ERDŐS–KAC ANALOGUES FOR GENERIC ABELIAN VARIETIES AND ABELIAN SURFACES

CHUANGXUN CHENG AND YIDING CUI

Abstract. Let K be a number field. We prove an analogue of the Erdős–Kac theorem for g-dimensional abelian varieties A/K whose adelic Galois representation has open image in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. For a prime v of K at which A has good reduction, we consider two arithmetic invariants, an expression related to the Frobenius trace at v, and the number of rational points on the reduction of A at v. Under the Generalized Riemann Hypothesis, we show that the number of prime divisors of each of these invariants, suitably normalized, follows a standard normal distribution. For a pair of non-isogenous abelian varieties of this type, we prove that the corresponding pairs of invariants have a joint normal distribution. This yields a criterion for geometric isogeny, which states that a positive density of coincidences between the number of prime divisors of these invariants implies that the two varieties are isogenous over $\overline{K}$. Moreover, we also prove Erdős–Kac analogues for the number of rational points on the reductions at good primes of absolutely simple abelian surfaces that are not of CM-type.

1. Introduction

Let $\omega(n)$ denote the number of distinct prime divisors of a nonzero integer n. The Erdős–Kac theorem [7] states that the random variables

$$\frac{\omega(n)-\log\log n}{\sqrt{\log\log n}}$$

defined on the set of natural numbers less than x, as x goes to infinity converge in distribution to the standard normal distribution. More precisely, for any $\alpha\in\mathbb{R}$, Erdős and Kac proved that

$$\lim_{x\to+\infty}\frac{1}{x}\sharp\left\{n\le x:\ \frac{\omega(n)-\log\log n}{\sqrt{\log\log n}}\le\alpha\right\}=G(\alpha):=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha}e^{-x^2/2}\mathrm{d}x.$$

Their proof is based on the central limit theorem and sieve methods, and this work inspires an approach for studying arithmetic functions through their statistical properties.

Subsequently, numerous generalizations of the Erdős–Kac theorem have been studied by many mathematicians. We refer to [10] and the references therein for more information. In particular, under the General Riemann Hypothesis (hereafter abbreviated as GRH), Murty–Murty [19] proved an analogue of the Erdős–Kac theorem for the Fourier coefficients of modular forms, and Liu [14] proved an analogue of the Erdős–Kac theorem for the numbers of rational points of elliptic curves over $\mathbb{Q}$. In [2], under the GRH, Bloom proved

2020 *Mathematics Subject Classification.* 11G10, 11F80.

Key words and phrases. generic abelian varieties, the Erdős–Kac theorem, Galois representations, general symplectic group, abelian surfaces.

The authors are supported by NSFC 11701272.

that for a principally polarized abelian variety $A/\mathbb{Q}$ of dimension g whose adelic Galois representation has open image in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$, and any $\alpha \in \mathbb{R}$, one has

$$\lim_{x\to+\infty} \frac{1}{\pi(x)} \sharp \left\{ p \leq x : p \text{ is of good reduction}, \frac{\omega(|A_p(\mathbb{F}_p)|) - \log\log p}{\sqrt{\log\log p}} \leq \alpha \right\} = G(\alpha),$$

where $\pi(x)$ is the number of primes $p \leq x$ and $A_p(\mathbb{F}_p)$ is the set of rational points of the reduction of A at p.

In [6], El-Baz–Loughran–Sofos generalized the work of predecessors and established a multivariate version of the Erdős–Kac theorem. Applying the result of [6] and generalizing the works of Murty–Murty and Liu, Wang–Cheng in [28] established a result regarding the joint distribution of the number of prime divisors of the Fourier coefficients of two distinct newforms and obtained a probabilistic multiplicity one theorem. Chen–Cheng–Cui in [4] established versions of the above result for independent compatible systems of Galois representations of rank one and of rank two over more general coefficients, and proved multiplicity one results for CM elliptic curves and abelian varieties of GL_2-type. In particular, for A_1/K and A_2/K two abelian varieties of GL_2-type, let N_x be the set of primes v of K such that $|v| := \mathrm{Norm}_{K/\mathbb{Q}}\, v \leq x$, and A_1 and A_2 have good reduction at v, $A_{1,v}(k_v)$ and $A_{2,v}(k_v)$ be the sets of k_v-rational points of the reductions of A_1 and A_2 at v, where k_v is the residue field of K at v. Then under the GRH, if

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \{ v \in N_x : \ \omega(|A_{1,v}(k_v)| + 1) = \omega(|A_{2,v}(k_v)| + 1) \} > 0,$$

then A_1 and A_2 are isogenous over $\overline{K}$. A natural question to ask is whether the above claim holds for general abelian varieties. In this paper, we follow the framework of [4] to study compatible systems of Galois representations with GSp-type image. By a trick of [3] and a counting formula of [13], we establish analogues of the Erdős–Kac theorem for two types of arithmetic invariants of abelian varieties over number fields admitting such representations, generalizing Bloom's result [2] and the results in [4] and [28]. To make our results precise, we start with the following definition.

Definition 1.1. Let K be a number field and let A/K be a principally polarized abelian variety of dimension g with adelic Galois representation $\hat{\rho} : G_K \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. We say that A is *generic* if the image of $\hat{\rho}$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$.

The study of the size of the image of Galois representations attached to abelian varieties has been a central topic in arithmetic geometry. A fundamental conjecture in this area is the Mumford-Tate conjecture, which predicts a deep connection between the Galois action and the Hodge structure of the variety.

Let A be a principally polarized abelian variety of dimension g defined over a number field K. The *Mumford–Tate group* $\mathrm{MT}(A)$ is the smallest $\mathbb{Q}$-algebraic subgroup of GSp_{2g} whose base change to $\mathbb{C}$ contains the image of the Hodge cocharacter. We say that A is of GSp-*type* (cf. [12]) if its Mumford–Tate group is generic, i.e., $\mathrm{MT}(A) = \mathrm{GSp}_{2g}$. For such varieties, the Mumford–Tate conjecture implies that the ℓ-adic Galois representation associated with the Tate module $T_\ell(A)$, $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(A)) \subset \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ has open image in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ for all primes ℓ, and equals $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ for sufficiently large ℓ.

Indeed, Serre [26, Section 136 and 137], Pink [21], and Hall [11] have shown that there exists a large, natural class of abelian varieties of GSp-type satisfying the Mumford–Tate conjecture unconditionally and whose adelic Galois representation has open image.

Theorem 1.2 (cf. [11, 21, 26])**.** *Let A be a principally polarized abelian variety of dimension g defined over a number field K with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. Assume that at least one of the following conditions holds:*

(1) *g does not belong to the exceptional set*

$$S = \left\{ g \geq 1 \;\middle|\; \exists k \geq 3 \text{ odd}, \exists a \geq 1, g = 2^{k-1}a^k \right\} \cup \left\{ g \geq 1 \;\middle|\; \exists k \geq 3 \text{ odd}, g = \frac{1}{2}\binom{2k}{k} \right\}$$
$$= \{4, 10, 16, 32, \ldots\}.$$

(2) *The Néron model of A over $\mathcal{O}_K$ has a semistable fiber with toric dimension equal to 1.*

Then A is generic.

In [12], Hindry–Ratazzi proved that if the Mumford–Tate conjecture holds for some abelian varieties of GSp-type, then it also holds for products of such abelian varieties. This leads to the following result describing the image of the product Galois representation from two generic abelian varieties. For an effective version of this result under the GRH, see the recent paper [17].

