The Lang–Trotter conjecture for products of non-CM elliptic curves

Hao Chen \(^1\) · Nathan Jones \(^2\) · Vlad Serban \(^3\)

Received: 3 September 2020 / Accepted: 23 November 2021 / Published online: 21 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Inspired by the work of Lang–Trotter on the densities of primes with fixed Frobenius traces for elliptic curves defined over \(\mathbb{Q}\) and by the subsequent generalization of Cojocaru–Davis–Silverberg–Stange to generic abelian varieties, we study the analogous question for abelian surfaces isogenous to products of non-CM elliptic curves over \(\mathbb{Q}\) that are not \(\overline{\mathbb{Q}}\)-isogenous. We formulate the corresponding conjectural asymptotic, provide upper bounds, and explicitly compute (when the elliptic curves lie outside a thin set) the arithmetically significant constants appearing in the asymptotic. This allows us to provide computational evidence for the conjecture.

Keywords
Elliptic curves · Abelian surfaces · Galois representations

Mathematics Subject Classification
11G05 · 11F80 · 11G10

1 Introduction
Let \(E/\mathbb{Q}\) be an elliptic curve and let \(p\) denote any prime of good reduction of \(E\). The coefficients \(a_p(E)\), which for such primes may be defined as the trace of a choice of absolute Frobenius \(\text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\) acting on the Tate module \(T_\ell(E)\) of \(E\) for \(\ell \neq p\), are of central importance in understanding the arithmetic of elliptic curves and related questions. For instance, these integers determine the size of the group over finite fields since \(|E(\mathbb{F}_p)| = 1 + p - a_p(E)|\), and via modularity \(a_p(E)|\) also equals

The third author’s research was partially funded by START-prize Y-966 of the Austrian Science Fund (FWF) under P.I. Harald Grobner.

\(^\circ\) Nathan Jones
ncjones@uic.edu

\(^1\) Microsoft Research, Redmond, WA 98052, USA
\(^2\) University of Illinois at Chicago, Chicago, IL 60607, USA
\(^3\) École Polytechnique Fédérale de Lausanne, Lausanne, VD, Switzerland
the \( p \)-th Fourier coefficient of the weight 2 newform \( f_E \) attached to \( E \). They are well-known to satisfy the Hasse bound \( |a_p(E)| \leq 2\sqrt{p} \), and several finer questions about their distribution have been considered. We focus here on a classical conjecture of Lang and Trotter [20] which examines the density of primes whose Frobenius trace \( a_p(E) \in \mathbb{Z} \) is equal to a fixed integer. When \( E \) does not have complex multiplication, for any trace \( t \in \mathbb{Z} \) they conjecture the asymptotic

\[
\pi_{E,t}(x) := \left| \{ p \leq x : p \nmid N_E \text{ and } a_p(E) = t \} \right| \sim C(E, t) \cdot \frac{\sqrt{x}}{\log x},
\]

where \( C(E, t) \) is an explicit constant depending on the compatible system of Galois representations attached to \( E \) and where \( N_E \) denotes the conductor of \( E \). When \( E \) has complex multiplication and \( t \neq 0 \) one similarly conjectures an asymptotic

\[
\pi_{E,t}(x) \sim C'(E, t) \cdot \frac{\sqrt{x}}{\log x},
\]

whereas supersingular primes, for which \( a_p(E) = 0 \), can be seen to occur half of the time. Despite some results in its direction, the Lang–Trotter conjecture remains open.

More generally, it is natural to study densities of primes with fixed Frobenius trace for higher dimensional motives and compatible systems of \( \ell \)-adic Galois representations. Considering principally polarized abelian varieties \( A/\mathbb{Q} \) of dimension \( g \) (abelian \( g \)-folds), the action of the Galois group on torsion points gives rise to Galois representations

\[
\rho_A : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GSp}_{2g}(\hat{\mathbb{Z}}),
\]

\[
\rho_{A,m} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_{\ell | m} \text{GSp}_{2g}(\mathbb{Z}/\ell),
\]

\[
\bar{\rho}_{A,m} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}),
\]

for any positive integer \( m \). The analogue to Lang and Trotter’s conjecture for those abelian varieties where \( \text{Im}(\rho_A) \subset \text{GSp}_{2g}(\hat{\mathbb{Z}}) \) is open, which we shall call \textit{generic}, was recently formulated and studied in [5]. In our paper, we shift the focus to non-generic abelian varieties and abelian surfaces in particular. With the goal of better understanding the distribution of Frobenius traces in the non-generic case, we examine abelian surfaces that are \( \mathbb{Q} \)-isogenous to a product of elliptic curves defined over \( \mathbb{Q} \) and without complex multiplication.

Let us first give a more precise formulation of the existing conjectures. For a prime \( p \) of good reduction of \( A \), denote more generally \( a_p(A) = \text{tr}(\rho_{A,\ell}(\text{Frob}_p)) \in \mathbb{Z} \) (well-defined for \( \ell \neq p \)). The conjectures study for a fixed trace \( T \) the asymptotics of

\[
\pi_{A,T}(x) := \left| \{ p \leq x : p \nmid N_A \text{ and } a_p(A) = T \} \right|,
\]

where \( N_A \) denotes the conductor of \( A \). The traces \( a_p(A) \) are a sum of \( 2g \) Weil numbers of modulus \( \sqrt{p} \) and thus \( |a_p(A)| \leq 2g \sqrt{p} \). The distribution of the normalized traces \( a_p(A)/\sqrt{p} \) is then governed by a compact real Lie group \( K \subset U(2g) \) known as the Sato-Tate group of \( A \), which is determined by the \( \ell \)-adic Galois representations \( \rho_{A,\ell} \).
attached to $A$. The Haar measure on $K$ gives rise to a distribution $\Phi_K : [-2g, 2g] \to \mathbb{R}$ for the trace on conjugacy classes of $K$. The equidistribution assumption then states:

**Conjecture 1.0.1** (Sato–Tate, Serre) Let $A/\mathbb{Q}$ be a generic abelian $g$-fold. Then $\frac{a_p(A)}{\sqrt{p}}$ is equidistributed in $[-2g, 2g]$ with respect to $\Phi_{USp(2g)}$.

Its content is one of the main statements of the Sato-Tate conjecture and is therefore known for elliptic curves over $\mathbb{Q}$, but for $g \geq 2$ is not known in general. Here and throughout the paper, for any positive integer $m$, any integer $T$ and any algebraic subgroup $G \subseteq GSp_{2g}$, we use the notation

$$G(m) := G(\mathbb{Z}/m\mathbb{Z}),$$

$$G(m, T) := \{ g \in G(m) : \text{tr} \; g \equiv T \mod m \},$$

$$H_A := \text{Im}(\rho_A) \subseteq GSp_{2g}(\hat{\mathbb{Z)}),$$

$$H_A(m) := \text{Im}(\bar{\rho}_{A,m}) \subseteq GSp_{2g}(\mathbb{Z}/m\mathbb{Z}),$$

$$H_A(m, T) := \{ h \in H_A(m) : \text{tr} \; h \equiv T \mod m \}.$$

Also, provided $H_A = \text{Im}(\rho_A)$ is an open subgroup of $G(\hat{\mathbb{Z}}) \subseteq GSp_{2g}(\hat{\mathbb{Z}})$, we let $m_A$ denote the conductor of $H_A$, i.e. the least positive integer $m$ such that in the commutative diagram

$$\begin{array}{ccc}
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_A} & G(\hat{\mathbb{Z}}) \\
& \downarrow{\rho_{A,m}} & \downarrow{\text{red}} \\
& G(m) & \end{array}
$$

we have $H_A := \text{Im}(\rho_A) = \text{red}^{-1}(H_A(m))$, and we abbreviate for nonzero trace $T$

$$m_{A,T} := m_A \prod_{\ell|m_A} \ell^{v_{\ell}(T)}. \tag{1.4}$$

We state the existing conjectures, when $\text{Im}(\rho_A) \subseteq G(\hat{\mathbb{Z}})$ is open for $G = GSp_{2g}$, uniformly for $T \neq 0$:

**Conjecture 1.0.2** (Lang–Trotter ($g = 1$), Cojocaru–Davis–Silverberg–Stange ($g \geq 2$)) Let $A/\mathbb{Q}$ be a generic abelian $g$-fold. Assume the equidistribution stated in Conjecture 1.0.1 holds for $A$. Then for $T \neq 0$ we have

$$\pi_{A,T}(x) \sim C(A, T) \cdot \frac{\sqrt{x}}{\log x},$$

where the constant $C(A, T) \geq 0$ is given by

$$C(A, T) = 2\Phi_{USp(2g)}(0) \cdot \frac{m_{A,T}|H_A(m_{A,T}, T)|}{|H_A(m_{A,T})|} \cdot \prod_{\ell|m_A} \ell^{v_{\ell}(T)+1} \cdot \frac{|GSp_{2g}(\ell^{v_{\ell}(T)+1}, T)|}{|GSp_{2g}(\ell^{v_{\ell}(T)+1})|}.$$
Conjecture 1.0.2 contains Lang and Trotter’s original conjecture [20] for $t \neq 0$ when $A$ is an elliptic curve without complex multiplication and therefore is generic by a well-known result of Serre [25], whereas in the higher dimensional case Conjecture 1.0.2 is due to [5] for nonzero trace.

Consider now abelian surfaces $\mathbb{Q}$-isogenous to products of non-CM elliptic curves $E_1 \times E_2$ defined over $\mathbb{Q}$ and note that

$$
\pi_{E_1 \times E_2, T}(x) = \left\{ p \leq x : p \nmid N_{E_1}, p \nmid N_{E_2}, \text{ and } a_p(E_1) + a_p(E_2) = T \right\}.
$$

**Remark 1.0.3** Since all but finitely many Frobenius traces $a_p(A)$ are invariant under $\mathbb{Q}$-isogeny, when $A \sim \mathbb{Q} E_1 \times E_2$ we have that $\pi_{A, T}(x) = \pi_{E_1 \times E_2, T}(x) + O(1)$. Hence for our purposes we may, and by and large in this paper do, just work with products of elliptic curves.

We also assume $E_1$ and $E_2$ are non-isogenous over $\mathbb{Q}$, so that denoting

$$
G := \text{GL}_2 \times \text{det} \text{GL}_2 = \{(g_1, g_2) \in \text{GL}_2 \times \text{GL}_2 : \det(g_1) = \det(g_2)\},
$$

the Galois image subgroup $\text{Im}(\rho_{E_1 \times E_2})$ is an open subgroup of $G(\hat{\mathbb{Z}})$ by [25, Th. 6]. Fixing an embedding $G \hookrightarrow \text{GSp}_4$, we may view $H_{E_1 \times E_2} := \text{Im}(\rho_{E_1 \times E_2}) \subseteq G(\hat{\mathbb{Z}}) \subseteq \text{GSp}_4(\hat{\mathbb{Z}})$ and use the notations in (1.2). An explicit embedding $G \hookrightarrow \text{GSp}_4$ is for instance given by

$$
\begin{pmatrix}
(a & b \\
(c & d)
\end{pmatrix} \cdot
\begin{pmatrix}
(a' & b' \\
(c' & d')
\end{pmatrix}
\mapsto
\begin{pmatrix}
a & 0 & b & 0 \\
0 & a' & 0 & b' \\
c & 0 & d & 0 \\
0 & c' & 0 & d'
\end{pmatrix}.
$$

In particular, this defines via (1.3) a conductor $m_{E_1 \times E_2}$ of the open subgroup $H_{E_1 \times E_2} \subseteq G(\hat{\mathbb{Z}})$.

Furthermore, in this setting the equidistribution result for the normalized traces of Frobenius with respect to the Sato-Tate measure is known (see e.g., [14, Th. 5.4]).

**Proposition 1.0.4** Let $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$ be non-CM and non-isogenous over $\overline{\mathbb{Q}}$. Then

$$
\frac{a_p(E_1 \times E_2)}{\sqrt{p}}
$$

is equidistributed with respect to $\Phi_{\text{SU}(2) \times 2} = \Phi_{\text{SU}(2)} \ast \Phi_{\text{SU}(2)}$ in $[-4, 4]$.

We adapt Lang and Trotter’s heuristic to this situation in Sect. 2 of this paper, proving convergence of the constant appearing in the asymptotic. This leads to the analogous conjecture:

**Conjecture 1.0.5** Let $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$ be non-CM elliptic curves that are not $\overline{\mathbb{Q}}$-isogenous. Let $A \sim \mathbb{Q} E_1 \times E_2$ be an abelian surface isogenous over $\mathbb{Q}$ to their product and let $T \in \mathbb{Z}$, $T \neq 0$. Then

$$
\pi_{A, T}(x) \sim C(E_1 \times E_2, T) \cdot \frac{\sqrt{x}}{\log x}.
$$

(1.6)
as \( x \to \infty \), where the constant \( C(E_1 \times E_2, T) \geq 0 \) is given by

\[
C(E_1 \times E_2, T) = 2\Phi_{SU(2)^2}(0) \cdot \frac{m_{E_1 \times E_2, T} |H_{E_1 \times E_2(m_{E_1 \times E_2, T}, T)}|}{|H_{E_1 \times E_2(m_{E_1 \times E_2, T})}|} \cdot \prod_{\ell \mid m_{E_1 \times E_2}} \frac{\ell^{v_\ell(T)+1} |G(\ell^{v_\ell(T)+1}, T)|}{|G(\ell^{v_\ell(T)+1})|},
\]

where \( G = GL_2 \times_{det} GL_2 \) and notations are as in (1.2), and where \( m_{E_1 \times E_2, T} \) are defined as in (1.3) and (1.4), respectively. In case \( C(E_1 \times E_2, T) = 0 \) we take the asymptotic 1.6 to mean that there are only finitely many primes \( p \) with \( \alpha_p(A) = T \).

The Sato–Tate factor appearing above is explicitly given by

\[
2\Phi_{SU(2)^2}(0) = 2 \int_{-2}^{2} \left( \frac{\sqrt{4 - t^2}}{2\pi} \right)^2 dt = \frac{16}{3\pi^2}.
\]

Furthermore, we are able in this setting to compute explicit formulas for the factors involved in the constant \( C(E_1 \times E_2, T) \) in the case where \( \text{Im}(\rho_{E_1 \times E_2}) \) and hence \( \text{Im}(\rho_A) \) are as large as possible. More precisely, the pair of elliptic curves \((E_1, E_2)\) is called a Serre pair if \( [G(\hat{\mathbb{Z}}) : \text{Im}(\rho_{E_1 \times E_2})] = 4 \), noting we always have \( [G(\hat{\mathbb{Z}}) : \text{Im}(\rho_{E_1 \times E_2})] \geq 4 \) (see, e.g., [17] or Sect. 4). For primes not dividing the conductor of the open subgroup \( \text{Im}(\rho_{E_1 \times E_2}) \subseteq G(\hat{\mathbb{Z}}) \) (universal primes), the explicit evaluation of the local factor is done in Sect. 3 and is valid for any pair \((E_1, E_2)\) of non-CM elliptic curves which are not \( \overline{Q}\)-isogenous. Section 4 then deals with the more delicate remaining factor, and the formulas are only valid when \((E_1, E_2)\) is a Serre pair. We summarize our results here:

**Theorem 1.0.6**  Let \( E_{1/\mathbb{Q}}, E_{2/\mathbb{Q}} \) be non-CM elliptic curves that are not \( \overline{Q}\)-isogenous. Then in the notations of Conjecture 1.0.5, for \( T \neq 0 \) we obtain:

(1) The factors away from \( m_{E_1 \times E_2} \) are given by

\[
\frac{\ell^{v_\ell(T)+1} |G(\ell^{v_\ell(T)+1}, T)|}{|G(\ell^{v_\ell(T)+1})|} = \begin{cases} 
\frac{\ell(\ell^4 - \ell^3 - 2\ell^2 + \ell + 2)}{(\ell^2 - 1)^2(\ell - 1)^2} + 2E(\ell, T) + \delta_2(\ell T) (\ell^4 - \ell) & \text{if } \ell \nmid m_{E_1 \times E_2} \cdot T, \\
\frac{\ell^6 - \ell^4 - 3\ell^2 + \ell}{\ell^8 - 2\ell^4 + \ell^2} & \text{if } \ell \mid m_{E_1 \times E_2}, \ell \mid |T|.
\end{cases}
\]

with notations for \( e_\ell(T), E(\ell, T), \delta_2(\ell T) \) specified below.
Moreover, if \((E_1, E_2)\) is a Serre pair, we compute the factor at the conductor \(m_{E_1 \times E_2}\) of the open subgroup \(\text{Im} \, \rho_{E_1 \times E_2} \subseteq G(\hat{\mathbb{Z}})\). Let

\[
D_i = \begin{cases} 
|\Delta_i| & \text{if } \Delta_i \equiv 1 \mod 4, \\
4|\Delta_i| & \text{otherwise,}
\end{cases}
\]

where \(\Delta_i\) denotes the square-free part of the discriminant of the curve \(E_i\). Then \(m_{E_1 \times E_2} = \text{lcm}(2, D_1, D_2)\). Abbreviating \(m = m_{E_1 \times E_2, T} = m_{E_1 \times E_2} \prod_{\ell | m_{E_1 \times E_2}} \ell^{v_{\ell}(T)}\) and writing \(D'_1\) and \(m'\) for the odd parts of these quantities, when \(|D'_1| \neq |D'_2|\) the factor \(\frac{m| \text{Im} \, E_{E_1 \times E_2}(m, T)}{|\text{Im} \, E_{E_1 \times E_2}(m)|}\) equals:

\[
\frac{m \cdot (m')^2 \varphi(m')}{(\text{rad}(m'))^2 |G(m)|} \left( \mathcal{G}_{\psi_2}(T) \prod_{\ell | m'} (A_{\ell}(T) + 1) + 2^s \left( \frac{m'}{|D'_1|} \right) \mathcal{G}^{(1)}_{\psi_2}(T) \prod_{\ell | D'_1} B_{\ell}(T) \right)
\]

with \(|G(m)| = \prod_{\ell | m} \ell^{7v_{\ell}(m) - 5} (\ell^2 - 1)^2 (\ell - 1)\). We obtain a similar formula when \(|D'_1| = |D'_2|\) (see Proposition 4.1.1).

Throughout these results we have used the following notations:

\[
e_{\ell}(T) := \left[ (v_{\ell}(T) - 1)/2 \right], \quad \delta_n(m) := \left\{ \begin{array}{ll} 1 & \text{if } n \text{ divides } m, \\
0 & \text{otherwise}, \end{array} \right.
\]

\[
E(\ell, T) := \frac{\ell^3(\ell + 1)(\ell^4e_{\ell}(T)+4) - 1}{(\ell^2 + 1)(\ell + 1)},
\]

\[
A_{\ell}(T) := \begin{cases} 
\ell^5 - \ell^3 - 3\ell^2 + 1 + \frac{2E(\ell, T)}{e_{\ell}(T)+1} + \delta_2(\ell, T) \frac{(\ell^3-1)}{e_{\ell}(T)+2} & \text{if } \ell \mid T, \\
(\ell^6 - \ell^5 - 2\ell^4 + \ell^3 + 2\ell^2)/((\ell - 1)) & \text{if } \ell \nmid T,
\end{cases}
\]

\[
B_{\ell}(T) := \begin{cases} 
-3\ell^2 + 1 + \frac{2E(\ell, T)}{e_{\ell}(T)+3} + \delta_2(\ell, T) \frac{(\ell^3-1)}{e_{\ell}(T)+2} & \text{if } \ell \mid T, \\
\ell^2/((\ell - 1)) & \text{if } \ell \nmid T,
\end{cases}
\]

\[
\mathcal{G}_{\psi_2}(T) := \left| G \left( 2v_2(m), T \right) \right|_{\text{Im} \, \psi_2 \subseteq \text{Im} \, \psi'},
\]

\[
\mathcal{G}^{(i)}_{\psi_2}(T) := \left| G \left( 2^{v_2(m)}, T \right) \right|_{\psi_{\psi_2}^{(i)} = 1 \text{ Im} \, \psi_2 \subseteq \text{Im} \, \psi'} - \left| G \left( 2^{v_2(m)}, T \right) \right|_{\psi_{\psi_2}^{(i)} = -1 \text{ Im} \, \psi_2 \subseteq \text{Im} \, \psi'},
\]

where in the last two expressions, the subscripts and superscripts denote the subset of \(G \left( 2^{v_2(m)}, T \right)\) cut out by the given conditions, where \(\psi^{(i)}(g) := \varepsilon(g \mod 2) \left( \frac{D_i}{\det g} \right)\), with \(\left( \frac{D_i}{\det g} \right)\) denoting the Kronecker symbol and \(\varepsilon\) denoting the non-trivial character of order two on \(\text{GL}_2(\mathbb{Z}/2\mathbb{Z})\), and a subscript \(n\) indicates restriction to the \(n\)-primary
part of the domain, i.e. \( \psi_m^{(i)}(g) := \left( \frac{\det g}{|D|} \right) \) and \( \psi_2^{(i)}(g) := \psi^{(i)}(g)\psi_m^{(i)}(g) \) (these pairs of functions define group homomorphisms \( \psi_2, \psi_m : \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \times \text{GL}_2(\mathbb{Z}/m'\mathbb{Z}) \rightarrow \{\pm1\}^2 \) via \( \psi_2 \left( ((g^{(1)}), g^{(2)})) :\right. \) \( = \left( \psi_2^{(1)}(g^{(1)}), \psi_2^{(2)}(g^{(2)}) \right) \) and \( \psi_m' \left( ((g^{(1)}), g^{(2)})) :\right. \) \( = \left( \psi_m'^{(1)}(g^{(1)}), \psi_m'^{(2)}(g^{(2)}) \right) \)). See Sect. 4 for details.

It has been shown by the second author [16,17] that almost all elliptic curves and pairs of curves (ordered by height) over \( \mathbb{Q} \) are Serre curves or Serre pairs, respectively, so that the restriction on computing the exceptional factor in Theorem 1.0.6 is reasonable. In general, this factor is quite intricate to compute and it would likely be hard to produce any kind of formula that works in much greater generality.

Several remarks concerning Conjecture 1.0.5 and Theorem 1.0.6 are in order:

Remarks

(i) Given a Serre pair \((E_1, E_2)\), one can compute the quantities \( \mathcal{S}_{\psi_2}(T) \) and \( \mathcal{S}_{\psi_2}^{(i)}(T) \) using formulas found in Sect. 4, specifically, Lemmas 4.1.3 and 4.1.4, together with (1.23). Thus, Theorem 1.0.6 may be used to explicitly compute numerical values for the constants \( C(E_1 \times E_2, T) \) when \((E_1, E_2)\) is a Serre pair.

