A. Dwarshuis et al. *Res. Number Theory* (2021) 7:7
https://doi.org/10.1007/s40993-020-00231-z

Research in Number Theory

RESEARCH

Mazur's rational torsion result for pointless genus one curves: examples

Arjan Dwarshuis, Majken Roelfszema and Jaap Top

*Correspondence:
j.top@rug.nl
Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

Abstract

This note reformulates Mazur's result on the possible orders of rational torsion points on elliptic curves over $\mathbb{Q}$ in a way that makes sense for arbitrary genus one curves, regardless whether or not the curve contains a rational point. The main result is that explicit examples are provided of 'pointless' genus one curves over $\mathbb{Q}$ corresponding to the torsion orders 7, 8, 9, 10, 12 (and hence, all possibilities) occurring in Mazur's theorem. In fact three distinct methods are proposed for constructing such examples, each involving different in our opinion quite nice ideas from the arithmetic of elliptic curves or from algebraic geometry.

Keywords: Curve of genus one, Automorphism, Rational point, Torsion

Mathematics Subject Classification: 14H45, 14G15, 14H25

1 Introduction

A famous theorem [10, Thm. (7')] by B. Mazur, confirming a conjecture by A.P. Ogg [12, p. 110] and [13, Conjecture 1], asserts that if E is an elliptic curve defined over the rational numbers $\mathbb{Q}$ then any point $P \in E(\mathbb{Q})$ of finite order has the property that $\mathrm{ord}(P)$ divides one of $\{7, 8, 9, 10, 12\}$. Moreover all positive divisors occur as order of rational points, for infinitely many pairwise non-isomorphic curves E.

We now reformulate Mazur's result in terms of the group $\mathrm{Isom}_{\mathbb{Q}}(E)$ of invertible morphisms $E \to E$ defined over $\mathbb{Q}$ of an elliptic curve $E/\mathbb{Q}$, as follows. Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E(\mathbb{Q})$. The translation τ_P over P is an element of $\mathrm{Isom}_{\mathbb{Q}}(E)$ and $\mathrm{ord}(\tau_P) = \mathrm{ord}(P)$. If $d := \mathrm{ord}(P) < \infty$ then the pair τ_P and $-\mathrm{id} \in \mathrm{Isom}_{\mathbb{Q}}(E)$ generate a dihedral group $D_d \subset \mathrm{Isom}_{\mathbb{Q}}(E)$ of order $2d$. Hence for every positive divisor d of one of $\{7, 8, 9, 10, 12\}$, examples of elliptic curves $E/\mathbb{Q}$ exist such that $\mathrm{Isom}_{\mathbb{Q}}(E)$ contains a dihedral group D_d of order $2d$.

Using Mazur's result, the converse also holds: let $D_d \subset \mathrm{Isom}_{\mathbb{Q}}(E)$ be a dihedral group of order $2d$. Take $\varphi \in D_d$ of order d. Write $\varphi = \tau_P \circ \alpha$ for some $P \in E$ and some $\alpha \in \mathrm{Aut}(E) = \mathrm{Isom}(E, O)$; i.e., α is an invertible morphism fixing the neutral element $O \in E(\mathbb{Q})$. Then $P = \varphi(O) \in E(\mathbb{Q})$ and hence $\alpha = \tau_P^{-1} \circ \varphi$ is defined over $\mathbb{Q}$. This implies $\alpha = \pm\mathrm{id}$. In case $\alpha = -\mathrm{id}$ one checks $d = \mathrm{ord}(\varphi) = 2$ which divides several of the integers $\{7, 8, 9, 10, 12\}$. In the remaining case one has $\tau_P = \varphi$, hence $d = \mathrm{ord}(\varphi) = \mathrm{ord}(\tau_P) = \mathrm{ord}(P)$ divides (at least) one of $\{7, 8, 9, 10, 12\}$ by Mazur's theorem.

The reformulation inspired the following seemingly more general assertion.

Theorem 1.1 *If X is a curve of genus one defined over $\mathbb{Q}$, then any automorphism of finite order defined over $\mathbb{Q}$ of X has order dividing one of* $\{7, 8, 9, 10, 12\}$. *In particular, if $D_d \subset Isom_{\mathbb{Q}}(X)$ then d divides one of these integers.*

A slightly weaker statement (formulated in the language of function fields) is given in [8, Corollary 1.3]. In the special case of Theorem 1.1 that the curve X contains a rational point P (so, (X, P) is an elliptic curve), a proof is given in the paragraph preceding the statement of the theorem. The general case also includes situations where no rational point is present. Concerning this, we prove the next result.

Theorem 1.2 *For every $d \in \{7, 8, 9, 10, 12\}$ there exists a genus one curve $X/\mathbb{Q}$ with $X(\mathbb{Q}) = \emptyset$ such that $Isom_{\mathbb{Q}}(X)$ contains a dihedral group of order $2d$.*

In fact, the following curves admit such isomorphisms:

$$\begin{aligned}
d = 7: &\quad y^2 = 1053x^4 - 9126x^3 + 13689x^2 + 8788.\\
d = 8: &\quad y^2 = -(x^2+1)(49x^2 + 64x + 49).\\
d = 9: &\quad y^2 = -9x^4 + 24x^3 + 150x^2 + 120x + 31.\\
d = 10: &\quad y^2 = (x^2+1)(63x^2 - 192x + 127).\\
d = 12: &\quad y^2 = 3(x^2+1)(61x^2 - 128x + 61).
\end{aligned}$$

A (simple and short) proof of Theorem 1.1 is presented in Sect. 2. Here also three approaches towards obtaining examples as the ones shown in Theorem 1.2 are discussed and compared. Section 3 illustrates the first two of these methods. Section 4 provides details on the remaining method, and in particular shows how the examples presented in Theorem 1.2 are constructed.