Theorem 1.3. *Let A_1/K and A_2/K be two generic abelian varieties of dimension g_1 and g_2 respectively. Assume that A_1 and A_2 are not $\overline{K}$-isogenous, then the image of the product of their adelic Galois representation is an open subgroup of $\Delta_{g_1,g_2}(\hat{\mathbb{Z}}) = \prod_\ell \Delta_{g_1,g_2}(\mathbb{Z}_\ell)$, where*

$$\Delta_{g_1,g_2}(\mathbb{Z}_\ell) := \left\{ (u_1, u_2) \in \mathrm{GSp}_{2g_1}(\mathbb{Z}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{Z}_\ell) : \mathrm{mult}(u_1) = \mathrm{mult}(u_2) \right\},$$

where $\mathrm{mult} : \mathrm{GSp}_{2g_i}(\mathbb{Z}_\ell) \twoheadrightarrow \mathbb{Z}_\ell^\times$ is the multiplier map.

The above theorem ensures that assumption (2) at the beginning of Section 4 holds for the generic abelian variety case that we focus on. Throughout this paper, for an abelian variety A/K and a prime v of K where A has good reduction, we denote by $A_v(k_v)$ the set of k_v-rational points of the reduction of A at v, where k_v is the residue field of K at v. The main results of this paper are the following.

Theorem 1.4. *Let A/K be a generic abelian variety of dimension g. Let N_x be the set of primes v of K such that $|v| \leq x$, and A has good reduction at v. Then under the GRH, for any $\alpha \in \mathbb{R}$, we have*

$$\lim_{x \to +\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \frac{\omega(a(v) + |v|^g) - \log\log x}{\sqrt{\log\log x}} \leq \alpha \right\} = G(\alpha),$$

and

$$\lim_{x \to +\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \frac{\omega(|A_v(k_v)|) - \log\log x}{\sqrt{\log\log x}} \leq \alpha \right\} = G(\alpha),$$

where $|v| = \mathrm{Norm}_{K/\mathbb{Q}}\, v$, $a(v) = \mathrm{Tr}\, \rho_\ell(\mathrm{Frob}_v) \in \mathbb{Z}$ (for a large ℓ with $v \nmid \ell$).

For a non-isogenous pair of generic varieties, we have the following result.

Theorem 1.5. *Let A_1/K and A_2/K be generic abelian varieties of dimension g_1 and g_2 respectively. For $i = 1, 2$, and primes v of K where A_1 and A_2 have good reduction, let $\rho_{i,\ell} : G_K \to \mathrm{GSp}_{2g_i}(\mathbb{Z}_\ell)$ be the ℓ-adic representation attached to A_i, $a_i(v) = \mathrm{Tr}\,\rho_{i,\ell}(\mathrm{Frob}_v) \in \mathbb{Z}$ (for a large ℓ with $v \nmid \ell$). For any positive number x, let N_x be the set of primes v of K such that $|v| = \mathrm{Norm}_{K/\mathbb{Q}}\, v \le x$, and A_1 and A_2 have good reduction at v. Then under the GRH, for any Borel set $\mathbb{B} \subseteq \mathbb{R}^2$, we have*

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \left(\frac{\omega\left(a_1(v) + |v|^{g_1}\right) - \log\log x}{\sqrt{\log\log x}}, \frac{\omega\left(a_2(v) + |v|^{g_2}\right) - \log\log x}{\sqrt{\log\log x}} \right) \in \mathbb{B} \right\} = \frac{1}{2\pi} \int_{\mathbb{B}} e^{-\frac{1}{2}(x_1^2+x_2^2)}\, dx_1\, dx_2,$$

and

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \left(\frac{\omega\left(|A_{1,v}(k_v)|\right) - \log\log x}{\sqrt{\log\log x}}, \frac{\omega\left(|A_{2,v}(k_v)|\right) - \log\log x}{\sqrt{\log\log x}} \right) \in \mathbb{B} \right\} = \frac{1}{2\pi} \int_{\mathbb{B}} e^{-\frac{1}{2}(x_1^2+x_2^2)}\, dx_1\, dx_2.$$

In particular,

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \omega\left(a_1(v) + |v|^{g_1}\right) < \omega\left(a_2(v) + |v|^{g_2}\right) \right\} = \frac{1}{2},$$

and

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \omega\left(|A_{1,v}(k_v)|\right) < \omega\left(|A_{2,v}(k_v)|\right) \right\} = \frac{1}{2}.$$

When we turn to abelian surfaces, the following analogous distribution results hold.

Theorem 1.6. *Let A/K be an absolutely simple abelian surface. Assume that $\mathrm{End}_{\overline{K}} A = \mathrm{End}_K A$. Let N_x be the set of primes v of K such that $|v| \le x$, and A has good reduction at v. Then under the GRH, for any $\alpha \in \mathbb{R}$, we have*

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \frac{\omega(|A_v(k_v)|) - \log\log x}{\sqrt{\log\log x}} \le \alpha \right\} = G(\alpha).$$

Theorem 1.7. *Let A_1/K and A_2/K be absolutely simple abelian surfaces of the same type I, II or III at the beginning of Section 5. Assume that $\mathrm{End}_{\overline{K}} A_i = \mathrm{End}_K A_i$ for $i = 1, 2$. For any positive number x, let N_x be the set of primes v of K such that $|v| = \mathrm{Norm}_{K/\mathbb{Q}}\, v \le x$, and A_1 and A_2 have good reduction at v. Then under the GRH, for any Borel set $\mathbb{B} \subseteq \mathbb{R}^2$, we have*

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \left(\frac{\omega\left(|A_{1,v}(k_v)|\right) - \log\log x}{\sqrt{\log\log x}}, \frac{\omega\left(|A_{2,v}(k_v)|\right) - \log\log x}{\sqrt{\log\log x}} \right) \in \mathbb{B} \right\} = \frac{1}{2\pi} \int_{\mathbb{B}} e^{-\frac{1}{2}(x_1^2+x_2^2)}\, dx_1\, dx_2.$$

In particular,

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \left\{ v \in N_x : \omega\left(|A_{1,v}(k_v)|\right) < \omega\left(|A_{2,v}(k_v)|\right) \right\} = \frac{1}{2}.$$

The content of this paper is as follows. In Section 2, we review the multivariate Erdős-Kac theorem of El-Baz, Loughran and Sofos. In Sections 3 and 4, we apply an effective Chebotarev density theorem and detailed analysis of Galois images to establish the univariate and bivariate distribution results for generic abelian varieties, respectively. In Section 5, we establish Erdős–Kac-type results for absolutely simple abelian surfaces by treating separately each possible type of their geometric endomorphism ring.

1.1. **Notation and conventions.** In this paper, K denotes a number field. Denote by Ω_K the set of primes of K. For $v \in \Omega_K$, denote by Frob_v the arithmetic Frobenius element at v, and denote $\mathrm{Norm}_{K/\mathbb{Q}}\, v$ by $|v|$. Denote by G_K the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$.

