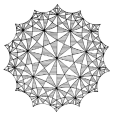
Rev. Mat. Iberoam. 42 (2026), no. 3, 803–830
DOI 10.4171/RMI/1607



On the acyclicity of reductions of elliptic curves modulo primes in arithmetic progressions

Nathan Jones and Sung Min Lee

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ and, for a prime p of good reduction for E, let $\tilde{E}_p$ denote the reduction of E modulo p. Inspired by an elliptic curve analogue of Artin's primitive root conjecture posed by S. Lang and H. Trotter in 1977, J.-P. Serre adapted methods of C. Hooley to prove a GRH-conditional asymptotic formula for the number of primes $p \leq x$ for which the group $\tilde{E}_p(\mathbb{F}_p)$ is cyclic. An illuminating proof of this asymptotic formula appeared in a 1983 paper of M. R. Murty, which also established the same unconditionally in the case where E has complex multiplication. More recently, Akbal and Güloğlu considered the question of cyclicity of $\tilde{E}_p(\mathbb{F}_p)$ under the additional restriction that p lie in an arithmetic progression. In this paper, we study the question of which arithmetic progressions $a \bmod n$ have the property that, for all but finitely many primes $p \equiv a \bmod n$, the group $\tilde{E}_p(\mathbb{F}_p)$ is *not* cyclic, answering a question of Akbal and Güloğlu on this issue.

1. Introduction and statement of results

Let E be an elliptic curve defined over $\mathbb{Q}$ and let p be a rational prime of good reduction for E, i.e., assume that the reduction $\tilde{E}_p$ of E modulo p, obtained by reducing a minimal Weierstrass model of E modulo p, is non-singular. Then $\tilde{E}_p$ is itself an elliptic curve over the finite field $\mathbb{F}_p$, and we may consider the group $\tilde{E}_p(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\tilde{E}_p$.

There are various open questions surrounding the nature of the abelian groups $\tilde{E}_p(\mathbb{F}_p)$, as p varies. One such example is the following conjecture about the cyclicity of $\tilde{E}_p(\mathbb{F}_p)$, which underlies an elliptic curve analogue of Artin's primitive root conjecture that was proposed by S. Lang and H. Trotter in 1977 [25].

Conjecture 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E. There is a constant $C_E \geq 0$ such that*

$$\lim_{x\to\infty} \frac{|\{p \leq x : p \nmid N_E,\ \tilde{E}_p(\mathbb{F}_p) \text{ is cyclic}\}|}{|\{p \leq x\}|} = C_E.$$

Mathematics Subject Classification 2020: 11F80 (primary); 11G05 (secondary).
Keywords: elliptic curves, Galois representations, cyclicity.

In fact, the constant C_E is given explicitly by

$$C_E = \sum_{n \geq 1} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]},$$

where $\mu(\cdot)$ denotes the Möbius function and $\mathbb{Q}(E[n])$ the n-division field of E.

Regarding the positivity of C_E, J-P. Serre (see pp. 465–466 of [34]) observed that

$$C_E = 0 \iff E[2] \subseteq E(\mathbb{Q}) \tag{1.1}$$

(a proof of this may be found on p. 619 of [14]). When (1.1) holds, the embedding $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq E[2] = E(\mathbb{Q})[2] \hookrightarrow \tilde{E}_p(\mathbb{F}_p)$ (see for instance Proposition 3.1 in Chapter VII of [35]), valid for every odd prime $p \nmid N_E$, shows that

$$C_E = 0 \implies |\{p \text{ prime} : p \nmid N_E,\ \tilde{E}_p(\mathbb{F}_p) \text{ is cyclic}\}| \leq 1.$$

It is well known that $\tilde{E}_p(\mathbb{F}_p) \simeq \mathbb{Z}/d_p(E)\mathbb{Z} \times \mathbb{Z}/e_p(E)\mathbb{Z}$ for certain $d_p(E), e_p(E) \in \mathbb{N}$ with $d_p(E)$ dividing $e_p(E)$; obviously, this group is cyclic if and only if its size $|\tilde{E}_p(\mathbb{F}_p)|$ is equal to its exponent $e_p(E)$. The quantities $d_p(E)$ and $e_p(E)$ have been extensively studied (see [3,11,17,19] and the references therein). The question of cyclicity of $\tilde{E}_p(\mathbb{F}_p)$ seems to have first appeared in a paper by I. Borosh, C. J. Moreno, and H. Porta in 1975; see [7], which calculates the structures of $\tilde{E}_p(\mathbb{F}_p)$ for various elliptic curves E and many primes p, and expresses a version of Conjecture 1.1 without completely determining the constant C_E.

In 1979, J-P. Serre observed (see pp. 465–468 of [34]) that Conjecture 1.1 follows from the generalized Riemann hypothesis (denoted GRH) by adapting techniques from C. Hooley's GRH-conditional proof of Artin's primitive root conjecture [21]. In 1983, M. Ram Murty [31] gave a detailed proof of Serre's result and also established the same unconditionally for elliptic curves with complex multiplication (denoted CM). In 1990, R. Gupta and M. Ram Murty proved unconditionally that, for any elliptic curve E over $\mathbb{Q}$ satisfying $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, there are $\gg_E x/(\log x)^2$ many primes $p \leq x$ for which $\tilde{E}_p(\mathbb{F}_p)$ is cyclic. In 2002, A. C. Cojocaru [12] proved a non-CM version of Conjecture 1.1 under a weaker hypothesis than GRH. Specifically, Cojocaru proved the bound

$$|\{p \leq x : p \nmid N_E,\ \tilde{E}_p(\mathbb{F}_p) \text{ is cyclic}\}| - C_E|\{p \leq x\}| = O\Big(\frac{x \log\log x}{\log^2 x}\Big)$$

under a quasi-GRH, i.e., assuming that the Dedekind zeta functions of the division fields of E do not vanish for $\Re(s) > 3/4$; further improvements on this remainder term may be found in [12], [31], and [2] (see also Theorem 45 in [13]). In addition to the above-mentioned results, Conjecture 1.1 has also been proved "on average" over elliptic curves E of bounded height [4], a result that was later refined by the second author [26]. Finally, Conjecture 1.1 has recently been considered in the more general context of elliptic curves over arbitrary number fields [10], in which case the question of vanishing of the conjectural density becomes more delicate.

Inspired by Conjecture 1.1, Y. Akbal and A. M. Güloğlu [1] considered the question of cyclicity of $\tilde{E}_p(\mathbb{F}_p)$ for the subset of those primes p which lie in a fixed arithmetic

progression. Specifically, for any fixed $a, n \in \mathbb{N}$ with $\gcd(a, n) = 1$, let us define the counting function $\pi_{E,a,n}(x)$ by

$$\pi_{E,a,n}(x) := |\{p \le x : p \nmid N_E,\, p \equiv a \bmod n,\ \text{and } \tilde{E}_p(\mathbb{F}_p) \ \text{ is cyclic}\}|. \tag{1.2}$$

Akbal and Güloğlu proved the following theorem, wherein the constant $C_{E,a,n} \ge 0$ is given by

$$C_{E,a,n} := \sum_{d=1}^{\infty} \frac{\mu(d)\, \gamma_{a,n}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n) : \mathbb{Q}]}. \tag{1.3}$$

In this definition, ζ_n denotes a primitive n-th root of unity, and

$$\gamma_{a,n}(\mathbb{Q}(E[d])) := \begin{cases} 1 & \text{if } \sigma_a \text{ fixes } \mathbb{Q}(E[d]) \cap \mathbb{Q}(\zeta_n) \text{ pointwise,} \\ 0 & \text{otherwise,} \end{cases} \tag{1.4}$$

where $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ refers to the unique automorphism satisfying $\sigma_a(\zeta_n) = \zeta_n^a$.

Theorem 1.2 (Theorems 3 and 6 in [1]). *Let E be an elliptic curve defined over $\mathbb{Q}$ and assume that, if E has CM, then it has CM by the full ring of integers of an imaginary quadratic field. Furthermore, fix $n \in \mathbb{N}$ and, for each square-free $d \ge 1$, assume the generalized Riemann hypothesis for the Dedekind zeta function of the field $\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n)$. For any $a \in \mathbb{N}$ with $\gcd(a, n) = 1$, we then have*

$$\pi_{E,a,n}(x) = C_{E,a,n}\, \mathrm{Li}(x) + O_{E,n}(x^{5/6}(\log x)^{2/3}),$$

where $\mathrm{Li}(x) := \int_2^x \frac{1}{\log t} dt$ denotes the logarithmic integral.

In particular, under GRH, Akbal and Güloğlu proved that $\pi_{E,a,n}(x) \sim C_{E,a,n}\, \mathrm{Li}(x)$ as $x \to \infty$, provided the constant $C_{E,a,n}$ is positive, motivating the question: under what conditions is $C_{E,a,n}$ positive? The Ph.D. dissertation of J. Brau [9], which also considered this question, established the positivity of $C_{E,a,n}$ when E is a Serre curve and exhibited an explicit formula for it under a mild additional hypothesis that was later removed in joint work of the second author with J. Mayle and T. Wang [27]. Akbal and Güloğlu proved that $C_{E,a,n} > 0$ for any non-CM elliptic curve E over $\mathbb{Q}$, provided n is coprime with $30N_E$ and is not divisible by any prime ℓ for which $[\mathbb{Q}(E[\ell]) : \mathbb{Q}] < |\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|$. Regarding conditions on (E, a, n) sufficient to guarantee that $C_{E,a,n} = 0$, they noted (see p. 3 of [1]) that, for any elliptic curve E over $\mathbb{Q}$,

$$\begin{aligned} &\exists \text{ a prime } \ell \text{ such that } \mathbb{Q}(E[\ell]) \subseteq \mathbb{Q}(\zeta_n) \text{ and } \sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1 \\ &\qquad\qquad \Longrightarrow \lim_{x\to\infty} \pi_{E,a,n}(x) < \infty. \end{aligned} \tag{1.5}$$

As a consequence of Lemma 4.1 and Theorem 1.5 below, the left-hand condition above implies that $C_{E,a,n} = 0$, so the implication (1.5) is consistent with Theorem 1.2. Akbal and Güloğlu then posed the following question (see Question 1 in [1]).

Question 1.3. *Let E be an elliptic curve over $\mathbb{Q}$ and assume the notation as above. Is the converse of (1.5) true?*

The main purpose of this paper is to answer Question 1.3 in the negative via a concrete example (see Example 1.7 and Theorem 1.10 below), and to propose a biconditional analogue of (1.5). First, we give a definition.

Definition 1.4. For an elliptic curve E over $\mathbb{Q}$ and a pair (a,n) of relatively prime positive integers, we call an integer $m \geq 2$ an *acyclicity level for* (E,a,n) if

$$\begin{aligned} &\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q}) \text{ with } \sigma|_{\mathbb{Q}(\zeta_n)} = \sigma_a, \\ &\qquad\qquad \exists \text{ a prime } \ell \mid m \text{ for which } \sigma|_{\mathbb{Q}(E[\ell])} \equiv 1. \end{aligned} \tag{1.6}$$

We further call m a *minimal* acyclicity level for (E,a,n) if no proper divisor m' of m is an acyclicity level for (E,a,n). We call m a (*minimal*) *acyclicity level for* E if it is a (minimal) acyclicity level for (E,a,n) for some pair (a,n) of relatively prime positive integers. Finally, we call E an *acyclicity elliptic curve* if E has an acyclicity level.

Here is our proposed biconditional analogue of (1.5), which articulates a precise (conjectural) interpretation of when $\lim_{x\to\infty} \pi_{E,a,n}(x) < \infty$ in terms of division fields of E:

$$\text{there exists an acyclicity level for } (E,a,n) \iff \lim_{x\to\infty} \pi_{E,a,n}(x) < \infty. \tag{1.7}$$

In fact, we will prove the following theorem connecting the left-hand side of (1.7) with the constant $C_{E,a,n}$.

Theorem 1.5. *Let E be an elliptic curve over $\mathbb{Q}$, let (a,n) be a pair of relatively prime positive integers, and let the constant $C_{E,a,n}$ be defined by (1.3). We then have*:

$$\textit{there exists an acyclicity level for } (E,a,n) \iff C_{E,a,n} = 0.$$

Remark 1.6. By the nature of the defining condition (1.6), it follows that if m is an acyclicity level of an elliptic curve E, then $\prod_{\ell\mid m} \ell$ is also an acyclicty level for E. Thus, acyclicty levels of elliptic curves may always be taken to be square-free, and minimal acyclicity levels are *necessarily* square-free.

The condition on the left-hand side of (1.5) is equivalent to the existence of a *prime* acyclicity level (namely, ℓ) for (E,a,n) (see Lemma 4.1 below). For the following elliptic curve E, the left-hand condition in (1.5) is false while the right-hand condition in (1.5) is true (E has minimal acyclicity level $m = 6$).

