Bounds for the distribution of the Frobenius traces associated to a generic abelian variety

Alina Carmen Cojocaru and Tian Wang

Abstract. Let \( g \geq 1 \) be an integer and let \( A \) be an abelian variety defined over \( \mathbb{Q} \) and of dimension \( g \). Assume that, for each sufficiently large prime \( \ell \), the image of the residual modulo \( \ell \) Galois representation of \( A \) is isomorphic to \( \text{GSp}_{2g}(\mathbb{Z}/\mathbb{Z}) \). For an integer \( t \) and a positive real number \( x \), denote by \( \pi_A(x, t) \) the number of primes \( p \leq x \), of good reduction for \( A \), for which the Frobenius trace \( a_1,p(A) \) associated to the reduction of \( A \) modulo \( p \) equals \( t \). Assuming the Generalized Riemann Hypothesis for Dedekind zeta functions, we prove that \( \pi_A(x, 0) \ll_A x^{1 - \frac{1}{2g^2 + g + 1}}/(\log x)^{1 - \frac{2}{2g^2 + g + 1}} \) and that \( \pi_A(x, t) \ll_A x^{1 - \frac{1}{2g^2 + g + 2}}/(\log x)^{1 - \frac{2}{2g^2 + g + 2}} \) if \( t \neq 0 \). These bounds largely improve upon those obtained by J-P. Serre in 1981 for \( g = 1 \) and by A.C. Cojocaru, R. Davis, A. Silverberg, and K.E. Stange for \( g \geq 2 \) in 2017. They may be viewed as generalizations to arbitrary \( g \) of the bounds obtained for \( g = 1 \) by M.R. Murty, V.K. Murty and N. Saradha in 1988, combined with a refinement in the power of \( \log x \) obtained by D. Zywina in 2015. Under the assumptions stated above, we also prove the existence of a density one set of primes \( p \) satisfying \( |a_1,p(A)| > p^{\frac{1}{g+2}}/(\log p)^\varepsilon \) for any fixed \( \varepsilon > 0 \). Assuming, in addition to the Generalized Riemann Hypothesis for Dedekind zeta functions, Artin’s Holomorphy Conjecture and a Pair Correlation Conjecture for Artin L-functions, we prove that \( \pi_A(x, 0) \ll_A x^{1 - \frac{1}{g+1}}/(\log x)^{1 - \frac{1}{g+1}} \) and that \( \pi_A(x, t) \ll_A x^{1 - \frac{1}{g+2}}/(\log x)^{1 - \frac{1}{g+2}} \) if \( t \neq 0 \), and we deduce the existence of a density one set of primes \( p \) satisfying \( |a_1,p(A)| > p^{\frac{1}{g+2}} \) for any fixed \( \varepsilon > 0 \). These are currently the best known conditional upper bounds for \( \pi_A(x, t) \) and the best known conditional lower bounds for \( |a_1,p(A)| \), for most primes \( p \).

1. Introduction

In 1976, Lang and Trotter \cite{LaTr76} proposed a prime distribution problem, which remains open, in the setting of elliptic curves. Known as the Lang-Trotter Conjecture on Frobenius traces, the problem aims to understand the reduction type of a given elliptic curve defined over the field of rational numbers. It may be described in terms of the distribution of Frobenius elements in an infinite family of Galois number fields derived from the given elliptic curve. This description may then be generalized to prime distribution
problems related to compatible systems of Galois representations, such as those associated to modular forms and those associated to higher dimensional abelian varieties. For example, such generalizations were proposed in [AkPa19], [BaGo97], [ChJoSe20], [CoDaSiSt17], [Ka09], and [Mu99]. The goal of our paper is to prove results related to the generalization of the Lang-Trotter Conjecture on Frobenius traces formulated in [CoDaSiSt17] in the setting of generic abelian varieties defined over \( \mathbb{Q} \), as explained below.

Let \( A \) be an abelian variety defined over \( \mathbb{Q} \), of dimension \( g \geq 1 \), and of conductor \( N_A \). For a rational prime \( \ell \), consider the group representation obtained from the action of the absolute Galois group \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) on the \( \ell \)-adic Tate module \( T_\ell(A) \) of \( A \). Recalling that there is an isomorphism of \( \mathbb{Z}_\ell \)-modules \( T_\ell(A) \cong \mathbb{Z}_\ell(\mathbb{Z}_\ell)^{2g} \) and fixing a \( \mathbb{Z}_\ell \)-basis of \( T_\ell(A) \), we obtain a Galois representation

\[
\rho_{A,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_{2g}(\mathbb{Z}_\ell),
\]

which we call the \( \ell \)-adic Galois representation of \( A \). Taking the projection of \( \text{GL}_{2g}(\mathbb{Z}_\ell) \) onto \( \text{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \), we obtain a Galois representation

\[
\overline{\rho}_{A,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}),
\]

which we call the residual modulo \( \ell \) Galois representation of \( A \).

For a rational prime \( p \nmid \ell N_A \), we denote by \( a_{1,p}(A) \) the trace of \( \rho_{A,\ell}(\text{Frob}_p) \), where \( \text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) is a fixed Frobenius element at \( p \). It is known that \( a_{1,p}(A) \) is an integer which does not depend on \( \ell \) and which satisfies the Hasse-Weil bound \( |a_{1,p}(A)| < 2gp^{\frac{1}{2}} \).

In [LaTr76], Lang and Trotter considered the case of an abelian variety over \( \mathbb{Q} \) of dimension 1 and having a trivial \( \mathbb{Q} \)-endomorphism ring, and proposed the investigation of the asymptotic behaviour of the function counting primes \( p \) for which \( a_{1,p}(A) \) equals a given integer. This problem may also be considered when \( g > 1 \), as follows.

Let \( t \in \mathbb{Z} \) and \( x \in \mathbb{R} \) with \( x > 0 \), and define

\[
\pi_A(x, t) := \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \}.
\]

Assume, for simplicity, that \( A \) is principally polarized, in which case the Galois representation \( \rho_A \), defined as the product of the \( \ell \)-adic Galois representations \( \rho_{A,\ell} \), has its image contained in \( \text{GSp}_{2g}(\mathbb{Z}) \). If \( \rho_A \) has open image in \( \text{GSp}_{2g}(\mathbb{Z}) \) and if the normalized traces \( \frac{a_{1,p}(A)}{\sqrt{p}} \) are equidistributed on the interval \([-2g, 2g]\) with respect to the projection by the trace map of the normalized Haar measure on the unitary symplectic group \( \text{USp}_{2g} \), then Cojocaru, Davis, Silverberg and Stange [CoDaSiSt17] conjectured that, provided \( t \neq 0 \) when \( g \geq 2 \), there exists an explicit constant \( c(A, t) \geq 0 \) such that, as \( x \to \infty \),

\[
\pi_A(x, t) \sim c(A, t) \frac{\sqrt{x}}{\log x}.
\]

In the case of an abelian variety of dimension \( g = 1 \) and having a trivial \( \mathbb{Q} \)-endomorphism ring, both the open image assumption and the equidistribution assumption are known to hold and the asymptotic formula \( (2) \) coincides with the Lang-Trotter Conjecture on Frobenius traces proposed in [LaTr76].
abelian variety of dimension $g \geq 2$, the open image assumption is known to hold if $g = 2, 6$, or odd, and the $\mathbb{Q}$-endomorphism ring of $A$ is trivial (see [Se85], [Se86]); in contrast, the equidistribution assumption – a special case of a broad conjecture that generalizes the Sato-Tate Conjecture (see [Se94] and [KaSa99]) – remains open.

The growth of the function $\pi_A(x, t)$ is intimately connected to the distribution of Frobenius elements in extensions of $\mathbb{Q}$ derived from $A$. For example, the Chebotarev Density Theorem, applied in extensions of $\mathbb{Q}$ associated to the division fields of $A$, plays a fundamental role in the study of $\pi_A(x, t)$. Since the best effective versions of this theorem depend on the assumption of a Generalized Riemann Hypothesis (denoted GRH, for short), it is natural to investigate the growth of $\pi_A(x, t)$ under such an assumption.

Currently, the best results about the growth of $\pi_A(x, t)$, obtained under some GRH, are as follows: provided that $g = 1$ and $A$ has a trivial $\mathbb{Q}$-endomorphism ring, it was proven in [MuMuSa88] and [Zy15] that

$$
\pi_A(x, t) \ll_A \begin{cases} 
\frac{x^{1 - \frac{1}{2g^2 + g + 1}}}{(\log x)^{1 - \frac{1}{2g^2 + g + 1}}} & \text{if } t \neq 0, \\
\frac{x^{1 - \frac{1}{2g^2 + g + 1}}}{(\log x)^{1 - \frac{1}{2g^2 + g + 1}}} & \text{if } t = 0;
\end{cases}
$$

provided that $g \geq 2$ and $\rho_A$ has open image in $\text{GSp}_{2g}(\hat{\mathbb{Z}})$, it was proven in [CoDaSiSt17] that, for any $\varepsilon > 0$,

$$
\pi_A(x, t) \ll_{A, \varepsilon} \begin{cases} 
x^{1 - \frac{1}{2g^2 - g + 3} + \varepsilon} & \text{if } t \neq \pm 2g, 0, \\
x^{1 - \frac{1}{2g^2 - g + 1} + \varepsilon} & \text{if } t = \pm 2g,
\end{cases}
$$

and

$$
\pi_A(x, 0) \ll_{A, \varepsilon} \begin{cases} 
x^{1 - \frac{1}{2g^2 + g + 1} + \varepsilon} & \text{if } g = 2, \\
x^{1 - \frac{1}{2g^2 - g + 3} + \varepsilon} & \text{if } g \geq 3.
\end{cases}
$$

Our main goal in this paper is to improve upon the above results when $g \geq 2$. Specifically, under a GRH assumption, we prove the following upper bounds for $\pi_A(x, t)$.

**Theorem 1.** Let $t \in \mathbb{Z}$ and let $A$ be an abelian variety defined over $\mathbb{Q}$ and of dimension $g$. Assume that, for any sufficiently large prime $\ell$, the image of the residual modulo $\ell$ Galois representation $\bar{\rho}_A,\ell$ of $A$ is isomorphic to $\text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. Assume the Generalized Riemann Hypothesis for Dedekind zeta functions. Then, for any sufficiently large $x$, we have

$$
\pi_A(x, t) \ll_A \begin{cases} 
\frac{x^{1 - \frac{1}{2g^2 + g + 2}}}{(\log x)^{1 - \frac{1}{2g^2 + g + 2}}} & \text{if } t \neq 0, \\
\frac{x^{1 - \frac{1}{2g^2 + g + 1}}}{(\log x)^{1 - \frac{1}{2g^2 + g + 1}}} & \text{if } t = 0.
\end{cases}
$$
Note that the bounds of Theorem 1 recover (3) when \( g = 1 \) and largely improve upon (4) - (5) when \( g \geq 2 \). When \( g = 2 \), Theorem 1 also matches a recent upper bound presented in [KuKuWe22] which, by [BoCaGePi21], is applicable to a modular abelian surface defined over \( \mathbb{Q} \) and having a trivial endomorphism ring.

We remark that the assumption made in Theorem 1 about the image of the residual modulo \( \ell \) Galois representation \( \mathfrak{p}_{A,\ell} \) of \( A \) being isomorphic to \( \text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \) is weaker than, but implied by, the open image assumption of (2). As mentioned earlier, this latter assumption is known to hold for all abelian varieties over \( \mathbb{Q} \) of dimension \( g = 1, 2, 6 \), or odd and having a trivial \( \overline{\mathbb{Q}} \)-endomorphism ring. Moreover, it is known to hold for any abelian \( g \)-fold that arises as the Jacobian of a hyperelliptic curve defined by \( Y^2 = f(X) \) for some monic polynomial \( f(X) \in \mathbb{Z}[X] \) of degree \( \deg f \in \{2g + 1, 2g + 2\} \) for some \( g \geq 2 \) and having the property that either the Galois group of \( f \) is the permutation group on \( \deg f \) elements, or there exists a rational prime \( p \) for which \( f(X) \pmod{p} \) has \( \deg f - 1 \) distinct roots over an algebraic closure of \( \mathbb{F}_p \), one of which is a double root (see the results of Hall and Kowalski in [Ha11] and of Zarhin in [Za00]). Consequently, the strongest assumption of Theorem 1 is that of a GRH.

Our secondary goal in this paper is to improve the bounds of Theorem 1 under additional hypotheses. It is known that if, in addition to a GRH, one assumes further hypotheses on the Artin L-functions associated to a given Galois extension, then one may improve the error term in the effective version of the Chebotarev Density Theorem pertaining to that extension. The impact of such improvements on the growth of \( \pi_A(x, t) \) motivated the bounds (3) of [MuMuSa88] and [Zy15] when \( g = 1 \), which, in turn, motivated the following results of Bellaïche [Be16] when \( g \geq 2 \): assume that, for any sufficiently large prime \( \ell \), the image of the \( \ell \)-adic Galois representation \( \rho_{A,\ell} \) of \( A \) is isomorphic to \( \text{GSp}_{2g}(\mathbb{Z}_\ell) \); assume GRH for Dedekind zeta functions; assume Artin’s Holomorphy Conjecture for Artin L-functions; then, for any \( \varepsilon > 0 \),

\[
\pi_A(x, t) \ll_{A, \varepsilon} \begin{cases} 
  x^{1-\frac{2}{2g^2-2g+4}}+\varepsilon & \text{if } t \neq 0, \\
  x^{1-\frac{2}{2g^2-2g+3}}+\varepsilon & \text{if } t = 0.
\end{cases}
\]

In [MuMuWo18], Murty, Murty, and Wong improved the error term in the effective version of the Chebotarev Density Theorem even further by assuming, in addition to GRH and Artin’s Holomorphy Conjecture, a Pair Correlation Conjecture for the Artin L-functions associated to the given Galois extension. As an application, they obtained the following improvement to (3): assume that \( g = 1 \) and that \( A \) has a trivial \( \overline{\mathbb{Q}} \)-endomorphism ring; assume GRH for Dedekind zeta functions; assume Artin’s Holomorphy Conjecture and a Pair Correlation Conjecture for Artin L-functions; then

\[
\pi_A(x, t) \ll_A \begin{cases} 
  x^{1-\frac{1}{2}}(\log x)^{\frac{1}{2}} & \text{if } t \neq 0, \\
  x^{1-\frac{1}{2}} \log x & \text{if } t = 0.
\end{cases}
\]
In this paper, we generalize (7) to the case of an abelian variety of higher dimensions and obtain the following upper bounds for $\pi_A(x,t)$.

**Theorem 2.** Let $t \in \mathbb{Z}$ and let $A$ be an abelian variety defined over $\mathbb{Q}$ and of dimension $g$. Assume that, for any sufficiently large prime $\ell$, the image of the residual modulo $\ell$ Galois representation $\overline{\rho}_{A,\ell}$ of $A$ is isomorphic to $\text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. Assume the Generalized Riemann Hypothesis for Dedekind zeta functions, Artin’s Holomorphy Conjecture for Artin $L$-functions, and a Pair Correlation Conjecture for Artin $L$-functions. Then, for any sufficiently large $x$, we have

$$\pi_A(x,t) \ll_A \begin{cases} \frac{x^{1-\frac{g+2}{g+1}}}{(\log x)^{\frac{1}{g+1}}} & \text{if } t \neq 0, \\ \frac{x^{1-\frac{g+1}{g+1}}}{(\log x)^{\frac{1}{g+1}}} & \text{if } t = 0. \end{cases}$$

By using Theorems 1 and 2, we obtain the following non-trivial lower bounds for $|a_{1,p}(A)|$ for almost all $p$.

**Theorem 3.** Let $A$ be an abelian variety defined over $\mathbb{Q}$ and of dimension $g$. Assume that, for any sufficiently large prime $\ell$, the image of the residual modulo $\ell$ Galois representation $\overline{\rho}_{A,\ell}$ of $A$ is isomorphic to $\text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.

(i) Assume the Generalized Riemann Hypothesis for Dedekind zeta functions. Then, for any $\varepsilon > 0$, the inequality

$$|a_{1,p}(A)| > \frac{p^{g+1}+g+1}{(\log p)^{\varepsilon}}$$

holds for a set of primes $p$ of density 1.

(ii) Assume the Generalized Riemann Hypothesis for Dedekind zeta functions, Artin’s Holomorphy Conjecture for Artin $L$-functions, and a Pair Correlation Conjecture for Artin $L$-functions. Then, for any $\varepsilon > 0$, the inequality

$$|a_{1,p}(A)| > p^{\frac{1}{2}-\varepsilon}$$

holds for a set of primes $p$ of density 1.

The motivation for Theorem 3 comes from a conjecture of Atkin and Serre on a lower bound for $\tau(p)$ for the Ramanujan $\tau$-function (see [Se76]). To see this, recall that, when $g = 1$, the integer $a_{1,p}(A)$ coincides with the $p$-th Fourier coefficient of the weight two normalized newform, of level $N_A$, associated to $A$ under the Shimura-Taniyama-Weil Conjecture. Using this point of view, Theorem 3 relates to results on the growth of the $p$-th Fourier coefficients of newforms pursued in [MuMu84] and [MuMuSa88], which had been motivated by the aforementioned conjecture of Atkin and Serre.

Before concluding the introduction, let us comment briefly on the proofs of our first two main results. The proofs of Theorems 1-2 have their roots in the observation that if $a_{1,p}(A) = t$, then $a_{1,p}(A) \equiv t(\text{mod } \ell)$.
for any prime ℓ, and in the interpretation of \( a_{1,p}(A)(\text{mod } ℓ) \) as the trace of the image of \( \text{Frob}_p \) under the residual modulo ℓ Galois representation of \( A \). An application of some version of the Chebotarev Density Theorem should then lead to some non-trivial upper bound for \( \pi_A(x,t) \). For example, when \( g = 1 \) and \( A \) has a trivial \( \mathbb{Q} \)-endomorphism ring, by assuming GRH and by using the effective version of the Chebotarev Density Theorem of Lagarias and Odlyzko [LaOd77], one obtains the upper bound \( \pi_A(x,t) \ll_{A,\varepsilon} x^{1-\frac{1}{8}+\varepsilon} \).

While this mod ℓ approach easily leads to a non-trivial upper bound for \( \pi_A(x,t) \) when \( g = 1 \), refining it to improve upon this bound or generalizing it to obtain a non-trivial upper bound for \( \pi_A(x,t) \) when \( g \geq 2 \) requires further tools and new ideas.

