SIMULTANEOUS TORSION IN THE LEGENDRE FAMILY

MICHAEL STOLL

Abstract. We improve a result due to Masser and Zannier, who showed that the set

$$\{\lambda \in \mathbb{C} \setminus \{0,1\} : (2, \sqrt{2(2-\lambda)}), (3, \sqrt{6(3-\lambda)}) \in (E_\lambda)_{\mathrm{tors}}\}$$

is finite, where $E_\lambda\colon y^2 = x(x-1)(x-\lambda)$ is the Legendre family of elliptic curves. More generally, denote by $T(\alpha,\beta)$, for $\alpha,\beta \in \mathbb{C}\setminus\{0,1\}$, $\alpha \neq \beta$, the set of $\lambda \in \mathbb{C}\setminus\{0,1\}$ such that all points with x-coordinate α or β are torsion on E_λ. By further results of Masser and Zannier, all these sets are finite. We present a fairly elementary argument showing that the set $T(2,3)$ in question is actually empty. More generally, we obtain an explicit description of the set of parameters λ such that the points with x-coordinate α and β are simultaneously torsion, in the case that α and β are algebraic numbers that not 2-adically close.

We also improve another result due to Masser and Zannier dealing with the case that $\mathbb{Q}(\alpha,\beta)$ has transcendence degree 1. In this case we show that $\#T(\alpha,\beta) \le 1$ and that we can decide whether the set is empty or not, if we know the irreducible polynomial relating α and β. This leads to a more precise description of $T(\alpha,\beta)$ also in the case when both α and β are algebraic. We performed extensive computations that support several conjectures, for example that there should be only finitely many pairs (α,β) such that $\#T(\alpha,\beta) \ge 3$.

1. Introduction

Let

$$E_\lambda\colon y^2 = x(x-1)(x-\lambda)$$

be the Legendre family of elliptic curves over $\mathbb{C}$. For $\alpha \in \mathbb{C}\setminus\{0,1\}$ let $P_\alpha(\lambda)$ be a point on E_λ with x-coordinate α and set

$$T(\alpha) = \{\lambda \in \mathbb{C}\setminus\{0,1\} : P_\alpha(\lambda) \in (E_\lambda)_{\mathrm{tors}}\}\,.$$

Write $T(\alpha,\beta) = T(\alpha) \cap T(\beta)$. In [MZ08, MZ10], Masser and Zannier show that $T(2,3)$ is finite. This was the first step in a series of successively more general finiteness results on the set of parameters such that a given section in a family of two-dimensional (semi-)abelian varieties is torsion, see [MZ12, MZ14, MZ] (or see the book [Zan12] for an overview). An alternative, 'dynamical' proof of the results of [MZ10, MZ12] is given by de Marco, Wang and Ye in a recent paper [dMWY14].

In this note, we give a 2-adic proof that $T(2,3)$ is actually empty. The proof is rather elementary and shows more generally that (for example) 2 and 3 can be replaced by any pair consisting of an even and an odd integer (different from 0 and 1). We also give examples of numbers α and β such that $T(\alpha,\beta)$ has exactly one or two elements. We then give a partial result along the same lines for the two-parameter Weierstrass family $y^2 = x^3 + Ax + B$.

Date: October 4, 2015.

Returning to the Legendre family, we consider the sets $T(\alpha,\beta)$ when α and β generate a field of transcendence degree 1 over $\mathbb{Q}$ (the case of transcendence degree 2 is trivial; we have $T(\alpha,\beta)=\emptyset$ in this case). In [MZ13], Masser and Zannier show that, if we are given an irreducible polynomial F over $\mathbb{Q}$ such that $F(\alpha,\beta)=0$, we can effectively compute the set $T(\alpha,\beta)$, and they give a bound on its size: $\#T(\alpha,\beta)\leq 6\cdot(12\deg F)^{32}$. We improve this result considerably; in fact, we prove the best possible bound $\#T(\alpha,\beta)\leq 1$ and also provide better upper bounds for the occurring torsion orders, leading to a more efficient determination of the set. We also obtain a fairly precise description of $T(\alpha,\beta)$ in general. See Proposition 20. This more precise description is then used as the basis for extensive computations studying pairs (α,β) such that $\#T(\alpha,\beta)\geq 2$. These computations exhibited only a small number of such pairs where the set $T(\alpha,\beta)$ has three or more elements, and so we conjecture that the set of such pairs is actually finite (Conjecture 23). Based on our computations, we also conjecture that the heights of α and β are uniformly bounded when $\#T(\alpha,\beta)\geq 2$ (Conjecture 27).

This note is organized as follows. We first prove a general statement on the 2-adic behavior of elements in a ring defined by a certain kind of recurrence relation. We then apply this to the division polynomials of the Legendre elliptic curve. This allows us to deduce 'mod 2' information on the set $T(\alpha)$, for $\alpha\in\bar{\mathbb{Q}}$, leading to our first main result that $T(\alpha,\beta)\subseteq\{\alpha,\beta\}$ if α and β are distinct 'mod 2' (see Corollary 4) or even 'mod 4' (Corollary 8 for rational α, β). We use this to show that the intersection of $T(\alpha)$ with the set of all roots of unity can be determined effectively; the set has size at most 3, and we determine all α that reach this bound. We also apply our approach to the Weierstrass family $y^2=x^3+Ax+B$. This leads to a partial result for the set of parameters (A,B) such that three x-coordinates are simultaneously torsion. The restriction is that we need to assume that B is integral at 2. See Corollary 15. We then turn to the case of transcendence degree 1 in the Legendre family and prove our second main result. The description of $T(\alpha,\beta)$ obtained as a consequence of this result is then used as the basis for the computations mentioned above. We report on the results and state the conjectures already mentioned.

Acknowledgments. I would like to thank the organizers of the *Second ERC Research Period on Diophantine Geometry* for inviting me to attend this event; the first result presented here was obtained during the meeting. I would also like to thank David Masser and Umberto Zannier for fruitful discussions. The computations we report on in Sections 6 and 7 were performed with the computer algebra system Magma [BCP97].

2. 2-adic behavior of division polynomials

Let R be a commutative ring and fix elements $f,g\in R$. Let $(h_n)_{n\geq 1}$ be a sequence of elements of R satisfying

$$h_1=1,\quad h_2=1,\quad h_3\equiv -g^2 \bmod 4R \quad\text{and}\quad h_4\equiv 2g^3 \bmod 4R$$

and the recurrence relations (for $m \geq 3, 1, 2$, respectively)

$$\begin{aligned} h_{2m} &= h_m\big(h_{m+2}h_{m-1}^2 - h_{m-2}h_{m+1}^2\big) \\ h_{4m+1} &= 4f h_{2m+2}h_{2m}^3 - h_{2m-1}h_{2m+1}^3 \\ h_{4m-1} &= h_{2m+1}h_{2m-1}^3 - 4f h_{2m-2}h_{2m}^3 \,. \end{aligned}$$

(Relations of this form are satisfied by the division polynomials of an elliptic curve; we will apply the results of this section soon in this setting.)

We define, for $n \in \mathbb{Z}_{>0}$,

$$d(n) = \left\lfloor \frac{n^2-1}{4} \right\rfloor$$

and

$$e(n) = \max\{0, v_2(n) - 1\}\,,$$

where v_2 denotes the 2-adic valuation.

Proposition 1. *For $n \in \mathbb{Z}_{>0}$, we have*

$$h_n \equiv 2^{e(n)} g^{d(n)} \bmod 2^{e(n)+1} R\,.$$

Proof. We first determine $h_n \bmod 4R$: We have

$$\begin{aligned} h_{2m+1} &\equiv (-1)^m g^{d(2m+1)} \bmod 4R \\ h_{4m+2} &\equiv (-1)^m g^{d(4m+2)} \bmod 4R \\ h_{8m+4} &\equiv 2g^{d(8m+4)} \bmod 4R \\ h_{8m} &\equiv 0 \bmod 4R \end{aligned}$$

The statements are correct by assumption for h_n with $n \le 4$. We proceed by induction using the recurrence relations. All congruences below are mod $4R$.

$$\begin{aligned}
h_{4m+1} &\equiv -h_{2m-1}h_{2m+1}^3 \\
&\equiv -(-1)^{m-1}(-1)^{3m}g^{d(2m-1)+3d(2m+1)} = (-1)^{2m}g^{d(4m+1)} \\
h_{4m-1} &\equiv h_{2m+1}h_{2m-1}^3 \\
&\equiv (-1)^{m}(-1)^{3(m-1)}g^{d(2m+1)+3d(2m-1)} = (-1)^{2m-1}g^{d(4m-1)} \\
h_{8m+2} &= h_{4m+1}(h_{4m+3}h_{4m}^2 - h_{4m-1}h_{4m+2}^2) \\
&\equiv (-1)^{2m}(-(-1)^{2m-1})g^{d(4m+1)+d(4m-1)+2d(4m+2)} = (-1)^{2m}g^{d(8m+2)} \\
h_{8m-2} &= h_{4m-1}(h_{4m+1}h_{4m-2}^2 - h_{4m-3}h_{4m}^2) \\
&\equiv (-1)^{2m-1}(-1)^{2m}g^{d(4m-1)+d(4m+1)+2d(4m-2)} = (-1)^{2m-1}g^{d(8m-2)} \\
h_{16m+4} &= h_{8m+2}(h_{8m+4}h_{8m+1}^2 - h_{8m}h_{8m+3}^2) \\
&\equiv 2g^{d(8m+2)+d(8m+4)+2d(8m+1)} = 2g^{d(16m+4)} \\
h_{16m-4} &= h_{8m-2}(h_{8m}h_{8m-3}^2 - h_{8m-4}h_{8m-1}^2) \\
&\equiv 2g^{d(8m-2)+d(8m-4)+2d(8m-1)} = 2g^{d(16m-4)} \\
h_{16m+8} &= h_{8m+4}(h_{8m+6}h_{8m+3}^2 - h_{8m+2}h_{8m+5}^2) \\
&\equiv 2\big(g^{d(8m+4)+d(8m+6)+2d(8m+3)} - g^{d(8m+4)+d(8m+2)+2d(8m+5)}\big) \equiv 0 \\
h_{16m} &= h_{8m}(h_{8m+2}h_{8m-1}^2 - h_{8m-2}h_{8m+1}^2) \equiv 0
\end{aligned}$$

The relations $d(2m-1) + 3d(2m+1) = d(4m+1)$ etc. are easily verified.