(ii) One can similarly formulate a conjecture for arbitrary products of non-CM, pairwise non-isogenous elliptic curves \( E_1 \times \cdots \times E_k \). It is known that the analogous open image theorem holds for such products; see [23, Theorem 3.5].

(iii) When two curves are \( \mathbb{Q} \)-isogenous, then for all primes \( p \nmid N_{E_1}N_{E_2} \) we have \( a_p(E_1) = a_p(E_2) \) and the distribution is then already predicted by Lang and Trotter’s original conjecture.

(iv) For trace \( T = 0 \), we similarly expect a constant \( C(E_1 \times E_2, 0) \) such that

\[
\pi_{A,0}(x) \sim C(E_1 \times E_2, 0) \cdot \sqrt{x} / \log(x),
\]

but we have not computed \( C(E_1 \times E_2, 0) \) explicitly. In this case, the situation is complicated, for instance, by the fact that factors at primes \( \ell \nmid m_{E_1} \times E_2 \) as computed in Theorem 1.0.6 are now all related to volumes of singular \( \ell \)-adic manifolds (see Sect. 2.2 below for more details). So although the heuristic still yields an expression for \( C(E_1 \times E_2, 0) \) as a limit (see Proposition 2.2.1), establishing its convergence and evaluating the limit would require a different approach.

(v) One may also formulate a conjecture when \( E_1, E_2 \), or both curves have complex multiplication after taking into account the correct Sato-Tate measure. For CM elliptic curves, Lang and Trotter still predict that for \( T \neq 0 \) there is a constant \( C'(E, T) \) such that \( \pi_{E,T}(x) \sim C'(E, T) \cdot \sqrt{x} / \log(x) \). On the other hand, when \( T = 0 \), Deuring [11] showed that half of the primes have supersingular reduction, i.e. that

\[
\pi_{E,0}(x) \sim 1/2 \cdot x / \log(x)
\]

for \( E \) with complex multiplication. This reflects the fact that the Sato-Tate measure has a discrete part of mass 1/2 at zero. When, say, both \( E_1 \) and \( E_2 \) are
CM and non-isogenous, we thus arrive at at least 1/4 of primes having trace $T = 0$ and the heuristic for general traces has to be adapted according to the Sato-Tate group (e.g., when both curves have CM the Sato-Tate group is $F_{a,b}$ in the notations of [12] with connected component $U(1) \times U(1)$).

(vi) It can indeed occur that $C(E_1 \times E_2, T) = 0$ for some $T$ because $\text{Im}(\rho_{E_1 \times E_2, m}) \subset G(m)$ is small enough not to contain any pairs of matrices with traces summing to $T$. For example, if $E_1$ and $E_2$ both have rational 2-torsion (implying that 2 divides $m_{E_1 \times E_2}$), then at all odd primes $p \nmid N_{E_1}N_{E_2}$ this forces $a_p(E_1) \equiv a_p(E_2) \equiv 0$ mod 2, and the constant $C(E_1 \times E_2, T) = 0$ vanishes for $T$ odd. For more details and related results and examples, including pairs $(E_1, E_2)$ for which the original Lang–Trotter constants $C(E_1, T)$ and $C(E_2, T)$ are non-zero for all $T$ but nevertheless $C(E_1 \times E_2, T) = 0$ for some $T$, see Sect. 2.3 below. The fact that this arithmetic information is captured by the exceptional factor in Conjecture 1.0.5 should indicate that it is difficult to compute it in general. Still, for Serre pairs, our results show the constant $C(E_1 \times E_2, T)$ never vanishes for nonzero trace (see Sect. 2.3).

Compared to the study of the Lang–Trotter Conjecture for a single elliptic curve over $\mathbb{Q}$, there are various additional complications that arise. For instance, one has to reckon with possible entanglements of the division fields of $E_1$ and $E_2$ when the Galois extension $\mathbb{Q}(\zeta_m)$ is strictly contained in $\mathbb{Q}(E_1[m]) \cap \mathbb{Q}(E_2[m])$. This increases the index $[G(\mathbb{Z}) : \text{Im}(\rho_{E_1 \times E_2})]$ which, as Remark 1.(v) already indicates, can lead to additional congruence obstructions which prevent the realization of some $T \in \mathbb{Z}$ as Frobenius traces. See Sect. 2.3 and Proposition 4.0.2 for some results illustrating this phenomenon. It is therefore also not surprising that the computation of the exceptional factor of the constant becomes even more onerous when considering the product $E_1 \times E_2$. Furthermore, it is harder to compute the factors $\lim_{n \to \infty} \ell^n |G(\ell^n, T)|/[G(\ell^n)]$ of the Lang–Trotter constant, which do not immediately stabilize for primes $\ell | T$. See for instance the difficulties appearing in Akbary and Parks’ [1] work where they study for $E_1 \times E_2$ the density of primes with both Frobenius traces fixed [1, Conjecture 1.2.].

With the formulas of Theorem 1.0.6 in hand, we are then able in Sect. 5 to provide and discuss computational evidence for Conjecture 1.0.5. The computations were performed using the MAGMA computational algebra system [4] as well as the SageMath mathematics software system [29] and can be reproduced with either software using the results of this paper. As hoped, we find a strong correlation between the predicted and actual counts of primes with fixed Frobenius trace, providing the first such evidence for higher-dimensional abelian varieties in the non-generic case. Moreover, as predicted, the counts are sensitive to the prime factorization of the trace and to the arithmetic of the abelian surface, lending further credibility to the intricate constant $C(E_1 \times E_2)$ appearing in the asymptotic. Extensive computations are more accessible here than in the setting of Akbary and Parks [1, Remark 1.3.(iv)] or in the setting of generic abelian varieties of dimension $\geq 2$ of [5], so this paper focuses primarily on explicit calculations. However, just as for elliptic curves, one can establish non-trivial upper bounds for $\pi_{A, T}(x)$ and we expect that one can prove along the lines of [10] that Conjecture 1.0.5 holds on average. Toward that end, we present an upper bound in Theorem 2.4.1 and relegate the rest to future work.
Similar densities for general compatible systems of Galois representations were studied in [21] and for primes where the Frobenius fields of two elliptic curves coincide in [2]. See also [18] for a discussion of the Lang–Trotter conjecture for elliptic curves and for results over function fields. Returning to abelian surfaces, there is now a complete classification of the Sato-Tate groups [12] and we hope that the study of the distribution of Frobenius traces for non-generic abelian surfaces can be completed in the future. Indeed, this was our initial motivation, but already the case of products of elliptic curves provided enough substance to warrant this paper.

2 The Lang–Trotter heuristic

In this section we adapt Lang and Trotter’s original heuristic in [20] to the situation of products of non-$\mathbb{Q}$-isogenous elliptic curves defined over $\mathbb{Q}$ without complex multiplication. We follow Lang and Trotter’s original reasoning as well as the formulation for generic abelian varieties in [5]. We normalize the continuous part of the Sato-Tate density function $\Phi : [-2g, 2g] \to \mathbb{R}$ so that $\Phi$ is of total mass one. In general, if the Sato-Tate measure were to have a discontinuous part (e.g., for CM elliptic curves one has $\mu_{\text{disc}} = \frac{1}{2} \delta_0$) the heuristic would need to be adapted (in particular, for $T \neq 0$, the value $\Phi(0)$ would need to be replaced by the appropriate limiting value at zero).

2.1 The probabilistic model

Fix integers $m \geq 1$ and $T \in \mathbb{Z}$ and recall the notations for the group $G(m) := GL_2(\mathbb{Z}/m\mathbb{Z}) \times det GL_2(\mathbb{Z}/m\mathbb{Z})$, the subgroup $H_A(m)$ and the subset $H_A(m, T)$ in (1.2). In what follows, we take $A = E_1 \times E_2$ for simplicity and typically drop the subscript for brevity, writing $H(m)$ and $H(m, T)$ when $A = E_1 \times E_2$ is implicit. The ratio

$$F_m(T) = \frac{m|H(m, T)|}{|H(m)|}$$

is $m$ times the probability that $\vec{\rho}_{A, m}(\text{Frob}_p)$ has trace $T$ modulo $m$, obtained by applying the Čebotarev density theorem to the division field generated by the $m$-torsion (we may ignore primes $p \mid m$ which ramify). The additional factor $m$ ensures that $F_m(T)$ has average value 1 over the congruence classes of $T$ modulo $m$. We also define the probability weights $\mu_{p, m}(T)$ by

$$\mu_{p, m}(T) := \begin{cases} c_{p, m} \Phi \left( \frac{T}{\sqrt{p}} \right) F_m(T) & \text{if } |T| \leq 2g \sqrt{p}, \\ 0 & \text{if } |T| > 2g \sqrt{p}, \end{cases} \quad (1.1)$$

where $c_{p, m}$ is the unique constant chosen so that
\[
\sum_{T \in \mathbb{Z}} \mu_{p,m}(T) = 1,
\]

namely
\[
c_{p,m} := \frac{1}{\sum_{|T| \leq 2g \sqrt{p}} \Phi \left( \frac{T}{\sqrt{p}} \right) F_m(T)}.
\]

The main probabilistic assumption, as found in [20], is that the function \( T \mapsto \mu_{p,m}(T) \) models the probability of the event \( \{ a_p(A) = T \} \), taking into account the Sato-Tate distribution and taking into account the Čebotarev density theorem for only the \( m \)-th division field; in particular, it assumes that these two are statistically independent from one another. We presently show that this model is in fact consistent with these two equidistribution results.

**Lemma 2.1.1** Fix integers \( T_0 \) and \( m \geq 1 \), and let \( I \subseteq [-2g, 2g] \) be any interval. We have
\[
\lim_{p \to \infty} \frac{m}{\sqrt{p}} \sum_{\substack{T \equiv T_0 \ (m) \ \text{mod} \ m \ \text{with} \ |T| \leq 2g \sqrt{p}}} \Phi \left( \frac{T}{\sqrt{p}} \right) = \int_I \Phi(s) \, ds.
\]

**Proof** When \( p \) is much larger than \( m \), this approaches a Riemann sum computing \( \int_I \Phi(s) \, ds \) by splitting the interval \( I \) into pieces of length \( m/\sqrt{p} \).
\[\Box\]

Taking \( I = [-2g, 2g] \), we obtain the following corollary.

**Corollary 2.1.2** For any \( m \geq 1 \) and \( T_0 \in \mathbb{Z} \) we have
\[
\lim_{p \to \infty} \frac{m}{\sqrt{p}} \sum_{\substack{T \equiv T_0 \ (m) \ \text{mod} \ m \ \text{with} \ |T| \leq 2g \sqrt{p}}} \Phi \left( \frac{T}{\sqrt{p}} \right) = 1.
\]

**Corollary 2.1.3** For all \( m \geq 1 \) we have
\[
\lim_{p \to \infty} \sqrt{p} \cdot c_{p,m} = 1.
\]

**Proof** This is [5, Lemma 21], mutatis mutandis. We include the details here for completeness. By choice of \( c_{p,m} \), and noting that the factor \( F_m(T) \) only depends on \( T \) modulo \( m \), we have
The Lang–Trotter conjecture for products of non-CM elliptic... 389

\[ 1 = \sum_{T \in \mathbb{Z}} \mu_{p,m}(T) = c_{p,m} \sum_{T \in \mathbb{Z}} \Phi \left( \frac{T}{\sqrt{p}} \right) F_m(T) \]

\[ = \sqrt{p} \cdot c_{p,m} \sum_{T_0 \in \mathbb{Z}/m\mathbb{Z}} \frac{1}{m} F_m(T_0) \cdot \frac{m}{\sqrt{p}} \sum_{T \equiv T_0 (m)} \Phi \left( \frac{T}{\sqrt{p}} \right). \]

Thus, using Corollary 2.1.2, we have

\[ \lim_{p \to \infty} \frac{1}{\sqrt{p}} \cdot c_{p,m} = \sum_{T_0 \in \mathbb{Z}/m\mathbb{Z}} \frac{1}{m} F_m(T_0) \lim_{p \to \infty} \frac{m}{\sqrt{p}} \sum_{T \equiv T_0 (m)} \Phi \left( \frac{T}{\sqrt{p}} \right) = 1, \]

proving the corollary. \( \square \)

**Corollary 2.1.4** The choice of model (1.1) agrees with the Čebotarev density theorem and the Sato-Tate equidistribution law as \( p \to \infty \).

**Proof** By (1.1) together with Corollaries 2.1.2 and 2.1.3, we find that

\[ \lim_{p \to \infty} \mu_{p,m} \left( \{ T \in \mathbb{Z} : T \equiv T_0 (m) \} \right) = \lim_{p \to \infty} \sum_{T \in \mathbb{Z}} c_{p,m} \Phi \left( \frac{T}{\sqrt{p}} \right) F_m(T_0) \]

\[ = \frac{1}{m} F_m(T_0) \lim_{p \to \infty} \sqrt{p} \cdot c_{p,m} \]

\[ \cdot \frac{m}{\sqrt{p}} \sum_{T \in \mathbb{Z}} \Phi \left( \frac{T}{\sqrt{p}} \right) \]

\[ = \frac{1}{m} F_m(T_0). \]

By the law of large numbers, we recover that the density of primes with Frobenius trace \( T_0 \) modulo \( m \) is asymptotically \( \frac{1}{m} F_m(T_0) \), in accordance with the Čebotarev density theorem. Similarly, for any interval \( I \subseteq [-2g, 2g] \), by Lemma 2.1.1 and Corollary 2.1.3 we have

\[ \lim_{p \to \infty} \mu_{p,m} \left( \left\{ \frac{a_p(A)}{\sqrt{p}} \in I \right\} \right) = \lim_{p \to \infty} \sqrt{p} \cdot c_{p,m} \sum_{T_0 \in \mathbb{Z}/m\mathbb{Z}} \frac{1}{m} F_m(T_0) \]

\[ \cdot \frac{m}{\sqrt{p}} \sum_{T \equiv T_0 (m)} \Phi \left( \frac{T}{\sqrt{p}} \right) \]

\[ = \int_I \Phi(s)ds. \]
Again the law of large numbers gives
\[
\lim_{x \to \infty} \frac{|\{p \leq x : \frac{a_p(A)}{\sqrt{p}} \in I\}|}{\pi(x)} = \int_I \Phi(s)ds,
\]
which by our choice of \(\Phi\) agrees with the Sato-Tate equidistribution. \qed

We have seen that the measure \(\mu_{p,m}\) on \(\mathbb{Z}\) models the probability of the event that \(a_p(A)\) takes on a fixed value \(T\), i.e.

\[
\text{Prob}\{a_p(A) = T\} \approx \mu_{p,m}(T),
\]

and that this model agrees with the Sato-Tate equidistribution law and with the Če­botarev density theorem for only the \(m\)-th division field of \(A\). It is natural to desire a limiting measure \(\mu_p\) on \(\mathbb{Z}\) modeling the probability of the event \(\{a_p(A) = T\}\) which agrees with Sato-Tate equidistribution as well as with the Če­botarev density theorem for all of the division fields of \(A\) simultaneously. This is (heuristically) achieved by taking the point-wise limit as \(m\) approaches infinity via any sequence of positive integers that is co-final with respect to divisibility. We denote this limit by \(\mu_p(T) := \lim_{m \to \infty} \mu_{p,m}(T)\); for the sake of concreteness, we may take

\[
\mu_p(T) := \lim_{m \to \infty} \mu_{p,m}(T) = \lim_{n \to \infty} \mu_{p,m_n}(T) = \left( m_n := \prod_{\ell \leq n} \ell^n \right).
\]

In Sect. 2.2, we establish the above pointwise convergence of the measures \(\mu_{p,m}\) by computing the limit

\[
F(t) := \lim_{m \to \infty} F_m(T) = \lim_{n \to \infty} F_{m_n}(T),
\]

which gives rise to the limiting probability measure

\[
\mu_p(T) = c_p \Phi \left( \frac{T}{\sqrt{p}} \right) F(T),
\]

where

\[
c_p = \lim_{m \to \infty} c_{p,m} = \frac{1}{\sum_{|T| \leq 2g\sqrt{p}} \Phi \left( \frac{T}{\sqrt{p}} \right) F(T)}.
\]

Note that, using Corollary 2.1.3 and interchanging limits, we obtain

\[
c_p \sim \frac{1}{\sqrt{p}} \quad \text{as} \quad p \to \infty. \quad (1.2)
\]
Assuming that the above-mentioned limit interchange is justified and that \( \mu_p(T) \) models \( \text{Prob}\{a_p(A) = T\} \), we arrive at Conjecture 1.0.5 by writing

\[
|\{p \leq x : \ p \nmid N_A, a_p(A) = T\}| \approx \sum_{p \leq x} \mu_p(T)
= \sum_{p \leq x} c_p \Phi \left( \frac{T}{\sqrt{p}} \right) F(T)
\sim F(T) \sum_{p \leq x} \frac{1}{\sqrt{p}} \cdot \Phi \left( \frac{T}{\sqrt{p}} \right),
\]

the last asymptotic as \( x \to \infty \) being justified by (1.2) and by our next lemma, which implies that the sum on the right-hand side approaches infinity with \( x \).

**Lemma 2.1.5** We have the asymptotic

\[
\sum_{p \leq x} \frac{1}{\sqrt{p}} \cdot \Phi \left( \frac{T}{\sqrt{p}} \right) \sim 2 \Phi(0) \cdot \frac{\sqrt{x}}{\log x},
\]
as \( x \to \infty \).

**Proof** First, observe that

\[
\sum_{p \leq x} \Phi \left( \frac{T}{\sqrt{p}} \right) \frac{1}{\sqrt{p}} = \sum_{p \leq x} \Phi(0) \frac{1}{\sqrt{p}} + \sum_{p \leq x} \left( \Phi \left( \frac{T}{\sqrt{p}} \right) - \Phi(0) \right) \frac{1}{\sqrt{p}}.
\]

Fix \( \varepsilon > 0 \). By continuity of \( \Phi \) at 0, there is a \( \delta > 0 \) for which

\[
\left| \frac{T}{\sqrt{p}} - 0 \right| < \delta \implies \left| \Phi \left( \frac{T}{\sqrt{p}} \right) - \Phi(0) \right| < \varepsilon.
\]

We divide the second sum on the right-hand side of (1.4), obtaining the bound

\[
\left| \sum_{\frac{T^2}{\delta^2} \leq p \leq x} \left( \Phi \left( \frac{T}{\sqrt{p}} \right) - \Phi(0) \right) \frac{1}{\sqrt{p}} \right|
\leq C_{\delta,T} + 2 \varepsilon \cdot \sum_{p \leq x} \frac{1}{2 \sqrt{p}}.
\]

Finally, by partial summation, we have the asymptotic \( \sum_{p \leq x} \frac{1}{2 \sqrt{p}} \sim \frac{\sqrt{x}}{\log x} \). Inserting this into (1.4), we find that

\[
\sum_{p \leq x} \Phi \left( \frac{T}{\sqrt{p}} \right) \cdot \frac{1}{\sqrt{p}} = 2 \Phi(0) \cdot \frac{\sqrt{x}}{\log x} + O \left( \varepsilon \cdot \frac{\sqrt{x}}{\log x} \right),
\]
with an absolute implied constant. Since $\varepsilon > 0$ was arbitrary, this establishes the lemma.

Combining Lemma 2.1.5 with (1.3), we arrive at Conjecture 1.0.5 in the form

$$\left|\left\{ p \leq x : \ p \nmid N_A, a_p(A) = T\right\}\right| \sim 2\Phi(0) \cdot F(T) \cdot \frac{\sqrt{x}}{\log x} \quad (x \to \infty).$$

Finally, it remains to show that $F(T) = \lim_{m \to \infty} F_m(T)$ converges, which is the subject of the next subsection.

Remark 2.1.6 In fact, the above heuristics lead to the conjecture that, for fixed $T \in \mathbb{Z} - \{0\}$, we have

$$\pi_{E_1 \times E_2, T}(x) \sim \frac{C(E_1 \times E_2, T)}{2\Phi(0)} \int_{\max\{2,(T/2g)^2\}}^{x} \Phi\left(\frac{T}{\sqrt{t}}\right) \frac{1}{2\sqrt{t} \log t} dt$$

as $x \to \infty$. For numerical computations, this integral expression is more accurate when $T$ is on the scale of $\sqrt{x}$.

2.2 Convergence of the constant

We consider the limit that yields the constant in the heuristic and prove it converges and is well-defined for any trace $T \neq 0$. We first show the following:

Proposition 2.2.1 Fix $T \neq 0$ an integer. One has the following product expansion, where $m_A$ denotes the conductor of the image of the Galois representation on torsion of $A = E_1 \times E_2$, where $H(m) = \text{Im}(\rho_{A,m})$ and where $H(m, T)$ denotes the trace $T$ elements in $H(m)$:

$$F(T) := \lim_{m \to \infty} \frac{m |H(m, T)|}{|H(m)|} = \frac{m_{A,T} |H(m_{A,T}, T)|}{|H(m_{A,T})|} \prod_{\ell | m_A} \frac{\ell^{v_\ell(T)+1} |H(\ell^{v_\ell(T)+1}, T)|}{|H(\ell^{v_\ell(T)+1})|}.$$  

We note that this shows not only that the limit splits into factors over each prime, but also that at each prime $\ell$ the factors eventually stabilize when increasing the powers $d \in \mathbb{N}$ such that $\ell^d | m$. This is a non-trivial feature of this setup, see for instance the failure thereof when considering products of elliptic curves where each individual trace is fixed in [1]. The reader may consult, e.g., Theorem 1.5., Proposition 1.8. and Conjecture 1.9. of [1] for the difficulties encountered.

In our setting, at primes $\ell \nmid T$, the stabilization is connected to the smoothness of the $\ell$-adic analytic manifold $X_T(\mathbb{Z}_\ell)$, where $X_T$ denotes the subvariety of $GL_2 \times_{\det GL_2}$ whose traces sum to $T$. Indeed, smoothness of $X_T(\mathbb{Z}_\ell)$ implies that

$$|X_T(\mathbb{Z}/\ell^n\mathbb{Z})| = V(X_T(\mathbb{Z}_\ell)) \cdot \ell^{6n}$$

for a constant $V(X_T(\mathbb{Z}_\ell))$ which computes the volume of the manifold $X_T(\mathbb{Z}_\ell)$, as proven by Serre in [26, Théorème 9]. The factors at each prime are just a rational
multiple of this volume. A computation of the Jacobian matrix of the defining equations of $X_T$ shows the following:

**Lemma 2.2.2** The $\ell$-adic analytic manifold $X_T(\mathbb{Z}_\ell)$ is smooth if and only if the prime $\ell$ does not divide the trace $T$.