For an integer $g \geq 1$, the general symplectic group over a commutative ring R is defined as

$$\mathrm{GSp}_{2g}(R) := \left\{ M \in \mathrm{GL}_{2g}(R) \mid M^T J M = \mu(M) J \text{ for some } \mu(M) \in R^\times \right\},$$

where J is the standard skew-symmetric matrix $\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. We have the multiplier map

$$\mathrm{mult} : \mathrm{GSp}_{2g}(R) \longrightarrow R^\times, \quad M \mapsto \mu(M).$$

It is a group homomorphism, and its kernel is the symplectic group $\mathrm{Sp}_{2g}(R)$.

For a nonzero integer n, denote by $\omega(n)$ the number of distinct prime divisors of n. For any positive number N, denote by Λ_N the set of prime numbers greater than N.

Let f and g be two complex-valued functions on a set D. If $g(x)$ is positive and there exists a constant C such that $|f(x)| \leq Cg(x)$ for all $x \in D$, then we write $f(x) = O(g(x))$.

For a finite set X, denote by $|X|$ or $\sharp X$ the cardinality of X.

2. A multivariate version of the Erdős–Kac theorem

We review the version of the multivariate Erdős–Kac theorem in [6] that we need for the study of systems of Galois representations. With the settings of [6, Section 2.1], let Ω be a set of prime ideals of the number field K with $|\Omega_K - \Omega| < \infty$. For any positive number B, define

$$N(B) := \{a \in \Omega : \ \mathrm{Norm}_{K/\mathbb{Q}}(a) \leq B\},$$

and for a subset S of Ω, define

$$P_B[S] := \frac{\sharp\{a \in S : \ \mathrm{Norm}_{K/\mathbb{Q}}(a) \leq B\}}{|N(B)|}.$$

The generalized Dirichlet density theorem shows that

$$\lim_{B \to +\infty} \frac{|N(B)| \cdot \log B}{B} = 1.$$

Let $m : \Omega \to \mathbb{N}^n$ $(a \in \Omega \mapsto (m_1(a), \ \ldots, \ m_n(a)))$ be a map on Ω. Under certain technical conditions, the multivariate Erdős–Kac theorem describes the distribution of the vector $(\omega(m_1(a)), \ \ldots, \ \omega(m_n(a))) \in \mathbb{N}^n$.

More precisely, we assume that the numbers $m_i(a)$ for $1 \leq i \leq n$ and $a \in \Omega$ satisfy the following conditions:

C1: There exists a map $\mathcal{F} : \mathbb{R}_{\geq 1} \to \mathbb{R}$, such that

$$\lim_{B \to +\infty} \frac{1}{|N(B)|} \sharp\{a \in N(B) : \ \max_{1 \leq i \leq n} m_i(a) \leq \mathcal{F}(B)\} = 1.$$

C2: There exists $P \in \mathbb{R}$ such that for all $\mathbf{d} = (d_1,\ \ldots,\ d_n) \in \mathbb{N}^n$ with prime divisors of d_i larger than P, the following limit exists

$$\lim_{B\to+\infty} \frac{\sharp\{a \in N(B) :\ d_i | m_i(a) \text{ for all } 1 \le i \le n\}}{|N(B)|} =: g(\mathbf{d}).$$

C3: The map g is multiplicative, i.e., for $\mathbf{a},\ \mathbf{b} \in \mathbb{N}^n$, if $\gcd(a_1 \cdots a_n,\ b_1 \cdots b_n) = 1$, then

$$g(a_1b_1,\ \ldots,\ a_nb_n) = g(\mathbf{a})g(\mathbf{b}).$$

We extend g to $\mathbb{N}^n$ by setting it equal to 0 for $\mathbf{d}$ such that $d_1 \cdots d_n$ has a prime factor $p \le P$. For each $1 \le i,\ j \le n$, let

$$g_i(d) := g(1, \ldots, 1, \underset{\uparrow}{d}, 1, \ldots, 1) \text{ and } g_{i,j}(d) := g(1, \ldots, 1, \underset{\uparrow}{d}, 1, \ldots, 1, \underset{\uparrow}{d}, 1, \ldots, 1).$$
$$\qquad\qquad\qquad\quad i \qquad\qquad\qquad\qquad\qquad\qquad\quad i \qquad\qquad\quad j$$

Note that with this definition, $g_{i,i} = g_i$. Assume that the maps g_i and $g_{i,j}$ satisfy the following conditions.

C4: For every $1 \le i,\ j \le n$, the following limit exists

$$\lim_{T\to+\infty} \frac{\sum_{p\le T} g_{i,j}(p)}{(\sum_{p\le T} g_i(p))^{1/2}(\sum_{p\le T} g_j(p))^{1/2}} =: \sigma_{ij}.$$

C5: For every $1 \le i \le n$,

$$\sum_{p>T} g_i^2(p) = O\left(\frac{1}{\log T}\right) \text{ and } \sum_{p\le T} g_i(p) = c_i \log\log T + c_i^{'} + O\left(\frac{1}{\log T}\right) \tag{2.1}$$

for some $c_i > 0, c_i^{'} \in \mathbb{R}$.

For each $\mathbf{d} \in \mathbb{N}^n$ and $B \ge 1$, define

$$\mathcal{R}(\mathbf{d}; B) = \sharp\{a \in N(B) :\ d_i | m_i(a) \text{ for all } 1 \le i \le n\} - g(\mathbf{d}) \cdot |N(B)|.$$

Assume that the following conditions are satisfied.

C6: Let $C = \mathcal{F}(B)^{\epsilon(B)}$, $\epsilon(B) = \log\log\log \mathcal{F}(B)/\sqrt{\log\log \mathcal{F}(B)}$. Then for all $\gamma > 0$,

$$\sum\nolimits^{'} |\mathcal{R}(d_1, \ldots, d_n; B)| = O\left(|N(B)| \cdot (\log\log \mathcal{F}(B))^{-\gamma}\right), \tag{2.2}$$

where $\sum^{'}$ runs through all n-tuples of square-free integers $(d_1, \ldots, d_n)$ which satisfy that the prime divisors of d_i are greater than P and $d_i < C$ for every i.

Define the random vector $K : \Omega \to \mathbb{R}^n$ via

$$K_a := \left(\frac{\omega\left(m_1(a)\right) - c_1 \log\log \mathcal{F}(B)}{\sqrt{c_1 \log\log \mathcal{F}(B)}}, \ldots, \frac{\omega\left(m_n(a)\right) - c_n \log\log \mathcal{F}(B)}{\sqrt{c_n \log\log \mathcal{F}(B)}}\right).$$

As a special case of [6, Theorem 2.1], we have the following result.

Theorem 2.1. *If the family of sequences $\{m_i(a)\}_{1\le i\le n, a\in\Omega}$ satisfies conditions **C1-C6**, then the random vectors*

$$(\Omega, P_B) \to \mathbb{R}^n :\ a \mapsto K_a,$$

converge in distribution as $B \to +\infty$ to the central multivariate normal distribution with covariance matrix $\Sigma = (\sigma_{ij})$.

Remark 2.2. The conditions **C1-C6** correspond to equations (2.7), (2.3), (2.4), (2.11), (2.5), (2.9) in [6, Section 2.1] respectively. The readers may find more information on the motivation and the necessity of these restrictions in [6, Section 2.1].

Remark 2.3. For our application, the number $m_i(a)$ is a polynomial of the trace and the determinant of the Frob_a from a geometric Galois representation. In particular, $m_i(a) = O(\mathrm{Norm}_{K/\mathbb{Q}}(a)^c)$ for some positive number c. In this case, one may take $\mathcal{F}(B) = B$.

