ELLIPTIC CURVES WITH COMMON TORSION x-COORDINATES AND HYPERELLIPTIC TORSION PACKETS

HANG FU AND MICHAEL STOLL

ABSTRACT. We establish a connection between torsion packets on curves of genus 2 and pairs of elliptic curves realized as double covers of the projective line $\mathbb{P}^1_x$ that have many common torsion x-coordinates. This can be used to show that the set of common torsion x-coordinates has size at least 22 infinitely often and has 34 elements in some cases. We also explain how we obtained the current record example of a hyperelliptic torsion packet on a genus 2 curve.

1 Introduction

Let E_1 and E_2 be elliptic curves over $\mathbb{C}$, together with double covers $\pi_1\colon E_1 \to \mathbb{P}^1$ and $\pi_2\colon E_2 \to \mathbb{P}^1$ such that the origin of E_j is a ramification point of π_j. It is known (as a consequence of Raynaud's [Ray83] proof of the Manin-Mumford Conjecture; see for example [BT07, Thm. 4.2]) that when $\pi_1(E_1[2]) \neq \pi_2(E_2[2])$, then the intersection

$$I(\pi_1, \pi_2) = \pi_1(E_{1,\mathrm{tors}}) \cap \pi_2(E_{2,\mathrm{tors}})$$

is finite, where $E_{j,\mathrm{tors}}$ denotes the set of torsion points on E_j. One can then ask how large this intersection can be, possibly depending on the size of $\pi(E_1[2]) \cap \pi_2(E_2[2])$. In [BFT18, Conjs. 2 and 12] (see also [BF16, Conj. 1.2]), it is conjectured that there should be a uniform bound for the size of $I(\pi_1, \pi_2)$ whenever it is finite. The recent paper [DKY20] by DeMarco, Krieger, and Ye establishes the existence of such a uniform bound in the case that $\#\bigl(\pi_1(E_1[2]) \cap \pi_2(E_2[2])\bigr) = 3$. The very recent results by Dimitrov, Gao, Ge, Habegger, and Kühne [DGH21, Küh21, Gao21, GGK21] on uniformity in the Mordell-Lang conjecture for subvarieties of abelian varieties (see also below) now imply the existence of a uniform bound for $\#I(\pi_1, \pi_2)$ as conjectured. This follows by applying their result to the families of curves in $E_1 \times E_2$ obtained as the pull-back of the diagonal in $\mathbb{P}^1 \times \mathbb{P}^1$ under (π_1, π_2). The bounds are (so far) not explicit, and so it is an interesting question how large they have to be.

An at first sight somewhat different question is how large a torsion packet on a curve of genus 2 over $\mathbb{C}$ can be. Recall that a *torsion packet* on a curve C of genus at least 2 is a maximal set of points on C such that the (linear equivalence class of the) difference of any two points in the set is a point of finite order on the Jacobian of C. Again by [Ray83], such a torsion packet is always finite, and one can ask for a bound on its size that depends only on the genus g [Maz86, top of page 234]. In [Poo00] it is shown that there are infinitely many

Date: August 18, 2021.
2020 *Mathematics Subject Classification.* 11G05, 11G30, 14H40, 14H45, 14H52.
Key words and phrases. Elliptic curves, Torsion points, Hyperelliptic curves, Torsion packets.

essentially distinct curves of genus 2 with a *hyperelliptic* torsion packet (i.e., containing the Weierstrass points) of size at least 22. Within the family giving rise to these examples, there is (at least) one with a torsion packet of size 34; see [Sto] and Section 4 below. Using the fact that in the case $\#\big(\pi_1(E_1[2]) \cap \pi_2(E_2[2])\big) = 3$, the (desingularization of the) pull-back of the diagonal in $\mathbb{P}^1 \times \mathbb{P}^1$ under (π_1, π_2) is a bielliptic curve of genus 2, DeMarco, Krieger, and Ye deduce the existence of a uniform bound on the size of hyperelliptic torsion packets on bielliptic curves of genus 2, and the work of Dimitrov, Gao, Ge, Habegger, and Kühne already mentioned above now establishes the existence of a bound that depends only on g, as expected (and much more).

In this article, we use the connection between bielliptic genus 2 curves and pairs (π_1, π_2) such that $\#\big(\pi_1(E_1[2]) \cap \pi_2(E_2[2])\big) = 3$ that was already mentioned above, together with a new observation that relates pairs (π_1, π_2) with differing sizes of $\pi_1(E_1[2]) \cap \pi_2(E_2[2])$ to establish a close relation between the largest size of an intersection $I(\pi_1, \pi_2)$ and the largest size of a hyperelliptic torsion packet on a bielliptic genus 2 curve. Specifically, we show the following (see Corollary 8).

Theorem 1. *The maximal size of a finite intersection $I(\pi_1, \pi_2)$ is at least as large as the maximal size of a hyperelliptic torsion packet on a bielliptic genus 2 curve.*

This follows from an explicit correspondence between bielliptic genus 2 curves and pairs (π_1, π_2). Under this correspondence, the family of genus 2 curves studied in [Poo00] is related to a family of pairs of elliptic curves with certain properties. As a consequence, we obtain the following result, which proves Conjecture 23 in [BFT18].

Theorem 2. *There are infinitely many essentially distinct pairs (π_1, π_2) as above such that $\#I(\pi_1, \pi_2) \geq 22$.*

Applying the correspondence to our example of a torsion packet of size 34, we obtain the following new record for the size of $I(\pi_1, \pi_2)$.