One strategy of refining the mod ℓ approach is to consider, simultaneously, mod ℓ\(^k\) congruences, for some fixed prime ℓ and varying positive integers \( k \geq 1 \). For example, in [Se81], Serre considered the case \( g = 1 \) and \( A \) has a trivial \( \mathbb{Q} \)-endomorphism ring, and related the problem of estimating \( \pi_A(x,t) \) to a prime counting problem in the setting of an infinite Galois extension of \( \mathbb{Q} \) having the ℓ-adic Lie group \( \text{GL}_2(\mathbb{Z}_\ell) \) as its Galois group, where ℓ is some sufficiently large prime defined in terms of \( x \). Then, he used an ℓ-adic version of the Chebotarev Density Theorem to estimate, from above, the emerging set of primes. In particular, by assuming GRH, Serre obtained the upper bound \( \pi_A(x,t) \ll_{A,\varepsilon} x^{1-\frac{1}{8}+\varepsilon} \). This ℓ-adic approach was generalized to \( g \geq 2 \) by Cojocaru, Davis, Silverberg, and Stange in [CoDaSiSt17], who proved the upper bounds (4) and (5), under GRH.

Another strategy of refining the mod ℓ approach is to improve the error term in the effective version of the Chebotarev Density Theorem. For example, in [MuMuSa88], by assuming, in addition to GRH, Artin’s Holomorphy Conjecture (denoted AHC, for short), Murty, Murty, and Saradha proved a refined version of the effective Chebotarev Density Theorem of [LaOd77]. Considering the case \( g = 1 \) and \( A \) has a trivial \( \mathbb{Q} \)-endomorphism ring, a direct application of this theorem in the mod ℓ approach would lead to the upper bound \( \pi_A(x,t) \ll_{A,\varepsilon} x^{1-\frac{1}{8}+\varepsilon} \), under GRH and AHC. To circumvent the assumption of AHC and still obtain this upper bound, Murty, Murty, and Saradha related the problem of estimating \( \pi_A(x,t) \) to a prime counting problem in the setting of a particular subextension \( L/K \) of number fields, having its Galois group isomorphic to an abelian and sufficiently large quotient of \( \text{GL}_2(\mathbb{F}_\ell) \), where ℓ is some sufficiently large prime defined in terms of \( x \). Then they estimated the emerging set of primes by appealing to their improved effective version of the Chebotarev Density Theorem, assuming only GRH, since AHC is known in an abelian setting. Overall, their refined mod ℓ approach, together with an improvement of [Zy15], led to the upper bounds (3). In [Be16], Bellaïche refined the aforementioned improved version of the effective Chebotarev Density Theorem of Murty, Murty, and Saradha in certain cases and succeeded in generalizing the proof of (3) in the case \( g = 2 \) and \( A \) has a trivial \( \mathbb{Q} \)-endomorphism ring, proving, under both GRH and AHC, that \( \pi_A(x,0) \ll_{A,\varepsilon} \frac{x^{1-\frac{1}{8}}}{(\log x)^{\frac{1}{2}+\varepsilon}} \). Unlike the final bound of Murty, Murty, and Saradha, which only assumes GRH, that of Bellaïche assumes both GRH and AHC.
One could also relate mod $\ell$ approach of estimating $\pi_A(x, t)$ to a sieve, such as the large sieve, and then use an improved version of the effective Chebotarev Density Theorem to execute the sieve application. This approach was elaborated on in [Be16], leading to the improved upper bounds (3), which hold for $g \geq 1$ and which assume both GRH and AHC.

In the case $g = 1$ and $A$ has a trivial $\mathbb{Q}$-endomorphism ring, the mod $\ell$ approach witnessed yet another refinement in [MuMuWo18]. Therein, by assuming, in addition to GRH and AHC, a Pair Correlation Conjecture (denoted PCC, for short), Murty, Murty, and Wong improved the effective Chebotarev Density Theorem of [MuMuSa88]. Then, they used this theorem directly in the mod $\ell$ approach to prove the upper bounds (7), under GRH, AHC, and PCC. Via this strategy, in order to take advantage of the power of the PCC assumption, one cannot circumvent the assumption of AHC by working in an abelian extension of number fields.

Our proof of Theorem 1 generalizes the mod $\ell$ approach of [MuMuSa88], under GRH, to the case $g \geq 2$, overcoming prior obstacles faced in [Be16] and [CoDaSiSt17]. The main challenges were those of unraveling, for some sufficiently large prime $\ell$, a suitable distinguished pair of subfields of a finite Galois extension of $\mathbb{Q}$ having its Galois group isomorphic to an abelian and sufficiently large quotient of $\text{GSp}_{2g}(\mathbb{F}_\ell)$, and of finding a suitable conjugacy class in this group for which the effective version of the Chebotarev Density Theorem of [MuMuSa88] could be applied successfully.

Our proof of Theorem 2 generalizes the mod $\ell$ approach of [MuMuWo18], under GRH, AHC, and PCC, to the case $g \geq 2$, overcoming obstacles faced in [CoDaSiSt17]. The main challenge was that of unraveling, for some sufficiently large prime $\ell$, a suitable conjugacy class in $\text{GSp}_{2g}(\mathbb{F}_\ell)$ for which the effective version of the Chebotarev Density Theorem of [MuMuWo18] could be applied successfully.

The statements of the Generalized Riemann Hypothesis, Artin’s Holomorphy Conjecture, and the Pair Correlation Conjecture, as well as the main notation used in the paper, are given in Section 2. The effective versions of the Chebotarev Density Theorem needed for our proofs are presented in Section 3. The distinguished subgroups and conjugacy classes of $\text{GSp}_{2g}(\mathbb{F}_\ell)$ needed in our approaches are discussed in Sections 4 - 5. The proofs of Theorems 1 - 3 are given in Section 6, with Propositions 18 - 19 playing the role of crucial ingredients. Following these proofs, brief remarks about possible other approaches towards obtaining conditional bounds for $\pi_A(x, t)$ are included in Section 7.

Acknowledgments. We thank Professor Kiran S. Kedlaya and Professor Peter Sarnak for stimulating discussions related to this work.

2. Notation

Throughout the paper, we use the following notation.

- Given a finite set $S$, we denote its cardinality by $\#S$. 

• Given suitably defined real functions \( h_1, h_2 \), we say that \( h_1 = o(h_2) \) if \( \lim_{x \to \infty} \frac{h_1(x)}{h_2(x)} = 0 \); we say that \( h_1 = \Omega(h_2) \) or, equivalently, that \( h_1 \ll h_2 \), if \( h_2 \) is positive valued and there exists a positive constant \( c \) such that \( |h_1(x)| \leq c h_2(x) \) for all \( x \) in the common domain of \( h_1 \) and \( h_2 \); we say that \( h_1 = \Omega_L(h_2) \) or, equivalently, that \( h_1 \ll_L h_2 \), if \( h_1 = O(h_2) \) and the implied \( O \)-constant \( c \) depends on priorly given data \( D \); we say that \( h_1 \sim h_2 \) if \( \lim_{x \to \infty} \frac{h_1(x)}{h_2(x)} = 1 \).

• Given the letters \( p \) and \( \ell \) to denote rational primes. We denote by \( \pi(x) \) the number of primes \( p \leq x \) and recall that, by the Prime Number Theorem, \( \pi(x) \sim \frac{x}{\log x} \).

• Given a positive integer \( m \), we denote by \( \mathbb{Z}/m\mathbb{Z} \) the ring of integers modulo \( m \). When \( m \) is a prime \( \ell \), we denote \( \mathbb{Z}/\ell\mathbb{Z} \) by \( \mathbb{F}_\ell \) to emphasize its field structure. For an integer \( a \), we denote by \( a \pmod{\ell} \) its residue class modulo \( \ell \).

• Given a prime \( \ell \), we denote by \( \mathbb{Z}_\ell \) the ring of \( \ell \)-adic integers. We set \( \hat{\mathbb{Z}} := \lim_{m \to \infty} \mathbb{Z}/m\mathbb{Z} \) and recall that there exists a ring isomorphism \( \hat{\mathbb{Z}} \cong \prod_{\ell} \mathbb{Z}_\ell \).

• Given a number field \( K \), we denote by \( \mathcal{O}_K \) its ring of integers, by \( \sum_K \) the set of non-zero prime ideals of \( \mathcal{O}_K \), by \( [K : \mathbb{Q}] \) the degree of \( K \) over \( \mathbb{Q} \), by \( d_K \in \mathbb{Z}\setminus\{0\} \) the discriminant of an integral basis of \( \mathcal{O}_K \), and by \( \text{disc}(K/\mathbb{Q}) = \mathbb{Z} d_K \subseteq \mathbb{Z} \) the discriminant ideal of \( K/\mathbb{Q} \). For a prime ideal \( \mathfrak{p} \in \sum_K \), we denote by \( N_{K/\mathbb{Q}}(\mathfrak{p}) \) its norm in \( K/\mathbb{Q} \). We say that \( K \) satisfies the Generalized Riemann Hypothesis (GRH) if the Dedekind zeta function \( \zeta_K \) of \( K \) has the property that, for any \( \rho \in \mathbb{C} \) with \( 0 \leq \text{Re} \rho \leq 1 \) and \( \zeta_K(\rho) = 0 \), we have \( \text{Re}(\rho) = \frac{1}{2} \).

When \( K = \mathbb{Q} \), the Dedekind zeta function is the Riemann zeta function, in which case we refer to GRH as the Riemann Hypothesis (RH).

• Given a finite Galois extension \( L/K \) of number fields and given an irreducible character \( \chi \) of the Galois group of \( L/K \), we denote by \( f(\chi) \subseteq \mathcal{O}_K \) the global Artin conductor of \( \chi \), by \( A_\chi := |d_L|^{\frac{1}{2}} N_{K/\mathbb{Q}}(f(\chi)) \in \mathbb{Z} \) the conductor of \( \chi \), and by \( A_\chi(T) \) the function of a positive real variable \( T > 3 \) defined by the relation

\[
\log A_\chi(T) = \log A_\chi + \chi(1)[K : \mathbb{Q}] \log T.
\]

• Given a finite Galois extension \( L/K \) of number fields, we say that it satisfies Artin’s Holomorphy Conjecture (AHC) if, for any irreducible character \( \chi \) of the Galois group of \( L/K \), the Artin L-function \( L(s, \chi, L/K) \) extends to a function that is analytic on the whole \( \mathbb{C} \), except at \( s = 1 \) when \( \chi = 1 \). We recall that, if we assume GRH for \( L \) and AHC for \( L/K \), then, given any irreducible character \( \chi \) of the Galois group of \( L/K \), and given any non-trivial zero \( \rho \) of \( L(s, \chi, L/K) \), the real part \( \text{Re} \rho \) of \( \rho \) satisfies \( \text{Re} \rho = \frac{1}{2} \).

In this case, we write \( \rho = \frac{1}{2} + i \gamma \), where \( \gamma \) denotes the imaginary part of \( \rho \).

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

\[
P_T(X, \chi) := \sum_{-T \leq \gamma_1 \leq T} \sum_{-T \leq \gamma_2 \leq T} w(\gamma_1 - \gamma_2)e((\gamma_1 - \gamma_2)X),
\]
where $\gamma_1$ and $\gamma_2$ range over all the imaginary parts of the non-trivial zeroes $\rho = \frac{1}{2} + \gamma$ of $L(s, \chi, L/K)$, counted with multiplicity, and where, for an arbitrary real number $u$, $e(u) := \exp(2\pi iu)$ and $w(u) := \frac{u}{1 + u^2}$. We say that the extension $L/K$ satisfies the Pair Correlation Conjecture (PCC) if, for any irreducible character $\chi$ of the Galois group of $L/K$ and for any $A > 0$ and $T > 3$, provided $0 \leq Y \leq A\chi(1)[K : \mathbb{Q}] \log T$, we have

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

- Given a field $F$, we denote by $\text{char } F$ its field characteristic, by $\overline{F}$ a fixed algebraic closure of $F$, by $F^{\text{sep}}$ a fixed separable closure of $F$ in $\overline{F}$, and by $\text{Gal}(F^{\text{sep}}/F)$ the absolute Galois group of $F$.
- Given a non-zero unitary commutative ring $R$, we denote by $R^\times$ its group of multiplicative units.
- Given a non-zero unitary commutative ring $R$ and a free module $\mathcal{M}$ over $R$, of finite rank $n \geq 1$, endowed with a non-degenerate alternating bilinear form $e : \mathcal{M} \times \mathcal{M} \to R$, we denote by $\text{GSp}(\mathcal{M}, e)$ the group of symplectic similitudes of $\mathcal{M}$ with respect to $e$, that is, the group of $R$-automorphisms $\sigma \in \text{Aut}(\mathcal{M})$ such that there exists $\mu \in R^\times$ with the property that $e(\sigma(v), \sigma(w)) = \mu e(v, w)$ for all $v, w \in \mathcal{M}$. Since $\mathcal{M}$ has a unique (up to isomorphism) non-degenerate alternating bilinear form, we may write $\text{GSp}_n(R)$ for $\text{GSp}(\mathcal{M}, e)$.
- Given a non-zero unitary commutative ring $R$ and an integer $n \geq 1$, we denote by $M_n(R)$ the ring of $n \times n$ matrices with entries in $R$ and by $I_n$ the identity matrix in $M_n(R)$. For an arbitrary matrix $M \in M_n(R)$, we denote by $\text{tr } M$ and $\det M$ its trace and determinant, and by $M^t$ its transpose. We define the general linear group $\text{GL}_n(R)$ as the collection of $M \in M_n(R)$ with $\det M \in R^\times$. For $a_1, \ldots, a_g \in R$, we define

$$\text{diag}(a_1, \ldots, a_n) := \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in M_n(R).$$

When $n = 2g$ for some integer $g \geq 1$, we define

$$J_{2g} := \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \in M_{2g}(R).$$

The general symplectic group over $R$ may then be described as

$$\text{GSp}_{2g}(R) = \left\{ M \in \text{GL}_{2g}(R) : M^t J_{2g} M = \mu J_{2g} \text{ for some } \mu \in R^\times \right\}.$$

Associated to $\text{GSp}_{2g}(R)$, we have the character $\text{GSp}_{2g}(R) \to R^\times$, $M \mapsto \mu$. The scalar $\mu$ corresponding to $M$ is called the multiplicator of $M$. We write the group of scalar matrices in $\text{GSp}_{2g}(R)$ as $\Lambda_{2g}(R)$ and note that it is isomorphic to $R^\times$. We define the projective general symplectic group $\text{PGSp}_{2g}(R)$ as the quotient $\text{GSp}_{2g}(R)/\Lambda_{2g}(R)$.

3. Frobenius distributions in number field extensions

In this section, we record results on the theme of Frobenius distributions in a number field Galois extension; these results will play a crucial role in the proofs of Theorems 11--12.
Let $L/K$ be a finite Galois extension of number fields. Denote by $\text{Gal}(L/K)$ the Galois group of $L/K$ and keep the number field notation introduced in Section 2. Denote by $[L : K]$ the degree of $L/K$ and by $\text{disc}(L/K)$ the discriminant ideal of $L/K$.

We define

$$P(L/K) := \{ p \text{ rational prime} : \exists p \in \sum K \text{ such that } p \mid p \text{ and } p \mid \text{disc}(L/K)\},$$

$$M(L/K) := 2[L : K][d_K] \prod_{p \in P(L/K)} p,$$

and we recall from [Se81] Prop. 5, p. 129 that

$$\log |N_{K/Q}(\text{disc}(L/K))| \leq ([L : Q] - [K : Q]) \left( \sum_{p \in P(L/K)} \log p \right) + [L : Q] \log[L : K].$$

For a place $\wp \in \Sigma_L$, we denote by $D_\wp$ its decomposition group in $L/K$, by $I_\wp$ its inertia group in $L/K$, and by $\left(\frac{L/K}{\wp}\right)$ its Frobenius element in $L/K$.

For a place $p \in \Sigma_K$, we set

$$\left(\frac{L/K}{p}\right) := \left\{ \left(\frac{L/K}{\wp}\right) : \wp \in \Sigma_L, \wp \text{ lies over } p \right\}.$$

For a non-empty set $C \subseteq \text{Gal}(L/K)$, stable under conjugation by elements of $\text{Gal}(L/K)$, we denote by $\delta_C : \text{Gal}(L/K) \rightarrow \{0, 1\}$ its characteristic function and, for an arbitrary place $p \in \Sigma_K$ and an arbitrary integer $m \geq 1$, we set

$$\delta_C\left(\left(\frac{L/K}{p}\right)^m\right) := \frac{1}{\#D_\wp} \sum_{\gamma \in P_\wp, \gamma x = \left(\frac{L/K}{p}\right)^m \in D_\wp/I_\wp} \delta_C(\gamma),$$

where $\wp \in \Sigma_L$ is an arbitrary place above $p$, whose choice leaves the above definition unchanged. For a real number $x \geq 2$, we set

$$\pi_C(x, L/K) := \sum_{p \in \Sigma_K \atop \text{disc}(L/K) \leq x} \delta_C\left(\left(\frac{L/K}{p}\right)\right),$$

$$\tilde{\pi}_C(x, L/K) := \sum_{m \geq 1} \frac{1}{m} \sum_{p \in \Sigma_K \atop \text{disc}(L/K) \leq x} \delta_C\left(\left(\frac{L/K}{p}\right)^m\right),$$

and we recall from [Se81] Proposition 7, p. 138 and [Zy15] Lemma 2.7, p. 8 that

$$\tilde{\pi}_C(x, L/K) = \pi_C(x, L/K) + O\left([K : Q] \left(\frac{x^{1/2}}{\log x} + \log M(L/K)\right)\right).$$

The variations of the effective version of the Chebotarev Density Theorem of [LaOd77] that relate to the proofs of our main theorems are as follows.

**Theorem 4.** Let $L/K$ be a Galois extension of number fields. Let $\emptyset \neq C \subseteq \text{Gal}(L/K)$ be a subset stable under conjugation by elements of $\text{Gal}(L/K)$. 
(i) Assume GRH for the Dedekind zeta function of $L$. Then
\[
\pi_C(x, L/K) = \frac{\#C}{[L : K]} \pi(x) + O\left(\left(\#C \cdot x^{\frac{1}{2}} [K : Q] \left(\frac{\log |d_L|}{[L : Q]} + \log x\right)\right)^{\frac{1}{2}} \frac{x}{\log x} \right).
\]

(ii) Assume GRH for the Dedekind zeta function of $L$ and AHC for the extension $L/K$. Then
\[
\pi_C(x, L/K) = \frac{\#C}{[L : K]} \pi(x) + O\left(\left(\#C \cdot x^{\frac{1}{2}} [K : Q] \log(M(L/K)x)\right)^{\frac{1}{2}} \frac{x}{\log x} \right).
\]

(iii) Assume GRH for the Dedekind zeta function of $L$, and AHC and PCC for the extension $L/K$. Then
\[
\pi_C(x, L/K) = \frac{\#C}{[L : K]} \pi(x) + O\left(\left(\#C \cdot x^{\frac{1}{2}} [K : Q] \log(M(L/K)x)\right)^{\frac{1}{2}} \frac{x}{\log x} \right).
\]

\textbf{Proof.} Part (i) is [Se81, Théorème 4, p. 133]. Part (ii) is [MuMuSa88, Corollary 3.7, p. 265]. Part (iii) is [MuMuWo18, Theorem 1.2, p. 402]. \qed

In the proofs of our main results, we do not always need the full strength of the effective asymptotic formulae in Theorem 4. For example, we do not use part (ii) of this theorem, which we included for clarity and for comparison with parts (i) and (iii). Instead of part (ii), we will use Theorem 5, stated below. We will also use Theorem 7, stated below, which is a consequence of part (iii).