Moreover, define $e(d_1,\ \ldots,\ d_n;\ B)$ by

$$e(d_1,\ \ldots,\ d_n;\ B) = \frac{\mathcal{R}(d_1,\ \ldots,\ d_n;\ B)}{|N(B)|}.$$

By [28, Remark 2], condition **C6** holds if there exist constants $k,\ \delta > 0$ such that

$$e(d_1,\ \ldots,\ d_n;\ x) = O\left((d_1 \cdots d_n)^k x^{-\delta}\right). \tag{2.3}$$

Corollary 2.4. *If the family of sequences $\{m_i(a)\}_{1\le i\le n, a\in\Omega}$ satisfies conditions **C1-C6**, $\sigma_{ij} = 0$ for $i \neq j$, and $m_i(a) = O(\mathrm{Norm}_{K/\mathbb{Q}}(a)^c)$ for some $c \in \mathbb{R}_{\ge 0}$. For any Borel set $\mathbb{B} \subseteq \mathbb{R}^n$,*

$$\lim_{B\to+\infty} \frac{1}{|N(B)|} \sharp\{a \in N(B) : (\omega_1, \ldots, \omega_n) \in \mathbb{B}\} = \frac{1}{(2\pi)^{n/2}} \int_{\mathbb{B}} e^{-\frac{1}{2}(x_1^2+\cdots+x_n^2)}\, \mathrm{d}\, x_1 \cdots \mathrm{d}\, x_n,$$

where for $1 \le i \le n$, $\omega_i = \frac{\omega(m_i(a)) - c_i \log\log B}{\sqrt{c_i \log\log B}}$. In particular, if $c_1 = \cdots = c_n$ and $\mathbb{B} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 < \cdots < x_n\}$, then

$$\lim_{B\to+\infty} \frac{1}{|N(B)|} \sharp\{a \in N(B) : \omega(m_1(a)) < \cdots < \omega(m_n(a))\} = \frac{1}{n!}.$$

3. The univariate distribution result

We start with a system of Galois representations with GSp-type image. Let $\{\rho_\ell : G_K \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)\}_{\ell\in\Lambda_N}$ be a system of rational Galois representations. Assume that these representations satisfy the following conditions.

(1) For all $\ell \in \Lambda_N$, the composition map $\mathrm{mult} \circ \rho_\ell$ is equal to the ℓ-adic cyclotomic character.
(2) For all $\ell \in \Lambda_N$, the representation ρ_ℓ is surjective. The system $\{\rho_\ell\}_{\ell\in\Lambda_N}$ is independent (cf. [4, Definition 1.6], [27]).
(3) The system is strictly compatible (cf. [23, I-11]), i.e., there exists a finite set R of primes of K such that each representation ρ_ℓ is unramified outside $R \cup \{v :\ v|\ell\}$, and for each $v \notin R$ and $v \nmid \ell$, $\det(tI_{2g} - \rho_\ell(\mathrm{Frob}_v))$ is in $\mathbb{Z}[t]$ and is independent of ℓ. In particular, $\mathrm{Tr}\,\rho_\ell(\mathrm{Frob}_v)$ is in $\mathbb{Z}$ and is independent of the choice of ℓ. Denote this number by $a(v)$.
(4) The coefficients of $\det(tI_{2g} - \rho_\ell(\mathrm{Frob}_v))$ have polynomial size. In particular, $a(v) = O((\mathrm{Norm}_{K/\mathbb{Q}}\, v)^c)$ for some positive number c.

Denote the mod ℓ reduction of ρ_ℓ by $\overline{\rho}_\ell$. By assumption (2), for each $\ell \in \Lambda_N$, the image of $\overline{\rho}_\ell$ is $G(\ell) := \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, and for a square-free integer d whose prime divisors are in Λ_N, the representation $\overline{\rho}_d := \prod_{\ell|d} \overline{\rho}_\ell$ has image equal to $G(d) := \prod_{\ell|d} \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

For each $\ell \in \Lambda_N$, let $F_\ell : \mathbb{Z}_\ell \times \mathbb{Z}_\ell \to \mathbb{Z}_\ell$ and $\overline{F}_\ell : \mathbb{F}_\ell \times \mathbb{F}_\ell \to \mathbb{F}_\ell$ be two maps such that for any $z \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, $F_\ell(z) \pmod{\ell} = \overline{F}_\ell(z \pmod{\ell})$. For a square-free integer d whose prime divisors are in Λ_N, define

$$C(d) = \left\{(u_\ell)_{\ell|d} \in G(d) : \overline{F}_\ell(\operatorname{Tr} u_\ell, \det u_\ell) = 0 \text{ for all } \ell \mid d\right\},$$

and

$$C'(d) = \left\{(u_\ell)_{\ell|d} \in G(d) : \det(I - u_\ell) = 0 \text{ for all } \ell \mid d\right\}.$$

Each of them is a subset of $G(d)$ that is stable under conjugation.

To gain the arithmetic information from the Galois representations, we need the effective Chebotarev's density theorem. The following version of Chebotarev's density theorem is [25, Théorème 4]. This is the part where the General Riemann Hypothesis appears and we only use this theorem in the verification of condition **C6**.

Theorem 3.1. *Let L/K be a finite Galois extension of number fields with Galois group G. Let C be a subset of G which is stable under conjugation, and let Frob_v be the Frobenius element at an unramified prime v of K. Denote by $\pi_C(x)$ the cardinality of the set of primes v unramified in L for which $\operatorname{Frob}_v \in C$ and $\operatorname{Norm}_{K/\mathbb{Q}} v \leq x$. Assuming that the Dedekind zeta function $\zeta_L(s)$ satisfies the GRH, then*

$$\pi_C(x) = \frac{|C|}{|G|}\pi_K(x) + O\left(\frac{|C|}{|G|}x^{\frac{1}{2}}\left(\log d_L + n_L \log x\right)\right),$$

where d_L and n_L are the discriminant and the degree of the extension $L/\mathbb{Q}$, respectively.

Applying Theorem 3.1 to the fixed field L of $\overline{K}$ by the group $\operatorname{Ker}\overline{\rho}_d$, we get

$$\begin{aligned}&\frac{1}{\pi_K(x)}\sharp\left\{v : \ |v| \leq x, \ F_\ell(a(v), |v|^g) \equiv 0 \pmod{\ell} \text{ for all } \ell|d\right\}\\ =&\frac{|C(d)|}{|G(d)|} + O\left(\frac{|C(d)|}{|G(d)|}x^{-\frac{1}{2}}\log x\left(\log d_L + n_L \log x\right)\right),\end{aligned}$$

and

$$\begin{aligned}&\frac{1}{\pi_K(x)}\sharp\left\{v : \ |v| \leq x, \ \det(I - \rho_\ell(\operatorname{Frob}_v)) \equiv 0 \pmod{\ell} \text{ for all } \ell|d\right\}\\ =&\frac{|C'(d)|}{|G(d)|} + O\left(\frac{|C'(d)|}{|G(d)|}x^{-\frac{1}{2}}\log x\left(\log d_L + n_L \log x\right)\right),\end{aligned}$$

Define

$$g(d) := |C(d)|/|G(d)|.$$

and

$$g'(d) := |C'(d)|/|G(d)|.$$

Then g and g' are clearly multiplicative.