2 Proof of Thm. 1.1 and discussion of constructions

Proof (of Theorem 1.1.) We use the notations introduced in the statement of the assertion. Put $E := \mathrm{Jac}(X)$, the Jacobian variety of the curve X. This is an elliptic curve defined over $\mathbb{Q}$. Any automorphism of X induces one on E. If $\varphi \in \mathrm{Isom}_{\mathbb{Q}}(X)$ has finite order d, then the corresponding $\varphi^* \in \mathrm{Isom}_{\mathbb{Q}}(E)$ has order d as well. Hence the argument preceding the statement of Theorem 1.1 (note that this uses Mazur's result for the elliptic curve E) completes the proof. □

We now discuss how to obtain examples of genus one curves $X/\mathbb{Q}$ without rational points, and with a dihedral group $D_d \subset \mathrm{Isom}_{\mathbb{Q}}(X)$ for given d. In terms of generators and relations D_d is generated by elements ρ, σ satisfying $\mathrm{ord}(\rho) = d$, $\mathrm{ord}(\sigma) = 2$, and $\sigma\rho\sigma = \rho^{-1}$. Given such $\rho, \sigma \in D_d$ and an integer m coprime to d, put $\tau := \sigma\rho^m$. Then D_d is also generated by the pair σ, τ, and $\sigma\tau$ has order d whereas both of σ, τ have order 2. In any group G containing two elements s, t of order 2 with product $r = st$ of order d, the subgroup generated by s and t is isomorphic to D_d as follows by observing $srs = ts = r^{-1}$.

So to find curves $X/\mathbb{Q}$ with $\mathrm{Isom}_{\mathbb{Q}}(X)$ containing a dihedral group of order $2d$, one either assures that X admits automorphisms ρ, σ of order d and 2, respectively, with $\sigma\rho\sigma = \rho^{-1}$, or one assures that X admits involutions σ, τ defined over $\mathbb{Q}$ such that their composition $\sigma\tau$ has order d. The subsections below discuss three approaches.

2.1 Examples via descent

A well known situation in which genus one curves without rational points occur, is in the theory of descent on elliptic curves. A standard reference for this is [14, Ch. X §3,4]. Given an elliptic curve E over $\mathbb{Q}$, any nontrivial element in the Shafarevich-Tate group $Ш(E/\mathbb{Q})$ is represented by a homogeneous space X for $E/\mathbb{Q}$. This is a genus one curve $X/\mathbb{Q}$ equipped with a simple transitive (right) action $\mu\colon X \times E \to X$ defined over $\mathbb{Q}$, of E on X. The notion and some properties of it already appear in a 1962 paper by J.W.S. Cassels [2, p. 97]. If furthermore $E(\mathbb{Q})$ contains a point P of order d, then $\rho := \mu(-, P)\colon X \to X$ is an element of $\mathrm{Isom}_{\mathbb{Q}}(X)$ of order d.

Moreover, nontrivial in Ш means $X(\mathbb{Q}) = \emptyset$ (although X has points over every completion of $\mathbb{Q}$). To obtain a dihedral group of automorphisms, one demands that the element in the Shafarevich-Tate group under consideration has order 2. Indeed, this implies that X is a so-called (unramified) 2-covering of E (compare, for example, [4, Section 4]). In particular it is well known how to find an explicit equation of the form $y^2 = f(x)$ for X, with $f(x)$ a quartic polynomial. The involution corresponding to $(x, y) \mapsto (x, -y)$ acts as -1 on regular 1-forms on X, hence corresponds to an automorphism given as $Q \mapsto T - Q$ on E. Together with the translation of order d on E, this generates a group D_d on E and hence on X as well.

A nice exposition of this theory, including a detailed more abstract explanation why a curve X defining an everywhere locally solvable 2-covering indeed admits an involution as described here (or equivalently, admits a map of degree 2 to $\mathbb{P}^1$), is presented in the master's thesis [5]. In particular his Proposition 1.5.2, which relies on an argument by Cassels [2, Lemma 7.1], is relevant here.

Using Magma one obtains explicit equations for the homogeneous spaces in question, as will be illustrated in Sect. 3. Obviously, a necessary condition for this to work is that one has an elliptic curve $E/\mathbb{Q}$ admitting a rational point of order d as well as a nontrivial element in $Ш(E/\mathbb{Q})[2]$. It is by no means evident how to find this. The LMFDB [7], containing over 3, 000, 000 elliptic curves, does not have a single entry where these conditions are met for $d = 9$, nor for $d = 12$. A search with Magma done by Steffen Müller using families of elliptic curves with a rational point of order 9 resp. 12, provided several examples with nontrivial $Ш(E/\mathbb{Q})[2]$ for these two cases.

Given a curve $X/\mathbb{Q}$ obtained in this way, one can by e.g. finding an isomorphism $X \cong E$ over an extension field and carefully tracing the steps in the proof of [14, Thm. X.3.6] in principle construct the action $X \times E \to X$ and thereby explicitly the elements in $D_d \subset \mathrm{Isom}_{\mathbb{Q}}(X)$.

2.2 Examples by twisting

Note that the strategy proposed in Sect. 2.1 gives more than what was asked: not only will the example have $X(\mathbb{Q}) = \emptyset$, it will also have points everywhere locally.

Relaxing the latter condition turns out to make it much simpler to obtain examples. Namely, again by starting from an elliptic curve $E/\mathbb{Q}$, and then constructing a suitable $X/\mathbb{Q}$ such that X is isomorphic to E over some quadratic extension $K \supset \mathbb{Q}$. This should be done such that

(a.) A translation over a point of order d on E and some involution $Q \mapsto T - Q$ on E both induce automorphisms on X that are defined over $\mathbb{Q}$;

(b.) The curve X should have no rational points.

These properties will now be analyzed.