This shows the claim when $e(n) \le 1$. We now show by induction on $e(n)$ that it holds in general. So let $n = 2^{e+1}m$ with $e \ge 2$ and m odd. Then

$$h_n = h_{2^e m}(h_{2^e m+2}h_{2^e m-1}^2 - h_{2^e m-2}h_{2^e m+1}^2)\,.$$

The second factor is (mod $4R$)

$$\begin{aligned}
h_{2^e m+2}h_{2^e m-1}^2 - h_{2^e m-2}h_{2^e m+1}^2 &\equiv (-1)^{2^{e-2}m}g^{d(2^e m+1)+2d(2^e m-1)} \\
&\qquad - (-1)^{2^{e-2}m-1}g^{d(2^e m-2)+2d(2^e m+1)} \\
&\equiv 2g^{d(2^{e+1}m)-d(2^e m)}\,,
\end{aligned}$$

whereas the first is

$$h_{2^e m} \equiv 2^{e-1}g^{d(2^e m)} \bmod 2^e R\,.$$

Multiplying gives the desired congruence

$$h_{2^{e+1}m} \equiv 2^e g^{d(2^{e+1}m)} \bmod 2^{e+1}R\,. \qquad \square$$

3. Application to the Legendre family

We consider the Legendre family $E_\lambda\colon y^2 = x(x-1)(x-\lambda)$ of elliptic curves. We denote by $\psi_n(\lambda, x)$ the nth reduced division polynomial of E_λ; its roots are the x-coordinates of

the points of order dividing n and > 2. These polynomials are related to the 'bicyclotomic polynomials' $B_n^*(x,T)$ of Masser and Zannier [MZ13] via

$$\psi_n(\lambda,x) = \prod_{2\neq d\mid n} B_d^*(x,\lambda)\,.$$

We have $\psi_1 = \psi_2 = 1$,

$$\psi_3(\lambda,x) = 3x^4 - 4(\lambda+1)x^3 + 6\lambda x^2 - \lambda^2$$
$$\psi_4(\lambda,x) = 2(x^2-\lambda)(x^2-2x+\lambda)(x^2-2\lambda x+\lambda)$$

and

$$\psi_{2m}(\lambda,x) = \psi_m(\lambda,x)\big(\psi_{m+2}(\lambda,x)\psi_{m-1}(\lambda,x)^2 - \psi_{m-2}(\lambda,x)\psi_{m+1}(\lambda,x)^2\big)$$
$$\psi_{4m+1}(\lambda,x) = 16x^2(x-1)^2(x-\lambda)^2\psi_{2m+2}(\lambda,x)\psi_{2m}(\lambda,x)^3 - \psi_{2m-1}(\lambda,x)\psi_{2m+1}(\lambda,x)^3$$
$$\psi_{4m-1}(\lambda,x) = \psi_{2m+1}(\lambda,x)\psi_{2m-1}(\lambda,x)^3 - 16x^2(x-1)^2(x-\lambda)^2\psi_{2m-2}(\lambda,x)\psi_{2m}(\lambda,x)^3$$

It follows that $\psi_n(\lambda,x) \in \mathbb{Z}[\lambda,x]$ for all $n \geq 1$.

We note that

$$\psi_3(\lambda,x) \equiv -(\lambda-x^2)^2 \bmod 4\mathbb{Z}[\lambda,x] \qquad \text{and}$$
$$\psi_4(\lambda,x) \equiv 2(\lambda-x^2)^3 \bmod 4\mathbb{Z}[\lambda,x]\,.$$

So we can apply Proposition 1 with $R = \mathbb{Z}[\lambda,x]$, $f = 4x^2(x-1)^2(x-\lambda)^2$ and $g = \lambda - x^2$. This gives the following.

Proposition 2. *For $n \in \mathbb{Z}_{>0}$, we have*

$$\psi_n(\lambda,x) \equiv 2^{e(n)}(\lambda-x^2)^{d(n)} \bmod 2^{e(n)+1}\mathbb{Z}[\lambda,x]\,.$$

Furthermore, $\deg_\lambda \psi_n(\lambda,x) = d(n)$ and $\deg \psi_n(\lambda,x) = \deg_x \psi_n(\lambda,x) = 2d(n)$, where $\deg$ denotes the total degree.

Proof. The congruence follows from Proposition 1. The upper bounds $\deg_\lambda \psi_n(\lambda,x) \leq d(n)$ and $\deg_x \psi_n(\lambda,x) \leq \deg \psi_n(\lambda,x) \leq 2d(n)$ follow easily by induction, using the recurrence relations. Since the reduction of $\psi_n(\lambda,x)$ modulo a suitable power of 2 has λ-degree $d(n)$ and x-degree $2d(n)$, we actually have equality. □

Recall the definitions

$$T(\alpha) = \{\lambda \in \mathbb{C}\setminus\{0,1\} : P_\alpha(\lambda) \in (E_\lambda)_{\mathrm{tors}}\} \quad \text{and} \quad T(\alpha,\beta) = T(\alpha)\cap T(\beta)\,.$$

It is clear that $T(\alpha) \subseteq \bar{\mathbb{Q}}$ if $\alpha \in \bar{\mathbb{Q}}$. More generally, if $\lambda \in T(\alpha)$, then λ is algebraic over $\mathbb{Q}(\alpha)$ and α is algebraic over $\mathbb{Q}(\lambda)$. This immediately implies that $T(\alpha,\beta) = \emptyset$ whenever the transcendence degree of $\mathbb{Q}(\alpha,\beta)$ is 2 (compare [MZ13, p. 636]). We will now consider the other extreme, when α and β are both algebraic over $\mathbb{Q}$.

For the following, fix an embedding $i\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_2$. Write $Z \subseteq \bar{\mathbb{Q}}$ for the subring of elements α such that $i(\alpha)$ is integral and denote the natural 'reduction' map $\bar{\mathbb{Q}} \hookrightarrow \mathbb{P}^1(\bar{\mathbb{Q}}_2) \to \mathbb{P}^1(\bar{\mathbb{F}}_2)$ by ρ. We write $v\colon \bar{\mathbb{Q}} \to \mathbb{Q}\cup\{\infty\}$ for the valuation associated to i, normalized such that $v(2) = 1$.

Theorem 3. *Let $\alpha \in \bar{\mathbb{Q}}\setminus\{0,1\}$. Then $T(\alpha) = \{\alpha\}\cup T'(\alpha)$, where $\rho\big(T'(\alpha)\big) \subseteq \{\rho(\alpha^2)\}$.*

Proof. Let $\lambda \in T(\alpha)$ and let $n \geq 2$ be the order of the point $P_\alpha(\lambda) \in E_\lambda(\bar{\mathbb{Q}})$. If $n = 2$, then $\lambda = \alpha$. Otherwise $n \geq 3$ and $\psi_n(\lambda, \alpha) = 0$.

First assume $\rho(\alpha) \neq \infty$, so that $\alpha \in Z$. Proposition 2 then shows that $2^{-e(n)}\psi_n(t, \alpha) \in Z[t]$ with unit leading coefficient, so $\lambda \in Z$ and

$$0 = 2^{-e(n)}\psi_n(\lambda, \alpha) \equiv (\lambda - \alpha^2)^{d(n)} \bmod 2Z\,,$$

which implies $\rho(\lambda) = \rho(\alpha^2)$ (note that $d(n) > 0$ for $n \geq 3$).

Now consider the case $\rho(\alpha) = \infty$. Assuming that $\lambda \in Z$, Proposition 2 shows that the term coming from the monomial $x^{2d(n)}$ is the unique term in $2^{-e(n)}\psi_n(\lambda, \alpha)$ with minimal valuation ($= 2d(n)v(\alpha)$), so $\psi_n(\lambda, \alpha)$ cannot vanish. This shows that $\lambda \in \bar{\mathbb{Q}} \setminus Z$, so $\rho(\lambda) = \infty = \rho(\alpha^2)$. □

We note that Mavraki [Mav15, Section 4] has recently given an alternative proof based on the 2-adic dynamics of the associated Lattès map. We come back to this approach after stating the following easy corollary.

Corollary 4. *Let $\alpha, \beta \in \bar{\mathbb{Q}} \setminus \{0, 1\}$ such that $\rho(\alpha) \neq \rho(\beta)$. Then*

$$T(\alpha, \beta) \subseteq \{\alpha, \beta\}\,.$$

In particular, $T(\alpha, \beta)$ is finite and effectively computable.

Proof. Theorem 3 shows that any $\lambda \in T(\alpha, \beta) \setminus \{\alpha, \beta\}$ must satisfy $\rho(\lambda) = \rho(\alpha^2) = \rho(\beta^2)$. The existence of such a λ would imply that $\rho(\alpha) = \rho(\beta)$ (recall that squaring is a bijection on $\mathbb{P}^1(\bar{\mathbb{F}}_2)$), contradicting the assumption. Regarding the effectivity statement, note that it is easy to decide for any given λ if $\lambda \in T(\alpha, \beta)$ or not: just check if the points with x-coordinate α or β are torsion on E_λ. □

To get somewhat stronger results, we use the Lattès map

$$f_\lambda \colon x \longmapsto \frac{(x^2 - \lambda)^2}{4x(x-1)(x-\lambda)}$$

that expresses the x-coordinate of $2P$ in terms of the x-coordinate of P, for a point $P \in E_\lambda$. Then $T(\alpha)$ can also be characterized as the set of $\lambda \in \mathbb{C} \setminus \{0, 1\}$ such that α is preperiodic under iteration of f_λ on $\mathbb{P}^1$. We will use the obvious fact that P is torsion if and only if $2P$ is, which implies that

$$\lambda \in T(\alpha) \iff f_\lambda(\alpha) \in \{0, 1, \lambda, \infty\} \quad \text{or} \quad \lambda \in T(f_\lambda(\alpha))\,.$$

Note that (for $\alpha, \lambda \neq 0, 1$)

$$f_\lambda(\alpha) \in \{0, 1, \lambda, \infty\} \iff \lambda \in \left\{\alpha, \alpha^2, \alpha(2-\alpha), \frac{\alpha^2}{2\alpha - 1}\right\}.$$

Lemma 5. *Let $\alpha, \lambda \in \bar{\mathbb{Q}} \setminus \{0, 1\}$ such that $\lambda \in T(\alpha)$. Then $\lambda \in \{\alpha, \alpha^2, \alpha(2-\alpha), \alpha^2/(2\alpha-1)\}$ or $\rho(f_\lambda(\alpha)) = \rho(\alpha)$.*

Proof. If $P_\alpha(\lambda)$ has order dividing 4, then λ is in the first set. Otherwise $2P_\alpha(\lambda) = P_{f_\lambda(\alpha)}(\lambda)$ is a point of order > 2, and the claim follows from (the proof of) Theorem 3, which tells us that $\rho(f_\lambda(\alpha)^2) = \rho(\lambda) = \rho(\alpha^2)$. □

We use this to strengthen Theorem 3 in the following way.

Theorem 6. *Let $\alpha \in Z \setminus \{0,1\}$. Then*

$$\begin{aligned} T(\alpha) &\subseteq \left\{\alpha, \alpha^2, \alpha(2-\alpha), \frac{\alpha^2}{2\alpha-1}\right\} \cup \{\alpha^2 + 2u\alpha(1-\alpha) : u \in Z, \rho(u^2) = \rho(\alpha)\} \\ &\subseteq \{\alpha\} \cup (\alpha^2 + 2Z)\,. \end{aligned}$$

For $\alpha \in \bar{\mathbb{Q}}$ with $\rho(\alpha) = \infty$ we have

$$T(\alpha) \subseteq \left\{\alpha, \alpha^2, \alpha(2-\alpha), \frac{\alpha^2}{2\alpha-1}\right\} \cup \left\{\frac{\alpha^2}{1+2(\alpha-1)u} : u \in Z, \rho(u) = 0\right\}.$$

Proof. We use Lemma 5; we have to show that $\rho(f_\lambda(\alpha)) = \rho(\alpha)$ implies that λ is in the secon set in the union in each case.

We first assume $\rho(\alpha) \notin \{0, 1, \infty\}$. Then $\rho(\lambda) = \rho(\alpha^2) \neq \rho(\alpha)$, so $\alpha(\alpha-1)(\alpha-\lambda) \in Z^\times$, and a necessary condition is that $f_\lambda(\alpha) \in Z^\times$, which is equivalent to $2v(\alpha^2 - \lambda) = 2$, so $\lambda = \alpha^2 + 2u\alpha(1-\alpha)$ with some $u \in Z^\times$.

