university of groningen

faculty of mathematics and natural sciences

Finite groups of automorphisms on genus one curves without rational points

Master thesis

July 2018

Student: Majken Roelfszema s2350629

Primary supervisor: prof. dr. J. Top

Secondary supervisor: prof. dr. M.K. Camlibel

Abstract

Mazur's theorem concerning rational torsion points on elliptic curves over $\mathbb{Q}$ can be reformulated as follows. Given is a genus one curve X over $\mathbb{Q}$. Let σ and τ be involutions in $\mathrm{Aut}_{\mathbb{Q}}(X)$, and suppose the group $G \subset \mathrm{Aut}_{\mathbb{Q}}(X)$ generated by σ and τ is finite. Then G is a dihedral group of order $2n$, with $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. Examples where $X = E$ is an elliptic curve over $\mathbb{Q}$ are relatively easy to construct. The aim of this thesis is for each possible n to find curves X where $X(\mathbb{Q}) = \emptyset$. In order to visualize the situation, the context of Poncelet figures is used. A Poncelet figure containing an n-gon can be made using X exactly when $\mathrm{Aut}_{\mathbb{Q}}(X)$ has such a subgroup G of order $2n$.

Contents

1 Introduction

Consider a curve $X/\mathbb{Q}$ of genus one. A dihedral group D_n of order $2n$ has the following form:

$$D_n = \{< \sigma, \rho > | \rho^n = \sigma^2 = id, \sigma\rho\sigma = \rho^{-1}\}.$$

We have that if $D_n \subset \mathrm{Aut}_{\mathbb{Q}}(X)$, then $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ (Theorem 2). To describe examples of such $D_n \subset \mathrm{Aut}_{\mathbb{Q}}(X)$, one considers two cases:

1. In the case that $X(\mathbb{Q}) \neq \emptyset$, choose a $P \in X(\mathbb{Q})$. The couple (X, P) then defines an elliptic curve over $\mathbb{Q}$, in particular X is a group over $\mathbb{Q}$ with unit element P. If such a (X, P) has an n-torsion point T, then one can define a dihedral group D_n where ρ translates over a point T of order n and σ is the (-1)-map. These ρ, σ trivially satisfy $\mathrm{ord}(\sigma) = 2$ and $\mathrm{ord}(\rho) = n$, and for every $Q \in X$ one has

   $$\sigma\rho\sigma(Q) = \sigma\rho(-Q) = \sigma(-Q + T) = Q - T = \rho^{-1}(Q).$$

   Therefore, $\sigma\rho\sigma = \rho^{-1}$. Using exercise 8.12 of [11], examples for all possible torsion groups $E(\mathbb{Q})_{tors}$ are given in the following table. In the table E is an elliptic curve, G is a group isomorphic to $E(\mathbb{Q})_{tors}$, and P is a point on E of order n.

n	E	G	P $(\mathrm{ord}(P) = n)$
1	$y^2 = x^3 - 2$	$\mathbb{Z}/\mathbb{Z}$	$(0:1:0)$
2	$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
3	$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
4	$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
5	$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
6	$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, -3)$
7	$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
8	$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-8, 40)$
9	$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(9, 19)$
10	$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
12	$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$

2. There is also the case that $X(\mathbb{Q}) = \emptyset$. In this case it is more difficult to find maps that generate such a dihedral group.

The aim of this thesis: *find for each* $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ *an example of a curve* $X/\mathbb{Q}$ *of genus one with* $X(\mathbb{Q}) = \emptyset$ *that has* $D_n \subset \mathrm{Aut}_{\mathbb{Q}}(X)$.

This will be done as follows. A genus one curve $X/\mathbb{Q}$ is created with two involutions $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ such that $\rho = \sigma\tau$ has finite order n. In this case $\sigma\rho\sigma = \sigma(\sigma\tau)\sigma = \tau\sigma = \rho^{-1}$, so the involutions σ, τ generate a dihedral group $D_n \subset \mathrm{Aut}_{\mathbb{Q}}(X)$. The curve X will in most cases be created using a Poncelet figure. Poncelet figures and why they can be used to find our examples are explained in section 2. Then, in section 3, the way examples can be found is explained. The examples that were found are given in section 5.

1.1 Some useful properties of elliptic curves

An elliptic curve E/k is a genus one curve over a field k with a point $\mathcal{O} \in k$. If the characteristic of k is not 2, then up to isomorphism over k such E can be given by an equation of the form

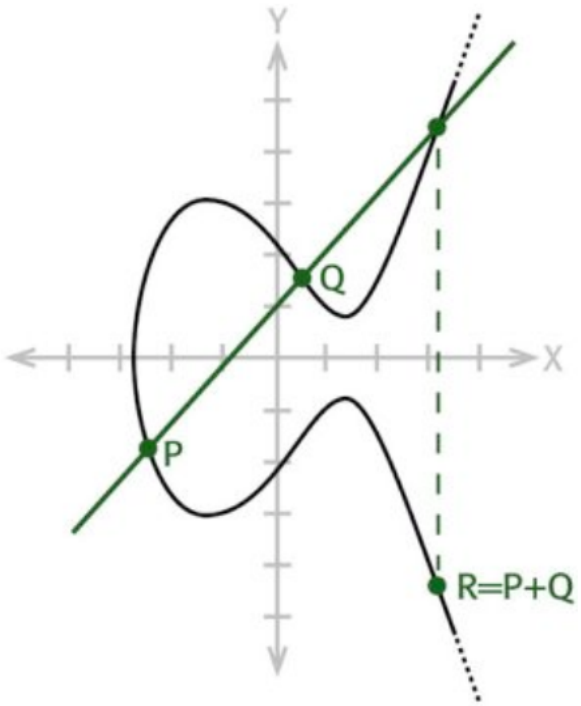
$$y^2 = x^3 + bx^2 + cx + d$$

Let $f \in \mathbb{Q}[x]$ be a separable polynomial of degree 4. It defines a smooth, complete curve $X/\mathbb{Q}$ corresponding to the equation $y^2 = f(x)$. The map $\Psi : X \to \mathbb{P}^1$ acting as $(x, y) \mapsto x$ sends two points to the point at infinity. (Looking at $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ at $x \neq 0$ can be done using the coordinates $\eta = \frac{y}{x^2}, \xi = \frac{1}{x}$. These lead to $\eta^2 = a + b\xi + c\xi^2 + d\xi^3 + e\xi^4$. The points at infinity (for x) correspond to $\xi = 0$, which are two points: $(0, \pm\sqrt{a})$.) Thus the map Ψ only ramifies when $y = 0$, and that gives four points. Therefore, by Hurwitz formula,

$$2g(X) - 2 = 2 \cdot (-2) + 4$$

gives $g(X) = 1$. Let $k = \overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. If a point $P \in X(k)$ is given, then that point can be used to define an elliptic curve structure for X.

One of the interesting properties of an elliptic curve E is its group law. We will denote it by '+'. It works as follows. Taking two points $P, Q \in E$, the line through P and Q intersects E in a third point $-R$. Then mirroring in the x-axis, we get $R = P + Q$. This is illustrated in the following picture [14].



Properties of this group action that will prove useful:

- If $m \cdot P$ has y-value 0, then the point has order dividing $2m$ as $mP + mP = \mathcal{O}$.
- If $r \cdot P$ and $s \cdot P$ have the same x-value, but different y-value, then P has order dividing $r + s$.

Lemma 1. *On an elliptic curve E over some field k, involutions in $Aut_k(X)$ can have two forms:*

$$\begin{aligned} \tau_i &: x \mapsto x + x_i \quad \text{with } x_i \in E \text{ of order 2} \\ \sigma_j &: x \mapsto x_j - x \quad \text{with } x_j \in E \end{aligned}$$

Proof. The following is a split exact sequence.

$$0 \to \{\text{translations}\} \to \mathrm{Aut}(E) \to \mathrm{Aut}(E, \mathcal{O}) \to 0$$

It is called split exact because in addition to being exact, there is a morphism $\mathrm{Aut}(E, \mathcal{O}) \to \mathrm{Aut}(E)$ that, composed with $\mathrm{Aut}(E) \to \mathrm{Aut}(E, \mathcal{O})$ is *id*. Involutions in $\mathrm{Aut}(E)$ can be sent to maps of order 1 or 2 in $\mathrm{Aut}(E, \mathcal{O})$.

- If an involution ϕ is sent to a map of order 1, that map can only be the identity map. In that case, ϕ is in the kernel, so it is translation over a point of order 2.
- If an involution is sent to a map of order 2 (then that can only be $[-1] \in \mathrm{Aut}(E, \mathcal{O})$). Then $\phi = [-1] \circ \tau$ for some translation τ.

□

1.2 Dihedral automorphism groups of genus one curves over $\mathbb{Q}$

Let E be an elliptic curve given by a Weierstrass equation. Take a rational point on E. Applying successively the chord and tangent method, other rational points on E are constructed. This corresponds to translating over a rational point T. Usually, this results in infinitely many rational points, but in specific cases it ends up in a kind of loop. This corresponds to T having finite order in E. Beppo Levi (in 1906-1908) already found that the following structures of the torsion subgroup inside $E(\mathbb{Q})$ of an elliptic curve $E/\mathbb{Q}$ occur infinitely often:

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z} && \text{for } n = 1, 2, \ldots, 10, 12. \\ &\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \text{for } n = 2, 4, 6, 8. \end{aligned}$$

He also showed that some structures do not occur. The conjecture that the above groups are in fact all cases, was studied over the years by Billing, Mahler, Nagell, Ogg, Ligozat, Kubert, Mazur and Tate. They proved that groups with forms as above do not occur as a torsion subgroup for several other values of n. The conjecture is also denoted as Ogg's conjecture and was finally proven in 1976 by Mazur, after which it is called Mazur's theorem [10]. In the case we consider, so $X(\mathbb{Q}) = \emptyset$, an alternative version of Mazur's theorem, as in the article [6] will be used. It states the following.

Theorem 2. *[Possible group orders] Let $X/\mathbb{Q}$ be a genus one curve. Let σ and τ be involutions in $\mathrm{Aut}_{\mathbb{Q}}(X)$, and suppose the group $G \subset \mathrm{Aut}_{\mathbb{Q}}(X)$ generated by σ and τ is finite. Then G is a dihedral group of order $2n$, with $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.*

Proof (as in [6]). Let $X/\mathbb{Q}$ be a curve of genus 1, and let $E = \mathrm{Jac}(X)$ be the Jacobian of X. Then E is an elliptic curve over $\mathbb{Q}$. The maps σ and τ are $\mathbb{Q}$-rational involutions of X and thereby also of E. By assumption, $\sigma\tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ has finite order, and we put $n = \mathrm{ord}(\sigma\tau)$. The corresponding automorphism on E then also has order n. The group $G =< \sigma, \tau >$ is isomorphic to the analogue group in $\mathrm{Aut}_{\mathbb{Q}}(E)$, so it suffices to analyse the latter one. As $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(E)$ has order 2, there are two possibilities (see Lemma 1):

$$\begin{aligned} \sigma &: x \mapsto x + x_i \quad \text{with } x_i \in E(\mathbb{Q}) \text{ a rational point of order 2} \\ \sigma &: x \mapsto x_j - x \quad \text{with } x_j \in E(\mathbb{Q}) \end{aligned}$$

The same holds for $\tau \in \mathrm{Aut}_{\mathbb{Q}}(E)$. Thus all possible cases with involutions $\sigma, \tau \in \mathrm{Aut}_k(X)$ are:

- σ, τ are both translations. Then they generate a group of order 2 or 4, depending on if they are the same or not, so $G = D_1$ or $G = D_2$.
- σ is a translation, τ is not. Then they generate a group of order 4, so $G = D_2$.
- τ is a translation, σ is not. Then they again generate a group of order 4, so $G = D_2$.
- $\sigma : x \mapsto x_1 - x, \tau : x \mapsto x_2 - x$. Then $\sigma\tau : x \mapsto (x_1 - x_2) + x$, so it translates over a point $(x_1 - x_2) \in E(\mathbb{Q})$. By assumption, $G =< \sigma, \tau >$ has finite order. Then $x_1 - x_2$ must be a torsion point. Let $\text{ord}(x_1 - x_2) = n$. Then, it follows from Mazur's theorem that $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. It follows that $G =< \sigma, \tau >= D_n \in \text{Aut}_{\mathbb{Q}}(E)$.

□

2 Poncelet

Jean-Victor Poncelet was a prisoner of war in Russia in 1812-1814. While he was imprisoned he made use of that time to study mathematics. He wrote seven notebooks. In Appendix III, a page from one of the notebooks is given. One of the many things he did in that time was state and prove the theorem now known as Poncelet's closure theorem. Before stating the theorem, some context is given.

