PAIRS OF ELLIPTIC CURVES WITH MAXIMAL GALOIS REPRESENTATIONS

NATHAN JONES

Abstract. Using a multidimensional large sieve inequality, we prove that, for almost all pairs (or indeed almost all k-tuples) of elliptic curves, the associated Galois representation on their torsion has maximal image. This generalizes the author's previous work and provides evidence for an affirmative answer to a higher-dimensional analogue of Serre's uniformity question for single elliptic curves. Furthermore, as a consequence of our main theorem, one deduces the triviality of the Brauer group of the Kummer surface attached to almost all pairs of elliptic curves.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. For a fixed positive integer n, let

$$E[n] := \{P \in E(\overline{\mathbb{Q}}) : nP = \mathcal{O}\}$$

denote the n-torsion of E, which is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Moreover, the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$. After fixing a $\mathbb{Z}/n\mathbb{Z}$-basis of $E[n]$, this action gives rise to a Galois representation

$$\varphi_{E,n} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}).$$

Taking the inverse limit over $n \geq 1$ (ordered by divisibility) and choosing $\mathbb{Z}/n\mathbb{Z}$-bases compatibly, one obtains a continuous Galois representation

$$\varphi_E : G_{\mathbb{Q}} \longrightarrow GL_2(\hat{\mathbb{Z}}), \tag{1}$$

where $\hat{\mathbb{Z}} := \lim_n \mathbb{Z}/n\mathbb{Z} \simeq \prod_\ell \mathbb{Z}_\ell$.

How large can $\varphi_E(G_{\mathbb{Q}})$ be? In 1972, Serre [14] proved an open-image theorem for elliptic curves over $\mathbb{Q}$. One formulation of his theorem states that, provided E has no complex multiplication (CM), one has

$$[GL_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] < \infty.$$

Equivalently, Serre's open image theorem states that if E has no CM, then $\varphi_{E,\ell}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > C_E$ for some positive constant C_E depending (at most) on E. Serre also asked [14, p. 299] (see also [15, p. 199]) whether one could take C_E to be independent of the elliptic curve E. In spite of deep partial results providing evidence for an affirmative answer to this uniformity question (e.g. [14], [10], [1]), it remains open (see also [2]). Further evidence for an affirmative answer was obtained by Duke [3], who showed that, for "almost all" elliptic curves E over $\mathbb{Q}$, $\varphi_{E,\ell}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes ℓ.

It is also natural to consider the question of how large the image can be in (1). As Serre pointed out [14, Proposition 22], as a consequence of the Kronecker-Weber theorem, φ_E can never be surjective if E is defined over $\mathbb{Q}$, and in this case one has

$$[GL_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] \geq 2.$$

Following Lang and Trotter, we call E a *Serre curve* if $[GL_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] = 2$, i.e. when $\varphi_E(G_{\mathbb{Q}})$ is as large as possible inside $GL_2(\hat{\mathbb{Z}})$. Inspired by [3], the author has previously shown [6] that almost all elliptic curves are Serre curves.

Similarly to the above, one may consider the Galois representation attached to a *pair* of elliptic curves. Indeed, let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ and let $n \geq 1$ be a positive integer. The action of $G_{\mathbb{Q}}$ on $E_1[n] \times E_2[n]$ gives rise to a Galois representation

$$\varphi_{(E_1,E_2),n} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}) \times GL_2(\mathbb{Z}/n\mathbb{Z}).$$

How large can $\varphi_{(E_1,E_2),n}(G_{\mathbb{Q}})$ be? We have a natural constraint coming from the Weil pairing (see [16]): given an elliptic curve E over $\mathbb{Q}$, an n-th root of unity ζ_n, and an automorphism $\sigma \in G_{\mathbb{Q}}$, the relation

$$\sigma(\zeta_n) = \zeta_n^{\det(\varphi_{E,n}(\sigma))}$$

always holds. Therefore, in our setting,

$$\varphi_{(E_1,E_2),n}(G_{\mathbb{Q}}) \subseteq \Delta_n, \tag{2}$$

where (here and throughout the paper)

$$\Delta_n := \{(g_1, g_2) \in GL_2(\mathbb{Z}/n\mathbb{Z}) \times GL_2(\mathbb{Z}/n\mathbb{Z}) : \det g_1 = \det g_2\}.$$

In [14, Théorème 6, p. 324], Serre already proved the analogous open-image theorem in this context, namely, provided neither E_1 nor E_2 has complex multiplication, and provided E_1 is not $\overline{\mathbb{Q}}$-isogenous to E_2[1], one has $\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) = \Delta_\ell$ for all primes $\ell > C_{E_1,E_2}$ for some positive constant C_{E_1,E_2} depending (at most) on the pair (E_1, E_2). Equivalently, considering the inverse limit

$$\varphi_{(E_1,E_2)} : G_{\mathbb{Q}} \longrightarrow \Delta := \{(g_1, g_2) \in (GL_2(\hat{\mathbb{Z}}))^2; \det g_1 = \det g_2\},$$

one has

$$[\Delta : \varphi_{(E_1,E_2)}(G_{\mathbb{Q}})] < \infty.$$

A conjecture of Mazur (see [12, Remark on p. 6] and the references therein) on congruence primes for modular forms would imply an affirmative answer to the analogue of Serre's uniformity question, that is, that the constant C_{E_1,E_2} above can be chosen independently of the pair (E_1, E_2). Like Serre's uniformity question itself, this is a deep open problem about which little is known.