Let $E/\mathbb{Q}$ be an elliptic curve and $T \in E(\mathbb{Q})$. Fix the involution $\iota \in \mathrm{Isom}_{\mathbb{Q}}(E)$ given by $\iota\colon P \mapsto T - P$. Write $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for the Galois group of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $K \subset \overline{\mathbb{Q}}$ be a quadratic extension of $\mathbb{Q}$. The composition

$$\xi\colon G_{\mathbb{Q}} \xrightarrow{\text{res}} \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{Isom}(E)$$

where the second arrow sends the nontrivial automorphism (from now on denoted α) to ι, defines an element in $H^1(G_{\mathbb{Q}}, \mathrm{Isom}(E))$ and hence a twist X of E (see, e.g., [14, Ch. X §2, §5]).

Explicitly, the function field $\mathbb{Q}(X)$ equals the field of invariants under the involution $\alpha \otimes \iota^{\#}$ on $K \otimes_{\mathbb{Q}} \mathbb{Q}(E) = K(E)$ where α generates $\mathrm{Gal}(K/\mathbb{Q})$ and $\iota^{\#}$ denotes the action of ι on the function field of E. Then $K(X) = K(E)$. An isomorphism $\psi : E \cong X$ exists (over K) such that for every $\gamma \in G_{\mathbb{Q}}$ one has

$$\psi^{\gamma} = \begin{cases} \psi & \text{if } \gamma \text{ acts trivially on } K, \\ \psi\iota & \text{otherwise.} \end{cases}$$

Using this one deduces the following.

Lemma 2.2.1 $X(\mathbb{Q}) = \{\psi(R) \mid R \in E(K) \text{ satisfies } \alpha(R) = T - R\}$.

Proof Take $P \in X(\overline{\mathbb{Q}})$ and $R = \psi^{-1}(P) \in E(\overline{\mathbb{Q}})$. For $\gamma \in G_{\mathbb{Q}}$ acting trivially on K we have $\psi^{\gamma} = \psi$ and therefore $\gamma(P) = P \Leftrightarrow \gamma(R) = R$. And in case $\gamma \in G_{\mathbb{Q}}$ does not restrict to the identity on K (which means that γ restricts to α) the condition $\psi^{\gamma} = \psi\iota$ implies the equivalence $\gamma(P) = P \Leftrightarrow \gamma(R) = T - R$. Hence P being fixed by all $\gamma \in G_{\mathbb{Q}}$ is equivalent to R being K-rational and moreover $\alpha(R) = T - R$. □

Lemma 2.2.2 *The involution $\psi\iota\psi^{-1}$ on X is defined over $\mathbb{Q}$.*

Proof Considering the two possibilities for the restriction of a $\gamma \in G_{\mathbb{Q}}$ to K, it follows that $(\psi\iota\psi^{-1})^{\gamma} = \psi^{\gamma}\iota(\psi^{-1})^{\gamma} = \psi\iota\psi^{-1}$ for all γ. □

Lemma 2.2.3 *For $P \in E(\overline{\mathbb{Q}})$ and $\tau := \psi\tau_P\psi^{-1} \in Isom(X)$ one has*

$$\tau \text{ is defined over } \mathbb{Q} \Longleftrightarrow P \in E(K) \text{ and } \iota(P) = -P.$$

Proof Having $\tau \in \mathrm{Isom}_{\mathbb{Q}}(X)$ means $\tau^{\gamma} = \tau$ for all $\gamma \in G_{\mathbb{Q}}$. For γ restricting to the identity on K, this says $\psi\tau_P\psi^{-1} = \psi\tau_{\gamma(P)}\psi^{-1}$, so $P = \gamma(P)$. This means $P \in E(K)$. For γ restricting to α on K, the condition $\tau^{\gamma} = \tau$ is equivalent to $\sigma\tau_{\gamma(P)}\sigma = \tau_P$ and therefore to $\gamma(P) = -P$. □

The lemmas suggest how to construct an example as desired. Namely, start from $E/\mathbb{Q}$ containing a rational point of order d. Then take a quadratic twist denoted E_D (in the notation from [14, Ch. X §5], this represents an element in $\mathrm{Twist}((E, O)/\mathbb{Q})$) of E, containing a rational point T not in $E_D(\mathbb{Q})[2]$. With $K = \mathbb{Q}(\sqrt{D})$, the point of order d results in a point P of order d in $E_D(K)$ satisfying $\alpha(P) = -P$. Using $\iota = \tau_T \circ [-\mathrm{id}]$, the maps τ_T and ι generate a group $D_d \subset \mathrm{Isom}(E_D)$. Using the twist as described here results by the lemmas in $X/\mathbb{Q}$ and $D_d \subset \mathrm{Isom}_{\mathbb{Q}}(X)$. By Lemma 2.2.1 one has $X(\mathbb{Q}) = \emptyset$ provided $T \in E_D(\mathbb{Q})$ cannot be written as $R + \alpha(R)$ for any $R \in E_D(K)$. In concrete examples it

turns out to be not hard to satisfy this condition (even locally over some completion of $\mathbb{Q}$: for example if $D < 0$ and $E(\mathbb{R})$ has two real connected components, then any $T \in E_D(\mathbb{R})$ not in the identity component of $E_D(\mathbb{R})$ cannot be written as $R + \alpha(R)$ with $R \in E_D(\mathbb{C})$ and $\alpha =$ complex conjugation).

An example of this twisting method is presented in Sect. 3. Note that in this approach it is straightforward to give an explicit equation for the curve X and for the automorphisms constructed on it. Finding for given d an appropriate curve E and nonsquare D turns out to be quite easy.

2.3 Examples starting from involutions

The final method for obtaining examples is in fact the one used to obtain the examples presented in Theorem 1.2. Also here, both the curves and generators of the group D_d are completely explicit. The curves X we wish to construct can be described as the ones satisfying four conditions:

(1) X admits two involutions;
(2) the genus of X is 1;
(3) the product of the two involutions has finite order d;
(4) there are no rational points on X.