For representations mentioned at the beginning of this section, we verify the conditions in Theorem 2.1 with $n = 1$ and $m_1(v) = a(v) + r(|v|^g)$ for some polynomial $r(t) \in \mathbb{Z}[t]$ and with $n = 1$ and $m_1(v) = \det(I_{2g} - \rho_\ell(\operatorname{Frob}_v))$, respectively. Conditions **C1-C3** hold by the assumptions on the Galois representations and the discussion above. Condition **C4** becomes vacuous in this case.

From the order of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ [20, Theorem 3.1.2] we have

$$|G(\ell)| = \left|\mathrm{GSp}_{2g}(\mathbb{F}_\ell)\right| = (\ell-1)\ell^{g^2}\prod_{i=1}^{g}(\ell^{2i}-1) = \ell^{2g^2+g+1} + O(\ell^{2g^2+g}). \tag{3.1}$$

Let $L := L_d$ be the fixed field of $\overline{K}$ by the group $\operatorname{Ker}\overline{\rho}_d$. From equation (3.1), the degree of the extension L/K is $O(d^{2g^2+2g+1})$. By [25, Proposition 6], we have

$$\log d_L \le (n_L - 1)\sum_{p\in P(L)} \log p + n_L|P(L)|\log n_L, \tag{3.2}$$

where $P(L)$ is the set of prime numbers that are ramified in L. As $L = \overline{L}^{\operatorname{Ker}\overline{\rho}_d}$, it is unramified outside $\{p : \ p \text{ is divisible by some primes in R}\} \cup \{p : \ p|d\}$. In particular, $|P(L)| \le |R| + \omega(d)$ and

$$\prod_{p\in P(L)} p \le rd,$$

where r is the product of prime numbers in $\{p : \ p \text{ is divisible by some primes in R}\}$. Therefore, by equation (3.2)

$$\begin{aligned}\log d_L + n_L\log x &\le n_L\log(rd) + n_L(|R|+\omega(d))\log n_L + n_L\log x\\ &= n_L(\log(rd) + (|R|+\omega(d))\log n_L + \log x).\end{aligned}$$

Hence for $c = 2g^2+g+1$ and some $\epsilon > 0$,

$$e\,(d;x) = O\left(d^{c+1}x^{\epsilon-\frac{1}{2}}\right).$$

By Remark 2.3, condition **C6** holds under the GRH.

For the verification of condition **C5**, we need the following lemma, which is a corollary of [13, Theorem 1].

Lemma 3.2. *Let $\mathbb{F}_\ell$ be a finite field with ℓ elements and g be a positive integer. For given $a \in \mathbb{F}_\ell$ and $b \in \mathbb{F}_\ell^\times$, let*

$$N(a,b) := \sharp\left\{u \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) : \operatorname{Tr} u = a, \det u = b\right\}.$$

Then

$$N(a,b) = \begin{cases} \gcd(g,\ell-1)\ell^{2g^2+g-1} + O(\ell^{2g^2+g-2}) & \text{if } b \in (\mathbb{F}_\ell^\times)^g,\\ 0 & \text{otherwise.}\end{cases}$$

Lemma 3.3. *Let $F_\ell(x,y) = x + r(y)$ and $\overline{F}_\ell(x,y) = x + \overline{r}(y)$, where $r(t) \in \mathbb{Z}[t]$. Then for $\ell \in \Lambda_N$,*

$$|C(\ell)| = \sharp\left\{u \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) : \overline{F}_\ell(\operatorname{Tr} u, \det u) = 0\right\} = \ell^{2g^2+g} + O(\ell^{2g^2+g-1}).$$

Proof. Define

$$M(\ell) := \left\{(a,b) \in \mathbb{F}_\ell \times (\mathbb{F}_\ell^\times)^g : a + \overline{r}(b) = 0\right\}.$$

Clearly

$$|M(\ell)| = |(\mathbb{F}_\ell^\times)^g| = \frac{\ell-1}{\gcd(g,\ell-1)}.$$

Therefore

$$\begin{aligned}|C(\ell)| &= \sum_{(a,b)\in M(\ell)} \sharp\left\{u \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) : \mathrm{Tr}\, u = a, \det u = b\right\} \\ &= \frac{\ell-1}{\gcd(g,\ell-1)}\left(\gcd(g,\ell-1)\ell^{2g^2+g-1} + O(\ell^{2g^2+g-2})\right) \\ &= \ell^{2g^2+g} + O(\ell^{2g^2+g-1}).\end{aligned}$$

The lemma follows. □

To estimate the size of $C'(\ell)$, we will use the following lemma, which follows from [3, Theorem 6] (see also [2, Proposition 4.10]). We state it here with notation adapted to our setting.

Lemma 3.4. *For $m \in \mathbb{F}_\ell^\times$, let*

$$G^{(m)}(\ell) := \{u \in G(\ell) : \mathrm{mult}(u) = m\}$$

and

$$C'^{(m)}(\ell) := C'(\ell) \cap G^{(m)}(\ell).$$

Then

$$\frac{|C'^{(m)}(\ell)|}{|G^{(m)}(\ell)|} = \begin{cases} -\sum_{r=1}^{g} \ell^r \prod_{j=1}^{r}\left(1-\ell^{2j}\right)^{-1} & \text{if } \ell \mid m-1, \\ -\sum_{r=1}^{g} \prod_{j=1}^{r}\left(1-\ell^{j}\right)^{-1} & \text{otherwise.}\end{cases}$$

We then obtain an estimate for the size of $C'(\ell)$.

Lemma 3.5. *For $\ell \in \Lambda_N$,*

$$|C'(\ell)| = \sharp\left\{u \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) : \det(I_{2g}-u) = 0\right\} = \ell^{2g^2+g} + O(\ell^{2g^2+g-1}).$$

Proof. By direct computation,

$$\begin{aligned}|C'(\ell)| &= \sum_{m\in\mathbb{F}_\ell^\times} \frac{|C'^{(m)}(\ell)|}{|G^{(m)}(\ell)|}|G^{(m)}(\ell)| \\ &= \frac{|G(\ell)|}{\ell-1}\cdot\left(-\sum_{r=1}^{g}\ell^r\prod_{j=1}^{r}\left(1-\ell^{2j}\right)^{-1} + (\ell-2)\left(-\sum_{r=1}^{g}\prod_{j=1}^{r}\left(1-\ell^{j}\right)^{-1}\right)\right) \\ &= \frac{1}{\ell-1}\left(\ell^{2g^2+g+1}+O(\ell^{2g^2+g})\right)\left(\ell^{-1}+O(\ell^{-2})+(\ell-2)(\ell^{-1}+O(\ell^{-2}))\right) \\ &= \ell^{2g^2+g} + O(\ell^{2g^2+g-1}).\end{aligned}$$

The lemma follows. □

Combining the above discussions, we obtain the following result, which is a specific case of Corollary 2.4.