Theorem 3. *Let $s \in \mathbb{C}$ satisfy $s^8 + 174s^4 + 81 = 0$. Consider*

$$E_1 \colon y^2 = (x^2 - s^2)(x^2 - (1/s)^2) \qquad \text{and} \qquad E_2 \colon y^2 = (x^2 - (s/3)^2)(x^2 - (3/s)^2)\,.$$

We take π_1 and π_2 to be the x-coordinate map (and fix the origins of E_1 and E_2 to be $(s, 0)$ and $(s/3, 0)$, respectively). Then

$$I(\pi_1, \pi_2) = \pi_1(E_1[48]) \cap \pi_2(E_2[48])$$

and $\#I(\pi_1, \pi_2) = 34$.

Note that except for the fact that all the torsion points with common x-coordinate have order dividing 48, the statement can be easily checked by a computation, which shows in particular that $\#I(\pi_1, \pi_2) \geq 34$.

The structure of this paper is as follows. In Section 2, we define a pair $P(\pi_1, \pi_2)$ of numerical invariants of (π_1, π_2) and set up a correspondence between pairs (π_1, π_2) and (π_1', π_2') whose invariants are related in a certain way. This implies a relation between $\#I(\pi_1, \pi_2)$ and $\#I(\pi_1', \pi_2')$. In Section 3, we explain the connection between pairs (π_1, π_2) such that $\#\big(\pi_1(E_1[2]) \cap \pi_2(E_2[2])\big) = 3$ and bielliptic curves of genus 2. This connection, together

with the correspondence from Section 2 then implies Theorems 1, 2 and 3. In Section 4, we explain how the example [Sto] of a large hyperelliptic torsion packet was obtained. Finally, in Section 5, we give more details on the pairs (π_1, π_2) with $\pi_1(E_1[2]) \cap \pi_2(E_2[2]) = \emptyset$ that correspond to the curves in the family considered by Poonen in [Poo00]. We show in particular that the curves E_1 and E_2 that appear in Theorem 2 are isogenous, which is unnecessary for the proof, but gives a hint of why we are able to get many common torsion x-coordinates in this way.

All geometric objects in this paper will be over the complex numbers unless explicitly stated otherwise.

Acknowledgments

The first named author would like to thank Laura DeMarco for her valuable comments to the first version of this article. The authors would like to thank Yuri Bilu for connecting us with each other.

2 Relations among various pairs (π_1, π_2)

Let $\pi\colon E \to \mathbb{P}^1$ be a double cover such that E is an elliptic curve and the origin of E is a ramification point of π. We note that the set $\pi(E_{\text{tors}})$ does not depend on which of the four ramification points we choose as the origin, since the difference of any two is a point of order 2. Given π as above, the action of $E[2]$ on E by translation induces an action on $\mathbb{P}^1$. We denote the isomorphic copy of the Klein Four Group inside $\mathrm{PGL}(2)$ that is the image of $E[2]$ by $G(\pi)$.

Given two double covers π_1, π_2 as above, we can then classify them according to the sizes of $\pi_1(E_1[2]) \cap \pi_2(E_2[2])$ and of $G(\pi_1) \cap G(\pi_2)$. Note that the first set is a union of orbits under the second group, on which the group acts without fixed points. If $\pi_1(E_1[2]) = \pi_2(E_2[2])$, then E_1 and E_2 are isomorphic (up to the choice of origin on the elliptic curves) and $I(\pi_1, \pi_2) = \pi_1(E_{1,\text{tors}}) = \pi_2(E_{2,\text{tors}})$ is infinite. Excluding this case, the possibilities for the pair

$$P(\pi_1, \pi_2) = \big(\#(\pi_1(E_1[2]) \cap \pi_2(E_2[2])), \#(G(\pi_1) \cap G(\pi_2))\big)$$

are

$$(3,1), \quad (2,1), \quad (1,1), \quad (0,1); \quad (2,2), \quad (0,2); \quad (0,4)\,.$$

We will now relate pairs with different invariants.

Proposition 4. *Let $\pi_1\colon E_1 \to \mathbb{P}^1$ and $\pi_2\colon E_2 \to \mathbb{P}^1$ be two double covers as above and fix a non-trivial element $\alpha \in G(\pi_1) \cap G(\pi_2)$ (in particular, we assume that $G(\pi_1) \cap G(\pi_2)$ is non-trivial). For $j \in \{1,2\}$, we denote by $T_j \in E_j[2]$ the point such that $\pi_j(P + T_j) = \alpha(\pi_j(P))$, and we write $E_j' = E_j/\langle T_j \rangle$. Then there are double covers $\pi_j'\colon E_j' \to \mathbb{P}^1$ and a morphism $\beta\colon \mathbb{P}^1 \to \mathbb{P}^1$ of degree 2 such that*

$$\#\big(\pi_1(E_1[2]) \cap \pi_2(E_2[2])\big) = 2\#\big(\pi_1'(E_1'[2]) \cap \pi_2'(E_2'[2])\big) - 4$$

and

$$I(\pi_1, \pi_2) = \beta^{-1}\big(I(\pi_1', \pi_2')\big)\,.$$

In particular, $\#I(\pi_1, \pi_2) = 2\#I(\pi_1', \pi_2') - 2$.

Conversely, given $\pi_1' \colon E_1' \to \mathbb{P}^1$ and $\pi_2' \colon E_2' \to \mathbb{P}^1$ such that $\#\big(\pi_1'(E_1'[2]) \cap \pi_2'(E_2'[2])\big) \geq 2$, there are double covers $\pi_1 \colon E_1 \to \mathbb{P}^1$ and $\pi_2 \colon E_2 \to \mathbb{P}^1$ and $\mathrm{id} \neq \alpha \in G(\pi_1) \cap G(\pi_2)$ such that (π_1', π_2') is obtained from (π_1, π_2) and α in the way described above.

