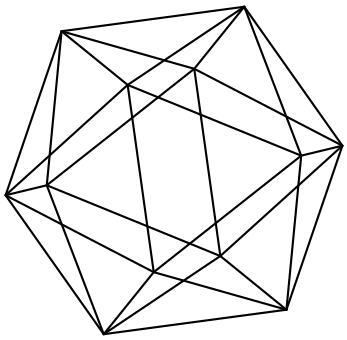
Max-Planck-Institut für Mathematik
Bonn

Distribution of supersingular primes for abelian surfaces

by

Tian Wang



Max-Planck-Institut für Mathematik
Preprint Series 2024 (11)

Date of submission: April 23, 2024

Distribution of supersingular primes for abelian surfaces

by

Tian Wang

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

MPIM 24-11

DISTRIBUTION OF SUPERSINGULAR PRIMES FOR ABELIAN SURFACES

TIAN WANG

Abstract. Let A/K be an absolutely simple abelian surface defined over a number field K. We give unconditional upper bounds for the number of prime ideals $\mathfrak{p}$ of K with norm up to x such that A has supersingular reduction at $\mathfrak{p}$ when A has a trivial endomorphism ring, real multiplication, and quaternion multiplication, respectively. Particularly, in the real multiplication case and when $K = \mathbb{Q}$, the bound is related to an upper bound for the distribution of Frobenius traces of A. Also in the real multiplication case, we provide unconditional upper bounds for a variant of the problem, which concerns the number of prime ideals for which the reduction of A at the prime has a particular Newton datum and is not simple.

1. Introduction

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. For a prime p that does not divide the conductor N_E of E, we denote by $\overline{E}_p$ the reduction of E at p. We say the elliptic curve $\overline{E}_p$ is *supersingular* if the $\overline{\mathbb{F}}_p$-points of the p-torsion group $\overline{E}_p[p]$ is trivial and such a prime p is called a *supersingular prime* of E. A famous open problem related to the distribution of supersingular primes for elliptic curves is the Lang-Trotter Conjecture. The conjecture predicts that for all sufficiently large x,

$$\pi_{E,ss}(x) := \#\{p \leq x : p \nmid N_E, \overline{E}_p \text{ is supersingular}\} \sim C_E \frac{x^{\frac{1}{2}}}{\log x} \tag{1}$$

for some constant $C_E \neq 0$ (see [LT76, p. 36]) that depends only on E.

The first nontrivial observation related to this conjecture is due to Serre [Ser98, I-25], where he showed the density of supersingular primes of E is 0. Later in [Ser81, Théorème 12, p. 357], he obtained the unconditional upper bound $\pi_{E,ss}(x) \ll x(\log x)^{-\frac{3}{2}+\epsilon}$ for any $\epsilon > 0$, using the effective Chebotarev Density Theorem [LMO79] and properties of ℓ-adic Lie groups. Incorporating a sieve theoretical lemma, the upper bound was improved by Wan [Wan90] to $\pi_{E,ss}(x) \ll x(\log x)^{-2+\epsilon}$ for any $\epsilon > 0$. In 1986, Elkies [Elk87] made a significant progress in this direction by showing that there are infinitely many supersingular primes for elliptic curves over $\mathbb{Q}$. Based on this work, Murty and Elkies [Elk91] also proved the unconditional upper bound $\pi_{E,ss}(x) \ll x^{\frac{3}{4}}$. It is worth mentioning that this bound matches with Serre's result under the Generalized Riemann Hypothesis (GRH) for Dedekind zeta functions [Ser81, p. 323].

In contrast, if $E/\mathbb{Q}$ is an elliptic curve with complex multiplication, then by Deuring's criterion [Deu41], we readily know that $\pi_{E,ss}(x) \sim x(2\log x)^{-1}$.

In this paper, our focus lies in investigating the distribution of supersingular primes for absolutely simple abelian surfaces. To establish the main results, we introduce the some necessary notation. Consider an absolutely simple abelian surface A defined over a number field K, and for a prime $\mathfrak{p}$ that does not divide the conductor N_A of A, we denote by $\overline{A}_\mathfrak{p}$ the reduction of A at $\mathfrak{p}$. Then, $\overline{A}_\mathfrak{p}$ is an abelian variety defined over the finite residue field $\mathbb{F}_\mathfrak{p}$. We say an abelian variety B over a finite field $\mathbb{F}_q$ is *supersingular* if B is isogenous over $\overline{\mathbb{F}}_q$ to a product of supersingular elliptic curves. For the abelian variety $\overline{A}_\mathfrak{p}/\mathbb{F}_\mathfrak{p}$, we say the prime $\mathfrak{p}$ is a *supersingular prime* of A if $\overline{A}_\mathfrak{p}$ is supersingular.

While it is known that for an abelian surface A/K, the density of supersingular primes is zero upon extending the base field (see, e.g., [BG97, Proposition 5.1, p. 61] or [DMOS82, Corollary 2.9,

2010 *Mathematics Subject Classification.* Primary 11G10, 11N45; Secondary 11G18, 11N13, 11N36.

p. 372]), much less is known about the upper bounds of the counting function

$$\pi_{A,ss}(x) := \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ is supersingular}\}. \tag{2}$$

Assume $K = \mathbb{Q}$. Motivated by the Lang-Trotter philosophy for elliptic curves, Bayer and González [BG97, Conjecture 8.2, p. 69 or p. 58] predicted the asymptotic behavior of $\pi_{A,ss}(x)$ for GL_2-type abelian surfaces over $\mathbb{Q}$. Specifically, let $f = \sum_{n\geq 1} a_n q^n$ be a weight 2 non-CM Hecke newform of level N and Nebetypus character ϵ, where $q = \exp(2\pi i z)$; let $K_f = \mathbb{Q}\left(\{a_n\}_{(n,N)=1}\right)$ and $F_f = \mathbb{Q}\left(\{a_n^2/\epsilon(n))\}_{(n,N)=1}\right)$; let A_f be Shimura's construction of the abelian variety associated to f. We assume A_f is absolutely simple. If

$$[K_f : \mathbb{Q}] = 2 \text{ and } [F_f : \mathbb{Q}] = 1, \tag{3}$$

then it is expected that $\pi_{A_f,ss}(x) \sim C_{A_f} x^{\frac{1}{2}}/\log x$, and if

$$[K_f : \mathbb{Q}] = [F_f : \mathbb{Q}] = 2, \tag{4}$$

then it is expected that $\pi_{A_f,ss}(x) \sim C'_{A_f} \log\log x$, where C_{A_f} and C'_{A_f} are constants that depends only on A_f [1]. In general, it seems that we do not have heuristics for the asymptotic behavior of $\pi_{A,ss}(x)$ for any abelian surfaces A/K. Nonetheless, by a conjecture of Cojocaru, Davis, Silverberg, and Stange [CDSS17], we expect there is a constant $C(A)$ that only depends on A such that $\pi_{A,ss}(x) \ll C(A) x^{\frac{1}{2}} (\log x)^{-1}$ holds [2] for a family of abelian surfaces that satisfy the equidistribution assumption and that the image of the adelic Galois representation of A is open in $\mathrm{GSp}_4(\widehat{\mathbb{Z}})$ (see [CDSS17, p. 3562]). Under GRH and certain assumptions on the image of the residue modulo ℓ Galois representations of A [CW22, Theorem 1], we have $\pi_{A,ss}(x) \ll x^{\frac{10}{11}} (\log x)^{-\frac{9}{11}}$; assuming both GRH and Artin's Holomorphy Conjecture (AHC) [Bel16, Theorem 20, p. 629], we have $\pi_{A,ss}(x) \ll x^{\frac{9}{10}} (\log x)^{-\frac{3}{5}}$; assuming GRH, AHC, and a Pair Correlation Conjecture (PCC) [CW22, Theorme 2], we have $\pi_{A,ss}(x) \ll x^{\frac{2}{3}} (\log x)^{\frac{1}{3}}$. In particular, these results show that the density of supersingular primes for these abelian surfaces is 0 without extending the base field.

We will give upper bounds of (2) for various abelian surfaces A/K, classified by their endomorphism algebras. We expect the growth of $\pi_{A,ss}(x)$ behave differently for abelian surfaces with distinct endomorphism rings, as we have seen in the elliptic curve case. First, we recall that by Albert's classification of division algebras with positive involutions, the endomorphism algebra $D := \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of A must be one of

(1) $\mathbb{Q}$;
(2) a real quadratic field, in which case we say A has *real multiplication (by D)*;
(3) an indefinite quaternion algebra over $\mathbb{Q}$, in which case we say A has *quaternion multiplication (by D)*;
(4) a CM quartic field, in which case we say A has *complex multiplication (by D)*.

Theorem 1. *Let A/K be an absolutely simple abelian surface. For all sufficiently large x, we have*

(1) if $D = \mathbb{Q}$, then

$$\pi_{A,ss}(x) \ll \frac{x(\log\log x)^{\frac{3}{2}}}{(\log x)^{\frac{3}{2}}};$$

(2) if $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ and A has real multiplication, then

$$\pi_{A,ss}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2};$$

[1] We also need to use Lemma 4 (3) to relate the p-rank of $\overline{A}_p$ and the supersingularity of $\overline{A}_p$.

[2] To show the upper bound holds, we also need to use Lemma 4, which says the reduction $\overline{A}_p$ is supersingular implies $a_p(A) = 0$ for $p \geq 17$.

(3) if $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ *and* A *has quaternion multiplication, then*

$$\pi_{A,ss}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

where the implicit constant in each $\ll$ *depends only on* A *and* K*.*

Remark 1. In case (1), if we use the unconditional bound in [CDSS17, Theorem 1], we obtain that for any $\epsilon > 0$, $\pi_{A,ss}(x) \ll \frac{x}{(\log x)^{\frac{9}{8}-\epsilon}}$.

If we are in case (2) and $K = \mathbb{Q}$, then A is a modular abelian surface constructed by Eichler-Shimura theory. In this case, this upper bound also serves as an upper bound for the Lang-Trotter type question for the distribution of the Frobenius traces of A. If A has complex multiplication, supersingular primes can be characterized using Shimura-Taniyama theory. These are discussed briefly in Section 7.1 and 7.2.

We also note that case (3) of Theorem 1 can not happen if $K = \mathbb{Q}$ [DR05, p. 618, Proposition 1.3].

In particular, these results already show (unconditionally) that the density of the supersingular primes for an absolutely simple abelian surface under one of the assumptions in Theorem 1 is 0.

We now sketch the proof for Theorem 1. First, we write the counting function (2) as the summation of

$$\#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_\mathfrak{p} \text{ splits and is supersingular}\} \tag{5}$$

and

$$\#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_\mathfrak{p} \text{ simple and is supersingular}\}, \tag{6}$$

where $\overline{A}_\mathfrak{p}$ splits means $\overline{A}_\mathfrak{p}$ is isogenous over $\mathbb{F}_\mathfrak{p}$ to a product of smaller dimensional abelian varieties over $\mathbb{F}_\mathfrak{p}$. Then, we use the characterization of simple and split supersingular abelian surfaces by Maisner and Nart [MN02] and Waterhouse [Wat69] to convert the original counting problem to the problem that counts prime ideals $\mathfrak{p}$ for which the characteristic polynomials of Frobenius for $\overline{A}_\mathfrak{p}$ satisfy certain properties. Inspired by an inclusion-exclusion principle by Wan in [Wan90, Lemma 4.1, p. 263], we give a useful counting lemma (Lemma 8) with the help of the Brun–Titchmarsh Theorem. Thanks to this lemma, we can focus on estimating the size of a smaller set of prime ideals $\mathfrak{p}$ of K for which $N(\mathfrak{p}) \leq x$ and the charcateristic polynomials of Frobenius endomorphism of $\overline{A}_\mathfrak{p}$ modulo ℓ splits into linear factors in $\mathbb{F}_\ell[X]$. We then apply the effective version of the Chebotarev Density Theorem by Thorner and Zaman [TZ18] to this subset, with extra effort to find appropriate Galois extensions of number fields.

Remark 2. A similar approach is employed in [TZ18] to establish an unconditional upper bound of

$$\#\{p \leq x : p \nmid N_E, a_p(E) = t\} \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

where $E/\mathbb{Q}$ is a non-CM elliptic curve, N_E is the conductor of E, $a_p(E) = p + 1 - |\overline{E}_p(\mathbb{F}_p)|$ is the Frobenius trace of E, and t is an integer. It is important to note that while this method gives nontrivial bounds for the Lang-Trotter conjecture, obtaining an unconditional upper bound becomes notably challenging for higher-dimensional abelian varieties.

The investigation of an upper bound for (5) motivates us to consider the intersection of various Newton strata in the space of (principally polarized) abelian surfaces. Indeed, primes counted by (5) contribute to nontrivial non-archimedean local intersection numbers of a special divisor in the family of Kuga-Satake abelian schemes (see [SSTT22, Section 2.5] or [ST20, Corollary 2.1.7]) with the supersingular locus of (principally polarized) abelian surfaces. Our next goal is to give an upper bound for the number of prime ideals $\mathfrak{p}$ of K with $N(\mathfrak{p}) \leq x$ for which $\overline{A}_\mathfrak{p}$ splits and presents an extra Newton datum.

We assume the endomorphism algebra $D = \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of A is a real quadratic field. As before, for a prime $\mathfrak{p} \nmid N_A$ of K, the reduction $\overline{A}_{\mathfrak{p}}$ at $\mathfrak{p}$ is an abelian variety defined over the finite field $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{p^k}$ for some $k \geq 1$. Then, the characteristic polynomial $P_{A,\mathfrak{p}}(X)$ of the Frobenius endomorphism of $\overline{A}_{\mathfrak{p}}$ is of the form

$$X^4 + a_{1,\mathfrak{p}}X^3 + a_{2,\mathfrak{p}}X^2 + p^k a_{1,\mathfrak{p}}X + p^{2k}.$$

We consider

$$\pi_{A,\mathrm{split},g(\cdot)}(x) := \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) = p^k \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, a_{2,\mathfrak{p}} = g(p)\}, \tag{7}$$

where $g(\cdot) : \mathbb{N} \to \mathbb{R}$ is an arithmetic function, defined on the set of all natural numbers $\mathbb{N}$ that satisfies $|g(p)| \leq 6p$ for all rational primes p. The subsequent result establishes upper bounds for $\pi_{A,\mathrm{split},g(\cdot)}(x)$.