Example 1.7. Let E be the (non-CM) elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$E:\ y^2 + xy + y = x^3 + 32271697x - 1200056843302.$$

The conductor of E is $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 31$; its LMFDB label is $71610.s6$ (see [28]), and its Cremona label is $71610s4$. Furthermore, we have:

(1) the counting function $\pi_{E,3,8}(x)$ defined by (1.2) satisfies $\pi_{E,3,8}(x) = 0$ for all $x \geq 0$;
(2) for each prime ℓ, $\mathbb{Q}(E[\ell]) \not\subseteq \mathbb{Q}(\zeta_8)$.

We remark that, for any elliptic curve E over $\mathbb{Q}$ that satisfies the left-hand condition in (1.5), $\tilde{E}_p(\mathbb{F}_p)$ fails to be cyclic for good primes $p \equiv a \bmod n$ because there exists a prime ℓ such that $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \subseteq \tilde{E}_p(\mathbb{F}_p)$ for every such p. In contrast, for the elliptic

curve E of Example 1.7, the reason that $\tilde{E}_p(\mathbb{F}_p)$ is not cyclic for any good prime $p \equiv 3 \bmod 8$ is that, for any such prime, either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq \tilde{E}_p(\mathbb{F}_p)$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \subseteq \tilde{E}_p(\mathbb{F}_p)$. For more details, see Remark 1.12 below.

We propose the following refinement of Question 1 in [1].

Conjecture 1.8. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E, let (a, n) be a pair of relatively prime positive integers, and suppose that there does* not *exist an acyclicity level for (E, a, n). Then*

$$\pi_{E,a,n}(x) \sim C_{E,a,n} \operatorname{Li}(x),$$

as $x \to \infty$, where $C_{E,a,n} > 0$ is defined as in (1.3).

Remark 1.9. Let us clarify what is known and what is conjectured. Conjecture 1.8 is known to be true for CM curves due to the work of P.-J. Wong [37], and to follow from the GRH for non-CM curves by Theorem 1.2. In case (E, a, n) *does* have an acyclicity level, it follows that $\lim_{x\to\infty} \pi_{E,a,n}(x) < \infty$ by a straightforward application of the Chebotarev density theorem.

The elliptic curve E in Example 1.7 is a specialization of an elliptic curve $\mathbb{E}$ defined over $\mathbb{Q}(t, d)$, infinitely many of whose specializations satisfy conditions (1) and (2) of Example 1.7, with appropriately chosen $a, n \in \mathbb{N}$ replacing 3 and 8, respectively. To describe $\mathbb{E}$, first define the polynomials $f(t), g(t) \in \mathbb{Q}[t]$ by

$$\begin{aligned} f(t) &:= 16t^6 - 24t^4 - 8t^3 + 36t^2 + 6t + 1, \\ g(t) &:= 64t^8 + 64t^7 + 64t^6 - 128t^5 - 56t^4 + 16t^3 + 64t^2 - 8t + 1. \end{aligned} \tag{1.8}$$

Next, define the Weierstrass coefficients $a_4(t), a_6(t) \in \mathbb{Q}(t)$ by

$$\begin{aligned} a_4(t) &:= \frac{-108(4t^3-1)^3(4t^3+6t-1)^3 f(t)^3}{(2t^2+2t-1)^2(4t^4-4t^3+6t^2+2t+1)^2(8t^4-8t^3-8t-1)^2 g(t)^2}, \\ a_6(t) &:= \frac{-432(4t^3-1)^3(4t^3+6t-1)^3 f(t)^3}{(2t^2+2t-1)^2(4t^4-4t^3+6t^2+2t+1)^2(8t^4-8t^3-8t-1)^2 g(t)^2}, \end{aligned}$$

where $f(t)$ and $g(t)$ are as in (1.8). Finally, define the elliptic curve $\mathbb{E}$ over $\mathbb{Q}(t, d)$ by the Weierstrass equation

$$\mathbb{E}: \; y^2 = x^3 + d^2 a_4(t) x + d^3 a_6(t). \tag{1.9}$$

The j-invariant $j_{\mathbb{E}}(t)$ and discriminant $\Delta_{\mathbb{E}}(t)$ of $\mathbb{E}$ are given by

$$j_{\mathbb{E}}(t) = \frac{(4t^3-1)^3(4t^3+6t-1)^3 f(t)^3}{t^3(t-1)^3(2t+1)^6(t^2+t+1)^3(4t^2-2t+1)^6}, \tag{1.10}$$

$$\Delta_{\mathbb{E}}(t) = \frac{2^{18}3^{12}d^6t^3(t-1)^3(2t+1)^6(t^2+t+1)^3(4t^2-2t+1)^6(4t^3-1)^6(4t^3+6t-1)^6 f(t)^6}{(2t^2+2t-1)^6(4t^4-4t^3+6t^2+2t+1)^6(8t^4-8t^3-8t-1)^6 g(t)^6}.$$

To clarify how specializations of $\mathbb{E}$ are related to Question 1.3, let $h_2(t), h_3(t) \in \mathbb{Q}(t)$ be defined by

$$\begin{aligned} h_2(t) &:= t(t-1)(t^2+t+1), \\ h_3(t) &:= \frac{6(4t^3-1)(4t^3+6t-1)(2t^2+2t-1)f(t)g(t)}{(4t^4-4t^3+6t^2+2t+1)(8t^4-8t^3-8t-1)}, \end{aligned} \tag{1.11}$$

where $f(t)$ and $g(t)$ are as in (1.8). A computation involving the appropriate division polynomials associated to $\mathbb{E}$ demonstrates that

$$\mathbb{Q}(t,d)(\mathbb{E}[2]) = \mathbb{Q}(t,d)\big(\sqrt{h_2(t)}\big), \quad \mathbb{Q}(t,d)(\mathbb{E}[3]) = \mathbb{Q}(t,d)\big(\sqrt{dh_3(t)}, \sqrt{-3}\big). \tag{1.12}$$

For any $t_0 \in \mathbb{Q} - \{0, 1, -1/2\}$ and $d_0 \in \mathbb{Q} - \{0\}$, we may consider the specialization $\mathbb{E}_{t_0,d_0}$ of $\mathbb{E}$ at (t_0, d_0), which is an elliptic curve over $\mathbb{Q}$. Furthermore, (1.12) specializes to

$$\mathbb{Q}(\mathbb{E}_{t_0,d_0}[2]) = \mathbb{Q}\big(\sqrt{h_2(t_0)}\big), \quad \mathbb{Q}(\mathbb{E}_{t_0,d_0}[3]) = \mathbb{Q}\big(\sqrt{d_0h_3(t_0)}, \sqrt{-3}\big). \tag{1.13}$$

In particular, we see that $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3])$ is either equal to $\mathbb{Q}(\sqrt{-3})$ or is a biquadratic extension of $\mathbb{Q}$ which contains $\mathbb{Q}(\sqrt{-3})$ as a subfield. In the latter case, $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3])$ contains three quadratic subfields, exactly two of which are ramified at the prime 3; in either case let us denote by

$$n_3(t_0, d_0) := \begin{cases} d_0 h_3(t_0) & \text{if 3 is unramified in } \mathbb{Q}\big(\sqrt{d_0h_3(t_0)}\big), \\ -3d_0 h_3(t_0) & \text{otherwise.} \end{cases}$$

Thus,

$$\big\{\mathbb{Q}(\sqrt{n_3(t_0,d_0)}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-3n_3(t_0,d_0)})\big\}$$

is the set of all quadratic subfields of $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3])$, and

$$\big\{\mathbb{Q}\big(\sqrt{-3}\big), \mathbb{Q}\big(\sqrt{-3n_3(t_0,d_0)}\big)\big\}$$

is the subset of those quadratic subfields that are ramified at 3. Finally, we define $n_0 \in \mathbb{N}$ by

$$n_0 := \operatorname{lcm}\big(\big|\operatorname{disc}\mathbb{Q}\big(\sqrt{-3h_2(t_0)}\big)\big|, \big|\operatorname{disc}\mathbb{Q}\big(\sqrt{-3n_3(t_0,d_0)h_2(t_0)}\big)\big|\big). \tag{1.14}$$

Note that, in case $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3]) = \mathbb{Q}(\sqrt{-3})$, we simply have

$$\mathbb{Q}(\sqrt{-3n_3(t_0,d_0)}) = \mathbb{Q}(\sqrt{-3}) \quad \text{and} \quad n_0 = |\operatorname{disc}\mathbb{Q}(\sqrt{-3h_2(t_0)})|.$$

In either case, n_0 is the smallest positive integer for which the containment

$$\mathbb{Q}\big(\sqrt{-3h_2(t_0)}, \sqrt{-3n_3(t_0,d_0)h_2(t_0)}\big) \subseteq \mathbb{Q}(\zeta_{n_0}) \tag{1.15}$$

holds. In Section 2, we will prove the following theorem.

Theorem 1.10. *Let the elliptic curve $\mathbb{E}$ over $\mathbb{Q}(t,d)$ be given by (1.9), and let $h_2(t), h_3(t) \in \mathbb{Q}(t)$ be as in (1.11), so that (1.12) holds.*

(a) *For any* $t_0 \in \mathbb{Q} - \{0, 1, -1/2\}$ *and* $d_0 \in \mathbb{Q} - \{0\}$, *the specialization* $\mathbb{E}_{t_0,d_0}$ *of* $\mathbb{E}$ *at* (t_0, d_0) *is an elliptic curve over* $\mathbb{Q}$. *For any elliptic curve* E *defined over* $\mathbb{Q}$ *satisfying* $j_E \notin \{0, 1728\}$, E *satisfies*

$$[\mathbb{Q}(E[2]) : \mathbb{Q}] \leq 2 \quad \textit{and} \quad [\mathbb{Q}(E[3]) : \mathbb{Q}] \leq 4$$

if and only if E *is isomorphic over* $\mathbb{Q}$ *to a specialization* $\mathbb{E}_{t_0,d_0}$ *for some* $t_0 \in \mathbb{Q} - \{0, 1, -1/2\}$ *and* $d_0 \in \mathbb{Q} - \{0\}$.

(b) *Suppose* $t_0 \in \mathbb{Q} - \{0, 1, -1/2\}$ *and* $d_0 \in \mathbb{Q} - \{0\}$ *are chosen so that*

$$\mathbb{Q}(\mathbb{E}_{t_0,d_0}[2]) \not\subseteq \mathbb{Q}(\mathbb{E}_{t_0,d_0}[3]). \tag{1.16}$$

Let $\{\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-3n_3(t_0, d_0)})\}$ *denote the set consisting of every quadratic subfield of* $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3])$ *in which the prime* 3 *ramifies. Define* $n_0 \in \mathbb{N}$ *by* (1.14) (*note that* (1.15) *then holds*), *and let* $a_0 \in \mathbb{Z}$ *be any integer coprime to* n_0 *such that the automorphism* $\sigma_{a_0} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{n_0})/\mathbb{Q})$ *satisfies*

$$\begin{aligned} \sigma_{a_0}\big(\sqrt{-3h_2(t_0)}\big) &= -\sqrt{-3h_2(t_0)}, \\ \sigma_{a_0}\big(\sqrt{-3n_3(t_0, d_0)h_2(t_0)}\big) &= -\sqrt{-3n_3(t_0, d_0)h_2(t_0)}. \end{aligned} \tag{1.17}$$

(*Note that, by* (1.16), *neither* $\sqrt{-3h_2(t_0)}$ *nor* $\sqrt{-3n_3(t_0, d_0)h_2(t_0)}$ *are in* $\mathbb{Q}$.) *We then have that, for each prime* $p \geq 5$ *of good reduction for* $\mathbb{E}_{t_0,d_0}$ *with* $p \equiv a_0 \bmod n_0$, *the group* $(\widetilde{\mathbb{E}_{t_0,d_0}})_p(\mathbb{F}_p)$ *is not cyclic. In particular, for each* $x \geq 0$, *we have* $\pi_{(\mathbb{E}_{t_0,d_0}),a_0,n_0}(x) \leq 2$.

(c) *Assume further that* $t_0 \in \mathbb{Q} - \{0, 1, -1/2\}$ *and* $d_0 \in \mathbb{Q} - \{0\}$ *are chosen so that* 3 *ramifies in* $\mathbb{Q}(\sqrt{h_2(t_0)})$ *and* 5 *does not ramify in* $\mathbb{Q}(\sqrt{-3h_2(t_0)}, \sqrt{-3n_3(t_0, d_0)h_2(t_0)})$. *Then, for each prime* ℓ, *we have* $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[\ell]) \not\subseteq \mathbb{Q}(\zeta_{n_0})$.

It follows from Theorem 1.10 that there exist infinitely many j-invariants corresponding to elliptic curves E over $\mathbb{Q}$ that answer Question 1.3 in the negative:

Corollary 1.11. *There are infinitely many* $j_E \in \mathbb{Q}$, *where each* j_E *is the* j*-invariant of an elliptic curve* E *over* $\mathbb{Q}$ *for which there exist coprime* $a, n \in \mathbb{N}$ *such that, for each* $x \geq 0$, $\pi_{E,a,n}(x) \leq 2$ *in spite of the fact that, for each prime* ℓ, $\mathbb{Q}(E[\ell]) \not\subseteq \mathbb{Q}(\zeta_n)$.

