2. The bidegree $(2, 2)$ equation should reflect the property that the point $P_b$ is on the line given by $y = \alpha(c)x + \beta(c)$.

The latter of these properties is easy to realize. Namely, we require
\[ \frac{2b}{b^2 + 1} = \alpha(c) \frac{b^2 - 1}{b^2 + 1} + \beta(c) \]
whenever $(b, c)$ satisfy $b^2 c + ubc - vb - c^2 - vc - uv = 0$. One readily checks that taking
\[ \alpha(c) = \frac{c^2 + vc - c + uv}{v - uc}, \quad \beta(c) = \frac{c^2 + vc - c + uv}{uc - v} \]
the desired property holds.

It remains to find the curve $D$ with the property that all lines in the family $y = \alpha(c)x + \beta(c)$ are tangent to it. Already in 19th century mathematics (papers by Cayley, Kummer, and others) such a curve is called the enveloping curve of a system of lines. One obtains its equation by eliminating $c$ from the system
\[ \begin{cases} y = \alpha(c)x + \beta(c), \\ 0 = \alpha'(c)x + \beta'(c) \end{cases} \]
with $\alpha', \beta'$ the derivative of $\alpha$ respectively, $\beta$ with respect to $c$. In the present case, a straightforward calculation shows that $D$ is given by
\[ (v^2 + 2v + 1 - 4uv)x^2 + (2uv + 2u + 4v)xy + u^2 y^2 + (8uv - 2v^2 + 2)x + (2u - 2uv + 4v)y = 4uv - v^2 + 2v - 1. \]
In fact, it is not hard to verify that indeed this conic section $D$ has the required property. This means that starting from any point $p \in E$, the sequence

$$(P_{b(p+nT)}, \ell_{c(p+nT)})_{n \geq 0}$$

is a Poncelet sequence with respect to the conic sections $C$ and $D$.

3. Elliptic Curves of Positive Rank with a Point of Given Finite Order

We now use Theorem 1.1 to determine which nontrivial $\mathbb{Q}$-rational periodic Poncelet sequences, and also $K$-rational ones for some real quadratic $K$, exist. A famous result of Mazur [16] (see [21] for the intriguing history of this problem) states that a rational point of finite order on an elliptic curve over $\mathbb{Q}$ exists if and only if there is a $j$-invariant of an elliptic curve in the set

$$\{\ldots, -237328, -32768, -768, -64, -27, -3, 0, 3, 27, 36729, 4104, 5472, 742982, 882\}$$

Moreover, we want the group of rational points on $E/K$ to be infinite, allowing one to have an abundance of starting points and lines for a periodic $K$-rational Poncelet sequence of exact period $n$. Finally, to be able to “see” the associated conic sections and points and lines in an actual real picture, we need an embedding $K \subset \mathbb{R}$. For quadratic fields, this means we will restrict to real quadratic fields.

3.1. Examples over the rational numbers

For each $n \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, an elliptic curve $E/\mathbb{Q}$ of smallest possible conductor $N$ and $E(\mathbb{Q})$ infinite and containing a point of exact order $n$ is presented here. The examples were obtained by consulting Cremona’s tables [23]. In all cases given below, in fact, one finds $E(\mathbb{Q}) \cong \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. For the curves listed, we present the conductor $N$, and a point $p$ generating the infinite cyclic group $E(\mathbb{Q})$ modulo torsion. The point $T = (0, 0)$ has order $n$ for the curves below. The results are