Nevertheless, a result of Oesterlé [22, Théorème 2] shows that the limit $\lim_{n \to \infty} \ell^{-6n} \cdot |X_T(\mathbb{Z}/\ell^n \mathbb{Z})|$ still converges to the volume $V(X_T(\mathbb{Z}_\ell))$. Proposition 2.2.1 shows that, in addition to that, at primes $\ell \nmid m_A$ the factors stabilize at exponent $n = v_\ell(T) + 1$. The computation of those stable factors will then be treated in Sect. 3.

We turn to the proof of Proposition 2.2.1, proceeding as in [5, Lemma 12]:

**Lemma 2.2.3** If $(m, m_A) = 1$ or $m_A | m$, then for any prime $\ell$ dividing $m$ we have

$$|H(m \ell v_\ell(T) + 1, S)| = |H(m \ell v_\ell(T) + 1, T)|$$

for any integer $S \equiv T \mod m \ell v_\ell(T)$.

**Proof** Assume $S \equiv T \mod m \ell v_\ell(T)$. Since the $\ell$-adic valuation $v_\ell(m) > 0$ is strictly positive it follows that $v_\ell(T) = v_\ell(S)$. We may write $T = T_0 \ell v_\ell(T)$ and $S = S_0 \ell v_\ell(T)$ for integers $T_0, S_0$. Moreover, writing $m = m_0 \ell v_\ell(m)$ there exists by the Chinese remainder theorem $u \in \mathbb{Z}$ such that

$$u \equiv T_0^{-1} S_0 \mod \ell v_\ell(m) + 1 \quad \text{and} \quad u \equiv 1 \mod m_0.$$  \hfill (1.5)

It follows from this and from the hypothesis $S \equiv T \mod m \ell v_\ell(T)$ that

$$uT \equiv S \mod \ell v_\ell(m) + v_\ell(T) + 1,$$

$$uT \equiv S \mod m_0.$$  \hfill (1.6)

Furthermore, by (1.5) we have $u \equiv 1 \mod m$, and thus the pair $U := u I_2 \times u I_2$ of integer matrices is congruent modulo $m$ to $I_1 \times I_2$, and it therefore lies in $H(m)$. By definition of $m_A$, it follows that $U \mod m \ell v_\ell(T) + 1$ belongs to $H(m \ell v_\ell(T) + 1)$, and therefore left multiplication by $U$ defines a bijection from $H(m \ell v_\ell(T) + 1)$ onto itself which, by (1.6), restricts to a bijection between the sets $H(m \ell v_\ell(T) + 1, T)$ and $H(m \ell v_\ell(T) + 1, S)$, as desired. \hfill $\Box$

**Lemma 2.2.4** If $(m, m_A) = 1$ or $m_A | m$, then for any prime $\ell$ dividing $m$ and $k \geq 1$ we have

$$\frac{m \ell v_\ell(T) + k |H(m \ell v_\ell(T) + k, T)|}{|H(m \ell v_\ell(T) + k)|} \cdot \frac{|H(m \ell v_\ell(T), T)|}{|H(m \ell v_\ell(T))|}.$$ 

**Proof** It suffices to establish the case $k = 1$ (we can then make the replacement $m \mapsto \ell m$ and repeat the argument). Considering the projection map

$$\pi : H(m \ell v_\ell(T) + 1) \to H(m \ell v_\ell(T)),$$
we note that, by the assumptions on \( m \), we have \( H(m^{\ell v(T)+1}) = \pi^{-1}(H(m^{\ell v(T)})) \). Thus, on the one hand we see that
\[
|H(m^{\ell v(T)+1})| = |\ker \pi| \cdot |H(m^{\ell v(T)})|.
\]
On the other hand, using Lemma 2.2.3 to show that the counts for all \( \ell \) lifts of \( T \) from \( \mathbb{Z}/m^{\ell v(T)}\mathbb{Z} \) to \( \mathbb{Z}/m^{\ell v(T)+1}\mathbb{Z} \) are the same, we obtain
\[
|H(m^{\ell v(T)+1}, T)| \cdot \ell = |\ker \pi| \cdot |H(m^{\ell v(T)}, T)|.
\]
The claim follows.

Proof of Proposition 2.2.1 We write any \( m \) as a product \( m = m_1 \cdot m_2 \) where \( m_1|m_\infty \) and \( (m_2, m_A) = 1 \). By the Chinese Remainder theorem, one has
\[
m|H(m, T)| = m_1|H(m_1, T)| \prod_{\ell|m_2} \ell^{v_\ell(m_2)}|H(\ell^{v_\ell(m_2)}, T)|
\]
and thus taking limits
\[
\lim_{m \to \infty} \frac{m|H(m, T)|}{|H(m)|} = \lim_{m_1 \to \infty} \frac{m_1|H(m_1, T)|}{|H(m_1)|} \prod_{\ell|m_A} \lim_{n \to \infty} \frac{\ell^{n}H(\ell^{n}, T)}{|H(\ell^{n})|}.
\]
The result now follows from Lemma 2.2.4.

It remains to show that the infinite product of rational functions in the primes \( \ell \nmid m_A \) converges:

Proposition 2.2.5 Assume \( T \neq 0 \). The infinite product \( \prod_{\ell|m_A} \ell^{v_\ell(T)+1}|H(\ell^{v_\ell(T)+1}, T)| \]
converges.

This follows from a straightforward explicit computation of the quantities involved which we record here:

Lemma 2.2.6 Let \( \ell \) be an odd prime. Then using the quadratic residue symbol we have
\[
|M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})|_{\text{det} = d} = \ell \left( \ell + \left( \frac{t^2 - 4d}{\ell} \right) \right).
\]

Proof We are counting the set of matrices
\[
\left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z}) : xw - yz = d, x + w = t \right\}.
\]
This amounts to computing \(|\{x, y, z \in \mathbb{Z}/\ell\mathbb{Z} : yz = -x^2 + tx - d\}|. \) If \(yz = 0\), there are \(\left(\frac{t^2 - 4d}{\ell}\right) + 1\) possibilities for \(x\). If \(yz \in \mathbb{F}_\ell^*\) then \(x\) can run through \(\ell - 1 - \left(\frac{t^2 - 4d}{\ell}\right)\) possibilities. We thus obtain
\[
|M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})|_{\text{det} = d}^{\text{tr} = t} = \left(1 + \left(\frac{t^2 - 4d}{\ell}\right)\right) \cdot (2\ell - 1) + \left(\ell - 1 - \left(\frac{t^2 - 4d}{\ell}\right)\right) \cdot (\ell - 1) = \ell\left(\ell + \left(\frac{t^2 - 4d}{\ell}\right)\right).
\]

Moreover, recalling the notation \(G = \text{GL}_2 \times \det \text{GL}_2\), we record here the counts:

**Lemma 2.2.7** Let \(\ell\) be a prime. Then \(|G(\ell)| = (\ell - 1)\ell^2(\ell^2 - 1)^2\).

**Lemma 2.2.8** Let \(\ell\) be an odd prime. Then
\(|G(\ell)| = (\ell - 1)\ell^2(\ell^2 - 1)^2\) and \(|G(\ell, 0)| = \ell^2(\ell - 1)(\ell^3 - \ell - 1)\).

**Proof** Note that
\[
|G(\ell, 0)| = \sum_{t \in \mathbb{Z}/\ell\mathbb{Z}} \sum_{d \in (\mathbb{Z}/\ell\mathbb{Z})^\times} |M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})|_{\text{det} = d}^{\text{tr} = t} |M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})|_{\text{det} = d}^{\text{tr} = -t}
\]
\[
= \sum_{t \in \mathbb{Z}/\ell\mathbb{Z}} \sum_{d \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \ell^2 \left(\ell + \left(\frac{t^2 - 4d}{\ell}\right)\right)^2.
\]
The \(t = 0\) term is
\[
\sum_{d \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \ell^2 \left(\ell + \left(\frac{4d}{\ell}\right)\right)^2 = (\ell - 1)/2 \cdot \ell^2((\ell + 1)^2 + (\ell - 1)^2)
\]
\[
= \ell^2(\ell - 1)(\ell^2 + 1).
\]
For fixed \(t \in (\mathbb{Z}/\ell\mathbb{Z})^\times\) it is easy to see that the set \(\{t^2 - 4d : d \in (\mathbb{Z}/\ell\mathbb{Z})^\times\}\) consists of zero, \(\frac{\ell-3}{2}\) squares, and \(\frac{\ell-1}{2}\) non-squares. Thus,
\[
\sum_{t \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \sum_{d \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \ell^2 \left(\ell + \left(\frac{t^2 - 4d}{\ell}\right)\right)^2
\]
\[
= \sum_{t \in (\mathbb{Z}/\ell\mathbb{Z})^\times} \ell^2 \left(\ell^2 + \frac{(\ell - 3)(\ell + 1)^2 + (\ell - 1)^2}{2} (\ell - 1)^2\right)
\]
\[
= \ell^2(\ell - 2)(\ell^2 + \ell + 1)(\ell - 1).
\]

\(\square\)
We conclude that, as desired,
\[
|G(\ell, 0)| = \ell^2(\ell - 1)(\ell^2 + 1) + \ell^2(\ell - 2)(\ell^2 + \ell + 1)(\ell - 1)
= \ell^2(\ell - 1)(\ell^3 - \ell - 1).
\]

\[\Box\]

**Lemma 2.2.9** Let \( \ell \) be an odd prime. Then
\[
\frac{\ell |G(\ell, T)|}{|G(\ell)|} = \begin{cases} 
\frac{\ell(\ell^3 - \ell - 1)}{(\ell^2 - 1)^2} & \text{if } T = 0, \\
\frac{\ell(\ell^4 - \ell^3 - 2\ell^2 + \ell + 2)}{(\ell^2 - 1)^2(\ell - 1)} & \text{else.}
\end{cases}
\]

Moreover if \( \ell \nmid T \), then \(|G(\ell^n, T)| = \ell^{6n-4} \cdot (\ell^4 - \ell^3 - 2\ell^2 + \ell + 2)\) and
\[
\frac{\ell |G(\ell, T)|}{|G(\ell)|} = \frac{\ell^n |G(\ell^n, T)|}{|G(\ell^n)|}.
\]

**Proof** For \( t \in (\mathbb{Z}/\ell\mathbb{Z})^\times \), the rule \( h \mapsto th \) gives a bijection \( G(\ell, 1) \to G(\ell, t) \). Thus \(|G(\ell, t)| = |G(\ell, 1)|\) for all \( t \in (\mathbb{Z}/\ell\mathbb{Z})^\times \). Using Lemma 2.2.8, it follows that for \( t \in (\mathbb{Z}/\ell\mathbb{Z})^\times \) we have
\[
|G(\ell, t)| = \frac{|G(\ell)| - |G(\ell, 0)|}{\ell - 1} = \ell^2(\ell^4 - \ell^3 - 2\ell^2 + \ell + 2).
\]

The first result follows easily and the second follows from Lemma 2.2.4. \( \Box \)

We deduce convergence of the product from these counts:

**Proof of Proposition 2.2.5** It suffices to consider the primes \( \ell \nmid (T \cdot m_A) \). For such primes, we have that \( H(\ell^n) = G(\ell^n) \) and from our previous results since \( T \neq 0 \) we have:
\[
\frac{\ell v_\ell(T+1)|H(\ell v_\ell(T)+1, T)|}{|H(\ell v_\ell(T)+1)|} = \frac{\ell |G(\ell, T)|}{|G(\ell)|} = \frac{\ell(\ell^4 - \ell^3 - 2\ell^2 + \ell + 2)}{(\ell^2 - 1)^2(\ell - 1)} = 1 + O\left(\frac{1}{\ell^3}\right).
\]

This proves convergence. \( \Box \)

In Sects. 3 and 4 below, we will prove Theorem 1.0.6, establishing explicit formulas for the universal factors and the exceptional factor (in the case where \((E_1, E_2)\) form a Serre pair), respectively.
2.3 Positivity of the conjectural constant

We now discuss briefly the question of when the conjectural constant $C(E_1 \times E_2, T)$ appearing in Conjecture 1.0.5 is positive. As we have seen in the previous section, the infinite product part of the constant is a convergent Euler product. In particular that product is non-zero, and so we have

$$C(A, T) = 0 \iff H_{A}(m_{A,T}, T) = \emptyset \quad (A = E_1 \times E_2). \quad (1.7)$$

This is analogous to the situation in the original Lang–Trotter conjecture, wherein, for a single elliptic curve $E$ over $\mathbb{Q}$ and an integer $t$, we have

$$C(E, t) = 0 \iff H_E(m_E, T) = \emptyset.$$

For each $m \in \mathbb{N}$, we are motivated to define the following subsets of $\mathbb{Z}/m\mathbb{Z}$:

$$T_{E_i}(m) := \{ t \in \mathbb{Z}/m\mathbb{Z} : \left| \{ p \text{ prime} : p \nmid N_{E_i}, \ a_p(E_i) \equiv t \pmod{m} \} \right| = \infty \}$$

$$= \text{tr} \left( H_{E_i}(m) \right) \subseteq \mathbb{Z}/m\mathbb{Z} \quad (i \in \{1, 2\}),$$

$$T_{E_1 \times E_2}(m) := \{ t \in \mathbb{Z}/m\mathbb{Z} : \left| \{ p \text{ prime} : p \nmid N_{E_1}N_{E_2}, \quad a_p(E_1 \times E_2) \equiv t \pmod{m} \} \right| = \infty \}$$

$$= \text{tr} \left( H_{E_1 \times E_2}(m) \right) \subseteq \mathbb{Z}/m\mathbb{Z}. \quad (1.8)$$

Evidently, we have

$$T_{E_1 \times E_2}(m) \subseteq T_{E_1}(m) + T_{E_2}(m) \subseteq \mathbb{Z}/m\mathbb{Z} \quad (1.9)$$

and, denoting by $\overline{t}_m$ the reduction modulo $m$ of an integer $t$,

$$C(E, t) = 0 \iff \exists m \mid m_E \text{ with } \overline{t}_m \notin T_E(m),$$

$$C(E_1 \times E_2, T) = 0 \iff \exists m \mid m_{E_1 \times E_2} \text{ with } \overline{t}_m \notin T_{E_1 \times E_2}(m). \quad (1.10)$$

Suppose that $A = E_1 \times E_2$ where $(E_1, E_2)$ is a Serre pair, let $m$ be any positive integer divisible by $m_A$, and write $m =: 2^{\alpha}m'$ with $m'$ odd. By the subgroup containment

$$\left( \pi_{2^\alpha,2}^{-1} \left( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \times \text{SL}_2(\mathbb{Z}/m'\mathbb{Z}) \right) \times \left( \pi_{2^\alpha,2}^{-1} \left( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \times \text{SL}_2(\mathbb{Z}/m'\mathbb{Z}) \right) \subseteq H_A(m),$$

together with (1.7), we may see that the constant $C(E_1 \times E_2, T)$ is positive for all $T \in \mathbb{Z}$. By [17], the condition that $(E_1, E_2)$ is a Serre pair represents the generic case, happening for almost all pairs $(E_1, E_2)$.

To find examples of products and values of $T$ for which $C(E_1 \times E_2, T) = 0$, the condition (1.10), together with (1.9), leads us to the observation that

$$T_{E_1}(m) + T_{E_2}(m) \neq \mathbb{Z}/m\mathbb{Z} \implies \exists T \in \mathbb{Z} \text{ with } C(E_1 \times E_2, T) = 0.$$
In particular, for any \( T \in \mathbb{Z} \) for which \( T_m \notin T_{E_1}(m) + T_{E_2}(m) \), we have \( C(E_1 \times E_2, T) = 0 \). A basic example of this occurs when

\[
E_1(\mathbb{Q})[2] \neq \{O_{E_1}\} \quad \text{and} \quad E_2(\mathbb{Q})[2] \neq \{O_{E_2}\}. \tag{1.11}
\]

Note in general that, if \( E(\mathbb{Q}) \) has a point of order \( m \) then for all primes \( p \nmid N_E \), we have

\[
m \text{ divides } p + 1 - a_p(E) = |E(\mathbb{F}_p)|.
\]

Taking \( m = 2 \), we deduce that, provided (1.11) holds, for all odd primes \( p \nmid N_{E_1}N_{E_2} \), each \( a_p(E_i) \) must be even, and therefore \( a_p(E_1 \times E_2) = a_p(E_1) + a_p(E_2) \) must be even as well; in this case we have

\[
T_{E_1}(2) = \{0\} = T_{E_2}(2), \quad \text{so} \quad T_{E_1}(2) + T_{E_2}(2) = \{0\}.
\]

A quick search produces many explicit examples, for instance taking

\[
E_1 : y^2 = x^3 + x^2 + x, \\
E_2 : y^2 + xy = x^3 + x^2 + x
\]

([28, E.C. 48.a5] and [28, E.C. 39.a4], respectively) leads to an abelian surface \( A = E_1 \times E_2 \) satisfying the conditions of Conjecture 1.0.5 where at most finitely many primes \( p \) have odd \( a_p(A) \).

Our next example shows that it is possible to find pairs \( (E_1, E_2) \) with \( C(E_1 \times E_2, T) = 0 \) for an appropriate \( T \) even when \( T_{E_1}(m) + T_{E_2}(m) = \mathbb{Z}/m\mathbb{Z} \) for all \( m \). Given (1.10) and (1.9), this is only possible if, for some \( m \in \mathbb{N} \), we have

\[
T_{E_1 \times E_2}(m) \subsetneq T_{E_1}(m) + T_{E_2}(m) = \mathbb{Z}/m\mathbb{Z}. \tag{1.12}
\]

We define \( E_1 \) and \( E_2 \) by

\[
E_1 : y^2 = x^3 + 6x - 2, \\
E_2 : y^2 = x^3 - 108x - 918.
\]

As demonstrated in [20], the elliptic curve \( E_1 \) is a Serre curve, and again using that

\[
\pi_{2y,2}^{-1} \left( \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right) \times \text{SL}_2(\mathbb{Z}/m'\mathbb{Z}) \subseteq \text{Im}(\rho_{E,2^e m'}),
\]

we may see that, for every \( m \in \mathbb{N} \), we have \( T_{E_1}(m) = \mathbb{Z}/m\mathbb{Z} \). In particular, this implies that \( T_{E_1}(m) + T_{E_2}(m) = \mathbb{Z}/m\mathbb{Z} \). On the other hand, [24, Theorem 1] implies that \( E_1[2] \) and \( E_2[2] \) are isomorphic as \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \)-modules, which in turn implies
that, for every prime $p \nmid N_{E_1}N_{E_2}$, we have $a_p(E_1) \equiv a_p(E_2) \mod 2$. From this, it follows that $a_p(E_1 \times E_2)$ must always be even, so

$$T_{E_1 \times E_2}(2) = [0] \subseteq \mathbb{Z}/2\mathbb{Z} = T_{E_1}(2) + T_{E_2}(2),$$

and thus $C(E_1 \times E_2, T) = 0$ for each odd $T \in \mathbb{Z}$.

Another example in this same spirit involves level 4 structure. Consider the elliptic curves

$E_1 : y^2 = x^3 - 4900172/45369x - 19600688/45369,$

$E_2 : y^2 = x^3 - 186732x - 746928.$

The elliptic curve $E_1$ admits a rational 4-isogeny (equivalently, $\text{Im}(\rho_{E_1,4}) \subseteq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$), whereas $E_2$ has a square discriminant (equivalently, $\text{Im}(\rho_{E_2,2}) \subseteq \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$). Taking $m = 4$ in (1.8), we have

$$T_{E_1}(4) = \{0, 2\},$$

$$T_{E_2}(4) = \{0, 1, 2, 3\}.$$  

However, because of the cyclotomic entanglement $\mathbb{Q}(i) \subseteq \mathbb{Q}(E_1[4]) \cap \mathbb{Q}(E_2[4])$, and the fact that

$$\forall g \in \text{GL}_2(\mathbb{Z}/4\mathbb{Z}), \ g \equiv I \ mod \ 2 \implies \text{tr} \ g \equiv 1 + \det g \ mod \ 4,$$

we may see that $2 \not\in T_{E_1 \times E_2}(4)$. In fact,

$$T_{E_1 \times E_2}(4) = \{0, 1, 3\},$$

and thus $C(E_1 \times E_2, T) = 0$ whenever $T \equiv 2 \ mod \ 4$.

Finally, one might ask whether there exists pairs $(E_1, E_2)$ such that for some $m \in \mathbb{Z}$ we have

$$T_{E_1}(m) \neq \mathbb{Z}/m\mathbb{Z} \ and \ T_{E_2}(m) \neq \mathbb{Z}/m\mathbb{Z}, \ but \ T_{E_1 \times E_2}(m) = \mathbb{Z}/m\mathbb{Z}.$$ 

Our final example shows that this can indeed happen. Let $E_1$ and $E_2$ be given by

$E_1 : y^2 = x^3 - 41399424/41971x - 496793088/41971,$

$E_2 : y^2 = x^3 + 533418040116/625x - 3633643689270192/3125.$

The elliptic curve $E_1$ has a rational 2-torsion point, and so, taking $m = 4$, we have $T_{E_1}(4) = \{0, 2\}$. The second elliptic curve $E_2$ has the property that $\mathbb{Q}(\sqrt{\Delta_{E_2}}) = \mathbb{Q}(i)$, which forces the sub-extension $\mathbb{Q}(i, \Delta_{E_2}^{1/4})$, which generically has Galois group $D_4$ over $\mathbb{Q}$, to be at most a bi-quadratic extension of $\mathbb{Q}$. For $E_2$, we further have
\( \mathbb{Q}(i, \Delta_{E_2}^{1/4}) = \mathbb{Q}(i) \), and this in turn forces \( \rho_{E_2,4}(G_{\mathbb{Q}}) \) to be contained in a certain index 4 subgroup of \( \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \). The traces of this subgroup are \{0, 2, 3\}, and we compute that, in fact, \( T_{E_2}(4) = \{0, 2, 3\} \). However, unlike the previous example, the cyclotomic entanglement does not manage to link up the traces in this case, and we may see by direct computation that

\[
\{a_p(E_1 \times E_2) \mod 4 : p \nmid N_{E_1}N_{E_2}\} = \mathbb{Z}/4\mathbb{Z}.
\]

All of the above examples suggest that the question of positivity of the conjectural constants \( C(E_1 \times E_2, T) \) is rather subtle and worthy of further study.