Proof. A straightforward calculation shows that, if $u_0 \in \mathbb{Z}_{(3)} \cap \mathbb{Z}_{(5)} \cap \mathbb{Z}_{(7)} \subseteq \mathbb{Q}$ and we take $t_0 := 21(15u_0 - 1)$, then the 3-adic, 5-adic and 7-adic valuations of $h_2(t_0) = t_0(t_0 - 1)(t_0^2 + t_0 + 1)$ are given by

$$v_3(h_2(t_0)) = 1, \quad v_5(h_2(t_0)) = 0, \quad \text{and} \quad v_7(h_2(t_0)) = 1.$$

Thus, 3 and 7 are ramified and 5 is unramified in $\mathbb{Q}(\sqrt{h_2(t_0)})$, and in particular this implies that

$$5 \text{ is unramified in the field } \mathbb{Q}\big(\sqrt{-3h_2(t_0)}\big). \tag{1.18}$$

Next, choosing $d_0 \in \mathbb{Q}$ so that

$$v_3(d_0 h_3(t_0)) = 0, \quad v_5(d_0 h_3(t_0)) = 0, \quad \text{and} \quad v_7(d_0 h_3(t_0)) = 0,$$

the primes 3, 5 and 7 are unramified in $\mathbb{Q}(\sqrt{d_0 h_3(t_0)})$. It follows from this and (1.13) that 7 is unramified in $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3])$ and ramified in $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[2])$, and so (1.16) holds. Furthermore, we have that $\mathbb{Q}(\sqrt{-3n_3(t_0,d_0)}) = \mathbb{Q}(\sqrt{-3d_0 h_3(t_0)})$, and this field is evidently unramified at 5. It follows from this and (1.18) that 5 is unramified in the field $\mathbb{Q}(\sqrt{-3h_2(t_0)}, \sqrt{-3n_3(t_0,d_0)h_2(t_0)})$. Thus, the conditions of parts (b) and (c) of Theorem 1.10 are satisfied, and so the specialized curve $E := \mathbb{E}_{t_0,d_0}$, together with the numbers $a_0 \in \mathbb{Z}$ and $n_0 \in \mathbb{N}$ as described in part (b), furnish an example with $\pi_{E,a_0,n_0}(x) \leq 2$ for every $x \geq 0$ even though $\mathbb{Q}(E[\ell]) \not\subseteq \mathbb{Q}(\zeta_{n_0})$ for every prime ℓ. ∎

Remark 1.12. Taking $t_0 = 3/5$ and $d_0 = -28\,910\,265\,879\,522\,405\,941\,333\,082$, we see that the specialization $\mathbb{E}_{t_0,d_0}$ is isomorphic over $\mathbb{Q}$ to the elliptic curve E of Example 1.7. For this specialization, we have

$$\mathbb{Q}(E[2]) = \mathbb{Q}\big(\sqrt{h(t_0)}\big) = \mathbb{Q}(\sqrt{-6}), \quad \mathbb{Q}(E[3]) = \mathbb{Q}\big(\sqrt{d_0 h_3(t_0)}, \sqrt{-3}\big) = \mathbb{Q}(\sqrt{-3}).$$

In particular, $\mathbb{Q}(E[2]) \not\subseteq \mathbb{Q}(E[3])$. Furthermore, taking $n = 8$ and $a = 3$, we see that $\mathbb{Q}(E[6]) \cap \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2})$, and (1.17) simply becomes

$$\sigma_3(\sqrt{2}) = -\sqrt{2}.$$

Thus, any $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q})$ whose restriction to $\mathbb{Q}(E[6]) \cap \mathbb{Q}(\zeta_8)$ agrees with that of σ_3 must act trivially either on $\mathbb{Q}(E[2])$ or on $\mathbb{Q}(E[3])$, so $m = 6$ is an acyclicity level for $(E, 3, 8)$. Since 2 and 3 divide N_E, we have that $\pi_{E,3,8}(x) = 0$ for all $x \geq 0$ (similar reasoning shows that $\pi_{E,5,8}(x) = 0$). Finally, 3 ramifies in $\mathbb{Q}(E[2])$ and 5 does not ramify in $\mathbb{Q}(E[6])$, so by part (c) of Theorem 1.10, we have $\mathbb{Q}(E[\ell]) \not\subseteq \mathbb{Q}(\zeta_8)$ for each prime ℓ.

Remark 1.13. For any elliptic curve E over $\mathbb{Q}$ and pair (a, n) of relatively prime positive integers, Theorems 1 and 2 of [1] give, for any $A \geq 2$, an unconditional lower bound

$$\frac{x}{(\log x)^A} \ll \pi_{E,a,n}(x), \tag{1.19}$$

provided none of the following four situations occurs:

(i) There is an odd prime dividing $\gcd(a-1, n)$.

(ii) The containment $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_n)$ holds and σ_a fixes $\mathbb{Q}(E[2])$ pointwise.

(iii) The conductor n_2 of the field $\mathbb{Q}(\sqrt{\Delta_E})$ satisfies that $n_2 = 3\gcd(n_2, n)$ and that $\chi_{-\delta_2/3}(a) = -1$, where δ_2 denotes the discriminant of $\mathbb{Q}(\sqrt{\Delta_E})$.

(iv) The containments $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_n)$ hold and σ_a fixes $\mathbb{Q}(\sqrt{\Delta_E})$ pointwise.

Whenever cases are excluded from a theorem, it is helpful to know which excluded cases arise just from limitations in the proof technique and which cases are excluded because they can actually contain instances for which the stated result is false. We endeavor here to shed light on the above four excluded cases in this regard. Considering case (i), for each $\ell \in \{3, 5\}$ it is possible (e.g., using results in [38]) to construct

an elliptic curve E over $\mathbb{Q}$ for which $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ is abelian. If we choose (a, n) such that $\mathbb{Q}(E[\ell]) \subseteq \mathbb{Q}(\zeta_n)$ and $\sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1$, then by (1.5), the bound (1.19) will be false. Furthermore, since $\mathbb{Q}(\zeta_\ell) \subseteq \mathbb{Q}(E[\ell])$, in this case ℓ divides n and $a \equiv 1 \bmod \ell$, which implies that $\gcd(a-1, n)$ is divisible by ℓ. We see that case (i) contains instances where (1.19) is false. For the same reason, if E satisfies (ii) then (1.19) is necessarily false. Case (iii) has the most relevance to the present paper, since every specialization $E = \mathbb{E}_{t_0,d_0}$ of $\mathbb{E}$ that gives rise to a negative answer to Question 1.3 satisfies the property stated therein. Thus, case (iii) contains instances where (1.19) is false. Finally, if we are in case (iv) but not in case (ii), then $\mathbb{Q}(E[2])$ is nonabelian of degree 6 over $\mathbb{Q}$, and hence we cannot have $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_n)$. It is unclear whether case (iv) contains any instances where (1.19) is false that are not already covered by the other three cases.

It is natural to ask: are there any examples of acyclicity elliptic curves E over $\mathbb{Q}$ for which the left-hand condition in (1.5) fails to hold other than those arising from specializations of $\mathbb{E}$? Could there be, hidden in the excluded cases mentioned in Remark 1.13, *other* elliptic curves with composite minimal acyclicity levels? By couching everything in terms of modular curves, translating the condition "E has a composite minimal acyclicity level" into group-theoretical information about $\rho_E(G_{\mathbb{Q}})$, and performing a computer calculation, we are also able to prove the following theorem, which partially addresses these questions.

Theorem 1.14. *Fix $m \in \mathbb{N}$ and define the set*

$$\mathcal{J}_m := \{j \in \mathbb{Q} : \exists E \text{ over } \mathbb{Q},\ m \text{ is a minimal acyclicity level for } E, \text{ and } j_E = j\}. \tag{1.20}$$

In case $m = \ell$ is prime, we have

$$|\mathcal{J}_\ell| = \infty \iff \mathcal{J}_\ell \neq \emptyset \iff \ell \in \{2, 3, 5\},$$

whereas in case m is composite, we have

$$|\mathcal{J}_m| = \infty \iff m = 6.$$

Furthermore, in case $\ell \in \{2, 3, 5\}$, each $j \in \mathcal{J}_\ell$ is the j-invariant of an elliptic curve E over $\mathbb{Q}$ for which there is a pair (a, n) of relatively prime positive integers satisfying $\mathbb{Q}(E[\ell]) \subseteq \mathbb{Q}(\zeta_n)$ and $\sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1$. In case $m = 6$, we have $\mathcal{J}_6 \subseteq j_{\mathbb{E}}(\mathbb{Q})$, where $j_{\mathbb{E}}$ is as in (1.10).

Remark 1.15. If $m \in \mathbb{N}$ is composite and $m \neq 6$, Theorem 1.14 asserts that $\mathcal{J}_m$ is finite, and one can ask for conditions on m which guarantee that $\mathcal{J}_m = \emptyset$. Serre's uniformity question (see p. 299 in Section 4.3 of [33] and also Conjecture 1.12 in [38]) asks whether, for each prime $\ell > 37$ and for each non-CM elliptic curve E over $\mathbb{Q}$, one has $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Despite significant progress (see [30], [5], [6]), this question remains open. Assuming an affirmative answer to it, we may see that, whenever m is divisible by a prime $\ell > 37$, $\mathcal{J}_m = \emptyset$. Thus, an affirmative answer to Serre's uniformity question implies that there are only finitely many j-invariants of acyclicity elliptic curves over $\mathbb{Q}$ having minimal acyclicity level that does not belong to $\{2, 3, 5, 6\}$.

2. Proof of Theorem 1.10

The proof of Theorem 1.10 falls naturally into three pieces. We will first prove the statements in part (a) of the theorem, and then we will prove the statements in parts (b) and (c). At various points in the proof (and later in the paper) we will make use of the symbols

$$\begin{aligned} \rho_E &: G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}), \\ \rho_{E,n} &: G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \end{aligned} \tag{2.1}$$

which denote the continuous Galois representations defined by letting $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on the adelic Tate module $T(E) := \varprojlim E[n]$ (respectively, on the n-torsion $E[n]$) of E, and choosing a $\hat{\mathbb{Z}}$-basis (respectively, a $\mathbb{Z}/n\mathbb{Z}$-basis) thereof. Furthermore, if $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is any subgroup and $n \in \mathbb{N}$, we will denote by $G(n) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the image of G under the projection map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Note that, with these conventions, if $G_E := \rho_E(G_{\mathbb{Q}})$ then, for an appropriate choice of basis, we have $G_E(n) = \rho_{E,n}(G_{\mathbb{Q}})$. When d divides n, we will use the symbol $\pi_{n,d} : \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ to denote the canonical projection map. We will denote by 1 the identity element of any group, except when the group is a matrix group, in which case we may use the symbol I to denote the identity matrix.

2.1. Preliminaries on modular curves

Suppose that $\tilde{G} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is an open subgroup (equivalently, a subgroup of finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$) which additionally satisfies

$$-I \in \tilde{G} \quad \text{and} \quad \det \tilde{G} = \hat{\mathbb{Z}}^{\times}.$$

There is then associated to $\tilde{G}$ a smooth, projective, geometrically irreducible curve $X_{\tilde{G}}$ defined over $\mathbb{Q}$. This modular curve $X_{\tilde{G}}$ comes equipped with a forgetful map

$$j_{\tilde{G}} : X_{\tilde{G}} \longrightarrow X(1) \xrightarrow{\simeq} \mathbb{P}^1.$$

Furthermore, for every elliptic curve E over $\mathbb{Q}$ whose j-invariant j_E satisfies $j_E \notin \{0, 1728\}$, we have that $\rho_E(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\hat{\mathbb{Z}})$-conjugate to a subgroup of $\tilde{G}^{\mathsf{T}} := \{g^{\mathsf{T}} : g \in \tilde{G}\}$ (where g^{T} denotes the transpose of the matrix g) if and only if $j_E \in j_{\tilde{G}}(X_{\tilde{G}}(\mathbb{Q}))$. We may also define a generic Weierstrass model over the field $\mathbb{Q}(d)(X_{\tilde{G}})$ by

$$\mathbb{E}^{(\tilde{G})} : y^2 = x^3 + \frac{108\, d^2 j_{\tilde{G}}}{1728 - j_{\tilde{G}}}\, x + \frac{432\, d^3 j_{\tilde{G}}}{1728 - j_{\tilde{G}}},$$

whose j-invariant is $j_{\tilde{G}}$. For any $t_0 \in X_{\tilde{G}}(\mathbb{Q}) - j_{\tilde{G}}^{-1}(\{0, 1728, \infty\})$ and $d_0 \in \mathbb{Q}^{\times}$, we may consider the specialization

$$\mathbb{E}^{(\tilde{G})}_{t_0,d_0} : y^2 = x^3 + \frac{108\, d_0^2 j_{\tilde{G}}(t_0)}{1728 - j_{\tilde{G}}(t_0)}\, x + \frac{432\, d_0^3 j_{\tilde{G}}(t_0)}{1728 - j_{\tilde{G}}(t_0)},$$

which is an elliptic curve over $\mathbb{Q}$. For any elliptic curve E over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$, we have that $j_E \in j_{\tilde{G}}(X_{\tilde{G}}(\mathbb{Q}))$ if and only if E is isomorphic over $\mathbb{Q}$ to such a specialization $\mathbb{E}^{(\tilde{G})}_{t_0,d_0}$. Henceforth, let us use the following notation: for subgroups $H_1, H_2 \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$,

$$H_1 \dot{\subseteq} H_2 \overset{\text{def}}{\iff} \exists g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \text{ such that } gH_1g^{-1} \subseteq H_2,$$
$$H_1 \doteq H_2 \overset{\text{def}}{\iff} \exists g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \text{ such that } gH_1g^{-1} = H_2.$$

