CrossMark

Division polynomials and intersection of projective torsion points

Fedor A. Bogomolov[1,2] (ID) · **Hang Fu**[1] (ID)

Abstract Given two elliptic curves, each of which is associated with a projection map that identifies opposite elements with respect to the natural group structure, we investigate how their corresponding projective images of torsion points intersect.

Keywords Elliptic curve · Division polynomial · Unlikely intersection · Jordan's totient function

Mathematics Subject Classification 14H52

1 Introduction

Throughout the article, let K be a field of characteristic 0, (E, O) an elliptic curve defined over K, $E[n]$ the collection of n-th torsion points, $E^*[n]$ the collection of torsion points of exact order n, $E[\infty]$ the collection of all torsion points, and $\pi \in K(E)$ an even morphism of degree 2.

✉ Hang Fu
  fu@cims.nyu.edu

  Fedor A. Bogomolov
  bogomolo@cims.nyu.edu

[1] Courant Institute of Mathematical Sciences, New York University, 251 Mercer Str., New York, NY 10012, USA

[2] Laboratory of Algebraic Geometry, NRU HSE, 7 Vavilova Str., Moscow, Russia 117312

Bogomolov and Tschinkel [1] observed that

Theorem 1.1 *If $\pi_1(E_1[2])$ and $\pi_2(E_2[2])$ are different, then the intersection of $\pi_1(E_1[\infty])$ and $\pi_2(E_2[\infty])$ is finite.*

Proof Consider the product map $\pi_1 \times \pi_2 \colon E_1 \times E_2 \to \mathbb{P}^1 \times \mathbb{P}^1$, let Δ be the diagonal curve. Suppose that $\#\pi_1(E_1[2]) \cap \pi_2(E_2[2]) = 0$ (resp. 1, 2, 3), then the preimage $(\pi_1 \times \pi_2)^{-1}(\Delta)$ is a curve of genus 5 (resp. 4, 3, 2), and hence contains only finitely many torsion points of $E_1 \times E_2$, by Raynaud's theorem [10]. $\square$

However, we expect not only the finiteness, but also the existence of a universal bound of the cardinality of their intersection.

Conjecture 1.2 $\sup(\#\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])) < \infty$, where supremum is taken over $(K, E_1, O_1, \pi_1, E_2, O_2, \pi_2)$ such that $\pi_1(E_1[2]) \neq \pi_2(E_2[2])$.

Here the supremum is taken over all K, but clearly we can restrict to $K = \overline{\mathbb{Q}}$ or $K = \mathbb{C}$. In Sect. 3, Theorems 3.1 and 3.2 will indicate that under some mild conditions, the cardinality is small, while Theorem 3.7 will give a construction to show that it can be at least 14. (See also Remark 3.8). The main tool to achieve these results is the explicit calculation of division polynomials, which will be introduced and developed in Sect. 2. Jordan's totient function, as an ingredient of division polynomials, will be briefly discussed in Appendix. Calculations were assisted by Mathematica 10.0 [14].

2 Division polynomials

Now let $E \colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ be in the generalized Weierstrass form with the identity element $O^W = (0{:}1{:}0)$, then it has a canonical projection map $\pi^W \colon E \to \mathbb{P}^1$, $(x, y) \mapsto x$. We have the standard quantities

$$b_2 = a_1^2 + 4a_2, \qquad\qquad b_4 = 2a_4 + a_1 a_3,$$
$$b_6 = a_3^2 + 4a_6, \qquad\qquad b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, \qquad\qquad c_6 = -b_2^3 + 36b_2 b_4 - 216b_6,$$
$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \quad j = c_4^3/\Delta,$$

with relations

$$4b_8 = b_2 b_6 - b_4^2, \qquad 1728\Delta = c_4^3 - c_6^2.$$

Traditionally, the division polynomials ψ_n [13] are defined by the initial values

$$\psi_1 = 1,$$
$$\psi_2 = 2y + a_1 x + a_3,$$
$$\psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,$$
$$\psi_4 = \psi_2 \cdot (2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3$$
$$+ 10b_8 x^2 + (b_2 b_8 - b_4 b_6)x + (b_4 b_8 - b_6^2)),$$

and the inductive formulas

$$\psi_{2n+1} = \psi_n^3 \psi_{n+2} - \psi_{n-1}\psi_{n+1}^3, \qquad\qquad n \geqslant 2,$$
$$\psi_2 \psi_{2n} = \psi_{n-1}^2 \psi_n \psi_{n+2} - \psi_{n-2}\psi_n \psi_{n+1}^2, \qquad n \geqslant 3.$$

Notice that

$$\psi_2^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6.$$

Since $\mathrm{char}(K) = 0$, we can eliminate b_8 and the leading coefficients.

Definition 2.1 Let $n > 1$,

(A) the *normalized n-th division polynomial* is

$$f_n(x) = \prod_{P \in E[n] \setminus \{O^W\}} (x - \pi^W(P));$$

(B) the *normalized n-th primitive division polynomial* is

$$F_n(x) = \prod_{\{\pi^W(P) : P \in E^*[n]\}} (x - \pi^W(P)).$$

Theorem 2.2 *We have the following explicit formulas:*

(A)

$$f_n(x) = \sum_{\substack{(r,s,t) \\ r+2s+3t \leqslant d(n)}} c_{r,s,t}(n) b_2^r b_4^s b_6^t x^{d(n)-(r+2s+3t)},$$

the degree and the first three coefficients are

$$d(n) = n^2 - 1,$$
$$c_{1,0,0}(n) = \frac{n^2 - 1}{12} = \frac{1}{12} n^2 - \frac{1}{12},$$
$$c_{0,1,0}(n) = \frac{(n^2 - 1)(n^2 + 6)}{60} = \frac{1}{60} n^4 + \frac{1}{12} n^2 - \frac{1}{10},$$
$$c_{0,0,1}(n) = \frac{(n^2 - 1)(n^4 + n^2 + 15)}{420} = \frac{1}{420} n^6 + \frac{1}{30} n^2 - \frac{1}{28};$$

(B)

$$F_n(x) = \sum_{\substack{(r,s,t) \\ r+2s+3t \leqslant D(n)}} C_{r,s,t}(n) b_2^r b_4^s b_6^t x^{D(n)-(r+2s+3t)},$$

the degree and the first three coefficients are

$$D(n) = \frac{1}{2} J_2(n) I(n),$$

$$C_{1,0,0}(n) = \frac{1}{24} J_2(n) I(n),$$

$$C_{0,1,0}(n) = \left(\frac{1}{120} J_4(n) + \frac{1}{24} J_2(n) \right) I(n),$$

$$C_{0,0,1}(n) = \left(\frac{1}{840} J_6(n) + \frac{1}{60} J_2(n) \right) I(n),$$

where

$$I(n) = \begin{cases} 2 & \text{if } n = 2, \\ 1 & \text{if } n > 2, \end{cases}$$

and

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k} \right)$$

is Jordan's totient function.