Theorem 2. *Let A/K be an absolutely simple abelian surface such that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$ and assume A has real multiplication by a real quadratic field F. Let $g(\cdot) : \mathbb{N} \to \mathbb{R}$ be an arithmetic function that satisfies $|g(p)| \leq 6p$ for all rational primes p. We have that*

(1) if for any integer m, the number of rational primes p for which the equation $g(p) = 2p + m$ holds is uniformly bounded (independent of m), then for all sufficiently large x,

$$\pi_{A,\mathrm{split},g(\cdot)}(x) \ll x^{\frac{1}{2}};$$

(2) if $K = \mathbb{Q}$ and $g(p) = 2p + m_0$ for a fixed integer m_0 and p is any rational prime (in particular, the function $g(\cdot)$ does not satisfy the uniform bound assumption in (1)), then for all sufficiently large x,

$$\pi_{A,\mathrm{split},g(\cdot)}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

In both cases, the implicit constants in $\ll$ depend on A, K, and $g(\cdot)$.

Observe that the theorem above applies to many cases, such as when $g(p)$ is a polynomial in p. In particular, we can take $g(p)$ to be a constant and apply Theorem 2 (1). Because of the power saving of $\frac{1}{2}$ in x, we obtain the following nontrivial upper bounds for a large range of $a_{2,\mathfrak{p}}$.

Corollary 3. *Let A/K be an absolutely simple abelian surface such that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$ and A has real multiplication by a real quadratic field F. Let $x > 0$ and $0 < \epsilon \leq 1$. Let $I \subset [-6x, 6x]$ be an interval satisfying $|I| \leq x^{\frac{1}{2}}(\log x)^{-(1+\epsilon)}$. Then for all sufficiently large x,*

$$\#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, a_{2,\mathfrak{p}} \in I\} \ll \frac{x}{(\log x)^{1+\epsilon}},$$

where the implicit constant in $\ll$ depends only on A, K, and ϵ.

Finally, we give an outline of the paper. Section 2 covers essential properties of abelian surfaces over finite fields and Galois representations for abelian surfaces over number fields. In Section 3, we introduce essential analytic ingredients of the proof, including a sieve theoretical lemma and results on the unconditional effective Chebotarev Density Theorem. In Section 4, we discuss counting results and delve into the algebraic properties of small dimensional algebraic groups, which may be of independent interest. In Section 5, we prove a lemma (Lemma 21) that offers an easy criterion for when the characteristic polynomial of Frobenius $P_{A,\mathfrak{p}}(X)$ of A splits modulo a prime ℓ, using the Legendre symbol. This lemma facilitates the application of the sieve theoretical lemma from Section 3, followed by an application of the effective Chebotarev Density Theorem to conclude our proof of Theorem 1. In Section 6, we prove Theorem 2 and Corollary 3. The first case of Theorem 2 is a straightforward consequence of Section 2.3; the proof of the second case requires the fact that $A/\mathbb{Q}$ is a GL_2-type (hence modular) abelian surface, where we prove a variation of Thorner-Zaman's result (see Remark 2) for such abelian surfaces.

Notation. Throughout, we use p and ℓ to denote rational primes; we use q to denote a prime power. We denote by $\mathbb{F}_q$ the finite field with q elements. For a prime ℓ and an integer n, we denote by $\left(\frac{n}{\ell}\right)$ the Legendre symbol; note that the value of $\left(\frac{n}{\ell}\right)$ only depends on the congruence class $n \pmod{\ell}$.

For a number field K, we denote by $\mathcal{O}_K$ the ring of integers of K, Σ_K the set of all nonzero prime ideals in $\mathcal{O}_K$, and $\mathfrak{p}$ a prime ideal in Σ_K. If $\mathfrak{p} \in \Sigma_K$, we also say $\mathfrak{p}$ is a prime of K. We denote by $N(\mathfrak{p})$ the norm of the ideal $\mathfrak{p}$. We write $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{N(\mathfrak{p})}$ for the finite residue field at $\mathfrak{p}$. If $N(\mathfrak{p}) = p$, we say $\mathfrak{p}$ is a prime of degree 1 of K. For a prime ideal $\mathfrak{p}$ and an integer N, we use the notation $\mathfrak{p} \nmid N$ to indicate that $\mathfrak{p}$ and the principal ideal generated by N are coprime.

For an abelian variety A over a number field K, we denote by $N_A \in \mathbb{Z}$ the absolute norm of the conductor ideal of A.

For a set X and two functions $f : X \to \mathbb{R}$ and $g : X \to \mathbb{R}_{\geq 0}$, we say $f \ll g$ if $|f| \leq Cg$ for some absolute constant C. We also write $f = \mathrm{O}(g)$ if $f \ll g$.

For a integer $n \geq 1$ and a unitary ring R with the group of units $R^\times$, we write $M_n(R)$ to denote the set of all $n \times n$ matrices with coefficients in R; we write $\mathrm{GL}_n(R)$ to denote the general linear group with coefficients in R; we write $\mathrm{GSp}_{2n}(R)$ to denote the general symplectic group defined by

$$\left\{M \in \mathrm{GL}_{2n}(R) : J^t M J = \mu M, \mu \in R^\times\right\},$$

where $J := \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ and J^t is the transpose of J.

Acknowledgments

I would like to thank the discussions related to this work with Alina Carmen Cojocaru while I was at the University of Illinois Chicago. I also appreciate enlightening and helpful comments from Valentin Blomer, Valentijn Karemaker, Junxian Li, Freddy Saia, and Yunqing Tang for their helpful comments on the preprint. Finally, I would like to thank the Max-Planck-Institut für Mathematik in Bonn for the stimulating atmosphere to finish this research.

2. Preliminaries on abelian surfaces

2.1. **Supersingular abelian surfaces over finite fields.** Let A be an abelian surface defined over $\mathbb{F}_q$. We begin by revisiting the properties of the characteristic polynomial of the Frobenius endomorphism of A. This endomorphism, denoted as $\pi_q(A)$, is induced by the Frobenius automorphism $x \mapsto x^q$ on $\mathbb{F}_q$. It is well-known that the characteristic polynomial of $\pi_q(A)$ is a q-Weil polynomial of the form

$$P_{A,q}(X) = X^4 + a_{1,q}X^3 + a_{2,q}X^2 + qa_{1,q}X + q^2 \in \mathbb{Z}[X]$$

and $P_{A,q}(X)$ has the following factorization over $\mathbb{C}[X]$:

$$P_{A,q}(X) = (X - \alpha)(X - \frac{q}{\alpha})(X - \beta)(X - \frac{q}{\beta}),$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha| = |\beta| = q^{\frac{1}{2}}$. Moreover, the coefficients of $P_{A,q}(X)$ satisfy the bounds given in [MN02, Lemma 2.1, p. 323]:

$$|a_{1,q}| \leq 4\sqrt{q},\ 2|a_{1,q}|\sqrt{q} - 2q \leq a_{2,q} \leq \frac{a_{1,q}^2}{4} + 2q. \tag{8}$$

The polynomial $P_{A,q}(X)$ is also called *the characteristic polynomial of* A and the constant

$$a_q(A) := -a_{1,q}$$

is referred as the *Frobenius trace* of A. We then define the *discriminant* of $P_{A,q}(X)$ as the constant

$$\Delta_{A,q} := a_{1,q}^2 - 4a_{2,q} + 8q.$$

The following lemma record several equivalent definitions of a supersingular abelian surfaces over the finite prime field $\mathbb{F}_p$.

Lemma 4. *Any one of the following statements can be taken as the definition of a supersingular abelian surface $A/\mathbb{F}_p$.*

(1) A is isogenous over $\overline{\mathbb{F}}_p$ to a product of two supersingular elliptic curves.
(2) The Newton polygon of A is a line segment of slope $\frac{1}{2}$.
(3) The p-rank of A is 0, i.e., $A[p](\overline{\mathbb{F}}_p) = \{0\}$.

Moreover if $p \geq 17$ then we have $a_p(A) = 0$.

Proof. (1) can be found in [RS02, p.339]. (2), (3), and their equivalence can be found in [Pri19, Proposition 3.1].

To show the last claim, since the Newton polygon of A is $\frac{1}{2}$, we have $v_p(a_{1,p}) \geq \frac{1}{2}$. So either $|a_{1,p}| \geq p$ or $a_{1,p} = 0$. But from the bound of $a_{1,p}$ in (8), we derive $p \leq 16$. □

Remark 3. If $A_f/\mathbb{Q}$ is a modular abelian variety in the context of Shimura-Taniyama theory, where f is a weight 2 non-CM newform, then the p-rank of A_f is 0 if and only if $a_p(f) = 0$ for all but finitely many primes $p \nmid N_{A_f}$ [BG97, Proposition 5.2 (ii), p. 62; p. 64]. In particular, if $A/\mathbb{Q}$ is an abelian surface such that $\mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a real quadratic field, then by a result of Ribet [Rib92], A is isogenous over $\mathbb{Q}$ to A_f for some weight 2 cuspidal Hecke eigenform f. So for all sufficiently large prime p, the reduction of A at p is supersingular if and only if $a_p(A) = 0$.

Remark 4. There are also many equivalent definitions of ordinary abelian varieties over $\mathbb{F}_q$. We refer the reader to [How95, (3.1), p. 2366] for details.

The last statement in Lemma 4 can be made explicit as follows.

Lemma 5. *Let $p \geq 7$ be a prime. Let $f(X) = X^4 + a_{1,p}X^3 + a_{2,p}X^2 + pa_{1,p}X + p^2$ be a p-Weil polynomial. Then,*

(1) $f(X)$ is the characteristic polynomial of a simple supersingular abelian surface over $\mathbb{F}_p$ if and only if

$$f(X) \in \{X^4 + pX^2 + p^2, X^4 - pX^2 + p^2, X^4 + p^2, X^4 - 2pX^2 + p^2\}.$$

(2) $f(X)$ is the characteristic polynomial of a supersingular abelian surface that splits over $\mathbb{F}_p$, i.e., the abelian surface is isogenous over $\mathbb{F}_p$ to a product of two (not necessarily distinct) elliptic curves over $\mathbb{F}_p$, if and only if

$$f(X) = X^4 + 2pX^2 + p^2.$$

Proof. Part (1) follows from [MN02, Corollary 2.11, p. 324].

Part (2) could be derived by considering possible slopes of the Newton polygon for the characteristic polynomial of supersingular abelian surfaces that splits. Here, we will give a more direct proof. The"only if" part of (2) follows from the Honda-Tate theory and the classification of the characteristic polynomial of supersingular elliptic curves over $\mathbb{F}_p$ in [Wat69, Theorem 4.1 (5), p.536]. For the "if" part, we first observe from [MN02, Theorem 2.9 and Corollary 2.10] that $f(X)$ corresponds to an nonordinary (i.e., $p \mid a_{2,p}$) abelian surface $A/\mathbb{F}_p$. Since A also splits over $\mathbb{F}_p$, it has to be supersingular based on the p-rank considerations. □

2.2. **Galois representations of abelian surfaces over number fields.** Let K be a number field. Let A be an absolutely simple abelian surface over the number field K. We denote by $D := \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ the endomorphism algebra of A. Let ℓ be a rational prime. We denote by $A[\ell]$ and $T_\ell(A)$ the ℓ-torsion group of A and the ℓ-adic Tate module of A, respectively. The action of

the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ on elements of $A[\ell]$ and $T_\ell(A)$ give the residue modulo ℓ and ℓ-adic Galois representations of A, which we denote by

$$\overline{\rho}_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}/\ell\mathbb{Z}}(A[\ell]) \quad \text{and} \quad \rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)),$$

respectively. Since A is isogenous over $\overline{K}$ to a principally polarized abelian surface, by the existence of the Weil paring, the images of $\overline{\rho}_{A,\ell}$ and $\rho_{A,\ell}$ lie in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and $\mathrm{GSp}_4(\mathbb{Z}_\ell)$, respectively, when ℓ is sufficiently large.

Next, we summarize the images of $\overline{\rho}_{A,\ell}$ and $\rho_{A,\ell}$ based on the structure of D. We have that for all sufficiently large prime ℓ,

(1) if $D = \mathbb{Q}$, then (see [Ser13])

$$\overline{\rho}_{A,\ell}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{GSp}_4(\mathbb{F}_\ell),\ \rho_{A,\ell}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{GSp}_4(\mathbb{Z}_\ell).$$

(2) if $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ and $D = F$ is a real quadratic field such that ℓ splits completely in F and ℓ is unramified in K, then (see [Rib76, Theorem (5.3.5), p. 800] or [Lom16, Remark 1.6, p. 29])

$$\overline{\rho}_{A,\ell}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{GL}_2(\mathbb{F}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{F}_\ell),\ \rho_{A,\ell}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{GL}_2(\mathbb{Z}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where $\mathrm{GL}_2(R) \times_{\det} \mathrm{GL}_2(R)$ denotes

$$\mathrm{GL}_2(R) \times_{\det} \mathrm{GL}_2(R) \coloneqq \{(M_1, M_2) \in \mathrm{GL}_2(R) \times \mathrm{GL}_2(R) : \det(M_1) = \det(M_2)\}$$

for $R \in \{\mathbb{F}_\ell, \mathbb{Z}_\ell\}$.

(3) if $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ and D is a indefinite quaternion algebra such that $\ell > 7$, ℓ splits D (i.e., $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq M_2(\mathbb{Q}_\ell)$), and ℓ is unramified in K, then (see [Oht74, Theorem 3.7] and [DR04])

$$\overline{\rho}_{A,\ell}(\mathrm{Gal}(\overline{K}/K)) \simeq \mathrm{GL}_2(\mathbb{F}_\ell),\ \rho_{A,\ell}(\mathrm{Gal}(\overline{K}/K)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

In fact, the images of $\overline{\rho}_{A,\ell}$ and $\rho_{A,\ell}$ are diagonal embeddings of $\mathrm{GL}_2(\mathbb{F}_\ell)$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$ into the fiber products $\mathrm{GL}_2(\mathbb{F}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{F}_\ell)$ and $\mathrm{GL}_2(\mathbb{Z}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{Z}_\ell)$, respectively.

Finally, we introduce the field K^{conn} and the algebraic group $G_{A,\ell}^{\mathrm{zar}}$ that will be mentioned in the proof of Lemma 7 in the next section. Using the notation mentioned earlier, we denote by $G_{A,\ell}^{\mathrm{zar}}$ the Zariski closure of the image of $\rho_{A,\ell}$ in the algebraic group $\mathrm{GL}_{4/\mathbb{Q}_\ell}$ and by $(G_{A,\ell}^{\mathrm{zar}})^0$ the connected component of $G_{A,\ell}^{\mathrm{zar}}$. Then, a result due to Serre [LP92, Proposition (6.14), p. 623] implies that there is a number field K^{conn}, independent of the choice of ℓ, such that the following map is an isomorphism:

$$\mathrm{Gal}(\overline{K}/K^{\mathrm{conn}}) \xrightarrow{\rho_{A,\ell}} G_{A,\ell}^{\mathrm{zar}} \twoheadrightarrow G_{A,\ell}^{\mathrm{zar}}/(G_{A,\ell}^{\mathrm{zar}})^0.$$

In other words, K^{conn} is the minimal subfield of $\overline{K}$ such that the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}(\overline{K}/K^{\mathrm{conn}}))$ is connected for all primes ℓ. Under the assumption that A is an abelian surface, the field K^{conn} is also the minimal field of definition for the endomorphisms of A. In other words, $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$ is equivalent to saying that $K = K^{\mathrm{conn}}$ (see [LP97] or [Lom19, p. 892, Lemma 2.8 and the paragraph above]).