The purpose of this paper is to prove that, as we vary the pair (E_1, E_2) in a family of elliptic curves, $\varphi_{(E_1,E_2)}(G_{\mathbb{Q}})$ is as large as possible inside Δ, for almost all pairs (E_1, E_2). First, we clarify precisely what this means. Observe that

$$\varphi_{(E_1,E_2)}(G_{\mathbb{Q}}) \subseteq (\varphi_{E_1}(G_{\mathbb{Q}}) \times \varphi_{E_2}(G_{\mathbb{Q}})) \cap \Delta.$$

Since the right-hand side has index at least 4 inside Δ, it is natural to make the following definition.

Definition 1.1. *A pair (E_1, E_2) of elliptic curves over $\mathbb{Q}$ is called a **Serre pair** if*

$$[\Delta : \varphi_{(E_1,E_2)}(G_{\mathbb{Q}})] = 4.$$

In the spirit of [6], we will prove that almost all pairs (E_1, E_2) of elliptic curves over $\mathbb{Q}$ are Serre pairs. This provides some evidence for an affirmative answer to the analogue of Serre's uniformity question for pairs of elliptic curves, since for any Serre pair (E_1, E_2), $\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) = \Delta_\ell$ for all primes ℓ. Additionally, our result has consequences to the study of the Brauer group of Kummer surfaces; indeed, combining Theorem 1.2 below with [17, Example A2], one deduces that, for almost all pairs of elliptic curves (E_1, E_2), the associated Kummer surface $\mathrm{Kum}(E_1 \times E_2)$ has trivial Brauer group.

In order to state our main result, let us introduce the following additional notation. For any elliptic curve E over $\mathbb{Q}$ (i.e. for any $\mathbb{Q}$-isomorphism class of elliptic curves over $\mathbb{Q}$), let $E_{r,s}$ denote the Weierstrass model $y^2 = x^3 + rx + s$. The integers $r, s \in \mathbb{Z}$ may be chosen such that

$$\forall \text{ prime } p, \quad p^{12} \nmid \gcd(r^3, s^2). \tag{3}$$

We then define the height $H(E)$ of E by $H(E) := \max\{|r|^3, |s|^2\}$. For a positive real number T, let

$$\mathcal{B}(T) := \{(E_1, E_2) : \max\{H(E_1), H(E_2)\} \leq T^6\},$$

where (E_1, E_2) denotes a pair of elliptic curves over $\mathbb{Q}$. Since $|\{E : H(E) \leq T^6\}| \asymp T^5$, we have that

$$|\mathcal{B}(T)| \asymp T^{10}.$$

Let us define

$$\mathcal{E}_{\text{non-Serre}}(T) := \{(E_1, E_2) \in \mathcal{B}(T) : (E_1, E_2) \text{ is not a Serre pair}\}.$$

[1] In fact, Serre makes the assumption that E_1 and E_2 have no complex multiplication and that the Galois representations φ_{E_1} and φ_{E_2} do not become isomorphic over a finite extension of $\mathbb{Q}$. Later work of Faltings [4] showed that this condition is equivalent to E_1 and E_2 not being $\overline{\mathbb{Q}}$-isogenous.

The main result of this paper is:

Theorem 1.2. *There is an explicit positive constant β such that, for any $T \geq 2$, we have*

$$|\mathcal{E}_{non\text{-}Serre}(T)| \ll T^9 (\log T)^\beta,$$

with an absolute implied constant. Consequently,

$$\lim_{T\to\infty} \frac{|\{(E_1, E_2) \in \mathcal{B}(T) : (E_1, E_2) \text{ is a Serre pair}\}|}{|\mathcal{B}(T)|} = 1.$$

In other words, "almost all" pairs (E_1, E_2) of elliptic curves have $\varphi_{(E_1,E_2)}(G_{\mathbb{Q}})$ as large as possible.

Theorem 1.2 has the following corollary regarding the corresponding ℓ-adic Galois representation $\varphi_{(E_1,E_2),\ell^\infty}$. The group $G_{\mathbb{Q}}$ acts on $E[\ell^\infty] := \bigcup_{n\geq 1} E[\ell^n]$, giving rise to a continuous group homomorphism

$$\varphi_{(E_1,E_2),\ell^\infty} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_\ell) \times GL_2(\mathbb{Z}_\ell),$$

where $\mathbb{Z}_\ell$ denotes the ring of ℓ-adic integers. As before, one must have

$$\varphi_{(E_1,E_2),\ell^\infty}(G_{\mathbb{Q}}) \subseteq \Delta_{\ell^\infty} := \{(g_1, g_2) \in GL_2(\mathbb{Z}_\ell) \times GL_2(\mathbb{Z}_\ell) : \det g_1 = \det g_2\}.$$

Corollary 1.3. *One has*

$$\lim_{T\to\infty} \frac{\left|\left\{(E_1, E_2) \in \mathcal{B}(T) : \varphi_{(E_1,E_2),\ell^\infty}(G_{\mathbb{Q}}) = \Delta_{\ell^\infty} \text{ for all } \ell\right\}\right|}{|\mathcal{B}(T)|} = 1.$$

As with previous results on this topic ([3], [6]), the bounds of Masser-Wüstholz ([8], [9]), Gallagher's multi-dimensional large sieve [5], and averages of Kronecker class numbers play a crucial role. However, in our present context, new problems arise: firstly, we now need to know that a proper subgroup of G must miss some entire conjugacy classes $\mathcal{C} \subset G$ when $G = \Delta_n$; secondly, we must bound the number of pairs $(E_1, E_2) \in \mathcal{B}(T)$ for which E_1 is $\overline{\mathbb{Q}}$-isogenous to E_2. These are dealt with in Lemmas 3.3 and 3.6 below.