Proof. First consider one double cover $\pi \colon E \to \mathbb{P}^1$. Up to post-composing with an automorphism of $\mathbb{P}^1$, we can assume that one element of $G(\pi)$ is $x \mapsto -x$; then E has the form

$$E \colon y^2 = (x^2 - s)(x^2 - t)$$

(up to scaling y) with $s \neq t$ and s, t nonzero. Let $T \in E[2]$ be the point such that translation by T on E is given by $(x, y) \mapsto (-x, -y)$. Then the isogeny $\phi \colon E \to E' = E/\langle T \rangle$ is

$$(x, y) \mapsto (x^2, xy)\,, \qquad \text{with} \qquad E' \colon y^2 = x(x - s)(x - t)\,.$$

Since ϕ is an isogeny, it follows that

$$\pi(E_{\mathrm{tors}}) = \{\xi \in \mathbb{P}^1 : \xi^2 \in \pi'(E'_{\mathrm{tors}})\}\,,$$

where $\pi' \colon E' \to \mathbb{P}^1$ is the x-coordinate map. Also note that $\{0, \infty\} \subset \pi'(E'[2])$.

Given π_1, π_2 and α as in the statement, we can again assume that $\alpha(x) = -x$, so that the curves E_1 and E_2 have the form $E_j \colon y^2 = (x^2 - s_j)(x^2 - t_j)$. Let E_1' and E_2' be as in the statement; by the above, we can take $E_j' \colon y^2 = x(x - s_j)(x - t_j)$, and we let π_j' denote the x-coordinate map. The first claim follows (with $\beta \colon x \mapsto x^2$).

Since both ramification points 0 and ∞ of the squaring map are in $I(\pi_1', \pi_2')$, the claim on the sizes of the sets also follows.

For the converse statement, we can assume that $E_j' \colon y^2 = x(x - s_j)(x - t_j)$ by moving two of the common ramification points to 0 and ∞. Then it is clear that the construction can be reversed. □

For (π_1, π_2) and (π_1', π_2') as in Proposition 4, we have that

$$P(\pi_1, \pi_2) = (2a, 2b) \qquad \text{and} \qquad P(\pi_1', \pi_2') = (a + 2, b)$$

for some $(a, b) \in \{(0, 1), (0, 2), (1, 1)\}$.

We write $T(a, b)$ for the maximum of $\#I(\pi_1, \pi_2)$ over all pairs (π_1, π_2) of double covers such that $P(\pi_1, \pi_2) = (a, b)$. By the uniform boundedness results mentioned in the introduction, this makes sense. We then have the following relations.

Corollary 5.

$$T(0, 4) = 2T(2, 2) - 2 = 4T(3, 1) - 6 \qquad \textit{and} \qquad T(0, 2) = 2T(2, 1) - 2\,.$$

This suggests that the maximal size of $\#I(\pi_1, \pi_2)$ is obtained when $P(\pi_1, \pi_2) = (0, 4)$.

3 Relation with genus 2 torsion packets

Let C be a curve of genus $g \geq 2$. Recall that a *torsion packet* on C is a maximal subset $T \subset C$ such that the difference of any two points in T, considered as a point on the Jacobian variety J of C, has finite order. Raynaud [Ray83] proved that a torsion packet is always finite (this was the statement of the Manin-Mumford conjecture); a nice and short proof, based on a deep result of Serre, can be found in [BR03]. When C is a hyperelliptic curve, then its *hyperelliptic torsion packet* is the torsion packet that contains the ramification points of the hyperelliptic double cover $C \to \mathbb{P}^1$. We now assume that C has genus 2 (and is therefore in particular hyperelliptic). The curve C is *bielliptic* if there is a double cover $\psi\colon C \to E$ with E an elliptic curve. This is equivalent to the existence of an "extra involution" α in $\mathrm{Aut}(C)$, i.e., an involution distinct from the hyperelliptic involution ι, which is the involution associated to the hyperelliptic double cover $C \to \mathbb{P}^1$. Then $E = C/\langle\alpha\rangle$, and there is another double cover $\psi'\colon C \to C/\langle\alpha\iota\rangle = E'$, where E' is also an elliptic curve. The involution α induces an involution of $\mathbb{P}^1$ (since ι is central in the automorphism group of C), which we can take to be $x \mapsto -x$. In this case, C can be given by an equation of the form

$$C\colon y^2 = (x^2 - u)(x^2 - v)(x^2 - w)$$

with u, v, w distinct and nonzero, with $\alpha(x, y) = (-x, y)$. Then we have

$$\begin{aligned} E\colon y^2 &= (x-u)(x-v)(x-w) && \text{with} \quad \psi(x,y) = (x^2, y)\,, \\ E'\colon y^2 &= x(x-u)(x-v)(x-w) && \text{with} \quad \psi'(x,y) = (x^2, xy)\,. \end{aligned}$$

There is an obvious birational morphism induced by ψ and ψ',

$$C \to \{(x, y, y') : (x, y) \in E, (x, y') \in E'\} = E \times_{\mathbb{P}^1} E'\,,$$

where the morphisms $\pi\colon E \to \mathbb{P}^1$, $\pi'\colon E' \to \mathbb{P}^1$ in the fibered product are the x-coordinate maps. We see that $P(\pi, \pi') = (3, 1)$. (The morphism $C \to E \times_{\mathbb{P}^1} E'$ is injective outside the ramification points of the hyperelliptic double cover, which are identified in pairs.)

Proposition 6. *In the situation described above, let $\rho\colon C \to \mathbb{P}^1$ be the natural map obtained via $C \to E \times_{\mathbb{P}^1} E' \to \mathbb{P}^1$. Then the hyperelliptic torsion packet of C is the full preimage under ρ of $I(\pi, \pi')$. In particular, its size is*

$$4\#I(\pi, \pi') - 6 - 2\#\big(I(\pi, \pi') \cap \{0, \infty\}\big)\,.$$

Proof. Under the map $\psi \times \psi'\colon C \to E \times E'$, the fixed points of ι on C are mapped to 2-torsion points on $E \times E'$. The map $C \to E \times E'$ induces an isogeny $J \to E \times E'$ such that the following diagram commutes, where the map on the lower left is the diagonal inclusion.

$$\begin{array}{ccccc} C & & \longrightarrow & & J \\ {\scriptstyle\rho}\downarrow & & \overset{\psi\times\psi'}{\searrow} & & \downarrow \\ \mathbb{P}^1 & \xrightarrow[\text{diag}]{} & \mathbb{P}^1 \times \mathbb{P}^1 & \xleftarrow[(\pi,\pi')]{} & E \times E' \end{array}$$

Here the embedding of C into J is $P \mapsto [P - W]$, where W is a fixed ramification point, and we take the origin on $E \times E'$ to be the image of W.

