Pairs of elliptic curves with maximal Galois representations at all primes

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 ℓ-torsion has maximal image, for all primes ℓ. This generalizes a result of W. Duke 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 prime ℓ, let

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

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

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

How large can $\varphi_{E,\ell}(G_{\mathbb{Q}})$ be? In 1972, Serre [12] proved an open-image theorem for elliptic curves over $\mathbb{Q}$. One formulation of his theorem states that, provided E has no complex multiplication, one has $\varphi_{E,\ell}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > C_E$ for some positive constant C_E depending (at most) on E. Serre also asked 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. [12], [9], [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.

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 ℓ be a prime. The action of $G_{\mathbb{Q}}$ on $E_1[\ell]$ and $E_2[\ell]$ gives rise to a Galois representation

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

How large can $\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}})$ be? We have a natural constraint coming from the Weil pairing (see [13]): given an elliptic curve E over $\mathbb{Q}$, an ℓ-th root of unity ζ_ℓ, and an automorphism $\sigma \in G_{\mathbb{Q}}$, the relation

$$\sigma(\zeta_\ell) = \zeta_\ell^{\det(\varphi_{E,\ell}(\sigma))}$$

always holds. Therefore, in our setting,

$$\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) \subseteq \left(GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z})\right)_{\det=\det}, \tag{1}$$

where

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

In [12], 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, one has $\varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) = (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$ 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). A conjecture of Mazur (see [10, 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, (1) is an equality for all primes ℓ for most pairs (E_1, E_2). Similarly to Duke's result, our theorem provides evidence for an affirmative answer to the analogue of Serre's uniformity question for pairs of elliptic curves. Additionally, our result has consequences to the study of the Brauer group of Kummer surfaces; indeed, combining Theorem 1 below with [14, 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 a positive real number T, let

$$\mathcal{B}_{\times 2}(T) := \{(E_1, E_2) : \max\{H(E_1), H(E_2)\} \leq T^6\},$$

where (E_1, E_2) denotes a pair of elliptic curves over $\mathbb{Q}$, and for each elliptic curve E over $\mathbb{Q}$, defined (uniquely) by a Weierstrass model $y^2 = x^3 + rx + s$ with $r, s \in \mathbb{Z}$ such that

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

the height $H(E)$ of E is defined by $H(E) := \max\{|r|^3, |s|^2\}$. Let us recall that

$$|\mathcal{B}_{\times 2}(T)| \asymp T^{10}.$$

For a prime ℓ, let

$$\mathcal{E}_\ell(T) := \left\{(E_1, E_2) \in \mathcal{B}_{\times 2}(T) : \varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) \subsetneq (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}\right\}.$$

The main result of this paper is:

Theorem 1. *There is an explicit positive constant β such that, for any $T \geq 2$, we have*

$$\left| \bigcup_{\ell \text{ prime}} \mathcal{E}_\ell(T) \right| \ll T^9 (\log T)^\beta,$$

with an absolute implied constant. Consequently,

$$\lim_{T\to\infty} \frac{\left| \bigcup_{\ell \text{ prime}} \mathcal{E}_\ell(T) \right|}{|\mathcal{B}_{\times 2}(T)|} = 0.$$

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

As with previous results on this topic ([3], [6]), the bounds of Masser-Wüstholz ([7], [8]), 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 $G = (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$; secondly, we must bound the number of pairs $(E_1, E_2) \in \mathcal{B}_{\times 2}(T)$ for which E_1 is $\overline{\mathbb{Q}}$-isogenous to E_2. These are dealt with in Lemmas 7 and 10 below.

Finally, as we shall point out in Section 4, our methods also prove the analogue of Theorems 1 in the context of arbitrary k-tuples $(E_1, \dots, E_k)$ 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. Cojocaru for comments on a previous version.