<table>
<thead>
<tr>
<th>$n$</th>
<th>$N$</th>
<th>Equation</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>117</td>
<td>$y^2 + xy + \frac{1}{4}y = x^3 + \frac{5}{4}x^2$</td>
<td>$(1, -2)$</td>
</tr>
<tr>
<td>5</td>
<td>123</td>
<td>$y^2 + 4xy + 3y = x^3 + 3x^2$</td>
<td>$(-1, 2)$</td>
</tr>
<tr>
<td>6</td>
<td>130</td>
<td>$y^2 + \frac{3}{2}xy - \frac{5}{16}y = x^3 - \frac{5}{16}x$</td>
<td>$(1/2, -1/4)$</td>
</tr>
<tr>
<td>7</td>
<td>574</td>
<td>$y^2 - 55xy - 448y = x^3 - 448x^2$</td>
<td>$(-42, -882)$</td>
</tr>
<tr>
<td>8</td>
<td>966</td>
<td>$y^2 + \frac{3}{2}xy - \frac{9}{16}y = x^3 - \frac{9}{16}x^2$</td>
<td>$(-70/3, 784/9)$</td>
</tr>
<tr>
<td>9</td>
<td>1482</td>
<td>$y^2 - 47xy - 624y = x^3 - 624x^2$</td>
<td>$(-6, 90)$</td>
</tr>
<tr>
<td>10</td>
<td>6270</td>
<td>$y^2 - \frac{19}{11}xy + \frac{120}{121}y = x^3 + \frac{120}{121}x^2$</td>
<td>$(12/11, 252/121)$</td>
</tr>
<tr>
<td>12</td>
<td>4290</td>
<td>$y^2 + 79xy - 390y = x^3 - 390x^2$</td>
<td>$(12, -432)$</td>
</tr>
</tbody>
</table>
3.2. Examples over real quadratic fields

Here we list, for each of the integers $n \in \{11, 13, 14, 15, 16, 18\}$, an example of a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ and of an elliptic curve $E : y^2 + uxy + vx = x^3 + vx^2$ over $K$, such that $E(K)$ is infinite and $(0, 0) \in E(K)$ has order $n$. To allow the verification that indeed for all of these cases $E(K)$ is infinite, we list in a second table for each instance a point of infinite order.

Elliptic curves with a point of exact order $n$ are parametrized by the modular curve $X_1(n)$. The values of $n$ considered here are precisely those for which this modular curve is either elliptic or hyperelliptic. In particular, this implies that points of $X_1(n)$ defined over quadratic fields are easy to find in the case at hand. We used explicit equations of these modular curves as provided, e.g., by Reichert [20] and by Sutherland [23]. We simply searched for examples until one was found (usually one of the first four attempts worked) with a real quadratic field and corresponding elliptic curve of positive rank. Only for the last case $n = 18$, this naive approach was unsuccessful. However, a paper [3] by Bosman et al. presents an example for this specific case. Note that in contrast with the case over $\mathbb{Q}$, here we make no claim concerning minimality in any sense of the given example. For example, the curve $X_1(11)$ has infinitely many points defined over $\mathbb{Q}((\sqrt{2}))$, so it can be expected that many of those points give rise to an elliptic curve over $\mathbb{Q}((\sqrt{2}))$ of positive rank and with a point of order 11. However, we did not find such an example, and instead present one over the field $\mathbb{Q}((\sqrt{73}))$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$u$</th>
<th>$v$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>$-(14 + \sqrt{73})/3$</td>
<td>$-15 - 3\sqrt{73}$</td>
</tr>
<tr>
<td>13</td>
<td>$(151 - 10\sqrt{193})/9$</td>
<td>$(1306 - 94\sqrt{193})/3$</td>
</tr>
<tr>
<td>14</td>
<td>$(2513 + 173\sqrt{105})/728$</td>
<td>$-555 + 87\sqrt{105}/18928$</td>
</tr>
<tr>
<td>15</td>
<td>$(993 + 2\sqrt{345})/875$</td>
<td>$(11750 + 146\sqrt{345})/109375$</td>
</tr>
<tr>
<td>16</td>
<td>$121 + 39\sqrt{10}$</td>
<td>$-3510 - 1107\sqrt{10}$</td>
</tr>
<tr>
<td>18</td>
<td>$(10100 - 21\sqrt{26521})/13625$</td>
<td>$-(13179867 + 81003\sqrt{26521})/37128125$</td>
</tr>
</tbody>
</table>