\textbf{Theorem 5.} Let $L/K$ be a Galois extension of number fields. Let $\emptyset \neq C \subseteq \text{Gal}(L/K)$ be a subset stable under conjugation by elements of $\text{Gal}(L/K)$. Assume GRH for the Dedekind zeta function of $L$ and AHC for the extension $L/K$. Then
\[
\pi_C(x, L/K) \ll \frac{\#C}{[L : K]} \pi(x) + \left(\#C \cdot x^{\frac{1}{2}} [K : Q] \log M(L/K)x\right)^{\frac{1}{2}} \frac{x}{\log x} \log x.
\]

\textbf{Proof.} This is [Zy15, Theorem 2.3, p. 5]. \qed

\textbf{Theorem 6.} Let $L/K$ be a Galois extension of number fields. Let $\emptyset \neq C_1 \subseteq C_2 \subseteq \text{Gal}(L/K)$ be subsets stable under conjugation by elements of $\text{Gal}(L/K)$. Let $H \leq \text{Gal}(L/K)$ be a subgroup of $\text{Gal}(L/K)$ and let $N \triangleleft H$ be a normal subgroup of $H$. Assume that:

(i) every element of $C_1$ is conjugate to some element of $H$;

(ii) $N(C_2 \cap H) \subseteq C_2 \cap H$;

(iii) $H/N$ is an abelian group;

(iv) GRH holds for the Dedekind zeta function of $L^N$.

Then
\[
\pi_{C_1}(x, L/K) \ll \frac{\#C_2 \cap H \cdot \#N}{\#H} \pi(x) + \left(\#C_2 \cap H \right)^{\frac{1}{2}} \frac{x^{\frac{1}{2}} [L^H : Q] \log M(L^N/L^H) + [K : Q] \log M(L/K)}{\log x},
\]

where $\overline{C_2 \cap H}$ denotes the image of $C_2 \cap H$ in $H/N$ under the canonical projection $H \twoheadrightarrow H/N$. 
Proof. Using assumption (i) and [Zy15] Lemma 2.6 (ii), we obtain that $\tilde{\pi}_{C_1}(x, L/K) \leq \tilde{\pi}_{C_1 \cap H}(x, L/L^H)$. Since $C_1 \subseteq C_2$, we obviously have $\tilde{\pi}_{C_1 \cap H}(x, L/L^H) \leq \tilde{\pi}_{C_2 \cap H}(x, L/L^H)$. Using assumption (ii), [Zy15] Lemma 2.6 (ii), and asymptotic formula (9), we obtain that

$$\pi_{C_2 \cap H}(x, L/L^H) = \tilde{\pi}_{C_2 \cap H}(x, L^N/L^H) = \pi_{C_2 \cap H}(x, L^N/L^H) + O \left( \frac{x^{\frac{1}{2}}}{\log x} + \log M \left( L^N/L^H \right) \right).$$

Using assumption (iii) and [Ar27], we deduce that AHC holds for the extension $L^N/L^H$. Then, using assumption (iv) and Theorem 3 we deduce that

$$\pi_{C_2 \cap H}(x, L^N/L^H) \ll \frac{\#(C \cap H)}{[H : N]} \pi(x) + \frac{x^{\frac{1}{2}}}{\log x} [L^H : Q] \log M \left( L^N/L^H \right).$$

Finally, putting all these observations together and using (9) again to relate $\pi_{C_1}(x, L/K)$ to $\pi_{C_1}(x, L/K)$, we infer that

$$\pi_{C_1}(x, L/K) \ll \frac{\#(C \cap H)}{[H : N]} \pi(x) + \frac{x^{\frac{1}{2}}}{\log x} [L^H : Q] \log M \left( L^N/L^H \right)$$

$$+ \frac{x^{\frac{1}{2}}}{\log x}([L^H : Q] + [K : Q]) + [L^H : Q] \log M \left( L^N/L^H \right) + [K : Q] \log M(L/K)$$

$$\ll \frac{\#(C \cap H)}{[H : N]} \pi(x) + \frac{x^{\frac{1}{2}}}{\log x} [L^H : Q] \log M \left( L^N/L^H \right) + [K : Q] \log M(L/K).$$

\[\square\]

**Theorem 7.** Let $L/K$ be a Galois extension of number fields. Let $\emptyset \neq C \subseteq \text{Gal}(L/K)$ be a subset stable under conjugation by elements of $\text{Gal}(L/K)$. Let $H \leq \text{Gal}(L/K)$ be a subgroup of $\text{Gal}(L/K)$ and let $N \trianglelefteq H$ be a normal subgroup of $H$. Assume that:

(i) every element of $C$ is conjugate to some element of $H$;

(ii) $N(C \cap H) \subseteq C \cap H$;

(iii) GRH holds for the Dedekind zeta function of $L^N$;

(iv) AHC and PCC hold for the number field extension $L^N/L^H$.

Then

$$\pi_C(x, L/K) \ll \frac{\#(C \cap H) \cdot N}{\#H} \pi(x) + \frac{\#(C \cap H)^{\frac{1}{2}}}{[H : N]} \left( \frac{\#C}{[H : N]} \right) \frac{x^{\frac{1}{2}}}{\log x} [L^H : Q] \log M \left( L^N/L^H \right)$$

$$+ \frac{x^{\frac{1}{2}}}{\log x} ([L^H : Q] + [K : Q]) + [L^H : Q] \log M \left( L^N/L^H \right) + [K : Q] \log M(L/K),$$

where $\hat{C \cap H}$ denotes the image of $C \cap H$ in $\hat{H}$ under the canonical projection $H \to \hat{H}$.

Proof. Similarly to the proof of the previous theorem, we obtain that

$$\tilde{\pi}_C(x, L/K) \leq \tilde{\pi}_{C \cap H}(x, L/L^H) = \tilde{\pi}_{\hat{C \cap H}}(x, L^N/L^H)$$

$$= \pi_{\hat{C \cap H}}(x, L^N/L^H) + O \left( [L^H : Q] \left( \frac{x^{\frac{1}{2}}}{\log x} + \log M(L^N/L^H) \right) \right),$$
Then, using assumptions (iii)-(iv) and part (iii) of Theorem 4, we deduce that

\[
\pi_{\hat{C} \cap H}(x, L^N/L^H) = \#(\hat{C} \cap H) \cdot \pi(x) + O\left(\left(\frac{\#(L^N/L^H)}{[L^N : L^H]}\right)^{\frac{1}{2}} L^H : Q \log (M(L^N/L^H)x)\right).
\]

Putting all these observations together, we infer that

\[
\pi_C(x, L/K) \ll \#(\hat{C} \cap H) \cdot \pi(x) + \#(\hat{C} \cap H) \cdot \left(\frac{\#(L^N/L^H)}{[L^N : L^H]}\right)^{\frac{1}{2}} x^{\frac{1}{2}} L^H : Q \log (M(L^N/L^H)x)
\]

\[
+ \frac{x^{\frac{1}{2}}}{\log x} ([L^H : Q] + [K : Q]) + [L^H : Q] \log M(L^N/L^H) + [K : Q] \log M(L/K)
\]

\[
\ll \#(\hat{C} \cap H) \cdot \pi(x) + \#(\hat{C} \cap H) \cdot \left(\frac{\#(L^N/L^H)}{[L^N : L^H]}\right)^{\frac{1}{2}} x^{\frac{1}{2}} L^H : Q \log (M(L^N/L^H)x)
\]

\[
+ [L^H : Q] \left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L^N/L^H)\right) + [K : Q] \log M(L/K).
\]

\[\square\]

In Section 6, we will apply Theorems 4, 6, and 7 to number field extensions associated to an abelian variety defined over \(\mathbb{Q}\).

4. Distinguished subgroups in the general symplectic groups over a finite prime field

In this section, we fix an arbitrary integer \(g \geq 1\) and an arbitrary rational prime \(\ell\), and turn our attention to particular subgroups of \(\text{GSp}_{2g}(\mathbb{F}_\ell)\). As we will see in Section 6, these subgroups give rise to particular subextensions of the \(\ell\)-division field of an abelian variety defined over \(\mathbb{Q}\), of dimension \(g\).

We will view the elements of \(\text{GSp}_{2g}(\mathbb{F}_\ell)\) using the following block matrix description

\[
\text{GSp}_{2g}(\mathbb{F}_\ell) = \left\{ M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{GL}_{2g}(\mathbb{F}_\ell) : \begin{array}{c} A, B, C, D \in M_g(\mathbb{F}_\ell), \quad -C^t A + A^t C = 0 \\
-C^t B + A^t D = \mu I_g \quad \text{for some} \quad \mu \in \mathbb{F}_\ell^\times \\
-D^t B + B^t D = 0 \end{array} \right\},
\]

where the element \(\mu\) above is the multiplicator of the matrix \(M\).
Before introducing the subgroups of $GSp_{2g}(F_{\ell})$ needed in the proofs of our main results, we introduce several subgroups of $GL_g(F_{\ell})$, as follows:

$$B_g(F_{\ell}) := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1g} \\
 & \ddots & \\
 & & a_{gg} \end{pmatrix} \in GL_g(F_{\ell}) : a_{ii} \in F_{\ell}^\times \forall 1 \leq i \leq g, a_{ij} \in F_{\ell} \forall 1 \leq i < j \leq g \right\};$$

$$U_g(F_{\ell}) := \left\{ \begin{pmatrix} 1 & \cdots & a_{1g} \\
 & \ddots & \\
 & & 1 \end{pmatrix} \in GL_g(F_{\ell}) : a_{ij} \in F_{\ell} \forall 1 \leq i < j \leq g \right\};$$

$$U'_g(F_{\ell}) := \left\{ \begin{pmatrix} \lambda & \cdots & a_{1g} \\
 & \ddots & \\
 & & \lambda \end{pmatrix} \in GL_g(F_{\ell}) : \lambda \in F_{\ell}^\times, a_{ij} \in F_{\ell} \forall 1 \leq i < j \leq g \right\};$$

$$T_g(F_{\ell}) := \left\{ \begin{pmatrix} a_{11} \\
 & \ddots \\
 & & a_{gg} \end{pmatrix} \in GL_g(F_{\ell}) : a_{ii} \in F_{\ell}^\times \forall 1 \leq i \leq g \right\};$$

For a matrix $A = \begin{pmatrix} \lambda & \cdots & a_{1g} \\
 & \ddots & \\
 & & \lambda \end{pmatrix} \in U'_g(F_{\ell})$, we set $d(A) := \lambda$.

Now we introduce four distinguished subgroups of $GL_{2g}(F_{\ell})$:

$$B_{2g}(F_{\ell}) := \left\{ \begin{pmatrix} A & \mu^{-1}AS \\
0 & \mu(A^t)^{-1} \end{pmatrix} \in GL_{2g}(F_{\ell}) : A \in B_g(F_{\ell}), \mu \in F_{\ell}^\times, S \in M_g(F_{\ell}) \text{ symmetric} \right\};$$

$$U_{2g}(F_{\ell}) := \left\{ \begin{pmatrix} A & AS \\
0 & (A^t)^{-1} \end{pmatrix} \in GL_{2g}(F_{\ell}) : A \in U_g(F_{\ell}), S \in M_g(F_{\ell}) \text{ symmetric} \right\};$$

$$U'_{2g}(F_{\ell}) := \left\{ \begin{pmatrix} A & \mu^{-1}AS \\
0 & \mu(A^t)^{-1} \end{pmatrix} \in GL_{2g}(F_{\ell}) : A \in U'_g(F_{\ell}), \mu = d(A)^2, S \in M_g(F_{\ell}) \text{ symmetric} \right\};$$

$$T_{2g}(F_{\ell}) := \left\{ \begin{pmatrix} A & 0 \\
0 & \mu(A^t)^{-1} \end{pmatrix} \in GL_{2g}(F_{\ell}) : A \in T_g(F_{\ell}), \mu \in F_{\ell}^\times \right\}.$$

For the rest of the section, we focus on properties of these subgroups that will be used in the proofs of Theorems\,\[11\] - \[13\].

**Proposition 8.**

(i) $B_{2g}(F_{\ell})$ is a subgroup of $GSp_{2g}(F_{\ell})$.

(ii) $U_{2g}(F_{\ell})$ is a normal subgroup of $B_{2g}(F_{\ell})$.

(iii) $U'_{2g}(F_{\ell})$ is a normal subgroup of $B_{2g}(F_{\ell})$. 

14
Proof. (i) Let
\[
M = \begin{pmatrix} A' & \mu^{-1}A'S \\ 0 & \mu(A'^{-1}) \end{pmatrix} \in B_{2g}(\mathbb{F}_\ell).
\]
Using the block matrix description of \(GSp_{2g}(\mathbb{F}_\ell)\) and taking
\[
A = A', \; B = \mu^{-1}A'S, \; C = 0, \; D = \mu(A'^{-1}),
\]
we can verify that
\[
-C'A + A'C = 0, \; -C'B + A'D = \mu I_g, \; -D'B + B'D = 0.
\]
This shows that \(M \in GSp_{2g}(\mathbb{F}_\ell)\).

Note that for any matrices
\[
M_1 = \begin{pmatrix} A_1 & \mu_1^{-1}A_1S_1 \\ 0 & \mu_1(A_1^{-1}) \end{pmatrix}, \; M_2 = \begin{pmatrix} A_2 & \mu_2^{-1}A_2S_2 \\ 0 & \mu_2(A_2^{-1}) \end{pmatrix} \in B_{2g}(\mathbb{F}_\ell),
\]
we have
\[
M_1^{-1}M_2^{-1} = \begin{pmatrix} A_1 & \mu_1^{-1}A_1S_1 \\ 0 & \mu_1(A_1^{-1}) \end{pmatrix}^{-1} \begin{pmatrix} A_2^{-1} & -\mu_2^{-2}S_2A_2^{-1} \\ 0 & \mu_2^{-1}A_2^{-1} \end{pmatrix}^{-1}
= \begin{pmatrix} A_1A_2^{-1} & -\mu_2^{-2}A_1S_2A_2^{-1} + \mu_1^{-1}\mu_2^{-1}A_1SA_2^{-1} \\ 0 & \mu_1\mu_2^{-1}(A_1A_2^{-1})^{-1} \end{pmatrix}.
\]
Then, by setting
\[
\mu_3 := \mu_1\mu_2^{-1}, \; A_3 := A_1A_2^{-1}, \; S_3 := (-\mu_1\mu_2^{-2} + \mu_2^{-2})A_2S_2A_2^{-1},
\]
we see that
\[
M_1^{-1}M_2^{-1} = \begin{pmatrix} A_3 & \mu_3^{-1}A_3S_3 \\ 0 & \mu_3(A_3^{-1}) \end{pmatrix} \in B_{2g}(\mathbb{F}_\ell).
\]
This shows that \(B_{2g}(\mathbb{F}_\ell)\) is a group, hence a subgroup of \(GSp_{2g}(\mathbb{F}_\ell)\).

(ii), (iii) It follows from an argument similar to the one used in the proof of (i) that both \(U_{2g}(\mathbb{F}_\ell)\) and \(U'_{2g}(\mathbb{F}_\ell)\) are subgroups of \(B_{2g}(\mathbb{F}_\ell)\). Note that, for any matrices
\[
M_1 = \begin{pmatrix} A_1 & \mu^{-1}A_1S_1 \\ 0 & \mu(A_1^{-1}) \end{pmatrix} \in B_{2g}(\mathbb{F}_\ell), \; M_2 = \begin{pmatrix} A_2 & A_2S_2 \\ 0 & (A_2^{-1}) \end{pmatrix} \in U_{2g}(\mathbb{F}_\ell),
\]
we have
\[
M_1^{-1}M_2^{-1} = \begin{pmatrix} A_1^{-1} & -\mu_1^{-2}S_1A_1^{-1} \\ 0 & \mu_1^{-1}A_1^{-1} \end{pmatrix} \begin{pmatrix} A_2 & A_2S_2 \\ 0 & (A_2^{-1}) \end{pmatrix} \begin{pmatrix} A_1 & \mu_1^{-1}A_1S_1 \\ 0 & \mu_1(A_1^{-1}) \end{pmatrix}
= \begin{pmatrix} A_1^{-1}A_2A_1 & \mu_1^{-1}A_1^{-1}A_2A_1S_1 + \mu_1A_1^{-1}A_2S_2(A_1^{-1})^{-1} - \mu_1^{-1}S_1A_1A_2(A_2^{-1})^{-1}(A_1^{-1})^{-1} \\ 0 & A_1^{-1}(A_1^{-1})^{-1} \end{pmatrix}.
\]
Since $S_1$ is symmetric and since $U_g(\ell) \leq B_g(\mathbb{F}_\ell)$, we obtain that $A_1^{-1}A_2A_1 \in U_g(\mathbb{F}_\ell)$. Then, by setting

$$A_3 := A_1^{-1}A_2A_1, \ S_3 := \mu_1^{-1}S_1 + \mu_1A_1^{-1}S_2(A_1^t)^{-1} - \mu_1A_2^{-1}S_1(A_2^t)^{-1},$$

we obtain that

$$M_1^{-1}M_2M_1 = \begin{pmatrix} A_3 & A_3S_3 \\ 0 & (A_3^t)^{-1} \end{pmatrix} \in U_{2g}(\mathbb{F}_\ell).$$

This proves that $U_{2g}(\mathbb{F}_\ell)$ is a normal subgroup of $B_{2g}(\mathbb{F}_\ell)$. Since $U_{2g}(\mathbb{F}_\ell) \leq U_{2g}'(\mathbb{F}_\ell)$, we deduce that $U_{2g}'(\mathbb{F}_\ell)$ is a normal subgroup of $B_{2g}(\mathbb{F}_\ell)$.