2.3. **Split reductions of abelian surfaces with real multiplication.** Let K be a number field, and let A be an abelian surface defined over K. In the following, we will explore various properties of A, focusing on the case where $F := \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a real quadratic field. We'll use notation introduced in previous sections.

In this section, we assume $F := \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a real quadratic field. We denote by $\mathcal{O}_K$ the ring of integers of K. For a prime $\mathfrak{p}$ of K such that $\mathfrak{p} \nmid N_A$, we denote by $\mathbb{F}_\mathfrak{p} = \mathbb{F}_q$ the residue field at $\mathfrak{p}$ and by $\overline{A}_\mathfrak{p}$ the reduction of A at $\mathfrak{p}$. We denote by the characteristic polynomial of the Frobenius endomorphsim of $\overline{A}_\mathfrak{p}$ by

$$P_{A,\mathfrak{p}}(X) := P_{\overline{A}_\mathfrak{p},q}(X) = X^4 + a_{1,\mathfrak{p}}X^3 + a_{2,\mathfrak{p}}X^2 + qa_{1,\mathfrak{p}}X + q^2 \in \mathbb{Z}[X]. \tag{9}$$

We recall that for a degree 1 prime $\mathfrak{p}$ of K, the reduction $\overline{A}_{\mathfrak{p}}/\mathbb{F}_p$ splits means $\overline{A}_{\mathfrak{p}}$ is isogenous over $\mathbb{F}_p$ to a product of elliptic curves over $\mathbb{F}_p$.

Lemma 6. *Let A/K be an abelian surface with $F = \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ being a real quadratic field. For any degree 1 prime ideal $\mathfrak{p}$ of K such that $\mathfrak{p} \nmid N_A$, if $\overline{A}_{\mathfrak{p}}$ splits, then*

$$P_{A,\mathfrak{p}}(X) \in \left\{(X^2 + bX + p)^2, (X^2 + bX + p)(X^2 - bX + p)\right\}$$

for some integer b such that $|b| \leq 2\sqrt{p}$. Moreover, if $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ and $\overline{A}_{\mathfrak{p}}$ splits, then $\overline{A}_{\mathfrak{p}}$ is isogenous over $\mathbb{F}_p$ to the square of an elliptic curve. In particular, we have $P_{A,\mathfrak{p}}(X) = (X^2+bX+p)^2$ for some integer b such that $|b| \leq 2\sqrt{p}$.

Proof. See [Wan23, Lemma 17]. □

Lemma 7. *Let A/K be an abelian surface with $F = \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ being a real quadratic field. Moreover, we assume $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$. Then for each prime ideal $\mathfrak{p}$ with $q = N(\mathfrak{p})$ and $\mathfrak{p} \nmid N_A$, we have the following factorization in $F[X]$:*

$$P_{A,\mathfrak{p}}(X) = (X^2 + bX + q)(X^2 + \iota(b)X + q),$$

where $b \in \mathcal{O}_F$ and $\iota(b)$ is the unique Galois conjugate of b in $\overline{\mathbb{Q}}$.

Proof. The proof is similar to the argument in [Lom19, Proposition 3.5, p. 902]. If $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$, then we have $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \in G_{A,\ell}^{\mathrm{zar}} = (G_{A,\ell}^{\mathrm{zar}})^0 \subseteq \mathrm{GL}_2(F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ for each prime ℓ (see Section 2.2). Therefore, for $\mathfrak{p} \nmid \ell N_A$, the characteristic polynomial of $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \subseteq \mathrm{GL}_4(\mathbb{Z}_\ell)$ is of the form $P_{A,\mathfrak{p}}(X) = f(X)\sigma(f(X))$, where $f(X)$ is the characteristic polynomial of the matrix $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ viewed in $\mathrm{GL}_2(F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ and ι is the nontrivial element in $\mathrm{Gal}(F/\mathbb{Q})$. □

The results above are sufficient for the proof of the first case of Theorem 2.

3. Preparations for analytic theory

3.1. **An inclusion-exclusion lemma.** Let $x \in \mathbb{R}_{>0}$ and $t = t(x) \in \mathbb{Z}_{>0}$ that goes to infinity as x increases to infinity. We also assume

$$t(x) \ll (\log x)^{\frac{1}{2}}. \tag{10}$$

Let $\mathcal{M}$ be a subset of rational primes up to x. The goal of this section is to give an upper bound of $\mathcal{M}$ using an inclusion-exclusion principle.

We consider a set $\mathcal{P}$ consisting of t primes that depends on x:

$$\ell_1 < \ell_2 < \ldots < \ell_t \ll \frac{\log x}{\log\log x}. \tag{11}$$

For each $\ell \in \mathcal{P}$, we denote by

$$\mathcal{M}_\ell = \{p \in \mathcal{M} : p \pmod{\ell} \notin \Omega_\ell\},$$

where

$$\Omega_\ell := \{n \pmod{\ell} : \left(\frac{n}{\ell}\right) = -1\}.$$

It is an easy observation that $|\Omega_\ell| = \frac{\ell-1}{2}$. Moreover, we set $P_t := \prod_{\ell \in \mathcal{P}} \ell$ and

$$\Omega_{P_t} := \{n \pmod{P_t} : \left(\frac{n}{\ell}\right) = -1 \ \forall \ell \in \mathcal{P}\}.$$

Then by the Chinese Remainder Theorem, we have $|\Omega_{P_t}| = \prod_{\ell \in \mathcal{P}} \frac{\ell - 1}{2}$. Therefore, for the set

$$\mathcal{S} := \mathcal{M} \setminus \bigcup_{\ell \in \mathcal{P}} \mathcal{M}_\ell = \{p \in \mathcal{M} : \left(\frac{p}{\ell}\right) = -1 \ \forall \ell \in \mathcal{P}\}$$

we have that for all sufficiently x,

$$\begin{aligned}|\mathcal{S}| &\leq \#\{p \leq x : p \pmod{\ell} \in \Omega_\ell \ \forall \ell \in \mathcal{P}\} \\ &= \#\{p \leq x : p \pmod{P_t} \in \Omega_{P_t}\} \\ &= \sum_{a \pmod{P_t} \in \Omega_{P_t}} \#\{p \leq x : p \equiv a \pmod{P_t}\} \\ &\leq \prod_{\ell \in \mathcal{P}} \left(\frac{\ell-1}{2}\right) \cdot \frac{2x}{\log(x/P_t) \prod_{\ell \in \mathcal{P}} (\ell-1)} \\ &\ll \frac{x}{2^t \log(x/P_t)},\end{aligned}$$

where in the second last step we use the Brun–Titchmarsh Theorem, which is applicable because $P_t < x$ for all sufficiently large x by (10).

Lemma 8. *With the notation above, we have for all sufficiently x,*

$$|\mathcal{M}| \ll \sum_{1 \leq j \leq t} |\mathcal{M}_{\ell_j}| + \frac{x}{2^t \log(x/P_t)}.$$

Proof. By using an inclusion-exclusion principle and the bound of $|\mathcal{S}|$, we immediately obtain

$$|\mathcal{M}| \leq \sum_{1 \leq j \leq t} |\mathcal{M}_{\ell_j}| + |\mathcal{S}| \ll \sum_{1 \leq j \leq t} |\mathcal{M}_{\ell_j}| + \frac{x}{2^t \log(x/P_t)}.$$

□

Remark 5. We observe from the proof of Lemma 8 that, to bound $\mathcal{M}$, it is sufficient to bound $|\mathcal{S}|$. The set $\mathcal{S}$ can be regarded as a sifted set (usually denoted by $\mathcal{S}(\mathcal{M}, \mathcal{P}, (\Omega_\ell)_{\ell \in \mathcal{P}})$) in sieve theory. By applying the Pólya-Vinogradov inequality and following the arguments in [Wan90, Proof of Lemma 4.1, pp. 264-265], we get

$$|\mathcal{S}| \leq \frac{x}{2^t} + \sqrt{P_t} \log P_t.$$

Alternatively, we can also apply the large sieve in ([IK04, Theorem 7.10, p. 180]), we get

$$|\mathcal{S}| \leq \frac{x}{2^t \left(1 + \sum_{1 \leq i \leq t} \frac{1}{\ell_i}\right)} + \frac{P_t^2}{\left(1 + \sum_{1 \leq i \leq t} \frac{1}{\ell_i}\right)}.$$

However, neither bound is better than the bound in Lemma 8, considering the constraints on $\mathcal{P}$ and t.

3.2. **Effective Chebotarev Density Theorem.** Let K be a number field. We denote by d_K and n_K the absolute discriminant and the degree of $K/\mathbb{Q}$, respectively. Let L/K be a finite extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. We set

$$\begin{aligned}\mathcal{P}(L/K) &:= \{p : \exists\ \mathfrak{p} \in \Sigma_K, \text{ such that } \mathfrak{p} \mid p \text{ and } \mathfrak{p} \text{ is ramified in } L\}, \\ M(L/K) &:= [L:K] d_K^{\frac{1}{n_K}} \prod_{p \in \mathcal{P}(L/K)} p\end{aligned}$$

Let $\mathcal{C} \subseteq G$ be a conjugation invariant set of G. We denote by

$$\pi_{\mathcal{C}}(x, L/K) := \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \text{ unramified in } L/K, \left(\frac{L/K}{\mathfrak{p}}\right) \subseteq \mathcal{C}\},$$

where $\left(\frac{L/K}{\mathfrak{p}}\right)$ is the Artin symbol of L/K at $\mathfrak{p}$.

First, we state the upper bound of $\log d_L$ due to Hensel, which is proved in [Ser81, Proposition 5, p. 129].

Lemma 9. *If L/K is a finite Galois extension of number fields, then*

$$\log d_L \leq [L:K]\log d_K + ([L:\mathbb{Q}] - [K:\mathbb{Q}])\log \operatorname{rad}(d_{L/K}) + [L:\mathbb{Q}]\log[L:K],$$

where $\operatorname{rad} n \coloneqq \prod_{p|n} p$ is the radical of the integer n.

Next, we recall an unconditional version of the effective Chebotarev Density Theorem due to Thorner and Zaman [TZ18, Theorem 9.1, p. 5022].

Theorem 10. *Let L/K be an abelian extension of number fields. Let $G = \operatorname{Gal}(L/K)$ and $\mathcal{C}$ be a conjugation invariant set of G. Then, for $\log x \gg n_K \log(M(L/K)x)$, we have*

$$\pi_{\mathcal{C}}(x, L/K) \ll \frac{|\mathcal{C}|}{|G|}\operatorname{Li}(x).$$

Finally, we present the following induction and restriction properties of $\pi_{\mathcal{C}}(x, L/K)$.

Lemma 11. *Let L/K be a finite extension of number fields with Galois group G. Let $\mathcal{C}$ be a conjugation invariant set of G. Let H be a subgroup of G and N be a normal subgroup of H. Assume that*

(1) every element of $\mathcal{C}$ is conjugate over G to an element in H.
(2) $N(\mathcal{C}\cap H) \subseteq \mathcal{C}\cap H$.

Then, we have for all sufficiently large x,

$$\pi_{\mathcal{C}}(x, L/K) \ll \pi_{\overline{\mathcal{C}\cap H}}(x, L^N/L^H) + \mathrm{O}\left(n_{L^H}\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L/K)\right)\right),$$

where L^H and L^N represent the fixed field of L by H and N, respectively, and $\overline{\mathcal{C}\cap H}$ represents the image of $\mathcal{C}\cap H$ in H/N.

Proof. By [Zyw15, Lemma 2.6 (i), p. 241 and Lemma 2.7, p. 242], we have

$$\begin{aligned}&\pi_{\mathcal{C}}(x, L/K) + \mathrm{O}\left(n_K\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L/K)\right)\right)\\ &\leq \pi_{\mathcal{C}\cap H}(x, L/L^H) + \mathrm{O}\left(n_{L^H}\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L/L^H)\right)\right).\end{aligned}$$

Therefore,

$$\begin{aligned}\pi_{\mathcal{C}}(x, L/K) \ll \pi_{\mathcal{C}\cap H}(x, L/L^H) &+ n_K\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L/K)\right)\\ &+ n_{L^H}\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L/L^H)\right).\end{aligned}$$

Similarly, by [Zyw15, Lemma 2.6 (ii), p. 241 and Lemma 2.7, p. 242], we have

$$\begin{aligned}\pi_{\mathcal{C}\cap H}(x, L/L^H) = \pi_{\overline{\mathcal{C}\cap H}}(x, L^N/L^H) &+ n_{L^H}\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L/L^H)\right)\\ &+ n_{L^H}\left(\frac{x^{\frac{1}{2}}}{\log x} + \log M(L^N/L^H)\right).\end{aligned}$$

The conclusion follows by combining the two results together. □

4. Results on matrix groups

4.1. **Subgroups and conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$.** Let ℓ be a rational prime. In this section, our attention is directed towards subsets of the general linear group $\mathrm{GL}_2(\mathbb{F}_\ell)$. We introduce the following subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

$$\begin{aligned}
\mathcal{B}(\ell) &:= \left\{ M \in \mathrm{GL}_2(\mathbb{F}_\ell) : M = \begin{pmatrix} \lambda_1 & a \\ 0 & \lambda_2 \end{pmatrix}, \lambda_1, \lambda_2 \in \mathbb{F}_\ell^\times, a \in \mathbb{F}_\ell \right\}, \\
\mathcal{U}(\ell) &:= \left\{ M \in \mathrm{GL}_2(\mathbb{F}_\ell) : M = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_\ell \right\}, \\
\mathcal{U}'(\ell) &:= \left\{ M \in \mathrm{GL}_2(\mathbb{F}_\ell) : M = \begin{pmatrix} \lambda & a \\ 0 & \lambda \end{pmatrix}, \lambda \in \mathbb{F}_\ell^\times, a \in \mathbb{F}_\ell \right\}, \\
\mathcal{T}(\ell) &:= \left\{ M \in \mathrm{GL}_2(\mathbb{F}_\ell) : M = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \lambda_1, \lambda_2 \in \mathbb{F}_\ell^\times \right\}.
\end{aligned}$$

We recall several properties of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Proposition 12. *Let $\ell \geq 5$. The following statements hold.*

(1)

$$\begin{aligned}
|\mathrm{GL}_2(\mathbb{F}_\ell)| &= (\ell-1)^2\ell(\ell+1), \\
|\mathcal{B}(\ell)| &= (\ell-1)^2\ell, \\
|\mathcal{U}(\ell)| &= \ell, \\
|\mathcal{U}'(\ell)| &= \ell(\ell-1), \\
|\mathcal{T}(\ell)| &= (\ell-1)^2.
\end{aligned}$$

(2) $\mathcal{U}(\ell)$ and $\mathcal{U}'(\ell)$ are normal subgroups of $\mathcal{B}(\ell)$.