2 Bounding Chebotarev error

In this section we describe an auxiliary result to Theorem 1, which bounds the mean-square error term in the Chebotarev Theorem for division fields of elliptic curves and is of independent interest. It is the direct analogue of [3, Theorem 2] in our context. Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ of conductors N_1 and N_2, respectively. For a fixed prime $\ell \geq 2$ and a subset $\mathcal{C} \subset (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$ stable by $(GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$-conjugation, define the counting function $\pi_{(E_1,E_2)}(X;\mathcal{C})$ by

$$\pi_{(E_1,E_2)}(X;\mathcal{C}) := \left|\left\{p \leq X : p \nmid \ell N_1 N_2,\ \varphi_{(E_1,E_2),\ell}(\mathrm{Frob}_p) \subseteq \mathcal{C}\right\}\right|.$$

(Here, Frob_p refers to any choice of Frobenius automorphism at p in $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$.) As usual, for positive integers d and ℓ with $\gcd(d,\ell) = 1$, denote the counting function for primes in arithmetic progressions by

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

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

$$\delta_{\mathcal{C}} := \frac{|\mathcal{C}|\varphi(\ell)}{|(GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}|} = \frac{|\mathcal{C}|(\varphi(\ell))^2}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|^2},$$

where $\varphi(\ell) := |(\mathbb{Z}/\ell\mathbb{Z})^\times| = \ell - 1$ denotes Euler's phi function evaluated at ℓ. The proof of Theorem 1 makes use of the following result, which generalizes Theorem 2 of [3] to products of elliptic curves.

Theorem 2. *Fix a prime $\ell \geq 2$ and a subset $\mathcal{C} \subset (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$ which is closed under conjugation and which represents a single determinant value:*

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

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

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

with an absolute implied constant.

Proof. Our proof of Theorem 2 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

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

Lemma 3. *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.

For an elliptic curve E defined over $\mathbb{F}_p$, recall that the ring $\mathrm{End}_{\mathbb{F}_p}(E)$ is isomorphic to an imaginary quadratic order, whose discriminant we denote by $\Delta(E)$. Further define the integers $a(E)$, $b(E)$ and $\delta(E)$ by

$$a(E) := p + 1 - |E(\mathbb{F}_p)|, \quad b(E) := \left[\mathrm{End}_{\mathbb{F}_p}(E) : \mathbb{Z}\left[\sqrt{a(E)^2 - 4p}\right]\right],$$

and

$$\delta(E) := \begin{cases} 1 & \text{if } \Delta(E) \equiv 1 \mod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Finally, define the matrix $\sigma(E) \in M_{2\times 2}(\mathbb{Z})$ by

$$\sigma(E) = \begin{pmatrix} (a(E) + b(E)\delta(E))/2 & b(E) \\ b(E)(\Delta(E) - \delta(E))/4 & (a(E) - b(E)\delta(E))/2 \end{pmatrix}. \tag{3}$$

Theorem 4. *Let E be an elliptic curve over $\mathbb{Q}$ and $p \neq \ell$ a prime of good reduction for E. Then $\varphi_{E,\ell}$ is unramified at p, and the matrix*

$$\sigma(E \mod p) \mod \ell \in GL_2(\mathbb{Z}/\ell\mathbb{Z})$$

represents the conjugacy class of $\varphi_{E,\ell}(Frob_p)$ in $\varphi_{E,\ell}(G_{\mathbb{Q}}) \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$.

Proof of Theorem 4. This is the main result of [4]. □

To prove Theorem 2, we apply Lemma 3 with $k = 4$, defining

$$\Omega(p) = \Omega_{\mathcal{C}}(p) := \{(r_1, s_1, r_2, s_2) \in (\mathbb{Z}/p\mathbb{Z})^4 : \prod_{i=1}^{2}(4r_i^3 + 27s_i^2) \neq 0,\ (\sigma_1, \sigma_2) \mod \ell \in \mathcal{C}\}$$

if $p \equiv d \mod \ell$ and $\Omega_{\mathcal{C}}(p) = \emptyset$ otherwise. Here, $\sigma_i := \sigma(y^2 = x^3 + r_i x + s_i)$ is as in (3). It follows from Theorem 4 that

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

We now turn to verifying the following lemma.

Lemma 5. *We have*

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

with an absolute constant.

