Quantitative upper bounds related to an isogeny criterion for elliptic curves

Alina Carmen Cojocaru, Auden Hinz, and Tian Wang

Abstract. For E_1 and E_2 elliptic curves defined over a number field K, without complex multiplication, we consider the function $\mathcal{F}_{E_1,E_2}(x)$ counting non-zero prime ideals $\mathfrak{p}$ of the ring of integers of K, of good reduction for E_1 and E_2, of norm at most x, and for which the Frobenius fields $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1))$ and $\mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$ are equal. Motivated by an isogeny criterion of Kulkarni, Patankar, and Rajan, which states that E_1 and E_2 are not potentially isogenous if and only if $\mathcal{F}_{E_1,E_2}(x) = \mathrm{o}\left(\frac{x}{\log x}\right)$, we investigate the growth in x of $\mathcal{F}_{E_1,E_2}(x)$. We prove that if E_1 and E_2 are not potentially isogenous, then there exist positive constants $\kappa(E_1,E_2,K)$, $\kappa'(E_1,E_2,K)$, and $\kappa''(E_1,E_2,K)$ such that the following bounds hold: (i) $\mathcal{F}_{E_1,E_2}(x) < \kappa(E_1,E_2,K)\frac{x(\log\log x)^{\frac{1}{9}}}{(\log x)^{\frac{19}{18}}}$; (ii) $\mathcal{F}_{E_1,E_2}(x) < \kappa'(E_1,E_2,K)\frac{x^{\frac{6}{7}}}{(\log x)^{\frac{5}{7}}}$ under the Generalized Riemann Hypothesis for Dedekind zeta functions (GRH); (iii) $\mathcal{F}_{E_1,E_2}(x) < \kappa''(E_1,E_2,K)x^{\frac{2}{3}}(\log x)^{\frac{1}{3}}$ under GRH, Artin's Holomorphy Conjecture for the Artin L-functions of number field extensions, and a Pair Correlation Conjecture for the zeros of the Artin L-functions of number field extensions.

1. Introduction

Let K be a number field, with $\mathcal{O}_K$ denoting its ring of integers and $\overline{K}$ denoting a fixed algebraic closure. In what follows, we use the letter $\mathfrak{p}$ to denote a non-zero prime ideal of $\mathcal{O}_K$ and refer to it as a *prime* of K, $\mathrm{N}_K(\mathfrak{p})$ to denote the norm of $\mathfrak{p}$, and $\mathbb{F}_{\mathfrak{p}}$ to denote the finite field $\mathcal{O}_K/\mathfrak{p}$.

Let E_1 and E_2 be elliptic curves over K. We denote by N_1 and N_2 the norms of the conductors of E_1 and E_2, respectively. For a prime $\mathfrak{p}$ of K that is of good reduction for both E_1 and E_2 and for each index $1 \le j \le 2$, we consider the polynomial $P_{E_j,\mathfrak{p}}(X) := X^2 - a_{\mathfrak{p}}(E_j)X + \mathrm{N}_K(\mathfrak{p}) \in \mathbb{Z}[X]$, where $\mathrm{N}_K(\mathfrak{p}) + 1 - a_{\mathfrak{p}}(E_j)$ is the number of $\mathbb{F}_{\mathfrak{p}}$-rational points of the reduction of E_j modulo $\mathfrak{p}$. We recall that, for any rational prime ℓ distinct from the field characteristic of $\mathbb{F}_{\mathfrak{p}}$, $P_{E_j,\mathfrak{p}}(X)$ is the characteristic polynomial of the image $\rho_{E_j,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ of a Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}\left(\overline{K}/K\right)$ under the ℓ-adic Galois representation $\rho_{E_j,\ell}$ of E_j defined by the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on the ℓ-division points of $E_j\left(\overline{K}\right)$. Viewing $P_{E_j,\mathfrak{p}}(X)$ in $\mathbb{C}[X]$ and denoting its

Key words and phrases: elliptic curves, Frobenius fields, Frobenius traces, Galois representations, prime density

2010 Mathematics Subject Classification: 11G05, 11G20, 11N05 (Primary), 11N80 (Secondary)

A.C.C. was partially supported by a Collaboration Grant for Mathematicians from the Simons Foundation under Award No. 709008.

T.W. was partially supported by a University of Illinois at Chicago Dean's Scholar Fellowship.

roots by $\pi_{\mathfrak{p}}(E_j)$ and $\overline{\pi_{\mathfrak{p}}(E_j)}$, we recall that $|\pi_{\mathfrak{p}}(E_j)| = \sqrt{\mathrm{N}_K(\mathfrak{p})}$, which implies that $|a_{\mathfrak{p}}(E_j)| \leq 2\sqrt{\mathrm{N}_K(\mathfrak{p})}$ and hence that $\mathbb{Q}(\pi_{\mathfrak{p}}(E_j))$ is either $\mathbb{Q}$ or an imaginary quadratic field. In what follows, we refer to $a_{\mathfrak{p}}(E_j)$ as the *Frobenius trace* and to $\mathbb{Q}(\pi_{\mathfrak{p}}(E_j))$ as the *Frobenius field* associated to E_j and $\mathfrak{p}$.

From now on, we assume that E_1 and E_2 are without complex multiplication. Given a field extension L of K, we say that E_1 and E_2 are *L-isogenous* if there exists an isogeny from E_1 to E_2, defined over L. We say that E_1 and E_2 are *potentially isogenous* if there exists a finite extension L of K such that E_1 and E_2 are L-isogenous. It is known that the following statements are equivalent: E_1 and E_2 are potentially isogenous; E_1 and E_2 are $\overline{K}$-isogenous; E_1 and E_2 are L-isogenous for some quadratic field extension L of K; either E_1 and E_2 are K-isogenous, or there exists a quadratic character χ such that E_1 and the quadratic twist E_2^{χ} are K-isogenous (e.g., see [**LeFNa20**, Lemma 3.1, p. 214; proof of Claim 3, p. 215]). Our goal in this paper is to investigate questions arising from a criterion regarding whether E_1 and E_2 are potentially isogenous, as we explain below.

In [**KuPaRa16**, Theorem 3, p. 90], Kulkarni, Patankar, and Rajan show that E_1 and E_2 are potentially isogenous if and only if the set of primes $\mathfrak{p}$ of K, of good reduction for E_1 and E_2, such that $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$, has a positive upper density within the set of primes of K, that is, the counting function

$$\mathcal{F}_{E_1,E_2}(x) := \#\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \mathrm{N}_K(\mathfrak{p}) \nmid N_1 N_2, \mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2))\}$$

satisfies

$$\limsup_{x \to \infty} \frac{\mathcal{F}_{E_1,E_2}(x)}{\#\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x\}} > 0.$$

Thus, E_1 and E_2 are not potentially isogenous if and only if $\mathcal{F}_{E_1,E_2}(x) = \mathrm{o}\left(\frac{x}{\log x}\right)$.

In relation to the above result, in [**KuPaRa16**, Conjecture 1, p. 91], Kulkarni, Patankar, and Rajan mention the following conjecture: *E_1 and E_2 are not potentially isogenous if and only if there exists a positive constant $c(E_1, E_2, K)$, which may depend on E_1, E_2, and K, such that, for any sufficiently large x, $\mathcal{F}_{E_1,E_2}(x) < c(E_1, E_2, K)\frac{x^{\frac{1}{2}}}{\log x}$.* While the "if" implication follows from the aforementioned result of Kulkarni, Patankar, and Rajan, the "only if" implication remains open and motivates the investigation of the growth of the function $\mathcal{F}_{E_1,E_2}(x)$.

In [**CoFoMu05**, p. 1174], the authors record the following remark of Serre, highlighting only the main idea of proof: if E_1 and E_2 are not potentially isogenous, then, under the Generalized Riemann Hypothesis for Dedekind zeta functions, there exists a positive constant $c'(E_1, E_2, K)$, which depends on E_1, E_2, and K, such that, for any sufficiently large x,

$$\begin{aligned}\#\{\mathfrak{p} \text{ degree one prime} : \mathrm{N}_K(\mathfrak{p}) \leq x, \mathrm{N}_K(\mathfrak{p}) \nmid N_1 N_2, \mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2)) \notin \{\mathbb{Q}(i), \mathbb{Q}(i\sqrt{3})\}\} \\ \leq c'(E_1, E_2, K) x^{\frac{11}{12}}.\end{aligned}$$

In [**BaPa18**, Theorem 2, p. 43], Baier and Patankar address the growth of $\mathcal{F}_{E_1,E_2}(x)$ in the case $K = \mathbb{Q}$ and prove that, under the Generalized Riemann Hypothesis for Dedekind zeta functions, there exists a positive constant $c''(E_1, E_2)$, which depends on E_1 and E_2, such that, for any sufficiently large x,

$$\mathcal{F}_{E_1,E_2}(x) < c''(E_1, E_2) x^{\frac{29}{30}} (\log x)^{\frac{1}{15}}.$$

In [**BaPa18**, Theorem 3, p. 43], Baier and Patankar also prove the following unconditional bound for $\mathcal{F}_{E_1,E_2}(x)$, resulting from an unconditional variation of the proof of their conditional result: there exists a positive constant $c'''(E_1, E_2)$, which depends on E_1 and E_2, such that, for any sufficiently large x,

$$\mathcal{F}_{E_1,E_2}(x) < c'''(E_1, E_2) \frac{x (\log \log x)^{\frac{22}{21}}}{(\log x)^{\frac{43}{42}}}.$$

The argument highlighted by Serre in [**CoFoMu05**, p. 1174] is based on a direct application of a conditional upper bound version of the Chebotarev density theorem in the setting of an infinite Galois extension of K defined by the ℓ-adic Galois representations of E_1 and E_2, for a suitably chosen rational prime ℓ. The proofs given by Baier and Patankar in [**BaPa18**] are based on indirect applications of conditional and unconditional effective asymptotic versions of the Chebotarev density theorem, via the square sieve, in the setting of a finite Galois extension of $\mathbb{Q}$ defined by the residual modulo $\ell_1 \ell_2$ Galois representations of E_1 and E_2, for distinct suitably chosen rational primes ℓ_1 and ℓ_2.