We briefly discuss each or these.
(1) Take (everything over $\mathbb{Q}$) a curve $X \subset C \times D$ for curves C, D in such a way that the projection maps $C \times D \to C$ and $C \times D \to D$ restrict to morphisms $X \to C$ and $X \to D$ of degree 2. The induced extensions of function fields $\mathbb{Q}(X) \supset \mathbb{Q}(C)$ and $\mathbb{Q}(X) \supset \mathbb{Q}(D)$ are quadratic, therefore each give rise to an involution on $\mathbb{Q}(X)$, and these correspond to involutions σ, τ defined over $\mathbb{Q}$ of the curve X.
(2) Suppose that the curves C, D mentioned in (1.) have genus 0, i.e., C and D are isomorphic over $\mathbb{Q}$ to a conic in $\mathbb{P}^2$, equivalently: isomorphic to $\mathbb{P}^1$ over a suitable (quadratic) extension of $\mathbb{Q}$. If $X \subset C \times D$ is regular and satisfies the condition mentioned in (1.) then the genus of X equals 1. This follows by either applying the adjunction formula to X regarded as a smooth bidegree (2, 2) curve in $\mathbb{P}^1 \times \mathbb{P}^1$ or by applying the Hurwitz formula to the degree 2 map $X \to C$ (which has 4 ramification points since X is regular).
(3) By construction, the involutions on the genus one curve X constructed as sketched in (1.), (2.) have the property that the quotient of X by any of these involutions is birational to either C or D, so in particular this quotient has genus 0. This implies that the (linear) action of the involutions on the 1-dimensional $\mathbb{Q}$-vector space of regular differentials on X is multiplication by -1. Choosing over a suitable extension field $K \supset \mathbb{Q}$ a rational point $P \in X(K)$ provides X with a group law defined over K. In terms of this, the involutions σ, τ are given by $Q \mapsto \sigma(Q) = P_\sigma - Q$ resp. $Q \mapsto \tau(Q) = P_\tau - Q$ for certain $P_\sigma, P_\tau \in X(K)$.

As a consequence the composition $\sigma\tau$ is translation over the point $P_\sigma - P_\tau = \sigma(\tau(P))$. So this composition has order d precisely when the point $\sigma(\tau(P))$ has order d in the group $X(K)$ with unit element P. This observation together with Theorem 1.1 explains and improves a result by V.A. Malyshev [9, Introduction]; we will see how with a small additional argument it also implies a result by B. Mirman [11, Cor. 3.5].

A naive strategy for finding examples with a given order d is therefore to start from a family $X_{a,b}$ or $X_{a,b,c}$ of curves as above, say parametrized by a Zariski-open subset of $\mathbb{A}^2$

or of $\mathbb{A}^3$. Moreover each $X_{a,b}$ is supposed to contain a point $P_{a,b}$ defined over a quadratic extension $K(a,b)$ of $\mathbb{Q}(a,b)$. The condition that $\sigma(\tau(P_{a,b}))$ has order dividing d in the group $X_{a,b}$ with unit element $P_{a,b}$ defines a closed condition in our parameter space. In our situations, a search for rational points satisfying this condition turns out to provide the desired examples.

Actually certain special geometric conditions on the conics C, D and the curve X contained in their product prevent the existence of order 7 and of order 9 automorphisms defined over $\mathbb{Q}$ on X. This will be discussed in Proposition 4.4.

(4.) A final condition is that we need to ensure that the curve X contains no rational points. Since by construction our examples admit nonconstant morphisms defined over $\mathbb{Q}$ to conics C, D a sufficient condition would be that either $C(\mathbb{Q}) = \emptyset$ or $D(\mathbb{Q}) = \emptyset$. In some of our examples it turns out that neither of these hold. This implies that X is over $\mathbb{Q}$ a double cover of $\mathbb{P}^1$. Hence it can be given by an equation $y^2 = f(x)$ with $f \in \mathbb{Q}[x]$ of degree 4. For a curve defined by such an equation it is straightforward to test whether it has any points defined over the p-adic numbers $\mathbb{Q}_p$, for a fixed prime p. We will show that $X(\mathbb{Q})$ is empty by presenting a prime p such that $X(\mathbb{Q}_p) = \emptyset$.

Section 4 presents details and explicit examples of this method.

3 Examples from Shafarevich–Tate groups and twists

We now illustrate §2.1 and §2.2 with an explicit example for each of these methods.

For the construction based on an everywhere locally solvable 2-covering, take $d = 10$. The LMFDB tables [7] contain precisely one elliptic curve $E/\mathbb{Q}$ with a rational point of order 10 and Ш$(E/\mathbb{Q})[2]$ nontrivial, namely

$$E: \quad y^2 + xy = x^3 - 1239337803x - 14349289224303$$

with Cremona label `219450e4`. The Magma code The Magma code

```
E:=EllipticCurve("219450e4");
TwoDescent(E)[1];
```

results in the example

$$X: \quad y^2 = 21520x^4 - 42952x^3 + 151129x^2 - 44436x + 164088.$$

As remarked earlier, this works in the same way for every $d \leq 8$, whereas for $d = 9$ and for $d = 12$ the LMFDB tables do not contain any elliptic curve with the desired properties. However, a search using Magma (performed by Steffen Müller) resulted, among others, in the following examples.

d = 9 : The elliptic curve

$$E: \quad y^2 + xy + y = x^3 - x^2 - 60183695642x + 5682868725861209$$

of conductor 19890090 contains the point $(19617, -67164809)$ of order 9 and has nontrivial Ш$(E/\mathbb{Q})[2]$. One of its 2-coverings without rational points but with rational points everywhere locally is given by

$$y^2 = 297225x^4 - 758970x^3 - 122979x^2 + 776116x + 310244.$$

d = 12 : The elliptic curve

$$E: \quad y^2 + xy = x^3 - 134552862320916160817 85x - 5194973697347125800426588960489 03$$

contains the point $(-83202493836, 4902473824946313)$ or order 12. The curve has conductor 5067056501430 (and rank 0) while Ш$(E/\mathbb{Q})[2]$ is nontrivial. The Magma code

```
TwoDescent(E : RemoveTorsion)[1];
```

results in

$$X\colon \quad y^2 = -9580166559x^4 + 90169866210x^3 + 307902943333x^2 \\ -1150290234460x - 2086645758524,$$

with $X(\mathbb{Q}) = \emptyset$ but with rational points over all completions, and with $D_{12} \subset \mathrm{Isom}_{\mathbb{Q}}(X)$.