Finally, as we shall point out in Section 4, our methods also prove the analogue of Theorems 1.2 in the context of arbitrary k-tuples $(E_1, \ldots, E_k)$ of elliptic curves over $\mathbb{Q}$ (or even over an arbitrary number field).

Acknowledgments. This note was inspired by a question posed to the author by A. Skorobogatov while visiting the Hausdorff Research Institute in Bonn, Germany. The author would like to thank A. Skorobogatov for his question, and the Hausdorff Institute for a stimulating work environment. He would also like to thank K. Ribet for a helpful discussion, and A.C. Cojocaru for comments on a previous version.

2. Chebotarev error on average

In this section we describe an auxiliary result to Theorem 1.2, which bounds the mean-square error term in the Chebotarev Theorem for division fields of elliptic curves and is of independent interest. Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ of conductors N_1 and N_2, respectively. For a fixed positive integer $n \geq 1$ and a subset $\mathcal{C} \subset \Delta_n$ stable by Δ_n-conjugation, define the counting function $\pi_{(E_1,E_2)}(X; \mathcal{C})$ by

$$\pi_{(E_1,E_2)}(X; \mathcal{C}) := \left|\left\{p \leq X : p \nmid nN_1N_2,\ \varphi_{(E_1,E_2),n}(\mathrm{Frob}_p) \subseteq \mathcal{C}\right\}\right|.$$

(Here and throughout the paper, Frob_p refers to the conjugacy class of a Frobenius automorphism at p in $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$. We note that the condition $p \nmid nN_1N_2$ guarantees that $\varphi_{(E_1,E_2),n}$ is unramified at p.) As usual, for positive integers d and n with $\gcd(d, n) = 1$, denote the counting function for primes in arithmetic progressions by

$$\pi(X; n, d) := |\{p \leq X : p \equiv d \mod n\}|.$$

Furthermore, let us denote the Chebotarev factor attached to $\mathcal{C}$ by

$$\delta_{\mathcal{C}} := \frac{|\mathcal{C}|\varphi(n)}{|\Delta_n|} = \frac{|\mathcal{C}|(\varphi(n))^2}{|GL_2(\mathbb{Z}/n\mathbb{Z})|^2} = \frac{|\mathcal{C}|}{|SL_2(\mathbb{Z}/n\mathbb{Z})|^2},$$

where $\varphi(n)$ is the Euler phi function. The proof of Theorem 1.2 makes use of the following result, which generalizes [3, Theorem 2] to products of elliptic curves. Let us call a subset $\mathcal{C} \subseteq \Delta_n$ *admissible* if it may be written as a union

$$\mathcal{C} = \bigsqcup_{j=1}^{r} \mathcal{A}_j \times \mathcal{B}_j,$$

where $\mathcal{A}_j, \mathcal{B}_j \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$ are subsets which are stable under $GL_2(\mathbb{Z}/n\mathbb{Z})$-conjugation. Notice that any admissible subset $\mathcal{C}$ is necessarily stable under Δ_n-conjugation.

Theorem 2.1. *Fix a positive integer $n \geq 1$ and an admissible subset $\mathcal{C} \subset \Delta_n$ which represents a single determinant value:*

$$\det(\mathcal{C}) = d \in (\mathbb{Z}/n\mathbb{Z})^{\times}. \tag{4}$$

Then, provided $T \geq X$, one has

$$\frac{1}{|\mathcal{B}(T)|} \sum_{(E_1,E_2)\in\mathcal{B}(T)} \big(\pi_{(E_1,E_2)}(X;\mathcal{C}) - \delta_{\mathcal{C}} \cdot \pi(X;n,d)\big)^2 \ll |\mathcal{C}|^2 X,$$

with an absolute implied constant.

2.1. **Proof of Theorem 2.1.** Our proof of Theorem 2.1 follows the same technique as that of Theorem 2 of [3]. It begins with the following multi-dimensional large sieve inequality of Gallagher (see [5, Lemma A]). Fix an integer $k \geq 1$ and, for each prime p, a subset $\Omega(p) \subseteq (\mathbb{Z}/p\mathbb{Z})^k$. For each fixed $m \in \mathbb{Z}^k$ we define

$$P(X;m) := |\{p \leq X : m \mod p \in \Omega(p)\}|$$

and

$$P(X) := \sum_{p\leq X} |\Omega(p)| p^{-k}. \tag{5}$$

Lemma 2.2. *Let B be a box in $\mathbb{R}^k$ whose sides are parallel to the coordinate planes and which has minimum width $W(B)$ and volume $V(B)$. If $W(B) \geq X^2$, then*

$$\frac{1}{V(B)} \sum_{m\in B\cap\mathbb{Z}^k} (P(X;m) - P(X))^2 \ll_k P(X),$$

where the implied constant depends only on k.