Theorem 3.6. *Let $\{\rho_\ell\}_{\ell\in\Lambda_N}$ be a system of Galois representations satisfying the conditions (1)-(4) at the beginning of this section. Let R be the finite set of ramified primes, $\Omega = \Omega_K - R$, and $N(B) = \{v \in \Omega : |v| \le B\}$. Let $G(\alpha) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha} e^{-x^2/2}dx$.*

(1) *Let $r(t) \in \mathbb{Z}[t]$. If*

$$\sharp\{v \in \Omega : \ |v| \leq x, \ a(v) + r(|v|^g) = 0\} = o(x/\log x), \tag{3.3}$$

then under the GRH, for any $\alpha \in \mathbb{R}$, we have

$$\lim_{x\to+\infty} \frac{1}{|N(B)|} \sharp \left\{ v \in N(B) : \frac{\omega(a(v) + r(|v|^g)) - \log\log x}{\sqrt{\log\log x}} \leq \alpha \right\} = G(\alpha).$$

(2) *If*

$$\sharp\{v \in \Omega : \ |v| \leq x, \ \det(I_{2g} - \rho_\ell(\mathrm{Frob}_v)) = 0\} = o(x/\log x), \tag{3.4}$$

then under the GRH, for any $\alpha \in \mathbb{R}$, we have

$$\lim_{x\to+\infty} \frac{1}{|N(B)|} \sharp \left\{ v \in N(B) : \frac{\omega(\det(I_{2g} - \rho_\ell(\mathrm{Frob}_v))) - \log\log x}{\sqrt{\log\log x}} \leq \alpha \right\} = G(\alpha).$$

Proof. From equation (3.1), Lemma 3.3 and Lemma 3.5 we find that $g(\ell)$ and $g'(\ell)$ are of the form $1/\ell + O(1/\ell^2)$, thus condition **C5** holds and the theorem follows. □

Theorem 1.4 is then a special case of Theorem 3.6. For a generic abelian variety A, there exists N such that the system of ℓ-adic representations with $\ell > N$ attached to A satisfies the conditions (1)-(4) at the beginning of this section. For the first identity, the Weil Conjecture (proved by Deligne [5]) shows that $\alpha_i(v) = O(|v|^{1/2})$, therefore for almost all v, $a_i(v) + |v|^g \in \mathbb{Z}_{>0}$. Taking $r(t) = t$, equation (3.3) holds and the first identity of Theorem 1.4 is then a special case of Theorem 3.6. For the second identity of Theorem 1.4, note that

$$|A_v(k_v)| = \det(I - \rho_\ell(\mathrm{Frob}_v)) > 0,$$

hence equation (3.4) holds and the second identity follows from Theorem 3.6.

4. The bivariate distribution result

In this section, we consider two independent systems of Galois representations and show that, for both kinds of arithmetic invariants, their joint distribution follows a bivariate standard normal distribution.

Let $\{\rho_{1,\ell} : G_K \to \mathrm{GSp}_{2g_1}(\mathbb{Z}_\ell)\}_{\ell\in\Lambda_N}$ and $\{\rho_{2,\ell} : G_K \to \mathrm{GSp}_{2g_2}(\mathbb{Z}_\ell)\}_{\ell\in\Lambda_N}$ be two systems of Galois representations. Assume that they satisfy the following conditions.

(1) Each of $\{\rho_{i,\ell}\}_{\ell\in\Lambda_N}$ satisfies the conditions (1)-(4) at the beginning of Section 3. Denote $a_i(v) = \mathrm{Tr}\,\rho_{i,\ell}(\mathrm{Frob}_v)$ for $i = 1, 2$.

(2) For all $\ell \in \Lambda_N$, the representations $\rho_{1,\ell}$ and $\rho_{2,\ell}$ are "independent up to multiplier", i.e., the product representation $\rho_{1,\ell} \times \rho_{2,\ell}$ has image equal to

$$\Delta_{g_1,g_2}(\mathbb{Z}_\ell) = \left\{(u_1, u_2) \in \mathrm{GSp}_{2g_1}(\mathbb{Z}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{Z}_\ell) : \mathrm{mult}(u_1) = \mathrm{mult}(u_2)\right\}.$$

The system $\{\rho_{1,\ell} \times \rho_{2,\ell}\}_{\ell\in\Lambda_N}$ is independent (cf. [4, Definition 1.6], [27]).

Denote the mod ℓ reduction of $\rho_{i,\ell}$ by $\overline{\rho}_{i,\ell}$ for $i = 1, 2$. Then for each $\ell \in \Lambda_N$, the image of $\overline{\rho}_{1,\ell}$ is $G(\ell, 1) := \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell)$ and the image of $\overline{\rho}_{2,\ell}$ is $G(1, \ell) := \mathrm{GSp}_{2g_2}(\mathbb{F}_\ell)$.

For primes ℓ and ℓ' in Λ_N, consider the direct sum representation

$$\overline{\rho}_{\ell,\ell'} := \overline{\rho}_{1,\ell} \oplus \overline{\rho}_{2,\ell'} : G_K \to \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{F}_{\ell'}).$$

If $\ell = \ell'$, the independence assumption (2) implies that the image of $\overline{\rho}_{\ell,\ell'}$ is

$$G(\ell,\ell) := \left\{(u_1,u_2) \in \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{F}_\ell) : \mathrm{mult}(u_1) = \mathrm{mult}(u_2)\right\}.$$

If $\ell \neq \ell'$, the image of $\overline{\rho}_{\ell,\ell'}$ is

$$G(\ell,\ell') := \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{F}_{\ell'}).$$

For two square-free integers $d_1,\ d_2$ whose prime divisors are in Λ_N, if their prime factorizations are $d_1 = p_1 \cdots p_r$ and $d_2 = q_1 \cdots q_s$, define representation

$$\overline{\rho}_{d_1,d_2} := \overline{\rho}_{1,p_1} \oplus \cdots \oplus \overline{\rho}_{1,p_r} \oplus \overline{\rho}_{2,q_1} \oplus \cdots \oplus \overline{\rho}_{2,q_s}.$$

We denote

$$H(d_1,d_2) := \prod_{\ell \mid d_1} \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \times \prod_{\ell \mid d_2} \mathrm{GSp}_{2g_2}(\mathbb{F}_\ell).$$

Without loss of generality, we write $d_1 = LP, d_2 = LQ$, $\gcd(P,Q) = 1$. Then the image of $\overline{\rho}_{d_1,d_2}$ is

$$G(d_1,d_2) := \prod_{\ell \mid L} G(\ell,\ell) \times \prod_{\ell \mid P} G(\ell,1) \times \prod_{\ell \mid Q} G(1,\ell) \subset H(d_1,d_2).$$

For each $\ell \in \Lambda_N$, let $F_{i,\ell} : \mathbb{Z}_\ell \times \mathbb{Z}_\ell \to \mathbb{Z}_\ell$ and $\overline{F}_{i,\ell} : \mathbb{F}_\ell \times \mathbb{F}_\ell \to \mathbb{F}_\ell$ be two maps such that for any $z \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, $F_{i,\ell}(z) \pmod{\ell} = \overline{F}_{i,\ell}(z \pmod{\ell})$.

For two square-free integers $d_1,\ d_2$ whose prime divisors are in Λ_N, define

$$Z(d_1,d_2) := \left\{((u_\ell)_{\ell \mid d_1}, (v_\ell)_{\ell \mid d_2}) \in H(d_1,d_2) : \begin{array}{l} \overline{F}_{1,\ell}(\mathrm{Tr}\, u_\ell, \det u_\ell) = 0 \text{ for all } \ell \mid d_1 \\ \overline{F}_{2,\ell}(\mathrm{Tr}\, v_\ell, \det v_\ell) = 0 \text{ for all } \ell \mid d_2 \end{array}\right\}$$

and

$$Z'(d_1,d_2) := \left\{((u_\ell)_{\ell \mid d_1}, (v_\ell)_{\ell \mid d_2}) \in H(d_1,d_2) : \begin{array}{l} \det(I - u_\ell) = 0 \text{ for all } \ell \mid d_1 \\ \det(I - v_\ell) = 0 \text{ for all } \ell \mid d_2 \end{array}\right\}.$$

Let $C(d_1,d_2) := Z(d_1,d_2) \cap G(d_1,d_2)$ and $C'(d_1,d_2) := Z'(d_1,d_2) \cap G(d_1,d_2)$. Each of them is a subset of $G(d_1,d_2)$ that is stable under conjugation.