The main goal of this paper is to improve the current upper bounds for $\mathcal{F}_{E_1,E_2}(x)$, as follows: unconditionally; under the Generalized Riemann Hypothesis for Dedekind zeta functions; under the Generalized Riemann Hypothesis for Dedekind zeta functions, Artin's Holomorphy Conjecture for the Artin L-functions of number field extensions, and a Pair Correlation Conjecture regarding the zeros of the Artin L-functions of number field extensions. We shall refer to these latter hypotheses as GRH, AHC, and PCC, and state them explicitly in the notation part of Section 1.

THEOREM 1. *Let E_1 and E_2 be elliptic curves over a number field K, without complex multiplication, and not potentially isogenous. Denote by N_1 and N_2 the norms of the conductors of E_1 and E_2, respectively.*

(i) *There exists a positive constant $\kappa(E_1, E_2, K)$, which depends on E_1, E_2, and K, such that, for any sufficiently large x,*

$$\mathcal{F}_{E_1,E_2}(x) < \kappa(E_1, E_2, K) \frac{x (\log \log x)^{\frac{1}{9}}}{(\log x)^{\frac{19}{18}}}.$$

(ii) *If GRH holds, then there exists a positive constant $\kappa'(E_1, E_2, K)$, which depends on E_1, E_2, and K, such that, for any sufficiently large x,*

$$\mathcal{F}_{E_1,E_2}(x) < \kappa'(E_1, E_2, K) \frac{x^{\frac{6}{7}}}{(\log x)^{\frac{5}{7}}}.$$

(iii) *If GRH, AHC, and PCC hold, then there exists a positive constant $\kappa''(E_1, E_2, K)$, which depends on E_1, E_2, and K, such that, for any sufficiently large x,*

$$\mathcal{F}_{E_1,E_2}(x) < \kappa''(E_1, E_2, K) x^{\frac{2}{3}} (\log x)^{\frac{1}{3}}.$$

Remark 2. Theorem 1 may be viewed under the general theme of strong multiplicity one results, such as those proven in [**JaSh76**], [**MuPu17**], [**Ra94**], [**Ra00**], [**Wa14**], and [**Wo22**]. In particular, the methods developed in [**MuPu17**] and [**Wo22**] are applicable to bounding $\mathcal{F}_{E_1,E_2}(x)$ from above in the case $K = \mathbb{Q}$ and under hypotheses different from ours. Specifically, letting E_1 and E_2 be elliptic curves over $\mathbb{Q}$, without complex multiplication, not potentially isogenous, and assuming the Generalized Riemann Hypothesis for the Rankin-Selberg L-functions associated to the symmetric power L-functions of E_1 and E_2, the methods of [**MuPu17**] lead to $\mathcal{F}_{E_1,E_2}(x) \leq \kappa_2(E_1,E_2)\frac{x^{\frac{7}{8}}}{(\log x)^{\frac{1}{2}}}$ (see [**Wo22**, Remark (ii), p. 567]), while the methods of [**Wo22**] lead to $\mathcal{F}_{E_1,E_2}(x) \leq \kappa_3(E_1,E_2)\frac{x^{\frac{5}{6}}}{(\log x)^{\frac{1}{3}}}$ (see [**Wo22**, Theorem 1.11, p. 566]), where $\kappa_2(E_1,E_2)$ and $\kappa_3(E_1,E_2)$ are positive constants that depend on E_1 and E_2. It is not obvious if these methods generalize easily to tackle the case $K \neq \mathbb{Q}$ of Theorem 1 or to tackle the case $(\alpha_1,\alpha_2) \neq (\pm 1, \pm 1)$ of Theorem 3.

An immediate application of Theorem 1 is another proof of the aforementioned isogeny criterion of Kulkarni, Patankar, and Rajan (see Section 5).

The proof of Theorem 1 relies on upper bounds related to the Lang-Trotter Conjecture for Frobenius fields of one elliptic curve. We formulate the relevant results here for the convenience of the reader. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let F be an imaginary quadratic field. Lang and Trotter [**LaTr76**] conjectured the asymptotic

$$\pi_{E,F}(x) := \#\{p \leq x : p \nmid N_E, \mathbb{Q}(\pi_p(E)) \simeq F\} \sim C(E,F)\frac{x^{\frac{1}{2}}}{\log x},$$

where $C(E,F)$ is an explicit constant depending on E and F. Zywina [**Zy15**, Theorem 1.3, p. 236] proved that unconditionally,

$$\pi_{E,F}(x) \leq \kappa_1(E,F)\frac{x(\log\log x)^2}{(\log x)^2},$$

and that under GRH,

$$\pi_{E,F}(x) \leq \kappa_1'(E,F)\frac{x^{\frac{4}{5}}}{(\log x)^{\frac{3}{5}}}.$$

Murty, Murty, and Wong [**MuMuWo18**, Corollary 1.6, p. 406] proved that under GRH, AHC, and PCC,

$$\pi_{E,F}(x) \leq \kappa_1''(E,F)\frac{x^{\frac{2}{3}}}{(\log x)^{\frac{1}{2}}}.$$

The proof of Theorem 1 also relies on the following result which relates to the generalization of the Lang-Trotter Conjecture on Frobenius traces formulated by Chen, Jones, and Serban in [**ChJoSe22**].

Theorem 3. *Let E_1 and E_2 be elliptic curves over a number field K, without complex multiplication, and not potentially isogenous. Denote by N_1 and N_2 the norms of the conductors of E_1 and E_2, respectively. Let α_1 and α_2 be coprime integers, not both zero. For $x > 0$, set*

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) := \#\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \gcd(\mathrm{N}_K(\mathfrak{p}), 6N_1N_2) = 1, \alpha_1 a_{\mathfrak{p}}(E_1) + \alpha_2 a_{\mathfrak{p}}(E_2) = 0\}.$$

(i) *There exists a positive constant $\kappa_0(E_1, E_2, K, \alpha_1, \alpha_2)$, which depends on E_1, E_2, K, α_1, and α_2, such that, for any sufficiently large x,*

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) < \kappa_0(E_1, E_2, K, \alpha_1, \alpha_2)\frac{x(\log\log x)^{\frac{1}{9}}}{(\log x)^{\frac{19}{18}}}.$$

(ii) *If GRH holds, then there exists a positive constant $\kappa_0'(E_1, E_2, K, \alpha_1, \alpha_2)$, which depends on E_1, E_2, K, α_1, and α_2, such that, for any sufficiently large x,*

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) < \kappa_0'(E_1, E_2, K, \alpha_1, \alpha_2)\frac{x^{\frac{6}{7}}}{(\log x)^{\frac{5}{7}}}.$$

(iii) *If GRH, AHC, and PCC hold, then there exists a positive constant $\kappa_0''(E_1, E_2, K, \alpha_1, \alpha_2)$, which depends on E_1, E_2, K, α_1, and α_2, such that, for any sufficiently large x,*

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) < \kappa_0''(E_1, E_2, K, \alpha_1, \alpha_2)x^{\frac{2}{3}}(\log x)^{\frac{1}{3}}.$$

Remark 4. Taking $K = \mathbb{Q}$ in the setting of Theorem 3 and invoking [**MaWa23**, Corollary 1.2, p. 3] instead of [**Lo16**, Lemma 7.1, p. 409] in the proofs of parts (ii) and (iii), our proof leads to the following more explicit bounds.

(ii') If GRH holds, then there exists an absolute, effectively computable, positive constant κ_1' such that, for any sufficiently large x, $\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) < \kappa_1' \frac{x^{\frac{6}{7}}}{(\log x)^{\frac{5}{7}}} \left(\log(N_1N_2)\right)^{\frac{7}{2}} \left(\alpha_1\alpha_2\right)^{\frac{5}{2}}$.

(iii') If GRH, AHC, and PCC hold, then there exists an absolute, effectively computable, positive constant κ_1'' such that, for any sufficiently large x, $\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) < \kappa_1'' x^{\frac{2}{3}}(\log x)^{\frac{1}{3}} \left(\log(N_1N_2)\right)^{\frac{3}{2}} \left(\alpha_1\alpha_2\right)^{\frac{1}{2}}$.