To prove Theorem 2.1, we apply Lemma 2.2 with $k = 4$, defining

$$\Omega(p) = \Omega_{\mathcal{C}}(p) := \{(r_1,s_1,r_2,s_2) \in (\mathbb{Z}/p\mathbb{Z})^4 : \prod_{i=1}^{2}(4r_i^3 + 27s_i^2) \neq 0,\ \varphi_{(E_{r_1,s_1},E_{r_2,s_2}),n}(\mathrm{Frob}_p) \subseteq \mathcal{C}\}. \tag{6}$$

Note that, by (4), $\Omega_{\mathcal{C}}(p) = \emptyset$ unless $p \equiv d \mod n$. Furthermore, it follows from the definitions that

$$P(X;m) := |\{p \leq X : m \mod p \in \Omega_{\mathcal{C}}(p)\}| = \pi_{(E_1,E_2)}(X,\mathcal{C}) + O(1). \tag{7}$$

The following lemma restates [6, Theorem 8], and will be used to evaluate $P(X)$ asymptotically as $X \to \infty$.

Lemma 2.3. *Let $\mathcal{A} \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$ be any subset which is stable under $GL_2(\mathbb{Z}/n\mathbb{Z})$-conjugation. Then, for any prime $p \nmid n$, one has*

$$\frac{\big|\big\{(r,s) \in \mathbb{F}_p^2 : -16(4r^3+27s^2) \neq 0,\ \varphi_{E_{r,s},n}(Frob_p) \subseteq \mathcal{A}\big\}\big|}{p^2} = \frac{|\mathcal{A}|}{|SL_2(\mathbb{Z}/n\mathbb{Z})|} + O(|\mathcal{A}|p^{-1/2}).$$

with an absolute implied constant.

Corollary 2.4. *With the definitions (5) and (6), one has*

$$P(X) = \delta_{\mathcal{C}}\pi(X;n,d) + O(\mathcal{C}X^{1/2}),$$

with an absolute implied constant.

Proof of Corollary 2.4. Since $\mathcal{C}$ is admissible and represents only one determinant value, then $\mathcal{C}$ may be decomposed as

$$\mathcal{C} = \bigsqcup_{j=1}^{r} \mathcal{A}_j \times \mathcal{B}_j,$$

where each $\mathcal{A}_j, \mathcal{B}_j \subset GL_2(\mathbb{Z}/n\mathbb{Z})$ is a single $GL_2(\mathbb{Z}/n\mathbb{Z})$-conjugation orbit and $\det(\mathcal{A}_j) = \det(\mathcal{B}_j) = d$ for each j. Further, since $\delta_{\mathcal{C}_1 \sqcup \mathcal{C}_2} = \delta_{\mathcal{C}_1} + \delta_{\mathcal{C}_2}$ and $|\Omega_{\mathcal{C}_1 \sqcup \mathcal{C}_2}(p)| = |\Omega_{\mathcal{C}_1}(p)| + |\Omega_{\mathcal{C}_2}(p)|$, it suffices to consider the case $\mathcal{C} = \mathcal{A} \times \mathcal{B}$. In this case, notice that $\Omega(p) = \Omega_{\mathcal{A}}(p) \times \Omega_{\mathcal{B}}(p)$, where

$$\Omega_{\mathcal{A}}(p) := \{(r_1, s_1) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4r_1^3 + 27s_1^2 \neq 0,\ \varphi_{E_{r,s},n}(\mathrm{Frob}_p) \subseteq \mathcal{A}\},$$
$$\Omega_{\mathcal{B}}(p) := \{(r_2, s_2) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4r_2^3 + 27s_2^2 \neq 0,\ \varphi_{E_{r,s},n}(\mathrm{Frob}_p) \subseteq \mathcal{B}\}.$$

It follows from Lemma 2.3 that

$$\frac{\Omega_{\mathcal{A}}(p)}{p^2} = \frac{|\mathcal{A}|}{|SL_2(\mathbb{Z}/n\mathbb{Z})|} + O(|\mathcal{A}|p^{-1/2}), \qquad \frac{\Omega_{\mathcal{B}}(p)}{p^2} = \frac{|\mathcal{B}|}{|SL_2(\mathbb{Z}/n\mathbb{Z})|} + O(|\mathcal{B}|p^{-1/2}), \tag{8}$$

from which we deduce Corollary 2.4. □

Theorem 2.1 now follows from Lemma 2.2, Corollary 2.4, and (7).

3. Proof of Theorem 1.2

We will now deduce Theorem 1.2 from Theorem 2.1. The following lemma characterizes Serre pairs. In its statement, ε denotes the character

$$\varepsilon : GL_2(\mathbb{Z}/36\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \frac{GL_2(\mathbb{Z}/2\mathbb{Z})}{[GL_2(\mathbb{Z}/2\mathbb{Z}), GL_2(\mathbb{Z}/2\mathbb{Z})]} \simeq \{\pm 1\}.$$

Lemma 3.1. *A pair (E_1, E_2) of elliptic curves over $\mathbb{Q}$ is a Serre pair if and only if the following two conditions hold.*

1. *For each prime $\ell \geq 5$, one has $\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) = \Delta_\ell$.*
2. *One has $\left[\varphi_{(E_1,E_2),36}(G_{\mathbb{Q}}), \varphi_{(E_1,E_2),36}(G_{\mathbb{Q}})\right] = (SL_2(\mathbb{Z}/36\mathbb{Z}) \cap \ker\varepsilon) \times (SL_2(\mathbb{Z}/36\mathbb{Z}) \cap \ker\varepsilon)$.*

Proof. This is [7, Corollary 6.7]. □

In particular, we have

$$(E_1, E_2) \text{ is not a Serre pair } \implies \begin{cases} \varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) \subsetneq \Delta_\ell & \text{for some } \ell \geq 5, \text{ or} \\ \varphi_{(E_2,E_2),36}(G_{\mathbb{Q}}) \subsetneq \Delta_{36}. \end{cases} \tag{9}$$