Applying Theorem 3.1 to the fixed field L of $\overline{K}$ by the group $\mathrm{Ker}\,\overline{\rho}_{d_1,d_2}$, we have

$$\begin{aligned} &\frac{1}{\pi_K(x)} \sharp \{v :\ |v| \le x,\ F_{i,\ell}(a_i(v), |v|^{g_i}) \equiv 0 \pmod{\ell} \text{ for all } \ell | d_i,\ i = 1,\ 2\} \\ =&\frac{|C(d_1,d_2)|}{|G(d_1,d_2)|} + O\left(\frac{|C(d_1,d_2)|}{|G(d_1,d_2)|} x^{-\frac{1}{2}} \log x \left(\log d_L + n_L \log x\right)\right). \end{aligned}$$

and

$$\begin{aligned} &\frac{1}{\pi_K(x)} \sharp \{v :\ |v| \le x,\ \det(I - \rho_{i,\ell}(\mathrm{Frob}_v)) \equiv 0 \pmod{\ell} \text{ for all } \ell | d_i,\ i = 1,\ 2\} \\ =&\frac{|C'(d_1,d_2)|}{|G(d_1,d_2)|} + O\left(\frac{|C'(d_1,d_2)|}{|G(d_1,d_2)|} x^{-\frac{1}{2}} \log x \left(\log d_L + n_L \log x\right)\right). \end{aligned}$$

Define

$$g(d_1,d_2) := |C(d_1,d_2)|/|G(d_1,d_2)|$$

and

$$g'(d_1,d_2) := |C'(d_1,d_2)|/|G(d_1,d_2)|.$$

Then g and g' are clearly multiplicative.

We verify the conditions in Theorem 2.1 for representations mentioned at the beginning of this section with $n = 2$ and $m_i(v) = a_i(v) + r_i(|v|^{g_i})$ for $r_i(t) \in \mathbb{Z}[t]$ and with $n = 2$ and $m_i = \det(I_{2g_i} - \rho_{i,\ell}(\mathrm{Frob}_v))$, respectively. For each type of $m_i(v)$, conditions **C1, C2, C3** and **C5** are the same as that in the $n = 1$ case. From the exact sequence

$$1 \to \mathrm{Sp}_{2g_1}(\mathbb{F}_\ell) \times \mathrm{Sp}_{2g_2}(\mathbb{F}_\ell) \to G(\ell,\ell) \xrightarrow{\text{mult} \times \text{mult}} \mathbb{F}_\ell^\times \to 1$$

we find that

$$|G(\ell,\ell)| = (\ell-1)\left|\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)\right|\left|\mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)\right| = \ell^{2g_1^2+2g_2^2+g_1+g_2+1} + O(\ell^{2g_1^2+2g_2^2+g_1+g_2}). \tag{4.1}$$

Applying an argument similar to that in Section 3, it is easy to verify that for $c = 2\max\{g_1,g_2\}^2 + \max\{g_1,g_2\} + 1$ and for some $\epsilon > 0$,

$$e(d_1,d_2;x) = O\left((d_1d_2)^{c+1}x^{\epsilon-\frac{1}{2}}\right).$$

Hence condition **C6** holds under the GRH.

We then verify condition **C4**. For the first type of invariant, we have the following lemma.

Lemma 4.1. *Let $r_1(t)$ and $r_2(t)$ be any polynomials with integer coefficients. For $i = 1, 2$ let $F_{i,\ell}(x,y) = x + r_i(y)$ and $\overline{F}_{i,\ell}(x,y) = x + \overline{r}_i(y)$. Then for $\ell \in \Lambda_N$,*

$$|C(\ell,\ell)| = O\left(\ell^{2g_1^2+2g_2^2+g_1+g_2-1}\right).$$

Proof. Define

$$M(\ell,\ell) := \left\{(a_1,b_1,a_2,b_2) \in \mathbb{F}_\ell^4 : a_i + \overline{r_i}(b_i) = 0, \text{and } \exists v \in \mathbb{F}_\ell^\times, b_i = v^{g_i}, i = 1,2\right\}.$$

Let $D = \{(v^{g_1}, v^{g_2}) : v \in \mathbb{F}_\ell^\times\}$. We have exact sequence

$$1 \to \langle \gamma^{\frac{\ell-1}{d}} \rangle \longrightarrow \mathbb{F}_\ell^\times \xrightarrow{\varphi} D \to 1,$$

where γ is a generator of $\mathbb{F}_\ell^\times$, $d = \gcd(\ell-1, g_1, g_2)$ and φ is defined by $v \mapsto (v^{g_1}, v^{g_2})$. Thus $|M(\ell,\ell)| = |D| = \frac{\ell-1}{d}$.

Then

$$\begin{aligned}
|C(\ell,\ell)| &= \sharp\left\{\begin{array}{l}(u_1,u_2) \in \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{F}_\ell) : \\ \mathrm{mult}(u_1) = \mathrm{mult}(u_2),\ \mathrm{Tr}\, u_i + r_i(\det u_i) = 0 \text{ for } i = 1,\ 2\end{array}\right\} \\
&\le \sharp\left\{\begin{array}{l}(u_1,u_2) \in \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \times \mathrm{GSp}_{2g_2}(\mathbb{F}_\ell) : \\ \exists v \in \mathbb{F}_\ell^\times, \det u_i = v^{g_i},\ \mathrm{Tr}\, u_i + r_i(\det u_i) = 0 \text{ for } i = 1,\ 2\end{array}\right\} \\
&= \sum_{(a_1,b_1,a_2,b_2) \in M(\ell,\ell)} \prod_{i=1,2} \sharp\left\{u \in \mathrm{GSp}_{2g_i}(\mathbb{F}_\ell) : \mathrm{Tr}\, u = a_i, \det u = b_i\right\} \\
&= \frac{\ell-1}{d} \prod_{i=1,2} \left(\gcd(\ell-1,g_i)\ell^{2g_i^2+g_i-1} + O(\ell^{2g_i^2+g_i-2})\right) \\
&= O\left(\ell^{2g_1^2+2g_2^2+g_1+g_2-1}\right).
\end{aligned}$$

The lemma follows. □

Applying Lemma 3.4, we have the following estimate.