Remark 5. Theorem 3 may be viewed under the general Lang-Trotter theme of results about the number of primes for which the Frobenius trace of an abelian variety is fixed, such as those proven in [**ChJoSe22**], [**CoWa22**], [**CoWa23**], [**Mu85**], [**MuMuSa88**], [**MuMuWo18**], [**Se81**], [**ThZa18**], and [**Zy15**]. The connection between Theorem 3, and thus Theorem 1, with the Lang-Trotter Conjectures on Frobenius traces formulated in [**LaTr76**, p. 33] and [**ChJoSe22**, p. 382] prompts the question of predicting, conjecturally, the asymptotic behavior of $\mathcal{F}_{E_1,E_2}(x)$ and $\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x)$ for E_1, E_2, α_1, and α_2 as in the setting of Theorem 3. We relegate such investigations to a future project.

Notation

• Given a number field K, we denote by $\mathcal{O}_K$ its ring of integers, by $\sum_K$ the set of non-zero prime ideals of $\mathcal{O}_K$, by n_K the degree of K over $\mathbb{Q}$, by $d_K \in \mathbb{Z}\backslash\{0\}$ the discriminant of an integral basis of $\mathcal{O}_K$, and by $\operatorname{disc}(K/\mathbb{Q}) = \mathbb{Z}d_K \trianglelefteq \mathbb{Z}$ the discriminant ideal of $K/\mathbb{Q}$. For a prime ideal $\mathfrak{p} \in \sum_K$, we denote by $\mathrm{N}_K(\mathfrak{p})$ its norm in $K/\mathbb{Q}$. We say that K satisfies the Generalized Riemann Hypothesis (GRH) if the Dedekind zeta function ζ_K of K has the property that, for any $\rho \in \mathbb{C}$ with $0 \le \operatorname{Re}\rho \le 1$ and $\zeta_K(\rho) = 0$, we have $\operatorname{Re}(\rho) = \frac{1}{2}$. When $K = \mathbb{Q}$, the Dedekind zeta function is the Riemann zeta function, in which case we refer to GRH as the Riemann Hypothesis (RH).

- Given a finite Galois extension L/K of number fields and a subset $\mathcal{C} \subseteq \operatorname{Gal}(L/K)$, stable under conjugation, we denote by $\pi_{\mathcal{C}}(x, L/K)$ the number of non-zero prime ideals of the ring of integers of K, unramified in L, of norm at most x, for which the Frobenius element is contained in $\mathcal{C}$. We set

$$M(L/K) := 2[L:K]|d_K|^{\frac{1}{n_K}} {\prod_p}' p,$$

with the dash on the product indicating that each of the primes p therein lies over a non-zero prime ideal $\wp$ of $\mathcal{O}_L$, with $\wp$ ramified in L.

- Given a finite Galois extension L/K of number fields and an irreducible character χ of the Galois group of L/K, we denote by $\mathfrak{f}(\chi) \trianglelefteq \mathcal{O}_K$ the global Artin conductor of χ, by $A_\chi := |d_L|^{\chi(1)} \operatorname{N}_K(\mathfrak{f}(\chi)) \in \mathbb{Z}$ the conductor of χ, and by $\mathcal{A}_\chi(T)$ the function of a positive real variable $T > 3$ defined by the relation

$$\log \mathcal{A}_\chi(T) = \log A_\chi + \chi(1) n_K \log T.$$

- Given a finite Galois extension L/K of number fields, we say that it satisfies Artin's Holomorphy Conjecture (AHC) if, for any irreducible character χ of the Galois group of L/K, the Artin L-function $L(s, \chi, L/K)$ extends to a function that is analytic on $\mathbb{C}$, except at $s = 1$ when $\chi = 1$. We recall that, if we assume GRH for L and AHC for L/K, then, given any irreducible character χ of the Galois group of L/K, and given any non-trivial zero ρ of $L(s, \chi, L/K)$, the real part of ρ satisfies $\operatorname{Re} \rho = \frac{1}{2}$. In this case, we write $\rho = \frac{1}{2} + i\gamma$, where γ denotes the imaginary part of ρ.

- Given a finite Galois extension L/K of number fields, let us assume GRH for L and AHC for L/K. For an irreducible character χ of the Galois group of L/K and an arbitrary $T > 0$, we define the pair correlation function of $L(s, \chi, L/K)$ by

$$\mathcal{P}_T(X, \chi) := \sum_{-T \leq \gamma_1 \leq T} \sum_{-T \leq \gamma_2 \leq T} w(\gamma_1 - \gamma_2) e((\gamma_1 - \gamma_2)X),$$

where γ_1 and γ_2 range over all the imaginary parts of the non-trivial zeroes $\rho = \frac{1}{2} + i\gamma$ of $L(s, \chi, L/K)$, counted with multiplicity, and where, for an arbitrary real number u, $e(u) := \exp(2\pi i u)$ and $w(u) := \frac{4}{4+u^2}$. We say that the extension L/K satisfies the Pair Correlation Conjecture (PCC) if, for any irreducible character χ of the Galois group of L/K and for any $A > 0$ and $T > 3$, provided $0 \leq Y \leq A\chi(1) n_K \log T$, we have

$$\mathcal{P}_T(Y, \chi) \ll_A \chi(1)^{-1} T \log \mathcal{A}_\chi(T).$$

2. From shared Frobenius fields to shared absolute values of Frobenius traces

We keep the general setting and notation from Section 1. To prove Theorem 1, we reduce the study of the primes $\mathfrak{p}$ for which the Frobenius fields of E_1 and E_2 coincide to a study of the primes $\mathfrak{p}$ for which the absolute values of the Frobenius traces of E_1 and E_2 coincide, as follows.

Lemma 6. *Let E_1 and E_2 be elliptic curves over a number field K, non-isogenous over K. Denote by N_1 and N_2 the norms of the conductors of E_1 and E_2, respectively. Let $\mathfrak{p}$ be a degree one prime of K such that the rational prime $p := \mathrm{N}_K(\mathfrak{p})$ satisfies $p \nmid 6N_1N_2$. Assume that $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1)), \mathbb{Q}(\pi_{\mathfrak{p}}(E_2)) \notin \left\{\mathbb{Q}(i), \mathbb{Q}(i\sqrt{3})\right\}$. Then $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$ if and only if $|a_{\mathfrak{p}}(E_1)| = |a_{\mathfrak{p}}(E_2)|$.*

Proof. The "if" implication is clear, since, for each $1 \leq j \leq 2$, $\mathbb{Q}(\pi_{\mathfrak{p}}(E_j)) = \mathbb{Q}\left(\sqrt{a_{\mathfrak{p}}(E_j)^2 - 4p}\right)$. To justify the "only if" implication, we distinguish between $\mathfrak{p}$ supersingular and ordinary for E_1 and E_2. If $\mathfrak{p}$ is supersingular for both E_1 and E_2, then $a_{\mathfrak{p}}(E_1) = a_{\mathfrak{p}}(E_2) = 0$. When $\mathfrak{p}$ is ordinary for both E_1 and E_2, or ordinary for one of E_1 or E_2, and supersingular for the other, we look at the prime ideal factorization of p in the ring of integers $\mathcal{O}_F$ of the imaginary quadratic field $F := \mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$. By the lemma's hypothesis, the group of units of $\mathcal{O}_F$ is $\mathcal{O}_F^{\times} = \{-1, 1\}$. If $\mathfrak{p}$ is ordinary for both E_1 and E_2, then p splits completely in $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1))$ and $\mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$, hence in F. Then, as ideals in $\mathcal{O}_F$, either $(\pi_{\mathfrak{p}}(E_1)) = (\pi_{\mathfrak{p}}(E_2))$, or $(\pi_{\mathfrak{p}}(E_1)) = \left(\overline{\pi_{\mathfrak{p}}(E_2)}\right)$. As such, $\pi_{\mathfrak{p}}(E_1) \in \{-\pi_{\mathfrak{p}}(E_2), \pi_{\mathfrak{p}}(E_2)\}$ or $\pi_{\mathfrak{p}}(E_1) \in \left\{-\overline{\pi_{\mathfrak{p}}(E_2)}, \overline{\pi_{\mathfrak{p}}(E_2)}\right\}$, which implies that $\mathrm{Tr}_{F/\mathbb{Q}}(\pi_{\mathfrak{p}}(E_1)) \in \left\{-\mathrm{Tr}_{F/\mathbb{Q}}(\pi_{\mathfrak{p}}(E_2)), \mathrm{Tr}_{F/\mathbb{Q}}(\pi_{\mathfrak{p}}(E_2))\right\}$, where $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)$ denotes the trace of the algebraic number $\alpha \in F$. Since, for each $1 \leq j \leq 2$, $a_{\mathfrak{p}}(E_j) = \mathrm{Tr}_{\mathbb{Q}(\pi_{\mathfrak{p}}(E_j))/\mathbb{Q}}(\pi_{\mathfrak{p}}(E_j))$, we obtain that $|a_{\mathfrak{p}}(E_1)| = |a_{\mathfrak{p}}(E_2)|$. If $\mathfrak{p}$ is ordinary for one of E_1 or E_2, say, for E_1, and supersingular for the other, say, for E_2, then p splits completely in $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1))$ and ramifies in $\mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$, contradicting that $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$. Thus, this case does not occur. □

3. Elliptic curves with shared absolute values of Frobenius traces

We keep the general setting and notation from Section 1. In light of Lemma 6, in order to prove Theorem 1, we focus on the primes $\mathfrak{p}$ for which $|a_{\mathfrak{p}}(E_1)| = |a_{\mathfrak{p}}(E_2)|$. We view this condition as a combination of two linear relations between the traces of E_1 and E_2, namely $a_{\mathfrak{p}}(E_1) + a_{\mathfrak{p}}(E_2) = 0$ and $a_{\mathfrak{p}}(E_1) - a_{\mathfrak{p}}(E_2) = 0$, which are particular cases of Theorem 3,. Our goal in this section is to prove Theorem 3.