If P is a point in the hyperelliptic torsion packet, then $[P - W]$ is torsion in J. This implies that $(\psi(P), \psi'(P))$ is torsion on $E \times E'$, so that $\rho(P) \in I(\pi, \pi')$.

Conversely, consider $\xi \in I(\pi, \pi')$. Then there are torsion points $P \in E$ and $P' \in E'$ such that $\pi(P) = \pi'(P') = \xi$. Let $Q \in C$ be a point with $\rho(Q) = \xi$. Then $(\psi(Q), \psi'(Q)) = (\pm P, \pm P')$, and so $(\psi(Q), \psi'(Q))$ is torsion. But then $[Q - W] \in J$ must be torsion as well, since its image under the isogeny $J \to E \times E'$ is torsion. So Q is in the hyperelliptic torsion packet of C.

For the last statement, note that ρ (which is $(x, y) \mapsto x^2$) has degree 4 and ramifies

(1) at the four points on C with $x = 0$ or $x = \infty$, and
(2) at the six ramification points of the hyperelliptic double cover, which map two-to-one onto $\pi(E[2]) \cap \pi'(E'[2])$. □

We can reverse this construction.

Proposition 7. *Let $\pi\colon E \to \mathbb{P}^1$ and $\pi'\colon E' \to \mathbb{P}^1$ be double covers such that $P(\pi, \pi') = (3, 1)$. Then there is a bielliptic genus 2 curve C such that C, E and E' fit into a diagram as in the proof of Proposition 6.*

Proof. By moving the fourth branch point of π to ∞ and the fourth branch point of π' to 0, we can assume that E and E' are as above, with π and π' the x-coordinate maps, i.e.,

$$E\colon y^2 = (x-u)(x-v)(x-w) \qquad \text{and} \qquad E'\colon y^2 = x(x-u)(x-v)(x-w)\,.$$

Then

$$C\colon y^2 = (x^2-u)(x^2-v)(x^2-w)$$

is the required curve. □

We denote by T the maximal size of a hyperelliptic torsion packet on a bielliptic curve of genus 2.

As mentioned in the introduction, the correspondence established in Propositions 6 and 7 is used by DeMarco, Krieger, and Ye [DKY20, §9] to deduce a bound on T from a bound B on $\#I(\pi_1, \pi_2)$ when $P(\pi_1, \pi_2) = (3, 1)$. Their bound is $T \leq 16B$; we can improve this as follows.

Corollary 8.

$$4T(3,1) - 6 \geq T \qquad \textit{and therefore} \qquad T(0,4) \geq T \geq 34\,.$$

Proof. The first statement follows from the previous two propositions. The first inequality in the second statement then follows by Corollary 5, and the last inequality comes from the example of Theorem 11. □

Proof of Theorems 2 and 3. By the main result of [Poo00], there are infinitely many (pairwise non-isomorphic) bielliptic genus 2 curves with a hyperelliptic torsion packet of size at least 22. Theorem 11 gives an example in this family with a hyperelliptic torsion packet of size 34. By Proposition 6 and the construction in the proof of Proposition 4 (applied twice backwards), we obtain corresponding pairs (π_1, π_2). □

4 Torsion packets on curves of genus 2

In this section, we explain how we found the example [Sto] of a hyperelliptic torsion packet of size 34 on a curve of genus 2. The approach is based on Poonen's result in [Poo00], where he shows that there are infinitely many essentially distinct curves of genus 2 with hyperelliptic torsion packets of size at least 22. We first give a rough sketch of the idea behind Poonen's result.

One important fact is that the hyperelliptic torsion packet of a hyperelliptic curve C is invariant under the automorphism group of C. This is because the automorphism group fixes the set of ramification points of the hyperelliptic double cover and the difference of any two ramification points is a torsion point (of order dividing 2). This implies that the points in the hyperelliptic torsion packet come in orbits under the automorphism group.

Now consider the moduli space of curves of genus 2. It has dimension 3. We can (in principle) write down the condition that some torsion point of given order n is in the image of the curve (we fix one of the ramification points as the base point of the embedding of the curve into its Jacobian); this gives a codimension-1 condition: we want to force one of finitely many points on the Jacobian of dimension 2 to lie on a subvariety of dimension 1 and hence also codimension 1. So we can expect to find curves with a hyperelliptic torsion packet of size at least $6 + 3 \cdot 2 = 12$, where the first summand counts the ramification points, which are always in the hyperelliptic torsion packet, and the second comes from the idea that we can impose three independent torsion points onto the curve, each giving us another one for free, since the hyperelliptic involution is a nontrivial automorphism. Barring accidents (or "unlikely intersections"), we would not expect more than that. Such accidents do indeed occur, as the following example shows.

Example 9. The curve

$$C\colon y^2 = 4x^6 - 12x^5 - 3x^4 + 46x^3 - 15x^2 - 24x + 40$$

has minimal (geometric) automorphism group and a hyperelliptic torsion packet of size 18 (which is larger by 6 than the number we expect to find infinitely often).

The first statement can be checked by looking at the invariants of C; for the second we can use Poonen's program for computing torsion packets described in [Poo01].