Next we consider $\rho(\alpha) = 1$. Write $\alpha = 1 + \delta$ and $\lambda = 1 + \delta - \varepsilon$ with $v(\delta), v(\varepsilon) > 0$. We have $\alpha(\alpha-1)(\alpha-\lambda) = \alpha\delta\varepsilon$ and $\alpha^2 - \lambda = \delta(\delta+1) + \varepsilon$, so the necessary condition $v(f_\lambda(\alpha)) = 0$ means

$$2v(\delta(\delta+1) + \varepsilon) = 2 + v(\delta) + v(\varepsilon)\,.$$

If $v(\delta) \neq v(\varepsilon)$, then we obtain the contradiction

$$2 + v(\delta) + v(\varepsilon) > 2 + 2\min\{v(\delta), v(\varepsilon)\} > 2v(\delta(\delta+1) + \varepsilon)\,.$$

Otherwise, we find that $v(\alpha^2 - \lambda) = 1 + v(\delta) = v(2\delta)$, so again $\lambda = \alpha^2 + 2\alpha(1-\alpha)u$ with a unit $u \in Z^\times$. Using this in the expression for $f_\lambda(\alpha)$, we find (in both cases considered) that

$$\rho(\alpha) \stackrel{!}{=} \rho(f_\lambda(\alpha)) = \rho(u^2)\,.$$

The cases $\rho(\alpha) = 0$ and $\rho(\alpha) = \infty$ can be reduced to $\rho(\alpha) = 1$ by noting that $\lambda \in T(\alpha)$ is equivalent to $1 - \lambda \in T(1-\alpha)$ and to $1/\lambda \in T(1/\alpha)$. □

Note that we have only used one step in the iteration of f_λ, so further improvements should be possible.

When $\alpha \in \bar{\mathbb{Q}} \setminus \{0,1\}$ we write

$$R(\alpha) = \begin{cases} \{\alpha^2 + 2u\alpha(1-\alpha) : u \in Z, \rho(u^2) = \rho(\alpha)\} & \text{if } \alpha \in Z, \\ \left\{\frac{\alpha^2}{1+2(\alpha-1)u} : u \in Z, \rho(u) = 0\right\} & \text{otherwise} \end{cases}$$

and

$$S(\alpha) = \left\{\alpha, \alpha^2, \alpha(2-\alpha), \frac{\alpha^2}{2\alpha-1}\right\}.$$

Proposition 7. *Let $\alpha, \beta \in \bar{\mathbb{Q}} \setminus \{0,1\}$. If $R(\alpha) \cap R(\beta) = \emptyset$, then*

$$T(\alpha,\beta) \subseteq \big(S(\alpha) \cap S(\beta)\big) \cup \big(S(\alpha) \cap R(\beta)\big) \cup \big(R(\alpha) \cap S(\beta)\big) \subseteq S(\alpha) \cup S(\beta)\,.$$

In particular, $T(\alpha,\beta)$ is finite and effectively computable.

The condition $R(\alpha) \cap R(\beta) = \emptyset$ holds in the following situations.

(1) $\rho(\alpha) \neq \rho(\beta)$;
(2) $\rho(\alpha) = \rho(\beta) \notin \{0, 1, \infty\}$ *and* $v(\alpha - \beta) \leq 1/2$;
(3) $\rho(\alpha) = \rho(\beta) = 1$, $0 < v(\alpha - 1) \leq 1$ *and* $v(\alpha - \beta) = v(\alpha - 1)$;
(4) $\rho(\alpha) = \rho(\beta) = 0$, $v(\alpha) \leq 1$ *and* $v(\alpha - \beta) = v(\alpha)$;
(5) $\rho(\alpha) = \rho(\beta) = \infty$, $v(\alpha) \geq -1$ *and* $v(\alpha - \beta) = v(\beta)$.

Proof. The first statement is clear, since by Theorem 6, $T(\alpha) \subseteq S(\alpha) \cup R(\alpha)$ and $S(\alpha)$ is finite.

Case (1) was already dealt with in Corollary 4. For case (2), we observe that $v(\alpha - \beta) \leq 1/2$ implies $v(\alpha^2 - \beta^2) \leq 1$. The difference δ of an element in $R(\alpha)$ and an element of $R(\beta)$ satisfies $v(\delta - (\alpha^2 - \beta^2)) > 1$, which implies that δ cannot be zero. In case (3), we write $\alpha = 1 + \varepsilon$, $\beta = 1 + \varepsilon'$; then $v(\varepsilon) \leq 1$ and either $v(\varepsilon') > v(\varepsilon)$ or $v(\varepsilon') = v(\varepsilon) = v(\varepsilon - \varepsilon')$. An element of $R(\alpha)$ has the form $1+2\varepsilon+\varepsilon^2+2\varepsilon(1+\varepsilon)(1+\eta_1) = 1+\varepsilon^2+2\varepsilon\eta$ where $v(\eta_1), v(\eta) > 0$, and similarly for $R(\beta)$. So the difference is $\delta = \varepsilon^2 - \varepsilon'^2 + 2(\varepsilon\eta - \varepsilon'\eta')$. If $v(\varepsilon) < v(\varepsilon')$, then $v(\delta) = 2v(\varepsilon)$, so $\delta \neq 0$. In the other case $v(\delta) = v(\varepsilon^2 - \varepsilon'^2) = 2v(\varepsilon - \varepsilon') = 2v(\varepsilon)$, so again $\delta \neq 0$. The remaining cases can be reduced to case (3) in the usual way. □

We consider the case of rational numbers in more detail.

Corollary 8. *Let* $\alpha, \beta \in \mathbb{Q} \setminus \{0, 1\}$.

(1) *If* $\rho(\alpha) \neq \rho(\beta)$, *then* $T(\alpha, \beta) = \emptyset$.
(2) *If* $\alpha \equiv 3 \bmod 4$ *and* $\beta \equiv 1 \bmod 4$, *then* $T(\alpha, \beta) \subseteq \{\alpha^2, \beta\}$.
(3) *If* $\alpha \equiv 2 \bmod 4$ *and* $\beta \equiv 0 \bmod 4$, *then* $T(\alpha, \beta) \subseteq \{\alpha(2 - \alpha), \beta\}$.
(4) *If* $v(\alpha) = -1$ *and* $v(\beta) \leq -2$, *then* $T(\alpha, \beta) \subseteq \{\alpha^2/(2\alpha - 1), \beta\}$.

Proof. For (1) see Corollary 4 and note that $\rho(\alpha^2) = \rho(\alpha)$ and $\rho(\beta^2) = \rho(\beta)$. Statement (2) follows by obseerving that all elements of $T(\beta)$ except possibly β are in $1 + 8Z$, whereas α^2 is the only element of $T(\alpha)$ with this property. Parts (3) and (4) are deduced from (2). □

This can be interpreted as saying that when α and β 'differ mod 4', then we can determine $T(\alpha, \beta)$ effectively and the set has at most two elements.

Examples 9. We apply the results above to give examples of numbers $\alpha, \beta \in \bar{\mathbb{Q}} \setminus \{0, 1\}$ such that $T(\alpha, \beta)$ can be determined explicitly and has zero, one or two elements.

(1) $T(2, 3) = \emptyset$. This is a special case of Corollary 8 (1).
(2) Let ω be a primitive cube root of unity. Then $T(\omega, \omega^2) = \{\omega, \omega^2\}$. The second statement of Corollary 4 gives the inclusion '$\subseteq$'. It is easily checked that $P_\omega(\omega)$ and $P_{\omega^2}(\omega^2)$ have order 2, while $P_\omega(\omega^2)$ and $P_{\omega^2}(\omega)$ have order 4.
(3) $T(2, 4) = \{4\}$. The inclusion $T(2, 4) \subseteq \{4\}$ follows from Corollary 8 (3) (recall that zero is not a permissible value). On the other hand, $4 = 2^2$ is clearly in $T(2, 4)$.
(4) $T(3, -3) = \{-3, 9\}$. The inclusion '$\subseteq$' follows from Corollary 8 (2). Clearly $9 = 3^2 = (-3)^2 \in T(3, -3)$, and one checks that $-3 \in T(3)$.

In a similar (but even simpler) way as we did it above regarding the 2-adic behavior of the ψ_n, one can show the following.

Proposition 10. *For every $n \geq 1$, we have*

$$\psi_n(\lambda, 0) = a_n \lambda^{d(n)}$$
$$\psi_n(\lambda, 1) = a_n (1-\lambda)^{d(n)}$$
$$\psi_n(\lambda, \lambda) = a_n \big(\lambda(1-\lambda)\big)^{d(n)}$$

where $a_{2m+1} = (-1)^m$ and $a_{2m} = (-1)^{m-1} m$.

From this, one can conclude that if a and b are integers and p is a prime such that $a \equiv 0 \bmod p$ and $b \equiv 1 \bmod p$, then for any $\lambda \in T(a,b) \setminus \{a, b\}$, the order of the points $P_a(\lambda)$ and $P_b(\lambda)$ must be a multiple of $2p$. Since this result is much weaker than what can be obtained from the consideration of the 2-adic behavior, we will not pursue this further here. It may be worth while, however, to study the p-adic behavior of the polynomials ψ_n for $p \neq 2$ in some detail.

4. An unlikely intersection problem of Habegger, Jones and Masser

In a recent preprint [HJM15] Habegger, Jones and Masser consider various specific unlikely intersection problems, one of which asks for the set $T(2) \cap \boldsymbol{\mu}$, where $\boldsymbol{\mu} = \exp(2\pi i \mathbb{Q}) \subseteq \mathbb{C}$ denotes the set of roots of unity. The result they obtain in this case (Theorem 5 in loc. cit.) is that there is an effective constant $C > 0$ such that $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq C$ for every $\zeta \in T(2) \cap \boldsymbol{\mu}$. In this section we use the results of the previous section to obtain a much stronger result.

We continue to work with the ring $Z \subseteq \bar{\mathbb{Q}}$, the reduction map $\rho\colon \bar{\mathbb{Q}} \to \mathbb{P}^1(\bar{\mathbb{F}}_2)$ and the valuation map $v\colon \bar{\mathbb{Q}} \to \mathbb{Q} \cup \{\infty\}$.

Corollary 11. *Let $\alpha \in \bar{\mathbb{Q}}$ be such that some conjugate of α is not in $Z^\times$ (i.e., is not a 2-adic unit). Then $T(\alpha) \cap \boldsymbol{\mu} = \emptyset$. In particular, $T(2) \cap \boldsymbol{\mu} = \emptyset$.*

Proof. After applying an automorphism of $\bar{\mathbb{Q}}$ we can assume that $\alpha \notin Z^\times$, which implies that $\rho(\alpha) \in \{0, \infty\}$. By Theorem 3 we have $T(\alpha) = \{\alpha\} \cup T'(\alpha)$ with $\rho(T'(\alpha)) \subseteq \{\rho(\alpha^2)\}$. So $\rho(T(\alpha)) \subseteq \{0\}$ or $\rho(T(\alpha)) \subseteq \{\infty\}$. Since clearly $\rho(\boldsymbol{\mu}) \cap \{0, \infty\} = \emptyset$, the claim follows. □

The case of 2-adic units is more interesting. Note that $\alpha \in T(\alpha) \cap \boldsymbol{\mu}$ when $\alpha \in \boldsymbol{\mu}$, so we can definitely have non-empty intersections in this case. Theorem 3 tells us that any $\alpha \neq \zeta \in T(\alpha) \cap \boldsymbol{\mu}$ must satisfy $\rho(\zeta) = \rho(\alpha^2)$. There is a unique $\zeta_0 \in \boldsymbol{\mu}$ of odd order satisfying this requirement, and we obtain that

$$T'(\alpha) \cap \boldsymbol{\mu} \subseteq \{\zeta_0 \zeta : \zeta \in \boldsymbol{\mu}_{2^\infty}\}$$

where $\boldsymbol{\mu}_{2^\infty}$ denotes the group of roots of unity of order 2^m for some m. From Theorem 6 we get the more precise requirement

$$T'(\alpha) \subseteq \alpha^2 + 2Z\,.$$

Write $\zeta_0^{-1}\alpha^2 = 1 + \varepsilon$ with $v(\varepsilon) > 0$. Then we must have

$$\zeta \equiv 1 + \varepsilon \bmod 2Z\,.$$

This leads to the following.