For any $m \in \mathbb{N}$, we define the relation $H_1 \dot{\subseteq} H_2$ for subgroups $H_1, H_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ similarly as subset containment up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Summarizing the above, for all $E/\mathbb{Q}$ with $j_E \notin \{0, 1728\}$, we have

$$\begin{aligned} \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}^{\mathsf{T}} &\iff j_E \in j_{\tilde{G}}(X_{\tilde{G}}(\mathbb{Q})) \\ &\iff \exists t_0 \in X_{\tilde{G}}(\mathbb{Q}), d_0 \in \mathbb{Q}^{\times} \text{ with } E \simeq_{\mathbb{Q}} \mathbb{E}^{(\tilde{G})}_{t_0,d_0}. \end{aligned} \tag{2.2}$$

For full details, we refer the reader to [16] (see also [32] for a helpful discussion about left versus right action of GL_2 on the underlying complete modular curve, which is responsible for the appearance of the transposed group $\tilde{G}^{\mathsf{T}}$ in (2.2)). In case we wish to use modular curves as above to study the question of which elliptic curves E satisfy $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G^{\mathsf{T}}$ for an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ for which $-I \notin G$, we will always first enlarge G by setting

$$\tilde{G} := \langle G, -I \rangle \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

2.2. Proof of part (a) of Theorem 1.10

Let the Borel subgroup $\mathcal{B}(2) \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and the split Cartan subgroup $\mathcal{C}_s(3) \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ be defined by

$$\mathcal{B}(2) := \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}),$$
$$\mathcal{C}_s(3) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in (\mathbb{Z}/3\mathbb{Z})^{\times} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$

Let $G(6) \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ be the subgroup that corresponds to $\mathcal{B}(2) \times \mathcal{C}_s(3)$ under the isomorphism

$$\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$$

of the Chinese remainder theorem and define

$$G_6 := \pi^{-1}(G(6)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

where $\pi : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ is the usual projection map.

Since $-I \in G_6$ and $\det(G_6) = \hat{\mathbb{Z}}^{\times}$, we are in the setting of the previous section, and so there is a smooth, projective, geometrically irreducible modular curve X_{G_6} with a forgetful map $j_{G_6} : X_{G_6} \to X(1) \simeq \mathbb{P}^1$, and we denote the generic Weierstrass model $\mathbb{E}^{(G_6)}$ simply

by $\mathbb{E}$. The specializations $\mathbb{E}_{t_0,d_0}$ of this Weierstrass model satisfy the property that, for each elliptic curve E over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$,

$$\begin{aligned} \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_6^{\mathsf{T}} &\iff j_E \in j_{G_6}(X_{G_6}(\mathbb{Q})) \\ &\iff \exists t_0 \in X_{G_6}(\mathbb{Q}), d_0 \in \mathbb{Q}^\times \text{ with } E \simeq_{\mathbb{Q}} \mathbb{E}_{t_0,d_0}. \end{aligned} \tag{2.3}$$

Moreover, a calculation shows that X_{G_6} has genus zero and satisfies $X_{G_6}(\mathbb{Q}) \neq \emptyset$. Thus, $X_{G_6} \simeq_{\mathbb{Q}} \mathbb{P}^1$, and, fixing a parameter t on X_{G_6}, the above-mentioned forgetful map may be realized as a rational map $j_{\mathbb{E}} \colon \mathbb{P}^1(t) \to \mathbb{P}^1(j)$ making the diagram

$$\begin{array}{ccccc} & & \overset{\text{forgetful map } j_{G_6}}{\curvearrowright} & & \\ X_{G_6} & \xrightarrow{\simeq} & \mathbb{P}^1_{\mathbb{Q}}(t) & \xrightarrow{j_{\mathbb{E}}} & \mathbb{P}^1_{\mathbb{Q}}(j) \end{array} \tag{2.4}$$

commute. Our goal is to produce a rational function $j_{\mathbb{E}}(t) \in \mathbb{Q}(t)$ that represents the above rational map $j_{\mathbb{E}}$.

As may be deduced from Theorems 1.1 and 1.2 of [38] (see also Tables 1 and 3 of [36]), for any elliptic curve E over $\mathbb{Q}$ with j-invariant $j_E \notin \{0, 1728\}$, we have that

$$\begin{aligned} [\mathbb{Q}(E[2]) : \mathbb{Q}] \leq 2 &\iff \rho_{E,2}(G_{\mathbb{Q}}) \dot{\subseteq} \mathcal{B}(2) \\ &\iff \exists t_0 \in \mathbb{Q} \text{ with } j_E = 256\,\frac{(t_0+1)^3}{t_0}, \\ [\mathbb{Q}(E[3]) : \mathbb{Q}] \leq 4 &\iff \rho_{E,3}(G_{\mathbb{Q}}) \dot{\subseteq} \mathcal{C}_s(3) \\ &\iff \exists t_0 \in \mathbb{Q} \text{ with } j_E = 27\,\frac{(t_0+1)^3(t_0+3)^3(t_0^2+3)^3}{t_0^3(t_0^2+3t_0+3)^3}. \end{aligned} \tag{2.5}$$

Thus, an elliptic curve E over $\mathbb{Q}$ simultaneously satisfies each of the left-hand conditions if and only if j_E is simultaneously a value of each of the rational functions on the right-hand side of (2.5), and we are led to the algebraic curve defined by

$$X_{G_6} : \; 256\,\frac{(u+1)^3}{u} = 27\,\frac{(v+1)^3(v+3)^3(v^2+3)^3}{v^3(v^2+3v+3)^3} \qquad \text{(singular model)}. \tag{2.6}$$

Using `Magma` [8] to resolve the singularities, we arrive at the rational functions

$$v = \frac{4t^3-3t-1}{3t}, \quad u = 256\,\frac{t^3(t-1)^3(t^2+t+1)^3}{(2t+1)^3(4t^2-2t+1)^3}.$$

Substituting these into (2.6) yields equality, and the resulting rational function $j_{\mathbb{E}}(t) \in \mathbb{Q}(t)$ is as in (1.10). Viewing $t \in \mathbb{Q}(X_{G_6})$, we have $\mathbb{Q}(X_{G_6}) = \mathbb{Q}(t)$, and $j_{\mathbb{E}}(t)$ may be taken to define the rational map $j_{\mathbb{E}}$ in (2.4). Part (a) of Theorem 1.10 then follows from this and (2.5), (2.6) and (2.3).

2.3. Proof of part (b) of Theorem 1.10

The proof of part (b) of Theorem 1.10 will utilize the following lemma, which, for any elliptic curve E over $\mathbb{Q}$, interprets the acyclicity of $\tilde{E}_p(\mathbb{F}_p)$ for a good prime p in terms of p splitting completely in an appropriate division field of E.

Lemma 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E, and p a prime with $p \nmid N_E$. Let $\ell \neq p$ be a prime. Then $\tilde{E}_p(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ if and only if p splits completely in $\mathbb{Q}(E[\ell])$.*

Proof. See Lemma 2.1 in [14]. ∎

Now let $\mathbb{E}$ be as in (1.9), let $t_0 \in \mathbb{Q} - \{0, 1, -1/2\}$ and $d_0 \in \mathbb{Q} - \{0\}$ satisfy the conditions in part (b) of Theorem 1.10, and let $\mathbb{E}_{t_0,d_0}$ be the specialization of $\mathbb{E}$ at (t_0, d_0). Let $n_0 \in \mathbb{N}$ be as in (1.14) and let $a_0 \in \mathbb{Z}$ be chosen coprime with n_0 and so that (1.17) holds. We will verify that, for each $x \geq 0$, $\pi_{(\mathbb{E}_{t_0,d_0}),a_0,n_0}(x) \leq 2$.

Consider the field

$$\mathbb{Q}(\mathbb{E}_{t_0,d_0}[6]) = \mathbb{Q}\big(\sqrt{h_2(t_0)}, \sqrt{-3n_3(t_0,d_0)}, \sqrt{-3}\big).$$

It follows from (1.17) that, for any prime $p \equiv a_0 \bmod n_0$, the automorphism $\sigma_p = \sigma_{a_0} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{n_0})/\mathbb{Q})$ must either act trivially on

$$\mathbb{Q}(\sqrt{h_2(t_0)}) = \mathbb{Q}(\mathbb{E}_{t_0,d_0}[2]) \quad \text{or on} \quad \mathbb{Q}(\sqrt{-3}, \sqrt{-3n_3(t_0,d_0)}) = \mathbb{Q}(\mathbb{E}_{t_0,d_0}[3]).$$

It then follows from Lemma 2.1 that, for each prime $p \geq 5$ of good reduction for $\mathbb{E}_{t_0,d_0}$, the group $(\widetilde{\mathbb{E}_{t_0,d_0}})_p(\mathbb{F}_p)$ either contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. In particular, for every good prime $p \geq 5$, $(\widetilde{\mathbb{E}_{t_0,d_0}})_p(\mathbb{F}_p)$ is not a cyclic group, and thus $\pi_{(\mathbb{E}_{t_0,d_0}),a_0,n_0}(x) \leq 2$ for every $x \geq 0$, as asserted. ∎

2.4. Proof of part (c) of Theorem 1.10

To verify part (c) of Theorem 1.10, we will make use of the following result, which follows from Theorem 1.1 in [20]

Theorem 2.2. *For any elliptic curve E defined over $\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(E[d])/\mathbb{Q})$ is abelian only if $d \in \{1, 2, 3, 4, 5, 6, 8\}$. Furthermore, for each $d \in \{1, 2, 3, 4, 5, 6, 8\}$, the set*

$$\{j \in \mathbb{Q} : j = j_E \text{ for some elliptic curve } E \text{ over } \mathbb{Q} \text{ with } \mathrm{Gal}(\mathbb{Q}(E[d])/\mathbb{Q}) \text{ abelian}\}$$

is infinite.

Theorem 2.2 allows us to restrict our verification of $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[\ell]) \not\subseteq \mathbb{Q}(\zeta_{n_0})$ to just those $\ell \in \{2, 3, 5\}$. By assumption, the prime 3 ramifies in $\mathbb{Q}(\sqrt{h_2(t_0)})$, and therefore 3 does *not* ramify in the field $\mathbb{Q}(\sqrt{-3h_2(t_0)}, \sqrt{-3n_3(t_0,d_0)h_2(t_0)})$, and, by hypothesis, neither does 5. Thus, neither 3 nor 5 divides n_0, and so neither 3 nor 5 ramifies in $\mathbb{Q}(\zeta_{n_0})$. Since 3 *does* ramify in $\mathbb{Q}(\sqrt{h_2(t_0)}) = \mathbb{Q}(\mathbb{E}_{t_0,d_0}[2])$ and in $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[3])$, we see that

$$\mathbb{Q}(\mathbb{E}_{t_0,d_0}[2]) \not\subseteq \mathbb{Q}(\zeta_{n_0}) \text{ and } \mathbb{Q}(\mathbb{E}_{t_0,d_0}[3]) \not\subseteq \mathbb{Q}(\zeta_{n_0}).$$

Similarly, since 5 ramifies in $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[5])$, we further conclude that $\mathbb{Q}(\mathbb{E}_{t_0,d_0}[5]) \not\subseteq \mathbb{Q}(\zeta_{n_0})$, finishing the proof of part (c) of Theorem 1.10. ∎

3. A criterion for $C_{E,a,n} = 0$

In this section, we prove Theorem 1.5. We begin by describing the constant $C_{E,a,n}$ in more detail.