**Proposition 9.** The following formulae hold:

$$\# \text{GSp}_{2g}(\mathbb{F}_\ell) = (\ell - 1) \prod_{1 \leq i \leq g} (\ell^{2i} - 1)^{\ell^{2i-1}};$$

$$\# \text{PGSp}_{2g}(\mathbb{F}_\ell) = \prod_{1 \leq i \leq g} (\ell^{2i} - 1)^{\ell^{2i-1}};$$

$$\# B_g(\mathbb{F}_\ell) = \ell^{\frac{g(g-1)}{2}}(\ell - 1)^g;$$

$$\# U_g(\mathbb{F}_\ell) = \ell^{\frac{g(g-1)}{2}};$$

$$\# U_g'(\mathbb{F}_\ell) = \ell^{\frac{g(g+1)}{2}}(\ell - 1);$$

$$\# T_g(\mathbb{F}_\ell) = (\ell - 1)^g;$$

$$\# B_{2g}(\mathbb{F}_\ell) = \ell^{g^2}(\ell - 1)^{g+1};$$

$$\# U_{2g}(\mathbb{F}_\ell) = \ell^{g^2};$$

$$\# U_{2g}'(\mathbb{F}_\ell) = \ell^{g^2}(\ell - 1);$$

$$\# T_{2g}(\mathbb{F}_\ell) = (\ell - 1)^{g+1}.$$

**Proof.** The formulae for $\# \text{GSp}_{2g}(\mathbb{F}_\ell)$ and $\# \text{PGSp}_{2g}(\mathbb{F}_\ell)$ are well-known (for example, see [O’Me78 Theorem 3.1.2, p. 35]). The formulae for the orders of $B_g(\mathbb{F}_\ell)$, $U_g(\mathbb{F}_\ell)$, $U_g'(\mathbb{F}_\ell)$ and $T_g(\mathbb{F}_\ell)$ are clear from the definitions of the groups. The formulae for the orders of $B_{2g}(\mathbb{F}_\ell)$, $U_{2g}(\mathbb{F}_\ell)$, $U_{2g}'(\mathbb{F}_\ell)$ and $T_{2g}(\mathbb{F}_\ell)$ can be obtained from the definitions of the groups by counting the number of each block matrices, as follows:

$$\# B_{2g}(\mathbb{F}_\ell) = \# B_g(\mathbb{F}_\ell) \cdot \#(\mathbb{Z}/\ell\mathbb{Z})^\times \cdot \ell^{\frac{g(g+1)}{2}} = \ell^{g^2}(\ell - 1)^{g+1};$$

$$\# U_{2g}(\mathbb{F}_\ell) = \# U_g(\mathbb{F}_\ell) \cdot \ell^{\frac{g(g+1)}{2}} = \ell^{g^2};$$

$$\# U_{2g}'(\mathbb{F}_\ell) = \# U_g'(\mathbb{F}_\ell) \cdot \#(\mathbb{Z}/\ell\mathbb{Z})^\times \cdot \ell^{\frac{g(g+1)}{2}} = \ell^{g^2}(\ell - 1);$$

$$\# T_{2g}(\mathbb{F}_\ell) = \# T_g(\mathbb{F}_\ell) \cdot \#(\mathbb{Z}/\ell\mathbb{Z})^\times = (\ell - 1)^{g+1}.$$

□
Proposition 10. The following upper bounds hold:

\[ \# \text{GSp}_{2g}(\mathbb{F}_\ell)^\# \ll_g \ell^{9g+1}, \]
\[ \# \text{PGSp}_{2g}(\mathbb{F}_\ell)^\# \ll_g \ell^9. \]

Proof. The upper bound for \(# \text{GSp}_{2g}(\mathbb{F}_\ell)^\# \) can be obtained from [Wa63] (iii), p. 36 and [Ga70], (2), p.1. To obtain an upper bound for \(# \text{PGSp}_{2g}(\mathbb{F}_\ell)^\# \), we proceed as follows. Note that each conjugacy class in \(\text{PGSp}_{2g}(\mathbb{F}_\ell)^\# \) may be viewed as the equivalence class of \(\Lambda_{2g}(\mathbb{F}_\ell)^\# \)-orbits of conjugacy classes in \(\text{GSp}_{2g}(\mathbb{F}_\ell)^\# \).

Now fix an arbitrary element \(C \in \text{GSp}_{2g}(\mathbb{F}_\ell)^\# \). If there is an element \(b \in \mathbb{F}_\ell^* \) such that \((bI_{2g})C = C\), then, by comparing determinants, we have \(b^{2g} = 1\). So \(b\) may take at most \(2g\) elements. By the orbit-stabilizer theorem in group theory, each \(\Lambda_{2g}(\mathbb{F}_\ell)^\# \)-orbit of \(\text{GSp}_{2g}(\mathbb{F}_\ell)^\# \) contains at least \(\frac{\#\Lambda_{2g}(\mathbb{F}_\ell)}{2g}\) conjugacy classes. Therefore,

\[ \# \text{PGSp}_{2g}(\mathbb{F}_\ell)^\# \leq \frac{\# \text{GSp}_{2g}(\mathbb{F}_\ell)^\#}{\#\Lambda_{2g}(\mathbb{F}_\ell)} \ll_g \ell^9. \]

Proposition 11. The groups \(B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell)\) and \(T_{2g}(\mathbb{F}_\ell)\) are isomorphic. Consequently, the quotient groups \(B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell)\) and \(B_{2g}(\mathbb{F}_\ell)/U_{2g}'(\mathbb{F}_\ell)\) are abelian.

Proof. By comparing the orders of \(B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell)\) and \(T_{2g}(\mathbb{F}_\ell)\), we deduce that the composition \(T_{2g}(\mathbb{F}_\ell) \rightarrow B_{2g}(\mathbb{F}_\ell) \rightarrow B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell)\) is a bijection. Then, recalling that \(T_{2g}(\mathbb{F}_\ell)\) is abelian, we obtain that \(B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell)\) is abelian. Furthermore, by observing that \(U_{2g}(\mathbb{F}_\ell) \leq U_{2g}'(\mathbb{F}_\ell) \leq B_{2g}(\mathbb{F}_\ell)\), we deduce that \(B_{2g}(\mathbb{F}_\ell)/U_{2g}'(\mathbb{F}_\ell)\) is also abelian.

5. Distinguished conjugacy classes in the general symplectic groups over a finite prime field

As in the previous section, we fix an arbitrary integer \(g \geq 1\) and an arbitrary rational prime \(\ell\). This time, we turn our attention to particular unions of conjugacy classes in \(\text{GSp}_{2g}(\mathbb{F}_\ell)\).

First, we recall that a matrix \(M \in M_{2g}(\mathbb{F}_\ell)\) is called semisimple if its minimal polynomial over \(\mathbb{F}_\ell\) has distinct roots in \(\mathbb{F}_\ell\), which is equivalent to the existence of a matrix \(N \in \text{GL}_{2g}(\mathbb{F}_\ell)\) such that \(NMN^{-1}\) is a diagonal matrix in \(M_{2g}(\mathbb{F}_\ell)\). Next, we recall that the eigenvalues of \(M\) are the roots of the characteristic polynomial \(\text{char}_M(X) := \det(XI_{2g} - M) \in \mathbb{F}_\ell[X]\) of \(M\). Finally, we recall that, when \(M \in \text{GSp}_{2g}(\mathbb{F}_\ell)\), its characteristic polynomial \(\text{char}_M(X)\) has the form

\[ \text{char}_M(X) = X^{2g} + b_1X^{2g-1} + \ldots + b_gX^g + \mu b_{g-1}X^{g-1} + \ldots + \mu^{g-1}b_1X + \mu^g \in \mathbb{F}_\ell[X], \]

where \(\mu\) is the multiplicator of \(M\). Therefore, upon factoring \(\text{char}_M(X)\) over \(\mathbb{F}_\ell\), we obtain that there exist \(\lambda_1(M), \ldots, \lambda_g(M) \in \mathbb{F}_\ell\) such that

\[ \text{char}_M(X) = \prod_{1 \leq i \leq g} (X - \lambda_i(M))(X - \mu \lambda_i^{-1}(M)) \in \mathbb{F}_\ell[X]. \]
With notation as above, we introduce the following subsets associated to $\text{GSp}_{2g}(\mathbb{F}_t)$, an integer $t$, and a positive real number $z$:

\[
\begin{align*}
C_0(\ell, t) &:= \{ M \in \text{GSp}_{2g}(\mathbb{F}_t) : \text{tr} M = -t(\mod \ell) \} ; \\
C(\ell, t) &:= \{ M \in \text{GSp}_{2g}(\mathbb{F}_t) : \lambda_i(M) \in \mathbb{F}_t^* \ 1 \leq i \leq g, \ \text{tr} M = -t(\mod \ell) \} ; \\
C^{ss}(\ell, t) &:= \{ M \in C(\ell, t) : M \text{ semisimple} \} ; \\
C_B(\ell, t) &:= C(\ell, t) \cap B_{2g}(\mathbb{F}_t) ; \\
C_0(\ell, 0) &:= \text{the image of } C_0(\ell, 0) \text{ in } \text{PGSp}_{2g}(\mathbb{F}_t) ; \\
C_B(\ell, t) &:= \text{the image of } C_B(\ell, t) \text{ in } B_{2g}(\mathbb{F}_t)/U_{2g}(\mathbb{F}_t) ; \\
\overline{C_B}(\ell, |t| \leq z) &:= \text{the image of } C_B(\ell, |t| \leq z) \text{ in } B_{2g}(\mathbb{F}_t)/U_{2g}(\mathbb{F}_t) .
\end{align*}
\]

For the rest of the section, we focus on properties of these subsets that will be used in the proofs of Theorems 1 - 3.

**Proposition 12.** Assume that the prime $\ell$ satisfies $\ell \nmid 2g$. Given any integer $t$ and any positive real number $z$, the following properties hold.

(i) The sets $C^{ss}(\ell, t)$ and $C^{ss}(\ell, |t| \leq z)$ are non-empty and stable under conjugation by elements of $\text{GSp}_{2g}(\mathbb{F}_t)$.

(ii) The sets $C_B(\ell, t)$ and $C_B(\ell, |t| \leq z)$ are non-empty and stable under conjugation by elements of $B_{2g}(\mathbb{F}_t)$.

(iii) Every element in $C^{ss}(\ell, t) \cup C^{ss}(\ell, |t| \leq z)$ is conjugate over $\text{GSp}_{2g}(\mathbb{F}_t)$ to some element of $B_{2g}(\mathbb{F}_t)$.

(iv) We have the set inclusions

\[
\begin{align*}
U_{2g}(\mathbb{F}_t) \ C_B(\ell, t) &\subseteq C_B(\ell, t) ; \\
U_{2g}'(\mathbb{F}_t) \ C_B(\ell, 0) &\subseteq C_B(\ell, 0) ; \\
U_{2g}(\mathbb{F}_t) \ C_B(\ell, |t| \leq z) &\subseteq C_B(\ell, |t| \leq z) .
\end{align*}
\]

**Proof.** (i) Since $\ell \nmid 2g$, the inverses $2^{-1}(\mod \ell)$ and $g^{-1}(\mod \ell)$ exist. We consider the cases $\ell \nmid (t + g)$ and $\ell | (t + g)$ separately and show that, in either case, $C^{ss}(\ell, t) \neq \emptyset$. 


If $\ell \nmid (t + g)$, then the inverse $(t + g)^{-1}(\text{mod } \ell)$ exists. We define

$$M := \text{diag} \left( (1 \text{ (mod } \ell)), \ldots, (1 \text{ (mod } \ell)), -(t + g)^{-1} \text{ (mod } \ell), -(t + g)^{-1}g^{-1} \text{ (mod } \ell) \right) \in T_{2g}(\mathbb{F}_\ell).$$

Since $M$ is semisimple and $\text{tr } M = -t(\text{mod } \ell)$, we obtain that $M$ belongs to $C^{ss}(\ell, t)$.

If $\ell \mid (t + g)$, we define

$$M := \text{diag} \left( 2^{-1} \text{ (mod } \ell), \ldots, 2^{-1} \text{ (mod } \ell), (1 - 2^{-1}) \text{ (mod } \ell), (1 - 2^{-1}) \text{ (mod } \ell) \right) \in T_{2g}(\mathbb{F}_\ell).$$

Since $(1 - 2^{-1}) \text{ (mod } \ell)$ is non-zero and $g \equiv -t(\text{mod } \ell)$, we obtain that $M$ is semisimple and $\text{tr } M = -t(\text{mod } \ell)$, that is, that $M$ belongs to $C^{ss}(\ell, t)$.

We will show now that the set $C^{ss}(\ell, t)$ is stable under conjugation by elements of $\text{GSp}_{2g}(\mathbb{F}_\ell)$. First, observe that, for any $M \in C^{ss}(\ell, t)$ and any $N \in \text{GSp}_{2g}(\mathbb{F}_\ell)$, we have

$$\text{tr}(NMN^{-1}) = \text{tr}(M) = -t(\text{mod } \ell).$$

It remains to check that $NMN^{-1}$ is semisimple. Since $M$ is semisimple, there exists $A \in \text{GL}_{2g}(\mathbb{F}_\ell)$, such that $AMA^{-1}$ is a diagonal matrix in $M_{2g}(\mathbb{F}_\ell)$. Taking $A' := AN^{-1} \in \text{GL}_{2g}(\mathbb{F}_\ell)$, we obtain that

$$A'(NMN^{-1})A'^{-1} = AMA^{-1}$$

is a diagonal matrix in $M_{2g}(\mathbb{F}_\ell)$. As a consequence, $C^{ss}(\ell, t)$ is stable under conjugation by elements of $\text{GSp}_{2g}(\mathbb{F}_\ell)$.

(ii) Since $C^{ss}(\ell, t) \subseteq C_B(\ell, t)$, we deduce from (i) that $C_B(\ell, t) \neq \emptyset$. The set $C_B(\ell, t)$ is stable under conjugation by elements of $B_{2g}(\mathbb{F}_\ell)$ because both $C^{ss}(\ell, t)$ and $B_{2g}(\mathbb{F}_\ell)$ are stable under conjugation by elements of $B_{2g}(\mathbb{F}_\ell)$. The similar result about $C_B(\ell, |t| \leq z)$ follows by noting that $C_B(\ell, |t| \leq z) = \bigcup_{|t| \leq z} C_B(\ell, t)$.

(iii) Let $M \in C^{ss}(\ell, t)$, with multiplicator $\mu$. Then

$$\text{char}_M(X) = \prod_{1 \leq i \leq g} (X - \lambda_i(M))(X - \mu \lambda_i^{-1}(M)) \in \mathbb{F}_\ell[X].$$

Define

$$M' := \text{diag} \left( \lambda_1(M), \ldots, \lambda_g(M), \mu \lambda_1^{-1}(M), \ldots, \mu \lambda_g^{-1}(M) \right) \in B_{2g}(\mathbb{F}_\ell).$$

Since $M', M$ are semisimple and $\text{char}_M(X) = \text{char}_{M'}(X)$, by [Ch97, Lemma 3.4] we deduce that $M$ is conjugate over $\text{GSp}_{2g}(\mathbb{F}_\ell)$ to some element of $B_{2g}(\mathbb{F}_\ell)$. Since each element $M$ of $C^{ss}(\ell, |t| \leq z)$ is an element of $C^{ss}(\ell, t)$ for some integer $t$ with $|t| \leq z$, by the previous argument we deduce that $M$ is also conjugate over $\text{GSp}_{2g}(\mathbb{F}_\ell)$ to some element of $B_{2g}(\mathbb{F}_\ell)$.

(iv) Let $M_1 \in U_{2g}(\mathbb{F}_\ell)$ and $M_2 \in C_B(\ell, t)$. Then $M_1M_2 \in B_{2g}(\mathbb{F}_\ell)$ and $M_1M_2$ has the same diagonal entries as $M_2$. Since $\text{tr } M_2 = -t(\text{mod } \ell)$, we obtain that $\text{tr}(M_1M_2) = -t(\text{mod } \ell)$. As such, $U_{2g}(\mathbb{F}_\ell)C_B(\ell, t) \subseteq C_B(\ell, t)$. 19
Now let $M_1 \in U'_2(\mathbb{F}_\ell)$ and $M_2 \in C_B(\ell,0)$. Denote the diagonal elements of $M_1$ by $a$. Then $M_1M_2 \in B_{2g}(\mathbb{F}_\ell)$ and $\text{tr}(M_1M_2) = a \text{ tr } M_2 = 0$. As such, $U'_2(\mathbb{F}_\ell) \ C_B(\ell,0) \subseteq C_B(\ell,0)$.

The result about $C_B(\ell, |t| \leq z)$ follows from the observation that $U_{2g}(\mathbb{F}_\ell) \ C_B(\ell, |t| \leq z) = \bigcup_{t \in \mathbb{Z}, |t| \leq z} U_{2g}(\mathbb{F}_\ell) \ C_B(\ell, t) \subseteq \bigcup_{t \in \mathbb{Z}, |t| \leq z} C_B(\ell, t)$.

\[ \text{Proposition 13. Assume that the prime } \ell \text{ is odd. Given any integer } t \text{ and any positive real number } z, \text{ the following upper bounds hold:} \]

\[ \# C_0(\ell, t) \ll \ell^{2g^2 + g}; \]

\[ \# \hat{C}_0(\ell, 0) \ll \ell^{2g^2 + g - 1}; \]

\[ \# C_B(\ell, t) \leq (\ell - 1)^g; \]

\[ \# \hat{C}_B(\ell, 0) \leq (\ell - 1)^{g - 1}; \]

\[ \# C_B(\ell, |t| \leq z) \leq (2z + 1)(\ell - 1)^g. \]

\[ \text{Proof. We recall from the calculation in [CoDaSiSt17] (9), p. 3569] that} \]

\[ \frac{\# C_0(\ell, t)}{\# \text{GSp}_{2g}(\mathbb{F}_\ell)} = \frac{1}{\ell} + O \left( \frac{1}{\ell^3} \right). \]

Then the upper bound for $\# C_0(\ell, t)$ follows from the asymptotic above and the upper bound $\# \text{GSp}_{2g}(\mathbb{F}_\ell) \ll \ell^{2g^2 + g + 1}$ derived from Proposition 9.