3.1. Preliminaries. We follow the methods developed in [**CoWa23**] and [**Wa23**]. These methods already give rise to the stated conditional estimates for $\mathcal{T}_{E_1,E_2}^{1,1}(x)$, but need to be adjusted for the general conditional and unconditional bounds, as we explain below.

Consider the abelian surface

$$A := E_1 \times E_2.$$

For an arbitrary rational prime ℓ, consider the residual modulo ℓ Galois representations $\overline{\rho}_{A,\ell}$, $\overline{\rho}_{E_1,\ell}$, and $\overline{\rho}_{E_2,\ell}$ of A, E_1, and E_2, respectively, defined by the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on the ℓ-division groups $A[\ell]$, $E_1[\ell]$, and $E_2[\ell]$, respectively. We recall that

$$\overline{\rho}_{A,\ell}(\sigma) = (\overline{\rho}_{E_1,\ell}(\sigma), \overline{\rho}_{E_2,\ell}(\sigma)) \text{ for any } \sigma \in \mathrm{Gal}\left(\overline{K}/K\right), \tag{1}$$

$$\mathrm{tr}(\overline{\rho}_{E_j,\ell}(\mathrm{Frob}_{\mathfrak{p}})) \equiv a_{\mathfrak{p}}(E_j) (\mathrm{mod}\, \ell) \text{ for any } \mathfrak{p} \text{ with} \gcd(\mathrm{N}_K(\mathfrak{p}), \ell N_j) = 1 \text{and for any } 1 \leq j \leq 2. \tag{2}$$

Setting

$$G(\ell) := \{(M_1, M_2) \in \mathrm{GL}_2(\mathbb{F}_\ell) \times \mathrm{GL}_2(\mathbb{F}_\ell) : \det M_1 = \det M_2\},$$

we recall from [**Lo16**, Lemma 7.1, p. 409] that, thanks to our assumptions that E_1 and E_2 are without complex multiplication and not potentially isogenous, there exists a positive integer $c(A, K)$, which depends on A and K, such that if $\ell > c(A, K)$, then $\operatorname{Im} \overline{\rho}_{A,\ell} = G(\ell)$, that is,

$$\mathrm{Gal}(K(A[\ell])/K) \simeq G(\ell). \tag{3}$$

For an arbitrary pair of matrices $(M_1, M_2) \in G(\ell)$ and for each $1 \leq j \leq 2$, we denote by $\lambda_1(M_j), \lambda_2(M_j) \in \overline{\mathbb{F}}_\ell$ the eigenvalues of M_j. Associated to $G(\ell)$, we consider the groups

$$B(\ell) := \left\{ \left(\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right) \in G(\ell) \right\}, \ \Lambda(\ell) := \left\{ \left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right) \in G(\ell) : a \in \mathbb{F}_\ell^\times \right\},$$

$$U(\ell) := \left\{ \left(\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right) \in G(\ell) \right\}, \ U'(\ell) := \Lambda(\ell) \cdot U(\ell), \quad P(\ell) := G(\ell)/\Lambda(\ell),$$

and the sets

$$\begin{aligned}
G(\ell)^{\#} &:= \text{the set of conjugacy classes of } G(\ell), \\
P(\ell)^{\#} &:= \text{the set of conjugacy classes of } P(\ell), \\
\mathcal{C}(\ell)^{\alpha_1,\alpha_2} &:= \left\{(M_1, M_2) \in G(\ell) : \lambda_1(M_j), \lambda_2(M_j) \in \mathbb{F}_\ell^\times \ \forall 1 \leq j \leq 2, \alpha_1 \operatorname{tr} M_1 + \alpha_2 \operatorname{tr} M_2 = 0\right\}, \\
\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2} &:= \{(M_1, M_2) \in G(\ell) : \alpha_1 \operatorname{tr} M_1 + \alpha_2 \operatorname{tr} M_2 = 0\}, \\
\mathcal{C}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2} &:= \mathcal{C}(\ell)^{\alpha_1,\alpha_2} \cap B(\ell), \\
\widehat{\mathcal{C}}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2} &:= \text{ the image of } \mathcal{C}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2} \text{ in } B(\ell)/U'(\ell), \\
\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2} &:= \text{ the image of } \mathcal{C}_0(\ell)^{\alpha_1,\alpha_2} \text{ in } G(\ell)/\Lambda(\ell).
\end{aligned}$$

With the above notation, our strategy for proving parts (i) and (iii) of Theorem 3 is to relate

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \text{ to } \pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right),$$

and our strategy for proving part (ii) of Theorem 3 is to relate

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \text{ to } \pi_{\mathcal{C}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}\right).$$

After establishing these relations, we apply different variations of the effective Chebotarev density theorem to obtain upper bounds for the number of primes $\mathfrak{p}$ whose Frobenius element satisfies the desired Chebotarev conditions. In the end, we minimize the bounds by choosing ℓ suitably as a function of x.

Before executing this strategy, we record a few properties of the groups and sets introduced above.

Lemma 7. *For ℓ an arbitrary rational prime, the following statements hold.*

(i) *$\Lambda(\ell)$ is a normal subgroup of $G(\ell)$.*

(ii) *$U'(\ell)$ is a normal subgroup of $B(\ell)$, with $B(\ell)/U'(\ell)$ an abelian group.*

Proof. Part (i) is clear. Part (ii) is [**CoWa23**, Lemma 11, p. 697]. □

Lemma 8. *For ℓ an arbitrary rational prime, the following statements hold.*

(i) $U'(\ell)\ \mathcal{C}_{Borel}(\ell)^{\alpha_1,\alpha_2} \subseteq \mathcal{C}_{Borel}(\ell)^{\alpha_1,\alpha_2}$.

(ii) *Every conjugacy class in $\mathcal{C}(\ell)^{\alpha_1,\alpha_2}$ contains an element of $B(\ell)$.*

(iii) $\Lambda(\ell)\ \mathcal{C}_0(\ell)^{\alpha_1,\alpha_2} \subseteq \mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}$.

Proof. For part (i), the case $\alpha_1 = \alpha_2 = 1$ is [**CoWa23**, Lemma 14 (vi), p. 699]. In general, let $M' = (M'_1, M'_2) \in U'(\ell)$ be such that the diagonals are equal to some $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ and let $M = (M_1, M_2) \in \mathcal{C}_{\text{Borel}}(\ell)^{\alpha_1,\alpha_2}$. Then $M'M \in B(\ell)$ and

$$\alpha_1 \operatorname{tr}(M'_1 M_1) + \alpha_2 \operatorname{tr}(M'_2 M_2) = a\,(\alpha_1 \operatorname{tr}(M_1) + \alpha_2 \operatorname{tr}(M_2)) = 0.$$

As such, $M'M \in \mathcal{C}_{\text{Borel}}(\ell)^{\alpha_1,\alpha_2}$.

For part (ii), the case $\alpha_1 = \alpha_2 = 1$ is [**CoWa23**, Lemma 16, p. 700]. In fact, by [**CoWa23**, Lemma 15, p. 700], every element in $\left\{(M_1, M_2) \in G(\ell) : \lambda_1(M_j), \lambda_2(M_j) \in \mathbb{F}_\ell^\times\ \forall 1 \leq j \leq 2\right\}$ is conjugate to an element in $B(\ell)$. In particular, every conjugacy class in $\mathcal{C}(\ell)^{\alpha_1,\alpha_2}$ contains an element of $B(\ell)$.

For part (iii), we provide a short proof.

Let $(aI, aI) \in \Lambda(\ell)$, with $a \in \mathbb{F}_\ell^\times$, and let $M = (M_1, M_2) \in \mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}$. Since (aI, aI) and M are in $G(\ell)$, the product $(aI, aI)M = (aM_1, aM_2)$ is in $G(\ell)$. Furthermore, since M is in $\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}$, we have $\alpha_1 \operatorname{tr}(M_1) + \alpha_2 \operatorname{tr}(M_2) = 0$, which implies that $\alpha_1 \operatorname{tr}(aM_1) + \alpha_2 \operatorname{tr}(aM_2) = 0$. Therefore, $(aI, aI)M \in \mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}$. □

Lemma 9. *For ℓ an odd rational prime, the following statements hold.*

(i) $|B(\ell)| = (\ell-1)^3\ell^2$.

(ii) $|U'(\ell)| = (\ell-1)\ell^2$.

(iii) $|\Lambda(\ell)| = \ell - 1$.

(iv) $|P(\ell)| = (\ell-1)^2\ell^2(\ell+1)^2$.

(v) $|G(\ell)^\#| \leq 4(\ell+1)^2(\ell-1)$ *and* $|P(\ell)^\#| \leq 16(\ell+1)^2$.

Proof. Parts (i) and (ii) follow from [**CoWa23**, Lemma 12, pp. 697–698]. Parts (iii) and (iv) are straightforward exercises derived from the definitions of the groups and the size of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Part (v) is [**Wa23**, Lemma 29, p. 45], whose proof we include below.