Corollary 12. *Let $\alpha \in \bar{\mathbb{Q}}$ be such that all conjugates of α are in $Z^\times$. Then $T(\alpha) \cap \boldsymbol{\mu}$ has at most two elements different from α; the set can be effectively determined.*

If $\alpha \in \boldsymbol{\mu}$, then

$$\{\alpha, \alpha^2\} \subseteq T(\alpha) \cap \boldsymbol{\mu} \subseteq \{\alpha, \alpha^2, -\alpha^2\}$$

except when $\alpha = -1$, where we have $T(-1) \cap \boldsymbol{\mu} = \{-1\}$.

Proof. We note first that $\boldsymbol{\mu} \cap (1+2Z) = \{-1, 1\}$. Assume that $\zeta \in \boldsymbol{\mu}$ satisfies $\zeta \equiv 1+\varepsilon \bmod 2$. If ζ' is another such root of unity, then $\zeta'\zeta^{-1} \in 1 + 2Z$ and so $\zeta' = \pm\zeta$. We conclude that $T'(\alpha) \cap \boldsymbol{\mu} \subseteq \{\pm\zeta_0\zeta\}$. Note that we can effectively decide whether ζ exists, and if so, find it. This implies effectivity.

For the second statement note that α and α^2 (unless $\alpha^2 = 1$) are always in $T(\alpha)$. If $\alpha \in \boldsymbol{\mu}$, then we can take $\zeta_0 = \alpha^2$ and $\varepsilon = 0$ in the argument above, so that $-\zeta_0 = -\alpha^2$ is the only remaining possibility. When $\alpha = -1$, we have $\{\alpha, \pm\alpha^2\} \setminus \{0, 1\} = \{-1\}$. □

When $\alpha \in \boldsymbol{\mu}$, we can actually rule out the occurrence of $-\alpha^2$ in most cases. Note that $-\alpha^2 \in T(\alpha)$ implies that

$$\rho(\alpha) = \rho(f_{-\alpha^2}(\alpha)) = \rho\Big(\frac{\alpha^2}{\alpha^2 - 1}\Big)\,.$$

This implies $\rho(\alpha^2 + \alpha + 1) = 0$, which means that the order of α is of the form $3 \cdot 2^m$. In the next step, we have

$$f_{-\alpha^2}\Big(\frac{\alpha^2}{\alpha^2 - 1}\Big) = \frac{(\alpha^4 - \alpha^2 + 1)^2}{4\alpha^2(\alpha^2 - 1)}\,,$$

which must be zero or a 2-adic unit. In the first case $\alpha^4 - \alpha^2 + 1 = 0$, which is satisfied by the primitive 12th roots of unity. Otherwise we must have $v(\alpha^4 - \alpha^2 + 1) = 1$. Since $\alpha^4 - \alpha^2 + 1 \equiv (\alpha^2 + \alpha + 1)^2 \bmod 2Z$ and $\alpha - 1$ is a unit, we get $\alpha^3 = 1 + \varepsilon$ with $v(\varepsilon) \geq 1/2$, and we know that $(1 + \varepsilon)^{2^m} = 1$ for some m. This implies $m \leq 2$, so that the order of α is 3, 6 or 12. One can check that in each of these cases we have indeed $-\alpha^2 \in T(\alpha)$. We summarize our findings.

Proposition 13. *If $\alpha \in \boldsymbol{\mu}$, then*

$$T(\alpha) \cap \boldsymbol{\mu} = \begin{cases} \{\alpha\} & \text{if } \alpha = -1, \\ \{\alpha, \alpha^2, -\alpha^2\} & \text{if } \operatorname{ord}(\alpha) \in \{3, 6, 12\}, \\ \{\alpha, \alpha^2\} & \text{otherwise.} \end{cases}$$

Together with the previous results of this section, this implies that

$$\max_{\alpha \in \mathbb{C} \setminus \{0,1\}} \#\big(T(\alpha) \cap \boldsymbol{\mu}\big) = 3$$

and the maximum is attained exactly for the eight roots of $x^8 + x^4 + 1$.

5. Application to the Weierstrass family

In this section, we consider the family

$$E_{A,B}\colon y^2 = x^3 + Ax + B$$

of elliptic curves. We denote the corresponding division polynomials by $\Psi_n(A, B, x)$. Then $\Psi_1 = \Psi_2 = 1$ as before, and

$$\begin{aligned}\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2\\ &\equiv -(A - x^2)^2 \bmod 4\mathbb{Z}[A, B, x]\\ \Psi_4 &= 2\big(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - (8B^2 + A^3)\big)\\ &\equiv 2(A - x^2)^3 \bmod 4\mathbb{Z}[A, B, x]\,.\end{aligned}$$

We have the same recurrence relations as before, with the factor $4x(x-1)(x-\lambda)$ replaced by $4(x^3 + Ax + B)$. We apply Proposition 1, taking $R = \mathbb{Z}[A, B, x]$, $f = 4(x^3 + Ax + B)^2$ and $g = A - x^2$, to obtain the following.

Proposition 14. *For all $n \geq 1$, we have*

$$\Psi_n(A, B, x) \equiv 2^{e(n)}(A - x^2)^{d(n)} \bmod 2^{e(n)+1}\mathbb{Z}[A, B, x]\,.$$

We also have $\deg_A \Psi_n = d(n)$.

For $\alpha \in \mathbb{C}$, let $P_\alpha(A, B)$ (for $4A^3 + 27B^2 \neq 0$) be a point with x-coordinate α on $E_{A,B}$ and define

$$T_W(\alpha) = \{(A, B) \in \mathbb{C}^2 : 4A^3 + 27B^2 \neq 0, P_\alpha(A, B) \in (E_{A,B})_{\text{tors}}\}\,.$$

For any subset $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{C}$, we set

$$T_W(\alpha_1, \ldots, \alpha_n) = T_W(\alpha_1) \cap \ldots \cap T_W(\alpha_n)\,.$$

Corollary 15. *Let $\alpha, \beta, \gamma \in Z$ such that $\rho(\alpha)$, $\rho(\beta)$ and $\rho(\gamma)$ are pairwise distinct. Then the intersection $T_W(\alpha, \beta, \gamma) \cap (\mathbb{C} \times Z)$ is contained in*

$$\{\big(-(\alpha^2+\alpha\beta+\beta^2), \alpha\beta(\alpha+\beta)\big), \big(-(\alpha^2+\alpha\gamma+\gamma^2), \alpha\gamma(\alpha+\gamma)\big), \big(-(\beta^2+\beta\gamma+\gamma^2), \beta\gamma(\beta+\gamma)\big)\}\,.$$

Proof. Assume that $(A, B) \in T_W(\alpha, \beta, \gamma)$ with $B \in Z$. Assume further that at least two of the points $P_\alpha(A, B)$, $P_\beta(A, B)$ and $P_\gamma(A, B)$ have order ≥ 3, say the first two. Then Proposition 14 implies that $A \in Z$ and that $\rho(\alpha^2) = \rho(A) = \rho(\beta^2)$, which contradicts the assumption. It follows that at least two of the points must have order 2, say again the first two. We must then have

$$\alpha^3 + A\alpha + B = \beta^3 + A\beta + B = 0\,.$$

The unique solution of this system of linear equations is

$$(A, B) = \big(-(\alpha^2 + \alpha\beta + \beta^2), \alpha\beta(\alpha + \beta)\big)\,.$$

The other two choices of two points give rise to the other two possible pairs. □

If one could rule out the possibility that $B \notin Z$, then it would follow that $T_W(\alpha, \beta, \gamma)$ is finite.

What one can say is the following. Assume that $B \notin Z$ and that $P_\alpha(A, B)$ has order 2. Then $A = -B/\alpha - \alpha^2$, so $v(A) \leq v(B)$. The polynomials $\Psi_n(A, B, x)$ are weighted-homogeneous of degree $2d(n)$ if x has weight 1, A has weight 2 and B has weight 3. Also, as a polynomial in A, $2^{-e(n)}\Psi_n$ has degree $d(n)$ and odd leading coefficient. This implies that in $\Psi_n(A, B, \beta)$ (say), the term involving the monomial $A^{d(n)}$ will be the unique term with minimal valuation, hence $\Psi_n(A, B, \beta) \neq 0$. So it remains to exclude the possibility that all three points have finite order ≥ 3 and $v(B) < 0$.

We note that Mavraki [Mav15] studies the case $A = 0$.

6. The case of transcendence degree 1 in the Legendre family

We now return to the Legendre family. We have seen above that $T(\alpha, \beta) = \emptyset$ if α and β are algebraically independent over $\mathbb{Q}$. What can we say when $\mathbb{Q}(\alpha, \beta)$ has transcendence degree 1? Let $F \in \mathbb{Z}[a, b]$ be primitive and irreducible and such that $F(\alpha, \beta) = 0$. Assume that $\lambda \in T(\alpha, \beta)$. This means that $\psi_m(\lambda, \alpha) = 0$ for some $m \geq 3$ or $\lambda = \alpha$, and $\psi_{m'}(\lambda, \beta) = 0$ for some $m' \geq 3$ or $\lambda = \beta$. We can replace both m and m' by their least common multiple n. Eliminating λ, we see that $F(a, b)$ must divide the resultant with respect to λ of $\psi_n(\lambda, a)$ and $\psi_n(\lambda, b)$, or else F divides $\psi_n(a, b)$ or $\psi_n(b, a)$.

Definition 16. For $m \geq 3$, let

$$R_m(a, b) = \frac{\mathrm{Res}_\lambda\big(\psi_m(\lambda, a), \psi_m(\lambda, b)\big)}{(a - b)^{\deg_\lambda \psi_m}} \in \mathbb{Z}[a, b]\,.$$

The following result provides the key step in the proof that $T(\alpha, \beta)$ has at most one element in the case of transcendence degree 1.

Proposition 17. *For all $m \geq 3$, the polynomial $R_m(a, b)$ is squarefree in $\mathbb{Q}[a, b]$.*

Proof. We consider the behavior of $R_m(a, b)$ as a tends to zero. By Proposition 10, if $\psi_m(\lambda, a) = 0$ and $a \to 0$, then $\lambda \to 0$ as well. Since clearly $R_m(a, b)$ divides $R_n(a, b)$ if m divides n, it is sufficient to consider the case that $m = 2n$ is even.

In the following, we use the symbol $\propto$ to denote equality up to a multiplicative constant. By standard properties of resultants, we have

$$(b - a)^{n^2-1} R_{2n}(a, b) \propto \prod_{j=1}^{n^2-1} \psi_{2n}(\lambda_j(a), b)\,,$$

where the $\lambda_j(a)$ are Puiseux series over $\mathbb{C}$ that represent the roots of $\psi_{2n}(\lambda, a)$ as a polynomial in λ over the power series ring $\mathbb{C}[\![a]\!]$. Since λ_j tends to zero with a, all these series have positive valuation. Factoring $\psi_{2n}(\lambda, x) \propto \prod_{j=1}^{2n^2-2}\big(x - x_j(\lambda)\big)$, where $x_j(\lambda)$ are Puiseux series in λ, we get the decomposition

$$(b - a)^{n^2-1} R_{2n}(a, b) \propto \prod_{j=1}^{n^2-1} \prod_{j'=1}^{2n^2-2} \big(b - (x_{j'} \circ \lambda_j)(a)\big)\,.$$

If we can show that the series $x_{j'} \circ \lambda_j$ are pairwise distinct (except when $(x_{j'} \circ \lambda_j)(a) = a$, which will occur for a unique j' for each j), then this will prove that $R_{2n}(a,b)$ is squarefree.