Noting that $\Lambda(\mathbb{F}_\ell) C_0(\ell,0) = C_0(\ell,0)$,

we obtain that the inverse image of $C_0(\ell, 0)$ in $\text{GSp}_{2g}(\mathbb{F}_\ell)$ is $C_0(\ell, 0)$. Therefore,

\[ \# \hat{C}_0(\ell, 0) = \frac{\# C_0(\ell, t)}{\# \text{GSp}_{2g}(\mathbb{F}_\ell)} \ll \ell^{2g^2 + g - 1}. \]

Recalling from Proposition 11 that $B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell) \simeq T_{2g}(\mathbb{F}_\ell)$, we deduce that, under this bijection, $\hat{C}_B(\ell, t)$ may be identified with the set of matrices

\[ \{ M \in T_{2g}(\mathbb{F}_\ell) : \text{ tr } M = -t(\mod \ell) \}. \]
Then, using the definition of $T_{2g}(F_{\ell})$, we obtain that
\[
\#\hat{C}_B(\ell, t) \leq \#\{ (a_1, \ldots, a_g, \mu) \in (F_{\ell}^\times)^{g+1} : \sum_{1 \leq i \leq g} a_i + \mu \sum_{1 \leq i \leq g} a_i^{-1} = -t (\mod \ell) \}
= \sum_{(a_1, \ldots, a_g) \in (F_{\ell}^\times)^g} \#\{ \mu \in F_{\ell}^\times : \sum_{1 \leq i \leq g} a_i + \mu \sum_{1 \leq i \leq g} a_i^{-1} = -t (\mod \ell) \}
\leq \sum_{(a_1, \ldots, a_g) \in (F_{\ell}^\times)^g} 1
= (\ell - 1)^g.
\]

To estimate $\#\hat{C}_B'(\ell, 0)$, we observe first that the set $\hat{C}_B(\ell, 0)$ surjects onto $\hat{C}_B'(\ell, 0)$ under the reduction map $B_{2g}(F_{\ell})/U_{2g}(F_{\ell}) \to B_{2g}(F_{\ell})/U_{2g}'(F_{\ell})$. Next, we observe that the inverse image of $\hat{C}_B'(\ell, 0)$ in $B_{2g}(F_{\ell})$ is of the form $U_{2g}(F_{\ell})C_B(\ell, 0)$, which is equal to $C_B(\ell, 0)$ by applying part (iv) of Proposition 12 and by noting that the inclusion is actually an equality. Thus the inverse image of $\hat{C}_B'(\ell, 0)$ in $B_{2g}(F_{\ell})/U_{2g}(F_{\ell})$ is $C_B(\ell, 0)$. Consequently,
\[
\#\hat{C}_B'(\ell, 0) = \frac{\#\hat{C}_B(\ell, 0)}{\#(U_{2g}(F_{\ell})/U_{2g}(F_{\ell}))} \leq (\ell - 1)^{g-1}.
\]

Lastly, to estimate the size of $\#\hat{C}_B(\ell, |t| \leq z)$, we simply observe that
\[
\#\hat{C}_B(\ell, |t| \leq z) = \sum_{|t| \leq z} \#\hat{C}_B(\ell, t) \leq (2z + 1)(\ell - 1)^g.
\]

6. Proofs of Theorems 1 - 3

In this section, we prove Theorems 1 - 3 using the preliminary results presented in Sections 3 - 5.

6.1. Background on abelian varieties. We start with a summary of properties of abelian varieties.

We refer the reader to the papers [Fa83, Ho68, Oo08, Se85, Se86, Ta66, Wa69, Za18] and to the books [CoSi86, La83, Mu70] for the theory of abelian varieties.

We start by considering an abelian variety $A$ defined over an arbitrary field $F$ and of dimension $g$. For an integer $n \geq 1$, we write $A[n]$ for the group of $n$-torsion elements of $A(F)$ and we write $F(A[n])$ for the extension of $F$ generated by $A[n]$. For a rational prime $\ell \neq \text{char } F$, we write $T_{\ell}(A)$ for the $\ell$-adic Tate module of $A$, defined as the inverse limit $\varprojlim A[\ell^k]$. We recall that, if $\gcd(n, \text{char } F) = 1$, then $A[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$, endowed with an action of the absolute Galois group $\text{Gal}(F^{\text{sep}}/F)$, and if $\ell \neq \text{char } F$, then $T_{\ell}(A)$ is a free $\mathbb{Z}_{\ell}$-module of rank $2g$, endowed with a continuous action of $\text{Gal}(F^{\text{sep}}/F)$. These Galois actions give rise to group homomorphisms
\[
(10) \quad \text{Gal}(F^{\text{sep}}/F) \longrightarrow \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(A[n])
\]
and

\( \text{Gal}(F^{\text{sep}}/F) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \),

which we call the residual modulo \( n \) Galois representation of \( A \) and the \( \ell \)-adic Galois representation of \( A \), respectively. The latter form a compatible system.

Next, we focus our attention on an abelian variety \( A \) defined over \( \mathbb{Q} \) and of dimension \( g \). We denote by \( N_A \) the conductor of \( A \). For a prime \( p \nmid N_A \), we denote by \( A_p \) the reduction of \( A \) modulo \( p \), which is an abelian variety defined over \( \mathbb{F}_p \) and of dimension \( g \).

Associated to \( A \) and an integer \( n \geq 1 \), we have the residual modulo \( n \) Galois representation

\( \rho_{A,n} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(A[n]) \),

about which it is known that

\( \mathbb{Q}(A[n]) = \overline{\mathbb{Q}}^{\text{Ker} \rho_{A,n}} \)

and that

\( \rho_{A,n} \) is unramified outside the primes dividing \( nN_A \).

Associated to \( A \) and a prime \( \ell \), we have the \( \ell \)-adic Galois representation

\( \rho_{A,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \).

Associated to \( A \), a prime \( p \nmid N_A \), and an integer \( n \geq 1 \) such that \( p \nmid n \), we have the residual modulo \( n \) Galois representation

\( \rho_{A_p,n} : \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(A_p[n]). \)

Associated to \( A \), a prime \( p \nmid N_A \), and another prime \( \ell \neq p \), we have the \( \ell \)-adic Galois representation

\( \rho_{A_p,\ell} : \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(A_p)). \)

Now let us fix primes \( p \) and \( \ell \) such that \( p \nmid \ell N_A \). The \( p \)-th power Frobenius \( \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p \), \( \alpha \mapsto \alpha^p \), gives rise to an \( \mathbb{F}_p \)-endomorphism \( \pi_p(A) \in \text{End}_{\mathbb{F}_p}(A_p) \) of \( A_p \), which, in turn, gives rise to a \( \mathbb{Z}_\ell \)-linear operator \( \pi_p(A)|_{T_\ell(A_p)} \) on \( T_\ell(A_p) \) and an \( \mathbb{F}_\ell \)-linear operator \( \pi_p(A)|_{A_p[\ell]} \) on \( A_p[\ell] \), both of which we shall also call \( \pi_p(A) \). We denote by \( P_{\pi_p(A)}(X) \in \mathbb{Z}_\ell[X] \) the characteristic polynomial of \( \pi_p(A) \) acting on \( T_\ell(A_p) \) and recall the following important properties.

**Proposition 14.** Let \( A \) be an abelian variety defined over \( \mathbb{Q} \), of conductor \( N_A \), and of dimension \( g \). Let \( p \) and \( \ell \) be primes such that \( p \nmid \ell N_A \). Then \( P_{\pi_p(A)}(X) \) is a \( p \)-Weil polynomial of degree \( 2g \), whose coefficients are integers that are independent of the choice of \( \ell \).

**Proof.** See [Mi86], Theorem 19.1, p. 143. \( \square \)
We write

\[ P_{\pi_p(A)}(X) = X^{2g} + a_{1,p}(A)X^{2g-1} + a_{2,p}(A)X^{2g-2} + \ldots + a_{g,p}(A)X^g + pa_{g-1,p}(A)X^{g-1} + p^2a_{g-2,p}(A)X^{g-2} + \ldots + p^g \in \mathbb{Z}[X]. \]

Over \( \overline{\mathbb{Q}} \), we write

\[ P_{\pi_p(A)}(X) = \prod_{1 \leq i \leq 2g} (X - \alpha_i) \in \overline{\mathbb{Q}}[X], \]

where \( \alpha_1, \ldots, \alpha_g \in \overline{\mathbb{Q}} \) have the property that, for any \( \sigma \in \text{Aut}(\mathbb{C}) \),

\[ |\sigma(\alpha_i)| = \sqrt{p} \quad \forall 1 \leq i \leq 2g. \tag{20} \]

Note that the discriminant \( \text{disc} P_{\pi_p(A)}(X) \) of the polynomial \( P_{\pi_p(A)}(X) \) is an integer, defined by the product

\[ \text{disc} P_{\pi_p(A)}(X) = \prod_{1 \leq i < j \leq 2g} (\alpha_i - \alpha_j)^2. \tag{21} \]

Thanks to (20), the absolute value of this discriminant satisfies the upper bound

\[ |\text{disc} P_{\pi_p(A)}(X)| \leq (4p)^{(2g-1)g}. \tag{22} \]

In light of Proposition 14, \( \pi_p(A) \) may be regarded as a \( p \)-Weil number, that is, as an algebraic integer for which, for any \( \sigma \in \text{Aut}(\mathbb{C}) \), we have that \( |\sigma(\pi_p(A))| = \sqrt{p} \). Associated to this algebraic integer, we have its minimal polynomial \( Q_{\pi_p(A)}(X) \in \mathbb{Z}[X] \) over \( \mathbb{Q} \), the number field \( \mathbb{Q}(\pi_p(A)) \) that it generates, and the Galois closure \( K_{A,p} \) of \( \mathbb{Q}(\pi_p(A)) \) in \( \overline{\mathbb{Q}} \). In what follows, we record properties of the extensions \( \mathbb{Q}(\pi_p(A))/\mathbb{Q} \) and \( K_{A,p}/\mathbb{Q} \).

**Proposition 15.** Let \( A \) be an abelian variety defined over \( \mathbb{Q} \), of conductor \( N_A \), and of dimension \( g \). Let \( p \) be a prime such that \( p \nmid N_A \).

(i) The degrees of \( \mathbb{Q}(\pi_p(A))/\mathbb{Q} \) and \( K_{A,p}/\mathbb{Q} \) satisfy the upper bounds

\[ [\mathbb{Q}(\pi_p(A)) : \mathbb{Q}] \leq 2g \quad \text{and} \quad [K_{A,p} : \mathbb{Q}] \leq g! \cdot 2^g. \]

(ii) The absolute values of the discriminants of \( \mathbb{Q}(\pi_p(A))/\mathbb{Q} \) and \( K_{A,p}/\mathbb{Q} \) satisfy the upper bounds

\[ |d_{K_{A,p}}| \leq |d_{\mathbb{Q}(\pi_p(A))}|g! \cdot 2^{g-1} \leq (4p)^g \cdot 2^{g-1}(2g-1) \cdot (2g-1)^g. \]

**Proof.** (i) For the degree of \( \mathbb{Q}(\pi_p(A))/\mathbb{Q} \), we observe that

\[ [\mathbb{Q}(\pi_p(A)) : \mathbb{Q}] = \deg Q_{\pi_p(A)}(X) \leq \deg P_{\pi_p(A)}(X) = 2g. \]

For the degree of \( K_{A,p}/\mathbb{Q} \), we sketch the following well-known argument. Recall from Proposition 14 that \( P_{\pi_p(A)}(X) \) is a \( p \)-Weil polynomial, having \( \pi_p(A) \) as one of its roots in \( \overline{\mathbb{Q}} \). The complex roots \( \alpha_1, \ldots, \alpha_{2g} \) of \( P_{\pi_p(A)}(X) \), introduced in (19), come in pairs \( \left( \alpha_1, \frac{\alpha_1}{p} \right), \ldots, \left( \alpha_g, \frac{\alpha_g}{p} \right) \). As such, the Galois group \( \text{Gal}(K_{A,p}/\mathbb{Q}) \)
of the Galois closure of \( \mathbb{Q}(\pi_p(A)) \) in \( \overline{\mathbb{Q}} \) embeds into the subgroup \( W_{2g} \) of the permutation group \( S_{2g} \) on \( 2g \) elements which induces a permutation on the set of pairs \( (1, 2), \ldots, (2g-1, 2g) \). The group structure of \( W_{2g} \) is obtained by noting that the action of \( W_{2g} \) on the above pairs of integers gives rise to a short exact sequence of groups \( 1 \to H \to W_{2g} \to S_g \to 1 \), where \( H \) is the group generated by the transpositions \( (1, 2), \ldots, (2g-1, 2g) \) and where \( S_g \) is the permutation group on \( g \) elements. Thus \( H \cong (\mathbb{Z}/2\mathbb{Z})^g \) and \( W_{2g} \cong (\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g \). Consequently, \( [K_{A,p} : \mathbb{Q}] \leq \#W_{2g} = g! 2^g \). For more details, see, for example, the discussion in [Ch97] pp. 168–169.

(ii) On one hand, we have the inclusion of orders \( \mathbb{Z}[\pi_p(A)] \subseteq \mathcal{O}_{\mathbb{Q}(\pi_p(A))} \) in \( \mathbb{Q}(\pi_p(A)) \). By comparing their discriminants, we obtain the relation

\[
disc_{\mathbb{Q}(\pi_p(A))} Q_{\pi_p(A)}(X) = c_{A,p}^2 d_{\mathbb{Q}(\pi_p(A))},
\]

where

\[
c_{A,p} := \#(\mathcal{O}_{\mathbb{Q}(\pi_p(A))}/\mathbb{Z}[\pi_p(A)]) \in \mathbb{Z}.
\]

In particular, we obtain the divisibility

\[
d_{\mathbb{Q}(\pi_p(A))} | disc_{\mathbb{Q}(\pi_p(A))} Q_{\pi_p(A)}(X) \text{ in } \mathbb{Z}.
\]

Since we also have the divisibility

\[
Q_{\pi_p(A)}(X) | P_{\pi_p(A)}(X) \text{ in } \mathbb{Z}[X],
\]

we deduce the divisibility relations

\[
d_{\mathbb{Q}(\pi_p(A))} | disc_{\mathbb{Q}(\pi_p(A))} Q_{\pi_p(A)}(X) | disc_{\mathbb{Q}(\pi_p(A))} P_{\pi_p(A)}(X) \text{ in } \mathbb{Z}.
\]

On the other hand, we have the inclusion of number fields \( \mathbb{Q}(\pi_p(A)) \subseteq K_{A,p} \). Since \( K_{A,p} \) is the smallest normal extension of \( \mathbb{Q}(\pi_p(A)) \) in \( \overline{\mathbb{Q}} \), by comparing discriminants and recalling [La94] p. 327, we obtain the inequality

\[
|d_{K_{A,p}}| \leq |d_{\mathbb{Q}(\pi_p(A))}| g! 2^{g-1}.
\]

Putting together (22), (25), and (26), we deduce the inequalities claimed in (ii). \( \square \)

Fixing a Frobenius element \( \text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) at \( p \), we obtain the \( \mathbb{Z}_l \)-linear operator \( \rho_{A,l}(\text{Frob}_p) \) on \( T_l(A) \) and the \( \mathbb{F}_l \)-linear operator \( \overline{\rho}_{A,l}(\text{Frob}_p) \) on \( A[l] \). We denote by \( P_{A,p}(X) \in \mathbb{Z}_l[X] \) the characteristic polynomial of \( \rho_{A,l}(\text{Frob}_p) \) acting on \( T_l(A) \) and by \( P_{A,p}(X) \in \mathbb{F}_l[X] \) the characteristic polynomial of \( \overline{\rho}_{A,l}(\text{Frob}_p) \) acting on \( A[l] \). We denote by \( Q_{A,p}(X) \in \mathbb{F}_l[X] \) the minimal polynomial of \( \overline{\rho}_{A,l}(\text{Frob}_p) \) acting on \( A[l] \). The latter two polynomials satisfy the following two divisibility relations:

\[
Q_{A,p}(X) | P_{A,p}(X) \text{ in } \mathbb{F}_l[X]
\]
and

\[(28) \quad \mathcal{P}_{A,p}(X) \mid Q_{A,p}(X)^\infty \text{ in } \mathbb{F}_\ell[X] \]

(see, for example, [A109] Corollary 7.10, Proposition 7.9, p. 376). In the next two propositions, we relate the polynomials $P_{A,p}(X)$ and $\mathcal{P}_{A,p}(X)$ to $P_{\pi_p(A)}(X)$, and the polynomial $Q_{A,p}(X)$ to $Q_{\pi_p(A)}(X)$.

**Proposition 16.** Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. Let $p$ and $\ell$ be primes such that $p \nmid \ell N_A$. Then

(i) $P_{A,p}(X) = P_{\pi_p(A)}(X) \in \mathbb{Z}[X]$;

(ii) $\mathcal{P}_{A,p}(X) = P_{\pi_p(A)}(X)(\mod \ell) \in \mathbb{F}_\ell[X]$.

**Proof.** The $\mathbb{Z}_\ell$-module isomorphisms

$$T_\ell(A_p) \simeq_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{2g} \simeq_{\mathbb{Z}_\ell} T_\ell(A)$$

and the $\mathbb{F}_\ell$-vector space isomorphisms

$$A_p[\ell] \simeq_{\mathbb{F}_\ell} \mathbb{F}_\ell^{2g} \simeq_{\mathbb{F}_\ell} A[\ell]$$

give rise to the following commutative diagram of ring isomorphisms, in which the top horizontal row is also an isomorphism of $\mathbb{Z}_\ell$-algebras and the bottom horizontal row is also an isomorphism of $\mathbb{F}_\ell$-algebras:

\[
\begin{array}{ccc}
\text{End}_{\mathbb{Z}_\ell}(T_\ell(A)) & \overset{\simeq_{\mathbb{Z}_\ell, \text{alg}}}{\longrightarrow} & \text{End}(T_\ell(A_p)) \\
\downarrow & & \downarrow \\
\text{End}_{\mathbb{F}_\ell}(A[\ell]) & \overset{\simeq_{\mathbb{F}_\ell, \text{alg}}}{\longrightarrow} & \text{End}_{\mathbb{F}_\ell}(A_p[\ell]).
\end{array}
\]

Under this diagram, by moving to the right and down, the operator $\rho_{A,\ell}(\text{Frob}_p) \in \text{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ is mapped to $\pi_p(A)|_{T_\ell(A_p)} \in \text{End}_{\mathbb{Z}_\ell}(T_\ell(A_p))$ and then to $\pi_p(A)|_{A_p[\ell]} \in \text{End}_{\mathbb{F}_\ell}(A_p[\ell])$; by moving down and to the left, it is mapped to $\mathfrak{p}_{A,\ell}(\text{Frob}_p) \in \text{End}_{\mathbb{F}_\ell}(A[\ell])$ and then again to $\pi_p(A)|_{A_p[\ell]} \in \text{End}_{\mathbb{F}_\ell}(A_p[\ell])$. Hence the polynomial relations (i) and (ii) between the various associated characteristic polynomials hold.