(3) The quotients $\mathcal{B}(\ell)/\mathcal{U}(\ell)$ and $\mathcal{B}(\ell)/\mathcal{U}'(\ell)$ are abelian. Moreover, we have the isomorphism $\mathcal{B}(\ell)/\mathcal{U}(\ell) \simeq \mathcal{T}(\ell)$.

Proof. The proofs are straightforward and can be found in [CW23, Section 4]. □

Next, we introduce some conjugation invariant sets of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

$$\mathcal{C}'^4(\ell) := \{M \in \mathrm{GL}_2(\mathbb{F}_\ell) : \mathrm{Char}_M(X) = X^2 - \mu = \prod_{1\leq j\leq 2}(X-\lambda_j), \lambda_j \in \mathbb{F}_\ell^\times, \mu \in \mathbb{F}_\ell^\times\}, \tag{12}$$

$$\mathcal{C}'^5(\ell) := \{M \in \mathrm{GL}_2(\mathbb{F}_\ell) : \mathrm{Char}_M(X) = X^2 + \mu = \prod_{1\leq j\leq 2}(X-\lambda_j), \lambda_j \in \mathbb{F}_\ell^\times, \mu \in \mathbb{F}_\ell^\times\}. \tag{13}$$

Remark 6. Note that (12) and (13) are the same set. Distinguishing their names will make the arguments in Section 5.4 easier.

Proposition 13. *Let $\ell \geq 5$. For each $i \in \{4, 5\}$, the following statements hold.*

(1) $\mathcal{C}'^i(\ell)$ is nonempty and is invariant under conjugation by $\mathrm{GL}_2(\mathbb{F}_\ell)$.

(2) Every element of $\mathcal{C}'^i(\ell)$ is conjugate over $\mathrm{GL}_2(\mathbb{F}_\ell)$ to an element in $\mathcal{B}(\ell)$.

(3) We have $\mathcal{U}'(\ell)\mathcal{C}'^i(\ell) \subseteq \mathcal{C}'^i(\ell)$.

Proof. Since $\mathcal{C}'^4(\ell) = \mathcal{C}'^5(\ell)$, it suffices to give a proof for $i = 4$.

For (1), we take $\mu \in \mathbb{F}_\ell^\times$ such that $\mu = \lambda^2$ for some $\lambda \in \mathbb{F}_\ell^\times$. Then, the matrix $\begin{pmatrix} -\lambda & 0 \\ 0 & \lambda \end{pmatrix}$ is an element in $\mathcal{C}'^4(\ell)$. So $\mathcal{C}'^4(\ell)$ is nonempty. The set $\mathcal{C}'^4(\ell)$ is invariant under conjugation over $\mathrm{GL}_2(\mathbb{F}_\ell)$ since eigenvalues are invariant under conjugation.

(2) is a basic fact of the Jordan normal form of matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

To prove part (3), we take an element $M \in \mathcal{C}'^4(\ell)$. Then for any $N \in \mathcal{U}'(\ell)$ with diagonal entries equal to the same value $\lambda \in \mathbb{F}_\ell^\times$, we have

$$\mathrm{Char}_{NM}(X) = X^2 + \mu\lambda^2 = \prod_{1 \le j \le 2} (X - \lambda\lambda_j).$$

Therefore, we have $\mathcal{U}'(\ell)\mathcal{C}'^4(\ell) \subseteq \mathcal{C}'^4(\ell)$. □

Finally, we set

$$\begin{aligned} &\mathcal{C}'^i_{\mathcal{B}}(\ell) := \mathcal{C}'^i(\ell) \cap \mathcal{B}(\ell),\ i \in \{4,5\}, \\ &\overline{\mathcal{C}'^i_{\mathcal{B}}(\ell)} := \text{image of } \mathcal{C}'^i_{\mathcal{B}}(\ell) \text{ in } \mathcal{B}(\ell)/\mathcal{U}'(\ell),\ i \in \{4,5\}. \end{aligned}$$

Proposition 14. *We have* $\left|\overline{\mathcal{C}^i_{\mathcal{B}}}(\ell)\right| \ll 1$ *for* $4 \le i \le 5$.

Proof. This follows from [CW23, Lemma 17 (iv), p. 701]. □

4.2. **Subgroups and conjugacy classes of** $\mathrm{GSp}_4(\mathbb{F}_\ell)$**.** Fix a prime $\ell > 5$. We introduce the following subgroups and conjugation invariant sets of the general symplectic group $\mathrm{GSp}_4(\mathbb{F}_\ell)$. These objects arise as Galois subgroups of $K(A[\ell])/K$ and their conjugation invariant sets, where $K(A[\ell])$ is the ℓ-division field of an absolutely simple abelian surface A satisfying $\mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

We recall the block matrix definition:

$$\mathrm{GSp}_4(\mathbb{F}_\ell) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_\ell) : \quad A,B,C,D \in M_2(\mathbb{F}_\ell), \mu \in \mathbb{F}_\ell^\times, \quad \begin{matrix} -C^tA + A^tC = 0 \\ -C^tB + A^tD = \mu I \\ -D^tB + B^tD = 0 \end{matrix} \right\}$$

and introduce the following subsets of $\mathrm{GSp}_4(\mathbb{F}_\ell)$:

$$\begin{aligned} GB(\ell) := \Bigg\{ &\begin{pmatrix} A & \mu^{-1}AS \\ 0 & \mu(A^t)^{-1} \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_\ell) : A \in \mathrm{GL}_2(\mathbb{F}_\ell) \text{ is an upper triangular matrix}, \\ &S \in M_2(\mathbb{F}_\ell) \text{ is a symmetric matrix}, \mu \in \mathbb{F}_\ell^\times \Bigg\}, \\ GU(\ell) := \Bigg\{ &\begin{pmatrix} A & AS \\ 0 & (A^t)^{-1} \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_\ell) : A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\ a \in \mathbb{F}_\ell, \\ &S \in M_2(\mathbb{F}_\ell) \text{ is a symmetric matrix} \Bigg\}, \\ GU'(\ell) := \Bigg\{ &\begin{pmatrix} A & \mu^{-1}AS \\ 0 & \mu(A^t)^{-1} \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_\ell) : A = \begin{pmatrix} \lambda & a \\ 0 & \lambda \end{pmatrix}, a \in \mathbb{F}_\ell, \lambda \in \mathbb{F}_\ell^\times, \mu = \lambda^2, \\ &S \in M_2(\mathbb{F}_\ell) \text{ is a symmetric matrix} \Bigg\}, \\ GT(\ell) := \Bigg\{ &\begin{pmatrix} A & 0 \\ 0 & \mu A^{-1} \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_\ell) : A \in \mathrm{GL}_2(\mathbb{F}_\ell) \text{ is diagonal}, \mu \in \mathbb{F}_\ell^\times \Bigg\}. \end{aligned}$$

It is easy to check that they are all subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (see [CW22, Proposition 8, p. 14] for a proof). The following properties of these groups will be used.

Proposition 15. *Let* $\ell \ge 5$. *The following statements hold.*

(1)

$$\begin{aligned}|\operatorname{GSp}_4(\mathbb{F}_\ell)| &= (\ell-1)^3\ell^4(\ell+1)^2(\ell^2+1),\\ |GB(\ell)| &= \ell^4(\ell-1)^3,\\ |GU(\ell)| &= \ell^4,\\ |GU'(\ell)| &= \ell^4(\ell-1),\\ |GT(\ell)| &= (\ell-1)^3.\end{aligned}$$

(2) $GU(\ell)$ and $GU'(\ell)$ are normal subgroups of $GB(\ell)$.
(3) The quotients $GB(\ell)/GU(\ell)$ and $GB(\ell)/GU'(\ell)$ are abelian. Moreover, we have the isomorphism $GB(\ell)/GU(\ell) \simeq GT(\ell)$.
(4) $GB(\ell)$ is a Borel subgroup of $\operatorname{GSp}_4(\mathbb{F}_\ell)$, $GU(\ell)$ is a unipotent subgroup of $\operatorname{GSp}_4(\mathbb{F}_\ell)$, and $GT(\ell)$ is a maximal torus of $\operatorname{GSp}_4(\mathbb{F}_\ell)$.

Proof. See [CW22, Proposition 8, p. 14, Proposition 9, p. 16, and Proposition 11, p. 17] for part (1)–(3). Part (4) follows from the fact that Borel subgroups (resp. unipotent subgroups and maximal torus) of $\operatorname{GSp}_4(\mathbb{F}_\ell)$ are conjugate with each other. Then, we can compare the cardinality of $|GB(\ell)|$, $|GU(\ell)|$, and $|GT(\ell)|$ with the "standard" ones such as those in [Bre15, p. 308]. □

Next, we define several conjugation invariant sets of $\operatorname{GSp}_4(\mathbb{F}_\ell)$.

$$\begin{aligned}G\mathcal{C}^1(\ell) := \big\{M \in \operatorname{GSp}_4(\mathbb{F}_\ell) : \operatorname{Char}_M(X) &= X^4+\mu X^2+\mu^2\\ &= \prod_{1\le j\le 2}(X-\lambda_j)(X-\mu\lambda_j^{-1}), \mu, \lambda_j \in \mathbb{F}_\ell^\times\big\}, \qquad (14)\\ G\mathcal{C}^2(\ell) := \big\{M \in \operatorname{GSp}_4(\mathbb{F}_\ell) : \operatorname{Char}_M(X) &= X^4-\mu X^2+\mu^2\\ &= \prod_{1\le j\le 2}(X-\lambda_j)(X-\mu\lambda_j^{-1}), \mu, \lambda_j \in \mathbb{F}_\ell^\times\big\}, \qquad (15)\\ G\mathcal{C}^3(\ell) := \big\{M \in \operatorname{GSp}_4(\mathbb{F}_\ell) : \operatorname{Char}_M(X) &= X^4+\mu^2\\ &= \prod_{1\le j\le 2}(X-\lambda_j)(X-\mu\lambda_j^{-1}), \mu, \lambda_j \in \mathbb{F}_\ell^\times\big\}, \qquad (16)\\ G\mathcal{C}^4(\ell) := \big\{M \in \operatorname{GSp}_4(\mathbb{F}_\ell) : \operatorname{Char}_M(X) &= (X^2-\mu)^2\\ &= \prod_{1\le j\le 2}(X-\lambda_j)(X-\mu\lambda_j^{-1}), \mu, \lambda_j \in \mathbb{F}_\ell^\times\big\}, \qquad (17)\\ G\mathcal{C}^5(\ell) := \big\{M \in \operatorname{GSp}_4(\mathbb{F}_\ell) : \operatorname{Char}_M(X) &= (X^2+\mu)^2\\ &= \prod_{1\le j\le 2}(X-\lambda_j)(X-\mu\lambda_j^{-1}), \mu, \lambda_j \in \mathbb{F}_\ell^\times\big\}. \qquad (18)\end{aligned}$$

Similar to Remark 6, the sets (14) and (15), (17) and (18) are the same. Distinguishing their name will make the arguments in Section 5.2 easier.

Proposition 16. *Let ℓ be an odd prime such that $\left(\frac{-1}{\ell}\right) = \left(\frac{2}{\ell}\right) = \left(\frac{3}{\ell}\right) = 1$. For each $1 \le i \le 5$, the following statements hold.*

(1) $G\mathcal{C}^i(\ell)$ is nonempty and is invariant under conjugation in $\operatorname{GSp}_4(\mathbb{F}_\ell)$.
(2) Each element of $G\mathcal{C}^i(\ell)$ is conjugate over $\operatorname{GSp}_4(\mathbb{F}_\ell)$ to some element of $GB(\ell)$.
(3) We have $GU'(\ell)G\mathcal{C}^i(\ell) \subseteq G\mathcal{C}^i(\ell)$.

Proof. For (1), the conjugation invariant properties are obvious since eigenvalues of any element in $\operatorname{GSp}_4(\mathbb{F}_\ell)$ is invariant under conjugation.

For each $1 \leq i \leq 5$ and ℓ satisfying the assumption of this proposition, we will prove the nonemptiness of $G\mathcal{C}^i(\ell)$ by constructing an element explicitly. To show the nonemptiness of $G\mathcal{C}^1(\ell)$, we choose $\mu \in \mathbb{F}_\ell^\times$ such that there exists an element $a \in \mathbb{F}_\ell^\times$ satisfying $a^2 = \mu$. Then, we find the matrix $M_1, M_2 \in \mathrm{GL}_2(\mathbb{F}_\ell)$ whose characteristic polynomials are $X^2 + aX + \mu$ and $X^2 - aX + \mu$, respectively. Since $\left(\frac{-3}{\ell}\right) = 1$, there is an element $b \in \mathbb{F}_\ell^\times$ such that $a^2 - 4\mu = -3\mu = b^2$. Therefore, the matrix

$$\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$$

is in $G\mathcal{C}^1(\ell)$. For the nonemptiness of $G\mathcal{C}^2(\ell)$, we select $\mu \in \mathbb{F}_\ell^\times$ with solutions $a \in \mathbb{F}_\ell^\times$ and $b \in \mathbb{F}_\ell^\times$ such that $a^2 = 3\mu$ and $b^2 = -\mu$. Similarly, we can find matrices $M_1, M_2 \in \mathrm{GL}_2(\mathbb{F}_\ell)$ whose characteristic polynomials are $X^2 + aX + \mu$ and $X^2 - aX + \mu$, respectively. Then the matrix $\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$ is in $G\mathcal{C}^2(\ell)$. For $G\mathcal{C}^3(\ell)$, we take $\mu \in \mathbb{F}_\ell^\times$ with solutions $a \in \mathbb{F}_\ell^\times$ and $b \in \mathbb{F}_\ell^\times$ such that $a^2 = 2\mu$ and $b^2 = -2\mu$; for $G\mathcal{C}^4(\ell)$, we take $\mu \in \mathbb{F}_\ell^\times$ with solutions $a \in \mathbb{F}_\ell^\times$ and $b \in \mathbb{F}_\ell^\times$ such that $a^2 = 4\mu$ and $b = 0$; for $G\mathcal{C}^5(\ell)$, we take $\mu \in \mathbb{F}_\ell^\times$ with solutions $a \in \mathbb{F}_\ell^\times$ and $b \in \mathbb{F}_\ell^\times$ such that $a = 0$ and $b = -4\mu$. The rest of the proof follow the same line as in the proof for $G\mathcal{C}^1(\ell)$ or $G\mathcal{C}^2(\ell)$.