This implication reduces us to considering $\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}})$ for primes $\ell \geq 5$ and $\varphi_{(E_1,E_2),36}(G_{\mathbb{Q}})$. For any integer $n \geq 1$, let

$$\begin{aligned}
\mathcal{E}_n(T) :=& \left\{(E_1, E_2) \in \mathcal{B}(T) : \varphi_{(E_1,E_2),n}(G_{\mathbb{Q}}) \subsetneq \Delta_n\right\} \\
\mathcal{E}_n^0(T) :=& \{(E_1, E_2) \in \mathcal{E}_n(T) : \varphi_{E_1,n}(G_{\mathbb{Q}}) \subsetneq GL_2(\mathbb{Z}/n\mathbb{Z}) \text{ or } \varphi_{E_2,n}(G_{\mathbb{Q}}) \subsetneq GL_2(\mathbb{Z}/n\mathbb{Z})\}, \\
\mathcal{E}_n^1(T) :=& \{(E_1, E_2) \in \mathcal{E}_n(T) : E_1 \text{ or } E_2 \text{ has complex multiplication}\}, \\
\mathcal{E}_n^2(T) :=& \mathcal{E}_n(T) - (\mathcal{E}_n^0(T) \cup \mathcal{E}_n^1(T)), \\
\mathcal{E}^i(T) :=& \mathcal{E}_{36}^i(T) \cup \bigcup_{\substack{\ell \text{ prime} \\ \ell \geq 5}} \mathcal{E}_\ell^i(T) \qquad (i \in \{0, 1, 2\}).
\end{aligned}$$

(Note that $\mathcal{E}_\ell^1(T) \subseteq \mathcal{E}_\ell^0(T)$ unless $\ell = 2$.) By (9), Theorem 1.2 is implied by

$$|\mathcal{E}^0(T) \cup \mathcal{E}^1(T) \cup \mathcal{E}^2(T)| \ll T^9(\log T)^\beta.$$

It follows from [3] that

$$|\mathcal{E}^0(T)| \ll T^9(\log T)^C \quad \text{and} \quad |\mathcal{E}^1(T)| \ll T^8.$$

Thus, Theorem 1.2 will follow from the estimate

$$|\mathcal{E}^2(T)| \ll T^9(\log T)^\beta. \tag{10}$$

To show this, we will use the following group-theoretic lemmas.

Lemma 3.2. *(Goursat's Lemma) Let G_0 and G_1 be groups and $G \subseteq G_0 \times G_1$ a subgroup satisfying*

$$\pi_i(G) = G_i \qquad (i \in \{0,1\}),$$

where π_i denotes the canonical projection onto the i-th factor. Let $N_i := \pi_i(G \cap \ker \pi_{1-i})$. Then there is an isomorphism of groups $\psi : G_0/N_0 \to G_1/N_1$ (whose graph is induced by G) for which

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi(g_0 N_0) = g_1 N_1\}.$$

Proof. See [13, Lemma (5.2.1)], which shows that the image of G in $G_0/N_0 \times G_1/N_1$ is the graph of an isomorphism ψ. Now note that $N_0 \times N_1 \subseteq G$. □

Lemma 3.3. *Let $n \geq 1$ be any positive integer and $G \subseteq \Delta_n$ be any subgroup satisfying*

$$\pi_1(G) = \pi_2(G) = GL_2(\mathbb{Z}/n\mathbb{Z}),$$

where π_i denotes the canonical projection on the i-th factor. Then either

$$G = \Delta_n,$$

or there exists a non-empty admissible subset $\mathcal{C} \subset \Delta_n$ for which

$$\begin{cases} G \cap \mathcal{C} = \emptyset, & \text{and} \\ \det(\mathcal{C}) = 1. \end{cases} \tag{11}$$

Proof. By Lemma 3.2, there are normal subgroups $N_1, N_2 \trianglelefteq GL_2(\mathbb{Z}/n\mathbb{Z})$ and a group isomorphism $\psi : GL_2(\mathbb{Z}/n\mathbb{Z})/N_1 \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})/N_2$ for which

$$G = \{(g_1, g_2) \in GL_2(\mathbb{Z}/n\mathbb{Z})^2 : \psi(g_1 N_1) = g_2 N_2\}. \tag{12}$$

Notice that

$$|GL_2(\mathbb{Z}/n\mathbb{Z})/N_1| = |GL_2(\mathbb{Z}/n\mathbb{Z})/N_2|. \tag{13}$$

Case 1: $SL_2(\mathbb{Z}/n\mathbb{Z}) \subseteq N_2$.

In this case, the containments

$$N_1 \times SL_2(\mathbb{Z}/n\mathbb{Z}) \subseteq N_1 \times N_2 \subseteq G \subseteq \Delta_n$$

imply that $N_1 \subseteq SL_2(\mathbb{Z}/n\mathbb{Z})$, which by (13) implies that $N_2 = SL_2(\mathbb{Z}/n\mathbb{Z}) = N_1$. It follows that ψ is the identity map, and $G = \Delta_n$ in this case.

Case 2: $SL_2(\mathbb{Z}/n\mathbb{Z}) \nsubseteq N_2$.