**Proposition 17.** Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. Let $p$ and $\ell$ be primes such that $p \nmid \ell N_A$. Then

$$Q_{A,p}(X) \mid Q_{\pi_p(A)}(X)(\mod \ell) \text{ in } \mathbb{F}_\ell[X].$$

**Proof.** Viewing $Q_{\pi_p(A)}(X)(\mod \ell) \in \mathbb{F}_\ell[X]$ as a polynomial over the ring of $\mathbb{F}_\ell$-linear operators on $A_p[\ell]$, we see that $\pi_p(A)|_{A_p[\ell]}$ is one of its roots. Recall that, under the isomorphism of $\mathbb{F}_\ell$-algebras $\text{End}_{\mathbb{F}_\ell}(A_p[\ell]) \rightarrow \text{End}_{\mathbb{F}_\ell}(A[\ell])$, the operator $\pi_p(A)|_{A_p[\ell]}$ is mapped to $\mathfrak{p}_{A,\ell}(\text{Frob}_p)$. Then, since $Q_{A,p}(X)$ is the minimal polynomial of $\mathfrak{p}_{A,\ell}(\text{Frob}_p)$, we deduce that $Q_{A,p}(X) \mid Q_{\pi_p(A)}(X)(\mod \ell)$ as polynomials in $\mathbb{F}_\ell[X]$.

Finally, we record the following result which will play an important role in the proofs of our main theorems.
**Proposition 18.** Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. Let $p$ and $\ell$ be primes such that $p \nmid \ell N_A$. Assume that $\ell \nmid c_{A,p}$ (defined in (24)) and that $\ell$ splits completely in $\mathbb{Q}(\pi_p(A))$. Then the $\mathbb{F}_\ell$-linear operator $\overline{\rho}_{A,\ell}(\text{Frob}_p) \in \text{End}_{\mathbb{F}_\ell}(A[\ell])$ is semisimple (that is, the minimal polynomial $Q_{A,p}(X)$ has distinct roots in $\mathbb{F}_\ell$) and has all its eigenvalues in $\mathbb{F}_\ell^\times$ (that is, all the roots of the characteristic polynomial $P_{A,p}(X)$ are in $\mathbb{F}_\ell^\times$).

**Proof.** Since $\ell \nmid c_{A,p}$ and $\ell$ splits completely in $\mathbb{Q}(\pi_p(A))$, by a classical theorem of Dedekind, the reduction modulo $\ell$ of the minimal polynomial $Q_{\pi_p(A)}(X)$ of the algebraic integer $\pi_p(A)$ factors into distinct linear factors in $\mathbb{F}_\ell[X]$. Then, using the divisibility relation $Q_{A,p}(X) \mid Q_{\pi_p(A)}(X) (\text{mod } \ell)$ as polynomials in $\mathbb{F}_\ell[X]$, proven in Proposition 17, we deduce that $Q_{A,p}(X)$ factors into distinct linear factors in $\mathbb{F}_\ell[X]$. Since $Q_{A,p}(X)$ is the minimal polynomial of the $\mathbb{F}_\ell$-linear operator $\overline{\rho}_{A,\ell}(\text{Frob}_p)$ acting on $A[\ell]$, we obtain that $\overline{\rho}_{A,\ell}(\text{Frob}_p)$ is semisimple. Furthermore, using (28), we obtain that the characteristic polynomial $P_{A,p}(X)$ has all its roots in $\mathbb{F}_\ell$. This means that all eigenvalues of $\overline{\rho}_{A,\ell}(\text{Frob}_p)$ are in $\mathbb{F}_\ell$. Since $\overline{\rho}_{A,\ell}(\text{Frob}_p)$ is invertible, the eigenvalues are in fact in $\mathbb{F}_\ell^\times$. □

**6.2. A variation on counting primes with a fixed Frobenius trace.** The first step in the proofs of Theorem 1 and part (i) of Theorem 3 is the following result established in analogy with [CoWa22, Lemma 18].

**Proposition 19.** Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. For each $x > 2$, let $y = y(x) > 2$ and $u = u(x) > 2$ be such that

$$u \leq y.$$  

Assume that, for any $\varepsilon > 0$,

$$u \geq c'(\varepsilon) y^{\frac{1}{2}} (\log y)^{2+\varepsilon}$$

for some constant $c'(\varepsilon) > 0$

and

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

Assume RH, as well as GRH for the number fields $K_{A,p}$ defined in Section 6.1., where $p \nmid N_A$ is an arbitrary prime. Then, for any $\varepsilon > 0$, there exists a constant $c(\varepsilon) > 0$ such that:

(i) for any $t \in \mathbb{Z}$ and any sufficiently large $x$, we have

$$\# \left\{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \right\} \leq c(\varepsilon) \max_{y \leq t \leq x} \# \left\{ p \leq x : p \nmid \ell N_A, a_{1,p}(A) = t, \ell \nmid d_{\mathbb{Q}(\pi_p(A))}\left(\mathcal{O}_{\mathbb{Q}(\pi_p(A))}/\mathbb{Z}[\pi_p(A)]\right), \ell \text{ splits completely in } \mathbb{Q}(\pi_p(A)) \right\}$$
(ii) for any $z > 0$ and any sufficiently large $x > 0$, we have

\[
\sum_{t \in \mathbb{Z}} \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \} \leq c(\varepsilon) \max_{y \leq \ell \leq y + u} \sum_{t \in \mathbb{Z}} \# \{ p \leq x : p \nmid \ell N_A, a_{1,p}(A) = t, \ell \nmid d_{\mathbb{Q}(\pi_p(A))} \mathbb{Z}[\pi_p(A)] \}, \quad \ell \text{ splits completely in } \mathbb{Q}(\pi_p(A)) \}.
\]

**Proof.** The proof follows the main steps of that of [CoWa22, Lemma 9], as we now explain. To simplify the exposition, for $x > 0$, $t \in \mathbb{Z}$, and $\ell$ a rational prime, we use the notation

\[
\pi_A(x, \ell, t) := \# \{ p \leq x : p \nmid \ell N_A, a_{1,p}(A) = t, \ell \nmid d_{\mathbb{Q}(\pi_p(A))}c_{A,p}, \ell \text{ splits completely in } \mathbb{Q}(\pi_p(A)) \}
\]

and

\[
\pi'_A(x, \ell, t) := \# \{ p \leq x : p \nmid \ell N_A, a_{1,p}(A) = t, \ell \nmid d_{K_A,p}c_{A,p}, \ell \text{ splits completely in } K_{A,p} \},
\]

where $c_{A,p} = \#(\mathcal{O}_{\mathbb{Q}(\pi_p(A))}/\mathbb{Z}[\pi_p(A)])$, as defined in Section 6.1. Since we have the inclusion of number fields $\mathbb{Q}(\pi_p(A)) \subseteq K_{A,p}$, we deduce that $d_{\mathbb{Q}(\pi_p(A))} \mid d_{K_A,p}$, which implies that

\[
\pi'_A(x, \ell, t) \leq \pi_A(x, \ell, t).
\]

Therefore, it is enough to prove that

\[
\# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \} \leq c(\varepsilon) \max_{y \leq \ell \leq y + u} \pi'_A(x, \ell, t)
\]

and

\[
\sum_{t \in \mathbb{Z}} \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \} \leq c(\varepsilon) \max_{y \leq \ell \leq y + u} \sum_{t \in \mathbb{Z}} \pi'_A(x, \ell, t).
\]

First, observe that

\[
\sum_{y \leq \ell \leq y + u} \pi'_A(x, \ell, t) \leq (\pi(y + u) - \pi(y)) \max_{y \leq \ell \leq y + u} \pi'_A(x, \ell, t).
\]
Next, observe that

\[
\pi_A'(x, \ell, t) = \sum_{y \leq \ell \leq y+u} \# \{ y \leq \ell \leq y + u : \ell \mid p \text{ } d_{K_{A,p}, c_{A,p}}, \text{ } \ell \text{ splits completely in } K_{A,p} \}
\]

\[
= \sum_{p \leq x \atop a_{1,p}(A) = e} \# \{ y \leq \ell \leq y + u : \ell \mid p \text{ } d_{K_{A,p}, c_{A,p}}, \ell \text{ splits completely in } K_{A,p} \}
\]

\[
- \sum_{p \leq x \atop \mu(N_{A,p}) = 0} \# \{ y \leq \ell \leq y + u : \ell \mid p \text{ } d_{K_{A,p}, c_{A,p}}, \ell \mid c_{A,p}, \ell \text{ splits completely in } K_{A,p} \}
\]

\[
\geq \sum_{p \leq x \atop \mu(N_{A,p}) = 0} \# \{ y \leq \ell \leq y + u : \ell \mid p \text{ } d_{K_{A,p}, c_{A,p}}, \ell \text{ splits completely in } K_{A,p} \}
\]

\[
- \sum_{p \leq x \atop \mu(N_{A,p}) = 0} \nu(c_{A,p}),
\]

where, for an integer \( m \geq 1 \), we write \( \nu(m) \) for the number of its distinct prime factors.

Using the bound \( \log m \leq \log 2 \), we obtain that

\[
\nu(c_{A,p}) \leq \log c_{A,p}.
\]

Using (22), (23) and (24), we obtain that

\[
c_{A,p}^2 \ll (4p)^{g(2g-1)}.
\]

Therefore,

\[
\nu(c_{A,p}) \ll g \log p.
\]

Using this estimate in the last line of the sequence of inequalities (40), we obtain that

\[
\sum_{y \leq \ell \leq y+u} \pi_A'(x, \ell, t) \geq \sum_{p \leq x \atop a_{1,p}(A) = e} \# \{ y \leq \ell \leq y + u : \ell \mid p \text{ } d_{K_{A,p}, c_{A,p}}, \ell \text{ splits completely in } K_{A,p} \}
\]

\[
+ O(g (\pi_A(x, t) \log x)).
\]

Now we focus on the summands \( \# \{ y \leq \ell \leq y + u : \ell \mid p \text{ } d_{K_{A,p}, c_{A,p}}, \ell \text{ splits completely in } K_{A,p} \} \) appearing in (41). Recalling that we are assuming that GRH holds for each of the fields \( K_{A,p} \), from the effective version
of the Chebotarev Density Theorem stated in part (i) of Theorem 4, we know that

\[(42) \quad \# \{ y \leq \ell \leq y + u : \ell \nmid p \text{ for } d_{K,A,p}, \ell \text{ splits completely in } K_{A,p} \} = \frac{1}{[K_{A,p} : Q]} (\pi(y + u) - \pi(y)) \]

\[+ E_1(y, u, K_{A,p}) + E_2(y, u, K_{A,p}), \]

where the terms \(E_1(y, u, K_{A,p}), E_2(y, u, K_{A,p})\) are real valued functions of \(y, u,\) and \(p,\) that satisfy the upper bounds

\[(43) \quad |E_1(y, u, K_{A,p})| \leq c_1(y + u)^\frac{1}{2} \left( \frac{\log |d_{K,A,p}|}{[K_{A,p} : Q]} + \log(y + u) \right), \]

\[(44) \quad |E_2(y, u, K_{A,p})| \leq c_2y^{\frac{1}{2}} \left( \frac{\log |d_{K,A,p}|}{[K_{A,p} : Q]} + \log y \right), \]

with \(c_1, c_2\) some absolute positive constants.

To obtain an upper bound for the quotient \(\frac{\log |d_{K,A,p}|}{[K_{A,p} : Q]}\), we invoke inequality (9):

\[\frac{\log |d_{K,A,p}|}{[K_{A,p} : Q]} \leq \sum_{\ell | d_{K,A,p}} \log \ell + \log[K_{A,p} : Q] \leq \log |d_{K,A,p}| + \log[K_{A,p} : Q].\]

We recall from Proposition 13 that \([K_{A,p} : Q] \leq g! 2^g\) and \(|d_{K,A,p}| \leq (4p)g! 2^{g-1(2g-1)}g\). Therefore

\[\frac{\log |d_{K,A,p}|}{[K_{A,p} : Q]} \leq c_3(g) \log p\]

for some positive constant \(c_3(g)\) that depends on \(g\), but not on \(p\). Using this bound in (43) - (44) and then in (42), we obtain that

\[(45) \quad \# \{ y \leq \ell \leq y + u : \ell \nmid p \text{ for } d_{K,A,p}, \ell \text{ splits completely in } K_{A,p} \}
\]

\[= \frac{1}{[K_{A,p} : Q]} (\pi(y + u) - \pi(y)) + O_g \left( (y + u)^{\frac{1}{2}} \log(xy) \right) \]

\[\geq \frac{1}{2^g g!} (\pi(y + u) - \pi(y)) + O_g \left( (y + u)^{\frac{1}{2}} \log(xy) \right).\]

To understand the growth of the difference \(\pi(y + u) - \pi(y)\), we recall that we are assuming RH and that, as a function of \(y\), the parameter \(u\) satisfies (31). Then, for any \(\varepsilon > 0\) (which we choose arbitrarily and keep fixed), we know that

\[\pi(y + u) - \pi(y) \geq c_4(\varepsilon) \frac{u}{\log u} > 0\]

for some positive constant that depends on \(\varepsilon\) (but not on \(u\) and \(y\)).

Recalling (31), we deduce that

\[
\max_{y \leq \ell \leq y + u} \pi'(x, \ell, t) \geq c_5(g, \varepsilon) \pi_A(x, t) + O_{g,\varepsilon} \left( \frac{(y + u)^{\frac{1}{2}} \log(xy) \log u}{u} \pi_A(x, t) \right)
\]

for some positive constant \(c_5(g, \varepsilon)\) that depends on \(g\) and \(\varepsilon\). Invoking (29) and (31), we see that, as \(x \to \infty\), the \(O_{g,\varepsilon}\)-term above is \(o(\pi_A(x, t))\). This completes the proof of (32).
To prove (33), we use the same argument as for (32), except for replacing \( \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \} \) with \( \# \{ p \leq x : p \nmid N_A, |a_{1,p}(A)| \leq z \} \).

6.3. Proof of Theorem 1 for arbitrary \( t \in \mathbb{Z} \). Let \( A \) be an abelian variety defined over \( \mathbb{Q} \), of conductor \( N_A \), and of dimension \( g \). Let \( t \in \mathbb{Z} \). Let \( x > 2 \) be a real number that goes to infinity. Our goal in this subsection is to prove the upper bound for \( \pi_A(x, t) = \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \} \) claimed in Theorem 1 under the main assumptions (46) and (50) stated below.

It is known that we may always choose a polarization \( e \) on \( A \), which we now do, and that, for any sufficiently large prime \( \ell \), the polarization \( e \) gives rise to a non-degenerate alternating bilinear form \( e_\ell \) on \( T_\ell(A) \), with respect to which the group \( \text{GSp}(T_\ell(A), e_\ell) \) of symplectic similitudes contains the image \( \text{Im} \rho_{A,\ell} \) of \( \rho_{A,\ell} \) (see [Se85 p. 34]). Upon choosing an isomorphism \( \text{GSp}(T_\ell(A), e_\ell) \simeq \text{GSp}_{2g}(\mathbb{Z}_\ell) \), we may thus assume that \( \text{Im} \rho_{A,\ell} \leq \text{GSp}_{2g}(\mathbb{Z}_\ell) \), and hence that \( \text{Im} \overline{\rho}_{A,\ell} \leq \text{GSp}_{2g}(\mathbb{F}_\ell) \).

We assume that, for any sufficiently large prime \( \ell \), the residual modulo \( \ell \) Galois representation \( \overline{\rho}_{A,\ell} \) has image isomorphic to \( \text{GSp}_{2g}(\mathbb{F}_\ell) \), which implies that

\[
\text{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}) \simeq \text{GSp}_{2g}(\mathbb{F}_\ell).
\]

Considering the subextensions of \( \mathbb{Q}(A[\ell]) \) fixed by the subgroups \( U_{2g}(\mathbb{F}_\ell) \) and \( B_{2g}(\mathbb{F}_\ell) \) of \( \text{GSp}_{2g}(\mathbb{F}_\ell) \),

\[
\mathbb{Q} \subseteq \mathbb{Q}(A[\ell])^{U_{2g}(\mathbb{F}_\ell)} \subseteq \mathbb{Q}(A[\ell])^{B_{2g}(\mathbb{F}_\ell)} \subseteq \mathbb{Q}(A[\ell]),
\]

and recalling that, by part (ii) of Proposition 8 \( U_{2g}(\mathbb{F}_\ell) \) is a normal subgroup of \( B_{2g}(\mathbb{F}_\ell) \), we obtain the following Galois group structures:

\[
\text{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}(A[\ell])^{U_{2g}(\mathbb{F}_\ell)}) \simeq B_{2g}(\mathbb{F}_\ell),
\]

\[
\text{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}(A[\ell])^{B_{2g}(\mathbb{F}_\ell)}) \simeq U_{2g}(\mathbb{F}_\ell),
\]

\[
\text{Gal}(\mathbb{Q}(A[\ell])^{U_{2g}(\mathbb{F}_\ell)}/\mathbb{Q}(A[\ell])^{B_{2g}(\mathbb{F}_\ell)}) \simeq B_{2g}(\mathbb{F}_\ell)/U_{2g}(\mathbb{F}_\ell).
\]

We assume that

\[
\text{GRH holds.}
\]

More precisely, we assume the validity of RH and of GRH for the Dedekind zeta functions of the number fields \( \mathbb{Q}(A[\ell])^{U_{2g}(\mathbb{F}_\ell)} \) for all sufficiently large primes \( \ell \), as well as of the number fields \( K_{A,p} \) for all primes \( p \nmid N_A \).

By (32) of Proposition 19 for any real numbers \( y = y(x) > 2 \) and \( u = u(x) > 2 \) that depend on and grow with \( x \) and that satisfy (29), (30), and (31), we know that, for any \( \varepsilon > 0 \), there exists \( c(\varepsilon) > 0 \) such
that

\[ \pi_A(x, t) \leq c(\varepsilon) \max_{y \leq \ell \leq y + u} \# \{ p \leq x : p \nmid \ell N_A, a_1, p(A) = t \}, \]

\[ (51) \]

\[ \ell \nmid d_Q(\pi_p(A)) \#(\mathbb{Q}(\pi_p(A))/\mathbb{Z}[\pi_p(A)]) \], \ \ell \text{ splits completely in } \mathbb{Q}(\pi_p(A)). \]

We will use this inequality with \( x \) sufficiently large so that any prime \( \ell \) satisfying \( y \leq \ell \leq y + u \) is itself sufficiently large and \( \ell \) holds.