### 2.4 Theoretical evidence

Although this is not the main focus of our paper, we conclude this section with some remarks about theoretical results towards Conjecture 1.0.5. Applying the effective Čebotarev results of Lagarias and Odlyzko [19], we obtain, following Serre’s original treatment for single elliptic curves [26, Théorème 20]:

**Theorem 2.4.1**  Let \( E_1/\mathbb{Q}, E_2/\mathbb{Q} \) be non-CM elliptic curves non-isogenous over \( \mathbb{Q} \). Let \( A \sim_{\mathbb{Q}} E_1 \times E_2 \) and let \( T \in \mathbb{Z} \setminus \{0\} \). Set \( \epsilon(x) = (\log x)(\log \log x)^{-2}(\log \log \log x)^{-1} \) and \( \epsilon_R(x) = \sqrt{x}(\log x)^{-2} \).

1. We have an unconditional upper bound as \( x \to \infty \) of

\[
\pi_{A,T}(x) = O(\text{Li}(x) \cdot \epsilon(x)^{-1/7}).
\]

2. Under GRH, we obtain the upper bound as \( x \to \infty \):

\[
\pi_{A,T}(x) = O(\text{Li}(x) \cdot \epsilon_R(x)^{-1/7}).
\]

In particular, for all \( \epsilon > 0 \) we have under GRH the bound \( \pi_{A,T}(x) = O(x^{1-\frac{1}{14}+\epsilon}) \) as \( x \to \infty \).

**Proof**  It suffices to consider the case \( A = E_1 \times E_2 \). Let \( \ell \) denote a large rational prime such that the image of the \( \ell \)-adic Galois representation \( \text{Im}(\rho_{A,\ell}) \) is all of the compact \( \ell \)-adic Lie group \( G(\mathbb{Z}_\ell) = \text{GL}_2(\mathbb{Z}_\ell) \times_{\text{det}} \text{GL}_2(\mathbb{Z}_\ell) \) and such that \( \ell \nmid T \). The latter condition implies smoothness of the \( \ell \)-adic analytic manifold \( X_T(\mathbb{Z}_\ell) := \{(g_1, g_2) \in \text{GL}_2(\mathbb{Z}_\ell) \times_{\text{det}} \text{GL}_2(\mathbb{Z}_\ell) \mid \text{tr}(g_1) + \text{tr}(g_2) = T\} \). Moreover, \( X_T(\mathbb{Z}_\ell) \subset G(\mathbb{Z}_\ell) \) is closed, stable under conjugation, and the dimensions as \( \ell \)-adic manifolds (in the sense of Serre-Oesterlé) of \( X_T(\mathbb{Z}_\ell) \) and \( G(\mathbb{Z}_\ell) \) are 6 and 7, respectively. Observing that

\[
\pi_{A,T}(x) \leq \left| \{p \leq x \text{ prime} : p \nmid \ell \cdot N_A \text{ and } \rho_{A,\ell}(\text{Frob}_p) \in X_T(\mathbb{Z}_\ell)\} \right|,
\]

it suffices to give an upper bound for the latter. This bound now follows from [26, Théorème 10], which is an application of effective Čebotarev results to Galois extensions \( K_\ell/\mathbb{Q} \) with Galois groups \( G_\ell = \text{Gal}(K_\ell/\mathbb{Q}) \) which are compact \( \ell \)-adic Lie groups. Indeed, in our setting taking \( K_\ell \) to be the fixed field of \( \ker(\rho_{A,\ell}) \) gives a

\[ \square \]
Galois extension $K_\ell = \mathbb{Q}(A_\ell)$ of $\mathbb{Q}$ with Galois group $\text{Gal}(\mathbb{Q}(A_\ell)/\mathbb{Q}) \cong G(\mathbb{Z}_\ell)$, and we are precisely counting the primes $p$ outside a finite set of ultrametric places such that $\rho_{A_\ell}(\text{Frob}_p) \in X_T(\mathbb{Z}_\ell)$.

Just as for single elliptic curves, these results can likely be refined and the upper bound improved using similar techniques, and we plan to address this in ongoing work [7].

Furthermore, we expect that Conjecture 1.0.5 can be shown to hold on average, as was proven for single elliptic curves by David and Pappalardi [10], extending results by Fouvry and Murty in the supersingular case [13]. More precisely, writing $E(a, b)$ with $a, b \in \mathbb{Z}$ for the elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$, David and Pappalardi show that:

**Theorem 2.4.2** (Corollary 1.3. of [10]) Fix $t \in \mathbb{Z}$. For $\varepsilon > 0$ and $A, B > x^{1+\varepsilon}$ we have as $x \to \infty$:

$$
\frac{1}{4AB} \sum_{a \leq A, b \leq B} \pi_{E(a,b),t}(x) \sim C_t \cdot \sqrt{x}/\log(x),
$$

where the constant $C_t$ is the universal part of the constant $C(E,t)$ given by

$$
C_t = \frac{2}{\pi} \prod_{\ell | t} \left(1 - \frac{1}{\ell^2}\right)^{-1} \prod_{\ell | t} \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)}.
$$

They also prove that the normal order of $\pi_{E(a,b),t}(x)$ is $C_t \cdot \sqrt{x}/\log(x)$ (see [10, Corollary 1.5.]). Moreover, it is known for Serre curves $E(a, b)$ and conditionally in general (see [15]) that

$$
\frac{1}{4AB} \sum_{a \leq A, b \leq B} C(E(a,b),t) \sim C_t
$$

as $A, B \to \infty$.

We anticipate that in our setting for large enough $A, B$ in relation to $x$ one has similarly the asymptotic

$$
\frac{1}{16A^2B^2} \sum_{a_1, a_2 \leq A, b_1, b_2 \leq B} \pi_{E(a_1,b_1) \times E(a_2,b_2),T}(x) \sim C_T \cdot (\sqrt{x}/\log(x)),
$$

where

$$
C_T := 2\Phi_{SU(2)^\times 2}(0) \cdot \prod_{\ell \text{ prime}} \frac{\ell^{v_\ell(T)+1} |G(\ell^{v_\ell(T)+1}, T)}{|G(\ell^{v_\ell(T)}+1)|}.
$$
Moreover, the normal order should also be the average order and it seems reasonable to expect that
\[ C_T = \lim_{A, B \to \infty} \left( \frac{1}{16A^2B^2} \sum_{a_1, a_2 \leq A} \sum_{b_1, b_2 \leq B} C(E(a_1, b_1) \times E(a_2, b_2), T) \right) \]
is the average constant.

### 3 Explicit constants

Let \( \ell \geq 3 \) be a fixed prime. The goal of this section is to compute the stable ratios given by

\[
\frac{\ell v_T + 1 |H(\ell v_T + 1, T)|}{|H(\ell v_T + 1)|} = \frac{\ell v_T + 1 |G(\ell v_T + 1, T)|}{|G(\ell v_T + 1)|}
\]

for primes \( \ell | T \) and coprime to \( m_A \), where \( T \) is some non-zero integer. As soon as \( \ell | T \), one has to take into consideration that the number of matrices of a given trace and determinant above a class modulo \( \ell \) scales differently depending on the \( \ell \)-adic distance to scalar matrices. Therefore a more detailed analysis is necessary.

#### 3.1 Fixed trace and determinant counts

We first consider counts for \( M_{2 \times 2}(\mathbb{Z}/\ell^n \mathbb{Z}) \). Denote by \( S_0 \) the matrices in \( M_{2 \times 2}(\mathbb{Z}) \) which are not congruent to scalar matrices modulo \( \ell \) and by \( S_0(j) \) the reduction of \( S_0 \) modulo \( \ell^j \):

\[
S_0 := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2 \times 2}(\mathbb{Z}) : \forall \lambda \in \mathbb{Z}/\ell \mathbb{Z}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \not\equiv \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mod \ell \right\},
\]

\[
S_0(j) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2 \times 2}(\mathbb{Z}/\ell^j \mathbb{Z}) : \forall \lambda \in \mathbb{Z}/\ell \mathbb{Z}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \not\equiv \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mod \ell \right\}.
\]

For fixed integers \( t, s \in \mathbb{Z} \), we let \( \mathcal{H}_{i, n}(t, s) \) denote the set of matrices in \( M_{2 \times 2}(\mathbb{Z}/\ell^n \mathbb{Z}) \) with trace (resp. determinant) congruent to \( t \) (resp. to \( s \)) modulo \( \ell^n \) and which are congruent to a scalar matrix modulo \( \ell^i \) but not \( \ell^{i+1} \) and denote by \( h_{i, n}(s, t) \) the cardinality of that set:

\[
\mathcal{H}_{i, n}(t, s) := \left\{ A \in M_{2 \times 2}(\mathbb{Z}/\ell^n \mathbb{Z}) : \exists \lambda \in \mathbb{Z}, \exists A' \in S_0 \text{ with } A \equiv \lambda I_2 + \ell^i A' \mod \ell^n \text{ and } \text{tr } A \equiv t \mod \ell^n \text{ and } \det A \equiv s \mod \ell^n \right\},
\]

\[
h_{i, n}(t, s) := |\mathcal{H}_{i, n}(t, s)|.
\]
Lemma 3.1.1  Fix $(t, s) \in \mathbb{Z}$. We have that

$$h_{i,n}(t, s) = \begin{cases} 
\ell^{2n-i} \left( \ell^i + \ell \left( \frac{\ell^{2i} + \ell^{2i}(t,s)}{\ell^i} \right) \right) / \ell^2 & \text{if } 0 \leq i < n/2 \text{ and } \ell^{2i} | \Delta(t, s), \\
\ell^{2n-(3i-n)} \left( \frac{\ell^{3i} - 1}{\ell^i} \right) & \text{if } n/2 \leq i < n \text{ and } \ell^n | \Delta(t, s), \\
1 & \text{if } i = n \text{ and } \ell^n | \Delta(t, s), \\
0 & \text{else},
\end{cases}$$

where $\Delta(t, s) = t^2 - 4s$.

Proof  We are counting matrices of trace and determinant $(t, s)$ of the form

$$aI + \ell^i \begin{pmatrix} b & c \\
& & \\
d & e \end{pmatrix} \mod \ell^n,$$

where $\begin{pmatrix} b & c \\
& & \\
d & e \end{pmatrix} \in S_0$ and $a \in \mathbb{Z}/\ell^i \mathbb{Z}$. We first consider the case when $i = 0$ and compute $h_{0,n}(t, s)$. We know from [20, p.127] that the count modulo $\ell$ is given by

$$h_{0,1}(t, s) = \ell^2 + \ell \left( \frac{\Delta(t, s)}{\ell} \right) + \left( \frac{\Delta(t, s)}{\ell} \right)^2 - 1.$$

Moreover, once an $\ell$-adic distance to scalar matrices is fixed, the count scales uniformly and only depends on the classes of $(t, s)$ in $\mathbb{F}_\ell$. This yields

$$h_{0,n}(t, s) = \ell^{2n-2} \left( \ell^2 + \ell \left( \frac{\Delta(t, s)}{\ell} \right) + \left( \frac{\Delta(t, s)}{\ell} \right)^2 - 1 \right).$$

Let now $i > 0$, the condition on the determinant amounts to the congruences

$$\ell^{2i} (be - dc) \equiv -a^2 - \ell^i a(b + e) + s \mod \ell^n,$$

$$\equiv a^2 - at + s \mod \ell^n,$$

$$\equiv 1/4((t - 2a)^2 - \Delta(t, s)) \mod \ell^n.$$

We observe that for our choice of $a$ we must have that $t - 2a \equiv 0 \mod \ell^i$ and therefore $a^2 - at + s$ is divisible by $\ell^{\min(2i,n)}$ if and only if the discriminant $\Delta(t, s)$ is divisible by $\ell^{\min(2i,n)}$ (here 4 is a unit). This proves that $h_{i,n}(t, s) = 0$ whenever $\Delta(t, s)$ is not divisible by $\ell^{\min(2i,n)}$. The condition on the trace amounts to the congruence

$$\ell^i (b + e) \equiv t - 2a \mod \ell^n,$$

which yields exactly one possibility for the sum $b + e$ modulo $\ell^{n-i}$.

If $i < n/2$ we must have $\ell^{2i} | \Delta(t, s)$ and in that case $be - dc$ has to project onto a fixed residue class modulo $\ell^{n-2i}$, yielding $\ell^i$ possibilities modulo $\ell^{n-1}$. Moreover, $\Delta(b + e, be - dc) \equiv \ell^{-2i} \Delta(t, s) \mod \ell$. Since the computation of $h_{0,n-i}(t, s)$ only
depends on the discriminant modulo \( \ell \), the count is \( \ell^i \) times the number of matrices in \( S_0(n-i) \) of a fixed discriminant \( \ell^{-2i} \Delta(t,s) \):

\[
h_{i,n}(t,s) = \ell^i \cdot \ell^{2(n-1)-2} \left( \ell^2 + \ell \left( \frac{\ell^{-2i} \Delta(t,s)}{\ell} \right) + \left( \frac{\ell^{-2i} \Delta(t,s)}{\ell} \right)^2 - 1 \right),
\]

as claimed.

Finally assume \( n/2 \leq i < n \), the case of \( i = n \) being trivial. We must then have \( a^2 - at + s \equiv 0 \mod \ell^n \) or equivalently \( \ell^n | \Delta(t,s) \) since \( \ell^i | (t-2a) \). We are reduced to counting matrices in \( S_0(n-i) \) of a fixed trace \( t_0 = (t-2a)/\ell^i \), where now the determinant \( be - dc \) is allowed to run through all of \( \mathbb{Z}/\ell^{n-i} \mathbb{Z} \). We obtain:

\[
h_{i,n}(t,s) = \ell^{2(n-i)-2} \sum_{s \in \mathbb{Z}/\ell^{n-i} \mathbb{Z}} \left( \ell^2 + \ell \left( \frac{\Delta(t_0,s)}{\ell} \right) + \left( \frac{\Delta(t_0,s)}{\ell} \right)^2 - 1 \right)
\]

\[
= \ell^{2(n-i)-2} (\ell^{n-i+2} + 0 - \ell^{n-i-1})
\]

\[
= \ell^{3n-3i} \ell^3 - \ell^3.
\]

\[3.2 \text{ Computation of } |H(\ell^n,T)|\]

We now fix a nonzero trace \( T \in \mathbb{Z} \) and assume that \( v_\ell(T) > 0 \). Let \( S_{i,i',n}(T) \) denote the number of \( \mathbb{Z}/\ell^n \mathbb{Z} \)-points on \( \text{GL}_2 \times \det \text{GL}_2 \) consisting of pairs of two-by-two matrices whose traces sum to \( T \) and which are congruent to scalars exactly modulo \( \ell^i \) and \( \ell^{i'} \), respectively:

\[
S_{i,i',n}(T) := \bigcup_{t \in \mathbb{Z}/\ell^n \mathbb{Z}} \bigcup_{s \in (\mathbb{Z}/\ell^n \mathbb{Z})^\times} \mathcal{H}_{i,n}(t,s) \times \mathcal{H}_{i',n}(T-t,s)
\]

\[
= \sum_{t \in \mathbb{Z}/\ell^n \mathbb{Z}} \sum_{s \in (\mathbb{Z}/\ell^n \mathbb{Z})^\times} h_{i,n}(t,s) h_{i',n}(T-t,s).
\]

We may as well assume that \( i' \geq i \). To simplify notation, we define the function \( h_i : \ell^{2i} \mathbb{Z} \to \mathbb{Z} \) by

\[
h_i(x) := \ell^2 + \ell \left( \frac{\ell^{-2i} x}{\ell} \right) + \left( \frac{\ell^{-2i} x}{\ell} \right)^2 - 1 \quad (\ell^{-2i} x \in \mathbb{Z}).
\]

\[\square \]
Lemma 3.2.1 Assume \( i' > 0 \) and \( v_\ell(T) > 0 \). We have that

\[
S_{i,i',n}(T) = \sum_{t \in (\mathbb{Z}/\ell^n)^\times} \sum_{s \equiv (t/2)^2(\ell^n)} \ell^{4n-(i+i')-4} h_i'(\Delta(t,s))h_i(\Delta(T-t,s)) \quad \text{if } n > 2i' \text{ and } \ell^{2i}|T
\]

\[
= (\ell - 1) \ell^{6n-(i+i')-6} (\ell^3 - 1) \left( \ell^2 + \left( \frac{\ell^2 - 1}{\ell} \right)^2 - 1 \right) \quad \text{if } 2n > 2i' \geq n > 2i \text{ and } \ell^{2i}|T
\]

\[
= (\ell - 1) \ell^{3n-i-3} \left( \ell^2 + \left( \frac{\ell^2 - 1}{\ell} \right)^2 - 1 \right) \quad \text{if } i' = n > 2i \text{ and } \ell^{2i}|T
\]

\[
= (\ell - 1) \ell^{7n-(3i+3i')-7}(\ell^3 - 1)^2 \quad \text{if } 2n > 2i' \geq 2i \geq n \text{ and } \ell^n|T
\]

\[
= (\ell - 1) \ell^{4n-3i-3}(\ell^3 - 1) \quad \text{if } 2n > 2i' \geq 2i \geq n \text{ and } \ell^n|T
\]

\[
= 0 \quad \text{if } \ell^{\min(2i',n)} \not| T
\]

**Proof** This follows from summing the contributions \( h_{i,n}(t,s) : h_{i',n}(T-t,s) \) in Lemma 3.1.1. Since \( i' > 0 \) we get from Lemma 3.1.1 positive contributions only when \( v_\ell((T-t)^2 - 4s) > 0 \). But here \( s \) is only running through units modulo \( \ell \neq 2 \) so that \( v_\ell(4s) = 0 \), and thus to get positive contributions \( T-t \) must be a unit, and similarly \( v_\ell(t) = 0 \) since \( v_\ell(T) > 0 \). Furthermore, writing \( \Delta(T-t,s) - \Delta(t,s) = T(T-2t) \), by Lemma 3.1.1 we only get positive contributions when \( \ell^{\min(2i',n)}|T \). Moreover,

\[
\ell^{\min(2i',n)}|\Delta(t,s) \iff s = (t/2)^2 \mod \ell^{\min(2i',n)}
\]

and this also guarantees that \( \ell^{2i}|\Delta(T-t,s) \) provided \( \ell^{\min(2i',n)}|T \). If \( n > 2i' \) the conclusion follows from Lemma 3.1.1. When \( 2n > 2i' \geq n > 2i \) we obtain from Lemma 3.1.1 the count:

\[
S_{i,i',n}(T) = \sum_{t \in (\mathbb{Z}/\ell^n)^\times} \sum_{s \equiv (t/2)^2(\ell^n)} \ell^{3n-3i'-3}(\ell^3 - 1)\ell^{2n-i-2} h_i(\Delta(T-t,s))
\]

\[
= \sum_{t \in (\mathbb{Z}/\ell^n)^\times} \ell^{5n-(i+3i')-5}(\ell^3 - 1)h_i(\Delta(T-t,t^2/4))
\]

\[
= \ell^{5n-(i+3i')-5}(\ell^3 - 1) \sum_{t \in (\mathbb{Z}/\ell^n)^\times} h_i(T(T-2t)).
\]

Similarly, when \( 2n = 2i' > 2i \) we get \( S_{i,i',n}(T) = \ell^{2n-i-2} \sum_{t \in (\mathbb{Z}/\ell^n)^\times} h_i(T(T-2t)) \).

The result follows from

\[
\sum_{u \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} h_i(Tu) = \begin{cases} (\ell - 1)\ell^{n-1}(\ell^2 - 1) & \text{if } \ell^{2i+1}|T, \\ (\ell - 1)\ell^{n-1}\ell^2 & \text{if } \ell^{2i} \parallel T. \end{cases}
\]

The first case is trivial since then all the residue symbols vanish. When \( \ell^{2i} \parallel T \), we obtain that

\[
\sum_{u \in (\mathbb{Z}/\ell^n)^\times} h_i(Tu) = \sum_{x \in (\mathbb{Z}/\ell^n)^\times} \left( \ell^2 + \ell \left( \frac{x}{\ell} \right) + \left( \frac{x}{\ell} \right)^2 - 1 \right)
\]
\[ = \ell^{n-1}(\ell - 1)\ell^2, \]

as claimed. All of the cases now follow by an easy calculation based on Lemma 3.1.1.

We now provide an exact count also in the first case when \( n > 2i' \). We first recall a useful standard result for reader convenience:

**Lemma 3.2.2** For integers \( a, b, c \in \mathbb{Z} \) with \( (a, b) \neq (0, 0) \) and for any odd prime \( \ell \) we have the formula

\[
\ell - 1 \sum_{x=0}^{\ell-1} \left( \frac{ax^2 + bx + c}{\ell} \right) = \begin{cases} -\left( \frac{a}{\ell} \right) & \text{if } \ell \nmid b^2 - 4ac, \\ (\ell - 1) \cdot \left( \frac{a}{\ell} \right) & \text{else.} \end{cases}
\]

**Proof** This is a straightforward computation: when \( \ell \mid a \) the result easily holds, and when \( \ell \nmid a \) the sum can be rewritten as

\[
\left( \frac{a}{\ell} \right) \cdot \ell - 1 \sum_{x=0}^{\ell-1} \left( \frac{(2ax + b)^2 + (4ac - b^2)}{\ell} \right).
\]

One immediately concludes when \( \ell \mid b^2 - 4ac \). When \( \ell \nmid b^2 - 4ac \), one concludes since \( \sum_{x=0}^{\ell-1} \left( \frac{x^2 + k}{\ell} \right) = -1 \) when \( \ell \nmid k \).

Subsequently we shall assume that \( n > v_\ell(T) \). Therefore we only get contributions when \( \ell^{2i} \mid T \) and hence only when \( n > 2i' \), so we only list these cases.