3.1. Heuristics connecting $C_{E,a,n}$ with $\pi_{E,a,n}(x)$

We begin by noting that, thanks to the Hasse bound

$$|p + 1 - |\tilde{E}_p(\mathbb{F}_p)|| \le 2\sqrt{p}$$

(see, e.g., Theorem 1.1 in Chapter V of [35]), for any prime $p \nmid 2N_E$, $\tilde{E}_p(\mathbb{F}_p)$ is cyclic if and only if every prime $\ell \neq p$ satisfies $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \not\subseteq \tilde{E}_p(\mathbb{F}_p)$. Thus, by Lemma 2.1, we have

$$\tilde{E}_p(\mathbb{F}_p) \text{ is cyclic} \iff \forall \text{ prime } \ell \neq p,\ \mathrm{Frob}_p \neq 1 \in \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}), \tag{3.1}$$

where here and henceforth, Frob_p denotes any choice of Frobenius automorphism at p in a given Galois group (which should be clear from context). In particular, we have

$$\lim_{x\to\infty} \pi_{E,a,n}(x) < \infty \iff \begin{array}{c} \exists S \subseteq \{\text{primes}\} \text{ with } |S| < \infty \text{ satisfying that } \forall p \notin S \text{ with} \\ p \equiv a \bmod n, \exists \ell \text{ prime and } \mathrm{Frob}_p = 1 \in \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}). \end{array}$$

The constant $C_{E,a,n}$ encodes the joint probability of the events (3.1) and $p \equiv a \bmod n$, as follows. Grouping the primes ℓ on the right-hand side of (3.1) according to whether they divide a "test level" $m \in \mathbb{N}$, we are led to the biconditional

$$\begin{array}{l} \tilde{E}_p(\mathbb{F}_p) \text{ is cyclic} \\ \quad \iff \forall m \in \mathbb{N} \text{ with } p \nmid m \text{ and } \forall \text{ prime } \ell \mid m,\ \mathrm{Frob}_p \neq 1 \in \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}). \end{array} \tag{3.2}$$

To study the density of such primes that also satisfy $p \equiv a \bmod n$ (equivalently, that also satisfy $\mathrm{Frob}_p = \sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$), we define the following sets:

$$\begin{aligned} S_{E,a,n}(m) &:= \{\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q}) : \sigma|_{\mathbb{Q}(\zeta_n)} = \sigma_a\}, \\ S'_{E,a,n}(m) &:= \{\sigma \in S_{E,a,n}(m) : \forall \ell \mid m,\ \sigma|_{\mathbb{Q}(E[\ell])} \neq 1\}, \\ S^{(d)}_{E,a,n}(m) &:= \{\sigma \in S_{E,a,n}(m) : \sigma|_{\mathbb{Q}(E[d])} = 1\}, \quad \text{for } d \mid m. \end{aligned}$$

Note that

$$S^{(1)}_{E,a,n}(m) = S_{E,a,n}(m).$$

The "probability visible at level m" that $\tilde{E}_p(\mathbb{F}_p)$ is cyclic is reflected in the right-hand condition in (3.2) for a *fixed* value of m. By the Chebotarev density theorem, the probability is given by

$$\mathrm{Prob}(\tilde{E}_p(\mathbb{F}_p)[\ell] \text{ is cyclic for each } \ell \mid m \text{ and } p \equiv a \bmod n) = \frac{|S'_{E,a,n}(m)|}{|\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q})|}. \tag{3.3}$$

Note that, for any fixed m, the number of primes $p \mid m$ is finite, so removing them from consideration does not affect this probability.

For any d dividing m, we let

$$\varpi_{m,d} : \mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

denote the restriction map. Using the observation $|S^{(d)}_{E,a,n}(d)| = \gamma_{a,n}(\mathbb{Q}(E[d]))$ (see (1.4)), we see that

$$\begin{aligned}\frac{|S^{(d)}_{E,a,n}(m)|}{|\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} &= \frac{|\varpi^{-1}_{m,d}(S^{(d)}_{E,a,n}(d))|}{|\varpi^{-1}_{m,d}(\mathrm{Gal}(\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n)/\mathbb{Q}))|} \\ &= \frac{\gamma_{a,n}(\mathbb{Q}(E[d]))}{|\mathrm{Gal}(\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n)/\mathbb{Q})|}.\end{aligned}$$

Moreover, since

$$S'_{E,a,n}(m) = S^{(1)}_{E,a,n}(m) - \bigcup_{\ell \mid m} S^{(\ell)}_{E,a,n}(m),$$

we may apply inclusion-exclusion, concluding that

$$\begin{aligned}\frac{|S'_{E,a,n}(m)|}{|\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} &= \sum_{d \mid m} \frac{\mu(d)\,|S^{(d)}_{E,a,n}(m)|}{|\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} \\ &= \sum_{d \mid m} \frac{\mu(d)\,\gamma_{a,n}(\mathbb{Q}(E[d]))}{|\mathrm{Gal}(\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n)/\mathbb{Q})|}.\end{aligned} \tag{3.4}$$

Thus, taking the limit in (3.3) as $m \to \infty$ through any sequence that is cofinal with respect to divisibility (for instance, we may simply take $m_n := \prod_{\ell \le n} \ell^n$), we arrive at the heuristic density

$$C_{E,a,n} = \lim_{n\to\infty} \sum_{d \mid m_n} \frac{\mu(d)\,\gamma_{a,n}(\mathbb{Q}(E[d]))}{|\mathrm{Gal}(\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} = \sum_{d=1}^{\infty} \frac{\mu(d)\,\gamma_{a,n}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n) : \mathbb{Q}]}. \tag{3.5}$$

Remark 3.1. Given any elliptic curve E over $\mathbb{Q}$, any pair (a, n) of relatively prime positive integers, and any $m \in \mathbb{N}$,

$$m \text{ is an acyclicity level for } (E, a, n) \iff S'_{E,a,n}(m) = \emptyset.$$

Furthermore, since $\mathrm{Gal}(\mathbb{Q}(E[m])\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to the group

$$\left\{(\sigma, \tau) \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : \sigma|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \tau|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)}\right\},$$

we may see that the set $S_{E,a,n}(m)$ is in one-to-one correspondence with the set

$$\{\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) : \sigma|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)}\}$$

and the set $S'_{E,a,n}(m)$ corresponds to

$$\{\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) : \sigma|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} \text{ and } \forall \ell \mid m, \sigma|_{\mathbb{Q}(E[\ell])} \neq 1\}.$$

3.2. The constant $C_{E,a,n}$ as an "almost Euler product."

We will presently describe the constant $C_{E,a,n}$ as a convergent Euler product multiplied by a certain rational number, which will allow us to deduce Theorem 1.5. Toward this end, let us describe in some detail the nature of the image of the Galois representation ρ_E in (2.1). In case E has CM by the order $\mathcal{O}_{K,f} \subseteq \mathcal{O}_K$ of conductor $f \in \mathbb{N}$ inside an imaginary quadratic field K, the image of ρ_E is not open inside the profinite group $\mathrm{GL}_2(\hat{\mathbb{Z}})$, but it is open inside a particular subgroup, which we now specify, following [29]. Let $\Delta_K \in \mathbb{Z}$ denote the discriminant of K and define the integers $\delta = \delta_{K,f}$ and $\phi = \phi_{K,f}$ by

$$(\delta, \phi) := \begin{cases} \left(\frac{\Delta_K f^2}{4}, 0\right) & \text{if } \Delta_K f^2 \equiv 0 \bmod 4, \\ \left(\frac{(\Delta_K - 1)}{4} f^2, f\right) & \text{if } \Delta_K f^2 \equiv 1 \bmod 4. \end{cases}$$

Then define the subgroups $\mathcal{C}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}) \subseteq \mathcal{N}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ by

$$\begin{aligned} \mathcal{C}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}) &:= \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/n\mathbb{Z}, a^2 + \phi ab - \delta b^2 \in (\mathbb{Z}/n\mathbb{Z})^\times \right\}, \\ \mathcal{N}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}) &:= \left\langle \mathcal{C}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle. \end{aligned} \tag{3.6}$$

Finally, set

$$\mathcal{N}_{\delta,\phi}(\hat{\mathbb{Z}}) := \varprojlim \mathcal{N}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}).$$

If E has CM by the imaginary quadratic order $\mathcal{O}_{K,f}$ then, for an appropriate choice of basis, we have

$$\rho_E(G_{\mathbb{Q}}) \subseteq \mathcal{N}_{\delta,\phi}(\hat{\mathbb{Z}}). \tag{3.7}$$

(Henceforth we will assume that, in the CM case, the underlying choice of basis is made so that (3.7) holds.) To uniformize notation, let us define $\mathbb{G}_E(\mathbb{Z}/n\mathbb{Z})$ by

$$\mathbb{G}_E(\mathbb{Z}/n\mathbb{Z}) := \begin{cases} \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) & \text{if } E \text{ has no CM}, \\ \mathcal{N}_{\delta,\phi}(\mathbb{Z}/n\mathbb{Z}) & \text{if } E \text{ has CM by } \mathcal{O}_{K,f}, \end{cases}$$

and

$$\mathbb{G}_E(\hat{\mathbb{Z}}) := \varprojlim \mathbb{G}_E(\mathbb{Z}/n\mathbb{Z}).$$

Thanks to Serre's open image theorem in the non-CM case and class field theory in the CM case, we have $[\mathbb{G}_E(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] < \infty$. It follows that there exists $m \in \mathbb{N}$ for which

$$\ker(\mathbb{G}_E(\hat{\mathbb{Z}}) \to \mathbb{G}_E(\mathbb{Z}/m\mathbb{Z})) \subseteq \rho_E(G_{\mathbb{Q}}). \tag{3.8}$$

Definition 3.2. For any elliptic curve E over $\mathbb{Q}$, we define $m_E \in \mathbb{N}$ to be the smallest $m \in \mathbb{N}$ for which (3.8) holds, and call it the *adelic level* of the group $\rho_E(G_{\mathbb{Q}}) \subseteq \mathbb{G}_E(\hat{\mathbb{Z}})$. More generally, for any open subgroup $G \subseteq \mathbb{G}_E(\hat{\mathbb{Z}})$, we define the *adelic level of* G to be the smallest $m \in \mathbb{N}$ for which $\ker(\mathbb{G}_E(\hat{\mathbb{Z}}) \to \mathbb{G}_E(\mathbb{Z}/m\mathbb{Z})) \subseteq G$.

A key property of the group $G_E := \rho_E(G_{\mathbb{Q}})$, that can be deduced from Definition 3.2, is that

$$\begin{aligned} &\forall M, m \in \mathbb{N} \text{ with } m \mid M,\ G_E(M) \subsetneq \pi_{M,m}^{-1}(G_E(m)) \\ &\qquad\qquad \Longrightarrow\ \gcd(M, m_E) > \gcd(m, m_E), \end{aligned} \tag{3.9}$$

where $\pi_{M,m}\colon \mathbb{G}_E(\mathbb{Z}/M\mathbb{Z}) \to \mathbb{G}_E(\mathbb{Z}/m\mathbb{Z})$ denotes the canonical projection map.

We are now ready to analyze the constant $C_{E,a,n}$ in further detail. Suppose that $f\colon \mathbb{N} \to \mathbb{C}$ is any function for which there exists $M \in \mathbb{N}$ so that

$$\forall d_1, d_2 \in \mathbb{N},\ \gcd(Md_1, d_2) = 1 \implies f(d_1 d_2) = f(d_1) f(d_2), \tag{3.10}$$

and for which the infinite sum $\sum_{d=1}^{\infty} \mu(d) f(d)$ converges absolutely. Writing any $d \in \mathbb{N}$ as $d = d_1 d_2$, with d_1 only divisible by primes dividing M and $\gcd(d_2, M) = 1$, it follows from (3.10) that

$$\begin{aligned} \sum_{d=1}^{\infty} \mu(d) f(d) &= \Big(\sum_{d_1 \mid M} \mu(d_1) f(d_1) \Big) \Big(\sum_{\substack{d_2 \in \mathbb{N} \\ \gcd(d_2, M) = 1}} \mu(d_2) f(d_2) \Big) \\ &= \Big(\sum_{d_1 \mid M} \mu(d_1) f(d_1) \Big) \prod_{\substack{\ell \text{ prime} \\ \ell \nmid M}} (1 - f(\ell)). \end{aligned} \tag{3.11}$$

We will apply the above with

$$f(d) := \frac{\gamma_{a,n}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)]} \quad \text{and} \quad M = m_E.$$

This application is justified by our next lemmas.