By observation \textbf{13} and Proposition \textbf{18} any prime \( p \) for which \( \ell \nmid d_Q(\pi_p(A)) \#(\mathbb{Q}(\pi_p(A))/\mathbb{Z}[\pi_p(A)]) \) and \( \ell \) splits completely in \( \mathbb{Q}(\pi_p(A)) \) has the property that, for any prime ideal \( \mathfrak{p} \) of \( \mathbb{Q}(\mathfrak{A}[\ell]) \) that lies over \( p \), we have that the matrix \( \mathfrak{p}_{A, \ell} \left( \left( \frac{Q(\mathfrak{A}[\ell])}{p} \right) \right) \in \text{GL}_2(\mathbb{F}_\ell) \) is semisimple and has all its eigenvalues in \( \mathbb{F}_\ell \). By part (ii) of Proposition \textbf{10} any prime \( p \nmid \ell N_A \) for which \( a_1, p(A) = t \) has the property that, for any prime ideal \( \mathfrak{p} \) of \( \mathbb{Q}(\mathfrak{A}[\ell]) \) that lies over \( p \), we have \( \text{tr} \mathfrak{p}_{A, \ell} \left( \left( \frac{Q(\mathfrak{A}[\ell])}{p} \right) \right) = \ell(t(\mod \ell)) \). Thus, every prime \( p \) counted on the right hand side of inequality \( (51) \) satisfies that, for any prime ideal \( \mathfrak{p} \) of \( \mathbb{Q}(\mathfrak{A}[\ell]) \) that lies over \( p \),

\[ \mathfrak{p}_{A, \ell} \left( \left( \frac{Q(\mathfrak{A}[\ell])}{p} \right) \right) \in C^{\ast \ast}(\ell, t). \]

Combining these observations with \( (51) \), we obtain the inequality

\[ (52) \]

\[ \pi_A(x, t) \leq c(\varepsilon) \max_{y \leq \ell \leq y + u} \pi_{C^{\ast \ast}(\ell, t)}(x, \mathbb{Q}(\mathfrak{A}[\ell])/\mathbb{Q}). \]

We estimate \( \pi_{C^{\ast \ast}(\ell, t)}(x, \mathbb{Q}(\mathfrak{A}[\ell])/\mathbb{Q}) \) by invoking Theorem \textbf{4} with \( K = \mathbb{Q}, L = \mathbb{Q}(\mathfrak{A}[\ell]), H = B_{2g}(\mathbb{F}_\ell), N = U_{2g}(\mathbb{F}_\ell), C_1 = C^{\ast \ast}(\ell, t), \) and \( C_2 = C(\ell, t) \). In this case, the hypotheses of Theorem \textbf{4} hold thanks to parts (iii) and (iv) of Proposition \textbf{12} to Proposition \textbf{11} and to our GRH assumption. We obtain that

\[ \pi_{C^{\ast \ast}(\ell, t)}(x, \mathbb{Q}(\mathfrak{A}[\ell])/\mathbb{Q}) \leq \frac{\#C_B(\ell, t) \cdot \#U_{2g}(\mathbb{F}_\ell)}{\#B_{2g}(\mathbb{F}_\ell)} \pi(x) \]

\[ + \left( \#C_B(\ell, t) \right)^{\frac{1}{2}} \frac{x^{\frac{1}{2}}}{\log x} \left[ Q(\mathfrak{A}[\ell])^{B_{2g}(\mathbb{F}_\ell)} : Q \right] \log M \left( Q(\mathfrak{A}[\ell])^{U_{2g}(\mathbb{F}_\ell)} / Q(\mathfrak{A}[\ell])^{B_{2g}(\mathbb{F}_\ell)} \right) \]

\[ + \log M(Q(A[\ell])/Q). \]

Using the Chebyshev bound \( \pi(x) \leq \frac{x}{\log x} \), the formulae for \# GSp_{2g}(\mathbb{F}_\ell), \# B_{2g}(\mathbb{F}_\ell), \# U_{2g}(\mathbb{F}_\ell) \) recorded in Proposition \textbf{3} and the estimate for \# C_B(\ell, t) \) given in Proposition \textbf{13} we deduce that, under GRH,

\[ (53) \]

\[ \pi_{C^{\ast \ast}(\ell, t)}(x, Q(A[\ell])/Q) \leq \frac{1}{\ell} \frac{x}{\log x} + \ell^{\frac{7}{2}} \frac{x^{\frac{1}{2}}}{\log x} \log M \left( Q(A[\ell])^{U_{2g}(\mathbb{F}_\ell)} / Q(A[\ell])^{B_{2g}(\mathbb{F}_\ell)} \right) \]

\[ + \log M(Q(A[\ell])/Q). \]

To estimate \( \log M(Q(A[\ell])/Q) \), we see that, by definition,

\[ (54) \]

\[ \log M(Q(A[\ell])/Q) = \log 2 + \log \left( Q(A[\ell])/Q \right) + \frac{1}{Q(A[\ell])/Q} \log \left| d_Q(A[\ell]) \right| + \sum_{p \mid d_Q(A[\ell])} \log p. \]
Using inequality (8), we deduce that

\[
\log \left| d_{Q(A[\ell])} \right| \leq \sum_{p \mid d_{Q(A[\ell])}} \log p + \log(Q(A[\ell]) : Q).
\]

Combining (14), (54) and (55) and using the first formula in Proposition 9, we derive that

\[
 \log M(Q(A[\ell]) / Q) \ll_{g} \log(\ell N_{A}).
\]

To estimate \( \log M \left( \frac{Q(A[\ell])^{U_{2g}(F_{\ell})}}{Q(A[\ell])^{B_{2g}(F_{\ell})}} \right) \), we proceed similarly and derive that

\[
 \log M \left( \frac{Q(A[\ell])^{U_{2g}(F_{\ell})}}{Q(A[\ell])^{B_{2g}(F_{\ell})}} \right) \ll_{g} \log(\ell N_{A}).
\]

Putting together (53), (56), and (57), we obtain the upper bound

\[
\pi_{C^{(\ell,t)}}(x, Q(A[\ell]) / Q) \ll_{g} \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell \theta^{2} + \frac{x^{\frac{1}{2}}}{\log x} \cdot \log(\ell N_{A}),
\]

which is valid for any sufficiently large prime \( \ell \). Then, recalling (52), we obtain that

\[
\pi_{A}(x, t) \leq c(A, \varepsilon) \max_{y \leq x \leq y + a} \left( \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell \theta^{2} + \frac{x^{\frac{1}{2}}}{\log x} \cdot \log \ell \right)
\]

for some positive constant \( c(A, \varepsilon) \) that depends on \( A \) and \( \varepsilon \).

Choosing

\[
y(x) := \frac{x^{\frac{1}{2} \theta^{2} + \frac{1}{2}}}{(\log x)^{\frac{1}{2} \theta^{2} + \frac{1}{2}}},
\]

recalling from (20) that \( u \leq y \), and fixing an arbitrary \( \varepsilon \), we deduce that

\[
\pi_{A}(x, t) \ll_{A} \frac{x^{1 - \frac{1}{2} \theta^{2} + \frac{1}{2}}}{(\log x)^{1 - \frac{1}{2} \theta^{2} + \frac{1}{2}}}
\]

This completes the proof of Theorem 1 for arbitrary \( t \).

### 6.4. Proof of Theorem 1 for \( t = 0 \)

Let \( A \) be an abelian variety defined over \( \mathbb{Q} \), of conductor \( N_{A} \), and of dimension \( g \). Let \( x > 2 \) be a real number that goes to infinity. Our goal in this subsection is to prove the upper bound for \( \pi_{A}(x, 0) = \# \{ p \leq x : p \mid N_{A}, A_{1,p}(A) = 0 \} \) claimed in Theorem 1 under the same two main assumptions (46) and (50) as in Subsection 6.3, that is, under the assumption that for any sufficiently large prime \( \ell \), the residual modulo \( \ell \) Galois representation \( \overline{\rho}_{A,\ell} \) has image isomorphic to \( GSp_{2g}(\mathbb{F}_{\ell}) \) and under the assumption of the validity of RH and of GRH for the Dedekind zeta functions of the number fields \( \mathbb{Q}(A[\ell])^{U_{2g}(F_{\ell})} \) for all sufficiently large primes \( \ell \), as well as of the number fields \( K_{A,p} \) for all primes \( p \mid N_{A} \).

Considering the subextensions of \( \mathbb{Q}(A[\ell]) \) fixed by the subgroups \( U'_{2g}(\mathbb{F}_{\ell}) \) and \( B_{2g}(\mathbb{F}_{\ell}) \) of \( GSp_{2g}(\mathbb{F}_{\ell}) \),

\[
\mathbb{Q} \subseteq \mathbb{Q}(A[\ell])^{B_{2g}(F_{\ell})} \subseteq \mathbb{Q}(A[\ell])^{U'_{2g}(F_{\ell})} \subseteq \mathbb{Q}(A[\ell]),
\]

and recalling that, by part (ii) of Proposition 8 \( U'_{2g}(\mathbb{F}_{\ell}) \) is a normal subgroup of \( B_{2g}(\mathbb{F}_{\ell}) \), in addition to (46) and (47), we obtain the following Galois group structures

\[
\text{Gal}(\mathbb{Q}(A[\ell]) / \mathbb{Q}(A[\ell])^{U'_{2g}(F_{\ell})}) \simeq U'_{2g}(\mathbb{F}_{\ell}),
\]

\[
\text{Gal}(\mathbb{Q}(A[\ell]) / \mathbb{Q}(A[\ell])^{B_{2g}(F_{\ell})}) \simeq B_{2g}(\mathbb{F}_{\ell}),
\]

\[
\text{Gal}(\mathbb{Q}(A[\ell]) / \mathbb{Q}(A[\ell])^{U_{2g}(F_{\ell})}) \simeq U_{2g}(\mathbb{F}_{\ell}),
\]

\[
\text{Gal}(\mathbb{Q}(A[\ell]) / \mathbb{Q}(A[\ell])) \simeq GSp_{2g}(\mathbb{F}_{\ell}).
\]

Thus, under these assumptions, we proceed similarly and derive that

\[
\pi_{A}(x, 0) \leq c(A, \varepsilon) \max_{y \leq x \leq y + a} \left( \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell \theta^{2} + \frac{x^{\frac{1}{2}}}{\log x} \cdot \log \ell \right)
\]

for some positive constant \( c(A, \varepsilon) \) that depends on \( A \) and \( \varepsilon \).

Choosing

\[
y(x) := \frac{x^{\frac{1}{2} \theta^{2} + \frac{1}{2}}}{(\log x)^{\frac{1}{2} \theta^{2} + \frac{1}{2}}},
\]

recalling from (20) that \( u \leq y \), and fixing an arbitrary \( \varepsilon \), we deduce that

\[
\pi_{A}(x, 0) \ll_{A} \frac{x^{1 - \frac{1}{2} \theta^{2} + \frac{1}{2}}}{(\log x)^{1 - \frac{1}{2} \theta^{2} + \frac{1}{2}}}
\]

This completes the proof of Theorem 1 for arbitrary \( t = 0 \).
where, by Proposition 11, the quotient $B_{2g}(\mathbb{F}_t)/U_{2g}(\mathbb{F}_t)$ is abelian.

Proceeding identically to the proof given in Subsection 6.3, we obtain that (61) leads to the inequality

\[
\pi_A(x,0) \leq c(A,\varepsilon) \max_{y \leq \ell \leq y^2} \pi_{C^{\varepsilon}G}(x, Q(A[\ell])/Q),
\]

where $\varepsilon > 0$ is arbitrary and where $y = y(x) > 2$ and $u = u(x) > 2$ are arbitrary real numbers that depend on and grow with $x$ and that satisfy (29), (30), and (31). Then we estimate $\pi_{C^{\varepsilon}G}(x, Q(A[\ell])/Q)$ by invoking Theorem 6 with $K = Q$, $L = Q(A[\ell])$, $H = B_{2g}(\mathbb{F}_t)$, $N = U_{2g}(\mathbb{F}_t)$, $C_1 = C^{\varepsilon}G(x,0)$, and $C_2 = C(\ell,0)$. Similarly to the case considered in Subsection 6.3, the hypotheses of Theorem 6 hold thanks to parts (iii) and (iv) of Proposition 12 to Proposition 11 and to our GRH assumption. We obtain that

\[
\pi_{C^{\varepsilon}G}(x, Q(A[\ell])/Q) \ll \frac{\#C^{\varepsilon}G(\ell,0) \cdot \#U_{2g}(\mathbb{F}_t)}{\#B_{2g}(\mathbb{F}_t)} \cdot \pi(x)
\]

\[
+ \left( \frac{\#C^{\varepsilon}G(\ell,0)}{\#B_{2g}(\mathbb{F}_t)} \right)^{1/2} \frac{x^{1/2}}{\log x} + \left[ Q(A[\ell])/B_{2g}(\mathbb{F}_t) : Q \right] \log M \left( Q(A[\ell])/U_{2g}(\mathbb{F}_t) : Q(A[\ell])/B_{2g}(\mathbb{F}_t) \right)
\]

\[
+ \log M(Q(A[\ell])/Q).
\]

Using the Chebyshev bound $\pi(x) \ll \frac{x}{\log x}$, the formulae for $\# GSp_{2g}(\mathbb{F}_t)$, $\#B_{2g}(\mathbb{F}_t)$, $\#U_{2g}(\mathbb{F}_t)$ recorded in Proposition 9 and the estimate for $\#C^{\varepsilon}G(\ell,0)$ given in Proposition 13 we deduce that

\[
\pi_{C^{\varepsilon}G}(x, Q(A[\ell])/Q) \ll \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell g^2 + \frac{x^{1/2}}{\log x} \cdot \log M \left( Q(A[\ell])/U_{2g}(\mathbb{F}_t) : Q(A[\ell])/B_{2g}(\mathbb{F}_t) \right)
\]

\[
+ \log M(Q(A[\ell])/Q).
\]

Using (59) and the estimate $\log M \left( Q(A[\ell])/U_{2g}(\mathbb{F}_t) : Q(A[\ell])/B_{2g}(\mathbb{F}_t) \right) \ll g \log(N\ell)$, obtained mutatis mutandis, we infer that

\[
\pi_{C^{\varepsilon}G}(x, Q(A[\ell])/Q) \ll_g \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell g^2 + \frac{x^{1/2}}{\log x} \cdot \log(N\ell).
\]

Recalling (62), we obtain that

\[
\pi_A(x,0) \leq c(A,\varepsilon) \max_{y \leq \ell \leq y^2} \left( \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell g^2 + \frac{x^{1/2}}{\log x} \cdot \log \ell \right)
\]

for some positive constant $c(A,\varepsilon)$ that depends on $A$ and $\varepsilon$. Choosing

\[
y(x) := \frac{x^{1/2} + g^2}{(\log x)^{1/2} + g^2},
\]

recalling from (29) that $u \leq y$, and fixing an arbitrary $\varepsilon$, we deduce that

\[
\pi_A(x, t) \ll_A \frac{x^{1/2} + g^{2}}{(\log x)^{1/2} + g^{2}}.
\]

This completes the proof of Theorem 1 for $t = 0$. 
6.5. Proof of Theorem 2 for arbitrary $t \in \mathbb{Z}$. Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. Let $x > 2$ be a real number that goes to infinity. Our goal in this subsection is to prove the upper bound for $\pi_A(x, t) = \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = t \}$ claimed in Theorem 2 under assumptions (40) and (50), as in Section 6.3, together with the assumptions that AHC and PCC hold for the extension $\mathbb{Q}(A[\ell])/\mathbb{Q}$, where $\ell$ is a sufficiently large arbitrary prime.

As in Section 6.3, we recall that, by part (ii) of Proposition 16 any prime $p \nmid N_A$ for which $a_{1,p}(A) = t$ has the property that, for any prime ideal $p$ of $\mathbb{Q}(A[\ell])$ that lies over $p$, $\text{tr}_{A,\ell} \left( \left( \frac{\mathbb{Q}(A[\ell])}{p} \right) \right) = -t(\text{mod } \ell)$.

Thus, every prime $p$ counted in $\pi_A(x, t)$ satisfies that, for any prime ideal $p$ of $\mathbb{Q}(A[\ell])$ that lies over $p$,

$$\text{tr}_{A,\ell} \left( \left( \frac{\mathbb{Q}(A[\ell])}{p} \right) \right) \in C_0(\ell, t).$$

As such, we have the inequality

$$\pi_A(x, t) \leq \pi_{C_0(\ell, t)}(x, \mathbb{Q}(A[\ell])/\mathbb{Q}).$$

By invoking Theorem 7 with $K = \mathbb{Q}$, $L = \mathbb{Q}(A[\ell])$, $H = \text{GSp}_{2g}(\mathbb{F}_\ell)$, $N = \{I_{2g}\}$, and $C = C_0(\ell, t)$, we obtain that, under GRH, AHC, and PCC,

$$\pi_{C_0(\ell, t)}(x, \mathbb{Q}(A[\ell])/\mathbb{Q}) \ll \frac{\# C_0(\ell, t)}{\# \text{GSp}_{2g}(\mathbb{F}_\ell)} \pi(x) + \frac{\# C_0(\ell, t)}{\# \text{GSp}_{2g}(\mathbb{F}_\ell)} x^{\frac{1}{2}} \log(M(\mathbb{Q}(A[\ell])/\mathbb{Q})x) + \frac{x^{\frac{1}{2}}}{\log x} + \log(M(\mathbb{Q}(A[\ell])/\mathbb{Q}).$$

Then, by applying the upper bounds for $\# \text{GSp}_{2g}(\mathbb{F}_\ell)$ from Proposition 9 for $\# C_0(\ell, t)$ from Proposition 13 for $\# \text{GSp}_{2g}(\mathbb{F}_\ell)$ from Proposition 10 as well as estimate (50), we deduce that

$$\pi_{C_0(\ell, t)}(x, \mathbb{Q}(A[\ell])/\mathbb{Q}) \ll_g \frac{1}{\ell} \frac{x}{\log x} + \ell^{\frac{1}{2}} \cdot x^{\frac{1}{4}} \cdot \log(\ell N_A x).$$

Finally, by choosing

$$y(x) := \frac{x^{\frac{1}{12}}}{(\log x)^{\frac{1}{6}}} ,$$

we derive that

$$\pi_A(x, t) \ll_A \frac{x^{1 - \frac{1}{12}}}{(\log x)^{\frac{1}{6}}}. $$

This completes the proof of Theorem 2 for arbitrary $t$.