Take two distinct irreducible conic sections $\mathcal{C}, \mathcal{D}$ in the plane. We describe the following construction: take a point $P = P_1$ on $\mathcal{C}$ and a line $l = l_1$ through P_1 that is tangent to $\mathcal{D}$. Next, define P_2 to be the other point of intersection of l_1 with $\mathcal{C}$ and define l_2 to be the other tangent line to D through P_2. Repeating this process for $i = 3, \ldots$ one obtains a sequence of couples of the form (P_i, l_i). If after a finite number of couples the process returns $(P_{n+1}, l_{n+1}) = (P_1, l_1)$, where $n+1 > 1$ is the smallest number for which this happens, the sequence is called a Poncelet sequence of order n. Also, in that case the figure created is called a Poncelet figure.

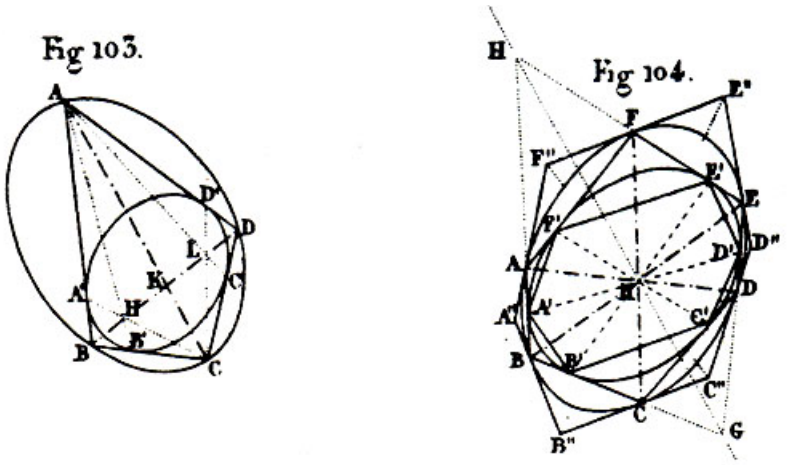


Figure 1: These pictures are included in the book of Poncelet called 'Traité des propriétés projectives des figures'[8].

The special cases where either $P_i \in \mathcal{C} \cap \mathcal{D}$ for some i, or l_i is tangent to both $\mathcal{C}$ and $\mathcal{D}$ for some i, both trivially result in a periodic sequence; these cases we will call 'trivial Poncelet sequences'.

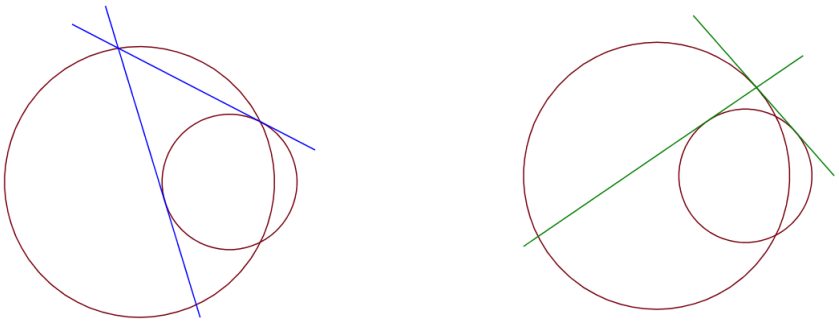


Figure 2: Trivial Poncelet sequences of respectively order 4 and 3.

Theorem 3 (Poncelet)**.** *Let $\mathcal{C}$ and $\mathcal{D}$ be conics in the plane. If an initial pair (P_1, l_1) creates a non-trivial Poncelet sequence of order n, then one obtains an n-periodic sequence for any starting point (P, l) with $P \in \mathcal{C} \cap l$ and l tangent to $\mathcal{D}$.*

The argument given here sketches what Griffiths did to prove this theorem [5]. With more details it can be found in [1].

Context for the proof: Given two conics $\mathcal{C}, \mathcal{D} \subset \mathbb{P}^2$, lines l tangent to $\mathcal{D}$ are the points of the "dual conic" $\mathcal{D}^\vee$. In this way,

$$X := \{(P, l) \ : \ P \in \mathcal{C} \cap l, \ l \text{ tangent to } \mathcal{D}\}$$

defines an algebraic curve embedded in $\mathcal{C} \times \mathcal{D}^\vee$. We study this in the general case, namely when $\mathcal{C}$ and $\mathcal{D}$ intersect without multiplicities, hence in 4 points. Then X has genus one, this is Lemma 7.1 in the section 7 of [1]. The curve X comes with additional structure:

1. The morphism $X \to \mathcal{C}$ given by $(P, l) \mapsto P$ has degree 2: for almost all P, there are precisely 2 lines l, l' containing P and tangent to $\mathcal{D}$.
2. The morphism $X \to \mathcal{D}$ given by $(P, l) \mapsto l \cap \mathcal{D}$ also has degree 2: for almost all $Q \in \mathcal{D}$, the tangent line l to $\mathcal{D}$ at Q will intersect $\mathcal{C}$ in two points P, P'.

The two involutions of X given by, respectively, $\sigma\colon (P, l) \leftrightarrow (P, l')$ and $\tau\colon (P, l) \leftrightarrow (P', l)$ each have 4 fixpoints. Hence X has genus 1, comes with two involutions, and the quotient by any of them has genus 0.

Fixing a point on X, it obtains the structure of an elliptic curve E/k where k is a field. As we saw in the introduction, the involutions in the automorphism group of an elliptic curve can only have two forms. By proposition 4.12 of chapter III of [11], taking the quotient over a translation map results in a curve with the same genus. Therefore, having as quotient a curve of genus 0 (the smooth conics $\mathcal{C}$ and $\mathcal{D}$) means that the involutions must be given as $\sigma\colon x \mapsto x_1 - x$ resp. $\tau\colon x \mapsto x_2 - x$ for certain $x_1, x_2 \in E$ (see Lemma 1). The composition $\sigma\tau$ therefore equals $x \mapsto (x_1 - x_2) + x$, i.e. translation over $x_1 - x_2 \in E$.

Proof. If a Poncelet figure with edges l_j and vertices P_j would exist for $\mathcal{C}, \mathcal{D}$, then $\sigma\tau$ acts as

$$(P_1, l_1) \mapsto (P_2, l_2) \mapsto \ldots \mapsto (P_n, l_n) \mapsto (P_1, l_1),$$

so $(\sigma\tau)^n = id$. Hence any starting point (P_1, l_1) will get mapped back to itself after n steps. This implies the closure theorem. □

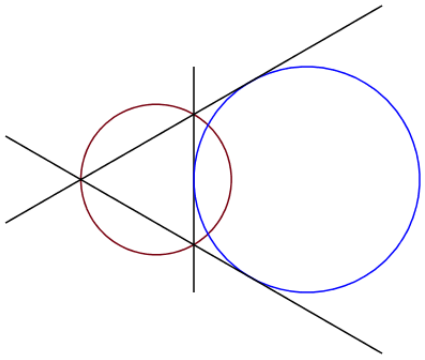
A very old example

The first example of a Poncelet figure was thought of before the theorem was made. An amateur, William Chapple (1746) [2], wrote an article about triangles inscribed in a circle and circumscribed by another circle. He made an equation relating the radii of the circles with the distance between their centers. Let δ be the distance between the centers of the two circles and let their radii be r_1 and r_2 with $r_2 = r \cdot r_1$. Then the equation relating δ and r

$$\delta^2 = 1 - 2r$$

guarantees that a triangle exists that is inscribed in one circle and circumscribed by the other. Thus the circles make a Poncelet figure of order $n = 3$. Similar expressions for $n = 4, 6, 8$ already appeared in two papers (1797 and 1802) by Nicolaus Fuss [3], [4].

We will give a derivation of the equation for $n = 3$ here. Note that we are working in $\mathbb{R}^2$. Also note that given two circles, we can always scale and rotate such that one of them is the unit circle, which we will call $\mathcal{C}$, and the center of the other circle is given by $(\delta, 0)$ for some $\delta \in \mathbb{R}$. The distance between the midpoints is then $|\delta|$. So let $\mathcal{C}$ be the unit circle and let $\mathcal{D} \neq \mathcal{C}$ be $(x-\delta)^2 + y^2 = r^2$. Let $P_1 = (-1, 0)$.



The lines through P_1 are

$$y = c \cdot (x + 1)$$

for some slope c. Assume $P_1 \notin \mathcal{D}$. Then two tangent lines to $\mathcal{D}$ can be found by calculating for which values of c the line intersects $\mathcal{D}$ in exactly one point. So with $c \cdot (x+1)$ substituted for y in $\mathcal{D}$, the discriminant of the resulting quadratic equation in x should be zero:

$$\text{discrim}((x-\delta)^2 + (c \cdot (x+1))^2 - r^2) = 0.$$

This gives the two solutions

$$c_1 = \frac{r\sqrt{\delta^2 + 2\delta - r^2 + 1}}{\delta^2 + 2\delta - r^2 + 1}, c_3 = -\frac{r\sqrt{\delta^2 + 2\delta - r^2 + 1}}{\delta^2 + 2\delta - r^2 + 1}$$

defining the tangent lines $l_1 : y = c_1 \cdot (x+1)$ and $l_3 : y = c_3 \cdot (x+1)$ to $\mathcal{D}$ through P_1. Taking the other intersection points P_2 and P_3 of $\mathcal{C}$ with l_1 and l_3 respectively, we obtain

$$P_2 = \left(\frac{\delta^2 + 2\delta - 2r^2 + 1}{\delta^2 + 2\delta + 1}, 2 \cdot \sqrt{\frac{(\delta^2 + 2\delta - r^2 + 1) \cdot r^2}{(\delta+1)^4}} \right)$$

In order to force this to become a Poncelet figure of order 3, the tangent line to $\mathcal{D}$ through P_2 that is not l_1 should be the vertical line through P_2 and P_3. This is forced by substituting the x-value of those points in $\mathcal{D}$ and demanding that the discriminant with respect to y is zero:

$$\text{discrim}\left(\left(\frac{\delta^2 + 2\delta - 2r^2 + 1}{\delta^2 + 2\delta + 1} - \delta \right)^2 + y^2 - r^2 \right) = 0.$$

Solving the result of this for r^2 gives $r^2 = (\delta+1)^2$ or $r^2 = \frac{1}{4}\delta^4 - \frac{1}{2}\delta^2 + \frac{1}{4} = \frac{(1-\delta^2)^2}{4}$. The first of these would result in $P_1 \in \mathcal{D}$, which we assumed not to be the case. The second gives

$$r^2 = \frac{(1-\delta^2)^2}{4} \Rightarrow \pm r = \frac{1-\delta^2}{2} \Rightarrow \pm 2r = 1 - \delta^2 \Rightarrow \delta^2 = 1 \mp 2r$$

which is essentially the equation Chapple found. So if the circles have distance δ between their centers and difference r between their radii and moreover $\delta^2 = 1 - 2r$, then there exists a non-trivial Poncelet sequence using those circles of order 3. The converse also holds. If there exists a nontrivial Poncelet sequence using $\mathcal{C}$ and $\mathcal{D}$ of order 3, then there is also a 3-periodic sequence for (P_1, l_1) as above as a starting point. Note that Chapple only considers one of the choices of the sign. On page 19 an example is given with the other choice of the sign.

Why Poncelet figures?

Consider a Poncelet figure. The couples (P_i, l_i) of a point on $\mathcal{C}$ and a line tangent to $\mathcal{D}$ through that point can be considered as points of X. This can be expressed using four coordinates. The first two coordinates (a, b) are the coordinates of the point P_i and the last two coordinates (c, d) describe the line l_i, with the equation $y = c \cdot x + d$. In this way, we obtain the points (a, b, c, d) of an affine algebraic model for X in $\mathbb{A}^4$. Also, this model comes with the additional structure as above, and there are involutions σ and τ that generate a dihedral group $D_n \in \mathrm{Aut}_{\mathbb{Q}}(X)$ exactly when the Poncelet figure has order n. We search for cases where X is defined over $\mathbb{Q}$, so we want $\mathcal{C}$ and $\mathcal{D}$ to be defined over $\mathbb{Q}$. Moreover we want that $X(\mathbb{Q}) = \emptyset$ and that $\mathcal{C}, \mathcal{D}$ correspond to a Poncelet figure of order n. Finally, we want $\#\mathcal{C} \cap \mathcal{D} = 4$ to ensure that the genus of the resulting curve equals 1. We will search for such $\mathcal{C}, \mathcal{D}$ using various types of conics.

3 Computations

In this section, the computations for making examples are given in three steps.