**Proposition 3.2.3** Assume \( i' > 0 \) and \( v_\ell(T) > 0 \). We have that

\[
S_{i,i',n}(T) := \begin{cases} (\ell - 1)\ell^{6n-3(i+3i')-6} (\ell^3 - 1) (\ell^2 + \left( \frac{\ell - 3}{\ell} \right)^2 - 1) & \text{if } n > i' > i, n > 2i \text{ and } \ell^{2i} \mid T \\ (\ell - 1)\ell^{6n-i+3i'}-6 (\ell^3 - 3)\ell^2 & \text{if } i' = i, n > 2i \text{ and } \ell^{2i} \parallel T \\ (\ell - 1)\ell^{6n-i+3i'}-6 (\ell - 1) (\ell^4 + \ell^3 + 2\ell^2 - \ell - 1) & \text{if } i' = i, n > 2i \text{ and } \ell^{2i+1} \mid T \\ (\ell - 1)\ell^{6n-i+3i'}-6 \ell^3 (\ell^2 + \left( \frac{\ell - 3}{\ell} \right)^2 - 1) & \text{if } n > n > 2i \text{ and } \ell^{2i} \mid T \\ 0 & \text{if } \ell^{\min(2i,n)} \nmid T. \end{cases}
\]

**Proof** Using Lemma 3.2.1 it remains to deal with the case of \( n > 2i' \) and compute the sum

\[
C_{i,i',n}(T) := \sum_{t \in (\mathbb{Z}/\ell^{n}\mathbb{Z})^\times} \sum_{s \equiv (t/2)^2 \mod \ell^{2i'}} h_i'(\Delta(t,s))h_i(\Delta(T-t,s))
\]
under the assumption that \( \ell^{2i} | T \). First observe that since discriminants run through all residue classes

\[
\sum_{s \equiv (t/2)^2 (2i')} \left( \frac{\ell^{-2i'} \Delta(t, s)}{\ell} \right) = \sum_{s \equiv (t/2)^2 (2i')} \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right) = 0.
\]

We can therefore ignore the corresponding terms in the expansion of \( h_i'(\Delta(t, s)) \cdot h_i'(\Delta(T - t, s)) \). In what follows, we use crucially that \( \Delta(T - t, s) - \Delta(t, s) = T \cdot \text{(unit)} \) to establish the formulas.

**Case 1** Assume \( i' > i \) and \( \ell^{2i+1} | T \). Since \( \ell^{2i+1} | \Delta(t, s) \) it follows that \( \ell^{2i+1} | \Delta(T - t, s) \) and thus

\[
\ell^2 + \ell \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right) + \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right)^2 - 1 = \ell^2 - 1.
\]

Therefore it follows that

\[
C_{i, i', n}(T) = \sum_{t \in \mathbb{Z}/(\ell)^n} \sum_{y \in \mathbb{Z}/(\ell^{n-2i'})} (\ell^2 - 1) \left( \ell^2 + \left( \frac{y}{\ell} \right) + \left( \frac{y}{\ell} \right)^2 - 1 \right)
= \sum_{t \in \mathbb{Z}/(\ell)^n} (\ell^2 - 1)(\ell^{n-2i' - 1}(\ell^2 - 1) + \ell^{n-2i' - 1}(\ell - 1)\ell^2)
= \sum_{t \in \mathbb{Z}/(\ell)^n} (\ell^2 - 1)\ell^{n-2i' - 1}(\ell^3 - 1)
= (\ell - 1)(\ell^2 - 1)\ell^{2n-2i' - 2}(\ell^3 - 1),
\]

establishing the claim in this case.

**Case 2** Assume \( i = i' \) and \( \ell^{2i+1} | T \). Since \( \ell^{-2i} (\Delta(t, s) - \Delta(T - t, s)) \equiv \ell^{-2i} T \equiv 0 \mod \ell \), we may write

\[
C_{i, i', n}(T) = \sum_{t \in (\mathbb{Z}/(\ell)^n Z)^n} \sum_{s \equiv (t/2)^2 (2i')} \left( \ell^2 + \ell \left( \frac{\ell^{-2i'} \Delta(t, s)}{\ell} \right) + \left( \frac{\ell^{-2i'} \Delta(t, s)}{\ell} \right)^2 - 1 \right)^2
= \sum_{t \in (\mathbb{Z}/(\ell)^n Z)^n} \sum_{y \in \mathbb{Z}/(\ell^{n-2i'})} \left( \ell^2 + \ell \left( \frac{y}{\ell} \right) + \left( \frac{y}{\ell} \right)^2 - 1 \right)^2
= \sum_{t \in (\mathbb{Z}/(\ell)^n Z)^n} \ell^{n-2i' - 1}(\ell^2 - 1)^2 + \ell^{n-2i' - 1}(\ell - 1)(\ell^4 + \ell^2)
= (\ell - 1)\ell^{2n-2i' - 2}(\ell - 1)(\ell^4 + \ell^3 + 2\ell^2 - \ell - 1).
\]

**Case 3** We assume that \( \ell^{2i} \parallel T \). For any unit \( t \) we set \( u_t := \ell^{-2i} T(T - 2t) \), a unit, and examine the contributions to \( C_{i, i', n}(T) \) of the different terms of \( h_i'(\Delta(t, s)) \) ·
$h_i(\Delta(T - t, s))$. We first evaluate the expression

$$
\sum_{t \in (\mathbb{Z}/\ell^n \mathbb{Z})^\times} \sum_{s = (t/2)^2(\ell^{2i'})} \left( \frac{\ell^{-2i'} \Delta(t, s)}{\ell} \right) \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right)
$$

$$
= \sum_{t \in (\mathbb{Z}/\ell^n \mathbb{Z})^\times} \sum_{s = (t/2)^2(\ell^{2i'})} \left( \frac{y}{\ell} \right)^2 \left( \frac{u_t + \ell^{2(i' - i)} y}{\ell} \right),
$$

writing $y$ for $\ell^{-2i'} \Delta(t, s)$. If $i' > i$ this equals $\sum_{y \in \mathbb{Z}/\ell^n - 2i'} \left( \frac{y u_t}{\ell} \right)^2 = 0$. However, if $i' = i$ this becomes:

$$
\sum_{y \in \mathbb{Z}/\ell^n - 2i'} \sum_{t \in (\mathbb{Z}/\ell^n)^\times} \left( \frac{y u_t + y^2}{\ell} \right)
= \sum_{y \in \mathbb{Z}/\ell^n - 2i'} \sum_{t \in (\mathbb{Z}/\ell^n)^\times} \left( \frac{y u_t + y^2}{\ell} \right)
= -\ell^{n-1}
= -\ell^{2n - 2i' - 2} (\ell - 1).
$$

Moreover, observe that the term

$$
\sum_{t \in (\mathbb{Z}/\ell^n)^\times} \sum_{s = (t/2)^2(\ell^{2i'})} \left( \left( \frac{\ell^{-2i'} \Delta(t, s)}{\ell} \right)^2 - 1 \right) \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right) = 0
$$

vanishes, and this also holds after exchanging the roles of $T - t$ and $t$ when $i = i'$. Indeed, for a fixed trace $t$ we have with notations as above:

$$
\sum_{s = (t/2)^2(\ell^{2i'})} \left( \left( \frac{\ell^{-2i'} \Delta(t, s)}{\ell} \right)^2 - 1 \right) \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right)
= \sum_{y \in \mathbb{Z}/\ell^n - 2i'} \left( \left( \frac{y}{\ell} \right)^2 - 1 \right) \left( \frac{u_t + \ell^{2(i' - i)} y}{\ell} \right)
= -\ell^{n-2i' - 1} \left( \frac{u_t}{\ell} \right)
$$

so that summing over $t$ we get

$$
\sum_{t \in (\mathbb{Z}/\ell^n)^\times} -\ell^{n-2i' - 1} \left( \frac{u_t}{\ell} \right) = \sum_{t \in (\mathbb{Z}/\ell^n)^\times} -\ell^{n-2i' - 1} \left( \frac{\ell^{-2i} T}{\ell} \right) = 0.
$$

The remaining terms need to be treated separately depending on whether $i = i'$ or not:
Case 3a First consider the situation when \( i' > i \). Since \( \Delta(T - t, s) - \Delta(t, s) = T(T - 2t) \) we see that \( \ell^{2i} \parallel \Delta(T - t, s) \) and thus

\[
\ell^2 + \ell \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right) + \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right)^2 - 1 = \ell \left( \ell + \left( \frac{\ell^{-2i} \Delta(T - t, s)}{\ell} \right) \right).
\]

Putting everything together we obtain when \( i' > i \) the count

\[
C_{i, i', n}(T) = \sum_{t \in \mathbb{Z}/\ell^n \times \mathbb{Z}/(\ell^2i')^2} \sum_{s \equiv (t/2)^2(\ell^2i')} \ell^4 + \ell^2 \left( \left( \frac{\ell^{-2i} \Delta(t, s)}{\ell} \right)^2 - 1 \right) = (\ell - 1) \ell^{2n - 2i}(\ell^3 - 1).
\]

Case 3b We now assume \( i' = i \). In this case we also remark that for fixed \( t \) with notations as above

\[
\sum_{y \in \mathbb{Z}/(\ell^{n - 2i'})} \left( \left( \frac{y}{\ell} \right)^2 - 1 \right) \left( \left( \frac{y + u_t}{\ell} \right)^2 - 1 \right) = 0
\]

since \( y \equiv 0 \equiv y + u_t \mod \ell \) is impossible, so we get no positive contribution from these terms. We also use:

\[
\sum_{y \in \mathbb{Z}/(\ell^{n - 2i'})} \left( \left( \frac{y}{\ell} \right)^2 - 1 \right) + \left( \left( \frac{y + u_t}{\ell} \right)^2 - 1 \right) = -2\ell^{n - 2i' - 1}.
\]

Eliminating the terms in \( h_{i'}(\Delta(t, s)) \cdot h_t(\Delta(T - t, s)) \) that cancel out, we thereby obtain that

\[
C_{i', i', n}(T) = \sum_{t \in \mathbb{Z}/\ell^n \times \mathbb{Z}/(\ell^{n - 2i'})} \sum_{y \in \mathbb{Z}/(\ell^{n - 2i'})} \left( \ell^4 + \ell^2 \left( \frac{y}{\ell} \right) \left( \frac{u_t + y}{\ell} \right) + \ell^2 \left( \left( \frac{y}{\ell} \right)^2 + \left( \frac{u_t + y}{\ell} \right)^2 - 2 \right) \right) = \ell^4(\ell - 1)\ell^{n - 1}\ell^{n - 2i'} + \ell^2(\ell - 1)(-\ell^{2n - 2i' - 2}) + \ell^2(\ell - 1)\ell^{n - 1}(-2\ell^{n - 2i' - 1}) = (\ell - 1)\ell^{2n - 2i'}(\ell^3 - 3).
\]

The result now follows easily using Lemma 3.2.1.
It remains to count pairs whose sum of traces is $T$ and which are not congruent to scalar matrices.

**Lemma 3.2.4** Assume $\ell | T$, then the number of pairs in $G(\ell^n, T)$ both not congruent to scalar matrices is $S_{0,0,n}(T) := \ell^{6n-6}(\ell - 1)^3 - 3\ell^2 + 1$.

**Proof** The count $S_{0,0,n}(T)$ by Lemma 3.1.1 equals

$$
\sum_{t \in \mathbb{Z}/\ell^n} \sum_{s \in (\mathbb{Z}/\ell^n)^*} \ell^{4n-4} \left( \ell^2 + \ell \left( \frac{\Delta(t,s)}{\ell} \right) + \left( \frac{\Delta(t,s)}{\ell} \right)^2 - 1 \right)^2
\times \left( \frac{\Delta(T - t, s)}{\ell} \right)^2 - 1.
$$

Since $\ell | T$, we have that $\Delta(t,s) \equiv \Delta(T - t, s) \mod \ell$ and we arrive at the count:

$$
S_{0,n}(T) = \ell^{4n-4} \sum_{t \in \mathbb{Z}/\ell^n} \sum_{s \in (\mathbb{Z}/\ell^n)^*} \left( \ell^2 + \ell \left( \frac{\Delta(t,s)}{\ell} \right) + \left( \frac{\Delta(t,s)}{\ell} \right)^2 - 1 \right)^2
\times \left( \frac{\Delta(T - t, s)}{\ell} \right)^2 - 1
= \ell^{4n-4} \sum_{s \in (\mathbb{Z}/\ell^n)^*} \left( \sum_{t^2 \equiv 4s(\ell)} (\ell^2 - 1)^2 + \sum_{t^2 \not\equiv 4s(\ell)} \ell^4 + 2\ell^3 \left( \frac{\Delta(t,s)}{\ell} \right) + \ell^2 \right)
= \ell^{4n-4} \sum_{s \in (\mathbb{Z}/\ell^n)^*} (\ell^{n-1}(\ell^2 - 1)^2 + (\ell - 1)\ell^{n-1}(\ell^4 + \ell^2) + 2\ell^3(-\ell^{n-1}))
= \ell^{6n-6}(\ell - 1)(\ell^5 - \ell^3 - 3\ell^2 + 1).
\quad \square
$$

We can now establish explicit formulas for these local densities:

**Theorem 3.2.5** Let $T \in \mathbb{Z}$ and let $\ell \neq 2$ be a prime so that $v_\ell(T) > 0$.

1. Assume $n \geq v_\ell(T) + 1$. Then the number of $\mathbb{Z}/\ell^n\mathbb{Z}$-points on $GL_2 \times \det GL_2$ consisting of pairs of matrices with sum of traces $T$ equals

$$
|H(\ell^n, T)| = (\ell - 1)\ell^{6n-4v_\ell(T)-9}(\ell^{4v_\ell(T)+3}(\ell^5 - \ell^3 - 3\ell^2 + 1) + 2E(\ell, T) + \delta_2(v_\ell(T))(\ell^4 - \ell)).
$$

2. We have that

$$
\lim_{n \to \infty} \frac{\ell^n |H(\ell^n, T)|}{|H(\ell^n)|} = \frac{\ell^6 - \ell^4 - 3\ell^2 + \ell}{\ell^6 - 2\ell^4 + \ell^2} + \frac{2E(\ell, T) + \delta_2(v_\ell(T))(\ell^4 - \ell)}{\ell^{4v_\ell(T)+4}(\ell^2 - 1)^2},$$

\[ Springer \]
where \( e_\ell(T) = [(v_\ell(T) - 1)/2] \), where \( \delta_2(v_\ell(T)) = 1 \) if \( 2|v_\ell(T) \) and \( \delta_2(v_\ell(T)) = 0 \) otherwise, and where \( E(\ell, T) \in \mathbb{Z}(\ell) \) is given by:

\[
E(\ell, T) = \frac{\ell^3(\ell + 1)(\ell^{4e_\ell(T)+4} - 1) + (\ell^4 + \ell^3 + 2\ell^2 - \ell - 1)(\ell^{4e_\ell(T)} - 1)}{(\ell^2 + 1)(\ell + 1)}.
\]

For instance, we deduce the following counts:

\[
|H(\ell^n, T)| = \begin{cases}
(\ell - 1)\ell^{6n-6}(\ell^5 - \ell^3 - \ell^2 - 1) & \text{when } v_\ell(T) = 1, \\
(\ell - 1)\ell^{6n-8}(\ell^7 - \ell^5 - \ell^4 + \ell^3 - \ell^2 - 1) & \text{when } v_\ell(T) = 2, \\
(\ell - 1)\ell^{6n-13}(\ell^{12} - \ell^{10} - \ell^7 + 3\ell^5 - \ell^3 - 3\ell^2 + 2\ell - 1) & \text{when } v_\ell(T) = 3,
\end{cases}
\]

**Proof** The second assertion follows from the first since

\[
|H(\ell^n) = \ell^{7(n-1)}|G(\ell)| = \ell^{7(n-1)}(\ell - 1)\ell^2(\ell^2 - 1)^2.
\]

To prove the formula for \( H(\ell^n, T) \) we observe that

\[
|H(\ell^n, T)| := 2^{[v_\ell(T)/2]} \sum_{i=0}^{n} \sum_{i' = \max(i+1,1)} S_{i,i',n}(T) + \sum_{i=0}^{[v_\ell(T)/2]} S_{i,i,n}(T).
\]

Recall \( e_\ell(T) = [(v_\ell(T) - 1)/2] \), so that in particular \( n \geq e_\ell(T) + 2 \). We evaluate the sum using Proposition 3.2.3. We compute the term:

\[
\sum_{i=0}^{e_\ell(T)} \sum_{i' = i+1}^{n-1} S_{i,i',n}(T) = e_\ell(T) \sum_{i=0}^{n-1} (\ell - 1)\ell^{6n-6-i}(\ell^3 - 1)(\ell^2 - 1)\ell^{-3i'} \\
= (\ell - 1)\ell^{6n-6}(\ell^3 - 1)(\ell^2 - 1) \sum_{i=0}^{e_\ell(T)} \ell^{-i} \ell^{-3i-3} - \ell^{-3n} \frac{1}{1 - \ell^{-3}} \\
= (\ell - 1)\ell^{6n-6}(\ell^2 - 1) \sum_{i=0}^{e_\ell(T)} (\ell^{-4i} - \ell^{3-3n} \ell^{-i}) \\
= (\ell - 1)\ell^{6n-6}(\ell^2 - 1) \\
\times \left( \frac{\ell^4 - \ell^{-4e_\ell(T)}}{\ell^4 - 1} - \ell^{-3n+3} \frac{\ell - \ell^{-e_\ell(T)}}{\ell - 1} \right) \\
= (\ell - 1)\ell^{6n-6} \frac{\ell^4 - \ell^{-4e_\ell(T)}}{\ell^2 + 1} - \ell^{3n-3}(\ell^2 - 1)(\ell - \ell^{-e_\ell(T)}).
We also compute the remaining terms:

\[
\sum_{i=0}^{e_\ell(T)} S_{i,n,n}(T) = \sum_{i=0}^{e_\ell(T)} (\ell - 1) \ell^{3n-i-6} \ell^3 (\ell^2 - 1)
\]

and also provided \( e_\ell(T) \geq 1 \):

\[
\sum_{i=1}^{e_\ell(T)} S_{i,i,n}(T) = (\ell - 1) \ell^{6n-6} (\ell - 1)(\ell^4 + \ell^3 + 2\ell^2 - \ell - 1) \sum_{i=1}^{e_\ell(T)} \ell^{-4i}
\]

\[
= (\ell - 1) \ell^{6n-9} (\ell^4 + \ell^3 + 2\ell^2 - \ell - 1) \left( \frac{1 - \ell^{-4e_\ell(T)}}{\ell^3 + \ell^2 + \ell + 1} \right).
\]

Finally, when \( v_\ell(T) \) is even we have that \( \ell^{2(e_\ell(T)+1)} \parallel T \) and there are the additional terms to account for:

\[
S_{\ell(T)+1,e_\ell(T)+1,n}(T) + 2 \sum_{i'=\ell(T)+2}^{n-1} S_{\ell(T)+1,i',n}(T) + 2S_{\ell(T)+1,n,n}(T)
\]

\[
= (\ell - 1) \ell^{6n-e_\ell(T)-7} \left( \ell^2(\ell^3 - 3)\ell^{-3(e_\ell(T)+1)} + 2(\ell^3 - 1)\ell^2 \sum_{i'=\ell(T)+2}^{n-1} \ell^{-3i'} + 2\ell^2\ell^{-3n+3} \right)
\]

\[
= (\ell - 1) \ell^{6n-4e_\ell(T)-8}(\ell^3 - 1).
\]

The result follows by adding all the terms and \( S_{0,0,n}(T) \) computed in Lemma 3.2.4.

### 3.3 The prime \( \ell = 2 \)

Throughout this subsection \( \ell = 2 \) as we deal with this remaining case. We will use both notations \( \ell \) and 2 interchangeably for comparison with the odd prime case. This prime requires special treatment. For instance the discriminant plays a crucial role in all of our calculations, but involves a factor of 4. This explains why we have to look modulo 8 in the following result:

**Lemma 3.3.1** Provided \( n \geq 1 \), the number of matrices in \( M_{2 \times 2}(\mathbb{Z}/\ell^n\mathbb{Z}) \) not congruent to scalar of trace and determinant \((t, s)\) is

\[
h_{0,n}(t, s) = \ell^{2n-2} \cdot \begin{cases} 
\ell^2 - 1 & \text{if } \Delta(t, s) \equiv 0 \mod 4, \\
\ell^2 - \ell & \text{if } \Delta(t, s) \equiv 5 \mod 8, \\
\ell^2 + \ell & \text{if } \Delta(t, s) \equiv 1 \mod 8, \\
0 & \text{otherwise.}
\end{cases}
\]
The Lang–Trotter conjecture for products of non-CM elliptic...