We can try to do better than what we can expect in the generic case by considering subfamilies of genus 2 curves that have a larger automorphism group. This gives us more points "for free" for any torsion point we get on the curve. On the other hand, the corresponding moduli spaces have smaller dimension, so we cannot force as many orbits of torsion points on the curve as in the generic case. These considerations lead to the following table, which lists the relevant data for each possible automorphism group. We describe it by specifying the reduced automorphism group $\mathrm{Aut}(C)/\langle\iota\rangle$, which is a group of automorphisms of $\mathbb{P}^1$.

f	$\mathrm{Aut}(C)/\langle\iota\rangle$	$\#\mathrm{Aut}(C)$	$\dim M$	$\#T_{\min}$	$\#T$
generic	$\{\mathrm{id}\}$	2	3	6	$12+2\delta$
$x^6+sx^4+tx^2+1$	C_2	4	2	6	$14+4\delta$
x^5+tx^3+x	$C_2\times C_2$	8	1	6	$14+8\delta$
x^6+tx^3+1	S_3	12	1	10	$\mathbf{22}+12\delta$
x^6+1	D_6	24	0	10	10
x^5+x	S_4	48	0	22	**22**
x^5+1	C_5	10	0	18	18

The curve can be given by an equation of the form $y^2=f(x)$. $\dim M$ is the dimension of the moduli space of curves admitting (at least) the given automorphism group, $\#T_{\min}$ is the size of the generic hyperelliptic torsion packet in the family, and

$$\#T=\#T_{\min}+(\dim M+\delta)\cdot\#\mathrm{Aut}(C)$$

is the size we can expect after forcing $\dim M$ orbits of torsion points; δ counts the number of additional full orbits we may be able to obtain (δ can be non-integral when there are nontrivial stabilizers).

The second line, with reduced automorphism group C_2, corresponds to the bielliptic curves that feature in Section 3. We can have $\delta>0$ in this case, too.

Example 10. The curve

$$C\colon y^2=(-9\sqrt{3}+16)x^6+(-63\sqrt{3}+113)x^4+(13\sqrt{3}-38)x^2+3\sqrt{3}+9$$

has $\mathrm{Aut}(C)\cong C_2\times C_2$ (and so is generic bielliptic) and a hyperelliptic torsion packet of size at least 18.

The claim on $\mathrm{Aut}(C)$ can be shown in a similar way as for the preceding example. The torsion packet contains the six ramification points and the points with x-coordinates $\pm\sqrt{3}$, $\pm\sqrt{3}/3$, and $\pm(\sqrt{3}+2)$. We cannot use Poonen's program for this curve, since it requires the curve to be defined over $\mathbb{Q}$.

The last three lines in the table correspond to a single point each in the moduli space of curves of genus 2. The most interesting case is the family with reduced automorphism group S_3, which has one parameter and has the additional benefit that there are four additional torsion points on the curve throughout the family: the points at infinity and the points with x-coordinate zero give points of order dividing 6 (they form an orbit of size 4). So we get 10 points as our baseline, and we should be able to force one full orbit of size 12 of torsion points on the curve in addition. This is precisely what Poonen proves.

Note that the curves in this family are also bielliptic (an extra involution is given by $(x,y)\mapsto(1/x,y/x^3)$). So we can use the correspondence between torsion packets and sets $I(\pi_1,\pi_2)$ that is described in Section 3. What we do is essentially the following. For each $n\geq 3$ up to some bound, we compute the n-division polynomials $h_{1,n}(t,x)$ and $h_{2,n}(t,x)$

of the two elliptic curves (which depend on the parameter t). Then we compute the resultants $R_{m,n}(t) = \mathrm{Res}_x\big(h_{1,m}(t,x), h_{2,n}(t,x)\big)$, which are rational functions (in fact, polynomials) in t. A root $t \neq \pm 2$ of $R_{m,n}$ then gives us a parameter value such that the corresponding curve C_t has an additional orbit of points in its hyperelliptic torsion packet. If the orbit does not contain fixed points of some nontrivial automorphism, then the torsion packet has size at least $10 + 12 = 22$.

We now search for common irreducible factors among the various $R_{m,n}$. If we find such a common factor, then its roots give us curves C_t with *two* additional orbits in the hyperelliptic torsion packet. And indeed, we do find one such coincidence, which gives the curve given in [Sto]. We state this result.

Theorem 11. *The curve*

$$C\colon y^2 = x^6 + 130x^3 + 13$$

has a hyperelliptic torsion packet of size 34. It consists of the ramification points for the hyperelliptic double cover, the points at infinity, the points with x-coordinate zero, and the points whose x-coordinates satisfy the equation

$$x^{12} - 91x^9 - 273x^6 - 1183x^3 + 169 = 0\,.$$

Proof. This can be shown using Poonen's pari/gp program for computing hyperelliptic torsion packets on genus 2 curves defined over $\mathbb{Q}$; see [Poo01]. □

5 Poonen's family

As mentioned above, in [Poo00], Poonen considers the subfamily

$$C_t\colon y^2 = (x^3 - 1)(x^3 - t^{12})$$

of the family of all bielliptic curves of genus 2 and shows that there are infinitely many t such that the hyperelliptic torsion packet of C_t has at least 22 points. (Here we use the 12-th power to avoid radicals in the sequel.) More precisely, let

$$\iota\colon (x,y) \mapsto (x,-y)\,, \quad \sigma\colon (x,y) \mapsto (\zeta_3 x, y)\,, \quad \tau\colon (x,y) \mapsto \left(\frac{t^4}{x}, \frac{t^6 y}{x^3}\right)\,,$$

where ζ_3 is a primitive third root of unity; these are automorphisms of C_t satisfying

$$\iota^2 = \sigma^3 = \tau^2 = \mathrm{id}\,, \quad \iota\tau = \tau\iota\,, \quad \iota\sigma = \sigma\iota \quad \text{and} \quad \sigma\tau = \tau\sigma^2\,.$$

As explained in the previous section, the 22 points are

(1) the six Weierstrass points (the fixed points of ι),
(2) the four points $0^+ = (0, t^6)$, $0^- = (0, -t^6)$, ∞^+, ∞^- (the fixed points of σ), and
(3) a full length orbit of the group $\langle \iota, \sigma, \tau \rangle$ of order 12.