Lemma 3.3. *Let E be an elliptic curve over $\mathbb{Q}$ and let m_E be its adelic level (see Definition 3.2). For any positive integers n, d_1, and d_2 with $\gcd(d_1 m_E, d_2) = 1$, we have*

$$(\mathbb{Q}(E[d_1]) \cap \mathbb{Q}(\zeta_n)) \cdot (\mathbb{Q}(E[d_2]) \cap \mathbb{Q}(\zeta_n)) = (\mathbb{Q}(E[d_1 d_2]) \cap \mathbb{Q}(\zeta_n)).$$

Proof. The containment "$\subseteq$" is obvious. We will establish the other containment. Let us set $d := d_1 d_2$, $N := \operatorname{lcm}(n, d_1 d_2)$, and $G_E := \rho_E(G_{\mathbb{Q}}) \subseteq \mathbb{G}_E(\hat{\mathbb{Z}})$. Write $N = N_1 N_2$ (respectively, $n = n_1 n_2$) with N_1 (respectively, n_1) supported on primes dividing $d_1 m_E$ and N_2 (respectively, n_2) coprime to $d_1 m_E$. We then have $d_2 \mid N_2$ and $\gcd(N_1 m_E, N_2) = 1$. Applying (3.9) with $M = N$ and $m = N_1$, we find that, under the isomorphism of the Chinese remainder theorem,

$$G_E(N) \simeq G_E(N_1) \times \mathbb{G}_E(\mathbb{Z}/N_2\mathbb{Z}). \tag{3.12}$$

Throughout the rest of this proof, we will at times make casual use of this isomorphism. Let $A := \operatorname{Gal}(\mathbb{Q}(E[d]) \cap \mathbb{Q}(\zeta_n)/\mathbb{Q})$ and define the map

$$\psi : G_E(N) \xrightarrow{\pi_{N,d}} G_E(d) \simeq \operatorname{Gal}(\mathbb{Q}(E[d])/\mathbb{Q}) \xrightarrow{\text{res.}} A$$

to be the natural projection map followed by the restriction map, and

$$\chi : G_E(N) \xrightarrow{\det_n} (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\text{res.}} A$$

to be the determinant modulo n map followed by the restriction map. Notice that, under $G_E(N) \simeq \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$, the maps χ and ψ both agree with the restriction map $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \to A$ (the key fact that the determinant map $\det_n : G_E(N) \to (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to the restriction map $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ follows from the Weil pairing being bilinear, alternating, non-degenerate and Galois invariant; see Proposition 8.1 in Chapter III of [35]). Thus, we have

$$\forall g \in G_E(N), \quad \chi(g) = \psi(g). \tag{3.13}$$

By virtue of the cartesian product decomposition (3.12), we may define the maps

$$\overline{\psi}_1 : G_E(N_1) \to A \quad \text{and} \quad \overline{\psi}_2 : \mathbb{G}_E(\mathbb{Z}/N_2\mathbb{Z}) \to A$$

by

$$\overline{\psi}_1(g_1) := \psi((g_1, I)) \quad \text{and} \quad \overline{\psi}_2(g_2) := \psi((I, g_2)),$$

and further extend these maps to $G_E(N)$ via

$$\psi_1(g) := \overline{\psi}_1(\pi_{N,N_1}(g)) \quad \text{and} \quad \psi_2(g) := \overline{\psi}_2(\pi_{N,N_2}(g)).$$

Similarly, we define

$$\bar{\chi}_1 : G_E(N_1) \to A, \quad \bar{\chi}_2 : \mathbb{G}_E(\mathbb{Z}/N_2\mathbb{Z}) \to A \quad \text{and} \quad \chi_1, \chi_2 : G_E(N) \to A.$$

First note that

$$\psi = \psi_1\psi_2 \quad \text{and} \quad \chi = \chi_1\chi_2.$$

Furthermore, if g corresponds under (3.12) to (g_1, g_2), then, using (3.13), we have

$$\psi_1(g) = \overline{\psi}_1(g_1) = \psi((g_1, I)) = \chi((g_1, I)) = \bar{\chi}_1(g_1) = \chi_1(g),$$
$$\psi_2(g) = \overline{\psi}_2(g_2) = \psi((I, g_2)) = \chi((I, g_2)) = \bar{\chi}_2(g_2) = \chi_2(g),$$

confirming that

$$\psi_1 = \chi_1 \quad \text{and} \quad \psi_2 = \chi_2. \tag{3.14}$$

Moreover, observe that, for $g_1 \in G_E(N_1)$, if $\det g_1 \equiv 1 \bmod n_1$, then $\det(g_1, I) \equiv 1 \bmod n$, which implies that, for any $g_2 \in \mathbb{G}_E(\mathbb{Z}/N_2\mathbb{Z})$,

$$\chi_1((g_1, g_2)) = \bar{\chi}_1(g_1) = \chi((g_1, I)) = 1,$$

and so $\ker \chi_1 \supseteq \ker \det_{n_1}$. Analogous reasoning shows that $\ker \chi_2 \supseteq \ker \det_{n_2}$ as well; thus

$$\ker \chi_i \supseteq \ker \det_{n_i} \quad (i \in \{1, 2\}). \tag{3.15}$$

Similarly, if $G_E(N_1) \ni g_1 \equiv I \bmod d_1$ then $(g_1, I) \equiv I \bmod d$, which implies that, for any $g_2 \in \mathbb{G}_E(\mathbb{Z}/N_2\mathbb{Z})$,

$$\psi_1((g_1, g_2)) = \overline{\psi}_1(g_1) = \psi((g_1, I)) = 1,$$

showing that $\ker \psi_1 \supseteq \ker \pi_{N,d_1}$. Likewise, $\ker \psi_2 \supseteq \ker \pi_{N,d_2}$, and we have verified

$$\ker \psi_i \supseteq \ker \pi_{N,d_i} \quad (i \in \{1,2\}). \tag{3.16}$$

Combining (3.14), (3.15), and (3.16), we see that

$$\langle \ker \pi_{N,d_1}, \ker \det{}_{n_1} \rangle \subseteq \ker \psi_1 \quad \text{and} \quad \langle \ker \pi_{N,d_2}, \ker \det{}_{n_2} \rangle \subseteq \ker \psi_2,$$

and it follows from this and $\ker \psi_1 \cap \ker \psi_2 \subseteq \ker \psi$ (which itself results from $\psi = \psi_1\psi_2$) that

$$\begin{aligned}\mathbb{Q}(E[d_1d_2] \cap \mathbb{Q}(\zeta_n)) &= \mathbb{Q}(E[N])^{\ker \psi} \subseteq \mathbb{Q}(E[N])^{\ker \psi_1} \cdot \mathbb{Q}(E[N])^{\ker \psi_2} \\ &\subseteq (\mathbb{Q}(E[d_1]) \cap \mathbb{Q}(\zeta_{n_1})) \cdot (\mathbb{Q}(E[d_2]) \cap \mathbb{Q}(\zeta_{n_2})) \\ &\subseteq (\mathbb{Q}(E[d_1]) \cap \mathbb{Q}(\zeta_n)) \cdot (\mathbb{Q}(E[d_2]) \cap \mathbb{Q}(\zeta_n)).\end{aligned}$$

■

Lemma 3.4. *Let E and m_E be as in Lemma 3.3, and define the arithmetic function $f\colon \mathbb{N} \to \mathbb{R}$ by*

$$f(d) := \frac{\gamma_{a,n}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)]}$$

(see (1.4)). For any $d_1, d_2 \in \mathbb{N}$, we have

$$\gcd(d_1 m_E, d_2) = 1 \implies f(d_1d_2) = f(d_1)f(d_2).$$

Proof. The fact that

$$\gcd(d_1 m_E, d_2) = 1 \implies \gamma_{a,n}(\mathbb{Q}(E[d_1d_2])) = \gamma_{a,n}(\mathbb{Q}(E[d_1]))\,\gamma_{a,n}(\mathbb{Q}(E[d_2]))$$

follows immediately from Lemma 3.3 and the definition of $\gamma_{a,n}$. We now establish the analogous statement for the denominator of f. In what follows, we set

$$K := \mathbb{Q}(\zeta_n) \quad \text{and} \quad G_E := \rho_E(G_{\mathbb{Q}}) \subseteq \mathbb{G}_E(\hat{\mathbb{Z}}).$$

By Galois theory, we have

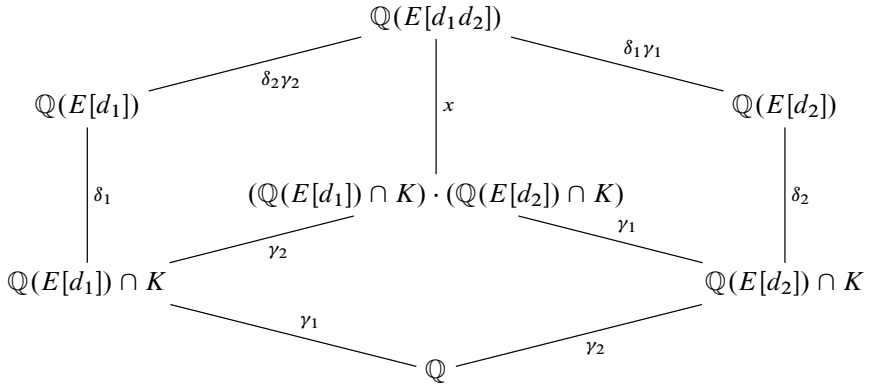
$$\begin{aligned}[K(E[d_1]) : K] &= [\mathbb{Q}(E[d_1]) : \mathbb{Q}(E[d_1]) \cap K] = \delta_1 \quad \text{in (3.18) below,} \\ [K(E[d_2]) : K] &= [\mathbb{Q}(E[d_2]) : \mathbb{Q}(E[d_2]) \cap K] = \delta_2 \quad \text{in (3.18) below,} \\ [K(E[d_1d_2]) : K] &= [\mathbb{Q}(E[d_1d_2]) : \mathbb{Q}(E[d_1d_2]) \cap K] = x \quad \text{in (3.18) below,}\end{aligned} \tag{3.17}$$

where we have used Lemma 3.3 to justify the last line of equalities. Applying (3.9) with $M = d_1d_2$ and $m = d_1$, we find that $G_E(d_1d_2) \simeq G_E(d_1) \times \mathbb{G}_E(\mathbb{Z}/d_2\mathbb{Z})$, which implies that

$$\mathbb{Q}(E[d_1]) \cap \mathbb{Q}(E[d_2]) = \mathbb{Q} \quad \text{and} \quad (\mathbb{Q}(E[d_1]) \cap K) \cap (\mathbb{Q}(E[d_2]) \cap K) = \mathbb{Q}.$$

We thus have the following diagram of fields, with γ_1, γ_2, δ_1, δ_2, and x defined as the degrees of the appropriate field extensions:

(3.18)



Computing $[\mathbb{Q}(E[d_1d_2]) : \mathbb{Q}]$ in two different ways, we see that $x = \delta_1\delta_2$, which, by (3.17), completes the proof of the lemma. ∎

Returning to (3.11), we set

$$f(d) := \frac{\gamma_{a,n}(\mathbb{Q}(E[d]))}{[\mathbb{Q}(E[d])\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)]} \quad \text{and} \quad M = m_E.$$

By Lemma 3.4 together with (3.5) and (3.4), we conclude that $C_{E,a,n}$ is equal to

$$\frac{|S'_{E,a,n}(\mathrm{rad}(m_E))|}{|\operatorname{Gal}(\mathbb{Q}(E[\mathrm{rad}(m_E)])\mathbb{Q}(\zeta_n)/\mathbb{Q})|} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \nmid m_E \\ \ell \mid \gcd(n, a-1)}} \Big(1 - \frac{\phi(\ell)}{|\mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z})|}\Big) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \nmid n m_E}} \Big(1 - \frac{1}{|\mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z})|}\Big),$$

where $\mathrm{rad}(m_E) := \prod_{\ell \mid m_E} \ell$. Since each of the products in this expression is a positive number (note that, by (3.6), we have $\ell \mid m_E \Rightarrow |\mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z})| > \phi(\ell) \geq 1$ and also $|\mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z})| \gg \ell^2$, ensuring convergence of the infinite product), it thus follows from Remark 3.1 that

$$\begin{aligned} C_{E,a,n} = 0 &\iff S'_{E,a,n}(\mathrm{rad}(m_E)) = \emptyset \\ &\iff \exists m \mid \mathrm{rad}(m_E) \text{ that is an acyclicity level for } (E, a, n), \end{aligned}$$

completing the proof of Theorem 1.5.

Remark 3.5. Since our proof of Theorem 1.5 gives a slightly stronger condition, our conjectural equivalence (1.7) may be restated in the following refined form:

$$\text{There exists an acyclicity level } m \mid \mathrm{rad}(m_E) \text{ for } (E, a, n) \iff \lim_{x \to \infty} \pi_{E,a,n}(x) < \infty.$$

Remark 3.6. The main ingredients in the proof of Theorem 1.5 are (3.4), (3.11), and Lemma 3.4, with (3.4) representing the key observation missing from the analysis in [1]. Rather than (3.11) and Lemma 3.4, we could have instead used Lemma 12 in [1]. We chose to include Lemma 3.4 both for the sake of completeness and also because it gives a slightly stronger result: our $\mathrm{rad}(m_E)$ is always a divisor of the M_E appearing in Lemma 12 of [1] (see for instance Lemma 3.6 and Lemma 4.4 of [22]), and in practice it is often a proper divisor.

4. Proof of Theorem 1.14

Let $m \in \mathbb{N}$ and assume that $\mathcal{J}_m \neq \emptyset$. We will presently separate into cases according to whether m is prime or not.

Lemma 4.1. *Let E be an elliptic curve over $\mathbb{Q}$ and let (a,n) be a pair of relatively prime positive integers. We have*

$$\ell \text{ is a prime } \textit{acyclicity level for } (E,a,n) \iff \mathbb{Q}(E[\ell]) \subseteq \mathbb{Q}(\zeta_n) \text{ and } \sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1.$$

Proof. Using Remark 3.1, the implication "$\Longleftarrow$" is straightforward; conversely, if $\mathbb{Q}(E[\ell]) \not\subseteq \mathbb{Q}(\zeta_n)$, then the restriction $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[\ell]) \cap \mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a nontrivial quotient map, so one can choose at least one nonidentity element mapping onto $\sigma_a|_{\mathbb{Q}(E[\ell])\cap\mathbb{Q}(\zeta_n)}$. Again using Remark 3.1, we see that $S'_{E,a,n}(\ell) \neq \emptyset$, contradicting that ℓ is an acyclicity level for (E,a,n). Thus, $\mathbb{Q}(E[\ell]) \subseteq \mathbb{Q}(\zeta_n)$, and then $\sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1$ follows from $S'_{E,a,n}(\ell) = \emptyset$. ∎

If $m = \ell$ is prime, then, by Lemma 4.1 and Theorem 2.2, we must have $\ell \in \{2,3,5\}$ and there exists a pair (a,n) of relatively prime positive integers for which $\mathbb{Q}(E[\ell]) \subseteq \mathbb{Q}(\zeta_n)$ and $\sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1$. Finally, Theorem 2.2 implies that, for each $\ell \in \{2,3,5\}$, $\mathcal{J}_\ell$ is infinite, finishing the case where m is prime.