To write down these series explicitly, we use the Tate parameterization of E_λ. Recall that there are power series

$$a_4(q) = -5\sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n} \qquad \text{and} \qquad a_6(q) = -\frac{1}{12}\sum_{n=1}^{\infty} \frac{(7n^5+5n^3)q^n}{1-q^n}$$

and

$$X(u,q) = \sum_{n=-\infty}^{\infty} \frac{uq^n}{(1-uq^n)^2} - 2\sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} \in \mathbb{Q}(u)[\![q]\!]$$
$$Y(u,q) = \sum_{n=-\infty}^{\infty} \frac{u^2q^n}{(1-uq^n)^3} + \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} \in \mathbb{Q}(u)[\![q]\!]$$

such that $\big(X(\cdot,q), Y(\cdot,q)\big)$ induces a group isomorphism of $\mathbb{C}^\times/q^{\mathbb{Z}}$ with the $\mathbb{C}$-points on $E_{\text{Tate}}(q)\colon y^2+xy = x^3+a_4(a)x+a_6(q)$, when $0<|q|<1$. See for example [Sil94, Chapter V].

We match this up with E_λ: for suitable $q = Q^2$, we have an isomorphism $\phi\colon E_{\text{Tate}}(Q^2) \cong E_\lambda$ such that $\phi\big(X(-1,Q^2), Y(-1,Q^2)\big) = (1,0)$ and $\phi\big(X(Q,Q^2), Y(Q,Q^2)\big) = (0,0)$. The x-coordinate on E_λ is then given in terms of u by

$$\begin{aligned} x(u,Q) &= \frac{X(u,Q^2)-X(Q,Q^2)}{X(-1,Q^2)-X(Q,Q^2)} \\ &= -\frac{4}{(1-u)^2}\Big(u - 2(1+u)^2Q + (1+u)^2(1+8u+u^2)\frac{Q^2}{u} \\ &\qquad\qquad - 8(1+u)^2(1+3u+u^2)\frac{Q^3}{u} + \dots\Big) \\ &\in \mathbb{Q}(u)[\![Q^2/u]\!] + Q\mathbb{Q}(u)[\![Q^2/u]\!] \end{aligned}$$

and from $x(-Q,Q) = \lambda$ we have the relation

$$\lambda = 16(Q - 8Q^2 + 44Q^3 - 192Q^4 + 718Q^5 - 2400Q^6 + 7352Q^7 + \dots)\,.$$

We use Q as our parameter instead of λ and $\xi(u,Q) = -x(u,Q)/4$ instead of x; this simplifies the formulas.

We first consider the series in Q expressing the ξ-coordinates. To obtain a further simplification, we set $\xi = \Xi/(1-\Xi)^2$ (with Ξ tending to zero with ξ). Then we get the somewhat simpler relation

$$\Xi(u,Q) = u - 2(1-u^2)Q + (1-u^2)(1-3u^2)\frac{Q^2}{u} + 4(1-u^2)^2Q^3 + O(Q^4/u)\,.$$

Fix an nth root w of Q. We set $\zeta_m = \exp(2\pi i/m)$. The Ξ-coordinates of the $2n$-torsion points are then given by $\Xi(\zeta_{2n}^k w^\ell, Q)$, where $\ell \in \{0,1,\dots,n\}$ and $k \in \{0,1,\dots,2n-1\}$. For $\ell = 0$ or $\ell = n$, we restrict to $0<k<n$ (this also excludes the 2-torsion points). Plugging $u = \zeta_{2n}^k w^\ell = \zeta_{2n}^k Q^{\ell/n}$ into the series for ξ, we obtain the relation

$$\Xi_{k,\ell}(Q) = \zeta_{2n}^k Q^{\ell/n} - 2Q + \zeta_{2n}^{-k} Q^{2-\ell/n} + O(Q^{1+2\ell/n})\,.$$

We set $\gamma_k = \zeta_{2n}^k - 2 + \zeta_{2n}^{-k} = 2(\cos\frac{k\pi}{n} - 1)$. For $\ell = 0$, we get

$$\xi_{k,0}(Q) = \frac{1}{\gamma_k}\big(1 - 2(\gamma_k+4)Q + (\gamma_k+4)(\gamma_k+10)Q^2 + \ldots\big)\,,$$

which tends to the nonzero value γ_k^{-1} as $Q \to 0$. For $0 < \ell < n$, the first two leading terms in $\Xi_{k,\ell}(Q)$ are

$$\Xi_{k,\ell}(Q) = \zeta_{2n}^k Q^{\ell/n} - 2Q + \ldots\,,$$

and for $\ell = n$, we have

$$\Xi_{k,n}(Q) = \gamma_k Q + 2\gamma_k(\gamma_k+2)Q^3 + \ldots\,.$$

Now we express Q in terms of Ξ. We know that Q tends to zero with Ξ, so we must have $0 < \ell \le n$ in the relations above. Solving for Q, we obtain for $0 < \ell < n$

$$Q_{k,\ell}(\Xi) = \zeta_{2\ell}^{-k}\Xi^{n/\ell} + \frac{2n}{\ell}\zeta_{2\ell}^{-2k}\Xi^{2n/\ell-1} + \ldots\,,$$

where we can restrict to $0 \le k < 2\ell$. For $\ell = n$, we get

$$Q_{k,n}(\Xi) = \frac{1}{\gamma_k}\Xi - 2\frac{\gamma_k+2}{\gamma_k^3}\Xi^3 + \ldots\,.$$

Here, $0 < k < n$ as before. In total, we obtain

$$\big(2+4+6+\ldots+(2n-2)\big) + (n-1) = (n-1)n + (n-1) = n^2 - 1 = d(2n) = \deg_\lambda \psi_{2n}$$

values of Q in terms of Ξ; this accounts for all possibilities. We observe that the n^2-1 series $Q_{k,\ell}$ all have distinct leading terms (note that $0 > \gamma_1 > \gamma_2 > \ldots > \gamma_{n-1} > -4$).

We first consider the series of the form $\xi_{k',0} \circ Q_{k,\ell}$. They have the form

$$(\xi_{k',0} \circ Q_{k,\ell})(\alpha) = \frac{1}{\gamma_{k'}}\big(1 - 2(\gamma_{k'}+4)Q_{k,\ell}(\alpha) + \ldots\big)\,.$$

The constant term determines k', and the next term determines the leading term of $Q_{k,\ell}$ and therefore k and ℓ. So all these series are pairwise distinct (and also distinct from all series $\xi_{k',\ell'} \circ Q_{k,\ell}$ with $\ell' > 0$, since these series have positive valuation).

For the remaining series, we work with Ξ instead of ξ, so we consider $\Xi_{k',\ell'} \circ Q_{k,\ell}$, where now $\ell' > 0$. We obtain the following different cases, where $\ell, \ell' < n$.

$$\begin{aligned}
(\Xi_{k',\ell'} \circ Q_{k,\ell})(\alpha) &= \zeta_{2\ell n}^{k'\ell - k\ell'}\alpha^{\ell'/\ell} + \frac{2\ell'}{\ell}\zeta_{2\ell n}^{k'\ell-k\ell'}\zeta_{2\ell}^{-k}\alpha^{(n+\ell')/\ell-1} + \ldots && \text{if } \ell' < \ell\\
(\Xi_{k',\ell'} \circ Q_{k,\ell})(\alpha) &= \zeta_{2n}^{k'-k}\alpha + 2(\zeta_{2n}^{k'-k} - 1)\zeta_{2\ell}^{-k}\alpha^{n/\ell} + \ldots && \text{if } \ell' = \ell\\
(\Xi_{k',\ell'} \circ Q_{k,\ell})(\alpha) &= \zeta_{2\ell n}^{k'\ell - k\ell'}\alpha^{\ell'/\ell} - 2\zeta_{2\ell}^{-k}\alpha^{n/\ell} + \ldots && \text{if } \ell' > \ell\\
(\Xi_{k',\ell'} \circ Q_{k,n})(\alpha) &= \frac{\zeta_{2n}^{k'}}{\gamma_k^{\ell'/n}}\alpha^{\ell'/n} - \frac{2}{\gamma_k}\alpha + \ldots\\
(\Xi_{k',n} \circ Q_{k,\ell})(\alpha) &= \gamma_{k'}\zeta_{2\ell}^{-k}\alpha^{n/\ell} + \frac{2n}{\ell}\gamma_{k'}\zeta_{2\ell}^{-2k}\alpha^{2n/\ell-1} + \ldots\\
(\Xi_{k',n} \circ Q_{k,n})(\alpha) &= \frac{\gamma_{k'}}{\gamma_k}\alpha + 2\frac{\gamma_{k'}(\gamma_{k'}-\gamma_k)}{\gamma_k^3}\alpha^3 + \ldots
\end{aligned}$$

We note that the second term vanishes if and only if $(k', \ell') = (k, \ell)$, in which case we obtain the excluded trivial series α. The last case in the list above is distinguished from the second by the fact that the leading coefficient has absolute value $\neq 1$. Taking this into account, the orders of the first two terms determine ℓ and ℓ'. In all cases but the last, one easily sees that the coefficients of the first and the second term together determine k and k'. In the last case, writing $\rho = \gamma_{k'}/\gamma_k \neq 1$ for the first coefficient, the second coefficient can be written as $2\rho(\rho-1)/\gamma_k$, so both together determine k and then also k' again.

So in all cases, the series $\Xi_{k',\ell'} \circ Q_{k,\ell}$ determines the two pairs (k, ℓ) and (k', ℓ') uniquely (unless $(k, \ell) = (k', \ell')$). As noted earlier, this implies the claim. □

Before we deduce consequences of this result, we need to introduce some further objects. For $n \geq 3$, let $Z_n \subseteq \mathbb{P}^1_a \times \mathbb{P}^1_b \times \mathbb{P}^1_\lambda$ be the curve given by the equations $\psi_n(\lambda, a) = \psi_n(\lambda, b) = 0$, but excluding the components contained in the plane $a = b$. Since (for given λ) the roots of $\psi_n(\lambda, x)$ correspond to the x-coordinates of the points in $E_\lambda[n] \setminus E_\lambda[2]$, the Galois group G_n of $\psi_n(\lambda, x)$ over $\mathbb{Q}(\lambda)$ is $\mathrm{PGL}(2, \mathbb{Z}/n\mathbb{Z})$ when n is odd, and is the subgroup of $\mathrm{PGL}(2, \mathbb{Z}/n\mathbb{Z})$ consisting of elements represented by matrices reducing to the identity mod 2 when n is even. Over $\mathbb{C}(\lambda)$, we have to replace PGL by PSL; write G'_n for the resulting group.

Denote by T_n the set of pairs of opposite elements of $(\mathbb{Z}/n\mathbb{Z})^2$ that are not killed by 2. Then the action of G_n on the roots is the standard action on T_n. It follows that over $\mathbb{C}$, $Z_n \to \mathbb{P}^1_\lambda$ is a Galois covering with group G'_n acting diagonally on $T_n \times T_n \setminus \Delta$, where Δ denotes the diagonal. Therefore Z_n splits into geometric components corresponding to the orbits of G'_n on $T_n \times T_n \setminus \Delta$. (The irreducible components over $\mathbb{Q}$ correspond to the orbits of G_n).

Note that the equation $R_n(a, b) = 0$ describes the projection of Z_n to $\mathbb{P}^1_a \times \mathbb{P}^1_b$. Proposition 17 then says that this projection maps Z_n birationally onto its image, which we denote C_n.