The number of conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is $\ell^2 - 1$ (see [**FeFi60**, p. 91]). Following [**JaLi01**, p. 324], these conjugacy classes can be classified into four types. By considering each type, we deduce that, for any $d \in \mathbb{F}_\ell^\times$, the number of conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with determinant d is at most $2\ell + 2$. Thus, $|G(\ell)^\#| \leq (2(\ell+1))^2 \cdot |\mathbb{F}_\ell^\times| = 4(\ell+1)^2(\ell-1)$. Now fix an arbitrary element $\mathcal{C} \in G(\ell)^\#$. If there is an element $a \in \mathbb{F}_\ell^\times$ such that $(aI_2)\mathcal{C} = \mathcal{C}$, then, by comparing determinants, we obtain $a^4 = 1$. So a takes at most 4 values in $\mathbb{F}_\ell^\times$. By the orbit-stabilizer theorem from group theory, each $\Lambda(\ell)$-orbit of $G(\ell)^\#$ contains at least $\frac{|\Lambda(\ell)|}{4}$ conjugacy classes. Therefore, $|P(\ell)^\#| \leq \frac{|G(\ell)^\#|}{|\mathbb{F}_\ell^\times|/4} \leq 16(\ell+1)^2$. This completes the proof of (v). □

Lemma 10. *For ℓ an odd rational prime such that ℓ does not divide at least one of α_1, α_2, the following statements hold.*

(i) $|\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}| \leq 2\ell^6$.

(ii) $|\widehat{\mathcal{C}}_{Borel}(\ell)^{\alpha_1,\alpha_2}| \leq 2(\ell-1)$.

(iii) $|\widehat{\mathcal{C}}_{Proj}(\ell)^{\alpha_1,\alpha_2}| \leq 2\ell^5$.

Proof. For parts (i), the case $\alpha_1 = \alpha_2 = 1$ is [**Wa23**, Lemma 33, p. 51]; the general case is proved similarly, as we explain in what follows. We recall that, for any $d \in \mathbb{F}_\ell^\times$ and $t \in \mathbb{F}_\ell$, the number of matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$ with determinant d and trace t is $\ell\left(\ell + \left(\frac{t^2-4d}{\ell}\right)\right)$, where $\left(\frac{\cdot}{\ell}\right)$ denotes the Legendre symbol. Therefore,

$$\begin{aligned}|\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}| &= \sum_{t\in\mathbb{F}_\ell}\sum_{d\in\mathbb{F}_\ell^\times}\sum_{\substack{M_1\in\mathrm{GL}_2(\mathbb{F}_\ell)\\ \det M_1=d, \operatorname{tr} M_1=t}} \#\left\{M_2\in\mathrm{GL}_2(\mathbb{F}_\ell) : \det M_2 = d, \operatorname{tr} M_2 = -\alpha_2^{-1}\alpha_1 t (\operatorname{mod} \ell)\right\}\\ &\leq 2\sum_{t\in\mathbb{F}_\ell}\sum_{d\in\mathbb{F}_\ell^\times}\sum_{\substack{M_1\in\mathrm{GL}_2(\mathbb{F}_\ell)\\ \det M_1=d, \operatorname{tr} M_1=t}} \ell^2 \leq 2\ell^6,\end{aligned}$$

where $\alpha_2^{-1}(\operatorname{mod}\ell)$ is the inverse of $\alpha_2(\operatorname{mod}\ell)$. Note that, since α_1 and α_2 are not both divisible by ℓ, either this inverse exists, or, if it does not, the inverse of $\alpha_1(\operatorname{mod}\ell)$ exists, in which case a similar argument works using $\alpha_1^{-1}(\operatorname{mod}\ell)$. This completes the proof of (i).

For part (ii), the case $\alpha_1 = \alpha_2 = 1$ is [**CoWa23**, Lemma 17, (iv), p.701] In the general case, we first consider the number of matrices in the image of $\mathcal{C}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2}$ in $B(\ell)/U(\ell) \simeq T(\ell)$. They are clearly determined by the diagonal entries and can be counted as follows:

$$\begin{aligned}&\sum_{a_1,a_2\in\mathbb{F}_\ell^\times} \#\left\{(b_1,b_2)\in\mathbb{F}_\ell^\times\times\mathbb{F}_\ell^\times : b_1+b_2 = -\alpha_2^{-1}\alpha_1(a_1+a_2)(\operatorname{mod}\ell), b_1b_2 = a_1a_2\right\}\\ &\leq 2(\ell-1)^2,\end{aligned}$$

where $\alpha_2^{-1}(\operatorname{mod}\ell)$ is the inverse of $\alpha_2(\operatorname{mod}\ell)$. As before, if the inverse does not exist, a similar argument works using $\alpha_1^{-1}(\operatorname{mod}\ell)$.

Next, we observe that the inverse image of $\widehat{\mathcal{C}}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2}$ under the projection $B(\ell)/U(\ell) \to B(\ell)/U'(\ell)$ is exactly the image of $\mathcal{C}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2}$ in $B(\ell)/U(\ell) \simeq T(\ell)$. In all,

$$|\widehat{\mathcal{C}}_{\mathrm{Borel}}(\ell)^{\alpha_1,\alpha_2}| \leq \frac{2(\ell-1)^2}{|U'(\ell)/U(\ell)|} \leq 2(\ell-1).$$

Finally, from part (iii) of Lemma 9 and part (i) of the current lemma, we deduce that $|\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}| \leq \frac{|\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}|}{|\Lambda(\ell)|} \leq 2\ell^5$. This completes the proof of (iii). □

We are now ready to prove Theorem 3.

3.2. Proof of part (i) of Theorem 3. The key ingredient is the unconditional effective Chebotarev density theorem of Lagarias and Odlyzko [**LaOd77**, Theorem 1.3, pp. 413–414], in the version stated in [**Se81**, Théorème 2, p. 132].

We fix a rational prime ℓ such that $\ell > c(A, K)$ and such that ℓ does not divide at least one of α_1, α_2. From (1) and (2), we deduce that

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \leq \pi_{\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}}(x, K(A[\ell])/K) + n_K + \log M(K/\mathbb{Q}). \tag{4}$$

In what follows, we bound from above the function on the right hand side of the inequality.

First, we relate $\pi_{\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}}(x, K(A[\ell])/K)$ to $\pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right)$ by appealing to [**Se81**, Proposition 7, p. 138, and Proposition 8 (b), p. 140]), in the version stated in [**CoWa23**, Corollary 5, p. 693]. Part (iii) of Lemma 8 ensures that we may apply these results to the Galois group $G(\ell) = \mathrm{Gal}(K(A[\ell])/K)$, its normal subgroup $\Lambda(\ell) = \mathrm{Gal}(K(A[\ell])/K(A[\ell])^{\Lambda(\ell)})$, and the set $\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}$. We deduce that

$$\begin{aligned}\pi_{\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}}(x, K(A[\ell])/K) &\ll \pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right) \\ &\quad + n_K\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(K(A[\ell])/K) + \log M(K(A[\ell])^{\Lambda(\ell)}/K)\right).\end{aligned}$$

To bound $\log M(K(A[\ell])/K)$ and $\log M\left(K(A[\ell])^{\Lambda(\ell)}/K\right)$, we proceed as in [**CoWa23**, (41), p. 708]. Specifically, relying on [**Se81**, Proposition 6, p. 130], on Lemma 9, and on the Néron–Ogg–Shafarevich criterion for abelian varieties, we obtain that

$$\log M(K(A[\ell])/K) \ll \frac{\log(\ell N_1 N_2 d_K)}{n_K},$$

$$\log M\left(K(A[\ell])^{\Lambda(\ell)}/K\right) \ll \frac{\log(\ell N_1 N_2 d_K)}{n_K}.$$

To estimate the counting function $\pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right)$, we apply [**Se81**, Théorème 2, p. 132] and obtain that there exists an absolute, effectively computable, positive constant a_0 such that, if

$$\log x > a_0 n_{K(A[\ell])^{\Lambda(\ell)}} \left(\log |d_{K(A[\ell])^{\Lambda(\ell)}}|\right)^2, \tag{5}$$

then, for any $b > 1$,

$$\pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right) \ll_b \frac{|\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}|}{|P(\ell)|}\,\mathrm{li}(x) + \left|\left(\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}\right)^{\#}\right| \frac{x}{(\log x)^b},$$

where $\left(\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}\right)^{\#}$ is the set of conjugacy classes in $\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}$ and $\mathrm{li}(x) := \int_2^x \frac{1}{\log t}\, dt$ is the logarithmic integral function. Then, by Lemmas 9 - 10, we deduce that

$$\pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right) \ll_b \frac{x}{\ell \log x} + \ell^2 \frac{x}{(\log x)^b}.$$

Finally, we choose the prime $\ell = \ell(x)$ such that $\ell > c(A, K)$, such that $\ell \nmid \alpha_1\alpha_2$, or $\alpha_1 = 0$, $\ell \nmid \alpha_2$, or $\alpha_2 = 0$, $\ell \nmid \alpha_1$, such that (5) is satisfied, and such that the final bounds are optimal, as follows.