- Start from two conics $\mathcal{C}$ and $\mathcal{D}$ defined over $\mathbb{Q}$, assume $\mathcal{C}(\mathbb{Q}) \neq \emptyset$. Then a rational parametrization over $\mathbb{Q}$ of $\mathcal{C}$ exists. This is used to create a model for X of the form $s^2 = f(t)$ with f of degree 4. This f contains some constants in $\mathbb{Q}$ depending on $\mathcal{C}$ and $\mathcal{D}$. Also two points P_1, P_2 of this curve are given, corresponding to a pair (P, l) and its image $\sigma\tau(P, l)$.
- Given such an expression $s^2 = f(t)$ with f of degree 4 with two points P_1, P_2, an elliptic curve E is defined using $s^2 = f(t)$ and P_1. Then the image of P_2 under the map $(s^2 = f(t)) \mapsto E$ will define our translation $\sigma\tau$. This is then forced to have order n.
- Finally, a way of checking if the example of X with $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ has the desired property $X(\mathbb{Q}) = \emptyset$ is discussed.

3.1 An expression for the genus one curve

We start from two conics $\mathcal{C}$ and $\mathcal{D}$ that are defined over $\mathbb{Q}$. A lot of different choices for the conics can be considered. In this part a few of them are shown.

In any case, start from three equations:

1. An equation representing a point $P = (a, b)$ on $\mathcal{C}$.
2. An equation forcing P to lie on the line l given by $y = c \cdot x + d$, so $b = ca + d$.
3. An equation forcing the line l to be tangent to $\mathcal{D}$. So $c \cdot x + d$ is substituted for y in the equation of $\mathcal{D}$ and then the discriminant with respect to x is required to be zero.

3.1.1 Two circles

This case is also studied by Boris Mirman [7]. Using the same starting point, it will be done differently here. Let $\mathcal{C}$ be the unit circle and let $\mathcal{D}$ be $(x - \delta)^2 + y^2 = \rho$ with $\rho \in \mathbb{Q}, \delta \in S = \{\nu^2 + \mu^2 | \nu, \mu \in \mathbb{Q}\}$.

Note that any circle K defined over $\mathbb{Q}$, with center $c = (\nu, \mu)$ with $\nu, \mu \in \mathbb{Q}$ can be rotated to be of the form of such a $\mathcal{D}$. Then the center of the corresponding $\mathcal{D}$ is $(\delta, 0)$ where $\delta^2 = \nu^2 + \mu^2$. Also note that $\rho \in \mathbb{Q}$ does not necessarily mean that the radius of $\mathcal{D}$ is rational.

The system of equations in Theorem 4 is made of the three equations: a point $P = (a, b)$ on $\mathcal{C}$, a line $l : y = c \cdot x + d$ tangent to $\mathcal{D}$ and $P \in l$.

Theorem 4. *The curve given by the system of equations*

$$\begin{cases} a^2 + b^2 = 1 \\ b = c \cdot a + d \\ (\rho - \delta^2)c^2 - 2\delta cd - d^2 + \rho = 0 \end{cases}$$

is birational over $\mathbb{Q}$ to the curve given in (t, s) coordinates by

$$s^2 = (t^2 + 1) \cdot \rho \cdot ((\delta^2 - \rho + 1)t^2 - 4\delta t + (\delta^2 - \rho + 1)). \tag{1}$$

A birational correspondence is given by

$$t = \tfrac{1-b}{a}, \qquad s = \tfrac{A(t)\cdot c + B(t)}{t^2+1}$$

where

$$\begin{aligned} A(t) &= (\delta^2-\rho)(t^4+1) - 4\delta(t^3+t) + (2\delta^2 - 2\rho + 4)t^2, \\ B(t) &= -\delta t^4 + 2t^3 - 2t + \delta. \end{aligned}$$

Proof. Parametrize the unit circle as

$$a = \frac{2t}{t^2+1}, b = \frac{1-t^2}{t^2+1}, \text{ with } t = \frac{1-b}{a}$$

Substitute $d = b - ca$ and this parametration for a and b in

$$(\rho - \delta^2)c^2 - 2\delta cd - d^2 + \rho = 0$$

to obtain

$$\begin{aligned} &c^2\delta^2t^4 - c^2\rho t^4 + 2c^2\delta^2t^2 - 4c^2\delta t^3 - 2c\delta t^4 - 2c^2\rho t^2 - \rho t^4 + c^2\delta^2 - 4c^2\delta t \\ &+4c^2t^2 + 4ct^3 + t^4 - c^2\rho - 2\rho t^2 + 2c\delta - 4ct - 2t^2 - \rho + 1 = 0 \end{aligned}$$

This is an equation of degree two in c since for (almost) every point of $\mathcal{C}$ there are two tangent lines to $\mathcal{D}$ through it given by two values of c.

$$\begin{aligned} &A(t)c^2 + 2\cdot B(t)c + C(t) = 0 \\ &A(t) = (\delta^2-\rho)(t^4+1) - 4\delta(t^3+t) + (2\delta^2 - 2\rho + 4)t^2 \\ &B(t) = -\delta t^4 + 2t^3 - 2t + \delta \\ &C(t) = (1-\delta)(t^4+1) - 2(\delta+1)t^2 \end{aligned}$$

This can be transformed as follows.

$$(A(t)\cdot c)^2 + 2B(t)(A(t)\cdot c) + A(t)C(t) = 0$$

$$(A(t)\cdot c + B(t))^2 + C(t)\cdot A(t) - B(t)^2 = 0$$

Now let $\tilde{c} = A(t)\cdot c + B(t)$. Then

$$\tilde{c}^2 - (t^2+1)^3\rho(\delta^2t^2 - \rho t^2 + \delta^2 - 4\delta t + t^2 - \rho + 1)$$

As this still contains a square, it can be simplified with $s = \frac{\tilde{c}}{t^2+1}$, giving equation (1):

$$s^2 = (t^2+1)\cdot\rho\cdot((\delta^2 - \rho + 1)t^2 - 4\delta t + (\delta^2 - \rho + 1))$$

□

Notice: filling in $\frac{1}{t}$ for t in equation (1), one obtains

$$(\tfrac{1}{t^2}+1)\cdot\rho\cdot((\delta^2-\rho+1)\tfrac{1}{t^2} - 4\delta\tfrac{1}{t} + (\delta^2-\rho+1))$$

$$= \tfrac{1}{t^4}\cdot(t^2+1)\cdot\rho\cdot((\delta^2-\rho+1)t^2 - 4\delta t + (\delta^2-\rho+1))$$

Hence if (t,s) is a point of X, so is $(\frac{1}{t}, \frac{s}{t^2})$. Geometrically this corresponds to the reflection in the x-axis. This is a special case of what we will see in Proposition 8 in Section 4.

Equation (1) is an equation for X in of the form $s^2 = f(t)$. One can easily see that $f(i) = 0$ with $i = \sqrt{-1}$. Hence $P_1 = (i, 0)$ is a point (t, s) of X. This point can be used to give X the structure of an elliptic curve. The next point in the Poncelet figure will be $P_2 = \sigma(\tau(P1))$. This will become the point of order n. The involutions σ, τ are induced by the Poncelet figure as described in Section 2: for points $P, P' \in \mathcal{C}$ and lines l, l' tangent to $\mathcal{D}$,

- $\sigma : (P, l) \mapsto (P, l')$
- $\tau : (P, l) \mapsto (P', l)$

Note that τ keeps c constant, but since s is as in Theorem 4, s does change with t. On the other hand, $\sigma : s \mapsto -s$ as for constant t, $s^2 = f(t)$ has two solutions that add up to zero. Hence $\sigma : (t, s) \mapsto (t, -s)$ and $\tau : (t, s) \mapsto (t_2, s_2)$. Together with

$$t_2 = \frac{c + t}{ct - 1}$$

and filling this in in the following equation

$$s_2 = \frac{A(t_2) \cdot c + B(t_2)}{t_2^2 + 1}$$

we obtain explicit equations for τ. Applying these two involutions to $P_1 = (i, 0)$ gives

$$P_2 = \sigma\tau(i, 0) = \sigma\left(\frac{\delta + i}{1 + i\delta}, \frac{-4\delta\rho}{(1 - i\delta)^2}\right) = \left(\frac{\delta + i}{1 + i\delta}, \frac{4\delta\rho}{(1 - i\delta)^2}\right).$$

3.1.2 Other curves

Circle and ellipse/hyperbola First consider the unit circle $\mathcal{C}$ and $\mathcal{D}$ a conic defined by $(x - \alpha)^2 + \gamma(y - \beta)^2 = \rho$. Also define that the line $y = \delta$ to be one of the tangent lines of $\mathcal{D}$. Then we obtain $\rho = \gamma(\delta - \beta)^2$. So we have the following equations.

Theorem 5. *The curve given by the system of equations*

$$\begin{cases} a^2 + b^2 = 1 \\ b = c \cdot a + d \\ \beta^2c^2\gamma^2 - 2\beta c^2\delta\gamma^2 + c^2\delta^2\gamma^2 - \alpha^2c^2\gamma + 2\alpha\beta c\gamma - 2\alpha cd\gamma + 2\beta d\gamma - 2\beta\delta\gamma - d^2\gamma + \delta^2\gamma = 0 \end{cases}$$

is birational over $\mathbb{Q}$ to the curve given in (s, t) by

$$s^2 = (2\beta\delta\gamma - \delta^2\gamma + \alpha^2 + 2\beta\gamma + \gamma)t^4 - 4\alpha t^3 + (4\beta\delta\gamma - 2\delta^2\gamma + 2\alpha^2 - 2\gamma + 4)t^2 - 4\alpha t \\ +2\beta\delta\gamma - \delta^2\gamma + \alpha^2 - 2\beta\gamma + \gamma.$$

A birational correspondance is given by

$$t = \tfrac{1-b}{a} \qquad s = \tfrac{A(t)\cdot c + B(t)}{\gamma\cdot(t^2+1)\cdot(\beta-\delta)}$$

with

$$A(t) = \gamma(((\beta - \delta)^2\gamma - \alpha^2)t^4 + 4\alpha t^3 + (2(\beta - \delta)^2\gamma - 2\alpha^2 - 4)t^2 + 4\alpha t + (\beta - \delta)^2\gamma - \alpha^2),$$
$$B(t) = \gamma((\beta + 1)t^2 + \beta - 1)(\alpha t^2 + \alpha - 2t).$$

Proof. Again, the unit circle is parametrized.

$$a = \frac{2t}{t^2 + 1}, b = \frac{1 - t^2}{t^2 + 1}, \text{ with } t = \frac{1 - b}{a}$$

Substitute $d = b - ca$ and this parametration for a and b in the third equation of the system. Then an equation in c and t is found. It is of degree two in c since for (almost) every point of $\mathcal{C}$ there are two tangent lines to $\mathcal{D}$ through it given by two values of c.

$$A(t)c^2 + 2 \cdot B(t)c + C(t) = 0$$
$$A(t) = \gamma(((\beta - \delta)^2\gamma - \alpha^2)t^4 + 4\alpha t^3 + (2(\beta - \delta)^2\gamma - 2\alpha^2 - 4)t^2 + 4\alpha t + (\beta - \delta)^2\gamma - \alpha^2)$$
$$B(t) = \gamma((\beta + 1)t^2 + \beta - 1)(\alpha t^2 + \alpha - 2t)$$
$$C(t) = \gamma((-2\beta\delta + \delta^2 - 2\beta - 1)t^4 + (-4\beta\delta + 2\delta^2 + 2)t^2 - 2\beta\delta + \delta^2 + 2\beta - 1)$$

As in the proof of Theorem 4, the following expression is found with $\tilde{c} = A(t) \cdot c + B(t)$.

$$\begin{aligned}\tilde{c}^2 = \quad & -\gamma^2(t^2+1)^2(\beta-\delta)^2((2\beta\delta\gamma - \delta^2\gamma + \alpha^2 + 2\beta\gamma + \gamma)t^4 - 4\alpha t^3 \\ & +(4\beta\delta\gamma - 2\delta^2\gamma + 2\alpha^2 - 2\gamma + 4)t^2 - 4\alpha t + 2\beta\delta\gamma - \delta^2\gamma + \alpha^2 - 2\beta\gamma + \gamma)\end{aligned}$$

Then, getting rid of the unneeded squares, let $s = \frac{A(t)\cdot c + B(t)}{\gamma\cdot(t^2+1)\cdot(\beta-\delta)}$ to obtain the wanted equation.

$$\begin{aligned}s^2 = (2\beta\delta\gamma - \delta^2\gamma + \alpha^2 + 2\beta\gamma + \gamma)t^4 - 4\alpha t^3 + (4\beta\delta\gamma - 2\delta^2\gamma + 2\alpha^2 - 2\gamma + 4)t^2 - 4\alpha t \\ +2\beta\delta\gamma - \delta^2\gamma + \alpha^2 - 2\beta\gamma + \gamma\end{aligned}$$

□

Given the tangent line $y = \delta$ of $\mathcal{D}$, we know that the point $(\sqrt{1-\delta^2}, \delta)$ of $\mathcal{C}$ gives a point (t_1, s_1) of X with

$$t_1 = \frac{1-\delta}{\sqrt{1-\delta^2}} \text{ and } s_1 = \frac{A(t_1)\cdot c + B(t_1)}{\gamma\cdot(t_1^2+1)\cdot(\beta-\delta)}$$

The involutions in this case are $\sigma : (t, s) \mapsto (t, -s)$ and $\tau : (t, s) \mapsto (t_2, s_2)$. Together with

$$t_2 = \frac{c+t}{ct-1} \text{ and } s_2 = \frac{A(t_2)\cdot c + B(t_2)}{\gamma\cdot(t_2^2+1)\cdot(\beta-\delta)}$$

Notice that t_2 here is the same as before, as this is only dependent on $\mathcal{C}$. The points of X were so horrible to work with, that it made sense to simplify the curve $\mathcal{D}$ (and later also the curve $\mathcal{C}$).