Henceforth, let us assume that m is composite and $|\mathcal{J}_m| = \infty$; we will finish the proof by deducing that $m = 6$ and $\mathcal{J}_m \subseteq j_{\mathbb{E}}(\mathbb{Q})$ (see (1.20) and (1.10)). Let $j \in \mathcal{J}_m \backslash \{0, 1728\}$ and let E be any elliptic curve over $\mathbb{Q}$ that has m as a minimal acyclicity level and for which $j = j_E$. Proposition 4.4 below lays out some conditions that $G := \rho_E(G_{\mathbb{Q}})$ must satisfy. First, we state a key group-theoretical lemma, whose proof is straightforward.

Lemma 4.2. *Let G be a group, let $N_1, N_2 \trianglelefteq G$ be two normal subgroups of G and let $\tilde{\sigma}, \tilde{\sigma}' \in G$. Suppose that $\sigma := \tilde{\sigma}N_1$ and $\sigma' := \tilde{\sigma}'N_1 \in G/N_1$ satisfy $\tilde{\sigma}N_1N_2 = \tilde{\sigma}'N_1N_2$. Then there exists $n_1 \in N_1$ for which $\tilde{\sigma}n_1N_2 = \tilde{\sigma}'N_2$.*

Corollary 4.3. *Let E be an elliptic curve over $\mathbb{Q}$ and let $m, m', n \in \mathbb{N}$, with m' a divisor of m. If $\sigma, \sigma' \in \mathrm{Gal}(\mathbb{Q}(E[m'])/\mathbb{Q})$ satisfy*

$$\sigma|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)} = \sigma'|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)},$$

then there exist lifts $\tilde{\sigma}, \tilde{\sigma}' \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ of σ and σ', respectively, which satisfy

$$\tilde{\sigma}|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \tilde{\sigma}'|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)}.$$

Proof. We apply Lemma 4.2 with $G := \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$, $N_1 := \ker \pi_1$ and $N_2 := \ker \pi_2$, where

$$\pi_1 : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[m'])/\mathbb{Q}),$$
$$\pi_2 : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[m] \cap \mathbb{Q}(\zeta_n))/\mathbb{Q})$$

are the restriction maps. Given $\sigma, \sigma' \in G/N_1 \simeq \mathrm{Gal}(\mathbb{Q}(E[m'])/\mathbb{Q})$, let us choose arbitrary lifts $\tilde{\sigma}, \tilde{\sigma}' \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. By the Galois correspondence, the condition $\tilde{\sigma} N_1 N_2 = \tilde{\sigma}' N_1 N_2$ is equivalent to $\sigma|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)} = \sigma'|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)}$, and the conclusion of Lemma 4.2 states that we may adjust $\tilde{\sigma}$ so that $\tilde{\sigma}|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \tilde{\sigma}'|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)}$. ∎

Proposition 4.4. *Let E be an acyclicity elliptic curve over $\mathbb{Q}$ and set $G_E := \rho_E(G_{\mathbb{Q}})$. Let m be a minimal acyclicity level for E and assume that m is composite. Then there exists a surjective group homomorphism $\chi: G_E(m) \twoheadrightarrow A$ onto an abelian group A whose kernel $N(m) := \ker \chi$ satisfies the following three properties, where in what follows, for any divisor d of m, we denote by $N(d)$ the reduction of $N(m)$ modulo d.*

(1) *Defining $\tilde{N}(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ to be the subgroup that corresponds under the Chinese remainder theorem to $\prod_{\ell|m} N(\ell)$, there exists an element $\tau \in \tilde{N}(m) \cap G_E(m)$ such that, for each $\sigma \in \tau N(m) \subseteq G_E(m)$, there exists a prime $\ell \mid m$ for which $\sigma \equiv I \bmod \ell$, and for each $\ell \mid m$, there exists $\sigma' \in \tau N(m)$ such that, for each prime ℓ' dividing m/ℓ, $\sigma' \not\equiv I \bmod \ell'$.*

(2) *For each prime ℓ dividing m, we have $|N(\ell)| > 1$.*

(3) *For each prime ℓ dividing m, writing $m = \ell \cdot m'$ (with $\ell \nmid m'$), we have $N(m) \cap \ker \pi_{m,m'} = \{I\}$. In particular, the group $N(\ell)$ is isomorphic to a quotient of the group $N(m')$.*

Proof. Define $A := \mathrm{Gal}(\mathbb{Q}(E[m]) \cap \mathbb{Q}(\zeta_n)/\mathbb{Q})$ and let $\chi: G_E(m) \twoheadrightarrow A$ be the surjective homomorphism corresponding under $G_E(m) \simeq \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ to the restriction map $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[m]) \cap \mathbb{Q}(\zeta_n)/\mathbb{Q})$. To prove item (1), pick any $\tau \in \chi^{-1}(\sigma_a)$ and note that then $\chi^{-1}(\sigma_a) = \tau N(m)$. Fixing any prime $\ell \mid m$, we observe that $\tau \bmod \ell \in N(\ell)$, or else for each $\sigma \in \tau N(m)$, $\sigma \not\equiv I \bmod \ell$, implying that m/ℓ is an acyclicity level of E, contradicting the minimality of m; thus $\tau \in \tilde{N}(m)$. The final two stated properties in item (1) are equivalent to the fact that m is a minimal acyclicity level of E. Indeed, the equivalence

$$S'_{E,a,n}(m) = \emptyset \iff \forall \sigma \in \tau N(m)\ \exists \ell \mid m \text{ for which } \sigma \equiv I \bmod \ell$$

follows directly from the definitions (through the lens of Remark 3.1), the identification $G_E(m) \simeq \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ and the other identifications mentioned above. For the second of the final two properties in (1), let ℓ be a prime divisor of m and let $m' := m/\ell$. Suppose for the sake of contradiction that

$$\forall \sigma' \in \tau N(m)\ \exists \text{ a prime } \ell' \mid m' \text{ for which } \sigma' \equiv I \bmod \ell'. \tag{4.1}$$

We then claim that $S'_{E,a,n}(m') = \emptyset$. To see this, let $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m'])/\mathbb{Q})$ be any automorphism satisfying

$$\sigma|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)}.$$

By Corollary 4.3, we may find a lift $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ of σ satisfying

$$\tilde{\sigma}|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)}.$$

By (4.1), there exists a prime $\ell' \mid m'$ for which $\tilde{\sigma}|_{\mathbb{Q}(E[\ell'])} \equiv 1$, and since $\tilde{\sigma}|_{\mathbb{Q}(E[\ell'])} = \sigma|_{\mathbb{Q}(E[\ell'])}$, we may see that $S'_{E,a,n}(m') = \emptyset$, contradicting the assumption that m is a minimal acyclicity level of E. This establishes item (1).

To prove item (2), assume for the sake of contradiction that $N(\ell) = \{I\}$ for some prime ℓ dividing m. Then $N(m) \subseteq \ker \pi_{m,\ell}$, and thus

$$\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(E[m]) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(E[m])^{\ker \chi} \supseteq \mathbb{Q}(E[m])^{\ker \pi_{m,\ell}} = \mathbb{Q}(E[\ell]).$$

Consider now the restriction to $\mathbb{Q}(E[\ell])$ of $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If $\sigma_a|_{\mathbb{Q}(E[\ell])} \equiv 1$, then $S'_{E,a,n}(\ell) = \emptyset$, contradicting the minimality of m. If on the other hand

$$\sigma_a|_{\mathbb{Q}(E[\ell])} \not\equiv 1, \tag{4.2}$$

then consider the group $G_E(m')$, where $m = \ell \cdot m'$ and $\ell \nmid m'$. If $\sigma \in G_E(m')$ is any Galois automorphism satisfying

$$\sigma|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)}, \tag{4.3}$$

then by Corollary 4.3 we may find a lift $\tilde{\sigma} \in G_E(m)$ for which

$$\tilde{\sigma}|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)}.$$

Since $S'_{E,a,n}(m) = \emptyset$, there must exist a prime $\ell' \mid m$ with $\tilde{\sigma}|_{\mathbb{Q}(E[\ell'])} \equiv 1$, and by (4.2), $\ell' \neq \ell$. Since $\sigma \in G_E(m')$ satisfying (4.3) was arbitrary, it follows that $S'_{E,a,n}(m') = \emptyset$, contradicting the minimality of m. We therefore conclude that $N(\ell) \neq \{I\}$, for any prime ℓ dividing m, establishing item (2).

To verify item (3), we assume for the sake of contradiction that

$$N(m) \cap \ker \pi_{m,m'} \neq \{I\}. \tag{4.4}$$

It follows from this that $S'_{E,a,n}(m') = \emptyset$. Indeed, fix any $\sigma' \in \mathrm{Gal}(\mathbb{Q}(E[m'])/\mathbb{Q})$ that satisfies

$$\sigma'|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m'])\cap\mathbb{Q}(\zeta_n)}.$$

By Corollary 4.3, we may find $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ satisfying

$$\sigma|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} = \sigma_a|_{\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)} \quad \text{and} \quad \sigma|_{\mathbb{Q}(E[m'])} = \sigma',$$

and by virtue of (4.4), we may find more than one such lift σ. In particular, we can arrange that $\sigma|_{\mathbb{Q}(E[\ell])} \not\equiv 1$. On the other hand, since $S'_{E,a,n}(m) = \emptyset$, we see using Remark 3.1 that there must exist a prime $\ell' \mid m$ with $\sigma|_{\mathbb{Q}(E[\ell'])} \equiv 1$, and since $\ell' \neq \ell$, we must have $\ell' \mid m'$. Since $\sigma' \in \mathrm{Gal}(\mathbb{Q}(E[m'])/\mathbb{Q})$ was arbitrary, this implies (again via Remark 3.1) that $S'_{E,a,n}(m') = \emptyset$, as asserted. Since this contradicts the minimality of m as an acyclicity level of E, we see that (4.4) is false, establishing item (3) and finishing the proof of Proposition 4.4. ∎

Remark 4.5. Let $E/\mathbb{Q}$ be an acyclicity elliptic curve with a composite minimal acyclicity level m, let $G_E := \rho_E(G_{\mathbb{Q}})$, and consider the group $H := \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \bmod m \in G_E(m)\}$. By item (3) of Proposition 4.4, the adelic level of H (which a priori is a divisor of m) must be equal to m. Indeed, if ℓ is a prime dividing m, $m' := m/\ell$, and $G_E(m) \simeq \mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z}) \times G_E(m')$, then since $\ker \chi \simeq N(\ell) \times_\psi N(m')$, we must have

$$\begin{aligned}[\mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z}), \mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z})] \times [G_E(m'), G_E(m')] &\subseteq N(\ell) \times_\psi N(m') \\ &\subseteq \mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z}) \times G_E(m'),\end{aligned}$$

contradicting that $(N(\ell) \times_\psi N(m')) \cap \ker \pi_{m,m'} = \{I\}$, since $\mathbb{G}_E(\mathbb{Z}/\ell\mathbb{Z})$ is always non-abelian.

Definition 4.6. We call a subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ an *open acyclicity group of composite type* if the following two conditions hold:

(1) G is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with composite, square-free adelic level,

(2) $G(m)$ satisfies the conclusions of Proposition 4.4, where m is the adelic level of G.

We call a subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ *admissible* if $\det(G) = \hat{\mathbb{Z}}^\times$ and G contains an element that is $\mathrm{GL}_2(\hat{\mathbb{Z}})$-conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ or to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$.