To show (2), we use the list of conjugacy classes for $\mathrm{GSp}_4(\mathbb{F}_\ell)$ in [Bre15, table 1, pp. 341-346]. By computing the characteristic polynomial of each conjugacy class, we conclude that if the characteristic polynomial of a matrix $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ split into linear polynomials in $\mathbb{F}_\ell[X]$, then M lies in the conjugacy class represented by an element in the Borel subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Therefore, M is conjugate to an element in $GB(\ell)$ by Proposition 15 (4). Since the characteristic polynomial of each element in $G\mathcal{C}^i(\ell)$ splits into linear factors, the element must conjugate to an element in $GB(\ell)$.

To show (3), we take an element $M \in G\mathcal{C}^i(\ell)$ and any $N \in GU'(\ell)$. Let λ be the common diagonal entry of N in $\mathbb{F}_\ell^\times$. Consequently,

$$\mathrm{Char}_{NM}(X) = \prod_{1 \leq j \leq 4} (X - \lambda\lambda_j) = X^4 + \mu\lambda^2 X^2 + (\mu\lambda^2)^2 \; i = 1, \tag{19}$$

$$\mathrm{Char}_{NM}(X) = \prod_{1 \leq j \leq 4} (X - \lambda\lambda_j) = X^4 - \mu\lambda^2 X^2 + (\mu\lambda^2)^2 \; i = 2, \tag{20}$$

$$\mathrm{Char}_{NM}(X) = \prod_{1 \leq j \leq 4} (X - \lambda\lambda_j) = X^4 + (\mu\lambda^2)^2 \; i = 3, \tag{21}$$

$$\mathrm{Char}_{NM}(X) = \prod_{1 \leq j \leq 4} (X - \lambda\lambda_j) = (X^2 - \mu\lambda^2)^2 \; i = 4, \tag{22}$$

$$\mathrm{Char}_{NM}(X) = \prod_{1 \leq j \leq 4} (X - \lambda\lambda_j) = (X^2 + \mu\lambda^2)^2 \; i = 5. \tag{23}$$

We observe that in each case, the inclusion $GU'(\ell)G\mathcal{C}^i(\ell) \subseteq G\mathcal{C}^i(\ell)$ holds.

□

We also need to consider the subsets associated to $G\mathcal{C}^i(\ell)$.

$$G\mathcal{C}_B^i(\ell) := G\mathcal{C}^i(\ell) \cap GB(\ell), \; 1 \leq i \leq 5,$$
$$\overline{G\mathcal{C}}_B^i(\ell) := \text{image of } G\mathcal{C}_B^i(\ell) \text{ in } GB(\ell)/GU'(\ell), \; 1 \leq i \leq 5.$$

The following proposition shows that the cardinality of $\overline{G\mathcal{C}}_B^i(\ell)$ is bounded independent of ℓ.

Proposition 17. *We have* $|\overline{G\mathcal{C}}_B^i(\ell)| \ll 1$ *for* $1 \leq i \leq 5$.

Proof. For each $1 \leq i \leq 5$ we consider the sets

$$\overline{G\mathcal{D}}_B^i(\ell) := \text{image of } G\mathcal{C}_B^i(\ell) \text{ in } GB(\ell)/GU(\ell).$$

Take $M \in G\mathcal{C}_B^i(\ell)$. Since $GB(\ell)/GU(\ell) \simeq GT(\ell)$, the matrix M is uniquely determined by its eigenvalues $\lambda_1, \lambda_2, \mu\lambda_1^{-1}, \mu\lambda_2^{-1} \in \mathbb{F}_\ell^\times$. Comparing the coefficients in each terms of (14)-(18), we get the following estimations.

$$\begin{aligned}
|\overline{G\mathcal{D}}_B^1(\ell)| &\leq \sum_{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times} \#\{\mu \in \mathbb{F}_\ell^\times : \sum_{1\leq j\leq 2} \lambda_j + \mu\lambda_j^{-1} = 0, \lambda_1\lambda_2 + \mu\lambda_1\lambda_2^{-1} + \mu\lambda_2\lambda_1^{-1} + 2\mu = \mu\} \\
&\leq \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1^{-1}+\lambda_2^{-1}=0}} 1 \right) + \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1^{-1}+\lambda_2^{-1}\neq 0,\ \lambda_1+\lambda_2\neq 0 \\ \lambda_1\lambda_2(\lambda_1^{-1}+\lambda_2^{-1})=(\lambda_1\lambda_2^{-1}+\lambda_1^{-1}\lambda_2+1)(\lambda_1+\lambda_2)}} 1 \right) \\
&\leq \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1^{-1}+\lambda_2^{-1}=0}} 1 \right) + \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1\lambda_2^{-1}+\lambda_1^{-1}\lambda_2+1=1}} 1 \right) \ll \ell.
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
|\overline{G\mathcal{D}}_B^2(\ell)| &\leq \sum_{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times} \#\{\mu \in \mathbb{F}_\ell^\times : \sum_{1\leq i\leq 2} \lambda_i + \mu\lambda_i^{-1} = 0, \lambda_1\lambda_2 + \mu\lambda_1\lambda_2^{-1} + \mu\lambda_2\lambda_1^{-1} + 2\mu = -\mu\}, \\
&\leq \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1^{-1}+\lambda_2^{-1}=0}} 1 \right) + \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1\lambda_2^{-1}+\lambda_1^{-1}\lambda_2+3=1}} 1 \right) \ll \ell, \\
|\overline{G\mathcal{D}}_B^3(\ell)| &\leq \sum_{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times} \#\{\mu \in \mathbb{F}_\ell^\times : \sum_{1\leq i\leq 2} \lambda_i + \mu\lambda_i^{-1} = 0, \lambda_1\lambda_2 + \mu\lambda_1\lambda_2^{-1} + \mu\lambda_2\lambda_1^{-1} + 2\mu = 0\} \\
&\leq \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1^{-1}+\lambda_2^{-1}=0}} 1 \right) + \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1\lambda_2^{-1}+\lambda_1^{-1}\lambda_2+2=1}} 1 \right) \ll \ell, \\
|\overline{G\mathcal{D}}_B^4(\ell)| &\leq \sum_{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times} \#\{\mu \in \mathbb{F}_\ell^\times : \sum_{1\leq i\leq 2} \lambda_i + \mu\lambda_i^{-1} = 0, \lambda_1\lambda_2 + \mu\lambda_1\lambda_2^{-1} + \mu\lambda_2\lambda_1^{-1} + 2\mu = -2\mu\} \\
&\leq \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1^{-1}+\lambda_2^{-1}=0}} 1 \right) + \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times \\ \lambda_1\lambda_2^{-1}+\lambda_1^{-1}\lambda_2+4=1}} 1 \right) \ll \ell,
\end{aligned}$$

$$|\overline{GD}^5_B(\ell)| \leq \sum_{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times} \#\{\mu\in\mathbb{F}_\ell^\times : \sum_{1\leq i\leq 2}\lambda_i+\mu\lambda_i^{-1}=0, \lambda_1\lambda_2+\mu\lambda_1\lambda_2^{-1}+\mu\lambda_2\lambda_1^{-1}+2\mu=2\mu\}$$
$$\leq \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times\\ \lambda_1^{-1}+\lambda_2^{-1}=0}} 1\right) + \left(\sum_{\substack{\lambda_1,\lambda_2\in\mathbb{F}_\ell^\times\\ \lambda_1\lambda_2^{-1}+\lambda_1^{-1}\lambda_2=1}} 1\right) \ll \ell.$$

Since the inverse image of $\overline{GC}^i_B(\ell)\subseteq GB(\ell)/GU(\ell)$ under the quotient map $GB(\ell)/GU(\ell)\to GB(\ell)/GU'(\ell)$ is exactly $\overline{GD}^i_B(\ell)$, the desired bounds follow from the fact that

$$|\overline{GC}^i_B(\ell)| = \frac{|\overline{GD}^i_B(\ell)|}{|GU'(\ell)/GU(\ell)|} \ll 1,\ 1\leq i\leq 5$$

□

4.3. **Subgroups and conjugacy classes of** $\mathrm{GL}_2(\mathbb{F}_\ell)\times\mathrm{GL}_2(\mathbb{F}_\ell)$**.** Now we focus on the subsets of

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

We consider the following subgroups of $G(\ell)$.

$$B(\ell) := \{(M_1,M_2)\in G(\ell) : M_1 \text{ and } M_2 \text{ are upper triangular}\},$$
$$U(\ell) := \left\{(M_1,M_2)\in G(\ell) : M_1 = \begin{pmatrix}1 & a_1\\ 0 & 1\end{pmatrix}, M_2 = \begin{pmatrix}1 & a_2\\ 0 & 1\end{pmatrix}, a_1,a_2\in\mathbb{F}_\ell\right\}$$
$$U'(\ell) := \left\{(M_1,M_2)\in G(\ell) : M_1 = \begin{pmatrix}\lambda & a_1\\ 0 & \lambda\end{pmatrix}, M_2 = \begin{pmatrix}\lambda & a_2\\ 0 & \lambda\end{pmatrix}, a_1,a_2\in\mathbb{F}_\ell,\lambda\in\mathbb{F}_\ell^\times\right\},$$
$$T(\ell) := \{(M_1,M_2)\in G(\ell) : M_1 \text{ and } M_2 \text{ are diagonal}\},$$

We will use the following properties of these groups.

Proposition 18. *Let $\ell\geq 5$. The following statements hold.*

(1)

$$|G(\ell)| = (\ell-1)^3\ell^2(\ell+1)^2,$$
$$|B(\ell)| = (\ell-1)^3\ell^2,$$
$$|U(\ell)| = \ell^2,$$
$$|U'(\ell)| = \ell^2(\ell-1),$$
$$|T(\ell)| = (\ell-1)^3.$$

(2) $U(\ell)$ and $U'(\ell)$ are normal subgroups of $B(\ell)$.
(3) The quotient groups $B(\ell)/U(\ell)$ and $B(\ell)/U'(\ell)$ are abelian. Moreover, we have the isomorphism $B(\ell)/U(\ell)\simeq T(\ell)$.

Proof. See [CW23, Lemma 11, Lemma 12, and Lemma 13 pp. 697-698] for the proofs. □

We also need the following conjugation invariant sets of $G(\ell)$.

$$\mathcal{C}^1(\ell) := \{M \in G(\ell) : \mathrm{Char}_M(X) = X^4 + \mu X^2 + \mu^2 = \prod_{1\le j\le 4}(X-\lambda_j), \lambda_j, \mu \in \mathbb{F}_\ell^\times\}, \tag{24}$$

$$\mathcal{C}^2(\ell) := \{M \in G(\ell) : \mathrm{Char}_M(X) = X^4 - \mu X^2 + \mu^2 = \prod_{1\le j\le 4}(X-\lambda_j), \lambda_j, \mu \in \mathbb{F}_\ell^\times\}, \tag{25}$$

$$\mathcal{C}^3(\ell) := \{M \in G(\ell) : \mathrm{Char}_M(X) = X^4 + \mu^2 = \prod_{1\le j\le 4}(X-\lambda_j), \lambda_j, \mu \in \mathbb{F}_\ell^\times\}, \tag{26}$$

$$\mathcal{C}^4(\ell) := \{M \in G(\ell) : \mathrm{Char}_M(X) = (X^2 - \mu)^2 = \prod_{1\le j\le 4}(X-\lambda_j), \lambda_j, \mu \in \mathbb{F}_\ell^\times\}, \tag{27}$$

$$\mathcal{C}^5(\ell) := \{M \in G(\ell) : \mathrm{Char}_M(X) = (X^2 + \mu)^2 = \prod_{1\le j\le 4}(X-\lambda_j), \lambda_j, \mu \in \mathbb{F}_\ell^\times\}. \tag{28}$$

Similar to Remark 6, (24) and (25), (27) and (28) are actually the same sets, but distinguishing their names will simplify the arguments in Section 5.3.

Proposition 19. *Let ℓ be an odd prime such that $\left(\frac{-1}{\ell}\right) = \left(\frac{2}{\ell}\right) = \left(\frac{3}{\ell}\right) = 1$. For each $1 \le i \le 5$, the following statements hold.*

(1) $\mathcal{C}^i(\ell)$ is nonempty and is invariant under conjugation in $G(\ell)$.
(2) Each element of $\mathcal{C}^i(\ell)$ is conjugate over $G(\ell)$ to an element of $B(\ell)$.
(3) We have $U'(\ell)\mathcal{C}^i(\ell) \subseteq \mathcal{C}^i(\ell)$.

Proof. For (1), the conjugation invariant property is obvious since the eigenvalues of $G(\ell)$ are invariant under conjugation. The proofs of nonemptiness of $\mathcal{C}^i(\ell)$ for $1 \le i \le 5$ is similar to the proof of Proposition 16 (1).

(2) follows from [CW23, Lemma 15, p. 700], since the characteristic polynomial of each element of $\mathcal{C}^i(\ell)$ splits into linear factors.

The proof of (3) also follows similarly from the proof of Proposition 16 (3).