Proof of Lemma 5. We first note that

$$(SL_2(\mathbb{Z}/\ell\mathbb{Z}) \times 1) \cup (1 \times SL_2(\mathbb{Z}/\ell\mathbb{Z})) \subset (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}.$$

It follows that, since $\mathcal{C}$ is closed under $(GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$-conjugation 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 $\mathcal{A}_j, \mathcal{B}_j \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is a single $SL_2(\mathbb{Z}/\ell\mathbb{Z})$-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

$$\Omega_{\mathcal{A}}(p) := \{(r_1, s_1) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4r_1^3 + 27s_1^2 \neq 0,\ \sigma_1 \mod \ell \in \mathcal{A}\},$$
$$\Omega_{\mathcal{B}}(p) := \{(r_2, s_2) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4r_2^3 + 27s_2^2 \neq 0,\ \sigma_2 \mod \ell \in \mathcal{B}\}.$$

It follows[1] from [6, Theorem 8] that

$$\frac{\Omega_{\mathcal{A}}(p)}{p^2} = \frac{|\mathcal{A}|\varphi(\ell)}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|} + O(|\mathcal{A}|p^{-1/2}), \tag{4}$$

from which we deduce Lemma 5. □

Having proved Lemma 5, Theorem 2 now follows from Lemma 3. □

3 Proof of Theorem 1

We will now deduce Theorem 1 from Theorem 2. We first reduce to counting pairs of elliptic curves (E_1, E_2) for which each $\varphi_{E_i,\ell}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$. Let

$$\begin{aligned}
\mathcal{E}_\ell^0(T) :=& \{(E_1, E_2) \in \mathcal{E}_\ell(T) : \varphi_{E_1,\ell}(G_{\mathbb{Q}}) \subsetneq GL_2(\mathbb{Z}/\ell\mathbb{Z}) \text{ or } \varphi_{E_2,\ell}(G_{\mathbb{Q}}) \subsetneq GL_2(\mathbb{Z}/\ell\mathbb{Z})\},\\
\mathcal{E}_\ell^1(T) :=& \{(E_1, E_2) \in \mathcal{E}_\ell(T) : E_1 \text{ or } E_2 \text{ has complex multiplication}\},\\
\mathcal{E}_\ell^2(T) :=& \mathcal{E}_\ell(T) \backslash (\mathcal{E}_\ell^0(T) \cup \mathcal{E}_\ell^1(T)),\\
\mathcal{E}^i(T) :=& \bigcup_\ell \mathcal{E}_\ell^i(T) \qquad (i \in \{0, 1, 2\}).
\end{aligned}$$

Thus, Theorem 1 states that

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

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 will follow from the estimate

$$|\mathcal{E}^2(T)| \ll T^9 (\log T)^\beta. \tag{5}$$

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

Lemma 6. *(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 [11, 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 $N_0 \times N_1 \subseteq G$. □

[1] In fact, the statement of [6, Theorem 8] seems to demand that $\mathcal{A}$ be stable by $GL_2(\mathbb{Z}/\ell\mathbb{Z})$-conjugation, but the proof only uses that $\mathcal{A}$ be stable by $SL_2(\mathbb{Z}/\ell\mathbb{Z})$-conjugation, and so it indeed applies in our case as well.

Lemma 7. *Let ℓ be any prime number and $G \subseteq (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$ be any subgroup satisfying*

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

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

$$G = (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det},$$

or there exists a non-empty subset $\mathcal{C} \subset (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$ which is closed under $(GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$-conjugation and for which

$$\begin{cases} G \cap \mathcal{C} = \emptyset, & \text{and} \\ \det(\mathcal{C}) = 1. \end{cases} \tag{6}$$

Proof. By Lemma 6, there are normal subgroups $N_1, N_2 \trianglelefteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$ and a group isomorphism $\psi : GL_2(\mathbb{Z}/\ell\mathbb{Z})/N_1 \longrightarrow GL_2(\mathbb{Z}/\ell\mathbb{Z})/N_2$ for which

$$G = \{(g_1, g_2) \in GL_2(\mathbb{Z}/\ell\mathbb{Z})^2 : \psi(g_1 N_1) = g_2 N_2\}. \tag{7}$$

Notice that

$$|GL_2(\mathbb{Z}/\ell\mathbb{Z})/N_1| = |GL_2(\mathbb{Z}/\ell\mathbb{Z})/N_2|. \tag{8}$$

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

In this case, the containments

$$N_1 \times SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq N_1 \times N_2 \subseteq G \subseteq (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$$

imply that $N_1 \subseteq SL_2(\mathbb{Z}/\ell\mathbb{Z})$, which by (8) implies that $N_2 = SL_2(\mathbb{Z}/\ell\mathbb{Z}) = N_1$. It follows that ψ is the identity map, and $G = (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$ in this case.