As explained earlier in this paper, from a bielliptic curve C of genus 2, we can obtain a pair (π_1, π_2) with $P(\pi_1, \pi_2) = (0, 4)$ and such that the size of $I(\pi_1, \pi_2)$ is usually the same as the size of the hyperelliptic torsion packet of C; see Corollary 8. The goal of this section is to explain which pairs correspond to the curves C_t in Poonen's family, and how the effect of the large automorphism group of C_t is reflected in the structure of $I(\pi_1, \pi_2)$.

Since C_t is bielliptic, by the construction in Section 3 we have two morphisms

$$\begin{aligned} \phi_1 \colon C_t &\longrightarrow C_t/\langle\tau\rangle \simeq E_1 \colon y^2 = (x-u)(x-v)(x-w) \\ (x,y) &\longmapsto \left(\frac{(x-t^2)^2}{(x+t^2)^2}, \frac{8t^3 y}{(t^6+1)(x+t^2)^3}\right) \end{aligned}$$

and

$$\begin{aligned} \phi_2 \colon C_t &\longrightarrow C_t/\langle\tau\iota\rangle \simeq E_2 \colon y^2 = x(x-u)(x-v)(x-w) \\ (x,y) &\longmapsto \left(\frac{(x-t^2)^2}{(x+t^2)^2}, \frac{8t^3 (x-t^2) y}{(t^6+1)(x+t^2)^4}\right). \end{aligned}$$

Here we choose the origin of E_1 to be ∞, and the origin of E_2 to be $(0,0)$.

We abuse notation and also write σ for the automorphism of $J(C_t)$ induced by σ. We use θ_j to denote the homomorphism $J(C_t) \to E_j$ induced by ϕ_j, and we write $\theta_j^\vee \colon E_j \to J(C_t)$ for the map induced by pull-back of divisors under ϕ_j.

Proposition 12. *Let $T_1 = \phi_1(0^+)$ and $T_2 = \phi_2(0^+)$. Then T_1 and T_2 have order 3. Moreover,*

$$\varphi_{12} = \theta_2 \circ \sigma \circ \theta_1^\vee \colon E_1 \longrightarrow E_2 \qquad \text{and} \qquad \varphi_{21} = \theta_1 \circ \sigma \circ \theta_2^\vee \colon E_2 \longrightarrow E_1$$

are isogenies with $\ker(\varphi_{12}) = \langle T_1\rangle$ and $\ker(\varphi_{21}) = \langle T_2\rangle$.

Proof. It is clear that φ_{12} is a homomorphism of elliptic curves. Let $P \in E_1$ and choose $Q, R \in C_t$ such that $\phi_1(Q) = P$ and $\phi_1(R) = \infty$ (so $R = (-t^2, \pm t^3(t^6+1))$ and $\iota\tau R = R$). Then, denoting the linear equivalence class of a divisor D on C_t by $[D]$,

$$\begin{aligned} \varphi_{12}(P) &= (\theta_2 \circ \sigma)([Q + \tau Q - R - \tau R]) = \theta_2([\sigma Q + \sigma\tau Q - \sigma R - \sigma\tau R]) \\ &= \theta_2([\sigma Q + \tau\sigma^2 Q - \sigma R - \sigma\tau R]) \overset{(*)}{=} \theta_2([\sigma Q - \iota\tau\sigma^2 Q - \sigma R + \iota\sigma\tau R]) \\ &= \theta_2([\sigma Q - \iota\tau\sigma^2 Q - \sigma R + \sigma\iota\tau R]) = \phi_2(\sigma Q) - \phi_2(\sigma^2 Q)\,. \end{aligned}$$

where at $(*)$ we use that $[Q_1 - Q_2] = [-\iota Q_1 + \iota Q_2]$ in $J(C_t)$, and for the last equality that $\iota\tau R = R$. So $P \in \ker(\varphi_{12})$ if and only if $\sigma Q = \sigma^2 Q$ or $\sigma Q = \tau\iota\sigma^2 Q = \sigma\tau\iota Q$; equivalently, $Q = \sigma Q$ or $Q = \tau\iota Q$. In the first case, $P = \pm T_1$, and in the second case, $P = \infty$. This also implies that T_1 has order 3. The claim regarding φ_{21} follows in the same way. □

We will also need the following.

Lemma 13. *With the notations introduced above, $\theta_j \circ \sigma \circ \theta_j^\vee$ is multiplication by -1 on E_j.*

Proof. We first observe that all divisors of the form $Q + \sigma Q + \sigma^2 Q$ on C_t are linearly equivalent. This is because the quotient $C_t/\langle\sigma\rangle$ is the curve $y^2 = (x-1)(x-t^{12})$ of genus zero.