□

Similarly as before, we consider the sets

$$\mathcal{C}_B^i(\ell) := \mathcal{C}^i(\ell) \cap B(\ell),\ 1 \le i \le 5,$$
$$\overline{\mathcal{C}}_B^i(\ell) := \text{image of } \mathcal{C}_B^i(\ell) \text{ in } B(\ell)/U'(\ell),\ 1 \le i \le 5.$$

Proposition 20. *We have $|\overline{\mathcal{C}}_B^i(\ell)| \ll 1$ for $1 \le i \le 5$.*

Proof. First, we consider the sets

$$\overline{\mathcal{D}}_B^i(\ell) := \text{image of } \mathcal{C}_B^i(\ell) \text{ in } B(\ell)/U(\ell), 1 \le i \le 5.$$

Take $M \in \mathcal{C}_B^i(\ell)$. Then the image of M in $B(\ell)/U(\ell) \simeq T(\ell)$ is uniquely determined by its eigenvalues. As abelian groups, we have the isomorphism (see Proposition 15 (1), (3) and Proposition 18 (1), (3))

$$T(\ell) \simeq B(\ell)/U(\ell) \simeq GB(\ell)/GU(\ell) \simeq GT(\ell).$$

So we can proceed similarly as in the proof of Proposition 17, and derive the bounds

$$|\overline{\mathcal{D}}_B^i(\ell)| \ll \ell,\ 1 \le i \le 5.$$

Finally, we get

$$|\overline{\mathcal{C}}_B^i(\ell)| = \frac{|\overline{\mathcal{D}}_B^i(\ell)|}{|\mathbb{F}_\ell^\times|} \ll 1,\ 1 \le i \le 5.$$

□

5. Proof of Theorem 1

5.1. **The setup.** We keep the notation in Section 2. Upon recalling Lemma 5, we obtain

$$\begin{aligned}
\pi_{A,ss}(x) &\leq \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ is supersingular and simple}\} \\
&\quad + \#\{\mathfrak{p} \in \Sigma_K, N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ is supersingular and splits}\} \\
&\leq \#\{\mathfrak{p} \in \Sigma_K, N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, P_{A,\mathfrak{p}}(x) = x^4 + px^2 + p^2\} && (29) \\
&\quad + \#\{\mathfrak{p} \in \Sigma_K, N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, P_{A,\mathfrak{p}}(x) = x^4 - px^2 + p^2\} && (30) \\
&\quad + \#\{\mathfrak{p} \in \Sigma_K, N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, P_{A,\mathfrak{p}}(x)(x) = x^4 + p^2\} && (31) \\
&\quad + \#\{\mathfrak{p} \in \Sigma_K, N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, P_{A,\mathfrak{p}}(x) = (x^2 - p)^2\} && (32) \\
&\quad + \#\{\mathfrak{p} \in \Sigma_K, N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, P_{A,\mathfrak{p}}(x) = (x^2 + p)^2\} && (33) \\
&\quad + \mathrm{O}(x^{\frac{1}{2}}), && (34)
\end{aligned}$$

where (29)-(32) together count prime ideals $\mathfrak{p} \nmid N_A$ such that $\overline{A}_{\mathfrak{p}}$ is supersingular and simple and (33) counts primes $\mathfrak{p} \nmid N_A$ such that $\overline{A}_{\mathfrak{p}}$ is supersingular and splits. For simplicity, we write $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_4$, and $\mathcal{S}_5$ to denote the sets counted by (29), (30), (31), (32), and (33), respectively.

For each prime ℓ and $1 \leq i \leq 5$, we denote by

$$\tilde{\pi}_A^i(\ell, x) := \{\mathfrak{p} \in \mathcal{S}_i : P_{A,\mathfrak{p}}(X) \pmod{\ell} \text{ splits into linear factors in } \mathbb{F}_\ell[X]\}.$$

We first apply Lemma 8 to bound $\pi_{A,ss}(x)$ in terms of $\tilde{\pi}_A^i(\ell, x)$, where ℓ lies in one of the following carefully-chosen sets:

(1) We define

$$\mathcal{L}_i := \begin{cases} \left\{\ell \text{ odd} : \left(\frac{-1}{\ell}\right) = \left(\frac{3}{\ell}\right) = 1\right\} = \{\ell : \ell \equiv 1 \pmod{12}\} & i = 1, 2 \\ \left\{\ell \text{ odd} : \left(\frac{-1}{\ell}\right) = \left(\frac{2}{\ell}\right) = 1\right\} = \{\ell : \ell \equiv 1 \pmod{8}\} & i = 3 \\ \{\ell \text{ odd prime}\} & i = 4 \\ \left\{\ell \text{ odd} : \left(\frac{-1}{\ell}\right) = 1\right\} = \{\ell : \ell \equiv 1 \pmod{4}\} & i = 5. \end{cases}$$

(2) If $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{d})$ for some $d > 0$, we define for each $i \in \{1, 2, 3, 4, 5\}$

$$\begin{aligned}
\mathcal{L}_i^{RM} &:= \mathcal{L}_i \cap \left\{\ell \text{ odd} : \ell \text{ is unramified in } K \text{ and } \left(\frac{-d}{\ell}\right) = 1\right\} \\
&= \mathcal{L}_i \cap \left\{\ell \text{ odd} : \ell \text{ is unramified in } K \text{ and splits in } \mathbb{Q}(\sqrt{d})\right\},
\end{aligned}$$

where $\mathcal{L}_i$ is defined in (1).

(3) If $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ is isomorphic to a quaternion algebra D with discriminant d_D, we define for each $i \in \{1, 2, 3, 4, 5\}$

$$\mathcal{L}_i^{QM} := \mathcal{L}_i \cap \{\ell \text{ odd} : \ell > 7 \text{ is unramified in } K \text{ and } \ell \nmid d_D\},$$

where $\mathcal{L}_i$ is defined in (1).

We observe that by the Chebotarev Density Theorem,

$$\left(\bigcap_{1 \leq i \leq 5} \mathcal{L}_i\right) \bigcap \{\ell : \ell \text{ split in } \mathbb{Q}(\sqrt{d})\} \bigcap \{\ell : \ell \nmid d_D\} \bigcap \{\ell > 7 : \ell \text{ unramified in } K\} \neq \emptyset.$$

It is worth pointing out that the construction of $\mathcal{L}_i$ follows a similar rationale to the assumptions of ℓ in Proposition 16 and Proposition 19.

The subsequent lemma provides a criterion for the splitting of $P_{A,\mathfrak{p}}(X) \pmod{\ell}$ over $\mathbb{F}_\ell[X]$ using the Legendre symbol $\left(\frac{N(\mathfrak{p})}{\ell}\right)$, where $N(\mathfrak{p}) = p$ is a rational prime.

Lemma 21. *Let ℓ be an odd prime. For each $\mathfrak{p} \in \mathcal{S}_i$ and $\ell \in \mathcal{L}_i$, $1 \leq i \leq 5$, the polynomial $P_{A,\mathfrak{p}}(X) \pmod{\ell}$ splits into linear factors in $\mathbb{F}_\ell[X]$ if and only if $\left(\frac{N(\mathfrak{p})}{\ell}\right) \neq -1$.*

Proof. We only present the argument in the case where $i = 1$, as the proofs for the other cases are very similar.

Let $\ell \in \mathcal{L}_1$, $\mathfrak{p} \in \mathcal{S}_1$, and write $p = N(\mathfrak{p})$. If $p = \ell$, then $P_{A,\mathfrak{p}}(X) \pmod{\ell}$ clearly splits into linear factors. So we assume $p \neq \ell$ and we will find the linear factors of $P_{A,\mathfrak{p}}(X) \pmod{\ell}$ in $\mathbb{F}_\ell[X]$.

We observe that since

$$P_{A,\mathfrak{p}}(X) \equiv X^4 + pX^2 + p^2 \equiv X^4\left(p^2(1/X)^4 + p(1/X)^2 + 1\right) \pmod{\ell},$$

the roots of $P_{A,\mathfrak{p}}(X) \equiv 0 \pmod{\ell}$ come in pairs $(\alpha_i, p/\alpha_i)$ for $i \in \{1, 2\}$. Hence we can always write the decomposition of the form

$$X^4 + pX^2 + p^2 \equiv (X^2 + b_1X + \mu)(X^2 + b_2X + \mu) \pmod{\ell} \quad b_1, b_2, \mu \in \overline{\mathbb{F}}_\ell. \tag{35}$$

First, we show such decomposition exists if and only if $\left(\frac{p}{\ell}\right) = 1$. By comparing coefficients on both sides of (35), we get

(1) $\mu^2 \equiv p^2 \pmod{\ell}$;
(2) $b_1 = -b_2$;
(3) $b_1b_2 + 2\mu \equiv p \pmod{\ell}$.

This implies

$$\begin{cases} \mu \equiv p \pmod{\ell} \\ b := b_1^2 = b_2^2 \equiv p \pmod{\ell} \end{cases} \quad \text{or} \quad \begin{cases} \mu \equiv -p \pmod{\ell}, \\ b := b_1^2 = b_2^2 \equiv -3p \pmod{\ell}. \end{cases} \tag{36}$$

Considering (36) and the definition of $\mathcal{L}_1$, we see that the decomposition (35) is over $\mathbb{F}_\ell[X]$ if and only if

$$\left(\frac{p}{\ell}\right) = 1 \text{ or } \left(\frac{-3p}{\ell}\right) = 1 \iff \left(\frac{p}{\ell}\right) = 1. \tag{37}$$

Suppose $\left(\frac{p}{\ell}\right) = 1$ holds. Using the discriminant criteria for the reducibility of quadratic polynomials, we observe that the polynomial (35) splits into linear polynomials in $\mathbb{F}_\ell[X]$ if and only if

$$\left(\frac{b^2 - 4\mu}{\ell}\right) \neq -1 \iff \left(\frac{p}{\ell}\right) \neq -1.$$

In conclusion, $P_{A,\mathfrak{p}}(X) \pmod{\ell}$ splits into linear factors if and only if $\left(\frac{p}{\ell}\right) \neq -1$. □

Based on Lemma 21, for each $\ell \in \mathcal{L}_i$ (or $\mathcal{L}_i^{\mathrm{RM}}$, $\mathcal{L}_i^{\mathrm{QM}}$) we can express $\tilde{\pi}_A^i(\ell, x)$ as follows:

$$\tilde{\pi}_A^i(\ell, x) = \#\{\mathfrak{p} \in \mathcal{S}_i : \left(\frac{N(\mathfrak{p})}{\ell}\right) \neq -1\},\ 1 \leq i \leq 5. \tag{38}$$

5.2. **Abelian surface with $D = \mathbb{Q}$.** We keep the notation and assumption from Section 3.1, Section 4.2 and Section 5.1. As before, let x be a positive real number and let $t = t(x) \ll (\log x)^{\frac{1}{2}}$ be a positive real number that goes to infinity as x increases to infinity. For each fixed $1 \leq i \leq 5$, we take

$$\mathcal{P}_i := \{\ell_1 < \ldots < \ell_t\} \subseteq \mathcal{L}_i \cap \left\{\ell \text{ odd} : \left(\frac{-1}{\ell}\right) = \left(\frac{2}{\ell}\right) = \left(\frac{3}{\ell}\right) = 1\right\}$$

such that $\ell \ll \frac{\log x}{\log\log x}$ for all $\ell = \ell(x) \in \mathcal{P}$. By the Prime Number Theorem in Arithmetic Progressions, we can always find such set $\mathcal{P}_i$. Applying Lemma 8, we obtain

$$\begin{aligned}|\mathcal{S}_i| &\leq \sum_{1\leq j\leq t} \tilde{\pi}_A^i(\ell_j, x) + \#\{\mathfrak{p} \in \mathcal{S}_i : \left(\frac{N(\mathfrak{p})}{\ell}\right) = -1 \text{ for all } \ell \in \mathcal{P}_i\} \\ &\ll \sum_{1\leq j\leq t} \tilde{\pi}_A^i(\ell_j, x) + \frac{x}{2^t \log(x/P_i)} \\ &\ll t \max_{\ell\in\mathcal{P}_i} \tilde{\pi}_A^i(\ell, x) + \frac{x}{2^t \log(x/P_i)}, \end{aligned} \tag{39}$$

where $P_i = \prod_{\ell\in\mathcal{P}_i} \ell$.

Now we recall from (1) in Section 2.2 that for any $\ell \in \mathcal{P}_i$ that is sufficiently large, the Galois group of the extension $K(A[\ell])/K$ is isomorphic to $\mathrm{GSp}_4(\mathbb{F}_\ell)$. As we have seen in Lemma 21, for each prime $\mathfrak{p}$ counted by $\tilde{\pi}_A^i(\ell, x)$, the polynomial $P_{A,\mathfrak{p}}(X) \pmod{\ell}$ splits into linear factors. In particular, the eigenvalues of $\overline{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ are in $\mathbb{F}_\ell^\times$. Therefore,

$$\tilde{\pi}_A^i(\ell, x) \ll \pi_{G\mathcal{C}^i(\ell)}(x, K(A[\ell])/K).$$

We invoke Proposition 16 and apply Lemma 11 with $K(A[\ell])/K$, $G = \mathrm{GSp}_4(\mathbb{F}_\ell)$, $H = GB(\ell)$, $N = GU'(\ell)$, and $\mathcal{C} = G\mathcal{C}^i(\ell)$ to get

$$\tilde{\pi}_A^i(\ell, x) \ll \pi_{\overline{G\mathcal{C}}_B^i(\ell)}(x, K(A[\ell])^{GU'(\ell)}/K(A[\ell])^{GB(\ell)}).$$

Next, we invoke Proposition 15 (1) and (3), Proposition 17, Lemma 9, and Theorem 10 with the extension $K(A[\ell])^{GU'(\ell)}/K(A[\ell])^{GB(\ell)}$ and the conjugation invariant set $\mathcal{C} = \overline{G\mathcal{C}}_B^i(\ell)$ to get

$$\tilde{\pi}_A^i(\ell, x) \ll \frac{1}{\ell^2}\frac{x}{\log x}, \tag{40}$$

under the restriction that

$$\log x \gg n_K \ell^4 \log(\ell N_A d_K x). \tag{41}$$

Combining (39) with (40), for all sufficiently large x, we obtain

$$|\mathcal{S}_i| \ll \frac{t}{\ell_1^2}\frac{x}{\log x} + \frac{x}{2^t \log(x/\ell_t^t)}$$

as long as (41) is satisfied. With this restriction in mind, we choose $\ell_1 = \ell_1(x)$ and $t = t(x)$ such that for sufficiently large $x > 0$,

$$\ell_1 \sim c_1 \left(\frac{\log x}{n_K \log\log(N_A d_K x)}\right)^{\frac{1}{4}},\ t \sim c \log\log x$$

for some sufficiently large positive real number c and some sufficiently small positive real number c_1. Again, the choices are possible because we can always find t primes $\ell_1, \ldots, \ell_t$ in the interval $[\ell_1, 2\ell_1]$ when x is sufficiently large. We conclude that for all sufficiently large $x > 0$,

$$|\mathcal{S}_i| \ll \frac{x(\log\log x)^{\frac{3}{2}}}{(\log x)^{\frac{3}{2}}},$$

where the implicit constant in $\ll$ depends on A and K.

Putting it all together, we obtain

$$\pi_{A,ss}(x) \ll \sum_{1\leq i\leq 5} |\mathcal{S}_i| \ll \frac{x(\log\log x)^{\frac{3}{2}}}{(\log x)^{\frac{3}{2}}},$$

where the implicit constant in the last $\ll$ depends on A and K. This completes the proof of part (1) of Theorem 1.

5.3. **Abelian surface with real multiplication.** We maintain the notation and assumption from Section 3.1, Section 4.3, and Section 5.1.