Points $p$ of infinite order:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>$(1 + \sqrt{73}, 4 + 4\sqrt{73})$</td>
</tr>
<tr>
<td>13</td>
<td>$(97 - 7\sqrt{193}, -5418 + 390\sqrt{193})$</td>
</tr>
<tr>
<td>14</td>
<td>$((105 - 51\sqrt{105})/56, (-1665 + 315\sqrt{105})/112)$</td>
</tr>
<tr>
<td>15</td>
<td>$((650 - 66\sqrt{345})/3125, (11592 - 424\sqrt{345})/78125)$</td>
</tr>
<tr>
<td>16</td>
<td>$(-24 - 9\sqrt{10}, 522 + 162\sqrt{10})$</td>
</tr>
<tr>
<td>18</td>
<td>$((1734 + 12\sqrt{26521})/13625, (7239978 + 26838\sqrt{26521})/185640625)$</td>
</tr>
</tbody>
</table>
Also, for integers $d$ with $d \in \{3, 4, 5, 6\}$ at least the set of primes $p$ such that a number field $K$ with $[K : \mathbb{Q}] = d$ and an elliptic curve $E/K$ exist with $E(K)$ containing a point of order $p$ are explicitly known, see [6]. We did not try to exhibit explicit examples of this kind with moreover $E(K)$ infinite and $K$ admitting a real embedding. Useful references for such an attempt are [11] (e.g., for elliptic curves with a point of order 20 over cubic fields), [12] (quartic number fields and various torsion orders $\leq 24$), and [7].

4. Explicit Rational Periodic Poncelet Sequences

Applying the construction explained in Sec. 2 to the elliptic curves presented in Sec. 3 with the points $T = (0, 0)$ (of order $n$) and $p$ (of infinite order), one obtains explicit periodic Poncelet sequences of exact period $n$. We illustrate this with the following examples. In all cases, $C$ is the circle with equation $x^2 + y^2 = 1$. The conic section $D$ is as constructed at the end of Sec. 2, and $P_j = P_{b_j} + p T$ for $0 \leq j < n$ are points on $C$ that yield a periodic Poncelet sequence with exact period $n$.

$n = 4$

\[
D : 4x^2 + 36xy + 9y^2 + 40x + 24y = 8 \quad \text{(hyperbola)}.
\]

\[
P_j : (8/17, -15/17) \rightarrow (0, 1) \rightarrow (5/13, -12/13) \rightarrow (-11/61, -60/61)
\]

$n = 7$

\[
D : 101249x^2 + 47378xy + 3025y^2 = 204286x + 51182y - 103041 \quad \text{(hyperbola)}.
\]

\[
P_j : (4508/4517, 285/4517) \rightarrow (1155/1157, 68/1157) \rightarrow (264/265, 23/265)
\]

\[
\rightarrow (760/761, 39/761) \rightarrow (399/401, 40/401) \rightarrow (18228/18253, 955/18253)
\]

\[
\rightarrow (70952/71177, 5655/71177)
\]

$n = 9$

\[
270817x^2 + 56066xy + 2209y^2 = 544126x + 61246y - 273313 \quad \text{(hyperbola)}.
\]

\[
P_j : (3960/3961, 89/3961) \rightarrow (3843/3845, 124/3845) \rightarrow (2952/2977, -385/2977)
\]

\[
\rightarrow (17472/17497, 935/17497) \rightarrow (24/25, 7/25) \rightarrow (1155/1157, 68/1157)
\]

\[
\rightarrow (12/13, 5/13) \rightarrow (39456/39505, 1967/39505)
\]

\[
\rightarrow (43488/43537, -2065/43537)
\]

$n = 11$

\[
D : (2529 + 72\sqrt{73})x^2 + (1950 + 228\sqrt{73})xy + (269 + 28\sqrt{73})y^2
\]