Proof This is easily checked for \( n = 1 \) and it suffices to show that there are \( \ell^2 \) lifts from \( \mathbb{Z}/\ell^n\mathbb{Z} \) to \( \mathbb{Z}/\ell^{n+1}\mathbb{Z} \) of trace and determinant congruent to \((t, s)\) modulo \( \ell^{n+1} \). The lifts of a fixed matrix may be written as

\[
\begin{pmatrix} b_0 & c_0 \\ d_0 & e_0 \end{pmatrix} + 2^n \begin{pmatrix} b & c \\ d & e \end{pmatrix}
\]

and we count the classes of \( b, c, d, e \) modulo 2. The trace condition yields \( e \equiv -b \mod \ell \) and the determinant condition yields \( b_0e + be_0 - cd_0 - dc_0 \equiv 0 \mod \ell \) yielding exactly \( \ell^2 \) solutions if and only if \( \begin{pmatrix} b_0 & c_0 \\ d_0 & e_0 \end{pmatrix} \) isn’t a scalar modulo \( \ell \). \( \square \)

We deduce the rest of the counts from Lemma 3.3.1. We summarize the results here:

Proposition 3.3.2 The number of matrices congruent to scalar matrices exactly modulo \( 2^i \) and of trace and determinant \((t, s)\) is, provided \( n \geq 3 \):

1. If \( i < n/2 \)

\[
h_{i,n}(t, s) = \ell^{2n-2-i} .
\]

\[
\begin{cases}
\ell^2 - 1 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 0 \mod 4, \\
\ell^2 - \ell & \text{if } \ell^{-2i} \Delta(t, s) \equiv 5 \mod 8, \\
\ell^2 + \ell & \text{if } \ell^{-2i} \Delta(t, s) \equiv 1 \mod 8, \\
0 & \text{otherwise}.
\end{cases}
\]

2. If \( n > i \geq n/2 + 1 \) then

\[
h_{i,n}(t, s) = \ell^{3n-3i-2} .
\]

\[
\begin{cases}
\ell^3 - 1 & \text{if } \ell^{n+2} | \Delta(t, s), \\
0 & \text{otherwise}.
\end{cases}
\]

3. and the remaining cases:

\[
h_{i,n}(t, s) = \ell^{3n-3i-2} .
\]

\[
\begin{cases}
\ell^2 - 1 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 0 \mod 4, \\
\ell^2 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 1 \mod 4, \\
0 & \text{otherwise}.
\end{cases}
\]

if \( i = n/2 \) as well as if \( i = (n + 1)/2 \)

\[
h_{i,n}(t, s) = \ell^{3n-3i-2} .
\]

\[
\begin{cases}
\ell^2 - 1 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 0 \mod 2, \\
\ell^2 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 1 \mod 2, \\
0 & \text{if } \ell^{2i} \nmid \Delta(t, s).
\end{cases}
\]

Proof We count matrices congruent to scalars exactly modulo \( 2^i \) of trace/det \((t, s)\), so of the form

\[
aI + 2^i \begin{pmatrix} b & c \\ d & e \end{pmatrix}.
\]
where \( \begin{pmatrix} b & c \\ d & e \end{pmatrix} \in S_0(n - i) \) are matrices not congruent to scalar in \( \mathbb{Z}/2^{n-i}\mathbb{Z} \) and \( a \in \mathbb{Z}/2^i\mathbb{Z} \). The trace \( t \) must be even and there are now two choices for \( a \) mod \( 2^i \) such that \( 2a \equiv t \) mod \( 2^i \) which are congruent modulo \( 2^{i-1} \). We must have for any choice of \( a \):
\[
\begin{align*}
2^{2i}(be - dc) &\equiv a^2 - at + s \quad \text{mod } \ell^n \text{ (det. condition),} \\
2^i(b + e) &\equiv t - 2a \quad \text{mod } \ell^n \text{ (trace condition).} 
\end{align*}
\]

First, observe that solving the determinant condition yields two choices of \( a \) congruent modulo \( 2^i \), whereas the trace condition yields two choices congruent modulo \( 2^{i-1} \). Thus when \( i < n/2 \) there is a unique \( a \) mod \( 2^i \) such that both conditions are satisfied, and this happens if and only if \( 2^{2i} \mid \Delta(t, s) \). Relating the discriminant of trace \( \tilde{t} = b + e \) and determinant \( \tilde{s} = be - dc \) of this new matrix to \( \Delta(t, s) \) one also has that:
\[
2^{2i}(\tilde{t}^2 - 4\tilde{s}) \equiv (t - 2a)^2 - 4(a^2 - at + s) \equiv \Delta(t, s) \mod 2^n.
\]

When \( i < n/2 \) we deduce the following count:
\[
\ell^{2n-2-i} \cdot \begin{cases} 
\ell^2 - 1 & \text{if } 2^{-2i} \Delta(t, s) \equiv 0 \mod 4, \\
\ell^2 - \ell & \text{if } 2^{-2i} \Delta(t, s) \equiv 5 \mod 8, \\
\ell^2 + \ell & \text{if } 2^{-2i} \Delta(t, s) \equiv 1 \mod 8, \\
0 & \text{otherwise.}
\end{cases}
\]

This follows from Lemma 3.3.1 as \( \tilde{t} \) is a fixed class mod \( 2^{n-i} \) and \( \tilde{s} \) has to be a fixed class mod \( 2^{n-2i} \), which yields \( 2^i \) choices for \( \tilde{s} \). So the count is \( 2^i h_{0,n-i}(\tilde{t}, \tilde{s}) \) as claimed.

Now let us consider the case of \( i \geq n/2 \). The determinant condition yields
\[
2^{2i} \tilde{s} = a^2 - at + s \\
\equiv 1/4(t - 2^i \tilde{t})^2 - t/2(t - 2^i \tilde{t}) + s \\
\equiv -t^2/4 - 2^{i-1} t \tilde{t} + 2^{i-1} t \tilde{t} + s + 2^{2i-2} \tilde{t}^2 \\
\equiv -\Delta(t, s)/4 + 2^{2i-2} \tilde{t}^2 \mod 2^n
\]

If \( i \geq n/2 + 1 \), this is equivalent to \( 2^{n+2} \mid \Delta(t, s) \). In this case for each of the two solutions for \( a \) mod \( 2^i \) we get that \( \tilde{t} \) mod \( 2^{n-i} \) is 0 or 1, respectively and \( \tilde{s} \) runs through all the classes modulo \( 2^{n-i} \). Summing over all possibilities and keeping track of \( \Delta(\tilde{t}, \tilde{s}) \mod 8 \) as in Lemma 3.3.1 we obtain:
\[
\ell^{2(n-i)-2} \cdot \begin{cases} 
\ell^{n-i}(\ell^2 - 1) + \ell^{n-i}(\ell^2) & \text{if } \ell^{n+2} \mid \Delta(t, s), \\
0 & \text{otherwise,}
\end{cases}
\]

as claimed.
It remains to treat the case of $i = [(n + 1)/2]$ when we still need to work modulo $\ell^{n+2}$. Since $\ell^2 \Delta(\tilde{t}, \tilde{s}) \equiv \Delta(t, s) \pmod{\ell^{n+2}}$ we get a trivial count if $\ell^2 \nmid \Delta(t, s)$. If $n$ is even then $i = n/2$, and we have $\Delta(\tilde{t}, \tilde{s}) \equiv \ell^{-n} \Delta(t, s) \pmod{4}$. Since $\Delta(t, s)$ doesn’t see if $\Delta(\tilde{t}, \tilde{s})$ is 1 or 5 modulo 8 we just get the average of those two counts for $h_{0,n-i}(\tilde{r}, \tilde{s})$, as there is no condition on $\tilde{s} \in \mathbb{Z}/\ell^{n-i}\mathbb{Z}$:

$$\ell^{3n-3i-2} \cdot \begin{cases} \ell^2 - 1 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 0 \pmod{4}, \\ \ell^2 & \text{if } \ell^{-2i} \Delta(t, s) \equiv 1 \pmod{4}, \\ 0 & \text{otherwise}. \end{cases}$$

Finally if $n$ is odd, then $i = (n + 1)/2$ and $\Delta(\tilde{t}, \tilde{s}) \equiv \ell^{-n} \Delta(t, s) \pmod{2}$. We get the count:

$$\ell^{3n-3i-2} \cdot \begin{cases} \ell^2 - 1 & \text{if } 2^{-2i} \Delta(t, s) \equiv 0 \pmod{2}, \\ \ell^2 & \text{if } 2^{-2i} \Delta(t, s) \equiv 1 \pmod{2}, \\ 0 & \text{if } 2^i \nmid \Delta(t, s) \end{cases}$$

where now again $\tilde{s}$ can vary in $\mathbb{Z}/\ell^{n-i}\mathbb{Z}$ and we get a similar average. \hfill $\Box$

## 4 The exceptional factor

This section is devoted to the study of the factor at the **conductor $m_A$** of the open subgroup $\text{Im}(\rho_A) \subseteq \hat{G}(\hat{\mathbb{Z}})$ where again we just take throughout this section $A = E_1 \times E_2$. Recall that $m_A$ is defined as the least integer $m$ such that, in the diagram

$$\xymatrix{ \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ar[r]^{\rho_A} & \hat{G}(\hat{\mathbb{Z}}) \ar[d]^{\text{red}} \ar[dl]_{\bar{\rho}_{A,m}} \ar[r] & G(m), }$$

we have $\text{Im}(\rho_A) = \text{red}^{-1} H_A(m)$, keeping with our notations of $G = \text{GL}_2 \times_{\text{det}} \text{GL}_2$ and $H_A(m) = \text{Im}(\bar{\rho}_{A,m})$. In particular, we would like to compute the stable factor

$$\frac{m_{A,T} |H_A(m_{A,T}, T)|}{|H_A(m_{A,T})|}$$

that appears in Conjecture 1.0.5. In general, it is difficult to compute this factor systematically and we have seen it can even vanish depending on the trace $T$. However, we will be able to compute it in the case when $\rho_A$ has image as large as possible in $\hat{G}(\hat{\mathbb{Z}})$:

**Definition 4.0.1** A pair $(E_1, E_2)$ of elliptic curves over $\mathbb{Q}$ is a **Serre pair** if the image of $\rho_{E_1 \times E_2}$ has index 4 in $G(\hat{\mathbb{Z}})$. 

$\square$ Springer
In particular, since the image of $\rho_{E_i}$ in $GL_2(\mathbb{Z})$ has index at least 2, each individual elliptic curve $E_i$ must have maximal possible image, ergo must be a Serre curve. It has been shown by the second author [16,17] that almost all (ordered by height) elliptic curves and pairs of curves over $\mathbb{Q}$ are Serre curves or Serre pairs, respectively.

This image of $\rho_{E_i}$ is going to be by definition the full preimage under red : $GL_2(\mathbb{Z}) \rightarrow GL_2(\mathbb{Z}/m_E\mathbb{Z})$ of an index two subgroup of $GL_2(\mathbb{Z}/m_E\mathbb{Z})$. We briefly characterize this subgroup, following [15, Section 3]: Since the discriminant of the elliptic curve has a concrete expression as a symmetric polynomial in the coordinates of the 2-torsion of $E$, it is easy to see that any element of the Galois group $\sigma \in Gal(E[2])$ has to act on $\sqrt{\Delta_E}$ via the unique non-trivial quadratic character of $GL_2(\mathbb{Z}/2\mathbb{Z})$, which we denote by $\epsilon : GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \rightarrow \{\pm 1\}$, so we have that:

$$\sigma(\sqrt{\Delta_E}) = \epsilon(\sigma)\sqrt{\Delta_E}$$

and $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2])$. By class field theory, we also have the containment $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_{D_E})$ for some primitive root of unity $\zeta_{D_E}$ of order $D_E$. Since the conductor of the quadratic field $\mathbb{Q}(\sqrt{\Delta_E})$ is the absolute value of its discriminant (for instance by the Führerdiskriminantenproduktformel), we have that

$$D_E = \begin{cases} \lvert \Delta_{sf} \rvert & \text{if } \Delta_{sf} \equiv 1 \mod 4, \\ 4\lvert \Delta_{sf} \rvert & \text{otherwise} \end{cases}$$

with $\Delta_{sf}$ denoting the squarefree part of the discriminant $\Delta_E$ of the elliptic curve. Letting now $m_E := \text{lcm}(D_E, 2)$ so that the field $\mathbb{Q}(E[m_E])$ is the compositum of $\mathbb{Q}(E[D_E])$ and $\mathbb{Q}(E[2])$, we must have that for $\sigma \in Gal(E[m_E])$:

$$\sigma(\sqrt{\Delta_E}) = \left(\frac{\Delta_{sf}}{\det \sigma}\right) \cdot \sqrt{\Delta_E},$$

using the Kronecker symbol. Therefore, for any elliptic curve $E$, the image of $\tilde{\rho}_{E,m_E} \subseteq GL_2(\mathbb{Z}/m_E\mathbb{Z})$ is contained in the index two subgroup $\text{ker}(\epsilon(\cdot) \left(\frac{\Delta_{sf}}{\det(\cdot)}\right))$. Moreover, $E$ is a Serre curve if and only if this subgroup is exactly the image of $\tilde{\rho}_{E,m_E}$ and $m_E$ is the conductor of the open subgroup $\text{Im}(\rho_E) \subseteq GL_2(\mathbb{Z})$.

Considering now pairs of elliptic curves and the abelian surface $A = E_1 \times E_2$, we get therefore an obstruction to the Galois representation on torsion having full image in the group $G(\mathbb{Z})$ for $G = GL_2 \times_{\det} GL_2$. Namely, considering the compositum $L = \mathbb{Q}(E_1[D_1]) \cdot \mathbb{Q}(E_2[D_2]) \cdot \mathbb{Q}((E_1 \times E_2)[2])$, we must have for $\sigma \in Gal(L)$:

$$\sigma(\sqrt{\Delta_{E_i}}) = \left(\frac{\Delta_{E_i,sf}}{\det \sigma}\right) \cdot \sqrt{\Delta_{E_i}}$$

for $i = 1, 2$. We remark that even though each individual elliptic curve is a Serre curve, there could be additional obstructions coming from entanglements between the division fields of the $E_i$. However, since this obstruction forces the image of $\rho_A$ to lie
in an index 4 subgroup of $G(\hat{\mathbb{Z}})$, for Serre pairs this has to be the only obstruction. Therefore, setting

$$m_A := \text{lcm}(m_{E_1}, m_{E_2}) = \text{lcm}(2, D_{E_1}, D_{E_2}),$$

$m_A$ is precisely the integer we called the conductor of the open subgroup $\text{Im}(\rho_A) \subseteq G(\hat{\mathbb{Z}})$ so that the image of $\bar{\rho}_{A,m_A} \subseteq G(m_A)$ is the index 4 subgroup $\ker(\psi : G(m_A) \rightarrow \{\pm 1\}^2)$ for

$$\psi(g) = (\varepsilon(g^{(1)}), \varepsilon(g^{(2)}), \frac{\Delta_{E_1,sf}}{\det(g^{(1)})}, \frac{\Delta_{E_2,sf}}{\det(g^{(2)})}),$$

where $g = (g^{(1)}, g^{(2)})$ denote the projections onto each $GL_2$-factor of $G$. The preimage of this subgroup under projection is the full image of $\rho_A$ inside $G(\hat{\mathbb{Z}})$. The next subsection is devoted to computing the relevant counts for Serre curves. We conclude this discussion by providing pairs of Serre curves which are not Serre pairs, showing that entanglements between division fields are indeed a prevalent issue.

**Proposition 4.0.2** There are infinitely many pairs $(E_1, E_2)$ of elliptic curves over $\mathbb{Q}$ for which each $E_i$ is a Serre curve but which, nevertheless, do not constitute a Serre pair.

**Proof** We prove this by exhibiting an explicit family. Such examples may be found via the following strategy: fix an explicit Serre curve $E_1/\mathbb{Q}$. One may then construct explicit families of elliptic curves with the same mod $n$ Galois representation for some $n$. Clearly any Serre curve $E_2$ in that family will then produce an abelian surface $A = E_1 \times E_2$ with $\bar{\rho}_{A,n}(G_\mathbb{Q})$ of index at least $|\text{SL}_2(\mathbb{Z}/n\mathbb{Z})|$ in $G(\mathbb{Z}/n\mathbb{Z})$. It remains to show that such a Serre curve can be found in the family, but one certainly expects most elliptic curves in such a family to be Serre curves. Concretely, Cojocaru, Grant and Jones show in the main result of [6] that for a non-isotrivial elliptic curve $E/\mathbb{Q}(t)$, a positive proportion of specializations are Serre curves, provided the Galois representation associated to $E$ is sufficiently large. Namely, they require that

$$[\text{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \text{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t))]=1.$$}

Moreover, they show [6, Proposition 4] that to prove full Galois image it suffices to show that $\mathbb{Q}(t)(\sqrt{\Delta_E}) \cap \mathbb{Q} = \mathbb{Q}$ and that

$$\text{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) = \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \text{ for } n \in \{36, 5, 7, 11, 13\}.$$}

The latter condition will be automatically satisfied if we start with a Serre curve $E_1$ where no primes $l \geq 5$ are exceptional and where $n = 36$ is not exceptional (meaning that the Galois representation modulo $n$ has image $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$). There are infinitely many such examples in [8]. Finally, checking non-isotriviality and that adjoining the square-root of the discriminant is geometric is straightforward for explicit families. Concretely, one may for instance take the Serre curve $E_1 : y^2 + xy = x^3 + 3$ and consider the family of elliptic curves with isomorphic Galois module $E[4]$ as given
explicitly in [27, Theorem 4.1.] to obtain such an infinite family of Serre curves $E_2$ such that $E_1, E_2$ is not a Serre pair.

\[\square\]

### 4.1 Computing the factor at $m_A$

The main result of this subsection, Proposition 4.1.1, can be in particular used to compute the quantity $|H_A(m_{A,T}, T)|$ appearing in Conjecture 1.0.5 in the case of Serre pairs, via our previous considerations.

It will be convenient to fix some additional notations here: we will be calculating the size of a certain subset of $G(m)$, where $m$ is a composite number, and this will utilize the Chinese Remainder Theorem. As such, we choose to reserve subscripts for the Chinese Remainder Theorem decomposition and superscripts for the decomposition inherent in $G = GL_2 \times \det GL_2$, i.e. we will use the following notation for $g \in G(m)$:

$$G(m) := GL_2(\mathbb{Z}/m\mathbb{Z}) \times \det GL_2(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_{\ell^a} GL_2(\mathbb{Z}/\ell^a\mathbb{Z}) \times \det GL_2(\mathbb{Z}/\ell^a\mathbb{Z})$$

$$g \leftrightarrow (g^{(1)}, g^{(2)}) \leftrightarrow \prod_{l|m} \left( \begin{array}{c} g_1^{(1)} \\ g_1^{(2)} \end{array} \right).$$

Let $D_1$ and $D_2$ be the discriminants of the quadratic fields $\mathbb{Q}(\sqrt{\Delta_{E_i}})$ for $i = 1, 2$. Since $(E_1, E_2)$ is a Serre pair, it follows that for $A = E_1 \times E_2$, we have $m_A = \text{lcm}(2, |D_1|, |D_2|)$. Let $m \in \mathbb{N}$ be any positive integer satisfying

$$m_A | m | m_A^\infty.$$

Let $\chi^{(i)}(\cdot) := \left( \frac{D_i}{\cdot} \right)$ denote the Kronecker symbol, and regard each character $\chi^{(i)}$ as a function on $(\mathbb{Z}/m\mathbb{Z})^\times$, which as before we further extend to a character on the group $GL_2(\mathbb{Z}/m\mathbb{Z})$ by pre-composing with the determinant map, i.e. we set $\chi^{(i)}(g) := \chi^{(i)}(\det g)$. We recall that $\varepsilon : GL_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \{\pm 1\}$ denotes the unique non-trivial character of order 2, viewed as a function on $GL_2(\mathbb{Z}/m\mathbb{Z})$ by first reducing modulo 2. Finally, we consider for general $m_A | m | m_A^\infty$ the map

$$\psi : G(m) \rightarrow \{\pm 1\}^2$$

defined by $\psi(g) := (\psi^{(1)}(g^{(1)}), \psi^{(2)}(g^{(2)})) \in \{\pm 1\}^2$ with $\psi^{(i)}(g) := \varepsilon(g) \cdot \chi^{(i)}(g) \in \{\pm 1\}$. We will use the abbreviation

$$G(m, T)_{\psi=1} := \{g \in G(m, T) : \psi(g) = 1\}, \quad (1.1)$$

and by our previous considerations it is precisely the size of this set when $m$ is divisible enough by any prime $\ell | m_A$ that we ultimately wish to evaluate.

---

1 We apologize for the abuse of notation here; in general when $\psi$ is a Dirichlet character of conductor dividing $m$, its domain will sometimes be regarded as $(\mathbb{Z}/m\mathbb{Z})^\times$ and sometimes as $GL_2(\mathbb{Z}/m\mathbb{Z})$, via pre-composing with determinant.
Write $m = 2^α m'$ where $α ≥ 1$ and $m'$ is odd and define the odd part of the discriminant $D_i$ to be

$$D'_i := \text{gcd}(m', D_i).$$ \quad (1.2)$$

We may write a decomposition $ψ = ψ_2 · ψ_{m'}$, where $ψ_{m'}^{(i)} := \left(\frac{m'}{|D'_i|}\right)$ and $ψ_2^{(i)}$ is a character modulo 8. The size $|G(m, T)ψ=1|$ depends somewhat on whether or not the characters $ψ_{m'}^{(1)}$ and $ψ_{m'}^{(2)}$ are equal, or, equivalently, whether or not $|D'_1| = |D'_2|$. In the following proposition, we denote:

$$e_ℓ(T) := \lceil (v_ℓ(T) - 1)/2 \rceil, \quad δ_n(m) := \begin{cases} 1 & \text{if } n \text{ divides } m, \\ 0 & \text{otherwise}, \end{cases}$$

$$E(ℓ, T) := \frac{ℓ^3(ℓ + 1)(ℓ^4ε(ℓ)+4 - 1) + (ℓ^4 + ℓ^3 + 2ℓ^2 + ℓ - 1)(ℓ^4ε(ℓ) - 1)}{(ℓ^2 + 1)(ℓ + 1)},$$

$$A_ℓ(T) := \begin{cases} ℓ^5 - ℓ^3 - ℓ^2 + 1 + \frac{2E(ℓ,T)}{ℓ^4ε(ℓ)+2} + δ_2(v_ℓ(T))\frac{(ℓ^3 - 1)}{ℓ^4ε(ℓ)+2} & \text{if } ℓ | T, \\ (ℓ^6 - ℓ^5 - 2ℓ^4 + ℓ^3 + 2ℓ^2)/(ℓ - 1) & \text{if } ℓ \nmid T, \end{cases}$$

$$B_ℓ(T) := \begin{cases} -3ℓ^2 + 1 + \frac{2E(ℓ,T)}{ℓ^4ε(ℓ)+2} + δ_2(v_ℓ(T))\frac{(ℓ^3 - 1)}{ℓ^4ε(ℓ)+2} & \text{if } ℓ | T, \\ ℓ^2/(ℓ - 1) & \text{if } ℓ \nmid T. \end{cases}$$ \quad (1.3)

$$σ_ψ_2(T) := \left| G \left( 2v_2(m), T \right) \right|_{\text{Im } ψ_2 \subseteq \text{Im } ψ_{m'}},$$

$$σ_ψ_2^{(i)}(T) := \left| G \left( 2v_2(m), T \right) \right|_{\text{Im } ψ_2^{(i)} \subseteq \text{Im } ψ_{m'}}^{ψ_2^{(i)} = 1} - \left| G \left( 2v_2(m), T \right) \right|_{\text{Im } ψ_2^{(i)} = -1}^{ψ_2^{(i)} = -1}.$$

Proposition 4.1.1 Assume the notation just outlined and let $T \in \mathbb{Z} - \{0\}$ be arbitrary. Assume that $m$ is large enough so that for all primes $ℓ | m_A$ we have $v_ℓ(m) > v_ℓ(T)$. In case $|D'_1| ≠ |D'_2|$, the quantity $|G(m, T)ψ=1|$ is equal to

$$\frac{(m')^{5}φ(m')}{4 (\text{rad}(m'))^5} \left( σ_ψ_2(T) \prod_{ℓ|m'} (A_ℓ(T) + 1) + 2^{ω(\frac{m'}{|D'_i|})} σ_ψ_2^{(1)}(T) \prod_{ℓ|D'_i} B_ℓ(T) + 2^{ω(\frac{m'}{|D'_2|})} σ_ψ_2^{(2)}(T) \prod_{ℓ|D'_2} B_ℓ(T) \right).$$