For the construction based on twists we take $d = 9$. The elliptic curve

$$E/\mathbb{Q}\colon \quad y^2 + xy + y = x^3 - x^2 - 14x + 29$$

with Cremona label `54b3` has a rational point $\widetilde{Q} := (9, 19)$ of order 9 (in fact, it is the curve of smallest conductor having such a point). Taking $x = 0$ results in points on E defined over $K := \mathbb{Q}(\sqrt{13})$, so we take the quadratic twist $E_{13}/\mathbb{Q}$ of E over K. An equation for it is

$$E_{13}/\mathbb{Q}\colon \quad y^2 + xy = x^3 - x^2 - 2313x + 57357.$$

We have $T = (-3, 255) \in E_{13}(\mathbb{Q})$ corresponding to one of the points with $x = 0$ on E. Furthermore the point Q yields a point $P \in E_{13}(K)$ of order 9, with the property $\alpha(P) = -P$ for α the nontrivial automorphism of K.

Take $\iota = \tau_T \circ [-\mathrm{id}] \in \mathrm{Isom}_{\mathbb{Q}}(E)$. The curve $X/\mathbb{Q}$ we look for is the one with function field $\mathbb{Q}(X) = K(E)^{\langle \tilde{\iota} \rangle}$ with $\tilde{\iota}$ the involution $\alpha \otimes \iota^{\#}$ on $K \otimes_{\mathbb{Q}} \mathbb{Q}(E)$. Note that

$$\mathbb{Q}(E)^{\langle \iota^{\#} \rangle} \subset K(E)^{\langle \tilde{\iota} \rangle} \subset K(E)$$

in which the successive extensions have degree 2. It is easy to obtain a generator of the leftmost field, e.g., using [8, Lemma 2.1]. Using a basis (such as $\{1, x, \sqrt{13}, x\sqrt{13}\}$) of the rightmost field as vector space over the leftmost one and the description of the linear map $\tilde{\iota}$ in terms of this basis, a straightforward calculation results in an equation

$$X\colon \quad y^2 = -13x^4 - 1014x^2 + 210912x - 1917981.$$

In this example $X(\mathbb{Q}_2) = \emptyset$ and also $X(\mathbb{Q}_{13}) = \emptyset$. So X has no rational points and $D_9 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$.

A similar approach works for all relevant d.

4 Examples in products of conics

A well-known classical appearance of genus one curves X embedded in a product $C \times D$ of conics, is in the context of Poncelet's closure theorem, see, e.g., [1] for its statement, an exposition, and many references. We briefly recall the construction. Given smooth conics C, C_2 intersecting (over an algebraic closure) in 4 distinct points, let $D = C_2^*$ be the dual conic of C_2. In affine coordinates, this means that a point (ξ, η) is on D precisely when the line defined by $y = \xi x + \eta$ is tangent to C_2. It is a classical and simple fact that if C_2 is a smooth conic, then so is $D = C_2^*$. As an example, if C_2 is given by an affine equation $(x - a)^2 + (y - b)^2 = c$ (a 'circle' provided $c \neq 0$) then C_2^* has equation $(a\xi + \eta - b)^2 - c\xi^2 = c$.

The curve $X \subset C \times D$ occurring in modern proofs of Poncelet's theorem is denoted by $E(C, C_2)$ in [1, § 7]; it describes the pairs (P, ℓ) with $P \in C, \ell \in C_2^* = D$ (so ℓ can be regarded as a line tangent to C_2) such that moreover $P \in \ell$. In affine coordinates as described above, the latter condition means $y = \xi x + \eta$. The two involutions σ, τ have the description $\sigma(P, \ell) = (P, \ell')$ and $\tau(P, \ell) = (P', \ell)$; here, for a given $P \in C$ and ℓ tangent to C_2 with $P \in \ell$, the intersection $C \cap \ell$ equals $\{P, P'\}$, and in the dual projective plane $(\mathbb{P}^2)^*$ the line m corresponding to all lines in $\mathbb{P}^2$ passing through P, satisfies $m \cap C_2^* = \{\ell, \ell'\}$.

Historically, in particular the case where one takes two (real) circles as conics C, C_2 was considered. After scaling and a translation, this means one assumes C is given by $x^2 + y^2 = 1$. After a rotation around the origin one moreover assumes that the center of circle C_2 is on the x-axis. In this way C_2 has equation $(x - \delta)^2 + y^2 = \rho$ for certain parameters δ, ρ. Various papers, interpreted in modern terms, determine conditions on δ, ρ under which the composition $\sigma\tau$ of the two involutions has a given finite order d. This is exactly what we are looking for, and in fact by recalling some of these results, examples for the cases with $d \in \{8, 10, 12\}$ in Theorem 1.2 will be given. After that, the remaining situations $d = 7$ and $d = 9$ are treated.