Let $P \in E_1$ and choose $Q, R \in C_t$ as in the preceding proof. Then

$$\begin{aligned} (\theta_1 \circ \sigma \circ \theta_1^\vee)(P) &= (\theta_1 \circ \sigma)([Q + \tau Q - R - \tau R]) = \theta_1([\sigma Q + \sigma\tau Q - \sigma R - \sigma\tau R]) \\ &= \theta_1([\sigma Q + \tau\sigma^2 Q - \sigma R - \tau\sigma^2 R]) = \theta_1([\sigma Q + \sigma^2 Q - \sigma R - \sigma^2 R]) \\ &= \theta_1([R - Q]) = -P\,. \end{aligned}$$

The argument for E_2 is identical. □

Now let

$$E_s\colon y^2 = (x^2 - s^2)\left(x^2 - \frac{1}{s^2}\right) \quad \text{with origin } (s, 0),$$

and

$$E'_s\colon y^2 = x(x-1)\left(x - \frac{(s^2+1)^2}{4s^2}\right) \quad \text{with origin } \left(\frac{(s^2+1)^2}{4s^2}, 0\right).$$

We have an isogeny

$$\psi\colon E_s \longrightarrow E'_s, \qquad (x, y) \longmapsto \left(\frac{(x^2+1)^2}{4x^2}, \frac{(x^4-1)y}{8x^3}\right).$$

Note that $\ker(\psi) = E_s[2]$ (in particular, E_s and E'_s are isomorphic as elliptic curves) and ψ is independent of s.

For any t, we have the two covering maps $\phi_j\colon C_t \to E_j$. By moving the three common 2-torsion x-coordinates of E_1 and E_2 to $\{0, 1, \infty\}$, we can assume that $E_j = E'_{s_j}$ for suitable s_1 and s_2. One of the four preimages under ψ of the point T_j of order 3 will also have order 3; let $S_j \in E_{s_j}$ be this point. Since T_1 and T_2 have the same x-coordinate (this is still true after applying an automorphism of $\mathbb{P}^1$), the x-coordinates of S_1 and S_2 are equal up to sign and/or taking inverses; by replacing s_2 by $\pm s_2$ or $\pm 1/s_2$, we can make sure that $x(S_1) = x(S_2)$.

Conversely, if $S_1 \in E_{s_1}[3]$ and $S_2 \in E_{s_2}[3]$ have the same x-coordinate, then $C = E'_{s_1} \times_{\mathbb{P}^1} E'_{s_2}$ contains four points $(\pm\psi(S_1), \pm\psi(S_2))$ whose differences have order 3 in $J(C)$ and form two orbits under the hyperelliptic involution. Any such curve has a model of the form C_t.

For $j = 1, 2$, ψ can be decomposed as $\psi = [2] \circ \lambda_{s_j}$, where λ_{s_j} is an isomorphism from E_{s_j} to E'_{s_j} such that $\lambda_{s_j}(S_j) = -T_j$. Proposition 12 shows that there are isogenies φ_{12} and φ_{21} between E'_{s_1} and E'_{s_2}. We use the same symbols for the induced isogenies between E_{s_1} and E_{s_2}.

$$\begin{array}{ccccc} E_{s_1} & \xrightarrow{\lambda_{s_1}} & E'_{s_1} & \xrightarrow{[2]} & E'_{s_1} \\ \downarrow{\scriptstyle \varphi_{12}} & & \downarrow{\scriptstyle \varphi_{12}} & & \downarrow \\ E_{s_2} & \xrightarrow{\lambda_{s_2}} & E'_{s_2} & \xrightarrow{[2]} & E'_{s_2} \end{array} \qquad \begin{array}{ccccc} E_{s_2} & \xrightarrow{\lambda_{s_2}} & E'_{s_2} & \xrightarrow{[2]} & E'_{s_2} \\ \downarrow{\scriptstyle \varphi_{21}} & & \downarrow{\scriptstyle \varphi_{21}} & & \downarrow \\ E_{s_1} & \xrightarrow{\lambda_{s_1}} & E'_{s_1} & \xrightarrow{[2]} & E'_{s_1} \end{array}$$

Proposition 14. *Let π_1 and π_2 be the x-coordinate maps of E_{s_1} and E_{s_2}. Assume that there are $S_1 \in E_{s_1}[3]$ and $S_2 \in E_{s_2}[3]$ with $\pi_1(S_1) = \pi_2(S_2)$. Then for any $P_1 \in E_{s_1}$ and $P_2 \in E_{s_2}$ with $\pi_1(P_1) = \pi_2(P_2)$, we have*

$$\pi_1\big([2]^{-1}(-P_1 \pm \varphi_{21}(P_2))\big) = \pi_2\big([2]^{-1}(-P_2 \pm \varphi_{12}(P_1))\big).$$

This gives usually eight further common torsion x-coordinates, in addition to the set $\pi_1(P_1 + E_1[2]) = \pi_2(P_2 + E_2[2])$ of size four, corresponding to an orbit on C_t under $\langle \iota, \sigma, \tau \rangle$.

Proof. We shall use the same notations as in the proof of Proposition 12, except that now we replace E_1 and E_2 with E'_{s_1} and E'_{s_2}.

Let $Q_1 = \lambda_{s_1}(P_1)$ and $Q_2 = \lambda_{s_2}(P_2)$. Then $[2]Q_1$ and $[2]Q_2$ have the same x-coordinate. So there is $Q \in C_t$ such that $(\phi_1(Q), \phi_2(Q)) = ([2]Q_1, [2]Q_2)$. Let $(R_1, R_2) \in E'_{s_1} \times E'_{s_2}$ be such that

$$(\theta_1, \theta_2)^\vee(R_1, R_2) = [Q - W],$$

where $W \in C_t$ is a fixed Weierstrass point. Then

$$\begin{aligned}([2]R_1, [2]R_2) &= \big((\theta_1, \theta_2) \circ (\theta_1, \theta_2)^\vee\big)(R_1, R_2) \\ &= (\theta_1, \theta_2)([Q - W]) = ([2]Q_1, [2]Q_2) - (\phi_1(W), \phi_2(W)).\end{aligned}$$