We draw analogous arguments in the previous section. Fix an integer $t \geq 1$. As before, let x be a positive real number and let $t = t(x) \ll (\log x)^{\frac{1}{2}}$ be a positive real number that goes to infinity as x increases to infinity. For each fixed $1 \leq i \leq 5$, we take

$$\mathcal{P}_i := \{\ell_1 < \ldots < \ell_t\} \subseteq \mathcal{L}_i^{RM} \cap \left\{\ell \text{ odd} : \left(\frac{-1}{\ell}\right) = \left(\frac{2}{\ell}\right) = \left(\frac{3}{\ell}\right) = 1\right\}$$

such that $\ell \ll \frac{\log x}{\log\log x}$ for all $\ell = \ell(x) \in \mathcal{P}$. By Lemma 8, we obtain

$$\begin{aligned} |\mathcal{S}_i| &\leq \sum_{1\leq j\leq t} \tilde{\pi}_A^i(\ell_j, x) + \#\{\mathfrak{p} \in \mathcal{S}_i : \left(\frac{N(\mathfrak{p})}{\ell}\right) = -1 \text{ for all } \ell \in \mathcal{P}_i\} \\ &\ll t \max_{\ell\in\mathcal{P}_i} \tilde{\pi}_A^i(\ell, x) + \frac{x}{2^t \log(x/P_i)}, \end{aligned} \tag{42}$$

where $P_i = \prod_{\ell\in\mathcal{P}_i} \ell$.

Now we recall the first part of (2) in Section 2.2 and observe that for any $\ell \in \mathcal{P}_i$ that is sufficiently large, the Galois group of the extension $K(A[\ell])/K$ is isomorphic to $G(\ell)$. Similar to the proof in the previous section, we have

$$\tilde{\pi}_A^i(\ell, x) \ll \pi_{\mathcal{C}^i(\ell)}(x, K(A[\ell])/K).$$

We invoke Proposition 19 and apply Lemma 11 with $G = G(\ell)$, $H = B(\ell)$, $N = U'(\ell)$, and $\mathcal{C} = \mathcal{C}^i(\ell)$ to get

$$\tilde{\pi}_A^i(\ell, x) \ll \pi_{\overline{\mathcal{C}}_B^i(\ell)}(x, K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}),\ 1 \leq i \leq 5.$$

Next, we apply Proposition 18 (1), (3), Proposition 20, Lemma 9, and Theorem 10 with Galois extension $K(A[\ell])^{U'(\ell)}/K(A[\ell])^{B(\ell)}$ and the conjugation invariant set $\mathcal{C} = \overline{\mathcal{C}}_B^i(\ell)$ to get

$$\tilde{\pi}_A^i(\ell, x) \ll \frac{1}{\ell^2}\frac{x}{\log x}, \tag{43}$$

under the restriction that

$$\log x \gg n_K \ell^2 \log(\ell N_A d_K x). \tag{44}$$

Therefore, for all sufficiently large $x > 0$, we have

$$|\mathcal{S}_i| \ll \frac{t}{\ell_1^2}\frac{x}{\log x} + \frac{x}{2^t \log(x/\ell_t^t)}$$

as long as (44) is satisfied for $\ell \in \mathcal{P}_i$. With this restriction in mind, we choose $\ell_1 = \ell_1(x)$ and $t = t(x)$ such that for all sufficiently large $x > 0$,

$$\ell_1 \sim c_1' \left(\frac{\log x}{n_K \log\log(N_A x)}\right)^{\frac{1}{2}},\ t \sim c' \log\log x$$

for some sufficiently large positive real number c' and some sufficiently small positive real number c_1'. We conclude that for all sufficiently large $x > 0$,

$$|\mathcal{S}_i| \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

where the implicit constant in $\ll$ depends on A and K.

Putting it all together, we obtain

$$\pi_{A,ss}(x) \ll \sum_{1\le i\le 5} |\mathcal{S}_i| \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

where the implicit constant in the last $\ll$ depends on A and K.

This completes the proof of part (2) of Theorem 1.

5.4. **Abelian surface with quaternion multiplication.** We keep the notation and assumption form Section 3.1, Section 4.1 and Section 5.1. Fix an integer $t \ge 1$. For each $4 \le i \le 5$, we take

$$\mathcal{P}_i := \{\ell_1 < \ldots < \ell_t\} \subseteq \mathcal{L}_i^{QM} \cap \left\{\ell \text{ odd} : \left(\frac{-1}{\ell}\right) = \left(\frac{2}{\ell}\right) = \left(\frac{3}{\ell}\right) = 1\right\},$$

such that $\ell \ll \frac{\log x}{\log\log x}$ for all $\ell = \ell(x) \in \mathcal{P}$. We recall from (3) in Section 2.2 that for ℓ sufficiently large, the Galois group of the extension $K(A[\ell])/K$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$ identified as the diagonal embedding of $\mathrm{GL}_2(\mathbb{F}_\ell)$ into $\mathrm{GSp}_4(\mathbb{F}_\ell)$. So for each prime ideal $\mathfrak{p}$ counted by $\pi_{A,ss}(x)$, the characteristic polynomial $P_{A,\mathfrak{p}}(X)$ is a square in $\mathbb{Z}[X]$. So we deduce that

$$\pi_{A,ss}(x) \le |\mathcal{S}_4| + |\mathcal{S}_5|.$$

For each $i \in \{4, 5\}$, by Lemma 8, we obtain that

$$\begin{aligned} |\mathcal{S}_i| &\le \sum_{1\le j\le t} \tilde{\pi}_A^i(\ell_j, x) + \#\{\mathfrak{p} \in \mathcal{S}_i : \left(\frac{N(\mathfrak{p})}{\ell}\right) = -1 \text{ for all } \ell \in \mathcal{P}_i\} \\ &\ll t \max_{\ell\in\mathcal{P}_i} \tilde{\pi}_A^i(\ell, x) + \frac{x}{2^t \log(x/P_i)}, \end{aligned} \tag{45}$$

where $P_i = \prod_{\ell\in\mathcal{P}_i} \ell$. Similar as before, we have

$$\tilde{\pi}_A^i(\ell, x) \ll \pi_{\mathcal{C}'^i(\ell)}(x, K(A[\ell])/K).$$

We invoke and apply Proposition 13 and Lemma 11 with $K(A[\ell])/K$, $G = \mathrm{GL}_2(\mathbb{F}_\ell)$, $H = \mathcal{B}(\ell)$, $N = \mathcal{U}'(\ell)$, and $\mathcal{C} = \mathcal{C}'^i(\ell)$ to get

$$\tilde{\pi}_A^i(\ell, x) \ll \pi_{\overline{\mathcal{C}'^i_{\mathcal{B}}(\ell)}}(x, K(A[\ell])^{\mathcal{U}'(\ell)}/K(A[\ell])^{\mathcal{B}(\ell)}),\ i \in \{4, 5\}.$$

Next, we apply Proposition 12 (1), Proposition 14, Lemma 9, and Theorem 10 and with Galois extension $K(A[\ell])^{\mathcal{U}'(\ell)}/\mathbb{Q}(A[\ell])^{\mathcal{B}(\ell)}$, $\mathcal{C} = \overline{\mathcal{C}'^i_{\mathcal{B}}}(\ell)$ to get

$$\tilde{\pi}_A^i(\ell, x) \ll \frac{1}{\ell}\frac{x}{\log x}, \tag{46}$$

under the restriction that

$$\log x \gg n_K \ell \log(\ell N_A d_K x). \tag{47}$$

So for all sufficiently large $x > 0$, we have

$$|\mathcal{S}_i| \ll \frac{t}{\ell_1}\frac{x}{\log x} + \frac{x}{2^t \log(x/\ell_t^t)}$$

as long as (47) is satisfied for $\ell \in \mathcal{P}_i$. As before, we choose $\ell_1 := \ell_1(x)$ and $t := t(x)$ such that for sufficiently large $x > 0$,

$$\ell_1 \sim c_1'' \frac{\log x}{n_K \log\log(N_A d_K x)},\ t \sim c'' \log\log x$$

for some sufficiently large positive real number c'' and some sufficiently small positive real number c_1''. We conclude that for all sufficiently large $x > 0$,

$$|\mathcal{S}_i| \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

where the implicit constant in $\ll$ depends on A and K.

Putting it all together, we obtain

$$\pi_{A,ss}(x) \ll |\mathcal{S}_4| + |\mathcal{S}_5| \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

where the implicit constant in the last $\ll$ depends on A and K. This finishes the proof of part (3) of Theorem 1.

6. Proofs of Theorem 2 and Corollary 3

In this section, we assume A is an abelian surface defined over a number field K such that $\mathrm{End}_K(A)\otimes_{\mathbb{Z}}\mathbb{Q} = \mathrm{End}_{\overline{K}}(A)\otimes\mathbb{Q} = \mathbb{Q}(\sqrt{d})$ for some squrefree integer $d > 1$. Let N_A be the conductor of A. Let $\mathfrak{p}$ be a degree 1 prime ideal of K such that $\mathfrak{p} \nmid N_A$, then the characteristic polynomial of the Frobenius endomorphism of $\overline{A}_{\mathfrak{p}}$ is $P_{A,\mathfrak{p}}(X) = X^4 + a_{1,\mathfrak{p}}X^3 + a_{2,\mathfrak{p}}X^2 + pa_{1,\mathfrak{p}}X + p^2 \in \mathbb{Z}[X]$.

First, we present the proof of Corollary 3 using Theorem 2.

Proof of Corollary 3. By elementary observations, we obtain that for any $\epsilon > 0$,

$$\begin{aligned}
&\#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \le x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, a_{2,\mathfrak{p}} \in I\} \\
&= \sum_{\substack{t\in\mathbb{Z}\\ t\in I}} \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \le x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, a_{2,\mathfrak{p}} = t\} \\
&\ll \#\{t \in \mathbb{Z} : t \in I\} \cdot x^{\frac{1}{2}} \qquad (48)\\
&\ll \frac{x}{(\log x)^{1+\epsilon}},
\end{aligned}$$

where Theorem 2 (1) with $g(p) = t$ is applied in the estimation of (48). □

Proof of Theorem 2. Let $\mathfrak{p} \in \Sigma_K$ be a degree 1 prime with $N(\mathfrak{p}) = p$ and assume $p \neq 2$. Under the assumption that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$, we can apply Lemma 7 and get $b_{\mathfrak{p}}(A) = \alpha_{\mathfrak{p}} + \beta_{\mathfrak{p}}\sqrt{d}$, where $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}} \in \mathbb{Z}$, such that

$$\begin{aligned}
P_{A,\mathfrak{p}}(X) &= (X^2 + b_{\mathfrak{p}}(A)X + p)(X^2 + (\alpha_{\mathfrak{p}} + \iota(b_{\mathfrak{p}}(A))X + p) \\
&= (X^2 + (\alpha_{\mathfrak{p}} + \beta_{\mathfrak{p}}\sqrt{d})X + p)(X^2 + (\alpha_{\mathfrak{p}} - \beta_{\mathfrak{p}}\sqrt{d})X + p).
\end{aligned}$$

If $\overline{A}_{\mathfrak{p}}$ also splits, then by Lemma 6, we get

$$a_{1,\mathfrak{p}} = 2b_1,\ a_{2,\mathfrak{p}} = 2p + b_1^2,$$

for some integer b_1 such that $|b_1| \le 2\sqrt{p}$. Comparing coefficients in (9), we obtain

$$\alpha_{\mathfrak{p}} = b_1,\ \beta_{\mathfrak{p}} = 0.$$

(1) If $g(\cdot)$ is an arithmetic function such that for any integer $m \in [-2\sqrt{p}, 2\sqrt{p}]$, the number of primes p satisfying the equation $g(p) = 2p + m^2$ is uniformly bounded (independent of the value of

m), then

$$\begin{aligned}
&\#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, a_{2,\mathfrak{p}} = g(p)\} \\
&= \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, a_{2,\mathfrak{p}} = g(p)\} + \mathrm{O}(x^{\frac{1}{2}}) \\
&\leq \sum_{\substack{m \in \mathbb{Z} \\ |m| \leq 2\sqrt{x}}} \#\{\mathfrak{p} \in \Sigma_K : N(\mathfrak{p}) = p \leq x, \mathfrak{p} \nmid N_A, \overline{A}_{\mathfrak{p}} \text{ splits}, \alpha_{\mathfrak{p}} = m, g(p) = 2p + \alpha_{\mathfrak{p}}^2\} + \mathrm{O}(x^{\frac{1}{2}}) \\
&\ll \sum_{\substack{m \in \mathbb{Z} \\ |m| \leq 2\sqrt{x}}} \#\{p \leq x, g(p) = 2p + m^2\} + x^{\frac{1}{2}} \\
&\ll x^{\frac{1}{2}}.
\end{aligned}$$

(2) Parallel to the proof above, we obtain that for the arithmetic function $g(\cdot)$ satisfying $g(p) = 2p + m_0$ for a fixed integer m_0 and all primes p,

$$\begin{aligned}
&\#\{p \leq x : p \nmid N_A, \overline{A}_p \text{ splits}, a_{2,p} = g(p)\} \\
&\leq \sum_{\substack{m \in \mathbb{Z} \\ |m| \leq 2\sqrt{x}}} \#\{p \leq x : p \nmid N_A, \overline{A}_p \text{ splits}, \alpha_p = m, 2p + m_0 = 2p + m^2\} + \mathrm{O}(x^{\frac{1}{2}}) \\
&\ll \#\{p \leq x : p \nmid N_A, \overline{A}_p \text{ splits}, \alpha_p = \pm\sqrt{m_0}\}.
\end{aligned}$$

To bound the first summand, we prove a slightly more general result. For any fixed integer $a \in \mathbb{Z}$, we will show

$$\pi_A(x, a) := \#\{p \leq x : p \nmid N_A, b_p(A) = a\} \ll \frac{x(\log\log x)^2}{(\log x)^2}. \tag{49}$$

Then from the discussion above, we have

$$\#\{p \leq x : p \nmid N_A, \overline{A}_p \text{ splits}, \alpha_p = a\} \leq \pi_A(x, a).$$

Let $F := \mathbb{Q}(\sqrt{d})$. Let ℓ be an odd prime that is coprime to p that splits completely into $\ell = \lambda_1\lambda_2$ in $\mathcal{O}_F$. Since $\mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{d})$, we know A is a GL_2-type abelian surface, hence by the result of Ribet [Rib92], A is associated with a weight 2 cuspidal Hecke eigenform f. From the Galois representation theory associated to weight 2 cuspidal Hecke eigenforms (see e.g., [RS01]), we have the residue modulo λ_1 Galois representation associated to f:

$$\overline{\rho}_{A,\lambda_1} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_F/\lambda_1\mathcal{O}_F) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Then, by switching λ_1 and λ_2 if necessary, for p counted in (49), we have that the characteristic polynomial of the matrix $\overline{\rho}_{A,\lambda_1}(\mathrm{Frob}_p)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ is

$$\mathrm{Char}_{\overline{\rho}_{A,\lambda_1}(\mathrm{Frob}_p)}(X) := X^2 + b_p(A)X + p \pmod{\lambda_1} \in \mathbb{F}_\ell[X],$$

where $b_p(A)$ shall be viewed as an algebraic integer in $\mathcal{O}_K$. By (2) in Section 2.2, we know that $\overline{\rho}_{A,\lambda_1}$ is surjective for all sufficiently large $\ell = N(\lambda_1)$. Hence there is a finite Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Im}(\overline{\rho}_{A,\lambda_1}) = \mathrm{GL}_2(\mathbb{F}_\ell)$. Moreover, the following relation $\mathrm{tr}\,\overline{\rho}_{A,\lambda_1}(\mathrm{Frob}_p) \equiv -b_p(A) \pmod{\lambda_1}$ holds.