Even cases: $d = 8$ and $d = 10$ and $d = 12$. The situation sketched above will now be discussed in more detail. Starting from parameters δ, ρ let C, C_2 be the conics defined by

$$C : x^2 + y^2 = 1 \quad \text{and} \quad C_2 : (x - \delta)^2 + y^2 = \rho.$$

The dual conic $D = C_2^*$ has equation $(\delta\xi + \eta)^2 - \rho\xi^2 = \rho$ and affine equations for $X \subset C \times D$ are

$$X : \begin{cases} x^2 + y^2 = 1, \\ y = \xi x + \eta, \\ (\delta\xi + \eta)^2 - \rho\xi^2 = \rho. \end{cases}$$

In these coordinates, the involutions σ, τ are given by

$$\sigma : (x, y, \xi, \eta) \mapsto \left(x, y, \xi' = -\xi - \frac{2y(\delta - x)}{(\delta - x)^2 - \rho}, y - \xi' x\right)$$

and

$$\tau : (x, y, \xi, \eta) \mapsto \left(x' = -x - \frac{2\xi\eta}{\xi^2 + 1}, y' = \xi x' + \eta, \xi, \eta\right).$$

The degree two morphism $\pi : X \to C$ given by $(x, y, \xi, \eta) \mapsto (x, y)$ helps one to obtain an easy plane model for X, as follows. Use the standard parametrization $x = 2t/(t^2 + 1), y = (t^2 - 1)/(t^2 + 1)$ for C, with inverse $t = x/(1 - y)$. Since $\eta = y - \xi x = (t^2 - 1 - 2t\xi)/(t^2 + 1)$, one obtains in the coordinates ξ, t that X is given by the equation

$$\left(\delta\xi + \frac{t^2 - 1 - 2t\xi}{t^2 + 1}\right)^2 - \rho\xi^2 = \rho.$$

Multiplying by $(t^2 + 1)^2$ results in an equation $A\xi^2 + B\xi + C = 0$ for polynomials $A, B, C \in \mathbb{Q}[\delta, \rho][t]$. Completing the square, which in this case means one replaces ξ by $u := 2A\xi + B$ (so $\xi = (u - B)/(2A)$), the high school equation $u^2 = B^2 - 4AC$ is obtained. In the present case it turns out that $B^2 - 4AC$ has a factor $(t^2 + 1)^3$. In terms of t and a variable $v := u/(2t^2 + 2)$; equivalently, $u = 2v(t^2 + 1)$, one arrives at the equation

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

describing the curve X. In these coordinates the involution σ is given by

$$\sigma : (t, v) \mapsto (t, -v).$$

One expresses τ more conveniently in terms of the coordinates ξ, t, providing

$$\tau : (\xi, t) \mapsto \left(\xi, \frac{t - \xi}{t\xi + 1}\right).$$

Via the formulas $v = (2A\xi + B)/(2t^2 + 2)$ and $\xi = \frac{(2t^2+2)v - B}{2A}$ it is straightforward to rewrite this in terms of v, t, but we will not need the resulting (complicated) expressions.

As a 'sanity check', observe that (in characteristic $\neq 2$) the quartic equation in t, v defines a genus 1 curve precisely when each of $\delta \neq 0$, $\rho \neq 0$, and $\rho \neq (\delta \pm 1)^2$ hold. The same conditions describe the cases where C, C_2 are smooth conics intersecting in 4 distinct points.

To obtain a group structure on the curve X, let i in a suitable extension field of $\mathbb{Q}(\delta, \rho)$ be a square root of -1 and put $K := \mathbb{Q}(\delta, \rho, i)$. Then $v = 0, t = i$ defines a smooth point O on X; it can also be described by $t = \xi = i$. We now compute $\sigma(\tau(O))$ using the interpretation of points on X as pairs (P, ℓ) consisting of a point $P \in C$ and a line $\ell \ni P$ tangent to C_2. Note that O: $v = 0$, $t = \xi = i$ corresponds to $P = (1 : i : 0) \in C$ and ℓ: $y = i(x - \delta)$. Then $\sigma(\tau(P, \ell)) = (P', \ell')$ with $\{P', P\} = C \cap \ell$ (so, $P' = \left(\frac{\delta^2+1}{2\delta}, i\frac{1-\delta^2}{2\delta}\right)$), and ℓ' is the tangent line to C_2 different from ℓ that contains P'. A small calculation shows ℓ': $y = \frac{ix(\delta^4+4\rho\delta^2-2\delta^2+1)-i\delta(\delta^4-2\delta^2+4\rho+1)}{\delta^4-4\rho\delta^2-2\delta^2+1}$. The pair (P', ℓ') is also described by $t = \frac{\delta+i}{i\delta+1}$ and $\xi = i(\delta^4 + 4\rho\delta^2 - 2\delta^2 + 1)/(\delta^4 - 4\rho\delta^2 - 2\delta^2 + 1)$, so $v = 4\delta\rho(\delta - i)^2$.

Some classical results in elementary geometry can be reformulated, in modern terms, as describing conditions on the pair (δ, ρ) such that $\sigma(\tau(O))$ has a given finite order in the elliptic curve (X, O) (and hence the composition $\sigma \circ \tau$ has that same order). There are standard routines implemented in, e.g., Magma for determining a Weierstrass model starting from a pair such as (X, O) and evaluating associated division polynomials in the coordinates of the point corresponding to $\sigma\tau(O)$). In this way the next results are easily verified and therefore we will not present further details.

Lemma 4.1 *(W. Chapple [3], 1746) If δ, ρ are such that the curve X has genus* 1 *and moreover $\rho = (\delta^2 - 1)^2/4$, then ord$(\sigma \circ \tau) = 3$.* □

Lemma 4.2 *(N. Fuss [6], 1802) If δ, ρ are such that the curve X has genus* 1 *and moreover $\rho = (\delta^2 - 1)^2/(4\delta)$, then ord$(\sigma \circ \tau) = 8$.* □

Using Lemma 4.2, the case $d = 8$ in Theorem 1.2 is shown as follows. Take $\delta = -2$ and $\rho = (\delta^2 - 1)^2/(4\delta) = -9/8$. The corresponding curve X has genus 1 and Lemma 4.2 implies that the automorphism $\sigma \circ \tau$ of X, which is defined over $\mathbb{Q}$, has order 8. Moreover, X is given by the equation

$$v^2 = -\frac{9}{8}\left(t^2 + 1\right)\left(\frac{49}{8}t^2 + 8t + \frac{49}{8}\right).$$

This is readily transformed into the form presented in Theorem 1.2. Since $X(\mathbb{R})$ and even $C_2(\mathbb{R})$ (equivalently(!), $C_2^*(\mathbb{R})$) are clearly empty, the same holds for $X(\mathbb{Q})$.