Once more relying on [**Se81**, Proposition 5, p. 129], Lemma 9, and the Néron–Ogg–Shafarevich criterion for abelian varieties, we obtain that

$$n_{K(A[\ell])^{\Lambda(\ell)}} \left(\log |d_{K(A[\ell])^{\Lambda(\ell)}}|\right)^2 \leq |P(\ell)| n_K \left((|P(\ell)| n_K - 1) \log(\ell N_1 N_2 d_K) + (|P(\ell)| n_K - 1) \log |P(\ell) n_K - 1|\right)^2$$
$$\ll n_K^3 \ell^{18} (\log(\ell N_1 N_2 d_K))^2.$$

From [**Lo16**, Lemma 7.1, p. 409], we know that there exists an effectively computable, positive constant $a(h_A, n_K)$, which depends on the Faltings height h_A of A and on n_K, such that, if $\ell > a(h_A, n_K)$, then (3) holds. Hence condition (5) on ℓ is ensured by the restrictions

$$a_1(h_A, n_K) < \ell^{18} (\log \ell)^2 < a_2(h_A, n_K, d_K, N_1, N_2) \log x$$

for some positive constants $a_1(h_A, n_K)$ and $a_2(h_A, n_K, d_K, N_1, N_2)$, which depend on h_A, n_K, d_K, N_1, and N_2. By taking $x > x_0(h_A, n_K, d_K, N_1, N_2)$ for some positive real number which depends on h_A, n_K, d_K, N_1, and N_2, we may choose the prime ℓ such that

$$\ell(x) = \left[a_3 \frac{(\log x)^{\frac{1}{18}}}{(\log \log x)^{\frac{1}{9}}} \right]$$

for some positive constant $a_3 = a_3(h_A, n_K, d_K, N_1, N_2, \alpha_1, \alpha_2)$, which depends on h_A, n_K, d_K, N_1, N_2, α_1, and α_2.

Putting the bounds together, we deduce that

$$\mathcal{T}_{E_1, E_2}^{\alpha_1, \alpha_2}(x) < \kappa_0(E_1, E_2, K, \alpha_1, \alpha_2) \frac{x (\log \log x)^{\frac{1}{9}}}{(\log x)^{\frac{19}{18}}}$$

for some positive constant $\kappa_0(E_1, E_2, K, \alpha_1, \alpha_2)$, which depends on E_1, E_2, K, α_1, and α_2. This completes the proof of part (i) of Theorem 3.

3.3. Proof of part (iii) of Theorem 3. The key ingredient is the conditional effective Chebotarev density theorem proved in [**MuMuWo18**, Theorem 1.2, p. 402], which we use in the reformulation stated in [**CoWa22**, Theorem 7, p. 12]).

We fix a rational prime ℓ such that $\ell > c(A, K)$ and such that ℓ does not divide at least one of α_1, α_2. As in the proof of part (i), after using (4), we focus our attention on estimating, from above, $\pi_{\mathcal{C}_0(\ell)^{\alpha_1, \alpha_2}}(x, K(A[\ell])/K)$, this time under the assumptions of GRH, AHC, and PCC.

First, we proceed identically to part (i) and deduce that

$$\pi_{\mathcal{C}_0(\ell)^{\alpha_1, \alpha_2}}(x, K(A[\ell])/K) \ll \pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1, \alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right) + n_K \left(\frac{x^{\frac{1}{2}}}{\log x} + \frac{\log(\ell N_1 N_2 d_K)}{n_K}\right).$$

Next, we apply [**MuMuWo18**, Theorem 1.2, p. 402] (which requires GRH, AHC, and PCC) to estimate the counting function $\pi_{\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])^{\Lambda(\ell)}/K\right)$. By putting all estimates together, we deduce that

$$\begin{aligned}\pi_{\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])/K\right) \ll \frac{\left|\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}\right|}{|P(\ell)|} \cdot \frac{x}{\log x} \\ + n_K^{\frac{1}{2}} \left|\widehat{\mathcal{C}}_{\mathrm{Proj}}(\ell)^{\alpha_1,\alpha_2}\right|^{\frac{1}{2}} \left(\frac{|P(\ell)^{\#}|}{|P(\ell)|}\right)^{\frac{1}{2}} x^{\frac{1}{2}} \left(\frac{\log\left(\ell N_1 N_2 d_K\right)}{n_K} + \log x\right) \\ + n_K \left(\frac{x^{\frac{1}{2}}}{\log x} + \frac{\log(\ell N_1 N_2 d_K)}{n_K}\right).\end{aligned}$$

Then, using Lemmas 9 - 10, we infer that

$$\pi_{\mathcal{C}_0(\ell)^{\alpha_1,\alpha_2}}\left(x, K(A[\ell])/K\right) \ll \frac{x}{\ell \log x} + n_K^{\frac{1}{2}} \ell^{\frac{1}{2}} x^{\frac{1}{2}} \left(\frac{\log(\ell N_1 N_2 d_K)}{n_K} + \log x\right).$$

Reasoning as in part (i), we may choose the prime ℓ such that

$$\ell(x) = \left[a_4 \frac{x^{\frac{1}{3}}}{(\log x)^{\frac{4}{3}}}\right] \tag{6}$$

for some positive constant $a_4 = a_4(h_A, n_K, d_K, N_1, N_2, \alpha_1, \alpha_2)$, which depends on h_A, n_K, d_K, N_1, N_2, α_1, and α_2. Finally, recalling (4), we obtain that

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \leq \kappa_0''(E_1, E_2, K, \alpha_1, \alpha_2) x^{\frac{2}{3}} (\log x)^{\frac{1}{3}}$$

for some positive constant $\kappa_0''(E_1, E_2, K, \alpha_1, \alpha_2)$, which depends on E_1, E_2, K, α_1, and α_2. This completes the proof of part (iii) of Theorem 3.

3.4. Proof of part (ii) of Theorem 3. We base our proof on two key ingredients, a modification of [**CoWa23**, Lemma 9, pp. 694–695] and [**Zy15**, Theorem 2.3, p. 240], as we explain below.

The first key ingredient is the following minor modification of [**CoWa23**, Lemma 9, pp. 694–695], which itself is a generalization of [**MuMuSa88**, Lemma 4.4, p. 269].

Lemma 11. *Let $\mathcal{S}$ be a non-empty set of prime ideals of K, let $(K_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}}$ be a family of finite Galois extensions of $\mathbb{Q}$, and let $(\mathcal{C}_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}}$ be a family of non-empty sets such that each $\mathcal{C}_{\mathfrak{p}}$ is a union of conjugacy classes of $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q})$. Assume that there exist an absolute constant $c_1 > 0$ and a function $f : \mathbb{R} \to (0, \infty)$ such that*

$$n_{K_{\mathfrak{p}}} \leq c_1, \tag{7}$$

$$\log |d_{K_{\mathfrak{p}}}| \leq f(z) \text{ for all } \mathfrak{p} \text{ such that } \mathrm{N}_K(\mathfrak{p}) \leq z. \tag{8}$$

For each $x > 2$, let $y = y(x) > 2$, $u = u(x) > 2$ be such that

$$u \leq y, \tag{9}$$

and assume that, for any $\varepsilon > 0$,

$$u \geq c_2(\varepsilon) y^{\frac{1}{2}} (\log y)^{2+\varepsilon} \text{ for some constant } c_2(\varepsilon) > 0 \tag{10}$$

and

$$\lim_{x \to \infty} \frac{f(x)}{(\log y)^{1+\varepsilon}} = 0. \tag{11}$$

Assume GRH for Dedekind zeta functions. Then, for any $\varepsilon > 0$, there exists a constant $c(\varepsilon) > 0$ such that, for any sufficiently large x,

$$\#\left\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \mathfrak{p} \in \mathcal{S}\right\} \leq c(\varepsilon) \max_{y \leq \ell \leq y+u} \#\left\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \mathfrak{p} \in \mathcal{S}, \ell \nmid d_{K_{\mathfrak{p}}}, \left(\frac{K_{\mathfrak{p}}/\mathbb{Q}}{\ell}\right) \subseteq \mathcal{C}_{\mathfrak{p}}\right\}. \tag{12}$$

We apply this lemma to the set $\mathcal{S}^{\alpha_1,\alpha_2} := \{\mathfrak{p} : \gcd(\mathrm{N}_K(\mathfrak{p}), 6N_1N_2) = 1, \alpha_1 a_{\mathfrak{p}}(E_1) + \alpha_2 a_{\mathfrak{p}}(E_2) = 0\}$, to the fields $K_{\mathfrak{p}} := \mathbb{Q}(\pi_{\mathfrak{p}}(E_1), \pi_{\mathfrak{p}}(E_2))$, to the conjugacy classes $\mathcal{C}_{\mathfrak{p}} := \{\mathrm{id}_{K_{\mathfrak{p}}}\}$, and to the function $f(v) := 2\log(4v)$. Note that, for $\mathcal{S}^{1,1}$, this application is precisely the case $g = 2$ of [**CoWa23**, Lemma 18, pp. 704–705]. We obtain that, under the Riemann Hypothesis for the Riemann zeta function and GRH for the Dedekind zeta functions of the number fields $K_{\mathfrak{p}}$, the following holds.