We can write

$$\psi_n(\lambda, x) = \prod_{d|n} \tilde{\psi}_d(\lambda, x)\,,$$

where $\tilde{\psi}_n(\lambda, x)$, considered as a polynomial in x over $\mathbb{Q}(\lambda)$, has as its roots exactly the x-coordinates of points of exact order n on E_λ (if $n > 2$; we obviously have $\tilde{\psi}_1 = \tilde{\psi}_2 = 1$). In [MZ13, Lemma 2.1], Masser and Zannier prove that $\tilde{\psi}_n$ is absolutely irreducible if $n \geq 3$ is odd and that $\tilde{\psi}_n$ splits into three irreducible factors in $\mathbb{Q}[\lambda, x]$, which are absolutely irreducible if $n \geq 4$ is even (they correspond to fixing the point of order 2 obtained as $(n/2) \cdot P_x(\lambda)$). We will reserve the term *bicyclotomic polynomial* for these (absolutely) irreducible factors. So in the notation of [MZ13], a bicyclotomic polynomial $B(\lambda, x)$ has the form (note the reversal of the order of the variables)

$$B(\lambda, x) = B^*_n(x, \lambda) \qquad \text{for } n \geq 3 \text{ odd}$$

or

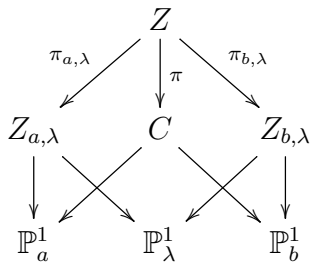
$$B(\lambda, x) = B^{(0)}_n(x, \lambda), B^{(1)}_n(x, \lambda) \quad \text{or} \quad B^{(\infty)}_n(x, \lambda) \qquad \text{for } n \geq 4 \text{ even.}$$

The index n is the *order* of B. (There are also the three polynomials x, $x - 1$ and $x - \lambda$ of order 2, which we will not call 'bicyclotomic'.)

Lemma 18. *Let C be some geometric irreducible component of C_n, for some $n \geq 3$. There are bicyclotomic polynomials $B_1(\lambda, x)$ and $B_2(\lambda, x)$ such that C is contained in the projection*

of $B_1(\lambda, a) = B_2(\lambda, b) = 0$. *Let* $F(a, b) = 0$ *be an equation for* C. *Then* $\deg_a F = \deg_b F$, *and this degree is a multiple of* $\operatorname{lcm}(\deg_\lambda B_1, \deg_\lambda B_2)$.

Proof. Since each ψ_n is a product of (absolutely irreducible) bicyclotomic polynomials, it is clear that every component of Z_n must be contained in a curve of the form $B_1(\lambda, a) = B_2(\lambda, b) = 0$. Let Z be the component of Z_n projecting to C. By Proposition 17, the map $\pi\colon Z \to C$ is birational. We have the following commuting diagram.



Here $Z_{a,\lambda} \subseteq \mathbb{P}^1_a \times \mathbb{P}^1_\lambda$ is given by $B_1(\lambda, a) = 0$; similarly for $Z_{b,\lambda}$. Note that $\pi_{a,\lambda}$ is dominant, since B_1 is irreducible; similarly for $\pi_{b,\lambda}$. It follows that

$$\deg_b F = (\deg \pi_{a,\lambda})(\deg_\lambda B_1) \qquad \text{and} \qquad \deg_a F = (\deg \pi_{b,\lambda})(\deg_\lambda B_2)\,. \tag{1}$$

Considering the two factorizations of $Z \to \mathbb{P}^1_\lambda$, we obtain (using that $\deg_x B_j = 2 \deg_\lambda B_j$)

$$2 \deg_b F = (\deg_x B_1)(\deg \pi_{a,\lambda}) = (\deg_x B_2)(\deg \pi_{b,\lambda}) = 2 \deg_a F\,.$$

This shows the equality of degrees, and the relations (1) imply that the common degree is divisible both by $\deg_\lambda B_1$ and by $\deg_\lambda B_2$. □

Corollary 19. *No geometric component of any of the curves* C_n *for* $n \geq 3$ *satisfies an equation* $B(a, b) = 0$ *or* $B(b, a) = 0$, *where* B *is any bicyclotomic polynomial.*

Proof. By Lemma 18, the polynomial F defining a component of C_n satisfies $\deg_a F = \deg_b F$. But we have $\deg_x B = 2 \deg_\lambda B$, so F cannot be a scalar multiple of B. □

We write $\mathcal{C}$ for the union of all the curves C_n, together with all curves given by equations of the form $B(a, b) = 0$ or $B(b, a) = 0$ with a bicyclotomic polynomial B. The results shown so far imply that for each (geometric) component C of $\mathcal{C}$ that is not of the form $B(a, b) = 0$ or $B(b, a) = 0$ for a bicyclotomic polynomial B, there is a unique $n \geq 3$ such that $C \subseteq C_m$ exactly when $n \mid m$.

Proposition 20. *Let* $\alpha, \beta \in \mathbb{C} \setminus \{0, 1\}$ *with* $\alpha \neq \beta$.

(1) *If* $(\alpha, \beta) \notin \mathcal{C}$, *then* $T(\alpha, \beta) = \emptyset$. *(This is true whenever* $\mathbb{Q}(\alpha, \beta)$ *has transcendence degree* 2.*)*

(2) *If* (α, β) *is a smooth point on* $\mathcal{C}$ *(i.e., it is a smooth point on one component of* $\mathcal{C}$ *and not contained in any other component), then* $\#T(\alpha, \beta) \leq 1$.
In particular, $\#T(\alpha, \beta) \leq 1$ *whenever* $\mathbb{Q}(\alpha, \beta)$ *has transcendence degree* 1.

(3) *If* $\#T(\alpha, \beta) \geq 2$, *then* (α, β) *is one of the countably many singular points of components of* $\mathcal{C}$ *or intersection points two distinct components of* $\mathcal{C}$. *In particular,* α *and* β *are algebraic.*

In general, $\#T(\alpha,\beta)$ is at most the number of branches of $\mathcal{C}$ passing through (α,β).

Proof. Let $\mathcal{Z}$ be the union of the Z_n, together with the curves defined by $\alpha=\lambda, B(\lambda,\beta)=0$ or by $B(\lambda,\alpha)=0, \beta=\lambda$. Then $\mathcal{Z}$ is smooth at all points (α,β,λ) with $\alpha,\beta,\lambda\notin\{0,1,\infty\}$. (This is because the x-coordinates of torsion points on E_λ are all distinct, as long as $\lambda\neq 0,1,\infty$. In particular, for every n the projection of $\{\psi_n(\lambda,x)=0\}\subseteq\mathbb{P}^1_x\times\mathbb{P}^1_\lambda$ to $\mathbb{P}^1_\lambda$ is étale over $\mathbb{P}^1_\lambda\setminus\{0,1,\infty\}$. Since Z_n is contained in the fiber square of this projection, its map to $\mathbb{P}^1_\lambda$ is also étale outside $0,1,\infty$. Including points of order 2 and passing to the filtered union of the Z_n, we get the claim.)

By definition, $T(\alpha,\beta)$ is the projection to $\mathbb{P}^1_\lambda$ of the preimage of (α,β) under the projection $\mathcal{Z}\to\mathbb{P}^1_a\times\mathbb{P}^1_b$, excluding $\{0,1,\infty\}$. Let $\lambda\in\mathbb{C}\setminus\{0,1\}$ be such that $P=(\alpha,\beta,\lambda)\in\mathcal{Z}$. Since P is smooth on $\mathcal{Z}$, there is exactly one branch of $\mathcal{C}$ passing through (α,β) that locally is the image of a neighborhood of P in the component of $\mathcal{Z}$ it lies on. The results shown above imply that no two such branches can coincide. So we get the last statement ('In general, ...') of the proposition; the others follow as special cases. □

Note that the inequality in the second statement of the proposition above is an equality unless the corresponding value of λ is in $\{0,1,\infty\}$. This will never be the case when α or β are transcendental. So in the case that the transcendence degree of $\mathbb{Q}(\alpha,\beta)$ is 1, we have the following (where we also use that non-smooth points on $\mathcal{C}$ must be algebraic).

Corollary 21. *Let $\alpha,\beta\in\mathbb{C}\setminus\{0,1\}$ with $\alpha\neq\beta$ and such that $\mathbb{Q}(\alpha,\beta)$ has transcendence degree 1.*

(1) *If $(\alpha,\beta)\in\mathcal{C}$, then $\#T(\alpha,\beta)=1$.*
(2) *Otherwise, $T(\alpha,\beta)=\emptyset$.*

Compare this to the upper bound $\#T(\alpha,\beta)\leq 6(12d)^{32}$ (where d is the degree of an irreducible polynomial $F\in\mathbb{Q}[u,v]$ such that $F(\alpha,\beta)=0$) given in [MZ13]!

We can also improve on [MZ13] regarding an effective statement in this case. If α and β satisfy a polynomial of degree d, then Masser and Zannier give a bound of $\pi(12d)^{17/2}$ in the main part of the paper and of $180\pi d\log(180\pi d)$ in the appendix for the orders of the corresponding torsion points on E_λ for $\lambda\in T(\alpha,\beta)$. We observe that the λ-degree of a bicyclotomic polynomial of order n is

$$\delta(n)=\frac{n^2}{4}\prod_{p\mid n}\Big(1-\frac{1}{p^2}\Big)>\frac{2n^2}{\pi^2}$$

when n is odd, and is

$$\delta(n)=\frac{n^2}{12}\prod_{p\mid n}\Big(1-\frac{1}{p^2}\Big)>\frac{n^2}{2\pi^2}$$

when n is even. By Lemma 18, any component of $\mathcal{C}$ that is related to points of order n must have degree (with respect to a or b) at least that large. So if α and β are related by an equation of degree d, this implies that $n<\pi\sqrt{2d}$. This makes it fairly easy to enumerate all curves of small degree that are components of $\mathcal{C}$.

In fact, we can obtain a list of the degrees of the components of $\mathcal{C}$ arising from two given bicyclotomic polynomials by the following combinatorial approach. Let $\hat{G}_0$ denote the principal congruence subgroup of level 2 of $\mathrm{GL}(2,\hat{\mathbb{Z}})$, where $\hat{\mathbb{Z}}$ is the pro-finite completion of $\mathbb{Z}$, so

$$\hat{G}_0 = \left\{\gamma \in \mathrm{GL}(2,\hat{\mathbb{Z}}) : \gamma \equiv \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \bmod 2\right\},$$

and let $\hat{G}$ be $\hat{G}_0/\{\pm I\}$, where I is the identity matrix. Then $\hat{G}$ acts on

$$M = \left((\mathbb{Q}/\mathbb{Z})^2 \setminus \{0\}\right)/\{\pm 1\},$$

which, after fixing a basis of the $\mathbb{Q}/\mathbb{Z}$-module $E_{\lambda,\mathrm{tors}}$, can be identified with the set of x-coordinates of torsion points of order ≥ 2 on E_λ. In particular, the $\hat{G}$-orbits on M (except the three consisting of a point of order 2) correspond bijectively to the bicyclotomic polynomials. Also, $\hat{G}$, with its diagonal action on $M \times M$, is the automorphism group of the pro-covering $\mathcal{Z} \to \mathbb{P}^1_\lambda$ over $\mathbb{Q}$. The components of $\mathcal{Z}$ (and therefore also the components of its birational image $\mathcal{C}$) correspond bijectively to the orbits of $\hat{G}$ on $M \times M$. Let O be such an orbit, corresponding to the component Z of $\mathcal{Z}$. Then the projection of $O \subseteq M \times M$ to the first factor will be an orbit of $\hat{G}$ on M, so corresponds to a bicyclotomic polynomial B_1. Similarly, the projection of O to the second factor corresponds to a bicyclotomic polynomial B_2, and Z is contained in the curve given by $B_1(\lambda, a) = B_2(\lambda, b) = 0$. We assume that none of the projections consists of a point of order 2 (they lead to components of $\mathcal{C}$ given by equations $B(a,b) = 0$ or $B(b,a) = 0$, where B is a bicyclotomic polynomial; these components are easy to describe). Then the component C of $\mathcal{C}$ that is the projection of Z is given by an equation $F(a,b) = 0$ with $\deg_a F = \deg_b F = d$, say. By the considerations in the proof of Lemma 18, we have $d = (\deg \pi_{a,\lambda})(\deg_\lambda B_1)$. So to determine d, we have to find the degree of the covering $Z \to Z_{a,\lambda}$, where $Z_{a,\lambda}$ is given by $B_1(\lambda, a) = 0$. But fixing a point on $Z_{a,\lambda}$ corresponds to fixing a representative $m \in M$ of the projection of O to the first component. Up to changing the basis of $E_{\lambda,\mathrm{tors}}$ used for the identification with $(\mathbb{Q}/\mathbb{Z})^2$, we can take $m = \frac{1}{n} \bmod \mathbb{Z}$, where n is the order of the points whose x-coordinates are the roots of $B_1(\lambda, \cdot)$. Then $\deg \pi_{a,\lambda}$ is the size of the fiber of O above m. The possible fibers are the orbits of the stabilizer of m in $\hat{G}$ on the subset M_2 of M corresponding to B_2. If the order of the points coming from B_2 is n', then the relevant group is

$$G_{n,n'} = \left\{\gamma \in \mathrm{GL}(2, \mathbb{Z}/n'\mathbb{Z}) : \gamma \equiv I \bmod \gcd(n', 2), \gamma \equiv \left(\begin{smallmatrix}1 & *\\ 0 & *\end{smallmatrix}\right) \bmod \gcd(n, n')\right\}/\{\pm I\},$$

acting on M_2. This allows us to find the degrees of all components of $\mathcal{C}$ arising from B_1 and B_2. To illustrate this, we present a table giving the number of components of $\mathcal{C}$ for small bidegrees (the *bidegree* of $F \in \mathbb{Q}[a,b]$ is the pair $(\deg_a F, \deg_b F)$).