Pick any $x \in SL_2(\mathbb{Z}/n\mathbb{Z}) - N_2$ and define

$$\mathcal{C} := \{1\} \times \left\{ gxg^{-1} : g \in GL_2(\mathbb{Z}/n\mathbb{Z}) \right\}.$$

Note that $\mathcal{C} \subseteq \Delta_n$ is admissible, and by (12), $\mathcal{C} \cap G = \emptyset$ in this case. □

Now let $n \in \{36\} \cup \{\ell \geq 5 : \ell \text{ prime}\}$. For each pair $(E_1, E_2) \in \mathcal{E}_n^2(T)$, we have that

$$G = \varphi_{(E_1,E_2),n}(G_{\mathbb{Q}}) \subsetneq \Delta_n$$

satisfies the hypotheses of Lemma 3.3, and so there is a subset $\mathcal{C} = \mathcal{C}(E_1, E_2)$ as in Lemma 3.3 which satisfies (11). Defining

$$\mathcal{E}_{n,\mathcal{C}}^2(T) := \{(E_1, E_2) \in \mathcal{E}_n^2(T) : \varphi_{(E_1,E_2),n}(G_{\mathbb{Q}}) \cap \mathcal{C} = \emptyset\},$$

it follows that $\mathcal{E}_n^2(T) = \bigcup_{\mathcal{C} \subseteq \Delta_n} \mathcal{E}_{n,\mathcal{C}}^2(T)$, where the union is over admissible subsets $\mathcal{C} \subseteq \Delta_n$. We turn to bounding each $\mathcal{E}_{n,\mathcal{C}}^2(T)$. For a fixed admissible set $\mathcal{C}$, we have

$$\sum_{(E_1,E_2) \in \mathcal{E}_{n,\mathcal{C}}^2(T)} \delta_{\mathcal{C}}^2 \pi(X; n, 1)^2 \leq \sum_{(E_1,E_2) \in \mathcal{B}(T)} \left(\pi_{(E_1,E_2)}(X; \mathcal{C}) - \delta_{\mathcal{C}} \cdot \pi(X; n, 1) \right)^2.$$

Let $A > 0$ be fixed. The Siegel-Walfisz Theorem ([18], see also [11]) implies that, uniformly for

$$\ell \leq (\log T)^A, \tag{14}$$

one has

$$\pi(T;\ell,1) \gg_A \frac{T}{\varphi(\ell)\log T}.$$

Thus, putting $X = T$ in Theorem 2.1 and noting that $GL_2(\mathbb{Z}/\ell\mathbb{Z})/\varphi(\ell) \ll \ell^3$, we conclude that

$$|\mathcal{E}^2_{\ell,\mathcal{C}}(T)| \ \ll \ |\mathcal{B}(T)| \cdot \frac{\ell^{12}T}{(\pi(T;\ell,1))^2} \ \ll_A \ \ell^{14}T^9\log^2 T.$$

Summing over the $O(\ell^2)$ many conjugacy classes $\mathcal{C} \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$, we find that

$$|\mathcal{E}^2_\ell(T)| \ \ll_A \ \ell^{16}T^9\log^2 T, \tag{15}$$

provided ℓ satisfies (14). In order to truncate the infinite union over primes ℓ occurring on the left-hand side of (10), we use the following two theorems due to Masser and Wüstholz.

Theorem 3.4. *There are absolute constants c_1 and γ such that, for any pair (E_1, E_2) of non-$\overline{\mathbb{Q}}$-isogenous, non-CM elliptic curves over $\mathbb{Q}$ and any prime $\ell > c_1(\max\{\log H(E_1), \log H(E_2)\})^\gamma$, we have*

$$\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) = \Delta_\ell.$$

Proof. See [9, Proposition 1]. □

Theorem 3.5. *There exists an absolute constant c_2 with the property that, given any elliptic curve E defined over $\mathbb{Q}$ and any other curve E' over $\mathbb{Q}$ which is $\overline{\mathbb{Q}}$-isogenous to E, there exists an isogeny between E and E' of degree at most $c_2\log^4(H(E))$.*

Proof. See [8, p. 1] □

From Theorem 3.5 we may deduce the following Lemma.

Lemma 3.6. *The number of pairs $(E_1, E_2) \in \mathcal{E}^2(T)$ which are $\overline{\mathbb{Q}}$-isogenous to each other is $\ll T^6\log^8 T$.*

Proof of Lemma 3.6. For each fixed E_1 over $\mathbb{Q}$, we consider the set

$$\mathrm{Isog}_{d,E_1}(T) := \{E_2 \in \mathcal{B}_1(T) : \ \exists \text{ a } \overline{\mathbb{Q}}\text{-isogeny } \psi : E_1 \to E_2 \text{ of degree } d\},$$

where $\mathcal{B}_1(T) := \{E \text{ over } \mathbb{Q} : \ H(E) \le T^6\}$. By Theorem 3.5, the set

$$\mathrm{Isog}(T) := \{(E_1, E_2) \in \mathcal{E}^2(T) : E_1 \text{ is } \overline{\mathbb{Q}}\text{-isogenous to } E_2\}$$

satisfies

$$|\mathrm{Isog}(T)| = \sum_{E_1\in\mathcal{B}(T)} \sum_{d=1}^{c_2(\log T)^4} |\mathrm{Isog}_{d,E_1}(T)|.$$