Proof (A) Notice that $f_n(x) = \psi_n^2(x)/n^2$, so the inductive formulas for ψ_n can be transformed to

$$f_{2n+1} = \left(\frac{n^3(n+2)}{2n+1} \sqrt{f_n^3 f_{n+2}} - \frac{(n-1)(n+1)^3}{2n+1} \sqrt{f_{n-1} f_{n+1}^3} \right)^2$$

for $n \geqslant 2$, and

$$f_{2n} = \left(\frac{(n-1)^2(n+2)}{4} \sqrt{\frac{f_{n-1}^2 f_n f_{n+2}}{f_2}} - \frac{(n-2)(n+1)^2}{4} \sqrt{\frac{f_{n-2} f_n f_{n+1}^2}{f_2}} \right)^2$$

for $n \geqslant 3$. In order to use induction to prove the formulas for $t(n) = d(n)$, $c_{1,0,0}(n)$, $c_{0,1,0}(n)$, and $c_{0,0,1}(n)$, we need to check the initial values $t(n)$ for $1 \leqslant n \leqslant 4$, and verify that they all satisfy

$$t(2n+1) = \frac{n^3(n+2)}{2n+1} (3t(n) + t(n+2)) - \frac{(n-1)(n+1)^3}{2n+1} (t(n-1) + 3t(n+1))$$

for $n \geqslant 2$, and

$$t(2n) = \frac{(n-1)^2(n+2)}{4} \left(2t(n-1) + t(n) + t(n+2) - t(2)\right)$$
$$- \frac{(n-2)(n+1)^2}{4} \left(t(n-2) + t(n) + 2t(n+1) - t(2)\right)$$

for $n \geqslant 3$. All of these can be easily done.

(B) By definition,

$$f_n(x) = \prod_{\substack{d|n \\ d \neq 1}} F_d(x)^{2/I(d)},$$

so for $T(n) = D(n)$, $C_{1,0,0}(n)$, $C_{0,1,0}(n)$, and $C_{0,0,1}(n)$, we have

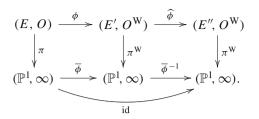$$t(n) = \sum_{\substack{d|n \\ d \neq 1}} \frac{2}{I(d)} T(d).$$

Then the rest is a standard application of the Möbius inversion formula. $\qquad \square$

Theorem 2.3 *Let E_1 and E_2 be two elliptic curves in the generalized Weierstrass form, then the following are equivalent:*

(A) $b_i(E_1) = b_i(E_2)$, $i = 2, 4, 6$;
(B) *for any n*, $\pi^W(E_1^*[n]) = \pi^W(E_2^*[n])$;
(C) $\pi^W(E_1[\infty]) = \pi^W(E_2[\infty])$;
(D) $\pi^W(E_1[\infty]) \cap \pi^W(E_2[\infty])$ *is infinite*;
(E) *for some $n > 1$*, $\pi^W(E_1^*[n]) = \pi^W(E_2^*[n])$;
(F) *for some $n_1, \ldots, n_k > 1$*, $\pi^W\left(\bigcup_{i=1}^k E_1^*[n_i]\right) = \pi^W\left(\bigcup_{i=1}^k E_2^*[n_i]\right)$.

Proof (A)$\Rightarrow$(B)$\Rightarrow$(C)$\Rightarrow$(D)$\Rightarrow$(E)$\Rightarrow$(F) is clear, where (D)$\Rightarrow$(E) is given by Theorem 1.1. Assume (F), then E_1 and E_2 share the same $\prod_{i=1}^k F_{n_i}(x)$. Since $C_{1,0,0}(n)$, $C_{0,1,0}(n)$, and $C_{0,0,1}(n)$ are all strictly positive, the coefficients of b_2, b_4, and b_6 in the product $\prod_{i=1}^k F_{n_i}(x)$ will always be nonzero, then b_2, b_4, and b_6 can be solved, which proves (A). $\qquad \square$

Now let us go back to the general (E, O, π), and assume that $\pi(O) = \infty$. By the Riemann–Roch theorem, there exists an isomorphism $\phi \colon E \to E'$ such that E' is in the generalized Weierstrass form. Then ϕ induces $\bar{\phi} \in \mathrm{Aut}(\mathbb{P}^1)$ fixing ∞, which must be a linear function [5]. Its inverse $\bar{\phi}^{-1}$ can be lifted to $\hat{\phi} \colon E' \to E''$ such that E'' remains in the generalized Weierstrass form. Thus the general case can be reduced to the Weierstrass case. Note that we can make everything above defined over K, except possibly $\hat{\phi}$ has to be defined over a quadratic extension of K.

$$(E, O) \xrightarrow{\phi} (E', O^{\mathrm{W}}) \xrightarrow{\widehat{\phi}} (E'', O^{\mathrm{W}})$$

$$\Big\downarrow \pi \qquad\qquad \Big\downarrow \pi^{\mathrm{W}} \qquad\qquad \Big\downarrow \pi^{\mathrm{W}}$$

$$(\mathbb{P}^1, \infty) \xrightarrow{\overline{\phi}} (\mathbb{P}^1, \infty) \xrightarrow{\overline{\phi}^{-1}} (\mathbb{P}^1, \infty).$$

$$\mathrm{id}$$

Corollary 2.4 *Given* (E_1, O_1, π_1) *and* (E_2, O_2, π_2) *such that* $\pi_1(O_1) = \pi_2(O_2)$, *then the following are equivalent:*

(A) *for any* n, $\pi_1(E_1^*[n]) = \pi_2(E_2^*[n])$;
(B) *for some* $n > 1$, $\pi_1(E_1^*[n]) = \pi_2(E_2^*[n])$;
(C) *for some* $n_1, \ldots, n_k > 1$, $\pi_1\big(\bigcup_{i=1}^k E_1^*[n_i]\big) = \pi_2\big(\bigcup_{i=1}^k E_2^*[n_i]\big)$;
(D) $\pi_1(E_1[\infty]) = \pi_2(E_2[\infty])$;
(E) $\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])$ *is infinite.*

Proof First move $\pi_1(O_1)$ and $\pi_2(O_2)$ to ∞ by a common fractional linear transformation, and then use the above argument. □

The following corollary gives the converse of Theorem 1.1.

Corollary 2.5 *Given* (E_1, O_1, π_1) *and* (E_2, O_2, π_2), *then the following are equivalent:*

(A) $\pi_1(E_1[2]) = \pi_2(E_2[2])$;
(B) $\pi_1(E_1[\infty]) = \pi_2(E_2[\infty])$;
(C) $\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])$ *is infinite.*

Proof Assume (A), if $\pi_1(O_1) = \pi_2(P)$ for some $P \in E_2[2]$, then the translation-by-P map $[+P]$ acts on $E_2[2]$ and $E_2[\infty]$ bijectively, the projection map $\pi_2 \circ [+P]$ satisfies $\pi_1(O_1) = \pi_2 \circ [+P](O_2)$, which implies (B), by Corollary 2.4. (B)$\Rightarrow$(C) is obvious, and (C)$\Rightarrow$(A) is a restatement of Theorem 1.1. □

Given Theorem 2.3, it is natural to ask

Question 2.6 Let E_1 and E_2 be two elliptic curves in the generalized Weierstrass form, if $\pi^{\mathrm{W}}(E_1^*[n_1]) = \pi^{\mathrm{W}}(E_2^*[n_2])$, can we always conclude that $n_1 = n_2$?