In case $|D'_1| = |D'_2| = D'$, $|G(m, T)ψ=1|$ is equal to

$$\frac{(m')^{5}φ(m')}{2 (\text{rad}(m'))^5} \left( σ_ψ_2(T) \prod_{ℓ|m'} (A_ℓ(T) + 1) + 2^{ω(\frac{m'}{D'})} σ_ψ_2^{(1)}(T) \prod_{ℓ|D'} B_ℓ(T) \right).$$
By (1.1), we find that

\[
\left| G(m, T)_{\psi=1} \right| = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^2} \left| \text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\psi^{(1)}=1} \times \text{det} \text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\psi^{(2)}=1} \right|
\]

\[
= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^2} \sum_{d \in (\mathbb{Z}/m\mathbb{Z})^\times} \left| \text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\psi^{(1)}=1} \right| \cdot \left| \text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\psi^{(2)}=1} \right|.
\]

(1.4)

Recall that \( m = 2^\alpha m' \) where \( \alpha \geq 1 \) and \( m' \) is odd, and likewise that \( D_i' \) is odd part of \( D_i \). As noted above, we may write \( \psi^{(i)} \) as a product \( \psi^{(i)}_{2} \cdot \psi^{(i)}_{m'} \), where \( \psi^{(i)}_{m'} \) factors through the determinant map. Thus, the condition \( \psi^{(i)}(g^{(i)}) = 1 \) is equivalent to \( \psi^{(i)}_{2}(g^{(i)}) = \psi^{(i)}_{m'}(\det(g^{(i)})) \). We will split the sum in (1.4) according to the common value of \( \psi^{(i)}_{2} \) and \( \psi^{(i)}_{m'} \), i.e. we consider the map

\[
\psi_{m'} : (\mathbb{Z}/m\mathbb{Z})^\times \to \{\pm 1\}^2,
\]

and, for fixed \( t \in (\mathbb{Z}/m\mathbb{Z})^2 \), we write the inner sum in (1.4) as

\[
\sum_{v \in \text{Im } \psi_{m'}} \sum_{d \in (\mathbb{Z}/m\mathbb{Z})^\times} \left| \text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\psi^{(1)}_{m'}=v^{(1)}} \right| \cdot \left| \text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\psi^{(2)}_{m'}=v^{(2)}} \right|.
\]

(1.5)

Since \( \psi^{(i)}_{m'}(\cdot) = \left( \cdot, \frac{1}{|D_i'|} \right) \) is simply the Jacobi symbol, we see that the image \( \text{Im } \psi_{m'} \subseteq \{\pm 1\}^2 \) satisfies

\[
\text{Im } \psi_{m'} = \begin{cases} \{(1, 1), (-1, -1)\} & \text{if } |D_1'| = |D_2'|, \\ \{\pm 1\}^2 & \text{otherwise}. \end{cases}
\]

We now wish to further analyze each factor \( i = 1, 2 \) in each summand in (1.4). We may write \( \psi^{(i)}_{m'}(\cdot) = \prod_{\ell | m'} \psi^{(i)}_{\ell}(\cdot) \) where, for an odd prime \( \ell \), we set

\[
\psi^{(i)}_{\ell}(\cdot) := \begin{cases} \left( \frac{\cdot}{\ell} \right) & \text{if } \ell \mid D_i', \\ 1 & \text{if } \ell \nmid D_i'. \end{cases}
\]

(1.6)

Consider now the Chinese Remainder Isomorphism

\[
\text{GL}_2(\mathbb{Z}/m\mathbb{Z})_{\text{det}=d} \cong \text{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})_{\text{det}=d_\ell} \times \prod_{\ell | m'} \text{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})_{\text{det}=d_\ell},
\]

(1.7)
where \( t_1^{(i)}, d_1, d_2 \) (resp. \( t_2^{(i)}, d_2 \)) denote the reductions of \( t^{(i)}, d \) modulo \( \ell^{\alpha \ell} \) (resp. modulo \( 2^{\alpha} \)). Since for any prime \( \ell \), the characters \( \psi_\ell^{(i)} \) factor through the \( \ell \)-primary part in the decomposition \( (1.7) \), we obtain with notations as above the factorization

\[
\psi^{(i)}_\ell(g^{(i)}) = \psi^{(i)}_2(g^{(i)}_2) \prod_{\ell \mid m'} \psi^{(i)}_\ell(\det(g^{(i)}_\ell)).
\]

(We have isolated the prime 2 in \( (1.7) \) because it is the only prime \( \ell \) for which \( \psi^{(i)}_\ell \) does not factor through the determinant map.) Thus, for a fixed \( v = (v^{(1)}, v^{(2)}) \in \text{Im} \, \psi_{m'} \), the inner sum of \( (1.5) \) becomes

\[
\left( \sum_{d_2 \in (\mathbb{Z}/2^{\alpha} \mathbb{Z})^{\times}} f_{\psi_2, v}(t_2, d_2) \right) \left( \sum_{(v_1^{(i)}, v_2^{(i)}) \in \{\pm 1\}^{\ell \mid m'}} \left( \prod_{\ell \mid \text{gcd}(D_1', D_2')} f_\ell(t_\ell, d_\ell) \right) \right),
\]

(1.8)

where we have introduced the notation

\[
f_{\psi_2, v}(t_2, d_2) := \prod_{i=1}^{2} \left| \text{GL}_2(\mathbb{Z}/2^{\alpha} \mathbb{Z})^{\text{tr} = v^{(i)}_2} \right|^{\psi_\ell_2(\cdot) = v^{(i)}_\ell(\cdot)} \left| \text{det} = d_2 \right|^{\psi_\ell(\cdot) = v^{(i)}_\ell(\cdot)}
\]

and

\[
f_\ell(t_\ell, d_\ell) := \prod_{i=1}^{2} \left| \text{GL}_2(\mathbb{Z}/\ell^{\alpha \ell} \mathbb{Z})^{\text{tr} = v^{(i)}_\ell} \right|^{\psi_\ell(\cdot) = v^{(i)}_\ell(\cdot)} \left| \text{det} = d_\ell \right|.
\]

(1.9)

Noting the condition

\[
\psi^{(i)}_\ell(d_\ell) = v^{(i)}_\ell \quad (i = 1, 2)
\]

(1.10)

in the inner sum above and considering \( (1.6) \), we see that this sum becomes an empty sum exactly when either some prime \( \ell \) does not divide \( D_1' \) and \( v^{(i)}_\ell = -1 \), or when some prime \( \ell \) divides both \( D_1 \) and \( D_2 \) and \( v^{(1)}_\ell \neq v^{(2)}_\ell \). Thus, we may impose the conditions

\[
v^{(i)}_\ell = 1 \quad \text{whenever} \quad \ell \nmid D_1',
\]

\[
v^{(1)}_\ell = v^{(2)}_\ell \quad \text{whenever} \quad \ell \mid \text{gcd}(D_1', D_2')
\]

(1.11)

in the outer sum without affecting the expression. Further noting that

\[
\begin{align*}
\psi^{(1)}_\ell(\cdot) &= \psi^{(2)}_\ell(\cdot) = \left( \frac{\cdot}{\ell} \right) \quad \text{if} \, \ell \mid D_1' \text{ and } \ell \mid D_2', \\
\psi^{(1)}_\ell(\cdot) &= 1 \quad \text{and} \quad \psi^{(2)}_\ell(\cdot) = \left( \frac{\cdot}{\ell} \right) \quad \text{if} \, \ell \mid D_1' \text{ and } \ell \nmid D_2', \\
\psi^{(1)}_\ell(\cdot) &= \left( \frac{\cdot}{\ell} \right) \quad \text{and} \quad \psi^{(2)}_\ell(\cdot) = 1 \quad \text{if} \, \ell \mid D_1' \text{ and } \ell \nmid D_2'.
\end{align*}
\]
we see that, for each \( \ell \mid m' \), the conditions (1.10) and (1.11) are equivalent to

\[
\psi^{(i \ell)}(d_{\ell}) = v^{(i \ell)}_{\ell},
\]

where \( i_{\ell} \in \{1, 2\} \) is any number for which \( \ell \mid D'_{i_{\ell}} \) (in the ambiguous case that \( \ell \mid D'_{i} \) for each \( i \), one may take either 1 or 2 for \( i_{\ell} \) since the value of \( \psi^{(i_{\ell})}_{\ell} \) is well-defined). We may thus replace the outer sum in (1.8) with a sum over \( \{\pm 1\}^{(\ell | m')} \), obtaining that (1.8) is equal to

\[
\left( \sum_{d_2 \in (\mathbb{Z}/2^a \mathbb{Z})^\times} f_{\psi_{2}, \nu}(t_2, d_2) \right) \prod_{(v_{\ell}) \in \{\pm 1\}^{(\ell | m')} \sum_{d_2 \in (\mathbb{Z}/\ell^a \mathbb{Z})^\times} \prod_{\psi_{\ell}(d_{\ell}) = v_{\ell}} f_{\ell}(t_{\ell}, d_{\ell}),
\]

(1.12)

where now \( \psi_{\ell} \) simply denotes the Legendre symbol. We insert this back into (1.5) and then further into (1.4), obtaining that (1.4) is equal to

\[
\sum_{t \in (\mathbb{Z}/m \mathbb{Z})^2} \sum_{\nu \in \text{Im} \psi_{m'}} \left( \sum_{d_2 \in (\mathbb{Z}/2^a \mathbb{Z})^\times} f_{\psi_{2}, \nu}(t_2, d_2) \right) \prod_{(v_{\ell}) \in \{\pm 1\}^{(\ell | m')} \sum_{d_2 \in (\mathbb{Z}/\ell^a \mathbb{Z})^\times} \prod_{\psi_{\ell}(d_{\ell}) = v_{\ell}} f_{\ell}(t_{\ell}, d_{\ell})
\]

(1.13)

\[
= \sum_{v \in \text{Im} \psi_{m'}} \left( \sum_{t_2 \in (\mathbb{Z}/2^a \mathbb{Z})^2} f_{\psi_{2}, \nu}(t_2, d_2) \right) \sum_{(v_{\ell}) \in \{\pm 1\}^{(\ell | m')} \sum_{t_2 \in (\mathbb{Z}/\ell^a \mathbb{Z})^2} \prod_{\psi_{\ell}(d_{\ell}) = v_{\ell}} f_{\ell}(t_{\ell}, d_{\ell}).
\]

The following lemma aids in evaluating the above summand. We recall the following notation:

\[
e_{\ell}(T_{\ell}) := [(v_{\ell}(T_{\ell}) - 1)/2], \quad \delta_n(m) := \begin{cases} 
1 & \text{if } n \text{ divides } m, \\
0 & \text{otherwise},
\end{cases}
\]

\[
E(\ell, T_{\ell}) := \frac{\ell^3(\ell + 1)(\ell^4e_{\ell}(T_{\ell}) + 4 - 1) + (\ell^4 + \ell^3 + 2\ell^2 + \ell - 1)(\ell^4e_{\ell}(T_{\ell}) - 1)}{(\ell^2 + 1)(\ell + 1)},
\]

\[
A_{\ell}(T_{\ell}) := \begin{cases} 
\ell^5 - \ell^3 - 3\ell^2 + 1 + \frac{2E(\ell, T_{\ell})}{\ell^4e_{\ell}(T_{\ell}) + 3} + \delta_2(v_{\ell}(T_{\ell}))(\ell^3 - 1) / (\ell^4 + 2) & \text{if } \ell \mid T_{\ell}, \\
(\ell^5 - \ell^3 - 3\ell^2 + 1 + \frac{2E(\ell, T_{\ell})}{\ell^4e_{\ell}(T_{\ell}) + 3} + \delta_2(v_{\ell}(T_{\ell}))(\ell^3 - 1) / (\ell^4 + 2)) & \text{otherwise},
\end{cases}
\]

\( \subseteq \) Springer
\[ B_\ell(T_\ell) := \begin{cases} 
-3t^2 + 1 + \frac{2E(\ell, T_\ell)}{\ell^{4\ell(T_\ell)+1}} + \delta_2(v_\ell(T_\ell)) \frac{(\ell^3-1)}{\ell^{4\ell(T_\ell)+2}} & \text{if } \ell \mid T_\ell, \\
(\ell^2)/(\ell - 1) & \text{if } \ell \nmid T_\ell. 
\end{cases} \quad (1.14) \]

**Lemma 4.1.2** Let \( \ell \) be an odd prime, let \( t_\ell \in (\mathbb{Z}/\ell^a\mathbb{Z})^2 \) and \( d_\ell \in (\mathbb{Z}/\ell^a\mathbb{Z})^\times \), and let \( f_\ell(t_\ell, d_\ell) \) be as defined in (1.9). Assume that \( \alpha_\ell > v_\ell(T_\ell) \). We have

\[
\sum_{t_\ell \in (\mathbb{Z}/\ell^a\mathbb{Z})^2} f_\ell(t_\ell, d_\ell) = \frac{\ell^5\alpha_\ell - 5\varphi(\ell^a)}{2} [A_\ell(T_\ell) + v_\ell B_\ell(T_\ell)],
\]

where \( \varphi \) denotes the Euler phi function and \( A_\ell(T_\ell) \) and \( B_\ell(T_\ell) \) are as in 1.14.

**Proof** We let \( F(-1, T_\ell) \) denote the sum above when \( v_\ell = -1 \) and put \( n = \alpha_\ell \).

It suffices to compute \( F(-1, T_\ell) \), since the result may then be deduced by setting \( A_\ell(T_\ell) = \frac{|G(\ell^n, T_\ell)|}{2(\ell-1)^{\ell n+4}} \) and \( B_\ell(T_\ell) = A_\ell(T_\ell) - \frac{2F(-1, T_\ell)}{(\ell-1)^{\ell n+6}} \). The computation of \( |G(\ell^n, T_\ell)| \) can then be read off from Theorem 3.2.5 when \( \ell \mid T_\ell \) and Lemma 2.2.9 otherwise.

To compute \( F(-1, T_\ell) \), observe that if \( d_\ell \mod \ell \) is a non-square the discriminant \( t_\ell^2 - 4d_\ell \mod \ell \) never vanishes and therefore we are counting only matrices which are not congruent to scalars modulo \( \ell \). Hence applying Lemma 3.1.1 with \( i = 0 \) we obtain:

\[
F(-1, T_\ell) = \sum_{t_\ell \in (\mathbb{Z}/\ell^a\mathbb{Z})^2} \sum_{d_\ell \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} \ell^{4n-2} \left( \ell + \left( \frac{(t_\ell^{(1)})^2 - 4d_\ell}{\ell} \right) \right) \times \left( \ell + \left( \frac{(t_\ell^{(2)})^2 - 4d_\ell}{\ell} \right) \right).
\quad (1.15)
\]

We have for any \( T_\ell \) the equality

\[
\sum_{t_\ell \in (\mathbb{Z}/\ell^n\mathbb{Z})^2} \sum_{d_\ell \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} \left( \frac{(t_\ell^{(1)})^2 - 4d_\ell}{\ell} \right) + \left( \frac{(T_\ell - t_\ell^{(1)})^2 - 4d_\ell}{\ell} \right) = -\ell^{n-1} (\ell - 1)
\quad (1.16)
\]

by exchanging the summation order and using from Lemma 3.2.2 that for any \( T \in \mathbb{Z} \) and prime \( \ell \nmid 2d_\ell \):

\[
\sum_{t_\ell \in (\mathbb{Z}/\ell^a\mathbb{Z})} \left( \frac{(T - t_\ell)^2 - 4d_\ell}{\ell} \right) = -1.
\]
To compute the quantity in equation 1.15, it remains to evaluate the expression

\[ P(T\ell,\ell) := \sum_{t^{(1)}_\ell \in \mathbb{Z}/\ell^n\mathbb{Z}, d\ell \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} \sum_{\psi(d\ell) = -1} \left( \frac{(t^{(1)}_\ell)^2 - 4d\ell}{\ell} \right) \cdot \left( \frac{(T_\ell - t^{(1)}_\ell)^2 - 4d\ell}{\ell} \right). \]

Observe that for any unit \( u \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \), we have \( P(u \cdot T_\ell, \ell) = P(T_\ell, \ell) \) provided \( \ell \nmid T_\ell \), whereas we trivially obtain \( P(0, \ell) = \ell^{2n-1}(\ell - 1)/2 \). Moreover, we may write

\[
\sum_{T_\ell=0}^{\ell^n-1} P(T_\ell, \ell) = \sum_{d\ell \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} \left( \sum_{t^{(1)}_\ell \in \mathbb{Z}/\ell^n\mathbb{Z}} \frac{t^{(1)}_\ell^2 - 4d\ell}{\ell} \right)^2
\]

\[
= \sum_{d\ell \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} (-\ell^{n-1})^2
\]

\[
= \ell^{3(n-1)}(\ell - 1)/2.
\]

We deduce therefore that

\[
P(T_\ell, \ell) = \begin{cases} 
\ell^{2n-1}(\ell - 1)/2 & \text{if } \ell | T_\ell, \\
-\ell^{2(n-1)}(\ell - 1)/2 & \text{else.}
\end{cases} \tag{1.17}
\]

Putting everything together, we obtain from equations (1.15), (1.16) and (1.17) the count:

\[
F(-1, T_\ell) = \ell^{6n-4} \cdot (\ell - 1)/2 \cdot \begin{cases} 
\ell^3 - \ell & \text{if } \ell | T_\ell, \\
\ell^3 - 2\ell - 1 & \text{else.}
\end{cases}
\]

The result now follows by simple calculation from our previous considerations. \qed

Inserting the result of the lemma into (1.13), we obtain

\[
|G(m, T)|_{\psi=1} = \frac{(m')^5 \varphi(m')}{2\omega(m') (\text{rad}(m'))^5} \sum_{v \in \text{Im} \psi_{m'}} S\psi_2(T_2, v)
\times \sum_{(v_\ell) \in \{\pm 1\}^{|\ell(m')\ell|} \ell|m'} \prod_{1 \leq i^{'}, v_{\ell} = v(i')} (A_{\ell}(T_\ell) + v_\ell B_{\ell}(T_\ell)), \tag{1.18}
\]

\[ \hat{\text{Springer}} \]
where

\[ S_{\psi_2}(T_2, v) := \sum_{\substack{t_2 \in (\mathbb{Z}/2^n \mathbb{Z})^2 \\ \ell_1^{(2)} + t_2 \equiv T_2 \\ d_2 \in (\mathbb{Z}/2^n \mathbb{Z})^3}} f_{\psi_2, v}(t_2, d_2). \]

Formally expanding out the innermost product of binomials and reversing summation, we observe that

\[
\sum_{(v_\ell) \in \{\pm 1\}^{\ell|m'|}} \prod_{\ell \mid \ell|m'} \psi_2(t_\ell, d_\ell) = \sum_{S \subseteq \ell|m'} \sum_{(v_\ell) \in \{\pm 1\}^{\ell|m'}} \left( \prod_{\ell \in S} A_\ell + \prod_{\ell \in S^c} v_\ell \prod_{\ell \in S} B_\ell \right).
\]

In the sum over \((v_\ell)\) on the second term \(\prod_{\ell \in S} v_\ell \prod_{\ell \in S^c} B_\ell\), we have perfect cancellation unless \(S = \{\ell \mid D_1'\} \) or \(S = \{\ell \mid D_2'\}\). Thus we have

\[
\sum_{(v_\ell) \in \{\pm 1\}^{\ell|m'|}} \prod_{\ell \mid \ell|m'} (A_\ell + v_\ell B_\ell)
\]

\[
= \begin{cases} 
2^{\omega(m') - 2} \left( \prod_{\ell \mid \ell|m'} (A_\ell + 1) + v^{(1)} \prod_{\ell \mid D_1'} B_\ell + v^{(2)} \prod_{\ell \mid D_2'} B_\ell \right) & \text{if } |D_1'| \neq |D_2'|, \\
2^{\omega(m') - 1} \left( \prod_{\ell \mid \ell|m'} (A_\ell + 1) + v^{(1)} \prod_{\ell \mid D_1'} B_\ell \right) & \text{if } |D_1'| = |D_2'|.
\end{cases}
\]

Inserting this back into (1.18), we find that our original expression (1.4) is equal to

\[
\begin{cases} 
\frac{(m')^5 \varphi(m')}{4 \left( \text{rad}(m') \right)^5} \left[ \sum_{\ell|m'} \left( S_{\psi_2}(T_2) \prod_{\ell \mid \ell|m'} (A_\ell + 1) + S_{\psi_2}(T_2) \prod_{\ell \mid D_1'} B_\ell \right) \right] + S_{\psi_2}(T_2) B_\ell & \text{if } |D_1'| \neq |D_2'|, \\
\frac{(m')^5 \varphi(m')}{2 \left( \text{rad}(m') \right)^5} \left[ \sum_{\ell|m'} \left( S_{\psi_2}(T_2) \prod_{\ell \mid \ell|m'} (A_\ell + 1) \right) \right] + S_{\psi_2}(T_2) B_\ell & \text{if } |D_1'| = |D_2'|.
\end{cases}
\]

(1.19)
where we have used the fact that
\[
\mathcal{G}_{\psi_2}(T_2) := \sum_{\nu \in \text{Im } \psi_{m'}} S_{\psi_2}(T_2, \nu),
\]
\[
\mathcal{G}^{(i)}_{\psi_2}(T_2) := \sum_{\nu \in \text{Im } \psi_{m'}} v^{(i)} S_{\psi_2}(T_2, \nu).
\]

This concludes the proof of the proposition. \( \square \)

We now establish formulas which lead to an explicit evaluation of the terms \( \mathcal{G}_{\psi_2}(T_2) \) and \( \mathcal{G}^{(i)}_{\psi_2}(T_2) \) above. To that end, recall that we have set
\[
\psi^{(i)}(\cdot) = \varepsilon(\cdot) \left( \frac{D_i}{\det(\cdot)} \right) \cdot \left( \frac{\det(\cdot)}{|D'_i|} \right).
\]

By quadratic reciprocity, this yields the following cases for \( \psi^{(i)}(\cdot) \) when \( i = 1, 2 \):

\[
\psi^{(i)}_2(g) = \begin{cases} 
\varepsilon(g) & \text{if } D_i \equiv 1 \mod 4, \\
\varepsilon(g) \cdot \chi_4(\det(g)) & \text{if } D_i = 4D'_i \text{ and } D'_i \equiv 3 \mod 4, \\
\varepsilon(g) \cdot \chi_8(\det(g)) & \text{if } D_i = 4D'_i \text{ and } D'_i \equiv 2 \mod 8, \\
\varepsilon(g) \cdot \chi_4 \chi_8(\det(g)) & \text{if } D_i = 4D'_i \text{ and } D'_i \equiv 6 \mod 8,
\end{cases}
\] (1.20)

where the characters \( \chi_4 \) and \( \chi_8 \) are the characters modulo 4 and 8 respectively defined by \( \chi_4(x) = \left( \frac{-1}{x} \right) \) and \( \chi_8(x) = \left( \frac{2}{x} \right) \) for odd integers \( x \). In the following lemma we also set
\[
e(n, t, d) := \min \left\{ \left\lceil \frac{n}{2} \right\rceil, \left\lfloor \frac{v_2(t^2 - 4d)}{2} \right\rfloor \right\}.
\] (1.21)

Furthermore, for any set of formulas \( S \), we abbreviate by \( \delta(S) \) the truth indicator of \( S \):
\[
\delta(S) := \begin{cases} 
1 & \text{if every formula in } S \text{ is true}, \\
0 & \text{otherwise}.
\end{cases}
\]

Finally, we will employ the abbreviations
\[
\Delta = \Delta(t, d) := t^2 - 4d, \quad v = v(t, d, n) := \begin{cases} 
v_2(\Delta(t, d)) & \text{if } \Delta(t, d) \neq 0 \\
v + 2 & \text{if } \Delta(t, d) = 0.
\end{cases}
\] (1.22)
Lemma 4.1.3 Let \( t, d \in \mathbb{Z} \) with \( d \) odd, let \( \Delta \in \mathbb{Z} \) and \( v \in \mathbb{Z}_{\geq 0} \) be defined by (1.22) and let \( e(n, t, d) \) be defined by (1.21). The quantity \(|\text{GL}_2(\mathbb{Z}/2^n \mathbb{Z})_{\text{det}=d}\rangle\) is equal to

\[
2^{2n-1} \left( 1 - 2^{-e(n,t,d)} \right) + \delta \left( \begin{array}{l}
v < n, \ n \in 2\mathbb{Z}, \\
\Delta/2^v \equiv 0, 1 \pmod{4}
\end{array} \right) 2^{2n-2-v/2} \left( 4 + 2 \chi_8 \left( \Delta/2^v \right) \right) \\
+ \delta \left( \begin{array}{l}
v \geq n, \ n \in 2\mathbb{Z}, \\
\Delta/2^n \equiv 0, 1 \pmod{4}
\end{array} \right) 2^{3n/2-2} \left( 3 + \chi_4 \left( \Delta/2^n \right) \right) \\
+ \delta \left( \begin{array}{l}
v \geq n+1, \ n \notin 2\mathbb{Z}
\end{array} \right) 2^{3(n-3)/2} \left( 7 - (-1)^{\Delta/2^{n+1}} \right) \\
+ \delta (v \geq n+2) 2^{3n-3[n/2]+2}.
\]

Proof This follows from Proposition 3.3.2.