bidegree	$(1,2)$	$(2,4)$	$(4,8)$	$(6,12)$	$(8,16)$	$(12,24)$	$(16,32)$	$(18,36)$	$(24,48)$
#components	3	4	3	4	3	4	3	4	3
bidegree	$(2,1)$	$(4,2)$	$(8,4)$	$(12,6)$	$(16,8)$	$(24,12)$	$(32,16)$	$(36,18)$	$(48,24)$
#components	3	4	3	4	3	4	3	4	3
bidegree	$(1,1)$	$(2,2)$	$(4,4)$	$(6,6)$	$(8,8)$	$(12,12)$	$(16,16)$	$(18,18)$	$(24,24)$
#components	3	18	45	44	57	68	96	76	161

This is related to the sets $\mathcal{F}_d$ defined in [MZ13], which consist of polynomials of total degre d defining components of $\mathcal{C}$. Working with the bidegree instead of the total degree appears to be more natural, since it is invariant under the action of the group S_3 (generated by the involutions $(a,b) \mapsto (1-a, 1-b)$ and $(a,b) \mapsto (1/a, 1/b)$) that stabilizes $\mathcal{C}$.

The file at [Stoa], when read into Magma, results in a list of defining polynomials F for all components of $\mathcal{C}$ such that $\deg_a F + \deg_b F \leq 192$.

$(1,1)$:	$a+b, \quad a+b-2, \quad 2ab-a-b.$
$(1,2)$:	$a-b^2, \quad a+b^2-2b, \quad 2ab-a-b^2.$
$(2,1)$:	$a^2-b, \quad a^2-2a+b, \quad a^2-2ab+b.$
$(2,2)$:	$a^2+b^2-2b, \quad a^2-2a+b^2, \quad a^2-2ab^2+b^2, \quad 2a^2b-a^2-b^2,$
	$a^2+2ab-4a+b^2, \quad a^2+2ab+b^2-4b, \quad a^2-2ab-3b^2+4b,$
	$a^2+2ab^2-4ab-b^2+2b, \quad a^2+4ab^2-2ab-3b^2, \quad a^2+4ab^2-6ab-3b^2+4b,$
	$a^2-4ab^2+2ab+b^2, \quad a^2-4ab^2+6ab-4a+b^2, \quad 3a^2+2ab-4a-b^2,$
	$2a^2b-a^2-4ab+2a+b^2, \quad 4a^2b-a^2-2ab-b^2, \quad 4a^2b-a^2-6ab-b^2+4b,$
	$4a^2b-3a^2-2ab+b^2, \quad 4a^2b-3a^2-6ab+4a+b^2.$
$(2,4)$:	$a^2+4ab^3-6ab^2-3b^4+4b^3, \quad a^2-4ab^3+6ab^2-4ab+b^4,$
	$4a^2b-a^2-6ab^2-b^4+4b^3, \quad 4a^2b-3a^2-6ab^2+4ab+b^4.$
$(4,2)$:	$a^4-4a^3b+6a^2b-4ab+b^2, \quad a^4-4a^3+6a^2b-4ab^2+b^2,$
	$a^4-6a^2b+4ab^2+4ab-3b^2, \quad 3a^4-4a^3b-4a^3+6a^2b-b^2.$

TABLE 1. Polynomials of small bidegree defining components of $\mathcal{C}$

As an illustration, in Table 1 we list the 35 polynomials of bidegrees $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$, $(2,4)$ and $(4,2)$ defining components of $\mathcal{C}$. The correctness of the list for bidegree $(1,1)$ provides a simple proof of [MZ13, Theorem 2]. In general, we obtain the following refinement of Corollary 21.

Corollary 22. *Let $\alpha, \beta \in \mathbb{C} \setminus \{0,1\}$ with $\alpha \neq \beta$ such that $\mathbb{Q}(\alpha,\beta)$ has transcendence degree 1. Then $\#T(\alpha,\beta) \leq 1$. If we are given an irreducible Polynomial $F \in \mathbb{Q}[a,b]$ such that $F(\alpha,\beta) = 0$, then we can effectively determine the set $T(\alpha,\beta)$.*

Note that for the effectivity statement, we need to *know* that α and β generate a field of transcendence degree 1, and we need to *know* the algebraic relation linking them. For example, we cannot say whether $T(e,\pi)$ is empty or not, since we do not know whether e and π are algebraically dependent or not.

We have computed the complete list of all polynomials of bidegree (d,d) defining components of $\mathcal{C}$ for all d up to 96. They were obtained either by computing resultants like R_m (but using two bicyclotomic polynomials instead of twice ψ_m) and factoring the result, or by using the relation between $x(P)$ and $x(nP)$ for suitable n, in cases where such a dependency was

satisfied in the relevant $\hat{G}$-orbit on $M \times M$. We used these polynomials as input for the computations described in the next section.

7. Speculations on the size of $T(\alpha, \beta)$

In the last case of Proposition 20 one would in general not expect that more than two branches pass through the same point: such intersections are unlikely. This leads to the following (perhaps somewhat bold) conjecture.

Conjecture 23. There are only finitely many pairs $(\alpha, \beta) \in \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}$ with $\alpha, \beta \notin \{0, 1\}$, $\alpha \neq \beta$ and $\#T(\alpha, \beta) \geq 3$.

It would be interesting to investigate if this conjecture would follow from some version of the Zilber-Pink Conjecture(s).

To get some evidence related to this question, we took all irreducible components over $\mathbb{Q}$ of $\mathcal{C}$ given by equations $f(a, b) = 0$ with $\deg_{ab} f := \deg_a f + \deg_b f \leq 192$ (as mentioned at the end of the previous section, we had computed all these equations). We then computed all intersections of two components $\{f_1 = 0\}$ and $\{f_2 = 0\}$ such that $(\deg_{ab} f_1) \cdot (\deg_{ab} f_2) \leq 384$, and all singularities of components $\{f = 0\}$ with $(\deg_{ab} f)^2 \leq 384$. After removing parts contained in $\{a(1-a)b(1-b)(a-b) = 0\}$, we split the resulting finite schemes into irreducible components over $\mathbb{Q}$ and computed the set $T_{50}(\alpha, \beta)$ for a representative point (α, β) for each of these irreducible components. Here

$$T_n(\alpha, \beta) = \{\lambda \in \mathbb{C} \setminus \{0, 1\} : P_\alpha(\lambda) \text{ and } P_\beta(\lambda) \text{ are both torsion of order} \leq n\}.$$

To reduce the amount of computation, we make use of the fact that the group $\Gamma = S_3 \times C_2$ acts on $\mathcal{C}$, where the action of S_3 is diagonal on both coordinates and generated by the involutions $x \mapsto 1 - x$ and $x \mapsto 1/x$, and the action of the cyclic group C_2 is given by swapping the coordinates. (This action lifts to an action on $\mathcal{Z}$, where S_3 acts diagonally on (a, b, λ).) This implies that Γ also acts on the countable disjoint union of $\mathbb{Q}$-integral finite schemes making up the set of all (α, β) with $\#T(\alpha, \beta) \geq 2$. It is therefore sufficient to find one representative scheme in each Γ-orbit.

This computation produced 82 717 irreducible finite schemes, falling into 8 083 Γ-orbits, and containing 2 212 784 geometric points in total, consisting of points (α, β) such that $\#T_{50}(\alpha, \beta) \geq 2$. Of these, 180 schemes making up 24 orbits and containing 558 geometric points have sets $T_{50}(\alpha, \beta)$ with three or more elements. This supports Conjecture 23 in that it shows that such pairs are quite rare. A list of representatives of all such orbits with $\#T_{50}(\alpha, \beta) = 2$ is obtained by loading the file at [Stob] into Magma. The orbits with $\#T_{50}(\alpha, \beta) \geq 3$ are given with more detailed information in the file at [Stoc]. The latter orbits are as follows. We begin with those that have $\#T_{50} = 3$.

There is one example with $\alpha, \beta \in \mathbb{Q}$, which is represented by

$$\{\alpha, \beta\} = \left\{\frac{3}{8}, -\frac{9}{16}\right\} \qquad \text{with} \qquad T_{50}(\alpha, \beta) = \left\{-\frac{9}{16}, \frac{3}{128}, \frac{81}{256}\right\}.$$

Note that α and β both reduce to ∞ mod 2, illustrating Corollary 4. The orders of the points with x-coordinate α and β on E_λ are $(4, 2)$, $(6, 6)$ and $(8, 4)$.

Then there are six examples with α and β in a quadratic field, as listed in the following table. The entry 'orders' records the torsion orders of the points with x-coordinate α and β, for each of the given values of λ. (Note that this order may change by a factor of 2 under the S_3-action, since $x \mapsto 1/x$ interchanges the origin on E_λ with a point of order 2.)

α	β	$T_{50}(\alpha,\beta)$	orders
$\frac{7+5\sqrt{-7}}{14}$	$\frac{7-11\sqrt{-7}}{14}$	$\{\frac{7-11\sqrt{-7}}{14}, \frac{21+31\sqrt{-7}}{42}, \frac{49-13\sqrt{-7}}{98}\}$	$(6,2),(8,8),(6,6)$
$1+\sqrt{2}$	$-1+\sqrt{2}$	$\{-1, 7-4\sqrt{2} \pm (4-2\sqrt{2})\sqrt{2-\sqrt{2}}\}$	$(4,4),(5,10),(5,10)$
$\frac{5+3\sqrt{-15}}{10}$	$\frac{15-7\sqrt{-15}}{30}$	$\{\frac{5-13\sqrt{-15}}{10}, \frac{45+11\sqrt{-15}}{90}, \frac{75+61\sqrt{-15}}{150}\}$	$(6,3),(4,6),(12,6)$
$\frac{15+7\sqrt{-15}}{30}$	$\frac{45-11\sqrt{-15}}{90}$	$\{\frac{27+19\sqrt{-15}}{54}, \frac{45-11\sqrt{-15}}{90}, \frac{75-61\sqrt{-15}}{150}\}$	$(5,5),(6,2),(6,3)$
$\frac{1+\sqrt{17}}{2}$	$\frac{-7+\sqrt{17}}{2}$	$\{\frac{-7+\sqrt{17}}{2}, \frac{33-7\sqrt{17}}{2}, \frac{-31-7\sqrt{17}}{2}\}$	$(4,2),(3,4),(3,6)$
$\frac{-7+\sqrt{17}}{2}$	$\frac{33-7\sqrt{17}}{2}$	$\{\frac{33-7\sqrt{17}}{2}, \frac{-895+217\sqrt{17}}{2}, \frac{3+11\sqrt{17}}{6}\}$	$(4,2),(6,4),(10,10)$

There are nine examples over quartic fields, one each over $\mathbb{Q}(\sqrt{2},\sqrt{3})$ (orders $((4,4),(6,3),(10,5))$), $\mathbb{Q}(\sqrt{-3},\sqrt{13})$ (orders $(4,6),(6,4),(10,10)$), a dihedral field containing $\mathbb{Q}(\sqrt{2})$ (orders $(4,8),(8,4),(10,10)$), one containing $\mathbb{Q}(\sqrt{5})$ (orders $(4,4),(6,7),(6,7)$), one containing $\mathbb{Q}(\sqrt{-7})$ (orders $(4,2),(6,6),(7,7)$), one containing $\mathbb{Q}(\sqrt{17})$ (orders $(3,4),(4,6),(5,10)$) and one containing $\mathbb{Q}(\sqrt{33})$ (orders $(3,6),(6,4),(9,6)$). Another dihedral field containing $\mathbb{Q}(\sqrt{17})$ shows up twice, with orders $(2,6),(4,6),(7,7)$ and $(4,6),(5,5),(7,7)$.