If Conjecture 1.2 is true, then the answer must be yes, at least when n_1 and n_2 are large enough. A naive attempt is to write their division polynomials more explicitly, and then compare those coefficients. Clearly, a necessary condition is $D(n_1) = D(n_2)$. However, since we have, for example,

$$D(5) = D(6) = 12,$$
$$D(35) = D(40) = D(42) = 576,$$
$$D(55) = D(57) = D(62) = D(66) = 1440,$$

$D(n)$ itself does not give a strong restriction on n. Notice that $C_{1,0,0}(n) = D(n)/12$, so $b_2(E_1) = b_2(E_2)$, we can assume the common value is 0, and consequently b_2 disappears in the formulas of $f_n(x)$ and $F_n(x)$. Based on the same approach as before, together with a tedious calculation, we can obtain all the coefficients $C_{0,s,t}(n)$ for $2s + 3t \leqslant 6$.

Theorem 2.7 *We have the following explicit formulas for the coefficients of $F_n(x)$:*

$$C_{0,2,0}(n) = -\left(\frac{1}{16800}J_8(n) + \frac{1}{600}J_4(n) + \frac{5}{672}J_2(n)\right)I(n)$$

$$+ \frac{1}{2}\left(\frac{1}{120}J_4(n) + \frac{1}{24}J_2(n)\right)^2 I^2(n),$$

$$C_{0,1,1}(n) = -\left(\frac{1}{92400}J_{10}(n) + \frac{1}{2800}J_6(n) + \frac{1}{1680}J_4(n) + \frac{1}{150}J_2(n)\right)I(n)$$

$$+ \left(\frac{1}{120}J_4(n) + \frac{1}{24}J_2(n)\right)\left(\frac{1}{840}J_6(n) + \frac{1}{60}J_2(n)\right)I^2(n),$$

$$C_{0,0,2}(n) = -\left(\frac{1}{1345344}J_{12}(n) + \frac{1}{7840}J_6(n) + \frac{1}{660}J_2(n)\right)I(n)$$

$$+ \frac{1}{2}\left(\frac{1}{840}J_6(n) + \frac{1}{60}J_2(n)\right)^2 I^2(n),$$

$$C_{0,3,0}(n) = \left(\frac{1}{2574000}J_{12}(n) + \frac{1}{42000}J_8(n) + \frac{17}{36000}J_4(n) + \frac{5}{2464}J_2(n)\right)I(n)$$

$$- \left(\frac{1}{16800}J_8(n) + \frac{1}{600}J_4(n) + \frac{5}{672}J_2(n)\right)$$

$$\cdot \left(\frac{1}{120}J_4(n) + \frac{1}{24}J_2(n)\right)I^2(n)$$

$$+ \frac{1}{6}\left(\frac{1}{120}J_4(n) + \frac{1}{24}J_2(n)\right)^3 I^3(n).$$

Proof When n is odd, write

$$\psi_n(x) = \sum_{\substack{(s,t) \\ 2s+3t \leqslant d(n)/2}} \widetilde{c}_{s,t}(n) b_4^s b_6^t x^{d(n)/2-(2s+3t)}.$$

For this case, McKee [8] proved the following recurrence relation for $\widetilde{c}_{s,t}(n)$:

$$(2s+3t)\left(2s + 3t + \frac{1}{2}\right)\widetilde{c}_{s,t}(n)$$

$$= \frac{1}{2}\left(\frac{n^2+3}{2} - 2s - 3t\right)\left(\frac{n^2}{6} - 1 + 2s + 3t\right)\widetilde{c}_{s-1,t}(n)$$

$$- \frac{1}{4}\left(\frac{n^2+5}{2} - 2s - 3t\right)\left(\frac{n^2+3}{2} - 2s - 3t\right)\widetilde{c}_{s,t-1}(n)$$

$$+ \frac{3}{2}(s+1)n^2\widetilde{c}_{s+1,t-1}(n) - \frac{2}{3}(t+1)n^2\widetilde{c}_{s-2,t+1}(n).$$

By this formula, we can first calculate $\widetilde{c}_{s,t}(n)$, and then $C_{0,s,t}(n)$. The case when n is even can be similarly dealt with another relation which is proved in the same paper.□

Remark 2.8 Clearly, these formulas have some beautiful patterns, which we expect are shared by all $C_{r,s,t}(n)$. Specifically, depending on (r, s, t), each $C_{r,s,t}(n)$ is an alternating sum of several components, each component is a product of several sub-components, and each subcomponent is a positive rational linear combination of $J_k(n)$.

If $j(E_1)$, $j(E_2) \neq 0, 1728$, it suffices to show that the map

$$n \mapsto \left(D(n), \frac{C_{0,2,0}(n)}{C_{0,1,0}^2(n)}, \frac{C_{0,1,1}(n)}{C_{0,1,0}(n)C_{0,0,1}(n)}, \frac{C_{0,0,2}(n)}{C_{0,0,1}^2(n)} \right)$$

is injective. Unfortunately, although it is supported by extensive calculations, we fail to prove it. On the other hand, we have

Theorem 2.9 *Let E_1 and E_2 be two elliptic curves in the generalized Weierstrass form such that $\pi^{\mathrm{W}}(E_1^*[n_1]) = \pi^{\mathrm{W}}(E_2^*[n_2])$ for some $n_1 \neq n_2$, then $j(E_1), j(E_2) \in \overline{\mathbb{Q}} \setminus \{0, 1728\}$.*

Proof We have assumed $b_2 = 0$, so $j = 0$ if and only if $b_4 = 0$, and $j = 1728$ if and only if $b_6 = 0$. Since $\pi^{\mathrm{W}}(E_1^*[n_1]) = \pi^{\mathrm{W}}(E_2^*[n_2])$, we have

$$\begin{cases} C_{0,1,0}(n_1)b_4(E_1) = C_{0,1,0}(n_2)b_4(E_2), \\ C_{0,0,1}(n_1)b_6(E_1) = C_{0,0,1}(n_2)b_6(E_2). \end{cases}$$

Thus there are three cases:

(A) $b_4(E_1) = b_4(E_2) = 0$. We can assume $b_6(E_1), b_6(E_2) \in \mathbb{Q}^\times$, then E_1 and E_2 are both elliptic curves with complex multiplication by $\mathcal{O}_L$, the integer ring of $L = \mathbb{Q}(\sqrt{-3})$. By class field theory [9] of imaginary quadratic fields [12],

$$L\left((\pi^{\mathrm{W}}(E_i^*[n_i]))^3 \right) = L\left((\pi^{\mathrm{W}}(E_i[n_i]))^3 \right) = L^{n_i}$$

is the ray class field of L for the modulus n_i. We want to determine all $\mathfrak{m} \neq \mathfrak{n}$ such that $L^{\mathfrak{m}} = L^{\mathfrak{n}}$. Since the common divisors of $\mathfrak{m}$ and $\mathfrak{n}$ give the same ray class field, it is enough to assume that $\mathfrak{m} | \mathfrak{n}$, thus

$$1 = C_L^{\mathfrak{m}}/C_L^{\mathfrak{n}} = \left(I_L^{\mathfrak{m}} \cdot L^\times/L^\times \right)/\left(I_L^{\mathfrak{n}} \cdot L^\times/L^\times \right) = \left(I_L^{\mathfrak{m}}/(I_L^{\mathfrak{m}} \cap L^\times) \right)/\left(I_L^{\mathfrak{n}}/(I_L^{\mathfrak{n}} \cap L^\times) \right),$$

so the indices

$$\left[(I_L^{\mathfrak{m}} \cap L^\times):(I_L^{\mathfrak{n}} \cap L^\times) \right] = \left[I_L^{\mathfrak{m}}:I_L^{\mathfrak{n}} \right] = \prod_{\mathfrak{p}} \left[U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))}:U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{n}))} \right].$$