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

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

$$\mathcal{C} := \{1\} \times \left(GL_2(\mathbb{Z}/\ell\mathbb{Z})^{-1} x GL_2(\mathbb{Z}/\ell\mathbb{Z})\right).$$

Note that $\mathcal{C} \subseteq (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$, and by (7), $\mathcal{C} \cap G = \emptyset$ in this case. □

For each pair $(E_1, E_2) \in \mathcal{E}_\ell^2(T)$, we have that

$$G = \varphi_{(E_1,E_2),\ell}(G_{\mathbb{Q}}) \subsetneq (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}$$

satisfies the hypotheses of Lemma 7, and so there is a subset $\mathcal{C} = \mathcal{C}(E_1, E_2)$ as in Lemma 7 which satisfies (6). Defining

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

it follows that $\mathcal{E}_\ell^2(T) = \bigcup_{\mathcal{C} \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})} \mathcal{E}_{\ell,\mathcal{C}}^2(T)$, where the union is over conjugacy classes $\mathcal{C}$ in $GL_2(\mathbb{Z}/\ell\mathbb{Z})$. We turn to bounding each $\mathcal{E}_{\ell,\mathcal{C}}^2(T)$. For a fixed conjugacy class $\mathcal{C}$, we have

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

Putting $X = T$ in Theorem 2 and noting that $GL_2(\mathbb{Z}/\ell\mathbb{Z})/\varphi(\ell) \ll \ell^3$, we conclude that

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

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

$$|\mathcal{E}_\ell^2(T)| \ll \ell^{16} T^9 \log^2 T. \tag{9}$$

In order to truncate the infinite union over primes ℓ occurring on the left-hand side of (5), we use the following two results.

Theorem 8. *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*

$$\varphi_{(E_1,E_2),\ell} = (GL_2(\mathbb{Z}/\ell\mathbb{Z}) \times GL_2(\mathbb{Z}/\ell\mathbb{Z}))_{\det=\det}.$$

Proof. See [8, Proposition 1]. □

Theorem 9. *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 [7, p. 1] □

From Theorem 9 we may deduce the following Lemma.

Lemma 10. *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 10. For each fixed E_1 over $\mathbb{Q}$, we consider the set

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

where $\mathcal{B}(T) := \{E \text{ over } \mathbb{Q} : H(E) \le T^6\}$. By Theorem 9, 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 (2), 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 $\sum_{d \leq X} \sigma(d) \ll X^2$. □

Theorem 8 and Lemma 10, together with (9), imply that

$$\begin{aligned} |\bigcup_{\ell \text{ prime}} \mathcal{E}_\ell^2(T)| &\ll \left(\sum_{\ell \leq c_1 (6 \log T)^\gamma} \ell^{16} T^9 \log^2 T \right) + O(T^6 \log^8 T) \\ &\ll T^9 \log^\beta T. \end{aligned}$$

We have proved (5), finishing the proof of Theorem 1.

4 Concluding remarks

4.1 Arbitrary finite products of elliptic curves

Our first remark is that Theorems 1 and 2 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

$$\varphi_{(E_1,\ldots,E_k),\ell} : G_{\mathbb{Q}} \longrightarrow (GL_2(\mathbb{Z}/\ell\mathbb{Z}))^k$$

defined by letting $G_{\mathbb{Q}}$ act on $E_1[\ell] \times \cdots \times E_k[\ell]$ and fixing $GL_2(\mathbb{Z}/\ell\mathbb{Z})$-bases. Define the notation