Circle and simpler ellipse/hyperbola Take again the unit circle $\mathcal{C}$ and let $\mathcal{D}$ be a conic defined by $x^2 + 2\cdot\alpha xy + \beta y^2 = \gamma$. Take again $y = \delta$ to be tangent to $\mathcal{D}$, then

$$\mathcal{D} : x^2 + \alpha xy + \beta y^2 = (\beta - \alpha^2)\delta^2$$

Theorem 6. *The curve given by the system of equations*

$$\begin{cases} a^2 + b^2 = 1 \\ b = c\cdot a + d \\ -4\alpha^2\beta c^2\delta^2 - 8\alpha^3 c\delta^2 + 4\beta^2 c^2\delta^2 + 8\alpha\beta c\delta^2 + 4\alpha^2 d^2 - 4\alpha^2\delta^2 - 4\beta d^2 + 4\beta\delta^2 = 0 \end{cases}$$

is birational over $\mathbb{Q}$ to the curve given in (s, t) by

$$s^2 = ((-\alpha^2\delta^2 + \beta\delta^2 - \beta)t^4 + 4\alpha t^3 + (-2\alpha^2\delta^2 + 2\beta\delta^2 + 2\beta - 4)t^2 - 4\alpha t - \alpha^2\delta^2 + \delta^2\beta - \beta)\cdot(-\alpha^2 + \beta).$$

A birational correspondance is given by

$$\begin{aligned} t &= \tfrac{1-b}{a}, \qquad s = \tfrac{A(t)\cdot c + B(t)}{4\delta(\alpha^2-\beta)(t^2+1)} \\ &\textit{with} \\ A(t) &= -4(\alpha^2-\beta)(\beta\delta^2 t^4 + (2\beta\delta^2 - 4)t^2 + \beta\delta^2), \\ B(t) &= -2(\alpha^2-\beta)(2\alpha\delta^2 t^4 - 4t^3 + 4\alpha\delta^2 t^2 + 4t + 2\alpha\delta^2). \end{aligned}$$

Proof. Take the proof for Theorem 5 with $A(t), B(t), s$ as in Theorem 6 and

$$C(t) = -4(\alpha^2-\beta)((\delta^2-1)t^4 + (2\delta^2+2)t^2 + \delta^2 - 1)$$

□

Given the tangent line $y = \delta$ of $\mathcal{D}$, we again have the point $(\sqrt{1-\delta^2}, \delta)$ of $\mathcal{C}$ and so a point (t_1, s_1) of X with

$$t_1 = \frac{1-\delta}{\sqrt{1-\delta^2}}, s_1 = \frac{A(t_1)\cdot c + B(t_1)}{4\delta\cdot(\alpha^2-\beta)\cdot(t_1^2+1)}.$$

The involutions in this case are $\sigma : (t, s) \mapsto (t, -s)$ and $\tau : (t, s) \mapsto (t_2, s_2)$. Together with

$$t_2 = \frac{c+t}{ct-1} \text{ and } s_2 = \frac{A(t_2)\cdot c + B(t_2)}{4\delta\cdot(\alpha^2-\beta)\cdot(t_2^2+1)}.$$

Parabola and ellipse/hyperbola *This case is fully worked out in Appendix I.* Let $\mathcal{C}$ be the parabola $y = x^2$. In this was x gives a parametrization of $\mathcal{C}$, which makes life easier. Let $\mathcal{D} : x^2 + axy + by^2 = c$. In order to make sure we have a point on our curve X, $\mathcal{D}$ is forced to have a horizontal tangent line $y = d$, which results in

$$\mathcal{D} : x^2 + axy + by^2 = \frac{d^2(4b-a^2)}{4}$$

Start from a tangent line $l : y = \gamma\cdot x + \delta$, and a point $(x, y) \in \mathcal{C} \cap l$. We obtain the three equations in the system of Theorem 7.

Theorem 7. *Assume $a^2 - 4b \neq 0$. Then the curve given by the system of equations*

$$\begin{cases} y = x^2 \\ y = \gamma\cdot x + \delta \\ bd^2\gamma^2 + ad^2\gamma + d^2 - \delta^2 = 0 \end{cases}$$

is birational over $\mathbb{Q}$ to the curve given in (s, t) by

$$s^2 = 4bx^4 + 4ax^3 + 4x^2 + a^2d^2 - 4bd^2.$$

A birational correspondance is given by

$$\begin{aligned} s &= \tfrac{2\cdot(A(x)\gamma+B(x))}{d} \\ \textit{with} & \\ A(x) &= bd^2 - x^2, \\ B(x) &= \tfrac{ad^2}{2} + x^3. \end{aligned}$$

Using the tangent line we created, we get a point on this curve. Note that since we took a parabola, it was parametrized by x, so the x in the formula is the x-value of the point on $\mathcal{C}$. As we took the tangent line $y = d$, that means we can take $x = \sqrt{d}$ with s coming from the slope of the tangent line. The next point will then have $x = -\sqrt{d}$. The involutions that were used to find these points can be found in Appendix I.

$$P_1 = \left(\sqrt{d}, -\frac{1}{2}ad - \sqrt{d}\right), P_2 = \left(-\sqrt{d}, \frac{1}{2}ad - \sqrt{d}\right)$$

3.2 Finding an example

Let $y = f(x)$ be our equation of degree 4 that describes X. Take two (non-rational) points P_1 and P_2 on X. We know X has genus one. Let E be the elliptic curve that is defined by X and P_1 and let $\phi : X \to E$. Then let $T = \phi(P_2)$. To create a Poncelet figure of order n, $n \cdot T$ must be forced to equal $\mathcal{O}$ on E. Note that $n \cdot T$ will be a projective point $[x, y, z]$ with coordinates expressed in coefficients, depending on which conics were used. Depending on n, it makes sense to compute $n \cdot T$ immediately, $\frac{n}{2} \cdot T$ or $\frac{n+1}{2} \cdot T$ and $\frac{n-1}{2} \cdot T$.

- For small n, $n \cdot T$ is computed directly and $n \cdot T = \mathcal{O}$ if it has $z = 0$. In practice this was only done for $n = 3$.
- For even n, $\frac{n}{2} \cdot T$ is computed and if this is equal to the point on E with $y = 0$, then $n \cdot T = \mathcal{O}$.
- For odd n, $\frac{n+1}{2} \cdot T$ and $\frac{n-1}{2} \cdot T$ are both computed. If they have the same x-value, but different y-value, then $n \cdot T = \mathcal{O}$.

In Magma, these points were calculated and using Maple, they were forced to have the wanted properties.

Recall that for the case of two circles the coefficients are $\{\delta, \rho\}$. Working as described above, we find the following equations in δ and ρ.

$$n = 3: \quad \rho = \frac{(\delta^2-1)^2}{4} \qquad n = 4: \quad \rho = \frac{(\delta^2-1)^2}{2(\delta^2+1)}$$

$$n = 6: \quad \rho = \frac{(\delta^2-1)^2}{4\delta^2} \qquad n = 8: \quad \rho = \frac{(\delta^2-1)^2}{4\delta}$$

As mentioned in the introduction, these four expressions were already known in some form. For $N = 5$ and $N = 10$, we also found equations, but those were not very nice to write down. Finding an example using those proved not to be easy. Fortunately Mirman [7] already found examples and we could check them with the equations we found.

The check

Using Magma [12], it can be tested for a genus one curve corresponding to an equation $y^2 = f(x)$ (with f of degree 4), whether primes p exist such that the curve has no points over $\mathbb{Q}_p$. If such p exists, then clearly the curve has no points over $\mathbb{Q}$ and we have an example of the form we want. The Magma code that was used for this can be found in Appendix II. An explicit calculation by hand is presented in an example on page 18.

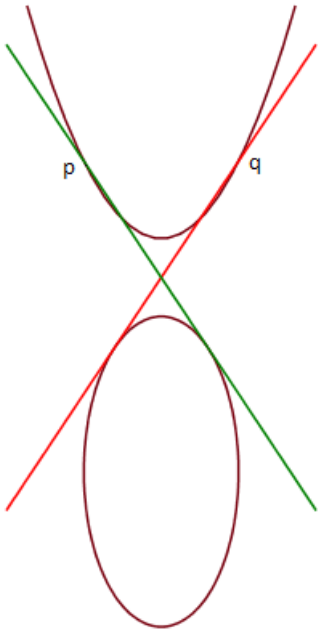
4 An inconvenience

In the previous section, different options for $\mathcal{C}$ and $\mathcal{D}$ were shown. This is because of an inconvenient property of Poncelet figures we came across. In this section that property will be shown.

Proposition 8. *Let $\mathcal{C}$ and $\mathcal{D}$ be two conics defined over $\mathbb{Q}$ that form a Poncelet figure of odd order n. The corresponding $X/\mathbb{Q}$ has $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ such that $\sigma\tau$ has order n. If $\mathcal{C}$ and $\mathcal{D}$ have an axis of symmetry in common, and this axis is defined over $\mathbb{Q}$, then there are also involutions $\sigma', \tau' \in \mathrm{Aut}_{\mathbb{Q}}(X)$ such that $\sigma'\tau'$ has order $2n$.*

In the tekst of Mirman [7], theorem 3.3 is a version of this with the conics being circles. He also gives an explicit description of the new circle $\tilde{\mathcal{D}}$ that together with $\mathcal{C}$ forms a Poncelet pair with order $2n$. A general and more straightforward proof is given here.

Proof. First of all, we take a look at the symmetry in the figure. Let μ denote the map that mirrors in the common symmetry axis.



In the picture that would be the y-axis $x = 0$. The red line with its point q on the parabola would then be mapped to the green line with p.
Then μ has fixed points, and commutes with σ and τ.

This can be checked using a picture, and one can see that given $\sigma : (P, l) \mapsto (P, l')$, $\tau : (P, l) \mapsto (P', l)$ as before and $\mu : (P, l) \mapsto (\tilde{P}, \tilde{l})$ denoting the mirroring in the axis of symmetry.

$$\begin{aligned}
\mu \circ \sigma : (P, l) &\mapsto (P, l') \mapsto (\tilde{P}, \tilde{l'}) \\
\sigma \circ \mu : (P, l) &\mapsto (\tilde{P}, \tilde{l}) \mapsto (\tilde{P}, \tilde{l'}) \\
\mu \circ \tau : (P, l) &\mapsto (P', l) \mapsto (\tilde{P'}, \tilde{l}) \\
\tau \circ \mu : (P, l) &\mapsto (\tilde{P}, \tilde{l}) \mapsto (\tilde{P'}, \tilde{l})
\end{aligned}$$

Let $\sigma : x \mapsto x_\sigma - x$, $\tau : x \mapsto x_\tau - x$ and $\mu : x \mapsto x_\mu - x$. It follows that $\sigma\mu$ is its own inverse, so $(\sigma\mu)^2(x) = x$ and $\sigma\mu : x \mapsto (x_\sigma - x_\mu) + x$ is translation over the point $(x_\sigma - x_\mu)$ of order two. We already know that $\sigma\tau$ translates over a point of odd order n, hence the composition $(\sigma\mu)(\sigma\tau)$ has order $2n$. □

Corollary 9. *There are no Poncelet figures of order 7 (or 9) with circles $\mathcal{C}, \mathcal{D}$ defined over $\mathbb{Q}$.*

Proof. Suppose $\mathcal{C}$ and $\mathcal{D}$ are two circles defined over $\mathbb{Q}$. This means that their centers $c_{\mathcal{C}}, c_{\mathcal{D}} \in \mathbb{Q}^2$ and the line containing both centers is also defined over $\mathbb{Q}$. That line is an axis of symmetry that $\mathcal{C}$ and $\mathcal{D}$ have in common. If $\mathcal{C}, \mathcal{D}$ would form a Poncelet figure of order 7 (or 9), then by Proposition 8 there exists a Poncelet figure of order 14 (or 18). It follows from Theorem 2 that this is impossible. □

An even more general inconvenience: A stronger statement holds. If the two conics have a line symmetry or point symmetry defined over $\mathbb{Q}$ in common, that will give an involution. Then a statement analogous to Proposition 8 holds.