Therefore, $(R_1, R_2) = (Q_1, Q_2) - (W_1, W_2)$ for some $(W_1, W_2) \in (E'_{s_1} \times E'_{s_2})[4]$. Since by Proposition 12 and Lemma 13

$$\begin{aligned}(-Q_1 + \varphi_{21}(Q_2)) - (-W_1 + \varphi_{21}(W_2)) &= \big(\theta_1 \circ \sigma \circ (\theta_1, \theta_2)^\vee\big)(R_1, R_2) \\ &= (\theta_1 \circ \sigma)([Q - W]) = \phi_1(\sigma Q) - \phi_1(\sigma W),\end{aligned}$$

we have

$$-Q_1 + \varphi_{21}(Q_2) - \phi_1(\sigma Q) = -W_1 + \varphi_{21}(W_2) - \phi_1(\sigma W) \in E'_{s_1}[4].$$

Therefore, $(P_1, P_2) \mapsto -Q_1 + \varphi_{21}(Q_2) - \phi_1(\sigma Q)$ gives a constant map from $E_{s_1} \times_{\mathbb{P}^1} E_{s_2}$ to E'_{s_1}. To determine this constant, we take $(P_1, P_2) = (S_1, S_2)$; then $(Q_1, Q_2) = (-T_1, -T_2)$ and $Q = \mathcal{O}^+$, which imply

$$\phi_1(\sigma Q) = \phi_1(Q) = T_1 = -Q_1 + \varphi_{21}(Q_2),$$

showing that the constant is in fact zero. Similarly, we have

$$\phi_1(\sigma^2 Q) = -Q_1 - \varphi_{21}(Q_2), \quad \phi_2(\sigma Q) = -Q_2 + \varphi_{12}(Q_1), \quad \phi_2(\sigma^2 Q) = -Q_2 - \varphi_{12}(Q_1).$$

Now consider a point $P'_1 \in E_{s_1}$ such that $[2]P'_1 = -P_1 \pm \varphi_{21}(P_2)$. Then

$$\psi(P'_1) = \lambda_{s_1}([2]P'_1) = -Q_1 \pm \varphi_{21}(Q_2) = \phi_1(\sigma^k Q)$$

(with $k = 1$ for the positive sign and $k = 2$ for the negative sign). Since $\phi_1(\sigma^k Q)$ and $\phi_2(\sigma^k Q)$ have the same x-coordinate, there is $P'_2 \in E_{s_2}$ with $[2]P'_2 = -P_2 \pm \varphi_{12}(P_1)$ such that $\psi(P'_2)$ has the same x-coordinate as $\psi(P'_1)$. Since $E_{s_j}[2]$ acts transitively on the fibers of ψ (and ψ is independent of s_j), the conclusion follows. □

References

[BR03] Matthew H. Baker and Kenneth A. Ribet, *Galois theory and torsion points on curves*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 11–32 (English, with English and French summaries). Les XXIIèmes Journées Arithmetiques (Lille, 2001). MR2018998 ↑5

[BF16] Fedor A. Bogomolov and Hang Fu, *Division polynomials and intersection of projective torsion points*, Eur. J. Math. **2** (2016), no. 3, 644–660, DOI 10.1007/s40879-016-0111-7. MR3536148 ↑1

[BFT18] Fedor Bogomolov, Hang Fu, and Yuri Tschinkel, *Torsion of elliptic curves and unlikely intersections*, Geometry and physics. Vol. I, Oxford Univ. Press, Oxford, 2018, pp. 19–37. MR3932255 ↑1, 2

[BT07] Fedor Bogomolov and Yuri Tschinkel, *Algebraic varieties over small fields*, Diophantine geometry, CRM Series, vol. 4, Ed. Norm., Pisa, 2007, pp. 73–91. MR2349648 ↑1

[DKY20] Laura DeMarco, Holly Krieger, and Hexi Ye, *Uniform Manin-Mumford for a family of genus 2 curves*, Ann. of Math. (2) **191** (2020), no. 3, 949–1001, DOI 10.4007/annals.2020.191.3.5. MR4088354 ↑1, 6

[DGH21] Vesselin Dimitrov, Ziyang Gao, and Philipp Habegger, *Uniformity in Mordell-Lang for curves*, March 31, 2021. https://arxiv.org/abs/2001.10276v3, to appear in Ann. of Math. ↑1

[Gao21] Ziyang Gao, *Recent developments of the uniform Mordell-Lang conjecture*, May 11, 2021. https://arxiv.org/abs/2104.03431v4. ↑1

[GGK21] Ziyang Gao, Tangli Ge, and Lars Kühne, *The uniform Mordell-Lang conjecture*, July 24, 2021. https://arxiv.org/abs/2105.15085v2. ↑1

[Küh21] Lars Kühne, *Equidistribution in families of abelian varieties and uniformity*, February 3, 2021. https://arxiv.org/abs/2101.10272v2. ↑1

[Maz86] Barry Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), no. 2, 207–259, DOI 10.1090/S0273-0979-1986-15430-3. MR828821 ↑1

[Poo00] Bjorn Poonen, *Genus-two curves with 22 torsion points*, C. R. Acad. Sci. Paris Sér. I Math. **330** (2000), no. 7, 573–576, DOI 10.1016/S0764-4442(00)00222-6 (English, with English and French summaries). MR1760441 ↑1, 2, 3, 6, 7, 9

[Poo01] ———, *Computing torsion points on curves*, Experiment. Math. **10** (2001), no. 3, 449–465. MR1917430 ↑7, 9

[Ray83] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), no. 1, 207–233, DOI 10.1007/BF01393342 (French). MR688265 ↑1, 5

[Sto] Michael Stoll, *A genus 2 curve over $\mathbb{Q}$ with a hyperelliptic torsion packet of size 34*. http://www.mathe2.uni-bayreuth.de/stoll/torsion.html. ↑2, 3, 7, 9

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN UNIVERSITY, TAIPEI, TAIWAN

Email address: drfuhang@gmail.com

MATHEMATISCHES INSTITUT, UNIVERSITÄT BAYREUTH, 95440 BAYREUTH, GERMANY.

Email address: Michael.Stoll@uni-bayreuth.de

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