$$\begin{aligned} GL_2(\mathbb{Z}/\ell\mathbb{Z})_\Delta^{(k)} :=& \{(g_1, g_2, \ldots, g_k) \in (GL_2(\mathbb{Z}/\ell\mathbb{Z}))^k : \det g_1 = \det g_2 = \cdots = \det g_k\}, \\ \mathcal{B}_{\times k}(T) :=& (\mathcal{B}(T))^k = \{(E_1, \ldots, E_k) \text{ over } \mathbb{Q} : \max(H(E_1), \ldots H(E_k)) \leq T^6\}, \\ \mathcal{E}_\ell^{(k)}(T) :=& \{(E_1, \ldots, E_k) \in \mathcal{B}_{\times k}(T) : \varphi_{(E_1,\ldots,E_k),\ell}(G_{\mathbb{Q}}) \subsetneq GL_2(\mathbb{Z}/\ell\mathbb{Z})_\Delta^{(k)}\}, \\ \pi_{(E_1,\ldots,E_k)}(X; \mathcal{C}) :=& |\{p \leq X : \ p \nmid \ell \prod_{i=1}^k N_i, \ \varphi_{(E_1,\ldots,E_k),\ell}(\mathrm{Frob}_p) \subseteq \mathcal{C}\}|, \\ \delta_{\mathcal{C}} :=& \frac{|\mathcal{C}|\varphi(\ell)}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})_\Delta^{(k)}|}. \end{aligned}$$

One may prove the following theorem.

Theorem 11. *Fix a positive integer k, a prime $\ell \geq 2$, and a subset $\mathcal{C} \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})_\Delta^{(k)}$ which is closed under conjugation and which represents a single determinant value:*

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

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

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

where the implied constant depends only on k.

Furthermore, since Lemma 7 may be readily generalized by induction to the analogous statement for k-fold products, and since Theorems 8 and 9 are in fact both stated for arbitrary products, our proof of Theorem 1 also gives

Theorem 12. *There is an explicit positive constant β_k such that, for any $T \geq 2$, we have*

$$\left| \bigcup_{\ell \ prime} \mathcal{E}_\ell^{(k)}(T) \right| \ll_k T^{5k-1} \log^{\beta_k} T.$$

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 [15] to prove the same result for k-tuples of elliptic curves defined over an arbitrary number field F. Indeed, fix a number field F and let $\mathcal{O}_F$ denote its ring of integers. Fix a norm $\| \cdot \|$ on $\mathcal{O}_F^2 \otimes \mathbb{R} \simeq \mathbb{R}^{2[F:\mathbb{Q}]}$ and define

$$\begin{aligned} \mathcal{B}_{F,\times k}(T) :=& \{(r,s) \in \mathcal{O}_F^2 : -16(4r^3+27b^2) \neq 0, \| (r,s) \| \leq T\}, \\ \mathcal{E}_{F,\ell}^{(k)}(T) :=& \{(r,s) \in \mathcal{B}_{F,\times k}(T) : SL_2(\mathbb{Z}/\ell\mathbb{Z})^{(k)} \nsubseteq \varphi_{E_{r,s},\ell}(G_F)\}, \end{aligned}$$

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

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

In a manner similar to the proof of Theorem 1, but employing a version of the large sieve tailored to the number field setting (see [15]), one proves the following theorem.

Theorem 13. *There is an explicit positive constant β such that, for any $T \geq 2$, we have*

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

References

[1] Y. Bilu and P. Parent, *Serre's uniformity question in the split Cartan case*, to appear in the Annals of Mathematics. Available at the following website: http://arxiv.org/abs/0807.4954

[2] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. 3, 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] W. Duke and A. Toth, *The splitting of primes in division fields of elliptic curves*, Experiment. Math. **11** (2003), 555–565..

[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] D. Masser and G. Wüstholz, *Estimating isogenies on elliptic curves*, Invent. math. **100**, (1990), 1–24.

[8] D. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), 247–254.

[9] B. Mazur, *Rational isogenies of prime degree*, Invent. Math., 44, no. 2 (1978), 129–162.

[10] 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, Vol. 66, Part 1, pp. 177–192, Amer. Math. Soc., 1999.

[11] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98**, no. 3 (1976), 751–804.

[12] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., **15** (1972), 259–331.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[14] 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

[15] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, preprint. Available at the following website: http://www.math.upenn.edu/∼zywina/papers/MaximalGalois.pdf