Lemma 4.3 *If δ, ρ are such that the curve X has genus* 1 *and moreover*

$$64\delta^4\rho^3 - 16(2\delta^6 - 3\delta^4 + 1)\rho^2 + 12(\delta^2 - 1)^4\rho - (\delta^2 - 1)^6 = 0,$$

then ord$(\sigma \circ \tau) = 5$. □

We now use two ideas that will allow us to obtain the $d = 10$ example in Theorem 1.2. The first one is a simple geometric observation: the preceding lemmas describes a situation of two circles with their center on the x-axis. Applying any affine transformation of the plane induces isomorphisms from the conics C, C_2 to other conics C', C_2' and from the initial curve X to a curve $X' \subset C' \times C_2'$. We exploit this as follows.

The pair $(\delta, \rho) = (\sqrt{10}, 81/16)$ satisfies the conditions in Lemma 4.3. Applying a suitable rotation around the origin, this implies that the conics

$$C\colon x^2 + y^2 = 1,$$
$$C_2\colon (x-3)^2 + (y-1)^2 = 81/16$$

result in a curve X for which the involutions $\sigma, \tau \in \mathrm{Isom}_{\mathbb{Q}}(X)$ satisfy $\mathrm{ord}(\sigma \circ \tau) = 5$. Now we explain the second idea. Reflection in the line through the two centers $(0, 0)$ and $(3, 1)$ of C, C_2 is defined over $\mathbb{Q}$; it induces a common symmetry of the two conics and another involution $\iota \in \mathrm{Isom}_{\mathbb{Q}}(X)$. Considering the action of σ, τ, ι on pairs (P, ℓ) one deduces that ι commutes with both σ and τ. This implies that $\sigma\tau\iota$ has order 10. Note that it is the product of the involutions σ and $\tau\iota$. Also, note that the requirement that C, C_2 intersect in 4 distinct points implies that ι has no fixpoints. Hence for the group law on X defined by the choice of a point $O \in X$ it follows that ι is translation over a point (of order two) in (X, O).

To complete the example, a model of X as a double cover of $\mathbb{P}^1$ is computed as before by parametrizing C. This results in an equation

$$v^2 = (t^2 + 1)(63t^2 - 192t + 127).$$

Since $X(\mathbb{Q}) \subset X(\mathbb{Q}_2) = \emptyset$, this finishes the construction and proof of the $d = 10$ case in Theorem 1.2.

Slightly generalizing the given example, one obtains the following.

Proposition 4.4 *Let C and C_2 be smooth conics defined over $\mathbb{Q}$ with $\#(C \cap C_2) = 4$, such that either they have a common center or they have a common axis of symmetry defined over $\mathbb{Q}$.*

If the involutions σ, τ on the curve $X \subset C \times C_2^*$ as given in this paper satisfy $\mathrm{ord}(\sigma\tau) = n$ is odd, then the group $\mathrm{Isom}_{\mathbb{Q}}(X)$ contains an element of order $2n$.

Proof This is shown analogously to the preceding example: reflection in the common center resp. axis defines an involution $\iota \in \mathrm{Isom}_{\mathbb{Q}}(X)$. Since ι commutes with σ and τ and $n = \mathrm{ord}(\sigma\tau)$ is odd, the product $\sigma\tau\iota$ has order $2n$. □

Remark Proposition 4.4 for the special case of two circles in some sense 'explains' a result of B. Mirman [11, Thm. 3.4]. His paper also contains the example for $d = 10$ discussed above, see loc. sit. Example 3.6. However, he did not discuss the (non-)existence of pairs (P, ℓ) defined over $\mathbb{Q}$.

To conclude the 'even cases', the case $d = 12$ is now discussed. It is not hard to formulate a lemma for this situation analogous to Lemmas 4.1–4.3; we will not do this. It turns out that $(\delta, \rho) = (1/4, 75/128)$ yields an example here. It is easy to transform the given equation into the form $y^2 = 3(x^2 + 1)(61x^2 - 128x + 61)$. One checks $X(\mathbb{Q}_2) = \emptyset$, finishing the example.

Odd cases: $d = 7$ and $d = 9$. Note that using two 'circles' over $\mathbb{Q}$, it is impossible to obtain via the method described above an example with $d > 5$ odd:

Corollary 4.5 *Let C and C_2 be smooth conics defined over $\mathbb{Q}$ with $\#(C \cap C_2) = 4$, such that either they have a common center or they have a common axis of symmetry defined over $\mathbb{Q}$.*

If the involutions σ, τ on the curve $X \subset C \times C_2^*$ as given in this paper satisfy $\mathrm{ord}(\sigma\tau) = n$ is odd, then $n \leq 5$.

Proof This follows by combining Proposition 4.4 and Theorem 1.1. □

Remark Note that this corollary is reminiscent to [11, Cor. 3.5], although the latter only discusses the case of two circles.

To obtain an example with $d = 7$, we fix the conic (parabola)

$$C\colon y = x^2$$

and consider as second conic one from the family

$$C_2\colon x^2 + 2\alpha xy + \beta y^2 = \delta^2(\beta - \alpha^2).$$

This choice assures that $P := (\sqrt{\delta}, \delta) \in C$ and the line $\ell\colon y = \delta$ is tangent to C_2 and $P \in \ell$. With the parametrization $x \mapsto (x, x^2)$ for C one obtains, analogous to the cases above, the model

$$v^2 = \beta x^4 + 2\alpha x^3 + x^2 + \delta^2(\alpha^2 - \beta)$$

for the corresponding curve X. Moreover the pair (P, ℓ) corresponds to the point $x = \sqrt{\delta}, v = -\alpha\delta - \sqrt{\delta}$ on this model.