In L, 2 is inert, $3 = \mathfrak{p}_3^2$ is ramified, and $7 = \mathfrak{p}_{7a}\mathfrak{p}_{7b}$ splits. Then

$$I_L^{\mathfrak{m}} \cap L^{\times} = \begin{cases} \mu_6 & \text{if } \mathfrak{m} = 1, \\ \mu_3 & \text{if } \mathfrak{m} = \mathfrak{p}_3, \\ \mu_2 & \text{if } \mathfrak{m} = 2, \\ \mu_1 & \text{otherwise,} \end{cases}$$

where μ_N is the group of N-th roots of unity, and

$$\prod_{\mathfrak{p}} [U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))} : U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{n}))}] = \begin{cases} 2 & \text{if } (\mathfrak{m}, \mathfrak{n}) = (1, \mathfrak{p}_3), (2, 2\mathfrak{p}_3), \\ 3 & \text{if } (\mathfrak{m}, \mathfrak{n}) = (1, 2), (\mathfrak{p}_3, 2\mathfrak{p}_3), \\ 6 & \text{if } (\mathfrak{m}, \mathfrak{n}) = (1, 2\mathfrak{p}_3), (1, \mathfrak{p}_{7a}), (1, \mathfrak{p}_{7b}). \end{cases}$$

We conclude that different moduli give different ray class fields except for

$$L^1 = L^2 = L^{\mathfrak{p}_3} = L^{2\mathfrak{p}_3} = L^{\mathfrak{p}_{7a}} = L^{\mathfrak{p}_{7b}}.$$

Thus the conductor of $L^{\mathfrak{n}}$ is $\mathfrak{n}/I(\mathfrak{n})$, $L^{\mathfrak{n}_1} = L^{\mathfrak{n}_2}$ implies $\mathfrak{n}_1 = \mathfrak{n}_2$.

(B) $b_6(E_1) = b_6(E_2) = 0$. We can assume $b_4(E_1), b_4(E_2) \in \mathbb{Q}^{\times}$, then E_1 and E_2 are both elliptic curves with complex multiplication by $\mathcal{O}_L$, the integer ring of $L = \mathbb{Q}(\sqrt{-1})$. By class field theory of imaginary quadratic fields,

$$L\big((\pi^{\mathrm{W}}(E_i^*[\mathfrak{n}_i]))^2\big) = L\big((\pi^{\mathrm{W}}(E_i[\mathfrak{n}_i]))^2\big) = L^{\mathfrak{n}_i}$$

is the ray class field of L for the modulus $\mathfrak{n}_i$. In L, $2 = \mathfrak{p}_2^2$ is ramified, and $5 = \mathfrak{p}_{5a}\mathfrak{p}_{5b}$ splits. Then

$$I_L^{\mathfrak{m}} \cap L^{\times} = \begin{cases} \mu_4 & \text{if } \mathfrak{m} = 1, \mathfrak{p}_2, \\ \mu_2 & \text{if } \mathfrak{m} = 2, \\ \mu_1 & \text{otherwise,} \end{cases}$$

and

$$\prod_{\mathfrak{p}} [U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))} : U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{n}))}] = \begin{cases} 1 & \text{if } \mathfrak{n} = \mathfrak{p}_2\mathfrak{m}, \text{ where } \mathfrak{p}_2 \nmid \mathfrak{m}, \\ 2 & \text{if } (\mathfrak{m}, \mathfrak{n}) = (1, 2), (\mathfrak{p}_2, 2), (2, 2\mathfrak{p}_2), \\ 4 & \text{if } (\mathfrak{m}, \mathfrak{n}) = (1, 2\mathfrak{p}_2), (\mathfrak{p}_2, 2\mathfrak{p}_2), (1, \mathfrak{p}_{5a}), \\ & \qquad (1, \mathfrak{p}_{5b}), (1, \mathfrak{p}_2\mathfrak{p}_{5a}), (1, \mathfrak{p}_2\mathfrak{p}_{5b}), \\ & \qquad (\mathfrak{p}_2, \mathfrak{p}_2\mathfrak{p}_{5a}), (\mathfrak{p}_2, \mathfrak{p}_2\mathfrak{p}_{5b}). \end{cases}$$

We conclude that different moduli give different ray class fields except for

$$L^1 = L^{\mathfrak{p}_2} = L^2 = L^{2\mathfrak{p}_2} = L^{\mathfrak{p}_{5a}} = L^{\mathfrak{p}_{5b}} = L^{\mathfrak{p}_2\mathfrak{p}_{5a}} = L^{\mathfrak{p}_2\mathfrak{p}_{5b}},$$
$$L^{\mathfrak{m}} = L^{\mathfrak{p}_2\mathfrak{m}}, \quad \text{where } \mathfrak{p}_2 \nmid \mathfrak{m}.$$

Thus the conductor of L^n is $n/I(n)$, $L^{n_1} = L^{n_2}$ implies $n_1 = n_2$.

(C) $b_4(E_1)$, $b_4(E_2)$, $b_6(E_1)$, $b_6(E_2) \neq 0$. The relation

$$\sum_{0 \leqslant k \leqslant s/3} C_{0,s-3k,2k}(n_1) b_4^{s-3k}(E_1) b_6^{2k}(E_1)$$

$$= \sum_{0 \leqslant k \leqslant s/3} C_{0,s-3k,2k}(n_2) b_4^{s-3k}(E_2) b_6^{2k}(E_2)$$

implies

$$\sum_{0 \leqslant k \leqslant s/3} \left(C_{0,s-3k,2k}(n_1) - \frac{C_{0,s-3k,2k}(n_2) C_{0,1,0}^{s-3k}(n_1) C_{0,0,1}^{2k}(n_1)}{C_{0,1,0}^{s-3k}(n_2) C_{0,0,1}^{2k}(n_2)} \right) \left(\frac{b_6^2(E_1)}{b_4^3(E_1)} \right)^k = 0.$$

Now $b_6^2(E_1)/b_4^3(E_1) \in \overline{\mathbb{Q}}$ unless all coefficients are zero. Part (B) implies that

$$\sum_{s:2s \leqslant D(n_1)} C_{0,s,0}(n_1) b_4^s(E_1) x^{D(n_1)-2s} \neq \sum_{s:2s \leqslant D(n_2)} C_{0,s,0}(n_2) b_4^s(E_2) x^{D(n_2)-2s}$$

as polynomials, so there exists some s such that

$$C_{0,s,0}(n_1) b_4^s(E_1) \neq C_{0,s,0}(n_2) b_4^s(E_2),$$

which in turn implies the constant term

$$C_{0,s,0}(n_1) - \frac{C_{0,s,0}(n_2) C_{0,1,0}^s(n_1)}{C_{0,1,0}^s(n_2)} \neq 0.$$

Thus $b_6^2(E_1)/b_4^3(E_1) \in \overline{\mathbb{Q}}$, which implies $j(E_1)$, $j(E_2) \in \overline{\mathbb{Q}}$. $\qquad \square$

3 Intersection of projective torsion points

Now let K be a number field, $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K,

$$\chi_K : G_K \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{cyc}}/K) \cong \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/K \cap \mathbb{Q}^{\mathrm{cyc}}) \hookrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times$$

the cyclotomic character of K. Consider the associated Galois representation

$$\rho_E : G_K \to \mathrm{Aut}(E[\infty]) \cong \mathrm{GL}(2, \widehat{\mathbb{Z}}).$$

Since $\chi_K = \det \circ \rho_E$, we always have $\rho_E(G_{K^{\mathrm{cyc}}}) \subseteq \mathrm{SL}(2, \widehat{\mathbb{Z}})$. Zywina [16] proved that if $K \neq \mathbb{Q}$, then for almost all elliptic curves defined over K, this is actually an equality, namely, $\rho_E(G_{K^{\mathrm{cyc}}}) = \mathrm{SL}(2, \widehat{\mathbb{Z}})$.

Theorem 3.1 *Given* (E_1, O_1, π_1) *and* (E_2, O_2, π_2), *all defined over a number field* $K \neq \mathbb{Q}$, *if*

(A) $\pi_1(O_1) = \pi_2(O_2)$,
(B) *Corollary* 2.4 *does not hold*,
(C) $\rho_{E_1}(G_{K^{\mathrm{cyc}}}) = \rho_{E_2}(G_{K^{\mathrm{cyc}}}) = \mathrm{SL}(2, \widehat{\mathbb{Z}})$,

then $\# \pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty]) = 1$.

Proof Suppose that there exists $a \in \pi_1(E_1^*[n_1]) \cap \pi_2(E_2^*[n_2])$ for some $n_1, n_2 > 1$. By assumption (C), $G_{K^{\mathrm{cyc}}}$ transitively acts on $\pi_i(E_i^*[n_i])$, which is therefore the orbit of a, and the degree of a is given by $D(n_i)$. We also have the exact sequence

$$1 \rightarrow G_{K^{\mathrm{cyc}}(\pi_i(E_i^*[n_i]))} \rightarrow G_{K^{\mathrm{cyc}}} \rightarrow \mathrm{PSL}(2, \mathbb{Z}/n_i\mathbb{Z}) \rightarrow 1,$$

as a consequence,

$$[K^{\mathrm{cyc}}(\text{orbit of } a):K^{\mathrm{cyc}}(a)] = \frac{[G_{K^{\mathrm{cyc}}}:G_{K^{\mathrm{cyc}}(\text{orbit of } a)}]}{[K^{\mathrm{cyc}}(a):K^{\mathrm{cyc}}]} = \frac{\# \mathrm{PSL}(2, \mathbb{Z}/n_i\mathbb{Z})}{D(n_i)} = n_i,$$

which implies that $n_1 = n_2$, hence contradicts (A) and (B). $\qquad\square$

For any $\sigma \in G_K$, $\sigma(\sqrt{\Delta}) = \epsilon(\rho_E(\sigma))\sqrt{\Delta}$, where

$$\epsilon: \ \mathrm{GL}(2, \widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) \rightarrow \{\pm 1\}$$

is the signature character. If $K = \mathbb{Q}$, then $\sqrt{\Delta} \in \mathbb{Q}^{ab} = \mathbb{Q}^{\mathrm{cyc}}$, so $\rho_E(G_{\mathbb{Q}^{\mathrm{cyc}}}) \subseteq \mathrm{SL}(2, \widehat{\mathbb{Z}}) \cap \ker(\epsilon)$, a subgroup of index 2 in $\mathrm{SL}(2, \widehat{\mathbb{Z}})$. Jones [6] proved that for almost all elliptic curves defined over $\mathbb{Q}$, this is actually an equality, namely, $\rho_E(G_{\mathbb{Q}^{\mathrm{cyc}}}) = \mathrm{SL}(2, \widehat{\mathbb{Z}}) \cap \ker(\epsilon)$.

Theorem 3.2 *Given* (E_1, O_1, π_1) *and* (E_2, O_2, π_2), *all defined over* $\mathbb{Q}$, *if*

(A) $\pi_1(O_1) = \pi_2(O_2)$,
(B) *Corollary* 2.4 *does not hold*,
(C) $\rho_{E_1}(G_{K^{\mathrm{cyc}}}) = \rho_{E_2}(G_{K^{\mathrm{cyc}}}) = \mathrm{SL}(2, \widehat{\mathbb{Z}}) \cap \ker(\epsilon)$,

then $\# \pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty]) = 1$.

Proof The proof is nearly the same as the case $K \neq \mathbb{Q}$, except that

$$[\mathbb{Q}^{\mathrm{cyc}}(\text{orbit of } a):\mathbb{Q}^{\mathrm{cyc}}(a)] = \begin{cases} n_i & \text{if } n_i \text{ is odd,} \\ n_i/2 & \text{if } n_i \text{ is even.} \end{cases}$$

If $n_1 \neq n_2$, then $n_1 = n_2/2$ is odd, which implies $D(n_1) = D(n_2)/3$, a contradiction. $\qquad\square$

Remark 3.3 If Question 2.6 has an affirmative answer, then assumption (C) in Theorems 3.1 and 3.2 can be weakened by assuming that G_K acts on $\pi_i(E_i^*[n_i])$ transitively. This suggests that our Conjecture 1.2, apparently an unlikely intersection type problem [15], might be somewhat related to Serre's uniformity conjecture [11].

With the condition $\pi_1(O_1) = \pi_2(O_2)$ dropped, more intersection points can be obtained. We begin with the classical results for 3-torsion points and 4-torsion points.

Proposition 3.4 *For any elliptic curve E defined over K, there exists an even morphism $\pi \in \overline{K}(E)$ of degree 2 such that $\pi(E^*[3]) = \{\infty, 1, \rho, \rho^2\}$, where ρ is a primitive cube root of unity.*

Proof Consider the family $E_\lambda: x^3 + y^3 + z^3 = 3\lambda xyz$, which is an elliptic curve provided $\lambda^3 \neq 1$. Its 3-torsion points are

$$
\begin{array}{lll}
(1:-1:0), & (1:-\rho:0), & (1:-\rho^2:0), \\
(0:1:-1), & (0:1:-\rho), & (0:1:-\rho^2), \\
(-1:0:1), & (-\rho:0:1), & (-\rho^2:0:1).
\end{array}
$$

If we take the origin to be $O_\lambda = (1:-1:0)$, then the projection map $\pi_\lambda: E_\lambda \to \mathbb{P}^1$, $(x:y:z) \mapsto -(x+y)/z$ maps $E_\lambda^*[3]$ to the desired set. Since every elliptic curve defined over K can be transformed to some E_λ via an isomorphism defined over $\overline{K}$, the conclusion follows. $\qquad\square$

Proposition 3.5 *For any elliptic curve E defined over K, there exists an even morphism $\pi \in \overline{K}(E)$ of degree 2 such that $\pi(E^*[4]) = \{0, \infty, \pm 1, \pm i\}$, where i is a primitive fourth root of unity.*

Proof Consider the family $E_\delta: y^2 = x^4 - (\delta^2 + 1/\delta^2)x^2 + 1$, which is a curve of genus 1 with a unique singularity at $(0:1:0)$ provided $\delta^4 \neq 0, 1$. Its 2-torsion points $(\pm \delta^{\pm 1}, 0)$ respectively induce $x \mapsto \pm x^{\pm 1} \in \mathrm{Aut}(\mathbb{P}^1)$ if we take $O_\delta = (\delta, 0)$, and $\pi_\delta: E_\delta \to \mathbb{P}^1$, $(x, y) \mapsto x$. The fixed points of those nontrivial ones, $\{0, \infty\}$, $\{\pm 1\}$, and $\{\pm i\}$, therefore constitute the collection of $\pi_\delta(E_\delta^*[4])$. Since every elliptic curve defined over K can be transformed to some E_δ via a birational isomorphism defined over $\overline{K}$, the conclusion follows. $\qquad\square$

Propositions 3.4 and 3.5 indicate that for any elliptic curve, the projective 3-torsion points are equivalent to the vertices of a regular tetrahedron, while the projective 4-torsion points are equivalent to the vertices of a regular octahedron. It is therefore tempting to guess the projective 5-torsion points are equivalent to the vertices of a regular icosahedron. However, this is not the case. Following Klein [7], consider the family

$$
\begin{aligned}
E_{s,t}: y^2 = x^3 &- 3\left(s^{20} + 228 s^{15} t^5 + 494 s^{10} t^{10} - 228 s^5 t^{15} + t^{20}\right)x \\
&+ 2\left(s^{30} - 522 s^{25} t^5 - 10005 s^{20} t^{10} - 10005 s^{10} t^{20} + 522 s^5 t^{25} + t^{30}\right).
\end{aligned}
$$

Its projective 5-torsion points can be explicitly expressed as

$$
x_\infty^+ = -\left[\left(5 + \frac{6}{\sqrt{5}}\right) s^{10} - \frac{66}{\sqrt{5}} s^5 t^5 + \left(5 - \frac{6}{\sqrt{5}}\right) t^{10}\right],
$$

$$x_\infty^- = -\left[\left(5 - \frac{6}{\sqrt{5}}\right)s^{10} + \frac{66}{\sqrt{5}}s^5 t^5 + \left(5 + \frac{6}{\sqrt{5}}\right)t^{10}\right],$$

$$x_k^+ = \left(s^{10} + 30s^5 t^5 + t^{10}\right) + \left(12s^9 t + 24s^4 t^6\right)\omega^k$$
$$+ \left(24s^8 t^2 - 12s^3 t^7\right)\omega^{2k} + \left(36s^7 t^3 + 12s^2 t^8\right)\omega^{3k} + 60s^6 t^4 \omega^{4k},$$

$$x_k^- = \left(s^{10} - 30s^5 t^5 + t^{10}\right) + \left(24s^6 t^4 - 12st^9\right)\omega^k$$
$$+ \left(12s^7 t^3 + 24s^2 t^8\right)\omega^{2k} + \left(12s^8 t^2 - 36s^3 t^7\right)\omega^{3k} + 60s^4 t^6 \omega^{4k},$$

where ω is a primitive fifth root of unity, and $k \in \mathbb{Z}/5\mathbb{Z}$. Since the cross ratio

$$\frac{(x_\infty^+ - x_0^-)(x_0^+ - x_\infty^-)}{(x_\infty^+ - x_\infty^-)(x_0^+ - x_0^-)}$$
$$= \frac{(s^2 - st + (3 - \sqrt{5})t^2/2)(s^2 + (3 + \sqrt{5})st/2 + (3 + \sqrt{5})t^2/2)}{\sqrt{5}\,st\,(s^2 - st - t^2)}$$

is not a constant, the projective 5-torsion points are not equivalent to any fixed collection of 12 points.

Although any single $\pi(E^*[2])$, $\pi(E^*[3])$, or $\pi(E^*[4])$ is insufficient to determine $\pi(E[\infty])$, any pair of them can do so.

Corollary 3.6 *Given (E_1, O_1, π_1) and (E_2, O_2, π_2), if*

(A) $\pi_1(E_1^*[2]) = \pi_2(E_2^*[2])$ *and* $\pi_1(E_1^*[3]) = \pi_2(E_2^*[3])$, *or*
(B) $\pi_1(E_1^*[2]) = \pi_2(E_2^*[2])$ *and* $\pi_1(E_1^*[4]) = \pi_2(E_2^*[4])$, *or*
(C) $\pi_1(E_1^*[3]) = \pi_2(E_2^*[3])$ *and* $\pi_1(E_1^*[4]) = \pi_2(E_2^*[4])$,

then $\pi_1(O_1) = \pi_2(O_2)$. In particular, Corollary 2.4 holds.

Proof (A) It suffices to show that $\pi(E^*[2])$ and $\pi(E^*[3])$ determine $\pi(O)$. By Proposition 3.4, we can assume $\pi(E^*[3]) = \{\infty, 1, \rho, \rho^2\}$. Let $\lambda = \pi(O)$, and consider $(E_\lambda, O_\lambda, \pi_\lambda)$. Since

$$\pi_\lambda\colon E_\lambda \to \mathbb{P}^1, \qquad (x:y:z) \mapsto -\frac{x+y}{z} = \frac{z^2 - 3\lambda xy}{x^2 - xy + y^2},$$

we have $\pi_\lambda(O_\lambda) = \lambda$. By Corollary 2.4, $\pi_\lambda(E_\lambda^*[2]) = \pi(E^*[2])$. Thus we just need to show that $\pi_\lambda(E_\lambda^*[2])$ determines λ. Since the points in $\pi_\lambda(E_\lambda^*[2])$ are the roots of $x^3 + 3\lambda x^2 - 4$, this is clear.

(B) $\pi_\delta(E_\delta^*[2]) = \{-\delta, 1/\delta, -1/\delta\}$ determines δ.

(C) We need to show that $\pi_\delta(E_\delta^*[3])$ determines δ. The nonsingular model of E_δ is

$$E_\delta^{ns}\colon Y^2 = X(X - 1)\left(X - \frac{1}{4}\left(\delta + \frac{1}{\delta}\right)^2\right),$$

where

$$X = \frac{(\delta^2 + 1)(\delta x - 1)}{2\delta(x - \delta)}, \qquad Y = \frac{(\delta^4 - 1)y}{4\delta(x - \delta)^2}.$$

The division polynomials of E_δ^{ns} imply the division polynomials of E_δ via this birational isomorphism. In particular, the points in $\pi_\delta(E_\delta^*[3])$ are the roots of $x^4 + 2\delta x^3 - (2/\delta)x - 1$, then the result is immediate. $\qquad\square$

Now we are ready to give the main result of this article. For any E_{δ_1} and E_{δ_2}, the intersection of $\pi_{\delta_1}(E_{\delta_1}[\infty])$ and $\pi_{\delta_2}(E_{\delta_2}[\infty])$ has at least six elements. If it contains another element a, then as we have seen in the proof of Proposition 3.5, it also contains $-a, 1/a$, and $-1/a$. Therefore, its cardinality must be $4k + 6$. If we fix δ_1 and vary δ_2, then $k = 1$ can be easily attained. In the next theorem, we construct an example to improve $k = 2$.

Theorem 3.7 sup $(\# \pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])) \geqslant 14$, where supremum is taken over $(K, E_1, O_1, \pi_1, E_2, O_2, \pi_2)$ such that $\pi_1(E_1[2]) \neq \pi_2(E_2[2])$.

Proof From the division polynomials of E_δ^{ns}, we know that the third and fifth primitive division polynomials of E_δ are

$$\widetilde{F_3}(x, \delta) = 2x^3\delta^2 + (x^4 - 1)\delta - 2x,$$
$$\widetilde{F_5}(x, \delta) = 8x^5\delta^6 - 4x^6(x^4 - 1)\delta^5 - 2x^3(x^8 + 6x^4 + 5)\delta^4$$
$$+ (x^{12} + 5x^8 - 5x^4 - 1)\delta^3 + 2x(5x^8 + 6x^4 + 1)\delta^2$$
$$- 4x^2(x^4 - 1)\delta - 8x^7.$$

Now we want to find δ_1 and δ_2 such that there exist $u \in \pi_{\delta_1}(E_{\delta_1}^*[3]) \cap \pi_{\delta_2}(E_{\delta_2}^*[3])$, and $v \in \pi_{\delta_1}(E_{\delta_1}^*[5]) \cap \pi_{\delta_2}(E_{\delta_2}^*[5])$. In other words, $\widetilde{F_3}(u, \delta_1) = \widetilde{F_3}(u, \delta_2) = 0$, and $\widetilde{F_5}(v, \delta_1) = \widetilde{F_5}(v, \delta_2) = 0$. Since $\widetilde{F_3}(x, \delta)$ is a quadratic polynomial in δ, any fixed u such that $u^4 \neq 0, 1$, and $u^8 + 14u^4 + 1 \neq 0$ gives exactly two roots satisfying $\delta_1^4, \delta_2^4 \neq 0, 1$, and $\delta_1 \neq \pm\delta_2^{\pm 1}$. Since δ_1 and δ_2 are also two roots of $\widetilde{F_5}(v, \delta) = 0$, we have $\widetilde{F_3}(u, \delta) | \widetilde{F_5}(v, \delta)$ as polynomials in δ. By long division, this is equivalent to require

$$C_0: \quad u^{15}v^{10} - u^{14}v^{11} - u^{13}v^{12} + u^{16}v^5 - u^{15}v^6 - 22u^{14}v^7 - 5u^{13}v^8$$
$$+ 20u^{12}v^9 + 5u^{11}v^{10} - 2u^{10}v^{11} + u^9v^{12} - 5u^{14}v^3 + 5u^{13}v^4$$
$$+ 32u^{12}v^5 - 5u^{11}v^6 - 12u^{10}v^7 + 5u^9v^8 - 5u^7v^{10} - u^6v^{11}$$
$$+ u^{13} + 4u^{12}v - 10u^{10}v^3 - 5u^9v^4 - 2u^8v^5 + 5u^7v^6$$
$$- 6u^6v^7 - u^3v^{10} - u^9 - 5u^6v^3 + 8u^4v^5 + u^3v^6 + v^5 = 0,$$

$$C_1: \quad u^{19}v^{10} - u^{18}v^{11} - u^{17}v^{12} + u^{20}v^5 - u^{19}v^6 - 6u^{18}v^7 - 5u^{17}v^8$$
$$+ 20u^{16}v^9 + 8u^{15}v^{10} - 5u^{14}v^{11} - 2u^{13}v^{12} - 5u^{18}v^3 + 5u^{17}v^4$$
$$+ 35u^{16}v^5 + 8u^{15}v^6 - 30u^{14}v^7 - 10u^{13}v^8 - 20u^{12}v^9 - 2u^{11}v^{10}$$
$$+ 5u^{10}v^{11} - u^9v^{12} + u^{17} + 4u^{16}v - 16u^{15}v^2 - 25u^{14}v^3$$
$$+ 10u^{13}v^4 - 14u^{12}v^5 + 2u^{11}v^6 + 30u^{10}v^7 - 5u^9v^8 + 8u^7v^{10}$$
$$+ u^6v^{11} + 2u^{13} - 4u^{12}v + 25u^{10}v^3 + 5u^9v^4 - 10u^8v^5 - 8u^7v^6$$

$$+ 6u^6v^7 + u^3v^{10} + u^9 + 5u^6v^3 - 11u^4v^5 - u^3v^6 - v^5 = 0.$$

Consider C_0 and C_1 as polynomials in v, then their resultant is

$$-2^{48}u^{204}(u^4 - 1)^{36}$$
$$\cdot \left(32u^{24} + 1369u^{20} + 18812u^{16} + 90646u^{12} + 18812u^8 + 1369u^4 + 32\right),$$

whose roots are the u-coordinates of their common points. Let u such that $u^4 \neq 0, 1$ be any nontrivial root, (u, v) the corresponding common point, δ_1 and δ_2 the roots of $\widetilde{F}_3(u, \delta) = 0$, then we have

$$\pi_{\delta_1}(E_{\delta_1}[2]) \neq \pi_{\delta_2}(E_{\delta_2}[2]), \qquad \pi_{\delta_1}(E^*_{\delta_1}[4]) = \pi_{\delta_2}(E^*_{\delta_2}[4]) = \{0, \infty, \pm 1, \pm i\},$$
$$u \in \pi_{\delta_1}(E^*_{\delta_1}[3]) \cap \pi_{\delta_2}(E^*_{\delta_2}[3]), \qquad -u, 1/u, -1/u \in \pi_{\delta_1}(E^*_{\delta_1}[6]) \cap \pi_{\delta_2}(E^*_{\delta_2}[6]),$$
$$v \in \pi_{\delta_1}(E^*_{\delta_1}[5]) \cap \pi_{\delta_2}(E^*_{\delta_2}[5]), \qquad -v, 1/v, -1/v \in \pi_{\delta_1}(E^*_{\delta_1}[10]) \cap \pi_{\delta_2}(E^*_{\delta_2}[10]),$$

so the supremum is at least 14.   □

Remark 3.8 After submitting this article, we have successfully improved the previous result from 14 points (using 3-torsion points and 5-torsion points) to 22 points (using 3-torsion points and 7-torsion points). We will give full details in the next publication.

Remark 3.9 The intersection can also be investigated using Tate's explicit parametrization of elliptic curves over p-adic fields [12]. We plan to explore the details of this approach in the future.

Appendix: Jordan's totient function

We are concerned with the values taken by $J_k(n)$ as well. $J_1(n)$ is simply Euler's totient function, for which we have the famous Ford's theorem [4] and Carmichael's conjecture [2,3]. $J_2(n)$ is far from being injective, which prevents a simple answer to Question 2.6. Even their combination is not injective, since

$$J_1(15) = J_1(16) = 8, \qquad J_2(15) = J_2(16) = 192.$$

It is quite surprising that $J_3(n)$ is still not injective, the smallest identical pair is

$$J_3(28268) = J_3(28710) = 19764446869440.$$

We do not know any identical pair for $k \geqslant 4$, and expect that such coincidence should be very rare.

Finally, let us conclude this article with a collection of partial results:

Proposition 4.1 *Let p, q, $p_1 \neq p_2$, $q_1 \neq q_2$ be primes, $v_p(n)$ the power of p in the prime decomposition of n, $\omega(n)$ the number of distinct prime divisors of n, then*

(A) *If $J_2(p^s) = J_2(q^t)$, then $p^s = q^t$ or $\{p^s, q^t\} = \{7, 8\}$.*

(B) *If $J_k(p_1 p_2) = J_k(q_1 q_2)$, $k = 2, 4$, then $p_1 p_2 = q_1 q_2$.*

(C) *If $J_k(m) = J_k(n)$, $k = 2, 4, 6$, then $v_p(m) = v_p(n)$ for $p = 2, 3$, $v_p(m) = v_p(n)$ or $\{v_p(m), v_p(n)\} = \{0, 1\}$ for any other $p \not\equiv 1 \bmod 12$, and $\omega(m) = \omega(n)$.*

(D) *If $J_k(m) = J_k(n)$ for infinitely many k, then $m = n$.*

Proof (A) Now we have $p^{2s-2}(p^2 - 1) = q^{2t-2}(q^2 - 1)$. If $p, q \neq 2$ and $s, t \neq 1$, then p (resp. q) is the largest prime divisor of left-hand side (resp. right-hand side). Hence $p = q$ and $s = t$. If $p = 2$, then $3 \cdot 2^{2s-2} = q^{2t-2}(q^2 - 1)$. Since 4 cannot be a common divisor of $q + 1$ and $q - 1$, one of them must be a divisor of 6. Hence $q = 2$ and $s = t$, or $\{p^s, q^t\} = \{7, 8\}$. If $s = 1$, then $p^2 - 1 = q^{2t-2}(q^2 - 1)$. We can assume $q \neq 2$, then q cannot be a common divisor of $p + 1$ and $p - 1$, so $q^{2t-2} \leqslant p \pm 1 = (p \mp 1) \pm 2 \leqslant (q^2 - 1) \pm 2$, so $t = 1$ and $p = q$, or $t = 2$. If $t = 2$, then either $q^2 = p + 1 = (p - 1) + 2 = (q^2 - 1) + 2$ or $2q^2 \leqslant p + 1 = (p - 1) + 2 \leqslant (q^2 - 1)/2 + 2$, neither is possible.

(B) It is straightforward that $(p_1^2 - 1)(p_2^2 - 1) = (q_1^2 - 1)(q_2^2 - 1)$ and $(p_1^4 - 1)$ $\cdot (p_2^4 - 1) = (q_1^4 - 1)(q_2^4 - 1)$ imply $p_1 p_2 = q_1 q_2$.

(C) Since $2 \nmid p^4 + p^2 + 1 = (p^2 + p + 1)(p^2 - p + 1)$, from $J_6(n)/J_2(n) = \prod_{p|n} p^{4v_p(n)-4}(p^4 + p^2 + 1)$, we can see $v_2(m) = v_2(n)$ or $\{v_2(m), v_2(n)\} = \{0, 1\}$. Since $3 \nmid p^2 + 1$, from $J_4(n)/J_2(n) = \prod_{p|n} p^{2v_p(n)-2}(p^2 + 1)$, we can see $v_3(m) = v_3(n)$ or $\{v_3(m), v_3(n)\} = \{0, 1\}$. This strategy works for any other $p \not\equiv 1 \bmod 12$, since either -1 or -3 is a quadratic nonresidue. If $v_2(m) = 0$ and $v_2(n) = 1$, then $5/3 = (2^2 + 1)/(2^2 - 1) \leqslant J_4(n)/J_2^2(n) = J_4(m)/J_2^2(m) \leqslant \prod_{p \geqslant 3}(p^2 + 1)/(p^2 - 1) = 3/2$, a contradiction. If $v_3(m) = 0$ and $v_3(n) = 1$, then $5/4 = (3^2 + 1)/(3^2 - 1) \leqslant J_4(n)/J_2^2(n) = J_4(m)/J_2^2(m) \leqslant \prod_{p \geqslant 5}(p^2 + 1)/(p^2 - 1) = 6/5$, again a contradiction. Moreover, since $2 | p^2 + 1$, but $4 \nmid p^2 + 1$, from $J_4(n)/J_2(n)$, we can see $\omega(m) = \omega(n)$.

(D) Assume $k > 1$, then $m^k/\zeta(k) < J_k(m) = J_k(n) \leqslant n^k$, thus $\zeta(k)^{-1/k} < m/n < \zeta(k)^{1/k}$ by symmetry. Since $\zeta(k)^{1/k} \to 1$ as $k \to \infty$, we have $m = n$. $\qquad \square$

References

1. Bogomolov, F., Tschinkel, Yu.: Algebraic varieties over small fields. In: Zannier, U. (ed.) Diophantine Geometry. CRM Series, vol. 4, pp. 73–91. Edizioni della Normale, Pisa (2007)
2. Carmichael, R.D.: On Euler's ϕ-function. Bull. Amer. Math. Soc. **13**(5), 241–243 (1907)
3. Carmichael, R.D.: Note on Euler's φ-function. Bull. Amer. Math. Soc. **28**(3), 109–110 (1922)
4. Ford, K.: The number of solutions of $\phi(x) = m$. Ann. Math. **150**(1), 283–311 (1999)
5. Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer, New York (1977)
6. Jones, N.: Almost all elliptic curves are Serre curves. Trans. Amer. Math. Soc. **362**(3), 1547–1570 (2010)
7. Klein, F.: Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree, 2nd edn. Dover, New York (1956)
8. McKee, J.: Computing division polynomials. Math. Comput. **63**(208), 767–771 (1994)
9. Neukirch, J.: Class Field Theory. Grundlehren der Mathematischen Wissenschaften, vol. 280. Springer, Berlin (1986)
10. Raynaud, M.: Courbes sur une variété abélienne et points de torsion. Invent. Math. **71**(1), 207–233 (1983)

11. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
12. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 151. Springer, New York (1994)
13. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106, 2nd edn. Springer, Dordrecht (2009)
14. Wolfram Research, Inc. Mathematica, Version 10.0. Champaign, IL (2014)
15. Zannier, U.: Some Problems of Unlikely Intersections in Arithmetic and Geometry. Annals of Mathematics Studies, vol. 181. Princeton University Press, Princeton (2012)
16. Zywina, D.: Elliptic curves with maximal Galois action on their torsion points. Bull. London Math. Soc. **42**(5), 811–826 (2010)