To bound $|\mathrm{Isog}_{d,E_1}(T)|$, note that, if $\psi : E_1 \to E_2$ and $\psi' : E_1 \to E_2'$ are $\overline{\mathbb{Q}}$-isogenies with $\ker\psi = \ker\psi' = G$, then $E_2 \simeq E_1/G \simeq E_2'$, and so E_2 is isomorphic over $\overline{\mathbb{Q}}$ to E_2'. Thus, it is natural to partition $\mathrm{Isog}_{d,E_1}(T)$ according to the associated kernel G. Having fixed a kernel G, it remains to count the elliptic curves E_2 which are $\overline{\mathbb{Q}}$-isomorphic to E_1/G. Now, for a given fixed elliptic curve $E_1/G = E'$ given by $y^2 = x^3 + r'x + s'$ with $r', s' \in \mathbb{Z}\backslash\{0\}$, the elliptic curves E_2 over $\mathbb{Q}$ which are $\overline{\mathbb{Q}}$-isomorphic to E are given by $y^2 = x^3 + rx + s$, with $r = r'd^2$ and $s = s'd^3$ for some $d \in \mathbb{Q}^\times$. By considering such models of E_2 which also satisfy (3), it follows that, provided $j(E') \notin \{0, 1728\}$ there are at most $O(T)$ many elliptic curves $E_2 \in \mathcal{B}(T)$ which are $\overline{\mathbb{Q}}$-isomorphic to E'. Since $\mathcal{E}^2(T)$ excludes elliptic curves with complex multiplication, we see that

$$\begin{aligned}
|\mathrm{Isog}(T)| &\ll \sum_{E_1\in\mathcal{B}(T)} \sum_{d=1}^{c_2\log^4 T} \sum_{\substack{G\subseteq E(\overline{\mathbb{Q}})\\ |G|=d}} T \\
&\ll T^6 \sum_{d=1}^{c_2\log^4 T} \sigma(d) \\
&\ll T^6\log^8 T,
\end{aligned}$$

where we have used that $|\{G \subset (\mathbb{Z}/d\mathbb{Z})^2 : G \text{ an additive subgroup, } |G| = d\}| = \sigma(d) := \sum_{\delta|d} \delta$, and that $\sum_{d \leq X} \sigma(d) \ll X^2$. □

Note that, for T large enough one has $(\log T)^{\gamma+1} \geq c_2(\log T)^{\gamma}$. Thus, taking $A = \gamma + 1$ in (14), Theorem 3.4 and Lemma 3.6 lead us to

$$\left| \mathcal{E}_{36}^2(T) \cup \bigcup_{\ell \text{ prime}} \mathcal{E}_{\ell}^2(T) \right| \ll \left(\sum_{\ell \leq (\log T)^{\gamma+1}} \ell^{16} T^9 \log^2 T \right) + O(T^6 \log^8 T)$$
$$\ll T^9 \log^{\beta} T.$$

We have proved (10), finishing the proof of Theorem 1.2.

4. Concluding remarks

4.1. **Arbitrary finite products of elliptic curves.** Our first remark is that Theorems 1.2 and 2.1 may be generalized without difficulty to the setting of arbitrary k-fold products of elliptic curves, for any $k \geq 2$. Given k elliptic curves $E_1, \ldots, E_k$ over $\mathbb{Q}$ of respective conductors $N_1, \ldots, N_k$, consider the Galois representation

$$\varphi_{(E_1,\ldots,E_k),n} : G_{\mathbb{Q}} \longrightarrow \Delta_n^{(k)} := \{(g_1, g_2, \ldots, g_k) \in (GL_2(\mathbb{Z}/n\mathbb{Z}))^k : \det g_1 = \det g_2 = \cdots = \det g_k\},$$

defined by letting $G_{\mathbb{Q}}$ act on $E_1[n] \times \cdots \times E_k[n]$ and fixing $(\mathbb{Z}/n\mathbb{Z})$-bases, and also the inverse limit

$$\varphi_{(E_1,\ldots,E_k)} : G_{\mathbb{Q}} \longrightarrow \Delta^{(k)} := \{(g_1, g_2, \ldots, g_k) \in (GL_2(\hat{\mathbb{Z}}))^k : \det g_1 = \det g_2 = \cdots = \det g_k\}.$$

In this context, Definition 1.1 becomes

Definition 4.1. *The k-tuple $(E_1, E_2, \ldots, E_k)$ is a **Serre k-tuple** if*

$$[\Delta^{(k)} : \varphi_{(E_1,\ldots,E_k)}(G_{\mathbb{Q}})] = 2^k.$$

Setting the notation

$$\mathcal{B}_{\times k}(T) := \{(E_1, \ldots, E_k) \text{ over } \mathbb{Q} : \max(H(E_1), \ldots H(E_k)) \leq T^6\},$$
$$\mathcal{E}_{\text{non-Serre}}^{(k)}(T) := \{(E_1, \ldots, E_k) \in \mathcal{B}_{\times k}(T) : (E_1, \ldots, E_k) \text{ is not a Serre } k\text{-tuple}\},$$
$$\pi_{(E_1,\ldots,E_k)}(X; \mathcal{C}) := |\{p \leq X : p \nmid n \prod_{i=1}^{k} N_i,\ \varphi_{(E_1,\ldots,E_k),n}(\text{Frob}_p) \subseteq \mathcal{C}\}|,$$
$$\delta_{\mathcal{C}} := \frac{|\mathcal{C}|\varphi(n)}{|\Delta_n^{(k)}|},$$

and calling a subset $\mathcal{C} \subseteq \Delta_n^{(k)}$ *admissible* if it may be written as a union

$$\mathcal{C} = \bigsqcup_{j=1}^{r} \mathcal{A}_j^{(1)} \times \mathcal{A}_j^{(2)} \times \cdots \times \mathcal{A}_j^{(k)},$$

where $\mathcal{A}_j^{(1)}, \mathcal{A}_j^{(2)}, \ldots, \mathcal{A}_j^{(k)} \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$ are subsets which are stable under $GL_2(\mathbb{Z}/n\mathbb{Z})$-conjugation. Note that any admissible subset $\mathcal{C}$ is necessarily closed under $\Delta_n^{(k)}$-conjugation. The proof of Theorem 2.1 generalizes to give the following.