Avoiding the inconvenience. In order to find examples for $n = 7, n = 9$, we need to look at conics with no common rational axis of symmetry. An option that gave a result for $n = 7$ is the construction with a parabola and an ellipse/hyperbola. It turned out to be a parabola with a hyperbola. This example is given in full in Appendix I.

5 Examples

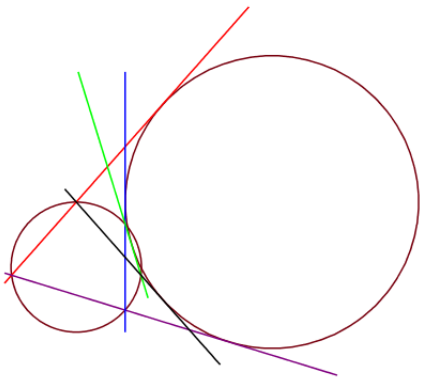
In this section examples for $n = 2, 3, 4, 5, 6, 7, 8, 10, 12$ are given. All of these examples have conics defined over $\mathbb{Q}$ that define an algebraic curve $X/\mathbb{Q}$ of genus one with $X(\mathbb{Q}) = \emptyset$ and involutions $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ generating a dihedral group $D_n \subset \mathrm{Aut}_{\mathbb{Q}}(X)$.

Throughout this section, when a curve X is claimed to have no points defined over a p-adic field $\mathbb{Q}_p$, it is tested for a corresponding equation $y^2 = f(x)$ (with f of degree 4), whether primes p exist such that the curve has no points over $\mathbb{Q}_p$. The Magma code that was used for this can be found in Appendix II. An explicit calculation by hand is presented for first example only.

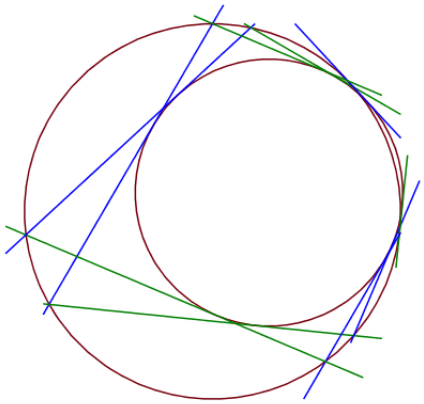
5.1 Examples with two circles: $n = 2, 3, 4, 5, 6, 8, 10, 12$

As mentioned in Corollary 9, no Poncelet figure of order 7 or 9 can exist where both of the conics $\mathcal{C}, \mathcal{D}$ are circles. For all other cases however, an example can be made with two circles. Throughout this subsection, $\mathcal{C}$ will be the unit circle $x^2 + y^2 = 1$. Examples for $n = 5, n = 10$ and $n = 12$ were already found by Boris Mirman [7]. First let us have a look at the examples he gave for $n = 5$ and $n = 10$. They consist of $\mathcal{C}$ and $\mathcal{D}$ as given.

n = 5
$\mathcal{D} : (x-3)^2 + (y-1)^2 = \frac{81}{16}$



n = 10
$\mathcal{D} : \left(x - \frac{3}{10}\right)^2 + \left(y - \frac{1}{10}\right)^2 = \frac{81}{160}$



To make life easier, the rotation with center $(0, 0)$ sending the line given by $3y = x$ to the x-axis is applied. This leads to the new equations

$$\mathcal{D} : (x - \sqrt{10})^2 + y^2 = \tfrac{81}{16}, \qquad \mathcal{D} : \left(x - \tfrac{1}{\sqrt{10}}\right)^2 + y^2 = \tfrac{81}{160}.$$

These two cases both result in the following equation for X:

$$s^2 = (t^2 + 1) \cdot (63 \cdot t^2 - 192 \cdot t + 127).$$

This curve does not have any points with coordinates in $\mathbb{Q}_2$ and therefore no rational points. Thus these examples are of the desired form. The fact that the curve X corresponding to $s^2 = (t^2+1) \cdot (63 \cdot t^2 - 192 \cdot t + 127)$ has no points with coordinates in $\mathbb{Q}_2$ is shown algebraically:

1. It has no $\mathbb{Q}_2$-rational points at ∞: Let $\eta = \frac{s}{t^2}$ and let $v = \frac{1}{t}$. The points of X at infinity are the points of $\eta^2 = 63 - 192v + 190v^2 - 192v^3 + 127v^4$ at $v = 0$. Then $\eta^2 = 63$, but 63 is not a square modulo 4, thus there are no $\mathbb{Q}_2$-rational points at ∞.

2. It has no $\mathbb{Q}_2$-rational points not at ∞: elements of $\mathbb{Q}_2$ are of the form $t = 2^a \cdot u$ with $u \in \mathbb{Z}_2^\times$.
   - $a < 0$: $(t^2+1)(63t^2 - 192t + 127) = 2^{4a} \cdot (u^2 + 2^{-2a})(63u^2 - 3u2^{6-a} + 127) = 2^{4a} \cdot U$. This $U \equiv 1 \cdot (3 + 0 + 0) \equiv 3 \mod 4$. This is not a square, so there are no solutions for this case.
   - $a > 0$: In this case, $t \in \mathbb{Z}_2$ and $t \equiv 0 \mod 2$. Then $(t^2+1)(63t^2 - 192t + 127) \equiv 1 \cdot 3 \mod 4$ which again is not a square, so there are no solutions.
   - $a = 0$: $t \in \mathbb{Z}_2^\times$, i.e. $t = u$. Then $(t^2+1)(63t^2 - 192t + 127) \equiv 12 \mod 16$, which is not a square, so this case also gives no solutions.

We will now 'explain' the relation between the two examples. Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be given as follows.

$$\mathcal{D}_1 : (x-\delta)^2 + y^2 = \rho \qquad\qquad \mathcal{D}_2 : (x - \tfrac{1}{\delta})^2 + y^2 = \tfrac{\rho}{\delta^2}$$

According to Proposition 2 of [7], given a Poncelet figure of odd order n with $\mathcal{C}$ and $\mathcal{D}_1$, the circles $\mathcal{C}$ and $\mathcal{D}_2$ make a Poncelet figure of order $2n$.

Next, examples for $n = 3$ and for $n = 6$ are made. For both, given the circle $\mathcal{D} : (x-\delta)^2 + y^2 = \rho$, a relation between δ and ρ was given in Section 3. These give the following sets.

$$n = 3 : \quad S_3 = \left\{ (\delta, \rho); \rho = \tfrac{(\delta^2-1)^2}{4} \right\}$$

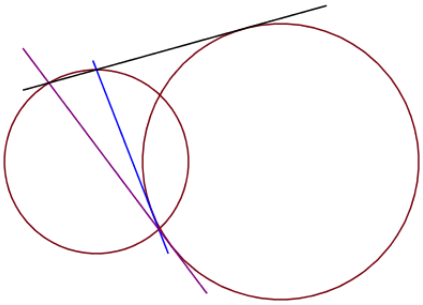
$$n = 6 : \quad S_6 = \left\{ (\delta', \rho'); \rho' = \tfrac{(\delta'^2-1)^2}{4\delta'^2} \right\}$$

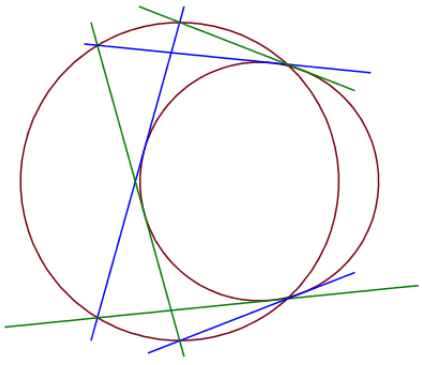
Notice that $\phi : (\delta, \rho) \mapsto (\frac{1}{\delta}, \frac{\rho}{\delta^2})$ maps elements of S_3 to elements of S_6 and $\phi' : (\delta', \rho') \mapsto (\frac{1}{\delta'}, \frac{\rho'}{\delta'^2})$ maps elements of S_6 to elements of S_3.

We take $\delta_3 = 2$ to create an example for $n = 3$. Then we make the corresponding example for $n = 6$, so with $\delta_6 = \frac{1}{\delta_3} = \frac{1}{2}$. This gives the following.

n = 3
$\mathcal{D} : (x-2)^2 + y^2 = \frac{9}{4}$

n = 6
$\mathcal{D} : \left(x - \frac{1}{2}\right)^2 + y^2 = \frac{9}{16}$





These both (for different s) result in the following equation for X.

$$s^2 = (t^2+1)\cdot\left(\frac{99}{16}\cdot t^2 - 18t + \frac{99}{16}\right)$$

This curve has no points with coordinates in $\mathbb{Q}_2$ and therefore no rational points.

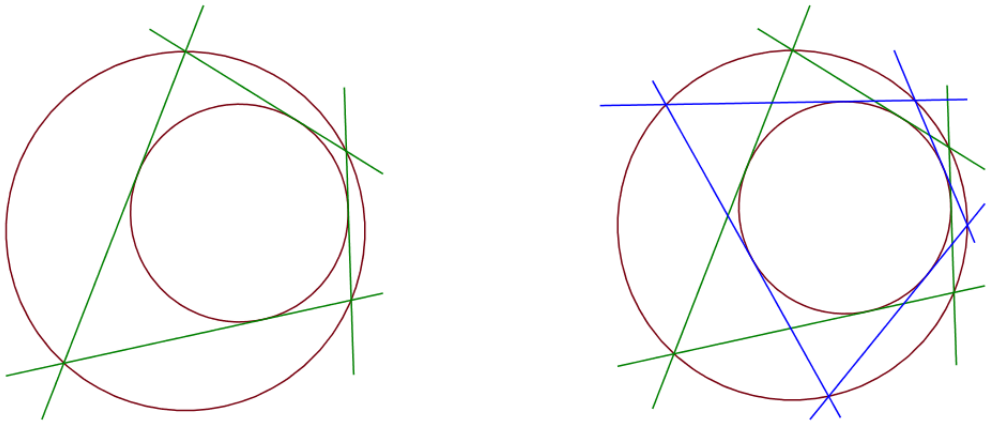
The next curves were again found using the relations found in Section 3. The relation found for $n = 4$ is the following.

$$\rho = \frac{(\delta^2-1)^2}{2(\delta^2+1)}$$

After trying a number of rational numbers for δ, it became clear that these do not give an example without rational points. Thus $\delta = \frac{1}{\sqrt{10}}$ was tried, as in the $n = 10$ case above and that gave a nice example with $\rho = \frac{81}{220}$. So $\mathcal{D} : (x-\frac{3}{10})^2 + (y-\frac{1}{10})^2 = \frac{81}{220}$, which gives as an equation for X

$$s^2 = (t^2+1)\cdot(117t^2 - 264t + 205)$$

This has no points with coordinates in $\mathbb{Q}_2$, so no rational points.



In the above case with $n = 4$, the involutions σ, τ satisfy $\rho = \sigma\tau$ has order 4. This way, $< \sigma, \rho >= D_4$. Then also $< \sigma, \rho^2 >= D_2 \subset \mathrm{Aut}_Q(X)$, which gives an example for $n = 2$.

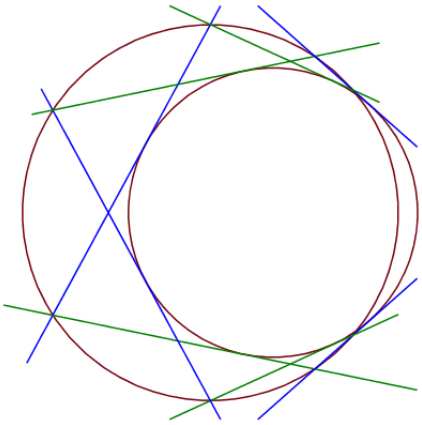
The relation for $n = 8$ is

$$\rho = \frac{(\delta^2-1)^2}{4\delta}$$

Using this relation, the circle $\mathcal{D} : (x-\frac{1}{3})^2 + y^2 = \frac{16}{27}$, so $\delta = \frac{1}{3}, \rho = \frac{16}{27}$ was created, giving an equation for X:

$$s^2 = (t^2+1)\cdot\frac{16}{27}\cdot\left(\frac{14}{27}t^2 - \frac{4}{3}t + \frac{14}{27}\right)$$

This equation has no points with coordinates in $\mathbb{Q}_2$ and no points with coordinates in $\mathbb{Q}_3$, so it certainly has no rational points.