\[
= (5562 + 252\sqrt{73})x + (3198 + 456\sqrt{73})y - 3069 - 180\sqrt{73} \quad \text{(hyperbola)}.
\]
\[ P_0: \left( \frac{-5 - 7\sqrt{73}}{74}, \frac{(7 - 5\sqrt{73})}{74} \right) \]
\[ P_1: \left( \frac{130 + 2\sqrt{73}}{173}, \frac{-20 + 13\sqrt{73}}{173} \right) \]
\[ P_2: \left( \frac{357 - 15\sqrt{73}}{514}, \frac{315 + 17\sqrt{73}}{514} \right) \]
\[ P_3: \left( \frac{9265 + 32\sqrt{73}}{11897}, \frac{-340 + 872\sqrt{73}}{11897} \right) \]
\[ P_4: \left( \frac{493 - 25\sqrt{73}}{914}, \frac{725 + 17\sqrt{73}}{914} \right) \]
\[ P_5: \left( \frac{1978 - 10\sqrt{73}}{2141}, \frac{-297 - 60\sqrt{73}}{2141} \right) \]
\[ P_6: \left( \frac{3 + 9\sqrt{73}}{82}, \frac{27 - \sqrt{73}}{82} \right) \]
\[ P_7: \left( \frac{1978 + 434\sqrt{73}}{5693}, \frac{2852 - 301\sqrt{73}}{5693} \right) \]
\[ n = 16 \]
\[ D: \left( 27993331 + 8852274\sqrt{10} \right)x^2 + \left( 29851 + 9438\sqrt{10} \right)y^2 \]
\[ + \left( 1699082 + 537324\sqrt{10} \right)y + 28007371 + 8856702\sqrt{10} \]
\[ = \left( 1726678 + 546024\sqrt{10} \right)x, \quad (\text{ellipse}). \]
\[ P_0: \left( \frac{20 + 1026\sqrt{10}}{3265}, \frac{285 - 72\sqrt{10}}{3265} \right) \]
\[ P_1: \left( \frac{49020 + 674058\sqrt{10}}{2180665}, \frac{-105336\sqrt{10} + 313685}{2180665} \right) \]
\[ P_4 \equiv \left( \frac{215 + 2744\sqrt{10}}{8899}, \frac{1204 - 490\sqrt{10}}{8899} \right) \]
\[ P_{11} \equiv \left( \frac{4160 + 55\sqrt{10}}{4346}, \frac{704 - 325\sqrt{10}}{4346} \right) \]
\[ P_{15} \equiv \left( \frac{9758658\sqrt{10} + 2203500}{33063601}, \frac{-2637000\sqrt{10} + 8154419}{33063601} \right) \]
\[ n = 18 \]

\[ D : (170676636883853 + 2020987228152\sqrt{26521})x^2 \]
\[ + (84433634152655 - 3149950125000\sqrt{26521})y^2 \]
\[ + (143082928547894 - 16071932493804\sqrt{26521})x \]
\[ + (565957711367150 - 13328897586900\sqrt{26521})y \]
\[ + 3664141366676053 + 14050945265652\sqrt{26521} \]
\[ = (393272425792150 + 19229646300600\sqrt{26521})xy \] \text{(hyperbola).}

\[ P_0 = \left( \frac{273193053407199 + 1799184268125\sqrt{26521}}{805814338160974}, \frac{-68947353579025 + 712898680275\sqrt{26521}}{805814338160974} \right), \]
\[ P_1 = \left( \frac{-417408914 + 1331194\sqrt{26521}}{635848277}, \frac{-324579151 - 1711916\sqrt{26521}}{635848277} \right), \]
\[ P_6 = \left( \frac{-9048474664 - 5291356\sqrt{26521}}{48763048217}, \frac{-47105895121 + 10164064\sqrt{26521}}{48763048217} \right), \]
\[ P_{11} = \left( \frac{-6419898738 - 9719050\sqrt{26521}}{55395520187}, \frac{-54499634815 + 1138060\sqrt{26521}}{55395520187} \right), \]
In all of these examples, infinitely many pairwise different periodic Poncelet sequences of period \( n \) with the points defined over the same field as above can be obtained: simply replace \( P_j \) by \( Q_j := P_{b(mp+jT)} \) with \( m > 1 \). For example, for \( n = 4 \) and \( m = 2 \) (conic sections as given in the first example), this yields the sequence
\[
\begin{pmatrix}
905 \\
16393
\end{pmatrix} \rightarrow \begin{pmatrix}
2145 \\
2273
\end{pmatrix} \rightarrow \begin{pmatrix}
5192 \\
5417
\end{pmatrix} \rightarrow \begin{pmatrix}
-1288 \\
25937
\end{pmatrix}.
\]

5. For Completeness: Period Three

Evidently, it is not hard to construct \( \mathbb{Q} \)-rational periodic Poncelet sequences of exact period 3: start with any three rational points \( P_1, P_2, P_3 \) in the plane, not all on a conic section. Many conic sections \( C \) defined over \( \mathbb{Q} \) exist containing the points \( P_j \), and similarly infinitely many conic sections \( D \) over \( \mathbb{Q} \) tangent to the three lines \( \ell_j \). Choosing these one constructs the desired sequence. Below, we show how this can also be achieved by the methods of the previous sections, so using a suitable elliptic curve.