Theorem 4.2. *Fix a positive integer k, a positive integer $n \geq 1$, and an admissible subset $\mathcal{C} \subset \Delta_n^{(k)}$ which represents a single determinant value:*

$$\det(\mathcal{C}) = d \in (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

Then, provided $T \geq X$, one has

$$\frac{1}{|\mathcal{B}_{\times k}(T)|} \sum_{(E_1,\ldots,E_k) \in \mathcal{B}_{\times k}(T)} \left(\pi_{(E_1,\ldots,E_k)}(X; \mathcal{C}) - \delta_{\mathcal{C}} \cdot \pi(X; n, d)\right)^2 \ll_k |\mathcal{C}|^2 X,$$

where the implied constant depends only on k.

Furthermore, since Lemma 3.3 may be readily generalized by induction to the analogous statement for k-fold products, and since Theorems 3.4 and 3.5 are in fact both stated for arbitrary products, our proof of Theorem 1.2 also gives

Theorem 4.3. *There is an explicit positive constant β_k such that, for any $T \geq 2$, we have*

$$\left|\mathcal{E}^{(k)}_{non\text{-}Serre}(T)\right| \ll_k T^{5k-1}\log^{\beta_k} T.$$

Since

$$|\mathcal{B}_{\times k}(T)| \asymp T^{5k},$$

one deduces the same "almost all" statement about k-tuples of elliptic curves.

4.2. **Elliptic curves over an arbitrary number field.** Our second remark is that one may adapt our methods in the style of Zywina [19] to prove the analogous result for k-tuples of elliptic curves defined over an arbitrary number field F. Indeed, fix a number field $F \neq \mathbb{Q}$ and let $\mathcal{O}_F$ denote its ring of integers. Fix a norm $\|\cdot\|$ on $\mathcal{O}_F^{2k} \otimes \mathbb{R} \simeq \mathbb{R}^{2k[F:\mathbb{Q}]}$ and define

$$\mathcal{B}_{F,\times k}(T) := \{(r,s) = (r_i,s_i)_i \in \left(\mathcal{O}_F^2\right)^k : \prod_{i=1}^{k}(4r_i^3+27s_i^2) \neq 0, \| (r,s) \| \leq T\},$$

$$\mathcal{E}^{(k)}_F(T) := \{(r,s) \in \mathcal{B}_{F,\times k}(T) : SL_2(\hat{\mathbb{Z}})^k \nsubseteq \varphi_{(E_{r_1,s_1},E_{r_2,s_2},\ldots,E_{r_k,s_k})}(G_F)\},$$

where $E_{r,s}$ denotes the elliptic curve $y^2 = x^3 + rx + s$, which is defined over F. Note that

$$\mathcal{B}_{F,\times k}(T) \asymp T^{2k[F:\mathbb{Q}]}.$$

In a manner similar to the proof of Theorem 1.2, but employing a version of the large sieve tailored to the number field setting (see [19]), one proves the following theorem.

Theorem 4.4. *There is an explicit positive constant β_k such that, for any $T \geq 2$, we have*

$$\left|\mathcal{E}^{(k)}_F(T)\right| \ll_{k,F,\|\cdot\|} T^{(2k-\frac{1}{2})[F:\mathbb{Q}]}(\log T)^{\beta_k}.$$

References

[1] Y. Bilu and P. Parent, *Serre's uniformity question in the split Cartan case*, Ann. of Math. **173**, no. 1 (2011), 569–584.
[2] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. **77**, no. 1 (1998), 1–38.
[3] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Math. Acad. Sci. Paris Sér. I **325** (1997), 813–818.
[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73**, (1983) 349–366.
[5] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, in Analytic number theory, Proc. Symp. Pure Math., Vol. XXIV (1972), 91–101.
[6] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), 1547–1570.
[7] N. Jones, *GL_2-representations with maximal image*, preprint. Available at the following web address: http://olemiss.edu/working/ncjones/Grepwmaximal.pdf
[8] D. Masser and G. Wüstholz, *Estimating isogenies on elliptic curves*, Invent. math. **100**, (1990), 1–24.
[9] D. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), 247–254.
[10] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44**, no. 2 (1978), 129–162.
[11] H. Montgomery and R. Vaughan, *Multiplicative Number Theory: I. Classical Theory*, Cambridge University Press, CITY, 2006.
[12] M. R. Murty, *Bounds for congruence primes*, in Automorphic Forms, Automorphic Representations and Arithmetic, edited by R. Doran, Ze-Li Dou and G. Gilbert, Proceedings of Symposia in Pure Mathematics, **66**, Part 1, pp. 177–192, Amer. Math. Soc., 1999.
[13] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98**, no. 3 (1976), 751–804.
[14] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., **15** (1972), 259–331.
[15] ———-, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. Inst. Hautes Études Sci. **54** (1981), 123–201.
[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
[17] A. Skorobogatov and Y. Zarhin, *The Brauer group of Kummer surfaces and torsion of elliptic curves*, preprint. Available at the following website: http://arxiv.org/abs/0911.2261
[18] A. Walfisz, *Zur additiven Zahlentheorie II*, Math. Z. **40**, no. 1 (1936) 592–607.

[19] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42**, no. 5 (2010) 811–826.