For a fixed arbitrary $x > 2$, let $y := y(x)$ and $u := u(x)$ be real numbers such that $2 < u(x) < y(x)$. Assume that, for any $\varepsilon > 0$, $\lim_{x \to \infty} \frac{\log x}{(\log y(x))^{1+\varepsilon}} = 0$ and there exists a positive constant $c'(\varepsilon)$ such that, for any sufficiently large x, $u(x) \geq c'(\varepsilon) y(x)^{\frac{1}{2}} (\log y(x))^{2+\varepsilon}$. Then, upon fixing an arbitrary $\varepsilon > 0$, there exist a positive constant $c(\varepsilon)$ and a positive real number x_ε such that, for any $x \geq x_\varepsilon$ and any $y(x)$, $u(x)$ satisfying the above conditions, we have

$$\begin{aligned} \mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \leq c(\varepsilon) \max_{y \leq \ell \leq y+u} \#\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \gcd(\mathrm{N}_K(\mathfrak{p}), 6N_1N_2) = 1, \alpha_1 a_{\mathfrak{p}}(E_1) + \alpha_2 a_{\mathfrak{p}}(E_2) = 0,& \\ \ell \text{ splits completely in } K_{\mathfrak{p}}\}.& \end{aligned}$$

From (1), (2), and (3), we deduce that

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \leq c(\varepsilon) \max_{y \leq \ell \leq y+u} \pi_{\mathcal{C}(\ell)^{\alpha_1,\alpha_2}}(x, K(A[\ell])/K). \tag{13}$$

The second key ingredient in our proof is [**Zy15**, Theorem 2.3, p. 240] (see also its restatements [**CoWa23**, Theorem 7, p. 693, and Corollary 8, p. 694])). We will use this result to obtain upper bounds for the right hand side of (13).

As in the proofs of parts (i) and (iii), we fix a rational prime ℓ such that $\ell > c(A, K)$ and such that ℓ does not divide at least one of α_1, α_2.

Parts (i) and (ii) of Lemma 8 show that the hypotheses about $\mathcal{C}(\ell)^{\alpha_1,\alpha_2}$ needed to apply [**Zy15**, Theorem 2.3, p. 240] are satisfied. Since $\mathrm{Gal}\left(K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}\right) \simeq B(\ell)/U'(\ell)$ is abelian, AHC holds for the extension $K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}$. Then, assuming GRH for the Dedekind zeta function of $K(A[\ell])^{U'(\ell)}$, by applying [**Zy15**, Theorem 2.3, p. 240], we obtain that

$$\begin{aligned}\pi_{\mathcal{C}(\ell)^{\alpha_1,\alpha_2}}(x, K(A[\ell])/K) \ll{}& \frac{\left|\widehat{\mathcal{C}}_{\text{Borel}}(\ell)^{\alpha_1,\alpha_2}\right| \cdot |U'(\ell)|}{|B(\ell)|} \cdot \frac{x}{\log x} \\ &+ \left|\widehat{\mathcal{C}}_{\text{Borel}}(\ell)^{\alpha_1,\alpha_2}\right|^{\frac{1}{2}} [K(A[\ell])^{B(\ell)} : K] \frac{x^{\frac{1}{2}}}{\log x} \log M\left(K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}\right) \\ &+ n_K\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M\left(K(A[\ell])/K\right)\right) \\ &+ n_{K(A[\ell])^{B(\ell)}}\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M\left(K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}\right)\right).\end{aligned}$$

To bound $|U'(\ell)|$ and $|B(\ell)|$, we use Lemma 9. To bound $\left|\widehat{\mathcal{C}}_{\text{Borel}}(\ell)^{\alpha_1,\alpha_2}\right|$, we use Lemma 10. To bound $\log M\left(K(A[\ell])/K\right)$ and $\log M\left(K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}\right)$, we proceed as in parts (i) and (iii) and obtain

$$\log M\left(K(A[\ell])/K\right) \ll \tfrac{\log(\ell N_1 N_2 d_K)}{n_K}, \ \log M\left(K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}\right) \ll \tfrac{\log(\ell N_1 N_2 d_K)}{n_K}.$$

Altogether, we deduce that

$$\pi_{\mathcal{C}(\ell)^{\alpha_1,\alpha_2}}(x, K(A[\ell])/K) \ll \frac{x}{\ell \log x} + \ell^{\frac{5}{2}} \frac{x^{\frac{1}{2}}}{\log x} \cdot \frac{\log(\ell N_1 N_2 d_K)}{n_K}.$$

Now, we use (13) and infer that

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \leq c(\varepsilon)\left(\frac{x}{y(x)\log x} + (y(x)+u(x))^{\frac{5}{2}} \frac{x^{\frac{1}{2}}}{\log x} \cdot \frac{\log((y(x)+u(x))N_1 N_2 d_K)}{n_K}\right).$$

Finally, by invoking [**Lo16**, Lemma 7.1, p. 409] and recalling our constraints on $u(x)$ and $y(x)$, we choose

$$y(x) = \left[a_5 \frac{x^{\frac{1}{7}}}{(\log x)^{\frac{2}{7}}}\right], \quad u(x) = \left[a_6 y(x)^{\frac{1}{2}} (\log y(x))^{2+\varepsilon}\right]$$

for some positive constants $a_5 = a_5(h_A, n_K, d_K, N_1, N_2, \alpha_1, \alpha_2)$ and $a_6 = a_6(h_A, n_K, d_K, N_1, N_2, \alpha_1, \alpha_2)$, which depend on h_A, n_K, d_K, N_1, N_2, α_1, and α_2. We deduce that

$$\mathcal{T}_{E_1,E_2}^{\alpha_1,\alpha_2}(x) \leq \kappa_0'(E_1, E_2, K, \alpha_1, \alpha_2) \frac{x^{\frac{6}{7}}}{(\log x)^{\frac{5}{7}}}$$

for some positive constant $\kappa_0'(E_1, E_2, K, \alpha_1, \alpha_2)$ which depends on E_1, E_2, K, α_1, and α_2. This completes the proof of part (ii) of Theorem 3.

4. Elliptic curves with shared Frobenius fields

Let E_1 and E_2 be elliptic curves over a number field K, without complex multiplication, and not potentially isogenous. We keep the associated notation from the previous sections and prove Theorem 1.

By Lemma 6, for any sufficiently large x, we have

$$\begin{aligned}(14)\qquad &\mathcal{F}_{E_1,E_2}(x) \leq \mathcal{T}^{1,1}_{E_1,E_2}(x) + \mathcal{T}^{1,-1}_{E_1,E_2}(x)\\ &+ \sum_{1\leq j\leq 2} \#\left\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \gcd(\mathrm{N}_K(\mathfrak{p}), 6N_1N_2) = 1, \mathfrak{p} \text{ a degree one prime}, \mathbb{Q}(\pi_{\mathfrak{p}}(E_j)) \in \left\{\mathbb{Q}(i), \mathbb{Q}\left(i\sqrt{3}\right)\right\}\right\}\\ &+ \#\left\{\mathfrak{p} : \mathrm{N}_K(\mathfrak{p}) \leq x, \mathrm{N}_K(\mathfrak{p}) = p^f \text{ for some rational prime } p \text{ and some integer } f \geq 2\right\}.\end{aligned}$$

Note that the last term is bounded from above by $cx^{\frac{1}{2}}$ for some positive constant c as explained in [**Se81**, Proposition 7, p. 138].

(i) For each of the first two terms on the right hand side of inequality (14), we invoke part (i) of Theorem 3 and obtain the combined upper bound $\kappa_0(E_1, E_2, K)\frac{x(\log\log x)^{\frac{1}{9}}}{(\log x)^{\frac{19}{18}}}$ for some positive constant $\kappa_0(E_1, E_2, K)$, which depends on E_1, E_2, and K. For each of the next two terms in the sum over $1 \leq j \leq 2$ on the right hand side of inequality (14), we invoke a modification of [**Zy15**, Theorem 1.3 (ii), p. 236] applied to the elliptic curve E_j defined over K by counting only degree one primes of norm at most x. This modification relies on a variation of [**Zy15**, Lemma 5.1, p. 246] applied to E_j defined over K by counting only degree one primes. We obtain the upper bound $\kappa_1(E_j, K)\frac{x(\log\log x)^2}{(\log x)^2}$ for some positive constant $\kappa_1(E_j, K)$, which depends on E_j and K. Putting everything together gives part (i) of Theorem 1.

(ii) For each of the first two terms on the right hand side of inequality (14), we invoke part (ii) of Theorem 3 and obtain the combined upper bound $2\kappa'_0(E_1, E_2, K)\frac{x^{\frac{6}{7}}}{(\log x)^{\frac{5}{7}}}$ for some positive constant $\kappa'_0(E_1, E_2, K)$, which depends on E_1, E_2, and K. For each of the next two terms in the sum over $1 \leq j \leq 2$, on the right hand side of inequality (14), we invoke a modification of [**Zy15**, Theorem 1.3 (i), p. 236] applied to E_j defined over K by counting only degree one primes, as before. We obtain the upper bound $\kappa'_1(E_j, K)\frac{x^{\frac{4}{5}}}{(\log x)^{\frac{3}{5}}}$ for some positive constant $\kappa'_1(E_j, K)$, which depends on E_j and K. Putting everything together gives part (ii) of Theorem 1.