There are two examples over fields of degree six, one over $\mathbb{Q}(\zeta_7)$ with orders $(7,7),(8,8),(9,9)$, and one over a quadratic extension of the cubic field of discriminant -31 (orders $(3,6),(6,6),(7,7)$). In addition, there is one example over the octic field $\mathbb{Q}(\zeta_{15})$ (orders $(8,4),(8,8),(6,10)$), one over another octic field that is Galois over $\mathbb{Q}$ and a quadratic extension of $\mathbb{Q}(\sqrt{-1},\sqrt{5})$ (orders $(4,4),(7,7),(7,7)$), and one example over a field of degree 16 (orders $(6,6),(10,10),(10,10)$).

Then there are two further orbits that have $\#T_{50} = 4$. One is represented by

$$\{\alpha,\beta\} = \left\{\frac{-7+\sqrt{17}}{2}, \frac{9+\sqrt{17}}{2}\right\} \qquad \text{with}$$
$$T_{50}(\alpha,\beta) = \left\{\frac{-31-7\sqrt{17}}{2}, \frac{33-7\sqrt{17}}{2}, \frac{17-23\sqrt{17}}{34}, \frac{3+11\sqrt{17}}{6}\right\}.$$

The pairs of orders of the points are $(6,4),(4,6),(6,6),(10,10)$. The other example is over the (sextic) Hilbert class field of $\mathbb{Q}(\sqrt{-23})$ and has orders $(3,6)$, $(6,6)$, $(7,7)$ and $(14,14)$.

Finally, we have

$$\{\alpha,\beta\} = \{\sqrt{-1},-\sqrt{-1}\} \qquad \text{with} \qquad T_{100}(\alpha,\beta) = \left\{-1, 3\pm 2\sqrt{2}, \frac{1\pm 2\sqrt{-2}}{3}\right\}$$

of size 5. The pairs of orders of the points are here $(4,4),(6,6),(6,6),(10,10),(10,10)$. All the number fields occurring here have trivial class group, except for $\mathbb{Q}(\sqrt{-15})$ and $\mathbb{Q}(\sqrt{-3},\sqrt{13})$, which both have class number 2.

Note that for any given bicyclotomic polynomial $B(\lambda, x)$, we can take the factors of $B(\lambda, \alpha)$ as a polynomial in λ over $\mathbb{Q}(\alpha)$ and for each factor f consider a root λ_0 of f and check if the points on E_{λ_0} with x-coordinate β have finite order or not (for example by considering the reductions modulo suitable prime ideals of small degree; note that a point of finite order reduces to a point of the same finite order modulo all odd primes of good reduction, so if we find two different orders in this way, we know that the point must have infinite order). In this way, we checked that for any $\lambda \in T(\sqrt{-1}, -\sqrt{-1})$ not in the list above, the orders of both pairs of points on E_λ must be larger than 200. We also found that all $B(\lambda, \sqrt{-1})$ of orders up to 200 are irreducible over $\mathbb{Q}(\sqrt{-1})$, with one exception at order 10. In addition, we checked for each of the other 23 orbits of points with $\#T_{50} \geq 3$ that for any unknown $\lambda \in T(\alpha, \beta)$ both points $P_\alpha(\lambda)$ and $P_\beta(\lambda)$ must have order > 100. This suggests the following conjecture.

Conjecture 24.

(1) $T(\sqrt{-1}, -\sqrt{-1}) = \{-1, 3 \pm 2\sqrt{2}, \frac{1}{3} \pm \frac{2}{3}\sqrt{-2}\}$.
(2) All other sets $T(\alpha, \beta)$ have at most four elements.

We also remark that in our computations, we never found more than two branches through any singular point of an irreducible component of $\mathcal{C}$. So we propose:

Conjecture 25. There is a number N such that for any irreducible component C of $\mathcal{C}$ and any (singular) point P on C outside the 'bad set' given by $a(a-1)b(b-1)(a-b) = 0$, there are at most N branches of C through P (equivalently, P has at most N preimages in the component Z of $\mathcal{Z}$ that maps birationally to C).

Our computations suggest that perhaps one can even take $N = 2$. Note that it would follow that every $\lambda \in T(\alpha, \beta)$ has the property that $[\mathbb{Q}(\alpha, \beta, \lambda) : \mathbb{Q}(\alpha, \beta)] \leq N$. This implies that Conjecture 25 with an explicit N would give an *effective* procedure for determining $T(\alpha, \beta)$ for algebraic α and β. Namely, we can find an explicit bound for the height of the elements of $T(\alpha)$, say (see [Sil83]); together with the bound on the degree, this leaves finitely many candidates for λ, which we can check for membership in $T(\alpha, \beta)$.

Our computations also suggest the following further conjecture.

Conjecture 26. Fix $d \geq 1$. Then there are only finitely many $\alpha, \beta \in \bar{\mathbb{Q}}$, both of degree at most d, with $\alpha, \beta \notin \{0, 1\}$, $\alpha \neq \beta$ and $\#T(\alpha, \beta) \geq 2$.

For example, it appears that other than the orbit mentioned above with $\#T(\alpha, \beta) \geq 3$, there might be only six further orbits (each of size 12) of pairs of rational numbers α and β with $\#T(\alpha, \beta) \geq 2$, represented by $(-3, 3)$, $(-5/4, 5/2)$, $(-4/5, 8/5)$, $(-3, 9)$, $(-9/16, 9/4)$ and $(-27/5, -3/5)$. Note that for the first two of these, one can deduce that in fact $\#T(\alpha, \beta) = 2$ via Corollary 8.

Conjecture 26 would follow from the following:

Conjecture 27. There is an absolute bound B such that for all $\alpha, \beta \in \bar{\mathbb{Q}} \setminus \{0, 1\}$ with $\alpha \neq \beta$ and $\#T(\alpha, \beta) \geq 2$, we have $h(\alpha), h(\beta) \leq B$.

degree	$[0,1)$	$[1,2)$	$[2,3)$	$[3,4)$	$[4,5)$	$[5,6)$	$[6,\infty)$
1	0	0	1	3	0	2	0
2	7	13	16	19	12	5	2
3	6	15	37	17	5	1	0
4	21	44	78	34	23	2	4
5	13	37	47	19	3	1	0
6	28	68	125	44	7	7	0
7	0	30	58	20	3	0	0
8	10	104	105	40	11	3	0
9	2	52	64	22	3	0	0
10	13	92	113	48	5	2	0
11	3	51	66	15	1	1	0
12	14	94	137	41	10	7	0
13	1	59	55	9	5	0	0
total	118	659	902	331	88	31	6

TABLE 2. Distribution of heights of schemes with $\#T \geq 2$

Here $h\colon \bar{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ denotes the absolute logarithmic height.

We set $\bar{h}(\alpha) = \big(h(\alpha) + h(1-\alpha) + h(1-1/\alpha)\big)/3$; then $\bar{h}$ is invariant under the S_3-action on $\mathbb{P}^1(\bar{\mathbb{Q}})$. Note that

$$\bar{h}(\alpha) - \frac{2}{3}\log 2 \leq h(\alpha) \leq \bar{h}(\alpha) + \frac{1}{3}\log 2$$

(with equality on the left for $\alpha = -1$ and on the right for $\alpha \in \{2, \frac{1}{2}\}$), so that we could formulate an equivalent conjecture using $\bar{h}$ instead of h. To test Conjecture 27, we computed $\bar{h}(\alpha) + \bar{h}(\beta)$ for a representative point (α, β) in each Γ-orbit of points of degree at most 13 that we encountered in our computation. This gave rise to the statistics in Table 2, where we give the distribution of these height sums according to intervals of length 1 for the orbits of given degree (excluding those with $\#T(\alpha,\beta) \geq 3$).

The largest height sum encountered was ≈ 6.723796, occurring for degree 4. There is no tendency towards a systematic increase of these heights with increasing degree of the points or with increasing degree of the curves that were intersected. This lends some credibility to Conjecture 27.

REFERENCES

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). ↑1

[HJM15] P. Habegger, G. Jones, and D. Masser, *Six unlikely intersection problems in search of effectivity*, September 22, 2015. arXiv:1509.06573v1 [math.NT]. ↑4

[dMWY14] Laura de Marco, Xiaoguang Wang, and Hexi Ye, *Torsion points and the Lattès family*, October 28, 2014. arXiv:1311.1792v3 [math.DS]; to appear in Amer. J. Math. ↑1

[MZ08] David Masser and Umberto Zannier, *Torsion anomalous points and families of elliptic curves*, C. R. Math. Acad. Sci. Paris **346** (2008), no. 9-10, 491–494, DOI 10.1016/j.crma.2008.03.024 (English, with English and French summaries). ↑1

[MZ10] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), no. 6, 1677–1691. ↑1

[MZ12] ———, *Torsion points on families of squares of elliptic curves*, Math. Ann. **352** (2012), no. 2, 453–484, DOI 10.1007/s00208-011-0645-4. ↑1

[MZ13] David Masser and Umberto Zannier, *Bicyclotomic polynomials and impossible intersections*, J. Théor. Nombres Bordeaux **25** (2013), no. 3, 635–659 (English, with English and French summaries). ↑1, 3, 3, 6, 6, 6

[MZ14] D. Masser and U. Zannier, *Torsion points on families of products of elliptic curves*, Adv. Math. **259** (2014), 116–133, DOI 10.1016/j.aim.2014.03.016. ↑1

[MZ] ———, *Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings*. (with Appendix by V. Flynn), Preprint. ↑1

[Mav15] Niki Myrto Mavraki, *Impossible intersections in a Weierstrass family of elliptic curves*, July 25, 2015. arXiv:1507.07047 [math.NT]. ↑3, 5

[Sil83] Joseph H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211, DOI 10.1515/crll.1983.342.197. ↑7

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. ↑6

[Stoa] Michael Stoll, *List of all components of $\mathcal{C}$ of total degree at most 192*. http://www.mathe2.uni-bayreuth.de/stoll/simultaneous-torsion/allcurves.magma. ↑6

[Stob] ———, *List of all pairs (α, β) found with $\#T_{50}(\alpha, \beta) = 2$*. http://www.mathe2.uni-bayreuth.de/stoll/simultaneous-torsion/twolambdas-sizes.magma. ↑7

[Stoc] ———, *List of all pairs (α, β) found with $\#T_{50}(\alpha, \beta) \geq 3$*. http://www.mathe2.uni-bayreuth.de/stoll/simultaneous-torsion/atleast3-all.magma. ↑7

[Zan12] Umberto Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Mathematics Studies, vol. 181, Princeton University Press, Princeton, NJ, 2012. With appendixes by David Masser. ↑1

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: Michael.Stoll@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/stoll/