The smallest conductor of an elliptic curve \( E \) over \( \mathbb{Q} \) of positive rank and admitting a point of order 3 is 91. Indeed, the strong Weil curve \( E \) of conductor 91 is given by
\[
y^2 + y = x^3 + x^2 - 7x + 5.
\]

The point \( p = (-1, 3) \in E(\mathbb{Q}) \) has infinite order, \( T = (1, 0) \in E(\mathbb{Q}) \) has order 3. In fact, \( p \) and \( T \) generate the Mordell–Weil group \( E(\mathbb{Q}) \cong \mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z}) \). We now adapt the construction presented in Sec. 2 to the present situation. The subfield of the function field \( \mathbb{Q}(E) \) of all functions invariant under \( (x, y) \mapsto T - (x, y) \) is, as follows from Lemma 1, generated by
\[
b := \frac{y + 1}{x - 1}.
\]

As before take \( c := x \), then
\[
b^2c - b^2 - c^2 - b - 2c + 5 = 0
\]
is the biquadratic equation for \( E \) in the coordinates \( b, c \). Using again the circle \( C : x^2 + y^2 = 1 \) and the isomorphism \( \mathbb{P}^1 \cong C \) defined by \( b \mapsto P_b = \left( \frac{b^2 - 1}{2b}, \frac{b^2 + 1}{2} \right) \) and lines \( \ell_c : y = \alpha(c)x + \beta(c) \), the biquadratic equation precisely represents the condition \( P_b \in \ell_c \) if one takes
\[
\alpha(c) = c^2 + 3c - 6, \quad \beta(c) = -c^2 - c + 4.
\]
In this case, the lines $\ell_c$ are tangent to the conic section (hyperbola) $D$ with equation

$$33x^2 + 4xy - 46x + 4y = 17.$$ 

Starting from the generator $p$ one obtains the triangle with vertices

$$\left(\frac{3}{5}, \frac{-4}{5}\right), \left(\frac{5}{13}, \frac{12}{13}\right), \text{ and } \left(\frac{21}{29}, \frac{20}{29}\right).$$

If instead the point $T \in E$ of order 3 is taken as starting point then on $E$ one obtains the sequence

$$(nT)_{n \geq 1}$$

of period 3, consisting of $(1,0)$, $(1,-1)$, $O = \infty$, $(1,0)$,... In terms of the $(b,c)$ coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$, this is

$$(\infty, 1), (2,1), (\infty, \infty), (\infty, 1), \ldots$$

On the circle $C$, this yields

$$(1,0), (3/5, 4/5), (1,0), (1,0), \ldots$$

and the corresponding lines tangent to the hyperbola $D$ are

$$y = -2x + 2, (x = 1), (y = -2x + 2), \ldots$$

which yields a trivial periodic Poncelet sequence: the line $x = 1$ is tangent to both $D$ and $C$.

The two previous examples show the $\mathbb{Q}$-rational Poncelet sequences with period 3 one obtains by using the points $(mp + nT)_{n=0,1,2}$, for the two cases $m = 1$ and $m = 0$. As in all examples presented in this text, infinitely many other such $\mathbb{Q}$-rational sequences, all with the same pair of conic sections, are obtained by taking different values of $m \in \mathbb{Z}$.

Acknowledgments

The work described in this paper started with two bachelor’s projects in mathematics at the university of Groningen: by the first author (2013) and by the second author (2017). The idea to make a paper out of that was inspired by discussions about it with Nurdagül Anbar Meidl. Her questions and suggestions made the text into how it appears now; for example Theorem 1.2 and Corollary 1.3 and the examples following this corollary, and also Lemma 2.1 were all motivated by discussions with her. We owe many thanks to Nurdagül, and we really regret her decision not to become a coauthor of the paper; we see her as such...
References

[23] A. V. Sutherland, Torsion subgroups of elliptic curves over number fields (2012); https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf.