THE SMALLEST INVARIANT FACTOR OF ELLIPTIC CURVES, AND COINCIDENCES

ALEXANDER MILNER AND JACK SHOTTON

Abstract. For an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ and a natural number j, Cojocaru has shown that there is an explicit constant $\mathcal{C}_{\mathcal{E},j}$ giving (under GRH) the density of primes p of good reduction such that the smallest invariant factor of $\mathcal{E}(\mathbb{F}_p)$ is j. For $\mathcal{E}$ without complex multiplication, we study the question of when $\mathcal{C}_{\mathcal{E},j}$ is positive (a necessary and, on GRH, sufficient condition for there to be infinitely many such p), strengthening the main result of [Kim15]. Our arguments are group-theoretic using the image of the adelic Galois representation of $\mathcal{E}$. Experimentally, $\mathcal{C}_{\mathcal{E},j}$ appears to vanish only when there is a coincidence of division fields; we document a number of families of such coincidences arising from abelian division fields.

1. Introduction

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}$ without complex multiplication, and let p be a prime of good reduction for $\mathcal{E}$. Then $\mathcal{E}(\mathbb{F}_p)$ is an abelian group that is a product of at most two cyclic groups, and so we may write

$$\mathcal{E}(\mathbb{F}_p) \cong \mathbb{Z}/d_{\mathcal{E},p}\mathbb{Z} \times \mathbb{Z}/e_{\mathcal{E},p}\mathbb{Z}$$

where $d_{\mathcal{E},p}, e_{\mathcal{E},p} \in \mathbb{N}$ with $d_{\mathcal{E},p} \mid e_{\mathcal{E},p}$. Thus $d_{\mathcal{E},p} = 1$ if and only if $\mathcal{E}(\mathbb{F}_p)$ is cyclic. We can ask how often, as p varies, $d_{\mathcal{E},p}$ takes a given value, and a conditional answer is given by Cojocaru.

Theorem 1.1 ([Coj04], Theorem 2)**.** *Let j be a positive integer. Under the generalised Riemann hypothesis (GRH) for the Dedekind zeta functions of the division fields $\mathbb{Q}(\mathcal{E}[n])$ of $\mathcal{E}$,*

$$\#\{p \leq x : d_{\mathcal{E},p} = j\} \sim \mathcal{C}_{\mathcal{E},j}\, Li(x)$$

where

$$\mathcal{C}_{\mathcal{E},j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\mathcal{E}[jk]) : \mathbb{Q}]}.$$

(Here μ is the Möbius function).

In fact, the same statement also holds if $\mathcal{E}$ has complex multiplication, and the GRH is then not required (see [Mur83]). We will only consider the case of elliptic curves without complex multiplication.

As stated, this theorem does not address the issue of whether $\mathcal{C}_{\mathcal{E},j} > 0$ — that is, whether (conditionally) there are infinitely many p with the smallest invariant factor of $\mathcal{E}(\mathbb{F}_p)$ equal to j.[1] Indeed, it is in fact possible that $\mathcal{C}_{\mathcal{E},j} = 0$, even if $j = 1$: if $\mathcal{E}$ has full rational 2-torsion, then $2 \mid d_{\mathcal{E},p}$ for all p. For $j = 1$ this is the only obstruction:

[1] If $\mathcal{C}_{\mathcal{E},j} = 0$ then it is easy to show $d_{\mathcal{E},p} \neq j$ for all but finitely many p, see Proposition 2.8 below.

Theorem 1.2 ([Ser86, Theorem 1.1])**.** *Suppose that* $\mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q}$*. Then*

$$\mathcal{C}_{\mathcal{E},1} > 0.$$

Remark 1.3. The statement also holds in the case that $\mathcal{E}$ has complex multiplication.

Remark 1.4. The theorem is due to Serre, but the proof is unpublished. In [GM90, Theorem 1] it is shown unconditionally that, if $\mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q}$, then $\mathcal{E}(\mathbb{F}_p)$ is cyclic for infinitely many p. This implies Theorem 1.2, by Proposition 2.8 below.

Another proof of Theorem 1.2 is given in [CM04, Section 6]. This proof contains a small error which we explain and correct in Section 5. Our main result also gives an alternative proof of Theorem 1.2.

In [Kim15], Kim proves[2] that the conclusion of Theorem 1.2 holds as long as j is coprime to the *adelic level* $m_{\mathcal{E}}$ of $\mathcal{E}$, the minimal integer such that the image of the adelic Galois representation of $\mathcal{E}$ is the full pre-image of a subgroup of $GL_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z})$. If $A(\mathcal{E})$ is the product of the primes such that the p-adic Galois representation associated to $\mathcal{E}$ is not surjective and $N_{\mathcal{E}}$ is the conductor of $\mathcal{E}$, then the prime factors of $m_{\mathcal{E}}$ divide $2N_{\mathcal{E}}A(\mathcal{E})$; see Proposition 2.9.[3] In Corollary 3.7, we prove the following generalisation of Kim's result.

Theorem 1.5. *Suppose that* j *is coprime to* $2A(\mathcal{E})$ *and that* $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j])$*. Then*

$$\mathcal{C}_{\mathcal{E},j} > 0.$$

In fact, we prove something stronger which allows us to handle some cases where j and $2A(\mathcal{E})$ have common factors. See Theorem 3.2 and the examples that follow. It is an interesting question, related to 'entanglements' and 'coincidences' of division fields, to classify all pairs $\mathcal{E}, j$ with $\mathcal{C}_{\mathcal{E},j} = 0$. We give some examples in Section 4. These examples all arise from coincidences $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[jp])$ with $p = 2$ or $p = 3$ and we conjecture that this is the only way that $\mathcal{C}_{\mathcal{E},j}$ can vanish.

Coincidences of division fields have recently been studied in (for example) [DLR23], [Yvo25], and [DR26]. In Section 4 we define a p-coincidence to be one of the form $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[jp])$ and conjecture that, for non-CM elliptic curves over $\mathbb{Q}$, p-coincidences occur only for $p = 2$ and $p = 3$. In Section 4.1 we document some infinite families of examples of p-coincidences stemming from elliptic curves with abelian mod n Galois representations for $n = 2, 3, 4$, and 8; in Section 4.2 we give a few sporadic examples that we found interesting.

We restrict attention to elliptic curves over $\mathbb{Q}$, although many of our results would continue to hold over number fields containing no nontrivial abelian extension of $\mathbb{Q}$. The vanishing of $\mathcal{C}_{\mathcal{E},1}$ for elliptic curves over number fields has been studied in [CS23], while coincidences over number fields are the subject of [Yvo25].

1.1. **Notation.** We summarise some of the key notation used throughout this paper:

- We let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}$ without complex multiplication.

[2]Kim states that this result is conditional on the GRH, but in fact his result only requires Theorem 1.2 which holds unconditionally if $\mathcal{C}_{\mathcal{E},j}$ is defined as an infinite sum.

[3]This definition of $A(\mathcal{E})$ has the same prime factors as that in [DG22] and differs from that of [CK05] by (perhaps) factors of 30. It is unclear what definition of $A(\mathcal{E})$ is used in [Kim15], but what is actually proved is the result as stated here in terms of the adelic level.

- We write $N_{\mathcal{E}}$ for the conductor of $\mathcal{E}$, and $m_{\mathcal{E}}$, $A(\mathcal{E})$ for its *adelic level* and *Serre constant* (defined in Section 2 below).
- We let ρ_n (for $n \in \mathbb{N}$) and ρ be the mod n and adelic Galois representations associated to $\mathcal{E}$ (defined in Section 2 below).
- We write μ for the Möbius function.
- For a positive integer b, let $\mathrm{rad}(b)$ be its radical and let $\langle b \rangle$ be the set of integers all of whose prime factors divide b.
- For a group G let $[G, G]$ be its commutator subgroup.
- The cardinality of the group $GL_2(\mathbb{Z}/n\mathbb{Z})$ is given by

$$\psi(n) = |GL_2(\mathbb{Z}/n\mathbb{Z})| = n^4 \prod_{p|n} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right).$$

1.2. **Acknowledgments and data availability.** AM was funded by a London Mathematical Society Undergraduate Research Bursary [grant reference URB-2023-11], by Durham University and by a studentship from the University of Edinburgh. In the final stages of preparing this article, JS was supported by the Engineering and Physical Sciences Research Council [grant number UKRI1020].

We thank Harris Daniels for useful conversations on the topic of this paper.

Supporting code is available at https://github.com/jackshotton/invariant-factors-public. Much of this code was produced with the assistance of GPT-5.4, including that used for the analysis of the explicit example in Section 4.1.1.

All data used in this work is freely available from the L-functions and Modular Forms Database [LMFDB].

1.3. **Compliance with ethical standards.** We declare no conflicts of interest.

2. Galois images

Associated to $\mathcal{E}$, we have the *adelic Tate module*

$$T(\mathcal{E}) = \varprojlim_n \mathcal{E}[n].$$

It is a free $\hat{\mathbb{Z}}$-module of rank 2, and we will fix a choice of basis. We then obtain a continuous representation

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\hat{\mathbb{Z}})$$

where $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$. Let

$$H = \mathrm{im}(\rho) \subset GL_2(\hat{\mathbb{Z}}).$$

For each $n \in \mathbb{N}$, let

$$\rho_n : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$$

be the mod-n reduction of ρ. We introduce the following notation:

- $\mathrm{mod}_n : GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ is the reduction mod n map;
- $\Gamma_n = \ker(\mathrm{mod}_n)$;
- for $G \subset GL_2(\hat{\mathbb{Z}})$, $G \bmod n = \mathrm{mod}_n(G)$;

If $G \subset GL_2(\hat{\mathbb{Z}})$ is an open subset, the *level* of G is the least integer m such that $\Gamma_m \subset G$. We note now, and use without comment, that if $A, B \subset GL_2(\hat{\mathbb{Z}})$ are subsets that both contain the same Γ_m, then $A \cup B \bmod m = A \bmod m \cup B \bmod m$, and similarly for intersections.

As $\mathcal{E}$ does not have complex multiplication, H is open by [Ser72, Théorème 3], and we define the *adelic level* $m_{\mathcal{E}}$ of $\mathcal{E}$ to be the level of H. For $k \in \mathbb{N}$ we have

$$[\mathbb{Q}(\mathcal{E}[k]) : \mathbb{Q}] = |\rho_k(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))| = |H \bmod k| = |H/H \cap \Gamma_k|.$$

As in Theorem 1.1, for $j \in \mathbb{N}$ we define

$$\mathcal{C}_{\mathcal{E},j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\mathcal{E}[jk]) : \mathbb{Q}]}.$$

The sum is absolutely convergent, as Serre's open image theorem implies that $[\mathbb{Q}(\mathcal{E}[k]) : \mathbb{Q}] \asymp \psi(k) \asymp k^4$ for k squarefree.

Let $m \in \mathbb{N}$ be any integer divisible by the adelic level $m_{\mathcal{E}}$ (usually we will have $m = m_{\mathcal{E}}$).

Lemma 2.1. *Suppose that $k \in \mathbb{N}$ and that p is a prime such that $v_p(k) \geq v_p(m)$. Then*

$$|H \bmod pk| = |H \bmod k| \cdot \begin{cases} p^4 & \text{if } p \mid k \\ \psi(p) & \text{if } p \nmid k. \end{cases}$$

Proof. This is the *Claim* in [FK14] Section 7. □

Proposition 2.2. *Let $j \in \mathbb{N}$. Let S be the set of prime numbers such that $v_p(j) < v_p(m)$. Then:*

$$\mathcal{C}_{\mathcal{E},j} = \sum_{k \in \langle S \rangle} \frac{\mu(k)}{|H \bmod jk|} \prod_{p \notin S, p \mid j} \left(1 - \frac{1}{p^4}\right) \prod_{p \notin S, p \nmid j} \left(1 - \frac{1}{\psi(p)}\right). \tag{1}$$

Furthermore, $\mathcal{C}_{\mathcal{E},j} > 0$ if and only if $\mathcal{C}_{\mathcal{E},\gcd(j,m)} > 0$.

Proof. If $n \in \mathbb{N}$ is squarefree and of the form kn', where all the prime factors of k are in S and all the prime factors of n' are not in S, then by Lemma 2.1 we have

$$\frac{\mu(n)}{|H \bmod jn|} = \frac{\mu(k)}{|H \bmod jk|} \prod_{p \mid n', p \mid j} \frac{-1}{p^4} \prod_{p \mid n', p \nmid j} \frac{-1}{\psi(p)}.$$

The factorisation (1) follows.

As $\prod_p \left(1 - \frac{1}{\psi(p)}\right)$ is easily shown to be positive, we see that $\mathcal{C}_{\mathcal{E},j} > 0$ if and only if

$$\sum_{k \in \langle S \rangle} \frac{\mu(k)}{|H \bmod jk|} > 0.$$

If p is a prime that divides $\frac{j}{\gcd(j,m)}$ then $p \notin S$ and so, for any $k \in \langle S \rangle$, $v_p(jk) = v_p(j) > v_p(m)$. So, by (repeated application of) Lemma 2.1,

$$|H \bmod jk| = A|H \bmod \gcd(j,m)k|$$

for a positive integer A independent of k. Thus

$$\sum_{k \in \langle S \rangle} \frac{\mu(k)}{|H \bmod jk|} = \frac{1}{A} \sum_{k \in \langle S \rangle} \frac{\mu(k)}{|H \bmod \gcd(j,m)k|}.$$

Since $S = \{p : v_p(j) < v_p(m)\} = \{p : v_p(\gcd(j,m)) < v_p(m)\}$, this is positive if and only if $\mathcal{C}_{\mathcal{E},\gcd(j,m)} > 0$ and we obtain the last part of the proposition. □

In particular, if we are interested in when $\mathcal{C}_{\mathcal{E},j} > 0$, we may restrict attention to integers j that divide the adelic level $m_{\mathcal{E}}$.

Proposition 2.3. *Suppose that $j \mid m$ and let $S = \{p : p \mid m/j\}$. Then $\mathcal{C}_{\mathcal{E},j} = 0$ if and only if*

$$H \cap \Gamma_j \bmod m = \bigcup_{p \in S} H \cap \Gamma_{jp} \bmod m.$$

Proof. By Proposition 2.2, $\mathcal{C}_{\mathcal{E},j} = 0$ if and only if

$$\sum_{k \in \langle S \rangle} \frac{\mu(k)}{|H \bmod jk|} = 0.$$

Multiplying this by $|H \bmod j|$ we see that this is equivalent to

$$\sum_{k \in \langle S \rangle} \mu(k) \left| \frac{H \cap \Gamma_{jk}}{H \cap \Gamma_j} \right| = 0$$

and, since each $jk \mid m$, this is equivalent to

$$\sum_{k \in \langle S \rangle} \mu(k) \frac{|H \cap \Gamma_{jk} \bmod m|}{|H \cap \Gamma_j \bmod m|} = 0.$$

For each $k \in \langle S \rangle$ squarefree, $H \cap \Gamma_{jk} \bmod m = \bigcap_{p \mid k} H \cap \Gamma_{jp} \bmod m$ and so, by the inclusion-exclusion principle,

$$\sum_{k \in \langle S \rangle} \mu(k) \frac{|H \cap \Gamma_{jk} \bmod m|}{|H \cap \Gamma_j \bmod m|} = 1 - \frac{1}{|H \cap \Gamma_j \bmod m|} \left| \bigcup_{p \in S} H \cap \Gamma_{jp} \bmod m \right|.$$

The proposition follows. □

Corollary 2.4. *Suppose that $m_{\mathcal{E}} \mid j$. Then $\mathcal{C}_{\mathcal{E},j} > 0$.*

Proof. We may assume that $j = m_{\mathcal{E}}$ and take $m = m_{\mathcal{E}}$ in Proposition 2.3. Then the set S is empty and so $\mathcal{C}_{\mathcal{E},j} > 0$. □

Corollary 2.5. *Let $j \in \mathbb{N}$. If there exists a prime p such that $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[pj])$, then $\mathcal{C}_{\mathcal{E},j} = 0$.*

Proof. Take $m = m_{\mathcal{E}} jp$. As

$$H \cap \Gamma_j \bmod m = \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}(\mathcal{E}[j])),$$

and similarly for pj, the hypothesis implies that

$$H \cap \Gamma_j \bmod m = H \cap \Gamma_{pj} \bmod m$$

and so $\mathcal{C}_{\mathcal{E},j} = 0$ by Proposition 2.3. □

Based on numerical evidence, we make the following conjecture.

Conjecture 2.6. *Suppose that $\mathcal{E}$ is a non-CM elliptic curve over $\mathbb{Q}$ and that $\mathcal{C}_{\mathcal{E},j} = 0$. Then there exists a prime p such that $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[pj])$.*

Remark 2.7. Equalities $\mathbb{Q}(\mathcal{E}[a]) = \mathbb{Q}(\mathcal{E}[b])$ are called 'coincidences' in [DLR23]. For more discussion, see Section 4 below.

Proposition 2.8. *Suppose that $j \in \mathbb{N}$ and that $\mathcal{C}_{\mathcal{E},j} = 0$. If l is a prime of good reduction for $\mathcal{E}$, then $d_{\mathcal{E},l} \neq j$ unless $j = 1$ and $l = 2$.*

Proof. Let l be a prime of good reduction such that $d_{\mathcal{E},l} = j$. In particular, $(\mathbb{Z}/j\mathbb{Z})^2 \subset \mathcal{E}(\mathbb{F}_l)$ which implies that $l \nmid j$. Suppose that $\mathcal{C}_{\mathcal{E},j} = 0$.

Let $m = m_{\mathcal{E}} j$. Then, by Proposition 2.3,

$$H \cap \Gamma_j \bmod m = \bigcup_{p \mid m_{\mathcal{E}}} H \cap \Gamma_{jp} \bmod m.$$

Let $K = \mathbb{Q}(\mathcal{E}[m])$ so that $\mathrm{Gal}(K/\mathbb{Q}) = H \bmod m$. Fix a prime of K above l and let I_l and $\tilde{\mathrm{Frob}}_l$ be the inertia group and lift of a Frobenius element. Since l is a prime of good reduction and $l \nmid j$, $I_l \subset H \cap \Gamma_j \bmod m$ and $(\mathbb{Z}/j\mathbb{Z})^2 \subset \mathcal{E}(\mathbb{F}_l)$ if and only if $\tilde{\mathrm{Frob}}_l \in H \cap \Gamma_j \bmod m$. As $\mathcal{C}_{\mathcal{E},j} = 0$, we have $\tilde{\mathrm{Frob}}_l \in H \cap \Gamma_{jp} \bmod m$ for some p.

If $p = l$, suppose for now that l is odd. Then $\mathbb{Q}(\mathcal{E}[jl])/\mathbb{Q}(\mathcal{E}[j])$ is ramified at primes above l (since $\mathbb{Q}(\mathcal{E}[jl])$ contains ζ_l but $\mathbb{Q}(\mathcal{E}[j])$ is unramified at l). We may therefore choose $\tilde{\mathrm{Frob}}_l$ so that its image in $H \cap \Gamma_j / H \cap \Gamma_{jl}$ is nontrivial. For this choice of $\tilde{\mathrm{Frob}}_l$, we must therefore have $\tilde{\mathrm{Frob}}_l \in H \cap \Gamma_{jp} \bmod m$ for some $p \neq l$.

But now $(\mathbb{Z}/jp\mathbb{Z})^2 \subset \mathcal{E}(\mathbb{F}_l)$ and so $jp \mid d_{\mathcal{E},l}$. Therefore, if $j \mid d_{\mathcal{E},l}$ then $jp \mid d_{\mathcal{E},l}$ for some p and so $d_{\mathcal{E},l} \neq j$.

It remains to deal with the case $l = 2$. Since $|\mathcal{E}(\mathbb{F}_2)| \leq 5$ and $|\mathcal{E}(\mathbb{F}_2)[2]| \leq 2$, we must have $j = 1$. (By Theorem 1.2, this case occurs exactly when $\mathcal{E}$ has good reduction at 2 and full rational 2-torsion.) □

Associated to $\mathcal{E}$ we also have the integers $A(\mathcal{E})$, the product of all primes p such that the p-adic Galois representation $\varprojlim \rho_{p^n}$ is not surjective, and $N_{\mathcal{E}}$, the conductor of $\mathcal{E}$. In the next proposition, we relate primes dividing $A(\mathcal{E})$, $m_{\mathcal{E}}$ and $N_{\mathcal{E}}$. It may be well-known to experts, but we could not find a reference in the generality stated (including primes $p = 3, 5$).

Proposition 2.9. *Let j be a positive integer and p be a prime.*

(1) If $p \mid A(\mathcal{E})$ then $p \mid m_{\mathcal{E}}$.
(2) If $p \mid m_{\mathcal{E}}$ then $p \mid 2N_{\mathcal{E}}A(\mathcal{E})$.
(3) If $\gcd(j, 2A(\mathcal{E})) = 1$ then ρ_j is surjective.

Proof. (1) If $p \nmid m_{\mathcal{E}}$ then $\Gamma_{m_{\mathcal{E}}} \to GL_2(\mathbb{Z}_p)$ is surjective and so $p \nmid A(\mathcal{E})$.

(2) Suppose that $p \nmid 2N_{\mathcal{E}}A(\mathcal{E})$. We want to show that $p \nmid m_{\mathcal{E}}$. Let $m_{\mathcal{E}} = p^r m'$ with $p \nmid m'$. Then

$$H \bmod m_{\mathcal{E}} = \mathrm{im}(\rho_{m_{\mathcal{E}}}) \subset GL_2(\mathbb{Z}/p^r\mathbb{Z}) \times GL_2(\mathbb{Z}/m'\mathbb{Z})$$

where the projection to the first factor is surjective as $p \nmid A(\mathcal{E})$. Let $N \times \{I\}$ be the kernel of $H \bmod m_{\mathcal{E}} \to H \bmod m'$. The conclusion $p \nmid m_{\mathcal{E}}$ follows if we can show that $N = GL_2(\mathbb{Z}/p^r\mathbb{Z})$; so suppose that N is a proper subgroup.

We have that

$$\mathbb{Q}(\mathcal{E}[p^r])^N = \mathbb{Q}(\mathcal{E}[p^r]) \cap \mathbb{Q}(\mathcal{E}[m']) \subset \mathbb{Q}(\mathcal{E}[m'])$$

is unramified at p, as $p \nmid N_{\mathcal{E}}$ and $p \nmid m'$. As

$$\mathbb{Q}(\mathcal{E}[p^r])^{SL_2(\mathbb{Z}/p^r\mathbb{Z})} = \mathbb{Q}(\zeta_{p^r})$$

is totally ramified at p, we see that $N \cdot SL_2(\mathbb{Z}/p^r\mathbb{Z}) = GL_2(\mathbb{Z}/p^r\mathbb{Z})$.

Suppose first that $GL_2(\mathbb{Z}/p^r\mathbb{Z})/N$ admits a nontrivial abelian quotient. Then there is K with $N \subset K \subset GL_2(\mathbb{Z}/p^r\mathbb{Z})$ and $GL_2(\mathbb{Z}/p^r\mathbb{Z})/K$ abelian.

By [Zyw24, Lemma 7.7] and the assumption $p > 2$, $SL_2(\mathbb{Z}/p^r\mathbb{Z}) \subset K$. Then

$$N \cdot SL_2(\mathbb{Z}/p^r\mathbb{Z}) = GL_2(\mathbb{Z}/p^r\mathbb{Z}) \subset N \cdot K = K,$$

contradicting that the quotient was nontrivial.

Therefore $GL_2(\mathbb{Z}/p^r\mathbb{Z})/N$ has a simple nonabelian quotient S, which implies that $p \geq 5$. Let $K \supset N$ be the corresponding maximal normal subgroup of $GL_2(\mathbb{Z}/p^r\mathbb{Z})$. If $K \bmod p = GL_2(\mathbb{F}_p)$ then, as $p \geq 5$, [Ser68, IV Lemma 3] shows that $SL_2(\mathbb{Z}/p^r\mathbb{Z}) \subset K$, contradicting that S is nonabelian. So

$$GL_2(\mathbb{Z}/p^r\mathbb{Z})/K \cong GL_2(\mathbb{F}_p)/(K \bmod p).$$

Since S is simple, we have $(K \bmod p) \cdot \mathbb{F}_p^\times = K \bmod p$ or $GL_2(\mathbb{F}_p)$. In the second case, S would be abelian. So we are in the first case, and S is a quotient of $PGL_2(\mathbb{F}_p)$. The natural map of simple groups $PSL_2(\mathbb{F}_p) \to S$ must then be an isomorphism, whence $PGL_2(\mathbb{F}_p) \cong PSL_2(\mathbb{F}_p) \times C_2$; this is false, so we have a contradiction.

(3) If $\gcd(j, 30A(\mathcal{E})) = 1$ then this is due to Serre, see the appendix to [CK05].

Write $\bar{H}$ for $H \bmod j$. We argue by induction on the largest prime factor p of j. If j is a power of 3 then the result is true by definition of $A(\mathcal{E})$. Suppose, then, that $p > 3$ and write $j = p^r j'$ where $r \geq 1$ and j' is coprime to p. The inductive hypothesis is that $\rho_{j'}$ is surjective.

Then $\bar{H}$ is a subgroup of $GL_2(\mathbb{Z}/p^r\mathbb{Z}) \times GL_2(\mathbb{Z}/j'\mathbb{Z})$ such that $\bar{H}$ surjects onto each factor and such that $\det|_{\bar{H}}$ is surjective. By Goursat's lemma, there are normal subgroups $M \subset GL_2(\mathbb{Z}/p^r\mathbb{Z})$ and $N \subset GL_2(\mathbb{Z}/j'\mathbb{Z})$ such that $M \times N \subset \bar{H}$ and $\bar{H}/(M \times N)$ is the graph of an isomorphism

$$\phi : GL_2(\mathbb{Z}/p^r\mathbb{Z})/M \xrightarrow{\sim} GL_2(\mathbb{Z}/j'\mathbb{Z})/N.$$

If $SL_2(\mathbb{Z}/p^r\mathbb{Z}) \subset M$, then $GL_2(\mathbb{Z}/j'\mathbb{Z})/N$ is abelian and so $SL_2(\mathbb{Z}/j'\mathbb{Z}) \subset N$ by (for example) [Zyw24, Lemma 7.7]. The surjectivity of $\det|_{\bar{H}}$ now forces $M = GL_2(\mathbb{Z}/p^r\mathbb{Z})$ and $N = GL_2(\mathbb{Z}/j'\mathbb{Z})$, as required.

So we may assume that $SL_2(\mathbb{Z}/p^r\mathbb{Z}) \not\subset M$ and ϕ restricts to an injective homomorphism from the nontrivial group $SL_2(\mathbb{Z}/p^r\mathbb{Z})/(M \cap SL_2(\mathbb{Z}/p^r\mathbb{Z}))$ to a normal subgroup of $GL_2(\mathbb{Z}/j'\mathbb{Z})/N$. It follows from [Ser68, IV Lemmas 2 and 3], using $p \geq 5$, that the only simple quotient of $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ is $PSL_2(\mathbb{F}_p)$. Thus $PSL_2(\mathbb{F}_p)$ occurs as a subquotient of $GL_2(\mathbb{Z}/j'\mathbb{Z})$. But either $p > 5$ and j' is coprime to p, or $p = 5$ and j' is a power of three. In either case, this is impossible (see [Ser68, IV p. 25]). □

3. A positivity criterion

We now prove our main positivity criterion for $\mathcal{C}_{\mathcal{E},j}$. To ease notation we redefine H to be the image of the mod $m_{\mathcal{E}}$ Galois representation:

$$\rho_{m_{\mathcal{E}}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow H \subset GL_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z}).$$

If $k \mid m_{\mathcal{E}}$, then define

$$\mathcal{D}_k : H \to (\mathbb{Z}/k\mathbb{Z})^\times$$

to be the composition of determinant map with reduction modulo k. Since the determinant of $\rho_{m_{\mathcal{E}}}$ is the cyclotomic character, we can also see $\mathcal{D}_k$ as the restriction map

$$\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[m_{\mathcal{E}}])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}).$$

Lemma 3.1. *Suppose that $j, k \in \mathbb{N}$ with $jk \mid m_{\mathcal{E}}$. Then*

$$\mathbb{Q}(\mathcal{E}[j]) \cap \mathbb{Q}(\zeta_{jk}) = \mathbb{Q}(\zeta_j)$$

if and only if

$$\mathcal{D}_{jk}(H \cap \Gamma_j) = (1 + j\mathbb{Z}/jk\mathbb{Z}) \subset (\mathbb{Z}/jk\mathbb{Z})^\times.$$

Proof. The image of the map

$$\mathcal{D}_{jk} : H \cap \Gamma_j = \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[m_{\mathcal{E}}])/\mathbb{Q}(\mathcal{E}[j])) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{jk})/\mathbb{Q}) = (\mathbb{Z}/jk\mathbb{Z})^\times$$

is $\mathrm{Gal}(\mathbb{Q}(\zeta_{jk})/(\mathbb{Q}(\zeta_{jk}) \cap \mathbb{Q}(\mathcal{E}[j])))$. The lemma follows, as $\mathrm{Gal}(\mathbb{Q}(\zeta_{jk})/\mathbb{Q}(\zeta_j)) = 1 + j\mathbb{Z}/jk\mathbb{Z}$. □

Theorem 3.2. *Let $j \mid m_{\mathcal{E}}$ be a natural number, let R be the product of j with the odd prime factors of $m_{\mathcal{E}}/j$.*

If $\mathbb{Q}(\mathcal{E}[j]) \cap \mathbb{Q}(\zeta_R) = \mathbb{Q}(\zeta_j)$ and $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j])$, then $\mathcal{C}_{\mathcal{E},j} > 0$.

Proof. Write $m_{\mathcal{E}}/j = \prod_{i=1}^r p_i^{a_i}$ with $a_i \in \mathbb{N}$ and p_i distinct primes. Let $m_i = v_{p_i}(m_{\mathcal{E}})$ and $j_i = v_{p_i}(j)$, so that $a_i = m_i - j_i$.

For any integer $n \geq 0$, set

$$K_n(p_i) = \begin{cases} I + p_i^n M_2(\mathbb{Z}/p_i^{m_i}\mathbb{Z}) & \text{if } n > 0, \text{ and} \\ GL_2(\mathbb{Z}/p_i^{m_i}\mathbb{Z}) & \text{if } n = 0. \end{cases}$$

Similarly, set

$$U_n(p_i) = \begin{cases} 1 + p_i^n\mathbb{Z}/p_i^{m_i}\mathbb{Z} & \text{if } n > 0, \text{ and} \\ (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times & \text{if } n = 0. \end{cases}$$

Then $H \cap \Gamma_j \subset \prod_{i=1}^r K_{j_i}(p_i)$ and to show that $\mathcal{C}_{\mathcal{E},j} > 0$ it is enough, by Proposition 2.3, to show that

$$H \cap \Gamma_j \neq \bigcup_{i=1}^r H \cap \Gamma_{p_i j}.$$

This is equivalent to showing that there is $h \in H \cap \Gamma_j$ such that $\pi_i(h) \neq e$ for all $1 \leq i \leq r$, where

$$\pi_i : H \cap \Gamma_j \to K_{j_i}(p_i)/K_{j_i+1}(p_i)$$

is the projection.

Suppose first that $2 \notin \{p_1, \ldots, p_r\}$. By our hypothesis and Lemma 3.1,

$$\det : H \cap \Gamma_j \to \prod_{i=1}^r U_{j_i}(p_i)/U_{j_i+1}(p_i)$$

is surjective. Since each factor in this product is nontrivial, there is $h \in H \cap \Gamma_j$ whose image in every factor is not the identity. This is the element h we need.

Otherwise, suppose without loss of generality that $p_1 = 2$. The image G_1 of $H \cap \Gamma_j$ in $K_{j_1}(2)/K_{j_1+1}(2)$ is isomorphic to $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2j])/\mathbb{Q}(\mathcal{E}[j]))$, and hence nontrivial by hypothesis.

Let $G_2 = \prod_{i=2}^r U_{j_i}(p_i)/U_{j_i+1}(p_i)$ and consider the homomorphism

$$\theta : H \cap \Gamma_j \to G_1 \times \left(\prod_{i=2}^r U_{j_i}(p_i)/U_{j_i+1}(p_i) \right) = G_1 \times G_2$$

and let $T = \mathrm{im}(\theta)$. It is enough to show that there is $(t_1, \ldots, t_r) \in T$ such that no t_i is the identity.

The projection p_1 of T onto G_1 is surjective by definition, while the projection p_2 of T onto G_2 is surjective by Lemma 3.1. Let $N_1 = \ker(p_2) \subset G_1$ and let $N_2 = \ker(p_1) \subset G_2$. By Goursat's Lemma, $N_1 \times N_2 \subset T$ and the image of T in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $\phi : G_2/N_2 \to G_1/N_1$.

Suppose that $x = (x_2, \dots, x_r) \in G_2$ with $x_i \neq e$ for every $2 \leq i \leq r$. Then $\phi(x) = e$ otherwise $(\phi(x), x_2, \dots, x_r)$ would be the required element t. So N_2 contains every element of this form.

Now let $x = (x_2, \dots, x_r) \in G_2$ be arbitrary. For each $2 \leq i \leq r$ we may choose y_i and z_i in $U_{j_i}(p_i)/U_{j_i+1}(p_i)$ such that $y_i z_i = x_i$ and $y_i, z_i \neq e$, *unless* $p_i = 3$, $j_i = 0$ and $x_i = 2$. Suppose for now that this does not happen. Then taking $y = (y_2, \dots, y_r)$ and $z = (z_2, \dots, z_r)$, we have $x = yz$ and, by the previous paragraph, $y, z \in N_2$. So $x \in N_2$. But then, as x was arbitrary, $N_2 = G_2$ and so $T = G_1 \times G_2$, in which case we can easily choose $t \in T$ that is not the identity in any factor.

If there is some i with $p_i = 3$, $j_i = 0$ and $x_i = 2$ then, without loss of generality, $i = 2$. We then take $w = (2, w_2, \dots, w_r)$, $y = (2, y_2, \dots, y_r)$ and $z = (2, z_2, \dots, z_r)$ where all $w_i, y_i, z_i \neq e$ and $w_i y_i z_i = x_i$ (for example, take $w_i \neq e$ arbitrary and then find $y_i, z_i \neq e$ such that $y_i z_i = x_i w_i^{-1}$). Then $w, y, z \in N_2$ and $x = wyz$; we conclude as before. □

3.1. **Corollaries.** As our first application of Theorem 3.2, we give a proof of Theorem 1.2 of the introduction. This is due to Serre (see [Ser86]); see Remark 1.4 for a discussion of the proofs in the literature.

Corollary 3.3. *If* $\mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q}$ *then* $\mathcal{C}_{\mathcal{E},1} > 0$.

Proof. Immediate from Theorem 3.2, taking $j = 1$. □

Corollary 3.4. *If* j *is odd,* $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j])$*, and the image* $\bar{H} = H \bmod j$ *of* $\rho_j : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/j\mathbb{Z})$ *satisfies*

$$[\bar{H}, \bar{H}] = \bar{H} \cap SL_2(\mathbb{Z}/j\mathbb{Z}),$$

then $\mathcal{C}_{\mathcal{E},j} > 0$.

Proof. The maximal abelian subextension of $\mathbb{Q}(\mathcal{E}[j])$ is equal to

$$\mathbb{Q}(\mathcal{E}[j])^{[\bar{H},\bar{H}]} = \mathbb{Q}(\mathcal{E}[j])^{\bar{H} \cap SL_2(\mathbb{Z}/j\mathbb{Z})} = \mathbb{Q}(\zeta_j).$$

In particular, Theorem 3.2 applies. □

Remark 3.5. If j is odd, $4 \nmid m_{\mathcal{E}}$, and $9 \nmid m_{\mathcal{E}}/j$, then one can show that the conditions in Corollary 3.4 are equivalent to those in Theorem 3.2.

Example 3.6. Let $\mathcal{E} : y^2 + y = x^3 + x^2 + x$ be the elliptic curve with LMFDB label 19.a3. Then ρ_3 has image

$$\left\{ \begin{pmatrix} 1 & \star \\ 0 & \star \end{pmatrix} \right\}$$

and $[\mathbb{Q}(\mathcal{E}[6]) : \mathbb{Q}(\mathcal{E}[3])] = 6$. Thus the hypotheses of Corollary 3.4 apply to show that $\mathcal{C}_{\mathcal{E},3} > 0$. There are infinitely many similar examples, see [Zyw15].

We now obtain a simple generalisation of the main theorem of [Kim15], removing the condition that $\gcd(j, N_{\mathcal{E}}) = 1$.

Corollary 3.7. *Suppose that* $\gcd(j, 2A(\mathcal{E})) = 1$ *and that* $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j])$*. Then* $\mathcal{C}_{\mathcal{E},j} > 0$.

Proof. This follows from Corollary 3.4 and Proposition 2.9, as the derived subgroup of $GL_2(\mathbb{Z}/p^a\mathbb{Z})$ is $SL_2(\mathbb{Z}/p^a\mathbb{Z})$ for $p \geq 3$ by (for example) [Zyw24, Lemma 7.7]. □

In Theorem 3.2, the condition $\mathbb{Q}(\mathcal{E}[2j]) \neq \mathbb{Q}(\mathcal{E}[j])$ is necessary, by Corollary 2.5. However, the other condition is certainly not necessary, as the following example shows.

Example 3.8. Let $\mathcal{E} : y^2 + xy + y = x^3 + x^2 - 3x + 1$ be the elliptic curve with LMFDB label 50.b3. Then the image of ρ_3 is the full group of upper triangular matrices, $R = 15$, and $\mathbb{Q}(\mathcal{E}[3]) \cap \mathbb{Q}(\zeta_R)$ is the quadratic extension of $\mathbb{Q}(\zeta_3)$ in $\mathbb{Q}(\zeta_{15})$. However, from the information in [LMFDB], we have

$$\frac{1}{|H \bmod 3|} - \frac{1}{|H \bmod 6|} - \frac{1}{|H \bmod 15|} + \frac{1}{|H \bmod 30|} > \frac{1}{12} - \frac{1}{72} - \frac{1}{120} > 0$$

and so $\mathcal{C}_{\mathcal{E},3} > 0$ by Proposition 2.2.

On the other hand, here is an example where the even j are the crucial ones to consider:

Example 3.9. Let $\mathcal{E} : y^2 = x^3 - 3x + 4$ with LMFDB label 5184.j1. Then $m_{\mathcal{E}} = 4$, so the first condition in Theorem 3.2 is vacuous. As $\mathbb{Q}(\mathcal{E}[4]) \neq \mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q}$, we see that $\mathcal{C}_{\mathcal{E},j} > 0$ for all $j \mid m_{\mathcal{E}}$ and hence for all positive integers j.

Jones [Jon10] shows that 100% of elliptic curves (ordered by naive height) are "Serre curves", meaning that the index of $\mathrm{im}(\rho)$ in $GL_2(\hat{\mathbb{Z}})$ is two (as small as possible). As we completely understand the adelic image in this case, the analysis is straightforward.

Proposition 3.10. *Let $\mathcal{E}$ be a Serre curve. Then $\mathcal{C}_{\mathcal{E},j} > 0$ for all j.*

Proof. We may assume (Proposition 2.2) that $j \mid m_{\mathcal{E}}$ and write $H = \mathrm{im}(\rho_{m_{\mathcal{E}}})$. Let $\Delta_{\mathcal{E}}$ be the discriminant of $\mathcal{E}$ and let χ be the quadratic (or trivial, if $\Delta_{\mathcal{E}}$ is square) Dirichlet character of conductor m associated to the extension $\mathbb{Q}(\sqrt{\Delta_{\mathcal{E}}})/\mathbb{Q}$, regarded as a character of $(\mathbb{Z}/m\mathbb{Z})^\times$. Then by [Jon09, section 3] we have that $m_{\mathcal{E}} = \mathrm{lcm}(2, m)$ and

$$H = \ker(\epsilon \cdot (\chi \circ \det)),$$

where ϵ is the nontrivial quadratic character of $GL_2(\mathbb{F}_2)$, inflated to $GL_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z})$.

Let $a = v_2(j)$, $b = v_2(m)$, $c = v_2(m_{\mathcal{E}}) = \max(1, b)$ and note that $m/2^b$ is odd and squarefree. We may write $\chi = \prod_{p|m} \chi_p$ where each χ_p is a nontrivial character of $(\mathbb{Z}/p\mathbb{Z})^\times$ (for p odd) or of $(\mathbb{Z}/2^b\mathbb{Z})^\times$ (if $p = 2$).

If S is the set of primes dividing $m_{\mathcal{E}}/j$ then, by Proposition 2.3, we need to show that $H \cap \Gamma_j$ contains an element whose image in each $GL_2(\mathbb{Z}/pj\mathbb{Z})$ is nontrivial. We can write

$$\Gamma_j = K_a(2) \times \prod_{p \in S, p \neq 2} GL_2(\mathbb{F}_p).$$

For p odd, let $g_p \in SL_2(\mathbb{F}_p)$ with $g_p \neq e$. If $a = 0$, let $g_2 \in SL_2(\mathbb{Z}/2^c\mathbb{Z})$ satisfy $\epsilon(g_2) = 1$ and $g_2 \bmod 2 \neq I$. If $a > 0$, let $g_2 \in K_a(2) \cap SL_2(\mathbb{Z}/2^c\mathbb{Z})$ with $g_2 \notin K_{a+1}(2)$.

In each case, we have $\chi_p(\det(g_p)) = 1$, while in the case $p = 2$ we also have $\epsilon(g_2) = 1$. The element $(g_p)_{p \in S}$ is then an element of $H \cap \Gamma_j$ and not an element of any Γ_{pj} for $p \in S$, as required. □

Remark 3.11. One can show that, in the case of Serre curves, Theorem 3.2 applies unless $m_{\mathcal{E}}/j$ is odd (and > 1). Otherwise it does not apply, but the conclusion $\mathcal{C}_{\mathcal{E},j} > 0$ still holds.

4. Coincidences

We now give some examples where $\mathcal{C}_{\mathcal{E},j} = 0$. Conjectures 2.6 and 4.2 predict that, in any such case with $\mathcal{E}$ non-CM, $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[jp])$ for $p = 2$ or 3 (which certainly implies that $\mathcal{C}_{\mathcal{E},j} = 0$ by Corollary 2.5). These are examples of 'coincidences' of division fields in the sense of [DLR23]. For p a prime, we call a *p-coincidence* one of the form $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[jp])$.

Given a p-coincidence $\mathbb{Q}(\mathcal{E}[d]) = \mathbb{Q}(\mathcal{E}[dp])$, we may construct further coincidences $\mathbb{Q}(\mathcal{E}[dk]) = \mathbb{Q}(\mathcal{E}[dkp])$ for all $k > 1$ coprime to p. Call these coincidences *imprimitive*, so that coincidences not arising in this way are *primitive*. There are simple constructions of elliptic curves with primitive coincidences $\mathbb{Q}(\mathcal{E}[1]) = \mathbb{Q}(\mathcal{E}[2])$, $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\mathcal{E}[4])$ and $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\mathcal{E}[6])$, giving the following proposition.

Proposition 4.1. *Given a positive integer j with $12 \nmid j$, there exists an elliptic curve $\mathcal{E}$ with $\mathcal{C}_{\mathcal{E},j} = 0$.*

Proof. If j is odd then we may simply take a curve with $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}$, such as $\mathcal{E} : y^2 = x^3 - 7x + 6$. Then $\mathcal{C}_{\mathcal{E},j} = 0$ by Corollary 2.5 with $p = 2$.

If j is even and not divisible by 4 then take a curve with $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\mathcal{E}[4])$, such as $y^2 = x^3 + 13x - 34$ (see [DLR23, Example 1.3]) and note that $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[2j])$ and so $\mathcal{C}_{\mathcal{E},j} = 0$ by Corollary 2.5 with $p = 2$.

If j is divisible by 4 then, by assumption, $3 \nmid j$. Let $\mathcal{E}$ be an elliptic curve with $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\mathcal{E}[3])$, such as $y^2 = x^3 + 405x - 9882$ (see [DLR23, Example 1.2]). Then $\mathbb{Q}(\mathcal{E}[3j]) = \mathbb{Q}(\mathcal{E}[j])$ and by Corollary 2.5 with $p = 3$, we have $\mathcal{C}_{\mathcal{E},j} = 0$. □

In Remark 1.9 of [DLR23], they speculate that the only coincidences $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[n])$ arise for $(n, m) \in \{(2,3), (2,4), (2,6), (3,6)\}$. This is not true, even if appropriately modified to take into account the fact that one may replace m and n in a coincidence by their least common multiples with a third integer k; we will see a number of examples below. However, we do make the following conjecture:

Conjecture 4.2. *Suppose that $p \geq 5$. Then there are no non-CM elliptic curves over $\mathbb{Q}$ with a p-coincidence.*

Remark 4.3. By [Yvo25, Corollary 3.10], if $\mathcal{E}$ is a non-CM elliptic curve over $\mathbb{Q}$ with a p-coincidence then $p \mid 2\Delta_{\mathcal{E}}$. Moreover, a standard argument shows that if there is a p-coincidence $\mathbb{Q}(\mathcal{E}[j]) = \mathbb{Q}(\mathcal{E}[jp])$ with $p > 5$ and $p \nmid j$, then $p \mid A(\mathcal{E})$.

Thanks to Zywina's algorithm [Zyw24], the LMFDB now contains data on the images of mod m Galois representations for elliptic curves over $\mathbb{Q}$. It is then straightforward to check[4] the following:

Proposition 4.4. *Conjectures 2.6 and 4.2 are true for all curves in the LMFDB[5], and in particular for all curves of conductor ≤ 500000.*

[4]Code available at https://github.com/jackshotton/invariant-factors-public. Note that we only need to check non-CM elliptic curves with adelic index > 2, by Proposition 3.10.

[5]As of 19th April 2026.

4.1. **Constructions from abelian division fields.** We can construct some infinite families of primitive p-coincidences starting with certain abelian division fields. These were classified in [GL16]. The simplest is when we have an abelian two-division field.

Proposition 4.5. *Suppose that $\mathbb{Q}(\mathcal{E}[2])$ is an abelian extension of $\mathbb{Q}$ with odd conductor m. That is, $\mathbb{Q}(\mathcal{E}[2])$ is either trivial, cubic, or a quadratic extension $\mathbb{Q}(\sqrt{m'})$ with $m' = 3 \bmod 4$ and $m = |m'|$.*

Then $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[2m])$.

Proof. By assumption, $\mathbb{Q}(\mathcal{E}[2]) \subset \mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\mathcal{E}[m])$ with m odd. Therefore $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[2m])$. □

4.1.1. *Abelian 2-power torsion.* More families occur when we have abelian division fields $\mathbb{Q}(\mathcal{E}[2^r])$ such that $\mathbb{Q}(\mathcal{E}[2^{r-1}])$ contains ζ_{2^r}. By [GL16], we must have $r \leq 3$ and $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2^r])/\mathbb{Q})$ is an elementary abelian 2-group.

Proposition 4.6.

(1) Suppose that $\mathcal{E}$ is an elliptic curve such that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ is abelian and that $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(i)$. Suppose also that the conductor of $\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}$ is $4j$ with j odd.

Then $\mathbb{Q}(\mathcal{E}[2j]) = \mathbb{Q}(\mathcal{E}[4j])$.

(2) Suppose that $\mathcal{E}$ is an elliptic curve such that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[8])/\mathbb{Q})$ is abelian and that $\zeta_8 \in \mathbb{Q}(\mathcal{E}[4])$. Suppose that the conductor of $\mathbb{Q}(\mathcal{E}[8])/\mathbb{Q}$ is $8j$ (and note that j is necessarily odd as $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[8])/\mathbb{Q}) \cong C_2^k$ for some k).

Then $\mathbb{Q}(\mathcal{E}[4j]) = \mathbb{Q}(\mathcal{E}[8j])$.

Proof. (1) We have that $\zeta_{2j} \in \mathbb{Q}(\mathcal{E}[2j])$ but also that $\zeta_4 \in \mathbb{Q}(\mathcal{E}[2])$. Thus

$$\mathbb{Q}(\mathcal{E}[4]) \subset \mathbb{Q}(\zeta_{4j}) \subset \mathbb{Q}(\mathcal{E}[2j])$$

and so $\mathbb{Q}(\mathcal{E}[2j]) = \mathbb{Q}(\mathcal{E}[4j])$.

(2) The proof is identical with 2 replaced by 4 and 4 replaced by 8.

□

In [RZB15] the possible 2-adic Galois images for elliptic curves over $\mathbb{Q}$ are classified; in [GL16] these are used to enumerate elliptic curves with abelian 2^r-division field. For each conjugacy class of elementary abelian 2-group $H \subset GL_2(\mathbb{Z}/2^r\mathbb{Z})$ there is an explicit modular curve X_H of genus 0 parametrising elliptic curves with $\mathrm{im}(\rho_{\mathcal{E},2^r}) \subset H$ (up to conjugation)[6]. The cases in which this modular curve actually has rational points are listed in [GL16, Tables 3 and 4]. Explicit generators for H and parametrisations for the curves may then be found at `https://users.wfu.edu/rouseja/2adic/`.

Suppose first that $r = 2$. To obtain subgroups H such that elliptic curves $\mathcal{E}$ on X_H satisfy the conditions of Proposition 4.6 we must have that $\ker(H \to GL_2(\mathbb{F}_2)) = H \cap SL_2(\mathbb{Z}/4\mathbb{Z})$. Checking each possibility, the relevant modular curves are `X60d`, `X60`, `X27f`, `X27h`, `X27`. The notation is such that e.g. `X27f` corresponds to a subgroup H not containing $\pm I$ and `X27` corresponds to the subgroup with $\pm I$ added; the elliptic curves on `X27` will be quadratic twists of those on `X27f`.

[6] There is a subtlety around quadratic twists, which we take care of below.

Curves on X60d (see [GL16] or https://users.wfu.edu/rouseja/2adic/X60d.html) have $\mathrm{im}(\rho_{\mathcal{E},4}) = \{I, \begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}\}$ up to conjugacy. Explicitly, we may take $\mathcal{E}$ given by

$$y^2 = x^3 + (-432t^8 + 1512t^4 - 27)x + (3456t^{12} + 28512t^8 - 7128t^4 - 54)$$

for $t \in \mathbb{Q}$ such that the discriminant is nonzero. In this case, $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(i)$, so this does not work for Proposition 4.6 unless $j = 1$; however, we can take quadratic twists (i.e. points on X60).

For $\mathcal{E} = \mathcal{E}_t$ in this family, if $\mathcal{E}^{(\pm j)}$ is the quadratic twist of $\mathcal{E}$ by $\pm j$ for $j > 1$ odd and squarefree, then $\rho_{\mathcal{E}^{(\pm j)},4} = \chi_{\pm j}\rho_{\mathcal{E},4}$, where $\chi_{\pm j}$ is the quadratic character associated to $\mathbb{Q}(\sqrt{\pm j})$, and the image of $\rho_{\mathcal{E}^{(\pm j)},4}$ is generated by

$$\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

For this subgroup, the kernel of reduction modulo 2 coincides with the kernel of the determinant, and so $\mathbb{Q}(\mathcal{E}^{(\pm j)}[2]) = \mathbb{Q}(i)$. Moreover, $\mathbb{Q}(\mathcal{E}^{(\pm j)}[4]) = \mathbb{Q}(i, \sqrt{\pm j})$ has conductor $4j$. Therefore $\mathcal{E}^{(\pm j)}$ satisfies the hypotheses of Proposition 4.6.

For X27h there is similarly a parametrisation (see [GL16, Section 6.2])

$$\mathcal{E}_t : y^2 = x^3 + (-432t^4 + 1512t^2 - 27)x + (3456t^6 + 28512t^4 - 7128t^2 - 54).$$

Curves in this family have mod 4 Galois image contained in the subgroup generated by

$$\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}, \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$$

and the hypotheses of Proposition 4.6 hold as long as we can arrange that the conductor of $\mathbb{Q}(\mathcal{E}_t[4])$ has the form $4j$ for j odd. An explicit calculation[7] using [GL16, Corollary 2.5] shows that $\mathbb{Q}(\mathcal{E}_t[4]) = \mathbb{Q}(i, \sqrt{t})$ and so we may take t to be any odd integer. Curves on X27 or X27f are quadratic twists of these by some squarefree integer j and we will obtain similar examples as long as j is odd.

Now we suppose that $r = 3$. In this case we look for subgroups $H \subset GL_2(\mathbb{Z}/8\mathbb{Z})$ such that $\ker(H \to GL_2(\mathbb{Z}/4\mathbb{Z})) \subset SL_2(\mathbb{Z}/8\mathbb{Z})$ and such that H is an elementary abelian 2-group. We check[8] each subgroup corresponding to a modular curve on the list in [GL16, Table 4]. The subgroups of the form X58? may be disregarded, as in these cases $I + 4M_2(\mathbb{Z}/8\mathbb{Z}) \subset H$ so our condition cannot hold. Of the remainder, our condition holds exactly for X183e, X183k, X187e, X187i, X189i and X189l.