A Magma calculation including a search for rational values reveals, among many other solutions, that $(\alpha, \beta, \delta) = (-1/3, 1/13, 13/3)$ defines a case where the automorphism $\sigma\tau \in \mathrm{Isom}_{\mathbb{Q}}(X)$ has order 7. The equation is easily transformed into

$$y^2 = 13 \cdot \left(27x^2(3x^2 - 26x + 39) + 26^2\right).$$

Here $X(\mathbb{Q}_{13}) = \emptyset$, and this is precisely the $d = 7$ case presented in Theorem 1.2. Incidently, $\mathbb{Q}_{13}$ is the *only* completion of $\mathbb{Q}$ over which the curve has no rational points.

The remaining situation is $d = 9$. Here, we obtain examples by starting from the conics (in projective coordinates)

$$C\colon x^2 + y^2 = \delta z^2,$$
$$C_2\colon yz = (x - \alpha z)^2 + \beta z^2.$$

The pair $P = (1 : i : 0)$ and $\ell\colon z = 0$ satisfy $P \in C$ and $P \in \ell$ and ℓ is tangent to C_2. Affine equations for the curve X are

$$\begin{cases} x^2 + y^2 = \delta, \\ y = 2\xi x + \eta, \\ \eta = \beta - \xi^2 - 2\alpha\xi. \end{cases}$$

Now eliminate η, y and replace x by $v := (4\xi^2 + 1)x - 2\xi(\xi^2 + 2\alpha\xi - \beta)$. This results in the equation

$$v^2 = -\xi^4 - 4\alpha\xi^3 - (4\alpha^2 - 2\beta - 4\delta)\xi^2 + 4\alpha\beta\xi + \delta - \beta^2.$$

The pair (P, ℓ) yields a point O defined over $\mathbb{Q}(i)(\alpha, \beta, \delta)$ (in fact, one of the points at infinity) on this model. The involution τ is, as before, given by

$$\tau\colon (\xi, v) \mapsto (\xi, -v).$$

The other involution is more conveniently described in terms of the earlier coordinates; it reads

$$\sigma\colon (x, y, \xi, \eta) \mapsto \left(x, y, x - \alpha - \xi, y - 2x^2 + 2\alpha x + 2x\xi\right).$$

Using Magma and the group law on (X, O) one obtains explicit (complicated) conditions on α, β, δ which ensure that $\sigma(\tau(O))$ has order 9 in (X, O). These conditions hold, e.g., for $(\alpha, \beta, \delta) = (-1/3, -5/4, 16/9)$. After some trivial rewriting, the associated curve X is given by

$$y^2 = -9x^4 + 24x^3 + 150x^2 + 120x + 31$$

which is the equation presented in the $d = 9$ case of Theorem 1.2. Note that $X(\mathbb{Q}_2) = \emptyset$, finishing the proof of 1.2.

5 Conclusion

The three methods proposed here for constructing genus one curves $X/\mathbb{Q}$ with $D_d \subset \mathrm{Isom}_{\mathbb{Q}}(X)$ and moreover $X(\mathbb{Q}) = \emptyset$ use rather different and in our opinion beautiful and interesting techniques, and all three work quite well. For the method using element of order 2 in a Shafarevich-Tate group, it is in general not immediate how to obtain examples of the elliptic curves needed to make the method work. The resulting curves satisfy the stronger property of containing rational points over every completion. The twisting technique appears to be the simplest one for constructing examples. For the method of finding examples in a product of two conics, very classical results or variations on those produce examples, although for the cases $d = 7$ and $d = 9$ only after a search in 3-parameter family these were found.

For all approaches and especially for those using twists and using products of conics, explicit generators of the dihedral group involved are easy to describe.

Authors' contributions

It is a pleasure to thank Nils Bruin for helpful remarks and Steffen Müller for suggestions on our use of Magma for various details, and providing examples of some 2-coverings. Incomplete versions of our results were presented by the second author during the Antalya Cebir Günleri XX in Nesin Village, Turkey and by the third author during a BIRS workshop on Rational and Integral Points in the Casa Matemática Oaxaca, Mexico. The first and second author contributed to this research as part of their master's thesis project supervised by the third author.

Received: 9 October 2020 Accepted: 10 December 2020 Published online: 6 January 2021

References

1. Bos, H.J.M., Kers, C., Oort, F., Raven, D.W.: Poncelet's closure theorem. Expos. Math. **5**, 289–364 (1987)
2. Cassels, J.W.S.: Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. Journal für die reine und angewandte Mathematik **211**, 95–112 (1962)
3. Chapple, W.: An essay on the properties of triangles inscribed in and circumscribed about two given circles. Misc. Curiosa Math. **4**, 117–124 (1746)
4. Cremona, J.E.: Classical invariants and 2-descent on elliptic curves. J. Symbolic Comput. **31**, 71–87 (2001)
5. de Jesus Campos Rodriguez, A.: Parametrizing the 2-Selmer group and the 3-Selmer group of an elliptic curve, Master's Thesis, Leiden (2016)
6. Fuss, N.: De polygonis symmetrice irregularibus circulo simul inscriptis et circumscriptis. Nova Acta Acad Sci. Imp. Petrop. **13**, 166–189 (1802)
7. LMFDB Collaboration, the *L*-functions and Modular Forms Database, https://www.lmfdb.org, 22 April 2020 (2020)
8. Los, J., Mepschen, T., Top, J.: Rational Poncelet. Int. J. Number Theory **14**, 2641–2655 (2018)
9. Malyshev, V.A.: Poncelet problem for rational conics. St. Petersb. Math. J. **19**(4), 597–601 (2008)
10. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math., 47, 33–186, With an appendix by Mazur and M. Rapoport (1977)
11. Mirman, B.: Explicit solutions to Poncelet's porism. Linear Algebra Its Appl. **436**, 3531–3552 (2012)
12. Ogg, A.P.: Rational points on certain elliptic modular curves. In: Analytic Number Theory. Proceeding of the Symposium Pure Math 1972, vol. XXIV, pp. 221–231. St. Louis Univ, St. Louis, MO (1973)
13. Ogg, A.P.: Diophantine equations and modular forms. Bull. Am. Math. Soc. **81**, 14–27 (1975)
14. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematic. Springer, Berlin (2009)

Publisher's Note