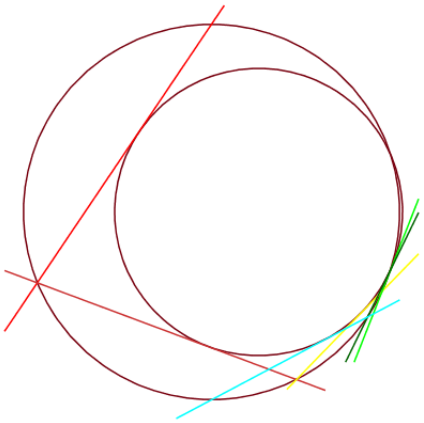


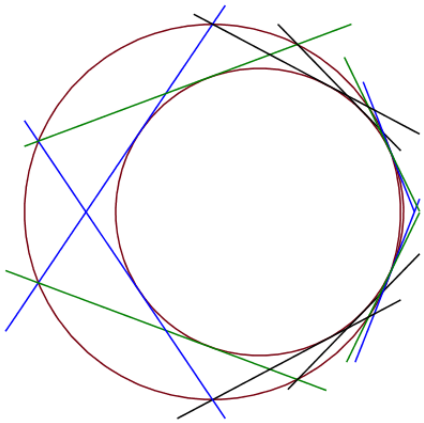
Finally, an example with two circles for $n = 12$ was also given by Mirman [7]. It consists of $\mathcal{C}$ and $\mathcal{D} : \left(x - \frac{1}{4}\right)^2 + y^2 = \frac{75}{128}$, which results in the following equation for X.

$$s^2 = (t^2 + 1) \cdot \frac{75}{128} \cdot \left(\frac{61}{128} t^2 - t + \frac{61}{128} \right)$$

This equation again has no points with coordinates in $\mathbb{Q}_2$ and no points with coordinates in $\mathbb{Q}_3$, so no rational points.

Note: as can be seen in the following pictures, when starting in the point $(0, 1)$*, after six steps one arrives exactly in the opposite point of the circle* $\mathcal{C}$*:* $(0, -1)$*. Hence after twelve steps the figure closes.*





5.2 An example for $n = 7$

An example for $n = 7$ was found using a parabola and a hyperbola. The equations we started with:

$$\mathcal{C} : y = x^2, \qquad \mathcal{D} : x^2 + axy + by^2 = \tfrac{d^2(4b-a^2)}{4}.$$

All the details of this example are given in Appendix I. A whole lot of options for the coefficients (a, b, d) were found. The first one that was tried already gave an example: $(-\frac{2}{3}, \frac{1}{13}, \frac{13}{3})$. So given are the conics

$$\begin{aligned} &\mathcal{C} : y = x^2 \\ &\mathcal{D} : x^2 - \tfrac{2}{3}xy + \tfrac{1}{13}y^2 = -\tfrac{52}{81} \end{aligned}$$

This leads to the following equation for X:

$$s^2 = 1053x^4 - 9126x^3 + 13689x^2 + 8788$$

This has no points with coordinates in $\mathbb{Q}_{13}$, so no rational points. By construction it has two involutions $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ and $\sigma\tau$ has order 7.

6 Other methods

In the previous part, two conics over $\mathbb{Q}$ were taken to create a Poncelet figure of order n. Because this method did not provide us with an example of the desired form for $n = 9$, some other methods are considered in this section.

6.1 A more general equation

In the calculations in the previous chapters, after parameterizing the conics, an equation that is of degree 2 in two different variables was arrived at. A general form of such an equation is

$$x^2y^2 + axy^2 + by^2 + 2cx^2y + 2dxy + 2ey + fx^2 + gx + h = 0 \tag{2}$$

Note that the aim of this thesis does not necessarily include finding a Poncelet figure. To find a curve $X/\mathbb{Q}$ of the desired form, one can also start from Equation (2). Similar to the previous, this is considered of the form $A(x)y^2 + 2B(x)y + C(x) = 0$. Then,

$$\tilde{y}^2 = B(x)^2 - A(x)C(x) = (cx^2 + dx + e)^2 - (x^2 + ax + b)(fx^2 + gx + h)$$

with $\tilde{y} = A(x)y + B(x)$. The constant term will then be $e^2 - bh$. This can be used to create a point on the curve. In our calculations, we fixed $e^2 - bh$ to be some non-square rational value. The coefficient of x^4 is $c^2 - f$. This should not be zero, so in calculations we also fixed this. Filling in coefficients and calculating as before, a lot of options were tried, none of which successful.

6.2 Twisting

In this section an easy way of twisting is considered. Let Y, Y' be two curves of genus one that are defined over $\mathbb{Q}$. Take $d \in \mathbb{Q}\backslash\mathbb{Q}^2$. Then Y' is a quadratic twist of Y if and only if Y, Y' are not isomorphic over $\mathbb{Q}$, but are isomorphic over $\mathbb{Q}(\sqrt{d})$.

This could be used in the search for a curve $X/\mathbb{Q}$ of genus one with $X(\mathbb{Q}) = \emptyset$ with $\mathbb{Q}(X)$ the function field of $X/\mathbb{Q}$ and $D_9 \subset \mathrm{Aut}(\mathbb{Q}(X))$.

Take an elliptic curve $E/\mathbb{Q}$ with $\mathbb{Q}(E)$ function field of $E/\mathbb{Q}$, $D_9 \subset \mathrm{Aut}(\mathbb{Q}(E))$. Let $T \in E(\mathbb{Q})$ be a point of order 9. As mentioned in the introduction, we can then take for $P \in E$

$$\begin{aligned} \sigma &: P \mapsto -P \\ \tau &: P \mapsto T - P \end{aligned}$$

as the involutions. Then $< \sigma, \tau >= D_9 \subset \mathrm{Aut}(Q(E))$.

Next, take $d \in \mathbb{Q}\backslash\mathbb{Q}^2$ and the field extension of degree 2:

$$\mathbb{Q}(E) \subset \mathbb{Q}(E, \sqrt{d})$$

Then define the extension of σ on this field as the involution

$$\begin{aligned} \tilde{\sigma} : \quad & x \mapsto x \\ & y \mapsto -y \\ & \sqrt{d} \mapsto -\sqrt{d} \end{aligned}$$

Taking the invariants, $\mathbb{Q}(E, \sqrt{d})^{\tilde{\sigma}} \subset \mathbb{Q}(E, \sqrt{d})$ is also of order 2. This $\mathbb{Q}(E, \sqrt{d})^{\tilde{\sigma}}$ is a twist of $\mathbb{Q}(E)$. Let E be given by $y^2 = f(x)$. Then $\mathbb{Q}(E, \sqrt{d})^{\tilde{\sigma}} = \mathbb{Q}(X)$ where X is defined by $\eta^2 = d \cdot f(x)$ and $\eta = y\sqrt{d}$.

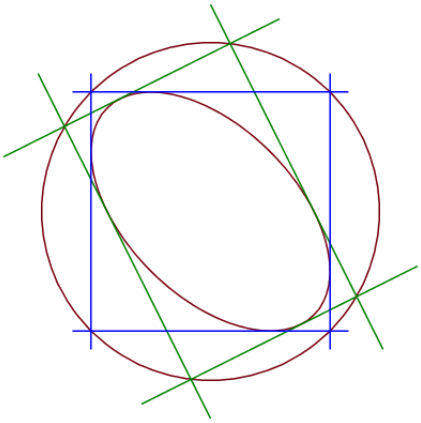
The following Poncelet figure can be made using a twist. Take $\mathcal{C}_1 : x^2 + y^2 = 1$ and $\mathcal{D}_1 : x^2 + xy + y^2 = \frac{3}{8}$. These curves make a Poncelet figure of order 4. Let $X_1/\mathbb{Q}$ be the curve corresponding to this figure. Consider the involution $\mu \in \mathrm{Aut}(\mathbb{Q}(X_1))$ that mirrors in the origin: $\mu(x, y) = (-x, -y)$. Let $d = 6$ and extend μ:

$$\begin{aligned} \tilde{\mu} : \quad & x \mapsto -x \\ & y \mapsto -y \\ & \sqrt{d} \mapsto -\sqrt{d} \end{aligned}$$

Then $\mathbb{Q}(X_1, \sqrt{d})^{\tilde{\mu}} = \mathbb{Q}(X)$ where X is defined by the two conics

$$\begin{aligned} \mathcal{C} &: \xi^2 + \nu^2 = 6 \\ \mathcal{D} &: \xi^2 + \xi\nu + \nu^2 = \tfrac{9}{4} \end{aligned}$$

where $\xi = x\sqrt{6}$ and $\nu = y\sqrt{6}$. Since $\mathcal{C}(\mathbb{Q}) = \emptyset$, and points of X can be seen as a point of $\mathcal{C}$ together with a line, none of the points of X are rational.



This example for $n = 4$ was shown in [6].

7 Conclusion

Recall the aim of this thesis was *to find for each* $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ *an example of a curve* $X/\mathbb{Q}$ *of genus one with* $X(\mathbb{Q}) = \emptyset$ *that has* $D_n \subset \mathrm{Aut}_{\mathbb{Q}}(X)$*, i.e.* $G \subset \mathrm{Aut}_{\mathbb{Q}}(X)$ *generated by two involutions* σ *and* τ *has finite order* $2n$*.*

In the text above this was approached using Poncelet figures. Poncelet figures consisting of two circles were used to create curves $X/\mathbb{Q}$ of genus one with $X(\mathbb{Q}) = \emptyset$ with two involutions σ and τ generating a subset of $\mathrm{Aut}_{\mathbb{Q}}(X)$ of finite order $2n$ for $n \in \{2, 3, 4, 5, 6, 8, 10, 12\}$. So all possible n except 7 and 9.

In fact, it was found that for $n = 7$ and $n = 9$ there cannot exist a Poncelet figure with two circles, or any two conics that have a point symmetry or line symmetry defined over $\mathbb{Q}$ in common. Using two conics without such a symmetry in common, namely a parabola and a hyperbola, an example of the desired form for $n = 7$ was created.

Some more general approaches were tried to find an example for the remaining case $n = 9$, but none of them were successful. Therefore, we conclude that for all of the possible values for n except $n = 9$, a genus one curve $X/\mathbb{Q}$ of the desired form was found.

8 Further research

Since no example of a genus one curve X defined over $\mathbb{Q}$ with $X(\mathbb{Q}) = \emptyset$ and $D_9 \subset \mathrm{Aut}_{\mathbb{Q}}(X)$ has been found, it is interesting to look for one. Possible ways in which this might work are the following.

1. Find a curve in two variables as in Section 6.1, for which the described approach works.
2. Take an elliptic curve $E/\mathbb{Q}$ with $D_9 \subset \mathrm{Aut}(\mathbb{Q}(E))$ (generated by involutions σ, τ). Taking a certain twist could perhaps create a curve $X/\mathbb{Q}$ that has no points over $\mathbb{Q}$. The corresponding involutions $\tilde{\sigma}, \tilde{\tau}$ will then generate $D_9 \in \mathrm{Aut}_{\mathbb{Q}}(X)$.

References

[1] H.J.M. Bos, C. Kers, F. Oort, and D.W. Raven, *Poncelet's closure theorem.*, Expositiones Mathematicae, 5 (1987), 289-364.

[2] W. Chapple, *An essay on the properties of triangles inscribed in and circumscribed about two given circles*, Miscellanea curiosa mathematica, 4 (1746), 117-124.

[3] N. Fuss, *De quadrilateris quibus circulum tam inscribere quam circumscribere licet*, Nova acta acad. sci. Petrop. 10 (1797), 103-125.

[4] N. Fuss, *De polygonis symmetrice irregularibus circulo simul inscriptis et circumscriptis*, Nova acta acad. sci. imp. Petrop. 13 (1802), 166-189.

[5] P.A. Griffiths, *Variations on a theorem of Abel*, Inventiones Mathematicae, 35 (1976) 321-390.

[6] J. Los, T. Mepschen, and J. Top, *Rational Poncelet*, International Journal of Number Theory (2018), to appear.

[7] B. Mirman, *Explicit solutions to Poncelet's porism*, Linear Algebra and its Applications 436 (2012) 3531-3552.