We work through the case of X187i. From https://users.wfu.edu/rouseja/2adic/187i we have the parametrisation:

$$\mathcal{E}_t : y^2 = x^3 + \left(-108t^{16} - 24192t^8 - 27648\right)x - 432t^{24} + 228096t^{16} + 3649536t^8 - 1769472.$$

Setting $t = 1$ we obtain the elliptic curve with LMFDB label 960.a5. This has equation

$$\mathcal{E} : y^2 = x^3 - x^2 - 641x + 3105 = (x - 23)(x - 5)(x + 27).$$

The pairwise differences of the roots are 18, 50 and 32, so [GL16, Corollary 2.5] gives

$$\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8).$$

[7] Code available at https://github.com/jackshotton/invariant-factors-public.
[8] Code available at https://github.com/jackshotton/invariant-factors-public.

For this curve one finds that $\mathbb{Q}(\mathcal{E}[8])$ is abelian of conductor $120 = 8 \cdot 15$, and hence by Proposition 4.6 we have

$$\mathbb{Q}(\mathcal{E}[60]) = \mathbb{Q}(\mathcal{E}[120]).$$

4.1.2. *Abelian 3-torsion.* We may also construct examples starting from abelian 3-division fields. These must be quadratic or biquadratic and in each case there is a simple parametrisation. To obtain coincidences, we exploit the fact that the adelic image is always contained in the Serre subgroup (see the proof of Proposition 3.10), the kernel of a particular quadratic character.

Proposition 4.7. *Suppose that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and that $3 \mid \Delta_{\mathcal{E}}^{sf}$, the squarefree part of the discriminant of $\mathcal{E}$. Let*

$$3m = \begin{cases} 2|\Delta_{\mathcal{E}}^{sf}| & \text{if } \Delta_{\mathcal{E}}^{sf} \equiv 1 \bmod 4 \\ 4|\Delta_{\mathcal{E}}^{sf}| & \text{otherwise.} \end{cases}$$

Then $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[3m])$.

Proof. Let χ be the primitive Dirichlet character associated to the quadratic extension $\mathbb{Q}(\sqrt{\Delta_{\mathcal{E}}})$ and let ϵ be as in the proof of Proposition 3.10. We may factor χ as $\chi_3\chi'$ where χ_3 is the quadratic character of conductor 3 and χ' is a quadratic character of conductor coprime to 3. Then the character $\epsilon \cdot \chi \circ \det$ of $GL_2(\mathbb{Z}/m_{\mathcal{E}}\mathbb{Z})$ is trivial on the image H of $\rho \bmod m_{\mathcal{E}}$. If $h \in H \cap \Gamma_m$, then $\chi'(\det(h)) = 1$ and $\epsilon(h) = 1$. It follows that $\chi_3(\det(h)) = 1$, so that h fixes ζ_3. Thus

$$\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\mathcal{E}[m])$$

and so $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\mathcal{E}[3m])$, as required. □

Remark 4.8. As in [GL16, Section 6.2], the curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ are parametrised by the family

$$\mathcal{E}_t : y^2 = x^3 - 27t(t^3+8)x + 54(t^6 - 20t^3 - 8).$$

where $t \in \mathbb{Q}$ and $t \neq 1$. This is the Weierstrass form of the Hesse plane cubic

$$x^3 + y^3 + z^3 = 3txyz.$$

As in [JQ01], the discriminant of this model is $2^{12}3^9(t^3-1)^3$. If we choose t so that $v_3(t^3-1)$ is even (for instance, $t = 3u$ for $u \in \mathbb{Z}$), then $3 \mid \Delta_{\mathcal{E}_t}^{sf}$ and $\mathcal{E}_t$ satisfies the hypotheses of Proposition 4.7.

Remark 4.9. Suppose that $\mathcal{E}$ and m are as in Proposition 4.7 and that d is squarefree with $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_m)$. If $\mathcal{E}^{(d)}$ is the quadratic twist of $\mathcal{E}$ by d then $\mathbb{Q}(\mathcal{E}^{(d)}[3]) = \mathbb{Q}(\zeta_3, \sqrt{d})$ and we still have

$$\mathbb{Q}(\mathcal{E}^{(d)}[m]) = \mathbb{Q}(\mathcal{E}^{(d)}[3m])$$

by exactly the same argument as in the proof of Proposition 4.7, noting that $\Delta_{\mathcal{E}^{(d)}}^{sf} = \Delta_{\mathcal{E}}^{sf}$.

We give a numerical example: let $t = 2$ in the above parametrisation and $\mathcal{E}$ be the resulting curve. We obtain the elliptic curve with LMFDB label 189.b2 which has discriminant $3^9 \cdot 7^3$ and so $\mathbb{Q}(\mathcal{E}[14]) = \mathbb{Q}(\mathcal{E}[42])$ by Proposition 4.7. By Remark 4.9, the same holds with $\mathcal{E}$ replaced by its quadratic twist $\mathcal{E}^{(7)}$ (with LMFDB label 1323.h3).

4.2. **Smorgasbord.** We finish with a small selection of examples of coincidences that we found interesting.

Example 4.10. (1) There are numerous examples in which $\mathbb{Q}(\mathcal{E}[2])$ is quadratic and contained in multiple division fields $\mathbb{Q}(\mathcal{E}[j])$ for j odd. For example, the elliptic curve with LMFDB label 198.c1 has

$$\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\sqrt{33}) \subset \mathbb{Q}(\mathcal{E}[33]) \cap \mathbb{Q}(\mathcal{E}[55]).$$

(2) The elliptic curve with LMFDB label 196.a1 has $\mathbb{Q}(\mathcal{E}[2])$ cubic of conductor 7 and therefore

$$\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\zeta_7)^+ \subset \mathbb{Q}(\mathcal{E}[7])$$

as in Proposition 4.5. However, in this case we also have $\mathbb{Q}(\mathcal{E}[2]) \subset \mathbb{Q}(\mathcal{E}[9])$ and therefore $\mathbb{Q}(\mathcal{E}[9]) = \mathbb{Q}(\mathcal{E}[18])$. In particular, $\mathcal{C}_{\mathcal{E},7} = \mathcal{C}_{\mathcal{E},9} = 0$, showing that $\mathcal{C}_{\mathcal{E},j}$ can vanish for two coprime values of j.

(3) The elliptic curve with LMFDB label 300.b1 has $\mathbb{Q}(\mathcal{E}[2]) \subset \mathbb{Q}(\mathcal{E}[9])$ and $\mathbb{Q}(\mathcal{E}[2])$ nonabelian.

(4) The elliptic curve with LMFDB label 300.b2 has

$$\mathbb{Q}(\mathcal{E}[2]) \subset \mathbb{Q}(\mathcal{E}[3]) \subset \mathbb{Q}(\mathcal{E}[10]).$$

Thus $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\mathcal{E}[6])$ and $\mathbb{Q}(\mathcal{E}[10]) = \mathbb{Q}(\mathcal{E}[30])$. Note that in this case the mod 3 representation has image of order 12, and so is nonabelian; in particular this curve has a 3-coincidence that is not explained by Proposition 4.7.

(5) The elliptic curve with LMFDB label 1680.g2 has $\mathbb{Q}(\mathcal{E}[4]) \subset \mathbb{Q}(\mathcal{E}[105])$ and so

$$\mathbb{Q}(\mathcal{E}[105]) = \mathbb{Q}(\mathcal{E}[210]) = \mathbb{Q}(\mathcal{E}[420]).$$

Here $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ is elementary abelian of order 8.

5. Positivity of $\mathcal{C}_{\mathcal{E},1}$

The purpose of this section is to explain and repair a small error in the proof of Corollary 3.3 given in [CM04, Section 6]. The following lemma, which is the key to the argument, is proved in [CM04] via an inclusion-exclusion argument.

Lemma 5.1 ([CM04], Lemma 6.1)**.** *Let $\mathcal{F} = (F_q)_{q\in\mathcal{P}}$, $\mathcal{F}' = (F'_q)_{q\in\mathcal{P}'}$ be two families of finite Galois extensions of a number field F, indexed by sets of rational primes $\mathcal{P}' \subset \mathcal{P}$. For any square-free integer k composed of primes from $\mathcal{P}$, define:*

- *fields $F_k = \prod_{q|k,q\in\mathcal{P}} F_q$ and $F'_k = \prod_{q|k,q\in\mathcal{P}'} F'_q$, where the product denotes compositum;*
- *integers $N_k = [F_k : F]$ and $N'_k = [F'_k : F]$ where $N_1 = N'_1 = 1$;*
- *quantities*

$$\delta(\mathcal{F}) = \sum_{\substack{k \\ q|k\Rightarrow q\in\mathcal{P}}} \frac{\mu(k)}{N_k}, \quad \delta(\mathcal{F}') = \sum_{\substack{k \\ q|k\Rightarrow q\in\mathcal{P}'}} \frac{\mu(k)}{N'_k}.$$

In addition, suppose that:

- *$\mathcal{F}$ covers $\mathcal{F}'$. That is: for all $q' \in \mathcal{P}'$, there exists $q \in \mathcal{P}$ such that $F'_{q'} \subseteq F_q$, and for all $q \in \mathcal{P}$, there exists $q' \in \mathcal{P}'$ such that $F'_{q'} \subseteq F_q$;*
- *The sums defining $\delta(\mathcal{F})$ and $\delta(\mathcal{F}')$ are absolutely convergent.*

Then $\delta(\mathcal{F}) \geq \delta(\mathcal{F}')$.