We now bound (49) following the proofs in [TZ18, Theorem 1.4] and [Wan90, Corollary 4.2]. We only give a sketch of the proof since it closely resembles the arguments in proofs of the results mentioned above. First, we introduce a function similar to the one in [Wan90, Section 4.1, (4.2)]:

$$\pi_A(x, a, \ell) := \#\{p \leq x : p \nmid N_A, b_p(A) = a, \left(\frac{a^2 - 4p}{\ell}\right) = 1\}.$$

Then the proof of [Wan90, Corollary 4.2] is still valid to bound $\pi_A(x,a)$ in (49). Namely, taking any t odd primes $\ell_1 < \ldots < \ell_t$ that splits completely in F, each less than $\exp(\log x/2t)$, such that $t \sim \tilde{c}\log\log x$ for some positive real number $\tilde{c}$, we have

$$\pi_A(x,a) \ll \sum_{1\le j\le t} \pi_A(x,a,\ell_j) + \frac{x}{(\log x)^2} \ll \log\log x \cdot \max_{1\le j\le t} \pi_A(x,a,\ell_j) + \frac{x}{(\log x)^2}.$$

Next, we apply Theorem 10 to bound each $\pi_A(x,a,\ell_j)$. We observe that for $a \in \mathbb{Z}$, if $\left(\frac{a^2-4p}{\ell}\right) = 1$, then the polynomial $X^2 + aX + p \pmod{\lambda_1}$ splits into linear polynomials in $\mathbb{F}_\ell[X]$. Therefore, if $\ell_1 \sim \tilde{c_1}\frac{\log x}{\log\log x}$ where $\tilde{c_1}$ is a well-chosen positive real number which may depends on F, $\ell_j \in [\ell_1, 2\ell_1]$ for all $1 \le j \le t$, and $t \sim \tilde{c_1}\log\log x$, then for $\ell_j = \lambda_{1,j}\lambda_{2,j}$, we have

$$\begin{aligned}
&\pi_A(x,a,\ell_j)\\
&\ll \max_{1\le i\le 2}\Big\{\#\{p \le x : p \nmid N_A, b_p(A) = a \pmod{\lambda_{i,j}},\\
&\qquad\qquad \mathrm{Char}_{\overline{\rho}_{A,\lambda_{i,j}}(\mathrm{Frob}_p)}(X) \text{ splits into linear factors in } \mathbb{F}_\ell[X]\}\Big\}
\end{aligned}$$

For each $i \in \{1,2\}$, using the same argument as [TZ18, Secttion 9.1, Proof of Theorem 1.4], we get

$$\begin{aligned}
&\#\{p \le x : p \nmid N_A, b_p(A) = a \pmod{\lambda_{i,j}},\\
&\qquad\qquad \mathrm{Char}_{\overline{\rho}_{A,\lambda_{i,j}}(\mathrm{Frob}_p)}(X) \text{ splits into linear factors in } \mathbb{F}_\ell[X]\}\\
&\ll \frac{x(\log\log x)}{(\log x)^2},
\end{aligned}$$

where the implicit constant in $\ll$ depends on A.

In conclusion, we obtain

$$\pi_A(x,a) \ll \log\log x \cdot \frac{x(\log\log x)}{(\log x)^2} + \frac{x}{(\log x)^2} \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

This completes the proof of (49) and hence the final bound holds.

□

7. Further discussions

7.1. **Frobenius trace for GL_2-type abelian surfaces.** Recall that an abelian variety A over $\mathbb{Q}$ is of GL_2-type if $\mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a number field of degree equal to $\dim A$. So in case (2) of Theorem 1, the abelian surface $A/\mathbb{Q}$ is of GL_2-type, hence is modular. We also want to look into the two assumptions (3) and (4): according to [Pyl04, Theorem 1.2, p. 192], (3) happens if and only if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an indefinite quaternion algebra over $\mathbb{Q}$ (A has quaternion multiplication); (4) happens if and only if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a real quadratic field (A has real multiplication). In fact, f satisfies (3) if and only if it admits a nontrivial inner twist [DR05].

Therefore, if A_f is associated with a non-CM cuspidal Hecke eigenform f of weight 2 and level N such that (4) holds, we invoke Remark 3 and immediately deduce

$$\#\{p \le x : p \nmid N_{A_f}, a_p(A_f) = 0\} \ll \frac{x(\log\log x)^2}{(\log x)^2}, \tag{50}$$

from Theorem 1 (2), where $a_p(A_f)$ is the Frobenius trace of A_f. This also serves as an unconditional upper bound for the Lang-Trotter Conjecture for abelian surfaces. Furthermore, by modularity, we have

$$a_p(A_f) = a_p(f) + a_p(f)^\sigma,$$

where σ is the unique nontrivial real embedding of $K_f = \mathbb{Q}(\sqrt{d})$ (d is a positive integer). Hence $a_p(A_f) = 0$ if and only if $a_p(f) = m\sqrt{d}$ for some integer m. Then (50) implies that

$$\sum_{m\in\mathbb{Z}} \#\{p \le x : p \nmid N, a_p(f) = m\sqrt{d}\} \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

Lastly, concerning the distribution of Frobenius traces of GL_2-type abelian surfaces, a generalized Sato-Tate Conjecture is also explored in [Gon14].

7.2. **CM abelian varieties.** Let A/K be an absolutely simple abelian surface such that $F := \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM quartic field. Let N_A be the conductor of A. In this short section, we consider the distribution of supersingular primes of the abelian surface A.

First, in the special case when $\mathcal{O}_F \subseteq \mathrm{End}_{\overline{K}}(A)$, $F(\subseteq K)$ is a quartic primitive CM field, Goren [Gor97, Theorem 1 and Theorem 2] classified the set of primes $\mathfrak{p}$ of K such that $\mathfrak{p} \nmid N_A$, $\mathfrak{p}$ is unramified in F, and $\overline{A}_{\mathfrak{p}}$ is supersingular. For example, let $K = F$ a degree 4 cyclic extension of $\mathbb{Q}$, then the density of supersingular primes for A/K is $\frac{3}{4}$. Moreover, by [Saw16, Theorem 2.3, p. 567], the density of ordinary primes for A is either $\frac{1}{4}$, $\frac{1}{2}$, or 1. We see that the density has to be $\frac{1}{4}$. Immediately, we have the two interesting observations: the minimal field of definition for all endomorphisms of A is a degree 4 extension of K and the density of the almost ordinary primes for A is 0.

In general, if A/K is an abelian variety of CM type (F, Φ) (e.g., see [Lan83, p. 13] for the definition), we can use Shimura-Taniyama theory [ST61] to characterize supersingular primes of A. Let $\mathfrak{p} \nmid N_A$ be an unramified prime in $K/\mathbb{Q}$. For any prime w of F such that $w \mid N(\mathfrak{p})$, we consider the completion F_w of F at w, the image H_w of $\mathrm{Hom}_{\mathbb{Q}_p}(F_w, \mathbb{C})$ in $\mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})$ (under the field isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$), and $\Phi_w = H_w \cap \Phi$. If $\mathfrak{p}$ is a supersingular prime of A, then the Shimura-Taniyama formula implies $\frac{|\Phi_w|}{|H_w|} = \frac{1}{2}$. This shows that the density of supersingular primes for a CM abelian variety depends on both F and K. To get the density, we need to consider elements of decomposition groups at primes of F to compute the density (see [Bla14, Example after Theorem 3.1, p. 1260]).

7.3. **Nonsimple abelian surfaces.** Let $A/\mathbb{Q}$ be an abelian surface that is $\mathbb{Q}$-isogenous to a product of two non-CM elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$. We now discuss the distribution of supersingular primes of the nonsimple abelian surface A.

By definition of supersingular primes, for $p \nmid N_A$, $\overline{A}_p$ is supersingular if and only if both $\overline{E}_p$ and $\overline{E'}_p$ are supersingular. If E and E' are $\overline{\mathbb{Q}}$-isogenous, then

$$\pi_{A,ss}(x) = \pi_{E,ss}(x) + \mathrm{O}(1) = \pi_{E',ss}(x) + \mathrm{O}(1).$$

This counting problem has already been discussed in the introduction; If E and E' are not $\overline{\mathbb{Q}}$-isogenous, relevant results are explored by Fouvry and Murty [FM95]. They predict that for all sufficiently x,

$$\pi_{A,ss}(x) \sim C_{E,E'} \log\log x,$$

where $C_{E,E'}$ is a constant that only depends on E and E', and prove that this prediction holds on average.

References

[Bel16] Joël Bellaïche. Théorème de Chebotarev et complexité de Littlewood. *Ann. Sci. Éc. Norm. Supér. (4)*, 49(3):579–632, 2016.

[BG97] Pilar Bayer and Josep González. On the Hasse-Witt invariants of modular curves. *Experiment. Math.*, 6(1):57–76, 1997.

[Bla14] Chris Blake. A Deuring criterion for abelian varieties. *Bull. Lond. Math. Soc.*, 46(6):1256–1263, 2014.

[Bre15] Jeffery Breeding, II. Irreducible characters of $\mathrm{GSp}(4, q)$ and dimensions of spaces of fixed vectors. *Ramanujan J.*, 36(3):305–354, 2015.

[CDSS17] Alina Carmen Cojocaru, Rachel Davis, Alice Silverberg, and Katherine E. Stange. Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre). *Int. Math. Res. Not. IMRN*, (12):3557–3602, 2017.

[CW22] Alina Carmen Cojocaru and Tian Wang. Bounds for the distribution of the Frobenius traces associated to a generic abelian variety, 2022.

[CW23] Alina Carmen Cojocaru and Tian Wang. Bounds for the distribution of the Frobenius traces associated to products of non-CM elliptic curves. *Canad. J. Math.*, 75(3):687–712, 2023.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih. *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1982.

[DR04] Luis V. Dieulefait and Victor Rotger. The arithmetic of QM-abelian surfaces through their Galois representations. *J. Algebra*, 281(1):124–143, 2004.

[DR05] Luis V. Dieulefait and Victor Rotger. On abelian surfaces with potential quaternionic multiplication. *Bull. Belg. Math. Soc. Simon Stevin*, 12(4):617–624, 2005.

[Elk87] Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[Elk91] Noam D. Elkies. Distribution of supersingular primes. Number 198-200, pages 127–132. 1991. Journées Arithmétiques, 1989 (Luminy, 1989).

[FM95] É. Fouvry and M. Ram Murty. Supersingular primes common to two elliptic curves. In *Number theory (Paris, 1992–1993)*, volume 215 of *London Math. Soc. Lecture Note Ser.*, pages 91–102. Cambridge Univ. Press, Cambridge, 1995.

[Gon14] Josep González. The Frobenius traces distribution for modular Abelian surfaces. *Ramanujan J.*, 33(2):247–261, 2014.

[Gor97] Eyal Z. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta Math.*, 94(1):33–43, 1997.

[How95] Everett W. Howe. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.*, 347(7):2361–2401, 1995.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Lan83] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[Lom16] Davide Lombardo. Explicit open image theorems for abelian varieties with trivial endomorphism ring, 2016. arXiv:1508.01293.

[Lom19] Davide Lombardo. Computing the geometric endomorphism ring of a genus-2 Jacobian. *Math. Comp.*, 88(316):889–929, 2019.

[LP92] M. Larsen and R. Pink. On l-independence of algebraic monodromy groups in compatible systems of representations. *Invent. Math.*, 107(3):603–636, 1992.

[LP97] Michael Larsen and Richard Pink. A connectedness criterion for l-adic Galois representations. *Israel J. Math.*, 97:1–10, 1997.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*, volume Vol. 504 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[MN02] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[Oht74] Masami Ohta. On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 21:299–308, 1974.

[Pri19] Rachel Pries. Current results on Newton polygons of curves. In *Open problems in arithmetic algebraic geometry*, volume 46 of *Adv. Lect. Math. (ALM)*, pages 179–207. Int. Press, Somerville, MA, [2019] ©2019.

[Pyl04] Elisabeth E. Pyle. Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 189–239. Birkhäuser, Basel, 2004.

[Rib76] Kenneth A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Rib92] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[RS01] Kenneth A. Ribet and William A. Stein. Lectures on Serre's conjectures. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 143–232. Amer. Math. Soc., Providence, RI, 2001.

[RS02] Karl Rubin and Alice Silverberg. Supersingular abelian varieties in cryptology. In *Advances in cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, pages 336–353. Springer, Berlin, 2002.

[Saw16] William F. Sawin. Ordinary primes for Abelian surfaces. *C. R. Math. Acad. Sci. Paris*, 354(6):566–568, 2016.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Ser13] Jean-Pierre Serre. Lettre à Marie-France Vignéras du 10/2/1986. In *Oeuvres/Collected papers. IV. 1985–1998*, Springer Collected Works in Mathematics, pages viii+694. Springer, Heidelberg, 2013. Reprint of the 2000 edition [MR1730973].

[SSTT22] Ananth N. Shankar, Arul Shankar, Yunqing Tang, and Salim Tayou. Exceptional jumps of Picard ranks of reductions of K3 surfaces over number fields. *Forum Math. Pi*, 10:Paper No. e21, 49, 2022.

[ST61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. Mathematical Society of Japan, Tokyo, 1961.

[ST20] Ananth N. Shankar and Yunqing Tang. Exceptional splitting of reductions of abelian surfaces. *Duke Math. J.*, 169(3):397–434, 2020.

[TZ18] Jesse Thorner and Asif Zaman. A Chebotarev variant of the Brun-Titchmarsh theorem and bounds for the Lang-Trotter conjectures. *Int. Math. Res. Not. IMRN*, (16):4991–5027, 2018.

[Wan90] Da Qing Wan. On the Lang-Trotter conjecture. *J. Number Theory*, 35(3):247–268, 1990.

[Wan23] Tian Wang. Distribution of primes of split reductions for abelian surfaces, 2023.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[Zyw15] David Zywina. Bounds for the Lang-Trotter conjectures. In *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, volume 655 of *Contemp. Math.*, pages 235–256. Amer. Math. Soc., Providence, RI, 2015.

Tian Wang, Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany
Email address: twang@mpim-bonn.mpg.de