6.6. Proof of Theorem 2 for $t = 0$. Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. Let $x > 2$ be a real number that goes to infinity. Our goal in this subsection is to prove the upper bound for $\pi_A(x, 0) = \# \{ p \leq x : p \nmid N_A, a_{1,p}(A) = 0 \}$ claimed in Theorem 2 under assumptions (40) and (50), together with the assumptions that AHC and PCC hold for the extension $\mathbb{Q}(A[\ell])/\mathbb{Q}$, where $\ell$ is a sufficiently large arbitrary prime.
As in the proof of Theorem 2 for arbitrary $t$, our starting point is inequality (66) for $t = 0$, that is,

$$\pi_A(x, 0) \leq \pi_{C_0(t, 0)}(x, Q(A|\ell))/Q).$$

We estimate the right hand side by invoking Theorem 7 with $K = \mathbb{Q}$, $L = Q(A|\ell)$, $H = GSp_{2g}(F_\ell)$, $N = \Lambda(F_\ell)$, and $C = C_0(\ell, 0)$. We obtain that, under GRH, AHC, and PCC,

$$\pi_{C_0(t, 0)}(x, Q(A|\ell))/Q) \ll \frac{\#C_0(\ell, 0)}{\#PGSp_{2g}(F_\ell)}\pi(x)$$

$$+ \#C_0(\ell, 0) \cdot \left( \frac{\#PGSp_{2g}(F_\ell)^\#}{\#PGSp_{2g}(F_\ell)} \right)^\frac{1}{2} \cdot x^{\frac{1}{2}} \cdot \log \left( M(Q(A|\ell)\Lambda(F_\ell)/Q) \right) x$$

$$+ \frac{1}{\log x} + \log M(Q(A|\ell)\Lambda(F_\ell)/Q).$$

Then, by applying the upper bounds for $\#PGSp_{2g}(F_\ell)$ from Proposition 9 for $\#C_0(\ell, 0)$ from Proposition 13 and for $\#PGSp_{2g}(F_\ell)^\#$ from Proposition 10 and by observing that

$$\log M(Q(A|\ell)\Lambda(F_\ell)/Q) \leq \log M(Q(A|\ell)/Q),$$

we deduce that

$$\pi_{C_0(t, 0)}(x, Q(A|\ell))/Q) \ll_{\varphi} \frac{1}{\ell} \cdot \frac{x}{\log x} + \ell^{\frac{1}{2} + 1} \cdot x^{\frac{1}{2}} \cdot \log(\ell N_A x).$$

Finally, by choosing

$$y(x) := \frac{x^{1/\varphi}}{(\log x)^{1/\varphi}},$$

we derive that

$$\pi_A(x, 0) \ll_{\varphi} A \frac{x^{1-\frac{1}{\varphi}}}{(\log x)^{1-\frac{1}{\varphi}}}.$$

This completes the proof of Theorem 2 for $t = 0$.

### 6.7. Proof of part (i) of Theorem 3

Once again, let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N_A$, and of dimension $g$. We keep the two main assumptions (46) and (50), as in Subsections 6.3 and 6.4. Our goal in this subsection is to prove that, for any $\varepsilon > 0$, the lower bound $|a_{1,p}(A)| \geq p^{2\varphi+\varphi+1} - \varepsilon$ holds for a set of primes $p$ of density 1. The proof proceeds similarly to that of [CoWa22, Theorem 3], as follows.

Let $x > 2$ be a real number that goes to infinity. Let $z = z(x) > 0$, $y = y(x) > 2$, and $u = u(x) > 2$ be real numbers that depend on and grow with $x$ and satisfy (29), (30), and (31). By (33) of Proposition 19 we know that, for any $\varepsilon > 0$, there exists $c(\varepsilon) > 0$ such that

$$\sum_{\ell \leq x} \pi_A(x, t) \leq c(\varepsilon) \max_{y \leq \ell \leq x + u} \sum_{\ell \leq y} \# p \leq \ell N_A, a_{1,\ell}(A) = t,$$

$$\ell \nmid d_{\mathbb{Q}(\pi_p(A))} \#(O_{\mathbb{Q}(\pi_p(A))}/\mathbb{Z}[\pi_p(A)], \ell \text{ splits completely in } \mathbb{Q}(\pi_p(A))).$$
Proceeding similarly to the proofs of (52) and (58), we obtain that

\[
\sum_{t \in \mathbb{Z}} |t| \leq z \pi(A(x, t)) \leq c(\varepsilon) \max_{y \leq \ell \leq y + u} \left( \frac{xz}{\log x} + \ell \sqrt{\frac{y}{\log x}} \cdot \log \ell \right)
\]

for some positive constant \(c(A, \varepsilon)\) that depends on \(A\) and \(\varepsilon\). Choosing

\[
y(x) := z(x)(\log x)\eta
\]

and

\[
z(x) := \frac{x^{\frac{1}{2g+2}}}{(\log x)^{\eta+\varepsilon}}
\]

for some fixed arbitrary \(\eta > 0\) and \(\varepsilon > 0\), we derive that

\[
\sum_{t \in \mathbb{Z}} \pi_A(x, t) \leq c(A, \varepsilon, \eta) \frac{x}{(\log x)^{\eta+1}} = o(\pi(x)).
\]

Using this estimate, we deduce that

\[
\pi(x) = \# \left\{ p \leq x : p \nmid N_A, |a_{1,p}(A)| > \frac{p^{2g+2+\varepsilon}}{(\log p)^{\eta+\varepsilon}} \right\}
\]

\[
+ \# \left\{ p \leq x : p \nmid N_A, |a_{1,p}(A)| \leq \frac{p^{\frac{1}{2g+2}}}{(\log p)^{\eta+\varepsilon}} \right\} + \# \{ p \leq x : p \mid N_A \}
\]

\[
= \# \left\{ p \leq x : p \nmid N_A, |a_{1,p}(A)| > \frac{p^{\frac{1}{2g+2}}}{(\log p)^{\eta+\varepsilon}} \right\} + o(\pi(x)).
\]

This completes the proof of part (i) of Theorem 3.

6.8. Proof of part (ii) of Theorem 3. Yet again, let \(A\) be an abelian variety defined over \(\mathbb{Q}\), of conductor \(N_A\), and of dimension \(g\). We keep the four main assumptions (46), (50), AHC, and PCC, as in Subsections 6.5 and 6.6. Our goal in this subsection is to prove that, for any \(\varepsilon > 0\), the lower bound

\[
|a_{1,p}(A)| \geq p^{\frac{1}{2g+2} - \varepsilon}
\]

holds for a set of primes \(p\) of density 1. The proof proceeds similarly to that of part (i), as follows.
Let $x > 2$ be a real number that goes to infinity and let $\varepsilon > 0$. Using Theorem 2, we deduce that

$$
\pi(x) = \# \left\{ p \leq x : p \nmid N_A, |a_1, p(A)| > p^{\frac{1}{g} + \varepsilon} \right\} \\
+ \# \left\{ p \leq x : p \nmid N_A, |a_1, p(A)| \leq p^{\frac{1}{g} - \varepsilon} \right\} + \# \{ p \leq x : p \mid N_A \}
\leq \# \left\{ p \leq x : p \nmid N_A, |a_1, p(A)| > p^{\frac{1}{g} + \varepsilon} \right\} \\
+ \sum_{t \in \mathbb{Z}} \left\{ p \leq x : p \nmid N_A, |a_1, p(A)| = t \right\} + o(\pi(x))
= \# \left\{ p \leq x : p \nmid N_A, |a_1, p(A)| > p^{\frac{1}{g} + \varepsilon} \right\} + O_{A, \varepsilon} \left( x^{\frac{1}{g} + \varepsilon} \cdot \frac{x^{1 - \frac{1}{2g}}}{\log x} \right)
= \# \left\{ p \leq x : p \nmid N_A, |a_1, p(A)| > p^{\frac{1}{g} + \varepsilon} \right\} + o(\pi(x)).
$$

This completes the proof of part (ii) of Theorem 3.

7. Final remarks

We conclude with brief remarks about the current conditional approaches towards obtaining upper bounds for $\pi_A(x, t)$ for a given generic abelian variety $A$ defined over $\mathbb{Q}$ and of dimension $g$, where by generic we mean that $\text{Im} \rho_A$ is open in $\text{GSp}_{2g}(\hat{\mathbb{Z}})$.

The main goal of the present paper is to prove the currently best upper bound for $\pi_A(x, t)$ under GRH. Theorem 1 does provide such bounds, substantially improving upon [CoDaSiSt17, Theorem 1, pp. 3560-3561] for any value of $g$ and any value of $t$. The secondary goal of the paper is to prove the currently best upper bound for $\pi_A(x, t)$ under other sensible unproven hypotheses. Theorem 2 does provide such bounds, substantially improving upon [Be16, Corollaire 17, p. 51]. However, while in the first comparison, both results assume some version of GRH, in the second comparison, the two results assume different hypotheses. Indeed, Theorem 2 assumes GRH, AHC, and PCC, in contrast with [Be16, Corollaire 17, p. 51], which assumes GRH and AHC. It is plausible that the methods of these two results may be combined to produce an improvement to the upper bounds for $\pi_A(x, t)$ under GRH, AHC, and PCC. We relegate such work to a future project.

In the case $g = 1$, a different conditional approach for proving upper bounds for $\pi_A(x, t)$ was initiated in [Mu85]. Therein, Murty assumed an effective version of the Sato-Tate Conjecture for $A$ and used it to deduce the upper bound $\pi_A(x, t) \ll_{A, t} x^{1 - \frac{1}{2}} (\log x)^{1/2}$. He also proved that the effective version of the Sato-Tate Conjecture for $A$ invoked in the above bound follows from the assumptions that each of the symmetric power $L$-functions of $A$ has an analytic continuation to $\mathbb{C}$, satisfies an appropriate functional equation, and satisfies an analogue of the Riemann Hypothesis. Thanks to recent work of Newton and Thorner [NeTh21], the assumption about the analytic continuation is now known to hold. Murty’s approach was exploited further by Rouse and Thorner [RoTh16], who proved, under similar hypotheses as those of Murty’s, together with the
additional assumption that the conductor $N_A$ of the elliptic curve $A$ is squarefree, that $\pi_A(x, t) \ll_{A,t} \frac{x^{1-rac{1}{2g}}}{(\log x)^{\frac{c}{2g^2+2g}}}$, a bound which improves on that of $[\text{Mu}85]$, but not on that of $[\text{MuMuWo}18]$. In the case $g \geq 2$, Bucur, Fité and Kedlaya $[\text{BuFiKe}20]$ proved an analogue of Murty’s result concerning the validity of an effective version of the Sato-Tate Conjecture for $A$, under assumptions similar to the ones of $[\text{Mu}85]$, together with the additional assumption that the Mumford-Tate Conjecture holds for the abelian variety $A$. Following the strategy of $[\text{Mu}85]$, the result of $[\text{BuFiKe}20]$ seems to give $\pi_A(x, t) \ll_{A,t} x^{1-rac{1}{2g^2+2g}}(\log x)^c$ for some (possibly non-negative) constant $c$, a bound which does not improve upon Theorem 1. We plan to explore this approach in depth in future work.

Finally, let us note that similar methods may be used to obtain upper bounds for $\pi_A(x, t)$ for other types of abelian varieties $A$. For example, in the case of an abelian variety isogenous to the product $E_1 \times \ldots \times E_g$ of elliptic curves $E_1, \ldots, E_g$ defined over $\mathbb{Q}$, pairwise non-isogenous over $\overline{\mathbb{Q}}$, and each with a trivial $\overline{\mathbb{Q}}$-endomorphism ring, the refined mod $\ell$ method of $[\text{MuMuSa}88]$, under GRH, was used in $[\text{CoWa}22]$, while the direct mod $\ell$ method of $[\text{MuMuWo}18]$, under GRH, AHC, and PCC, as well as the Sato-Tate method of $[\text{Mu}85]$, under assumptions similar to the case $g = 1$, will be used in an upcoming paper of the authors.

References

[AkPa19] A. Akbari and J. Park, On the Lang-Trotter for two elliptic curves, Ramanujan Journal 49, 2019, pp. 585–623.

[A109] P. Aluffi, Algebra: Chapter 0, Graduate Studies in Mathematics Vol. 104, American Mathematical Society, 2009.

[Ar27] E. Artin, Beweis des allgemeinen Reziprozitätsgesetzes, Hamb. Abh. 5, 1927, pp. 353–363.

[BaGo97] P. Bayer and J. González, On the Hasse-Witt invariants of modular curves, Experimental Mathematics 6, 1997, No. 1, pp. 57–76.

[Be16] J. Bellaïche, Théorème de Chebotarev et complexité de Littlewood, Ann. Sci. Éc. Norm. Supé. (4) 49, No. 3, 2016, pp. 579–632.

[BoCaGePi21] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, Abelian surfaces over totally real fields are potentially modular, Publ. Math. de l’IHES 134, 2021, pp. 153–501.

[BuFiKe20] A. Bucur, F. Fité, and K. Kedlaya, Effective Sato-Tate conjecture for abelian varieties and applications. preprint available at https://arxiv.org/abs/2002.08807

[Ch97] N. Chavdarov, The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy, Duke Mathematical Journal 87, No. 1, 1997, pp. 151–180.

[ChJoSe20] H. Chen, N. Jones, and V. Serban, The Lang-Trotter conjecture for products of non-CM elliptic curves, to appear in Ramanujan Journal, preprint available at https://arxiv.org/abs/2006.11269

[CoDaSiSt17] A.C. Cojocaru, R. Davis, A. Silverberg, and K.E. Stange, Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre), International Mathematics Research Notices 12, 2017, pp. 3557–3602.

[CoWa22] A.C. Cojocaru and T. Wang, Bounds for the distribution of the Frobenius traces associated to products of non-CM elliptic curves, Canadian Journal of Mathematics 2022, pp. 1–26, available at http://dx.doi.org/10.4153/S0008414X22000086
[CoSi86] G. Cornell and J.H. Silverman (editors), *Arithmetic Geometry*, Springer-Verlag New York, 1986.

[El91] N. Elkies, *Distribution of supersingular primes*, Astérisque No. 198-200, 1991, pp. 127–132.

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

[FoMu96] E. Fouvry, M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. 48, No. 1, 1996, pp. 81–104.

[FuGu12] J. Fulman and R. Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. 364, No. 6, 2012, pp. 3023–3070.

[Ga70] P.X. Gallagher, *The number of conjugacy classes in a finite group*, Math. Z. 118, 1970, pp. 175–179.

[Ha11] C. Hall, *An open image theorem for a general class of abelian varieties*, Bulletin of the London Mathematical Society 43, No. 4, 2011, pp. 703–711.

[He02] K. Hensel, *Über die Entwicklung der algebraischen Zahlen in Potenzreihen*, Mathematische Annalen 55, 1902, pp. 301–336.

[Ho68] T. Honda, *Isogeny classes of abelian varieties over finite fields*, Journal of the Mathematical Society of Japan 20, 1968, pp. 83–95.

[Hu75] J.E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics 21, Springer-Verlag, New York - Heidelberg, 1975.

[Ka09] N.M. Katz, *Lang-Trotter revisited*, Bulletin of the American Mathematical Society 46, No. 3, 2009, pp. 413–457.

[KaSa99] N.M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications 45, Providence, RI, 1999.

[KuKuWe22] A. Kumar, M. Kumari, and A. Weiss, *On the Lang-Trotter conjecture for Siegel modular forms*, preprint available at https://arxiv.org/abs/2201.09278

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

[La83] S. Lang, *Abelian varieties*, Springer - Verlag, New York - Berlin, 1983.

[La94] S. Lang, *Algebraic number theory*, 2nd edition, Graduate Texts in Mathematics 110, Springer - Verlag, New York - Berlin - Heidelberg, 1994.

[LaTr76] S. Lang and H. Trotter, *Frobenius distributions in GL₂-extensions*, Lecture Notes in Mathematics 504, Springer Verlag, Berlin - New York, 1976.

[Mi86] J.S. Milne, *Abelian varieties*, in *Arithmetic geometry*, by G. Cornell and J.H. Silverman (editors), Springer-Verlag New York, 1986, pp. 103–150.

[Mu70] D. Mumford, *Abelian varieties*, Oxford University Press, 1970.

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

[MuMu84] M.R. Murty and V.K. Murty, *Prime divisors of Fourier coefficients of modular forms*, Duke Mathematical Journal 51, No. 1, 1984, pp. 57–76.

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

[MuMuWo18] M.R. Murty, V.K. Murty, and P-J. Wong, *The Chebotarev density theorem and the pair correlation conjecture*, J. Ramanujan Math. Soc. 33, No. 4, 2018, pp. 399–426.
V.K. Murty, *Modular forms and the Chebotarev density theorem II*, Analytic number theory (Kyoto, 1996), London Math. Soc. Lecture Notes Series 247, Cambridge University Press, 1997, pp. 287–308.

V.K. Murty, *Frobenius distributions and Galois representations*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math. 66, Part 1, American Mathematical Society, Providence, 1999, pp. 193–211.

J. Newton and J. Thorne, *Symmetric power functoriality for holomorphic modular forms, II*, Publ. Math. Inst. Hautes Études Sci. 134, 2021, pp. 117–152.

J. Newton and J. Thorne, *The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions*, Trans. Amer. Math. Soc. 369, No 5, 2017, pp. 3575–3604.

F. Oort, *Abelian varieties over finite fields. Higher-dimensional geometry over finite fields*, NATO Peace Secur. Ser. D Inf. Commun. Secur., 16, IOS, Amsterdam, 2008, pp. 123–188.

J. Rouse and J. Thorner, *The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions*, Trans. Amer. Math. Soc. 369, No 5, 2017, pp. 3575–3604.

J-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, New York - Amsterdam, 1968.

J-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Inventiones Math. 15, No. 4, 1972, pp. 259–331.

J-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L’Ens. Math. 22, 1976, pp. 227–260.

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

J-P. Serre, *Résumé des cours de 1985-1986*, in Oeuvres. Collected Papers, Vol. IV, 1985-1998, 2nd edition, Springer Verlag, Heidelberg, 2003, pp. 33–37.

J-P. Serre, *Lettre à Marie-France Vignéras du 10/2/1986*, in Oeuvres. Collected Papers, Vol. IV, 1985-1998, 2nd edition, Springer Verlag, Heidelberg, 2003, pp. 38–55.

J-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques*, in Motives (Seattle, WA, 1991), Proceedings Symposium Pure Mathematics 55, part I, Providence, RI, American Mathematical Society, 1994, pp. 377–400.

J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics 88, 1968, pp. 492–517; Oeuvres/Collected Papers OO, Springer Verlag, Berlin, 1985, pp. 472–497.

J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2, 1966, pp. 134–144.

G.E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. 3, 1963, pp. 1–62.

W.C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sc. Ec. Norm. Sup. 2, 1969, pp. 521–560.

Y.G. Zarhin, *Hyperelliptic Jacobians without complex multiplication*, Mathematical Research Letters 7, No.1, 2000, pp. 123–132.

Y.G. Zarhin, *G. Endomorphism rings of reductions of elliptic curves and Abelian varieties*, St. Petersburg Math. J. 29, No. 1, 2018, pp. 81–106.

D. Zywina, *Bounds for the Lang-Trotter Conjectures*, in SCHOLAR – a scientific celebration highlighting open lines of arithmetic research, Contemporary Mathematics 655, American Mathematical Society, Providence, 2015, pp. 235–256.
Email address, Alina Carmen Cojocaru: cojocaru@uic.edu

(Tian Wang)

Email address, Tian Wang: twang213@uic.edu