If E' is any elliptic curve over $\mathbb{Q}$, then thanks to the Weil pairing, which guarantees that $\det(\rho_{E'}(G_{\mathbb{Q}})) = \hat{\mathbb{Z}}^\times$, and Lemma 2.8 in [36], which guarantees that $\rho_{E'}(G_{\mathbb{Q}})$ satisfies the second condition for admissibility, we have that $\rho_{E'}(G_{\mathbb{Q}})$ is always an admissible subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Define the following collection of open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$:

$$\mathfrak{G} := \{G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}) : G \text{ is an admissible open acyclicity group of composite type}\}. \tag{4.5}$$

Inspecting the conclusions of Proposition 4.4, we may see that

$$G \in \mathfrak{G} \iff G^{\mathsf{T}} \in \mathfrak{G}. \tag{4.6}$$

Returning to the elliptic curve E for which the composite number m is a minimal acyclicity level and $j_E = j \in \mathcal{J}_m \backslash \{0, 1728\}$, let us consider the group $H := \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \bmod m \in G_E(m)\}$. Now G_E may not be in $\mathfrak{G}$ (if E has CM then G_E is not an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$), but by Proposition 4.4 and Remark 4.5, $G_E \subseteq H \in \mathfrak{G}$. Therefore, by (2.2) and (4.6), we must have $j_E \in j_{\tilde{H}}(X_{\tilde{H}}(\mathbb{Q}))$, where $\tilde{H} := \langle H, -I \rangle$. Furthermore, since $\mathcal{J}_m$ is infinite and the number of such H is finite, by the pigeonhole principle and Faltings' theorem [18], there must exist an acyclicity group $H \in \mathfrak{G}$ with adelic level m and for which $\mathrm{genus}(X_{\tilde{H}}) \leq 1$. Moreover, the set of adelic levels of $G \in \{G \in \mathfrak{G} : \mathrm{genus}(X_{\tilde{G}}) \leq 1\}$ is bounded, as will be shown below in Corollary 4.8. Define the *special adelic level* of an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ to be the smallest $m \in \mathbb{N}$ for which

$$\ker(\mathrm{SL}_2(\hat{\mathbb{Z}}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \subseteq G.$$

It is not difficult to prove that, for any open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, the special adelic level of G divides the adelic level of G. In general, the quotient (adelic level of G)/(special adelic level of G) $\in \mathbb{N}$ is unbounded, as $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ varies over all open subgroups.

Lemma 4.7. *Let $\mathfrak{G}$ be as in (4.5). If $G \in \mathfrak{G}$, then the special adelic level of $\tilde{G}$, the special adelic level of G, and the adelic level of G are all equal.*

Proof. Let us denote by m the adelic level of G and set $S := G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$. Assume for the sake of contradiction that the special adelic level of G is strictly less than m. Let ℓ be any prime number dividing m that does *not* divide the special adelic level of G (since m is square-free by Definition 4.6, such a prime ℓ must exist). Writing $m =: \ell m'$ with $\ell \nmid m'$, we then have that, under the isomorphism of the Chinese remainder theorem,

$$S(m) \simeq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times S(m').$$

It follows that

$$[G(m), G(m)] \supseteq [S(m), S(m)] \simeq [\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})] \times [S(m'), S(m')].$$

Thus, if $\chi\colon G(m) \to A$ is as in Proposition 4.4 and $N(m) := \ker \chi$, we have

$$N(m) \supseteq [G(m), G(m)] \supseteq [\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})] \times \{I\},$$

contradicting part (3) of Proposition 4.4. Thus, the special adelic level of G is equal to m, as asserted.

Next, suppose that the special adelic level of $\tilde{G}$ is less than the special adelic level of G. By Lemma 2.1 in [23], the latter is twice the former, and the proof of Lemma 2.4 in [23] shows that, denoting by $\tilde{m}$ the special adelic level of $\tilde{G}$, we have

$$S(2\tilde{m}) \simeq \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi} S(\tilde{m}) := \{(s_2, s_{\tilde{m}}) \in \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \times S(\tilde{m}) : \psi_2(s_2) = \psi_{\tilde{m}}(s_{\tilde{m}})\},$$

where

$$\psi_2\colon \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \to \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad \psi_{\tilde{m}}\colon S(\tilde{m}) \to \mathbb{Z}/2\mathbb{Z}$$

are surjective homomorphisms. Since the common quotient $\mathbb{Z}/2\mathbb{Z}$ is cyclic, it follows from Lemma 1 on p. 174 of [24] that, under the isomorphism of the Chinese remainder theorem,

$$[S(2\tilde{m}), S(2\tilde{m})] \simeq [\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})] \times [S(\tilde{m}), S(\tilde{m})],$$

and thus

$$N(m) \supseteq [\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})] \times \{I\}$$

in this case as well, again contradicting part (3) of Proposition 4.4. This proves that the special adelic levels of $\tilde{G}$ and G agree, concluding the proof of the lemma. ∎

Corollary 4.8. *Let $\mathfrak{G}$ be as in (4.5). If $G \in \mathfrak{G}$ and $\mathrm{genus}(X_{\tilde{G}}) \leq 1$, then the adelic level of G belongs to the set* $\{6, 10, 14, 15, 21, 22, 26, 30, 33, 39, 42\}$.

Proof. By Lemma 4.7, the (square-free, composite) adelic level of G is equal to the special adelic level of $\tilde{G}$; from Table 2 of [15], one can read off the special adelic levels of all $\tilde{G}$ for which $\mathrm{genus}(X_{\tilde{G}}) \leq 1$. This yields our list of adelic levels. ∎

Corollary 4.8, taken together with a computer calculation using the computational software package `Magma` [8], shows that the following hold:

- if $G \in \mathfrak{G}$ satisfies $\mathrm{genus}(X_{\tilde{G}}) \leq 1$, then the adelic level of G is 6;
- if $G \in \mathfrak{G}$ has adelic level 6 then $G \dot{\subseteq} G_6$, where $G_6 \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is the group introduced in Section 2.2.

In particular, we must have $m = 6$ and $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_6$, and so

$$j = j_E \in j_{G_6}(X_{G_6}(\mathbb{Q})).$$

By (2.4), $j_{G_6}(X_{G_6}(\mathbb{Q})) = j_{\mathbb{E}}(\mathbb{Q})$, so this completes the proof of Theorem 1.14. The code used to perform the above-mentioned computation can be found at the following link:

https://github.com/ncjones-uic/AcyclicReductions.

Acknowledgments. The authors thank A. C. Cojocaru for comments on a previous version of this manuscript, and A. Sutherland for stimulating communications on this topic. The authors gratefully acknowledge the anonymous referees for several helpful suggestions for improvement. A prior version of this paper is included in the second author's doctoral thesis; he would like to express appreciation to all the members of the doctoral committee for their valuable advice and constructive comments.

References

[1] Akbal, Y. and Güloğlu, A. M.: Cyclicity of elliptic curves modulo primes in arithmetic progressions. *Canad. J. Math.* **74** (2022), no. 5, 1277–1309. Zbl 1529.11078 MR 4504664

[2] Akbary, A. and Murty, V. K.: An analogue of the Siegel–Walfisz theorem for the cyclicity of CM elliptic curves mod p. *Indian J. Pure Appl. Math.* **41** (2010), no. 1, 25–37. Zbl 1205.11061 MR 2650098

[3] Banks, W. D., Pappalardi, F. and Shparlinski, I. E.: On group structures realized by elliptic curves over arbitrary finite fields. *Exp. Math.* **21** (2012), no. 1, 11–25. Zbl 1257.11060 MR 2904904

[4] Banks, W. D. and Shparlinski, I. E.: Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.* **173** (2009), 253–277. Zbl 1250.11064 MR 2570668

[5] Bilu, Y. and Parent, P.: Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)* **173** (2011), no. 1, 569–584. Zbl 1278.11065 MR 2753610

[6] Bilu, Y., Parent, P. and Rebolledo, M.: Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)* **63** (2013), no. 3, 957–984. Zbl 1307.11075 MR 3137477

[7] Borosh, I., Moreno, C. J. and Porta, H.: Elliptic curves over finite fields. II. *Math. Comput.* **29** (1975), 951–964. Zbl 0345.14012 MR 0404264

[8] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265. Zbl 0898.68039 MR 1484478

[9] Brau, J.: *Galois representations of elliptic curves and abelian entanglements*. Ph.D. Thesis, Leiden University, 2015.

[10] Campagna, F. and Stevenhagen, P.: Cyclic reduction densities for elliptic curves. *Res. Number Theory* **9** (2023), no. 3, article no. 61, 21 pp. Zbl 1530.11054 MR 4623047

[11] Chandee, V., David, C., Koukoulopoulos, D. and Smith, E.: The frequency of elliptic curve groups over prime finite fields. *Canad. J. Math.* **68** (2016), no. 4, 721–761. Zbl 1365.11071 MR 3518992

[12] Cojocaru, A. C.: On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves. *J. Number Theory* **96** (2002), no. 2, 335–350. Zbl 1038.11034 MR 1932460

[13] Cojocaru, A. C.: Primes, elliptic curves and cyclic groups. In *Analytic methods in arithmetic geometry*, pp. 1–69. Contemp. Math. 740, American Mathematical Society, Providence, RI, 2019. Zbl 1452.11069 MR 4033729

[14] Cojocaru, A. C. and Murty, M. R.: Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. *Math. Ann.* **330** (2004), no. 3, 601–625. Zbl 1087.11037 MR 2099195

[15] Cummins, C. J. and Pauli, S.: Congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus less than or equal to 24. *Experiment. Math.* **12** (2003), no. 2, 243–255. Zbl 1060.11021 MR 2016709

[16] Deligne, P. and Rapoport, M.: Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 143–316. Lecture Notes in Math. 349, Springer, Berlin-New York, 1973. Zbl 0281.14010 MR 0337993

[17] Duke, W.: Almost all reductions modulo p of an elliptic curve have a large exponent. *C. R. Math. Acad. Sci. Paris* **337** (2003), no. 11, 689–692. Zbl 1048.11045 MR 2030403

[18] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), no. 3, 349–366. Zbl 0588.14026 MR 0718935

[19] Freiberg, T. and Kurlberg, P.: On the average exponent of elliptic curves modulo p. *Int. Math. Res. Not. IMRN* (2014), no. 8, 2265–2293. Zbl 1366.11079 MR 3194018

[20] González-Jiménez, E. and Lozano-Robledo, Á.: Elliptic curves with abelian division fields. *Math. Z.* **283** (2016), no. 3-4, 835–859. Zbl 1410.11051 MR 3519984

[21] Hooley, C.: On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220. Zbl 0221.10048 MR 0207630

[22] Jones, N.: A bound for the conductor of an open subgroup of GL_2 associated to an elliptic curve. *Pacific J. Math.* **308** (2020), no. 2, 307–331. Zbl 1465.11144 MR 4190460

[23] Jones, N. and McMurdy, K.: Elliptic curves with non-abelian entanglements. *New York J. Math.* **28** (2022), 182–229. Zbl 1497.11150 MR 4374148

[24] Lang, S. and Trotter, H.: *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics 504, Springer, Berlin-New York, 1976. Zbl 0329.12015 MR 0568299

[25] Lang, S. and Trotter, H.: Primitive points on elliptic curves. *Bull. Amer. Math. Soc.* **83** (1977), no. 2, 289–292. Zbl 0345.12008 MR 0427273

[26] Lee, S. M.: On the average congruence class bias for cyclicity and divisibility of the groups of $\mathbb{F}_p$-points of elliptic curves. *J. Number Theory* **278** (2026), 746–785. Zbl 08072261 MR 4925929

[27] Lee, S. M., Mayle, J. and Wang, T.: Opposing average congruence class biases in the cyclicity and Koblitz conjectures for elliptic curves. To appear in *Canad. J. Math.*, published online (2025), DOI 10.4153/S0008414X25101156.

[28] The LMFDB Collaboration: The L-functions and modular forms database. https://www.lmfdb.org, visited on 30 March 2026.

[29] Lozano-Robledo, Á.: Galois representations attached to elliptic curves with complex multiplication. *Algebra Number Theory* **16** (2022), no. 4, 777–837. Zbl 1504.14064 MR 4467123

[30] Mazur, B.: Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44** (1978), no. 2, 129–162. Zbl 0386.14009 MR 0482230

[31] Murty, M. R.: On Artin's conjecture. *J. Number Theory* **16** (1983), no. 2, 147–168. Zbl 0526.12010 MR 0698163

[32] Rouse, J. and Zureick-Brown, D.: Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory* **1** (2015), article no. 12, 34 pp. Zbl 1397.11095 MR 3500996

[33] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331. Zbl 0235.14012 MR 0387283

[34] Serre, J.-P.: *Oeuvres. Vol. III*. Springer, Berlin, 1986. Zbl 0849.01049 MR 0926691

[35] Silverman, J. H.: *The arithmetic of elliptic curves*. Second edition. Grad. Texts in Math. 106, Springer, Dordrecht, 2009. Zbl 1194.11005 MR 2514094

[36] Sutherland, A. V. and Zywina, D.: Modular curves of prime-power level with infinitely many rational points. *Algebra Number Theory* **11** (2017), no. 5, 1199–1229. Zbl 1374.14022 MR 3671434

[37] Wong, P.-J.: Cyclicity and exponent of elliptic curves modulo p in arithmetic progressions. *Q. J. Math.* **75** (2024), no. 2, 757–777. Zbl 07936866 MR 4765791

[38] Zywina, D.: On the possible images of the mod ell representations associated to elliptic curves over $\mathbb{Q}$. Preprint 2015, arXiv:1508.07660v1.

Received September 24, 2023; revised December 20, 2025.

Nathan Jones
Department of Mathematics, Statistics, and Computer Science, University of Illinois Chicago
851 S. Morgan St., 322 SEO, Chicago, IL 60607, USA;
ncjones@uic.edu
Author IDs: zbMATH jones.nathan-a MR 842244 ORCID 0000-0002-7705-247X

Sung Min Lee
Department of Mathematics, Wake Forest University
127 Manchester Hall, Winston-Salem, NC 27109, USA;
lesum@wfu.edu
Author IDs: zbMATH lee.sung-min.1 MR 1674371 ORCID 0000-0001-5902-6676