Corollary 5.2. *If, in addition to the hypotheses in Lemma 5.1, the fields $(F'_q)_{q\in\mathcal{P}'}$ are linearly disjoint over F then*

$$\delta(\mathcal{F}) \geq \delta(\mathcal{F}') = \prod_{q\in\mathcal{P}'} \left(1 - \frac{1}{N'_q}\right).$$

In [CM04] this is applied as follows. Let $\mathcal{E}$ be a non-CM elliptic curve over $\mathbb{Q}$ with $\mathbb{Q}(\mathcal{E}[2]) \neq \mathbb{Q}$ and let $F_q = \mathbb{Q}(\mathcal{E}[q])$ for each prime q (with $\mathcal{P}$ the set of all primes). Let $K_2 \subset F_2$ be the largest abelian extension of $\mathbb{Q}$ contained in F_2, which is either quadratic or cubic by assumption. Let

$$\mathcal{P}' = \{q \in \mathcal{P} : \mathbb{Q}(\zeta_q) \cap K_2 = \mathbb{Q}\}$$

and, for $q \in \mathcal{P}'$, define

$$F'_q = \begin{cases} F_q & \text{if } q \nmid m_{\mathcal{E}} \\ \mathbb{Q}(\zeta_q) & \text{if } q \mid m_{\mathcal{E}},\ q \neq 2 \\ K_2 & \text{if } q = 2. \end{cases}$$

Then with $\mathcal{F} = \{F_q\}_{q\in\mathcal{P}}$ and $\mathcal{F}' = (F'_q)_{q\in\mathcal{P}'}$ we have that $\mathcal{F}$ covers $\mathcal{F}'$. It is asserted in [CM04] that the fields $\mathcal{F}'$ are linearly disjoint, and it would then follow from Corollary 5.2 that

$$\mathcal{C}_{\mathcal{E},1} = \delta(\mathcal{F}) > 0.$$

However, although the fields F'_q are *pairwise* linearly disjoint, they are *not* linearly disjoint if (for example) the conductor of $\mathbb{Q}(\sqrt{\Delta_{\mathcal{E}}})$ is composite and odd. This is the gap in [CM04, Section 6]. It may be fixed by making a closer examination of $\delta(\mathcal{F}')$, which we now do.

Define

$$R = \prod_{\substack{q\mid m_{\mathcal{E}} \\ q\neq 2 \\ K_2\cap\mathbb{Q}(\zeta_q)=\mathbb{Q}}} q$$

and define S to be the minimal integer dividing R such that $K_2 \subset \mathbb{Q}(\zeta_S)$ (if there is no such integer S, then the families $\mathcal{F}$ and $\mathcal{F}'$ as defined above fulfil the conditions of Corollary 5.2 and we argue as in [CM04]).

Let $d = [K_2 : \mathbb{Q}] = 2$ or 3. Then, for $k|R$, we have, $N'_k = \phi(k)$ and

$$N'_{2k} = \begin{cases} d\phi(k) & \text{if } S \nmid k \\ \phi(k) & \text{if } S|k. \end{cases}$$

Thus

$$\begin{aligned}
\sum_{k|R} \mu(k) \left(\frac{1}{N'_k} - \frac{1}{N'_{2k}}\right) &= \sum_{k|R} \mu(k) \left(\frac{1}{\phi(k)} - \frac{1}{d\phi(k)}\right) - \sum_{k|\frac{R}{S}} \mu(Sk) \left(\frac{1}{\phi(Sk)} - \frac{1}{d\phi(Sk)}\right) \\
&= \left(1 - \frac{1}{d}\right) \left(\prod_{q|R} \left(1 - \frac{1}{\phi(q)}\right) - \frac{\mu(S)}{\phi(S)} \prod_{q|\frac{R}{S}} \left(1 - \frac{1}{\phi(q)}\right)\right) \\
&= \frac{1}{\phi(S)} \left(1 - \frac{1}{d}\right) \prod_{q|\frac{R}{S}} \left(1 - \frac{1}{\phi(q)}\right) \left(\prod_{q|S} (\phi(q) - 1) - \mu(S)\right) \\
&> 0
\end{aligned}$$

since $S \geq 3$. Therefore

$$\delta(\mathcal{F}') = \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}'}} \frac{\mu(k)}{N'_k} = \sum_{k|R} \mu(k) \left(\frac{1}{N'_k} - \frac{1}{N'_{2k}} \right) \prod_{q \nmid m_{\mathcal{E}}} \left(1 - \frac{1}{N'_q} \right) > 0.$$

Therefore, by Lemma 5.1,

$$\mathcal{C}_{\mathcal{E},1} = \delta(\mathcal{F}) \geq \delta(\mathcal{F}') > 0$$

as required.

References

[CK05] Alina Carmen Cojocaru and Ernst Kani. "On the surjectivity of the Galois representations associated to non-CM elliptic curves". In: *Canadian Mathematical Bulletin* 48.1 (Mar. 2005), pp. 16–31.

[CM04] Alina Carmen Cojocaru and M. Ram Murty. "Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem". In: *Mathematische Annalen* 330.3 (Nov. 2004), pp. 601–625.

[Coj04] Alina Carmen Cojocaru. "Questions about the reductions modulo primes of an elliptic curve". In: *Number theory*. Vol. 36. CRM Proc. Lecture Notes. Amer. Math. Soc., Providence, RI, 2004, pp. 61–79.

[CS23] Francesco Campagna and Peter Stevenhagen. "Cyclic reduction densities for elliptic curves". In: *Research in Number Theory* 9.3 (2023), Paper No. 61, 21.

[DG22] Harris B. Daniels and Enrique González-Jiménez. "Serre's constant of elliptic curves over the rationals". In: *Experimental Mathematics* 31.2 (Apr. 2022), pp. 518–536.

[DLR23] Harris B. Daniels and Álvaro Lozano-Robledo. "Coincidences of division fields". In: *Annales de l'Institut Fourier* 73.1 (2023), pp. 163–202.

[DR26] Harris B. Daniels and Jeremy Rouse. "Near coincidences and nilpotent division fields". In: *Pacific Journal of Mathematics* 342.1 (Mar. 2026), pp. 79–113.

[FK14] Tristan Freiberg and Pär Kurlberg. "On the average exponent of elliptic curves modulo p". In: *International Mathematics Research Notices. IMRN* 8 (2014), pp. 2265–2293.

[GL16] Enrique González–Jiménez and Álvaro Lozano-Robledo. "Elliptic curves with abelian division fields". In: *Mathematische Zeitschrift* 283.3-4 (Aug. 2016), pp. 835–859.

[GM90] Rajiv Gupta and M. Ram Murty. "Cyclicity and generation of points mod p on elliptic curves". In: *Inventiones mathematicae* 101.1 (Dec. 1990), pp. 225–235.

[Jon09] Nathan Jones. "Averages of elliptic curve constants". In: *Mathematische Annalen* 345.3 (Nov. 2009), pp. 685–710.

[Jon10] Nathan Jones. "Almost all elliptic curves are Serre curves". In: *Transactions of the American Mathematical Society* 362.3 (2010), pp. 1547–1570.

[JQ01] Marc Joye and Jean-Jacques Quisquater. "Hessian Elliptic Curves and Side-Channel Attacks". In: *Cryptographic Hardware and Embedded Systems — CHES 2001*. Ed. by Çetin K. Koç, David Naccache, and Christof Paar. Berlin, Heidelberg: Springer, 2001, pp. 402–410.

[Kim15] Sungjin Kim. "Positivity of constants related to elliptic curves". In: *Journal of Number Theory* 157 (2015), pp. 54–63.

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database*. https://www.lmfdb.org. 2024.

[Mur83] M. Ram Murty. "On Artin's conjecture". In: *Journal of Number Theory* 16.2 (1983), pp. 147–168.

[RZB15] Jeremy Rouse and David Zureick-Brown. "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois". In: *Research in Number Theory* 1.1 (Oct. 2015), p. 12.

[Ser68] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser72] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Inventiones Mathematicae* 15.4 (1972), pp. 259–331.

[Ser86] Jean-Pierre Serre. "Résumé des cours 1977-78". In: *Collected Papers* III (1986), pp. 465–468.

[Yvo25] Zoé Yvon. *Coincidences of Division Fields of an elliptic curve defined over a number field*. June 2025. arXiv: 2407.14370.

[Zyw15] David Zywina. *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*. Aug. 2015. arXiv: 1508.07660.

[Zyw24] David Zywina. *Explicit open images for elliptic curves over $\mathbb{Q}$*. Mar. 2024. arXiv: 2206.14959.

School of Mathematics, University of Edinburgh
Email address: a.j.c.milner@sms.ed.ac.uk

Department of Mathematical Sciences, Durham University
Email address: jack.g.shotton@durham.ac.uk