[8] J.-V. Poncelet, *Traité de Propriétés Projectives de Figures* , 1822.

[9] J.-V. Poncelet, *Applications d'analyse et de géométrie* , 1862.

[10] N. Schappacher and R. Schoof, *Beppo Levi and the Arithmetic of Elliptic Curves*, The Mathematical Intelligencer, 18:57âĂŞ68, 1996.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves* second edition, Springer, 2016.

[12] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235-265.

[13] Maple (2017). Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[14] Image elliptic curve, URL: `https://www.oktot.com/elliptic-curve-cryptography/`

Appendices

Appendix I

In this appendix the calculations for the example that is given in Section 5 for $n = 7$ will be given in full. *Goal: find a genus one curve X, with $X(\mathbb{Q}) = \emptyset$ and involutions $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(X)$ with $\sigma\tau$ of order 7.*

This will be done using a Poncelet figure. As noticed in Section 4, this cannot be done if the two conics of the Poncelet figure have an axis of symmetry in common. The computations where $\mathcal{C}$ was taken to be a circle became slightly complicated quite fast because of the parametrization of the circle. It makes sense to use a curve that has an easier parametrization. This is why the standard parabola is chosen.

$$\mathcal{C} : y = x^2$$

The second conic must then not have $x = 0$ as an axis of symmetry. The following formula is taken.

$$\mathcal{D} : x^2 + axy + by^2 = c$$

Depending on $a, b, c \in \mathbb{Q}\backslash 0$ this is an ellipse, a set of lines or a hyperbola. Doing calculations like this didn't give a point automatically like in the circles case, so we force X to have points that we can find easily by taking $y = d$ to be a tangent line to $\mathcal{D}$. That means that (x, d) must have exactly one solution.

$$\begin{aligned} x^2 + axd + bd^2 &= c \\ x^2 + adx + bd^2 - c &= 0 \end{aligned}$$

Taking the discriminant and solving for c gives

$$\begin{aligned} a^2d^2 - 4(bd^2 - c) &= 0 \\ 4c &= d^2(4b - a^2) \\ c &= \tfrac{d^2(4b-a^2)}{4} \end{aligned}$$

Thus, we take the equation

$$\mathcal{D} : x^2 + axy + by^2 = \frac{d^2(4b - a^2)}{4}$$

Next, an equation for X must be found. Let $l : y = \gamma x + \delta$ be a tangent line of $\mathcal{D}$. That is forced by filling in $\gamma x + \delta$ for y in $\mathcal{D}$ and then taking the discriminant w.r.t. x and solving it.

$$\begin{aligned} &\mathrm{discrim}(x^2 + ax(\gamma x + \delta) + b(\gamma x + \delta)^2 - \tfrac{d^2(4b-a^2)}{4}) \\ &= -(a^2 - 4b)(bd^2\gamma^2 + ad^2\gamma + d^2 - \delta^2) = 0 \end{aligned}$$

Note that $a^2 - 4b$ should not be zero. This leaves us with

$$bd^2\gamma^2 + ad^2\gamma + d^2 - \delta^2 = 0$$

Since we want $(x, y) \in \mathcal{C} \cap l$, we take $x^2 = \gamma x + \delta$ and we substitute $\delta = -\gamma x + x^2$ in the previous equation. This results in

$$-x^4 + 2\gamma x^3 - \gamma^2 x^2 + bd^2\gamma^2 + ad^2\gamma + d^2 = 0$$

This can be written in the form $A(x)\gamma^2 + 2B(x)\gamma + C(x) = 0$ with

$$\begin{aligned} A(x) &= -x^2 + bd^2 \\ B(x) &= x^3 + \tfrac{ad^2}{2} \\ C(x) &= -x^4 + d^2 \end{aligned}$$

Then, computations can be done as follows.

$$\begin{array}{lll} c_2 = A(x)\gamma & \rightarrow & c_2^2 + 2B(x)c_2 + A(x)C(x) = 0 \\ c_3 = A(x)\gamma + B(x) & \rightarrow & c_3^2 + A(x)C(x) - B(x)^2 = \\ & & c_3^2 - \frac{d^2}{4} \cdot (4bx^4 + 4ax^3 + 4x^2 + a^2d^2 - 4bd^2) = 0 \\ s = \frac{2(A(x)\gamma + B(x))}{d} & \rightarrow & s^2 = 4bx^4 + 4ax^3 + 4x^2 + a^2d^2 - 4bd^2 \end{array}$$

This last expression is a representation of the curve $X : s^2 = 4bx^4 + 4ax^3 + 4x^2 + a^2d^2 - 4bd^2$.

Next, using the tangent line $y = d$ we created, we get a point on this curve. Note that since we took a parabola, it was parametrized by x. This means that the x in the formula is the x-value of the point on $\mathcal{C}$. As we took the tangent line $y = d$, that means we can take $x_1 = \sqrt{d}$ with s_1 coming from the slope of the tangent line, which is $\gamma = 0$.

$$s_1 = \frac{2(A(\sqrt{d}) \cdot 0 + B(\sqrt{d}))}{d} = \frac{2B(\sqrt{d})}{d} = -ad - 2\sqrt{d}$$

The next point will then have $x_2 = -\sqrt{d}$. The other tangent line of $\mathcal{D}$ through $(-\sqrt{d}, d)$ has slope $\gamma = \frac{-ad+2\cdot\sqrt{d}}{bd-1}$, as found with the code in Maple.

```
solve(discrim(subs(y = g*(x+sqrt(d))+d, Kvgl), x), g);
```

Then s_2 can be calculated:

$$s_2 = \frac{2\left(A(-\sqrt{d}) \cdot \frac{-ad+2\cdot\sqrt{d}}{bd-1} + B(-\sqrt{d})\right)}{d} = ad - 2\sqrt{d}$$

So we have the two points

$$P_1 = (x_1, s_1) = \left(\sqrt{d}, -ad - 2\sqrt{d}\right), P_2 = (x_2, s_2) = \left(-\sqrt{d}, ad - 2\sqrt{d}\right)$$

Let E be the elliptic curve over $\mathbb{Q}(\sqrt{d})$ defined by $(X, P1)$ and let $\phi : X \rightarrow E$. Then let $T = \phi(P_2)$. To create a Poncelet figure of order n, $n \cdot T$ must be forced to equal $\mathcal{O}$ on E. In this case it makes sense to compute $3 \cdot T$ and $4 \cdot T$. This is what is done in the following code.

```
F<a>:=FunctionField(Rationals());
FF<b>:=FunctionField(F);
FFF<d>:=FunctionField(FF);
P<x>:=PolynomialRing(FFF);
K<r>:=ext<FFF|x^2-d>;
D:=BaseChange(HyperellipticCurve(4*b*x^4+4*a*x^3+4*x^2+a^2*d^2-4*b*d^2),K);
Pt:=D![r,-a*d-2*r];
E,f:=EllipticCurve(D,Pt);
Q:=D![-r,a*d-2*r];
Pt1:=f(Q);
(3*Pt1)[1];
(4*Pt1)[1];
```

Let $T = Pt1$. If $T \neq \mathcal{O}$ and $3T$ and $4T$ have the same x-value, then $7 \cdot T = \mathcal{O}$. Using Maple, we calculate for which (a, b, d) that is the case.

```
x3 := ((512*b^2/a^5-160*b/a^3+8/a)*d^8+(2048*b^3/a^7-1280*b^2/a^5+64*b/a^3
+32/a)*d^7/b+(-512*b^3/a^7+128*b^2/a^5+64*b/a^3-16/a)*d^6/b^2+(-6144
*b^4/a^7+3072*b^3/a^5-512*b^2/a^3+96*b/a-16*a)*d^5/b^4+(1024*b^3/a^7
+1280*b^2/a^5-928*b/a^3+136/a)*d^4/b^4+(256*b/a^5-64/a^3)*d^3
/b^4+(-512*b/a^7+128/a^5)*d^2/b^4)*r/(d^8-16*d^7/a^2+(96*b^2/a^4
-2)*d^6/b^2+(-256*b^2/a^6+32/a^2)*d^5/b^2+(256*b^4/a^8-192*b^2/a^4
+1)*d^4/b^4+(512*b^2/a^6-16/a^2)*d^3/b^4(-512*b^2/a^8+96/a^4)*d^2/b^4
-256*d/(a^6*b^4)+256/(a^8*b^4))+((-64*b^2/a^4+16*b/a^2)*d^9+(-1536
*b^3/a^6+640*b^2/a^4-32*b/a^2-8)*d^8/b+(-1024*b^2/a^8+1280*b/a^6-256
/a^4)*d^7+(2560*b^4/a^6-1152*b^3/a^4+160*b^2/a^2-24*b+4*a^2)*d^6/b^4+
(4096*b^4/a^8-3072*b^3/a^6+320*b^2/a^4+112*b/a^2-16)*d^5/b^4+(-2048*b^2
/a^6+1024*b/a^4-128/a^2)*d^4/b^4+(1024*b/a^8-256/a^6)*d^3/b^3)/(d^8
-16*d^7/a^2+ (96*b^2/a^42)*d^6/b^2(-256*b^2/a^6+32/a^2)*d^5/b^2+(256
*b^4/a^8-192*b^2/a^4+1) *d^4/b^4+(512*b^2/a^6-16/a^2)*d^3/b^4+(-512*b^2
/a^8+96/a^4)*d^2/b^4-256*d/(a^6*b^4)+256/(a^8*b^4)):
```

```
x4 := (-4*b^2*d^10/a^3+(544*b^2/a^5-160*b/a^3+8/a)*d^9+(1984*b^3/a^7
-1280*b^2/a^5+240*b/a^3-8/a)*d^8/b+(-512*b^4/a^7+768*b^3/a^5-768*b^2
/a^3+176*b/a-8*a)*d^7/b^3+(4864*b^4/a^7-4736*b^3/a^5+1640*b^2/a^3
-208*b/a+4*a)*d^6/b^4+(-1024*b^5/a^7+1472*b^4/a^5-672*b^3/a^3
+264*b^2/a-48*a*b+2*a^3)*d^5/b^6+(1664*b^4/a^7-3584*b^3/a^5
+2032*b^2/a^3-488*b/a+44*a)*d^4/b^6+(-512*b^3/a^7+768*b^2/a^5
-448*b/a^3+64/a)*d^3/b^6+(-256*b^2/a^7+384*b/a^5-68/a^3)*d^2/b^6
+32*d/(a^5*b^6)-64/(a^7*b^6))*r/(d^9-16*d^8/a^2+(96*b^3/a^4+2*b
-a^2)*d^7/b^3+(-256*b^3/a^6-32*b/a^2+16)*d^6/b^3+(256*b^6/a^8
+192*b^4/a^4-96*b^3/a^2+b^2-a^2*b+(1/4)*a^4)*d^5/b^6+(-512*b^4
/a^6+256*b^3/a^4-16*b^2/a^2+16*b-4*a^2)*d^4/b^6+(512*b^4
/a^8-256*b^3/a^6+96*b^2/a^4-96*b/a^2+24)*d^3/b^6+(-256*b^2
/a^6+256*b/a^4-64/a^2)*d^2/b^6+(256*b^2/a^8-256*b/a^6+64
/a^4)*d/b^6)+(b^2*d^11/a^2+(-68*b^2/a^4+16*b/a^2)*d^10+
(-1552*b^3/a^6+640*b^2/a^4-76*b/a^2+2)*d^9/b+(-960*b^4
/a^8+1280*b^3/a^6-336*b^2/a^4+88*b/a^2-16)*d^8/b^2+(-2880
*b^4/a^6+2784*b^3/a^4-762*b^2/a^2+68*b-a^2)*d^7/b^4+
(-2816*b^5/a^8+3712*b^4/a^6-1880*b^3/a^4+320*b^2/a^2-28*b
+4*a^2)*d^6/b^5+(-1632*b^4/a^6+2112*b^3/a^4-1068*b^2/a^2
+218*b-15*a^2)*d^5/b^6+(-640*b^4/a^8+2560*b^3/a^6-1872*b^2
/a^4+600*b/a^2-68)*d^4/b^6+(-64*b^2/a^6+96*b/a^4-15/a^2)*d^3
/b^6+(256*b^2/a^8-384*b/a^6+60/a^4)*d^2/b^6-16*d/(a^6*b^6)
+64/(a^8*b^6))/(d^9-16*d^8/a^2+(96*b^3/a^4+2*b-a^2)*d^7
/b^3+(-256*b^3/a^6-32*b/a^2+16)*d^6/b^3+(256*b^6/a^8
+192*b^4/a^4-96*b^3/a^2+b^2-a^2*b+(1/4)*a^4)*d^5/b^6+(-512*b^4
/a^6+256*b^3/a^4-16*b^2/a^2+16*b-4*a^2)*d^4/b^6+(512*b^4/a^8
-256*b^3/a^6+96*b^2/a^4-96*b/a^2+24)*d^3/b^6+(-256*b^2/a^6+256*b/a^4
-64/a^2)*d^2/b^6+(256*b^2/a^8-256*b/a^6+64/a^4)*d/b^6):
```

```
xvgl := numer(simplify(x3-x4));

xvgl := (4*(a^2*d-4*a*r+4))*(-b^12*d^12-10*a^2*b^9*d^10+46*b^10*d^10
+13*a^4*b^6*d^8-72*a^2*b^7*d^8+65*b^8*d^8-6*a^6*b^3*d^6+45*a^4*b^4*d^6
-108*a^2*b^5*d^6+a^8*d^4+116*b^6*d^6-10*a^6*b*d^4+39*a^4*b^2*d^4
-72*a^2*b^3*d^4+33*b^4*d^4-a^4*d^2+6*a^2*b*d^2-2*b^2*d^2-1)
```