(iii) For each of the first two terms on the right hand side of inequality (14), we invoke part (iii) of Theorem 3 and obtain the combined upper bound $\kappa''_0(E_1, E_2, K)x^{\frac{2}{3}}(\log x)^{\frac{1}{3}}$ for some positive constant $\kappa''_0(E_1, E_2, K)$, which depends on E_1, E_2, and K. For each of the next two terms in the sum over $1 \leq j \leq 2$ on the right hand side of inequality (14), we invoke two modifications of [**MuMuWo18**, Corollary 1.6, p. 406] applied to E_j defined over K by counting only degree one primes. The first modification is a variation of the proof ingredient [**CoDa08**, Lemma 15, p. 1548]), which we make in order to work with an elliptic curve over K and to count degree one primes of K. The second modification is a variation of the argument in the proof of the second part of [**MuMuWo18**, Corollary 1.6, p. 406], which we make in order to improve the resulting bound $x^{\frac{2}{3}}(\log x)^{\frac{1}{2}}$ to $x^{\frac{2}{3}}(\log x)^{\frac{1}{3}}$, as follows. Letting $\ell(x)$ be as in (6), instead of as in [**MuMuWo18**, p. 422], we deduce that each of the terms on the right hand side of inequality (14) is bounded from above by $\kappa''_1(E_j, K)x^{\frac{2}{3}}(\log x)^{\frac{1}{3}}$ for some positive constant $\kappa''_1(E_j, K)$, which depends on E_j and K. Putting everything together gives part (iii) of Theorem 1.

5. Isogeny criterion for elliptic curves

As an immediate corollary of Theorem 1, we deduce the following isogeny criterion of Kulkarni, Patankar, and Rajan [**KuPaRa16**, Theorem 3, p. 90].

Corollary 12. *Let E_1 and E_2 be two elliptic curves over a number field K. Then E_1 and E_2 are potentially isogenous if and only if $\mathcal{F}_{E_1,E_2}(x)$ has a positive upper density within the set of primes of K.*

Proof. For the"only if" implication, we assume that E_1 and E_2 are potentially isogenous. This implies that E_1 is isogenous over K to a quadratic twist of E_2. Therefore, $|a_{\mathfrak{p}}(E_1)| = |a_{\mathfrak{p}}(E_2)|$ for all but finitely many primes $\mathfrak{p}$ of K. As in the "if" implication of Lemma 6, we have that $\mathbb{Q}(\pi_{\mathfrak{p}}(E_1)) = \mathbb{Q}(\pi_{\mathfrak{p}}(E_2))$ for all but finitely many primes $\mathfrak{p}$ of K. So $\mathcal{F}_{E_1,E_2}(x)$ has density one in the set of primes of K.

For the "if" implication, we prove the contrapositive. Assume that E_1 and E_2 are not potentially isogenous. Then, from part (i) of Theorem 1, we deduce that $\mathcal{F}_{E_1,E_2}(x)$ is bounded from above by a set of density zero in the set of primes of K. □

References

[BaPa18] S. Baier and V.M. Patankar, *Applications of the square sieve to a conjecture of Lang and Trotter for a pair of elliptic curves over the rationals,* Geometry, Algebra, Number Theory, and Information Technology Applications, pp. 39–57, Springer Proc. Math. Stat. 251, Springer, Cham, 2018.

[ChJoSe22] H. Chen, N. Jones, and V. Serban, *The Lang-Trotter conjecture for products of non-CM elliptic curves,* Ramanujan Journal 59, No. 2, 2022, pp. 379–436.

[CoDa08] A.C. Cojocaru and C. David, *Frobenius fields for elliptic curves,* American Journal of Mathematics 130, No. 6, 2008, pp. 1535–1560.

[CoFoMu05] A.C. Cojocaru, Étienne Fouvry, and M.R. Murty, *The square sieve and the Lang-Trotter conjecture,* Canadian Journal of Mathematics Vol. 57, Issue 6, 2005, pp. 1155–1177.

[CoWa22] A.C. Cojocaru and T. Wang, *Bounds for the distribution of the Frobenius traces associated to a generic abelian variety,* preprint 2022, pp. 1–41, available at https://arxiv.org/abs/2207.02913

[CoWa23] A.C. Cojocaru and T. Wang, *Bounds for the distribution of the Frobenius traces associated to products of non-CM elliptic curves,* Canadian Journal of Mathematics Vol. 75, Issue 3, 2023, pp. 687–712.

[Fa83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Inventiones Mathematicae 73, 1983, pp. 349–366.

[Fi22] F. Fité, *On a local-global principle for quadratic twists of abelian varieties,* preprint 2022, available at https://arxiv.org/abs/2108.11555

[FeFi60] W. Feit and N.J. Fine, *Pairs of commuting matrices over a finite field,* Duke Mathematical Journal 27, 1960, pp. 91–94.

[JaSh76] H. Jacquet and J.A. Shalika, *A non-vanishing theorem for zeta functions of GL_n,* Inventiones Mathematicae 38, 1976, No. 1, pp. 1–16.

[Ja16] K. James, *Variants of the Sato-Tate and Lang-Trotter conjectures, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures,* Contemp. Math., 663, Amer. Math. Soc., Providence, RI, 2016, pp. 175–184.

[JaLi01] G. James and M. Liebeck, *Representations and characters of groups,* 2nd edition, Cambridge University Press, New York, 2001.

[KhLa20] C.B. Khare and M. Larsen, *Abelian varieties with isogenous reductions,* Comptes Rendus Mathématique Académie des Sciences Paris 358, No. 9-10, 2020, pp. 1085–1089.

[KuPaRa16] M. Kulkarni, V.M. Patankar, and C.S. Rajan, *Locally potentially equivalent two dimensional Galois representations and Frobenius fields for elliptic curves,* Journal of Number Theory 164, 2016, pp. 87–102.

[LaOd77] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem,* in: A. Fröhlich (Ed.), Algebraic Number Fields, Academic Press, New York, 1977, pp. 409–464.

[LaTr76] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions,* Lecture Notes in Mathematics 504, Springer Verlag, Berlin - New York, 1976.

[Lo16] D. Lombardo, *An explicit open image theorem for products of elliptic curves,* Journal of Number Theory 168, 2016, pp. 386–412.

[LeFNa20] S. Le Fourn and F. Najman, *Torsion of* $\mathbb{Q}$*-curves over quadratic fields,* Mathematical Research Letters 27, No. 1, 2020, pp. 209–225.

[MaWa23] J. Mayle and T. Wang, *An effective open image theorem for products of principally polarized abelian varieties*, preprint 2023, available at https://arxiv.org/abs/2212.11472

[MuMuSa88] M.R. Murty, V.K. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem,* American Journal of Mathematics 110, No. 2, 1988, pp. 253–281.

[MuMuWo18] M.R. Murty, V.K. Murty, and P-J. Wong, *The Chebotarev density theorem and the pair correlation conjecture,* Journal of the Ramanujan Mathematical Society 33, No. 4, 2018, pp. 399–426.

[MuPu17] M.R. Murty and S. Pujahari, *Distinguishing Hecke eigenforms,* Proceedings of the American Mathematical Society 145, No. 5, 2017, pp. 1899–1904.

[MuRa95] M.R. Murty and C.S. Rajan, *Stronger multiplicity one theorems for forms of general type on* GL_2*,* Analytic Number Theory, Vol. 2 (Allerton Park, IL, 1995), pp. 669–683, Progr. Math. 139, Birkhäuser Boston, Boston, MA, 1996.

[Mu85] V.K. Murty, *Explicit formulae for the Lang-Trotter conjecture,* Rocky Mountain Journal of Mathematics 15, No. 2, 1985, pp. 535–551.

[PrRa22] D. Prasad and R. Raghunathan, *Relations between cusp forms sharing Hecke eigenvalues,* Representation Theory 26, 2022, pp. 1063–1079.

[Ra94] D. Ramakrishnan, *A refinement of the strong multiplicity one theorem for GL(2). Appendix to: "l-adic representations associated to modular forms over imaginary quadratic fields. II",* Inventiones Mathematicae 116, No. 1-3, 1994, pp. 645–649.

[Ra00] C.S. Rajan, *Refinement of strong multiplicity one for automorphic representations of GL(n),* Proceedings of the American Mathematical Society 128, 2000, No. 3, pp. 691–700.

[Se81] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev,* Publ. Math. I. H. E. S., No. 54, 1981, pp. 123–201.

[ThZa18] J. Thorner and A. Zaman, *A Chebotarev variant of the Brun-Titchmarsh theorem and bounds for the Lang-Trotter conjectures,* International Mathematics Research Notices IMRN 2018, No. 16, pp. 4991–5027.

[Wa14] N. Walji, *Further refinement of strong multiplicity one for GL(2),* Transactions of the American Mathematical Society 366, 2014, No. 9, pp. 4987–5007.

[Wa23] T. Wang, *Arithmetic properties of abelian varieties,* Ph.D. Thesis, University of Illinois at Chicago, Department of Mathematics, Statistics, and Computer Science, 2023.

[Wo22] P-J. Wong, *Refinements of strong multiplicity one for* GL(2), Mathematical Research Letters 29, No. 2, 2022, pp. 559–598.

[Zy15] D. Zywina, *Bounds for the Lang-Trotter Conjectures,* in *SCHOLAR – a scientific celebration highlighting open lines of arithmetic research,* Contemporary Mathematics 655, American Mathematical Society, Providence, 2015, pp. 235–256.

(Alina Carmen Cojocaru)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA
- Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

Email address, Alina Carmen Cojocaru: `cojocaru@uic.edu`

(Auden Hinz)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 1313 SEO, Chicago, 60607, IL, USA

Email address, Auden Hinz: `audenmh2@uic.edu`

(Tian Wang)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 1222 SEO, Chicago, 60607, IL, USA
- Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany

Email address, Tian Wang: `twang213@uic.edu; twang@mpim-bonn.mpg.de`