The next lemma is the result of a tedious computation, making repeated use of Proposition 3.3.2.

Lemma 4.1.4 Distinguishing cases as in 1.20 we obtain the following counts at the prime 2:

If \( \psi_2 = \epsilon \) and \( n \geq 1 \), then we have

\[
|\text{GL}_2(\mathbb{Z}/2^n \mathbb{Z})_{\text{det}=d}^{\psi_2=-1}| = \begin{cases} 
3 \cdot 4^{n-1} & \text{if } t \text{ is even}, \\
0 & \text{if } t \text{ is odd}.
\end{cases}
\]

If \( \psi_2 = \epsilon \chi_4 \) and \( n \geq 3 \), then we have

\[
|\text{GL}_2(\mathbb{Z}/2^n \mathbb{Z})_{\text{det}=d}^{\psi_2=-1}| = \begin{cases} 
3 \cdot 4^{n-1} & \text{if } t \text{ is even and } \chi_4(d) = 1, \\
2 \cdot 4^{n-1} & \text{if } t \text{ is odd and } \chi_4(d) = -1, \\
3 \cdot 4^{n-1} & \text{if } t \equiv d + 1 \pmod{8} \text{ and } \chi_4(d) = -1, \\
4^{n-1} & \text{if } t \equiv d + 5 \pmod{8} \text{ and } \chi_4(d) = -1, \\
0 & \text{otherwise}.
\end{cases}
\]

If \( \psi_2 = \epsilon \chi_8 \) and \( n \geq 5 \), then we have
\[
\left| \text{GL}_2(\mathbb{Z}/2^n\mathbb{Z})_{\text{det} \equiv d}^{\text{tr} \equiv t}_{\psi_2 = -1} \right| = \begin{cases} 
3 \cdot 4^n - 1 & \text{if } t \text{ is even and } \chi_8(d) = 1, \\
2 \cdot 4^n - 1 & \text{if } t \text{ is odd and } \chi_8(d) = -1, \\
3 \cdot 4^n - 1 & \text{if } t \equiv 4 \mod 8 \text{ and } d \equiv 3 \mod 8, \\
1 \cdot 4^n - 1 & \text{if } t \equiv 0 \mod 8 \text{ and } d \equiv 3 \mod 8, \\
6 \cdot 4^n - 2 & \text{if } t \equiv 2 \mod 8 \text{ and } d \equiv t + 3 \mod 16, \\
6 \cdot 4^n - 2 & \text{if } t \equiv 6 \mod 8 \text{ and } d \equiv t + 7 \mod 16, \\
\left[10 + 2\chi_8 \left( \frac{\Delta}{16} \right) \right] \cdot 4^n - 2 & \text{if } t \equiv 2 \mod 8 \text{ and } d \equiv t - 5 \mod 16, \\
\left[10 + 2\chi_8 \left( \frac{\Delta}{16} \right) \right] \cdot 4^n - 2 & \text{if } t \equiv 6 \mod 8 \text{ and } d \equiv t - 1 \mod 16, \\
0 & \text{otherwise.} 
\end{cases}
\]

Finally, if \( \psi_2 = \varepsilon \chi_8 \chi_4 \) and \( n \geq 5 \), then we have

\[
\left| \text{GL}_2(\mathbb{Z}/2^n\mathbb{Z})_{\text{det} \equiv d}^{\text{tr} \equiv t}_{\psi_2 = -1} \right| = \begin{cases} 
3 \cdot 4^n - 1 & \text{if } t \text{ is even and } \chi_8(d) \chi_4(d) = 1, \\
2 \cdot 4^n - 1 & \text{if } t \text{ is odd and } \chi_8(d) \chi_4(d) = -1, \\
3 \cdot 4^n - 1 & \text{if } t \equiv 0 \mod 8 \text{ and } d \equiv 7 \mod 8, \\
1 \cdot 4^n - 1 & \text{if } t \equiv 4 \mod 8 \text{ and } d \equiv 7 \mod 8, \\
6 \cdot 4^n - 2 & \text{if } t \equiv 2 \mod 8 \text{ and } d \equiv t + 3 \mod 16, \\
6 \cdot 4^n - 2 & \text{if } t \equiv 6 \mod 8 \text{ and } d \equiv t + 7 \mod 16, \\
\left[10 + 2\chi_8 \left( \frac{\Delta}{16} \right) \right] \cdot 4^n - 2 & \text{if } t \equiv 2 \mod 8 \text{ and } d \equiv t - 5 \mod 16, \\
\left[10 + 2\chi_8 \left( \frac{\Delta}{16} \right) \right] \cdot 4^n - 2 & \text{if } t \equiv 6 \mod 8 \text{ and } d \equiv t - 1 \mod 16, \\
0 & \text{otherwise.} 
\end{cases}
\]

We remark that Lemmas 4.1.3 and 4.1.4 result in explicit evaluations of

\[
\left| \text{GL}_2(\mathbb{Z}/2^n\mathbb{Z})_{\text{det} \equiv d}^{\text{tr} \equiv t}_{\psi_2 = \pm 1} \right|.
\]
These evaluations, in turn, lead to an evaluation of the quantities $S_{\psi^2}(T)$ and $S^{(i)}_{\psi^2}(T)$, via the formulas

$$S_{\psi^2}(T) = \sum_{v \in \text{Im } \psi^m} \sum_{t \in (\mathbb{Z}/2^\alpha \mathbb{Z})^2} \prod_{i=1}^{2} \begin{vmatrix} \text{GL}_2(\mathbb{Z}/2^\alpha \mathbb{Z})_T \equiv d \mod 2^\alpha \\ \psi^{(i)}_2 = v^{(i)} \end{vmatrix},$$

$$S^{(i)}_{\psi^2}(T) = \sum_{v \in \text{Im } \psi^m} v^{(i)} \sum_{t \in (\mathbb{Z}/2^\alpha \mathbb{Z})^2} \prod_{i=1}^{2} \begin{vmatrix} \text{GL}_2(\mathbb{Z}/2^\alpha \mathbb{Z})_T \equiv d \mod 2^\alpha \\ \psi^{(i)}_2 = v^{(i)} \end{vmatrix}. (1.23)$$

Finally, by virtue of Proposition 4.1.1, the evaluation of these quantities leads to an explicit evaluation of the factor at $m_{E_1 \times E_2}$ (the conductor of the open subgroup $\text{Im}(\rho_{E_1 \times E_2}) \subseteq G(\mathbb{Z})$) of the constant appearing in Conjecture 1.0.5. The other factors, as presented in Theorem 1.0.6, have already been previously computed in Sect. 3.

## 5 Numerical evidence

We now present the results of some computations geared towards gathering evidence for Conjecture 1.0.5. The results of the previous sections provide explicit formulas for the constants appearing therein when $E_1 \times E_2$ is a Serre pair, summarized in Theorem 1.0.6. Using the computational packages MAGMA and SageMath, we worked with the explicit family of Serre pairs found in [9], wherein it is shown that, for primes $\ell_1, \ell_2$ satisfying

$$\ell_1, \ell_2 \not\in \{2, 7\}, \quad \gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1, \quad (1.1)$$

the elliptic curves

$$E_{\ell_1} : y^2 + xy = x^3 + \ell_1,$$
$$E_{\ell_2} : y^2 + xy = x^3 + \ell_2 \quad (1.2)$$

form a Serre pair. We note that each $E_{\ell_i}$ has discriminant $\Delta_{\ell_i} = -432\ell_i^2 - \ell_i$. With all of this in hand, we computed a whole range of examples for distinct primes $(\ell_1, \ell_2)$ satisfying (1.1). We computed the actual count

$$\pi_{E_{\ell_1} \times E_{\ell_2}, T}(x) := \# \{ p \leq x : p \nmid N_{E_{\ell_1}} N_{E_{\ell_2}}, \ a_p(E_{\ell_1}) + a_p(E_{\ell_2}) = T \} \quad (1.3)$$

for $x = 10^7$ and all non-zero integers $T$ in the Hasse interval $|T| \leq 4\sqrt{x}$. Furthermore, for all such non-zero $T$, we computed a value closely related to the one predicted by
Conjecture 1.0.5. In the spirit of the computations carried out in [3], we calculated the value

$$\pi_{E_3 \times E_{11}, T}^{\text{pred}}(x) := \frac{C(E_1 \times E_2, T)}{2\Phi(0)} \int_{\max\{2, (T/2g)^2\}}^{x} \Phi\left(\frac{T}{\sqrt{t}}\right) \frac{1}{2\sqrt{t} \log t} \, dt,$$  \hspace{0.5cm} (1.4)
The Lang–Trotter conjecture for products of non-CM elliptic... 431

which is asymptotic to what is predicted by Conjecture 1.0.5 for fixed $T$ as $x \to \infty$ but which is more accurate when $T$ is on the scale of $\sqrt{x}$ (see Remark 2.1.6). Furthermore, we computed the absolute error $\mathcal{E}_{E_{\ell_1} \times E_{\ell_2}, T}(x)$, relative error $\mathcal{E}^{\text{rel}}_{E_{\ell_1} \times E_{\ell_2}, T}(x)$ and the “Central Limit Theorem error” $\mathcal{E}^{\text{CLT}}_{E_{\ell_1} \times E_{\ell_2}, T}(x)$, defined respectively by

$$
\mathcal{E}^{\text{abs}}_{E_{\ell_1} \times E_{\ell_2}, T}(x) := \pi_{E_{\ell_1} \times E_{\ell_2}, T}(x) - \pi^{\text{pred}}_{E_{\ell_1} \times E_{\ell_2}, T}(x),
$$
Fig. 7 $\pi_{E_{31} \times E_{107}, T}^{\text{actual}} (10^7)$

Fig. 8 $\pi_{E_{79} \times E_{107}, T}^{\text{abs}} (10^7)$

Fig. 9 $\pi_{E_{79} \times E_{107}, T}^{\text{pred}} (10^7)$

$\mathcal{E}_{E_{t_1} \times E_{t_2}, T}^{\text{rel}} (x) := \frac{\pi_{E_{t_1} \times E_{t_2}, T}^{\text{actual}} (x) - \pi_{E_{t_1} \times E_{t_2}, T}^{\text{pred}} (x)}{\pi_{E_{t_1} \times E_{t_2}, T}^{\text{pred}} (x)}$, 

$\mathcal{E}_{E_{t_1} \times E_{t_2}, T}^{\text{CLT}} (x) := \frac{\pi_{E_{t_1} \times E_{t_2}, T}^{\text{actual}} (x) - \pi_{E_{t_1} \times E_{t_2}, T}^{\text{pred}} (x)}{\sqrt{\pi_{E_{t_1} \times E_{t_2}, T}^{\text{pred}} (x)}}$. 

$\mathcal{E}$ Springer
The Lang–Trotter conjecture for products of non-CM elliptic... 433

Fig. 10 $\pi_{E_{79} \times E_{107}, T}^{\text{actual}}(10^7)$

Fig. 11 $E_{abs}^{E_{79} \times E_{107}, T}(10^7)$

With all of the results in this paper, such computations should be easily reproducible and we present here a few representative examples for the Serre pairs $E_3 \times E_{11}$, $E_{31} \times E_{107}$, and $E_{79} \times E_{107}$. For the first pair, we display data plots for the sets

$$\left\{ \left( T, \pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{pred}}(x) \right) : |T| \leq 4\sqrt{x} \right\},$$

$$\left\{ \left( T, \pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{actual}}(x) \right) : |T| \leq 4\sqrt{x} \right\},$$

and similarly for each of the error functions in (1.5); for the latter two pairs, we only display such data for $\pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{pred}}(x)$, for $\pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{actual}}(x)$ and for absolute error $E_{E_{\ell_1} \times E_{\ell_2}, T}(x)$ (see Figs. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11).

In each case, there are various “stripes” appearing in our prediction $\pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{pred}}(10^7)$, corresponding to values of $T$ lying in certain residue classes modulo 12. As may be seen in the numerical evidence presented in [3], similar stripes are also present in the analogous plot of the points $\left\{ \left( T, \pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{pred}}(x) \right) : |T| \leq 2\sqrt{x} \right\}$ associated to the original Lang–Trotter conjecture for fixed trace $T$ involving a single elliptic curve $E$. In that case stripes also emerge in the actual data $\left\{ \left( T, \pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{actual}}(x) \right) : |T| \leq 2\sqrt{x} \right\}$. By
contrast, in the plots associated to pairs of elliptic curves we computed, the stripes appearing in the predictions are situated closer to one another, and the statistical noise present in the actual data causes them to “blur together” and no longer be visible in the plots of $\pi_{E_{79} \times E_{107}, T}^{\text{actual}}(10^7)$. To remedy this and further validate our conjectural constants $c(E_{\ell_1} \times E_{\ell_2}, T)$, we additionally exhibit rainbow-colored graphs for the Serre pair $E_{79} \times E_{107}$ (see Figs. 12 and 13), in which data points are colored according to their greatest common divisor with 12, as detailed in the following table.

| $\gcd(T, 12)$ | Color of $\left(T, \pi_{E_{\ell_1} \times E_{\ell_2}, T}^{\text{actual}}(10^7)\right)$ |
|---------------|-----------------------------------------------|
| 1             | Red                                           |
| 3             | Orange                                        |
| 2             | Yellow                                        |
| 4 or 6        | Green                                         |
| 12            | Blue                                          |

The reason for the appearance of $\gcd(T, 12)$ here is that the local factor of our constant at a prime $\ell$ is larger when $\ell$ divides $T$ than when $\ell$ does not divide $T$ (see Lemma 2.2.9,
Theorem 3.2.5 and Proposition 4.1.1). Furthermore, the difference in size between the factor when $\ell \mid T$ versus when $\ell \nmid T$ is most dramatic when $\ell$ is small, and decreases very quickly as $\ell$ grows. Because of this, the primes 2 and 3 account for the stripes in our prediction. The color coding of the stripes in the rainbow graphs allows us to observe a more precise agreement between the predicted and actual data in this regard, giving yet more credence to the conjectural constants $c(E_{\ell_1} \times E_{\ell_2}, T)$.

Acknowledgements We would like to express our thanks to Alina Carmen Cojocaru and Andrew Sutherland for pointing us toward this project and engaging in enlightening discussions, and to the organizers of the Arizona Winter School for providing the stimulating environment where the research was initiated. We would also like to thank Daniel Miller and Gabor Wiese for helpful conversations on some aspects of this paper. Finally, we would like to thank the anonymous referee for carefully reading the manuscript and offering several helpful comments.

References

1. Akbary, A., Parks, J.: On the Lang-Trotter conjecture for two elliptic curves. Ramanujan J. 49(3), 585–623 (2019). https://doi.org/10.1007/s11139-018-0050-7
2. Baier, S., Patankar, V.M.: Applications of the square sieve to a conjecture of Lang and Trotter for a pair of elliptic curves over the rationals. In: Geometry, Algebra, Number Theory, and Their Information Technology Applications. vol. 251. Springer Proc. Math. Stat. Springer, Cham, pp. 39–57 (2018). https://doi.org/10.1007/978-3-319-97379-1_3
3. Baier, S., Jones, N.: A refined version of the Lang-Trotter conjecture. Int. Math. Res. Not. 2009 (2008). https://doi.org/10.1093/imrn/rnn136
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. 24.3-4 (1997). Computational Algebra and Number Theory (London, 1993), pp. 235–265. https://doi.org/10.1006/jsco.1996.0125
5. Cojocaru, A.-C., Davis, R., Silverberg, A., Stange, K.E.: Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre). Int. Math. Res. Not. IMRN 12, 3557–3602 (2017). https://doi.org/10.1093/imrn/rnw058
6. Cojocaru, A.-C., Grant, D., Jones, N.: One-parameter families of elliptic curves over Q with maximal Galois representations. Proc. Lond. Math. Soc. 103(4), 654–675 (2011). https://doi.org/10.1112/plms/pdr001
7. Cojocaru, A.C., Jones, N., Serban, V., Wang, T.: Bounds for distributions of Frobenius traces on abelian varieties with small Sato-Tate group (in preparation)
8. Daniels, H.B.: An infinite family of Serre curves. J. Number Theory 155, 226–247 (2015). https://doi.org/10.1016/j.jnt.2015.03.016
9. Daniels, H.B., Hatley, J., Ricci, J.: Elliptic curves with maximally disjoint division fields. Acta Arith. 175(3), 211–223 (2016)
10. David, C., Pappalardi, F.: Average Frobenius distributions of elliptic curves. Int. Math. Res. Not. 4, 165–183 (1999). https://doi.org/10.1155/S1073792899000082
11. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ. 14, 197–272 (1941). https://doi.org/10.1007/BF02940746
12. Fité, F., Kedlaya, K.S., Rotger, V., Sutherland, A.V.: Sato-Tate distributions and Galois endomorphism modules in genus 2. Compos. Math. 148(5), 1390–1442 (2012). https://doi.org/10.1112/S0010437X12000279
13. Foucry, E., Marty, M.R.: On the distribution of supersingular primes. Can. J. Math. 48(1), 81–104 (1996). https://doi.org/10.4153/CJM-1996-004-7
14. Harris, M.: Potential automorphy of odd-dimensional symmetric powers of elliptic curves and applications. In: Algebra, Arithmetic, and Geometry: In Honor of Yu. I. Manin, vol. II. vol. 270. Progr. Math. Birkhäuser Boston, Inc., Boston, pp. 1–21 (2009). https://doi.org/10.1007/978-0-8176-4747-6_1
15. Jones, N.: Averages of elliptic curve constants. Math. Ann. 345(3), 685–710 (2009). https://doi.org/10.1007/s00208-009-0373-1
16. Jones, N.: Almost all elliptic curves are Serre curves. Trans. Am. Math. Soc. 362(3), 1547–1570 (2010). https://doi.org/10.1090/S0002-9947-09-04804-1
17. Jones, N.: Pairs of elliptic curves with maximal Galois representations. J. Number Theory 133(10), 3381–3393 (2013). https://doi.org/10.1016/j.jnt.2013.03.002
18. Katz, N.M.: Lang-Trotter revisited. Bull. Am. Math. Soc. 46(3), 413–457 (2009). https://doi.org/10.1090/S0273-0979-09-01257-9
19. Lagarias, J.C., Odlyzko, A.M.: Effective versions of the Chebotarev density theorem. In: Algebraic Number Fields: L-Functions and Galois Properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464 (1977)
20. Lang, S., Trotter, H.: Frobenius Distributions in GL2-Extensions. Lecture Notes in Mathematics, vol. 504. Springer, Berlin (1976)
21. Murty, V.K.: Frobenius distributions and Galois representations. In: Automorphic Forms, Automorphic Representations, and Arithmetic (Fort Worth, TX, 1996), vol. 66. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, pp. 193–211 (1999)
22. Oesterlé, J.: Réduction modulo $p^n$ des sous-ensembles analytiques fermés de $\mathbb{Z}_p^N$. Invent. Math. 66(2), 325–341 (1982). https://doi.org/10.1007/BF01389398
23. Ribet, K.: On $\ell$-adic representations attached to modular forms. Invent. Math. 28, 245–275 (1975). https://doi.org/10.1007/bf01425561
24. Rubin, K., Silverberg, A.: Mod 2 representations of elliptic curves. Proc. Am. Math. Soc. 129, 53 (1999). https://doi.org/10.2307/2649028
25. Serre, J.-P.: Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. Invent. Math. 15(4), 259–331 (1972)
26. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Etudes Sci. Publ. Math. 54, 323–401 (1981)
27. Silverberg, A.: Explicit families of elliptic curves with prescribed mod N representations. In: Modular Forms and Fermat’s Last Theorem (Boston, MA, 1995), pp. 447–461. Springer, New York (1997)
28. The LMFDB Collaboration. The L-Functions and Modular Forms Database (2013). http://www.lmfdb.org. Accessed 16 Sept 2013
29. The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.0) (2020). https://www.sagemath.org

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.