The first part of this equation did not give solutions. Therefore solutions to the second, bigger part need to be found. This is done using a 'Pointsearch' in Magma.

```
A3<a,b,d>:= AffineSpace(Rationals(),3);
f:= -b^12*d^12-10*a^2*b^9*d^10+46*b^10*d^10+13*a^4*b^6*d^8-72*a^2*b^7*d^8
+65*b^8*d^8-6*a^6*b^3*d^6+45*a^4*b^4*d^6-108*a^2*b^5*d^6+a^8*d^4+116*b^6*d^6
-10*a^6*b*d^4+39*a^4*b^2*d^4-72*a^2*b^3*d^4+33*b^4*d^4-a^4*d^2+6*a^2*b*d^2
-2*b^2*d^2-1 ;
V:=Scheme(A3,f);
PointSearch(V,1000)

(-2/3 : 1/13 : 13/3 : 1), (46/25 : -23/25 : -5/23 : 1),
(-46/25 : -23/25 : `5/23 : 1), (2/5 : -1/23 : -23/5 : 1),
(4/5 : -4/23 : 23/20 : 1), (-26/3 : 13 : -1/39 : 1),
(46/25 : -23/25 : 5/23 : 1), (4/3 : 4/13 : -13/12 : 1),
(-2/5 : -1/23 : 23/5 : 1), (-26/9 : 13/9 : 3/13 : 1),
(13/6 : 13/16 : -16/39 : 1), (2/3 : 1/13 : 13/3 : 1),
(13/3 : 13/4 : -4/39 : 1), (2 : 9/13 : 13/27 : 1),
(-4/5 : -4/23 : -23/20 : 1), (-46/25 : -23/25 : -5/23 : 1),
(-13/6 : 13/16 : -16/39 : 1), (13/9 : 13/36 : 12/13 : 1),
(-13/3 : 13/4 : 4/39 : 1), (-4/5 : -4/23 : 23/20 : 1),
(26/9 : 13/9 : 3/13 : 1), (-13/9 : 13/36 : 12/13 : 1),
(-2/3 : 1/13 : -13/3 : 1), (-2 : 9/13 : -13/27 : 1),
(-4/3 : 4/13 : 13/12 : 1), (-2/5 : -1/23 : -23/5 : 1),
(-13/6 : 13/16 : 16/39 : 1), (-26/3 : 13 : 1/39 : 1),
(4/5 : -4/23 : -23/20 : 1), (2/5 : -1/23 : 23/5 : 1),
(13/6 : 13/16 : 16/39 : 1), (2 : 9/13 : -13/27 : 1),
(13/9 : 13/36 : -12/13 : 1), (26/3 : 13 : -1/39 : 1),
(2/3 : 1/13 : -13/3 : 1), (-13/9 : 13/36 : -12/13 : 1),
(-13/3 : 13/4 : -4/39 : 1), (26/9 : 13/9 : -3/13 : 1),
(4/3 : 4/13 : 13/12 : 1), (-4/3 : 4/13 : -13/12 : 1),
(-2 : 9/13 : 13/27 : 1), (13/3 :\ 13/4 : 4/39 : 1),
(-26/9 : 13/9 : -3/13 : 1), (26/3 : 13 : 1/39 : 1)
```

These results are of the form $(a : b : d : 1)$. The first one $(-2/3 : 1/13 : 13/3 : 1)$ already gives an example X: $y^2 = 1053x^4 - 9126x^3 + 13689x^2 + 8788$. Note that it indeed satisfies $a^2 - 4b \neq 0$. Using Magma, it can be shown that this X has no points with coordinates in $\mathbb{Q}$. It does have points with coordinated in $\mathbb{Q}_p$ for all primes p except $p = 13$. For the primes up to $p = 13$, this was found using Magma as below. For all other primes p, this can be shown as follows.

The equation $y^2 = 1053x^4 - 9126x^3 + 13689x^2 + 8788$ describes a genus one curve X in all

characteristics that do not divide its discriminant. So we get a smooth curve over $\mathbb{F}_p$ for all primes $p \neq 2, 3, 13$. Then, it follows from the Hasse-Weil inequality that

$$\begin{aligned} |\#X(\mathbb{F}_p) - (p+1)| &\leq 2\sqrt{p} \\ -2\sqrt{p} < \#X(\mathbb{F}_p) - (p+1) &< 2\sqrt{p} \\ 0 < (\sqrt{p}-1)^2 < \#X(\mathbb{F}_p) &< (\sqrt{p}+1)^2 \end{aligned}$$

Therefore, $\#X(\mathbb{F}_p) > 0$ and since X is smooth in characteristic p, the Hensel lift can be used to find a point in $\mathbb{Q}_p$.

```
Q:=Rationals();
P<x>:=PolynomialRing(Q);
C:=GenusOneModel(HyperellipticCurve(1053*x^4 - 9126*x^3 + 13689*x^2 + 8788));
IsLocallySoluble(C);
IsLocallySoluble(C,2);
IsLocallySoluble(C,3);
IsLocallySoluble(C,5);
IsLocallySoluble(C,7);
IsLocallySoluble(C,11);
IsLocallySoluble(C,13);

false
true (97145*2^2 + O(2^21) : 1 + O(2^21) : -69509*2 + O(2^21))
true (12265523756*3^-2 + O(3^20) : 1 + O(3^23) : -503728424*3^-2 + O(3^20))
true (-26210518217449 + O(5^20) : 1 + O(5^20) : 2 + O(5^20))
true (4 + O(7^20) : 1 + O(7^20) : 9099286549721223 + O(7^20))
true (-298553994353347754240 + O(11^20) : 1 + O(11^20) : 4 + O(11^20))
false
```

Appendix II

In this appendix all of the used code will be given. It is in a general form, so it can be applied to multiple examples.

The Maple code used for finding an expression for X is in every case a little bit different, but the general idea is the same. Here the code for the circles case is given.

```
Kvgl := (x-delta)^2+y^2-rho;
simplify((1/4)*discrim(subs(y = c*x+d, Kvgl), x));
subs(b = (-t^2+1)/(t^2+1), subs(a = 2*t/(t^2+1), subs(d = -a*c+b, %)));
VGL := -numer(factor(%));
A := coeff(VGL, c, 2); B := coeff(VGL, c, 1)/2; C := coeff(VGL, c, 0);
VGLn := A*C+B*c2+c2^2;
VGLnn := simplify(c3^2+C*A-(1/4)*B^2);
CC := coeff(VGLnn, c3, 0);
factor(CC);
CCn := simplify(CC/(t^2+1)^2); VGLd := s^2+CCn;
```

Here $f(t) = -CCn$ gives the correct $s^2 = f(x)$ describing X. The next step is finding two points of X. This also depends on the conics, but in all cases, they are found using the involutions that you canonically get from the Poncelet situation. Here the code for the case of two circles is given. In that case the first point $(i, 0)$ is already known. So $t_1 = i$ and $s_1 = 0$. In other cases, s_1 can be found using the formula for s of that case.

```
a2 := -a-2*c*d/(c^2+1);
b2 := a2*c+d;
t2 := simplify((1-b2)/a2);
t2 := subs(d = -a*c+b, t2);
t2 := simplify(subs(b = (-t^2+1)/(t^2+1),subs(a = 2*t/(t^2+1), t2)));
An := subs(t = t2, A);
B2n := subs(t = t2, (1/2)*B);
s2 := simplify((An*c+B2n)/(t2^2+1));
```

As these $t2, s2$ depend on c, they still need to be updated with the new value of c.

```
T := simplify(subs(c = ((alpha-delta)*(t^2+1)*s-(1/2)*B)/A, t2));
S := simplify(subs(c = ((alpha-delta)*(t^2+1)*s-(1/2)*B)/A, s2));
T2 := simplify(subs(s = 0,subs(t = I, T)));
S2 := simplify(subs(s = 0, subs(t = I, S)));
```

Our second point is then $(t_2, s_2) = (T2, S2)$.

Given are an expression for X of the form $s^2 = f(t)$, and two points on this curve pt and $pt2$. Using the following code in Magma, one can find n times a point on the elliptic curve E defined using X and pt. In this particular case it depends on (a, b, c, d):

```
F<a>:=FunctionField(Rationals());
FF<b>:=FunctionField(F);
FFF<c>:=FunctionField(FF);
FFFF<d>:=FunctionField(FFF);
P<x>:=PolynomialRing(FFFF);
K<r>:=ext<FFFF|x^2-d>;
```

```
D:=BaseChange(HyperellipticCurve(f(x)),K);
Pt:=D![pt];
E,f:=EllipticCurve(D,Pt);
Q:=D![pt2];
Pt1:=f(Q);
n*Pt1;
```

Then there are three options to make $Pt1$ have order n;

1. The point $n \cdot Pt1$ is calculated and the next step is to show that this is $\mathcal{O}$, hence to solve the denominator of its x- or y-value is solved.
2. The point $m \cdot Pt1$ is calculated with $2m = n$. Its y-value is calculated and solved.
3. The points $n_1 \cdot Pt1$ and $n_2 \cdot Pt1$ with $n_1 + n_2 = n$ and $n_1 \cdot Pt1 \neq n_2 \cdot Pt1$, are calculated and the difference of their x-coordinates is solved.

This results in an expression in the coefficients of the corresponding conics. Now assume these are (a, b, d). Given such an expression $g(a, b, d) = 0$, the following code in Magma will (very probably) find solutions in (a, b, d) if they exist.

```
A3<a,b,d>:= AffineSpace(Rationals(),3);
f:= g(a,b,d);
V:=Scheme(A3,f);
PointSearch(V,1000);
```

Finally, given $s^2 = f(x)$ with a solution (a, b, d) filled in, it can be checked whether this curve has any points over $\mathbb{Q}$ or $\mathbb{Q}_p$ using the following code in Magma.

```
Q:=Rationals();
P<x>:=PolynomialRing(Q);
C:=GenusOneModel(HyperellipticCurve(f(x)));
IsLocallySoluble(C);
IsLocallySoluble(C,p)
```

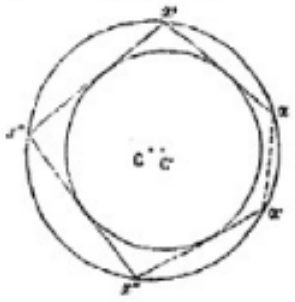
If this gives no solutions in $\mathbb{Q}$, an example is found.

Appendix III

This is a page from Poncelet's book 'Applications d'analyse et de géométrie' [9]. In this page he describes a Poncelet figure.

Soient (C) et (C'), (*fig.* 146) les deux circonférences dont il s'agit; concevons un polygone quelconque $\alpha x' x'' \ldots \alpha'$ inscrit dans le cercle (C) et dont tous les côtés $\alpha x'$, $x' x''$, etc., soient tangents au cercle (C'), à l'exception d'un dernier côté

Fig. 146.



$\alpha\alpha'$, qui évidemment ne saurait, en général, devenir tangent à ce dernier cercle que pour des positions particulières du polygone dont il fait partie. Supposons qu'on déforme ce polygone de la manière indiquée au n° *II*, il est évident qu'il pourra prendre toutes les positions imaginables autour du cercle (C'), et que, s'il est possible d'inscrire à la circonférence (C) un certain polygone d'un égal nombre de côtés, qui soit en même temps circonscrit à l'autre (C'), il y aura nécessairement une position du polygone ci-dessus $\alpha x' \ldots \alpha'$, telle que le côté $\alpha x'$ soit tangent au cercle (C); or je dis que c'est impossible si, pour cette position ou une position quelconque du polygone, la corde $\alpha\alpha'$ n'est pas tangente à ce cercle.