Lemma 4.2.

$$C'(\ell,\ell)=\ell^{2g_1^2+2g_2^2+g_1+g_2-1}+O\left(\ell^{2g_1^2+2g_2^2+g_1+g_2-2}\right).$$

Proof. By direct computation,

$$\begin{aligned}
|C'(\ell,\ell)| &= \sharp\left\{\begin{array}{l}(u_1,u_2)\in \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell)\times \mathrm{GSp}_{2g_2}(\mathbb{F}_\ell):\\ \mathrm{mult}(u_1)=\mathrm{mult}(u_2),\ \det(I-u_i)=0 \text{ for } i=1,\ 2\end{array}\right\}\\
&=\sum_{m\in\mathbb{F}_\ell^\times}|C'^{(m)}(\ell,1)||C'^{(m)}(1,\ell)|\\
&=|G^{(m)}(\ell,1)||G^{(m)}(1,\ell)|\sum_{m\in\mathbb{F}_\ell^\times}\frac{|C'^{(m)}(\ell,1)|}{|G^{(m)}(\ell,1)|}\frac{|C'^{(m)}(1,\ell)|}{|G^{(m)}(1,\ell)|}\\
&=\frac{|G(\ell,1)|}{\ell-1}\frac{|G(1,\ell)|}{\ell-1}\left(\prod_{i=1,2}\left(-\sum_{r=1}^{g_i}\ell^r\prod_{j=1}^{r}\left(1-\ell^{2j}\right)^{-1}\right)\right.\\
&\qquad\left.+(\ell-2)\prod_{i=1,2}\left(-\sum_{r=1}^{g_i}\prod_{j=1}^{r}\left(1-\ell^{j}\right)^{-1}\right)\right)\\
&=\ell^{2g_1^2+2g_2^2+g_1+g_2-1}+O\left(\ell^{2g_1^2+2g_2^2+g_1+g_2-2}\right).
\end{aligned}$$

The lemma follows. □

From equation (4.1), Lemmas 4.1 and 4.2, we have $g(\ell,\ell)=O(1/\ell^2)$ and $g'(\ell,\ell)=1/\ell^2+O(1/\ell^3)$. Hence $\sum_{\ell\le x}g(\ell,\ell)<\infty$ and $\sum_{\ell\le x}g'(\ell,\ell)<\infty$, then condition **C4** holds with $\sigma_{12}=\sigma_{21}=0$. We obtain the following result, which is also a specific case of Corollary 2.4.

Theorem 4.3. *Let $\{\rho_{1,\ell}\}_{\ell\in\Lambda_N}$ and $\{\rho_{2,\ell}\}_{\ell\in\Lambda_N}$ be two systems of Galois representations. Assume that these representations satisfy the conditions (1), (2) at the beginning of this section. Let R be the finite set of ramified primes, $\Omega=\Omega_K-R$, $N(B)=\{v\in\Omega:|v|\le B\}$.*

(1) *Let $r_i(t)\in\mathbb{Z}[t]$. If for each $i=1,\ 2$,*

$$\sharp\{v\in\Omega:\ |v|\le x,\ a_i(v)+r_i(|v|^{g_i})=0\}=o(x/\log x),$$

then under the GRH, for any Borel set $\mathbb{B}\subseteq\mathbb{R}^n$,

$$\lim_{B\to+\infty}\frac{1}{|N(B)|}\sharp\{v\in N(B):(\omega_1,\omega_2)\in\mathbb{B}\}=\frac{1}{2\pi}\int_{\mathbb{B}}e^{-\frac{1}{2}(x_1^2+x_2^2)}dx_1dx_2,$$

where for $i=1,\ 2$, $\omega_i=\frac{\omega(m_i(v))-\log\log B}{\sqrt{\log\log B}}$, $m_i(v)=a_i(v)+r_i(|v|^{g_i})$. In particular,

$$\lim_{B\to+\infty}\frac{1}{|N(B)|}\sharp\{v\in N(B):\omega\left(a_1(v)+r_1(|v|^{g_1})\right)<\omega\left(a_2(v)+r_2(|v|^{g_2})\right)\}=\frac{1}{2}.$$

(2) *If for each $i=1,\ 2$,*

$$\sharp\{v\in\Omega:\ |v|\le x,\ \det(I_{2g_i}-\rho_{i,\ell}(\mathrm{Frob}_v))=0\}=o(x/\log x),$$

then under the GRH, for any Borel set $\mathbb{B} \subseteq \mathbb{R}^n$,

$$\lim_{B\to+\infty} \frac{1}{|N(B)|} \sharp \{v \in N(B) : (\omega_1, \omega_2) \in \mathbb{B}\} = \frac{1}{2\pi} \int_{\mathbb{B}} e^{-\frac{1}{2}(x_1^2+x_2^2)}\, dx_1\, dx_2,$$

where for $i = 1,\ 2$, $\omega_i = \frac{\omega(m_i(v)) - \log\log B}{\sqrt{\log\log B}}$, $m_i(v) = \det(I_{2g_i} - \rho_{i,\ell}(\mathrm{Frob}_v))$. *In particular,*

$$\lim_{B\to+\infty} \frac{1}{|N(B)|} \sharp \{v \in N(B) : \omega\left(\det(I_{2g_1} - \rho_{1,\ell}(\mathrm{Frob}_v))\right) < \omega\left(\det(I_{2g_2} - \rho_{2,\ell}(\mathrm{Frob}_v))\right)\} = \frac{1}{2}.$$

Combining Theorem 1.3 and Theorem 4.3, we obtain Theorem 1.5 and the following multiplicity one result.

Theorem 4.4. *Let* A_1/K *and* A_2/K *be generic abelian varieties of dimension* g_1 *and* g_2 *respectively. For* $i = 1, 2$, *and primes* v *of* K *where* A_1 *and* A_2 *have good reduction, let* $\rho_{i,\ell} : G_K \to \mathrm{GSp}_{2g_i}(\mathbb{Z}_\ell)$ *be the* ℓ*-adic representation attached to* A_i, $a_i(v) = \rho_{i,\ell}(\mathrm{Frob}_v) \in \mathbb{Z}$ *(for a large* ℓ *with* $v \nmid \ell$*). For any positive number* x, *let* N_x *be the set of primes* v *of* K *such that* $|v| = \mathrm{Norm}_{K/\mathbb{Q}}\, v \le x$, *and* A_1 *and* A_2 *have good reduction at* v. *Under the GRH, if*

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \{v \in N_x : \omega\left(a_1(v) + |v|^{g_1}\right) = \omega\left(a_2(v) + |v|^{g_2}\right)\} > 0,$$

or if

$$\lim_{x\to+\infty} \frac{1}{x/\log x} \sharp \{v \in N_x : \omega(|A_{1,v}(k_v)|) = \omega(|A_{2,v}(k_v)|)\} > 0,$$

then A_1 *and* A_2 *are isogenous over* $\overline{K}$. *In particular,* $g_1 = g_2$.

5. Erdős–Kac analogues for abelian surfaces

The preceding discussion indicates that for other types of abelian varieties, once the open image and independence results for the Galois representations are available, one can establish Erdős–Kac analogues and multiplicity one results by carrying out the corresponding computations. In this section we turn to abelian surfaces, i.e., two-dimensional abelian varieties. For simplicity we work with absolutely simple abelian surfaces A/K and assume that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$. By the classification of the geometric endomorphism algebras of abelian surfaces (a particular case of the Albert classification, cf. for example [18, p. 203]), only four cases can arise:

- Type I, trivial endomorphisms: $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ (so A is in particular a generic abelian variety by Theorem 1.2);
- Type II, real multiplication: $\mathrm{End}_{\overline{K}}(A)$ is an order in a real quadratic field (so A is in particular an abelian variety of GL_2-type);
- Type III, quaternionic multiplication: $\mathrm{End}_{\overline{K}}(A)$ is an order in a quaternion algebra over $\mathbb{Q}$;
- Type IV, complex multiplication: $\mathrm{End}_{\overline{K}}(A)$ is an order in a quartic CM field.

Our aim is to prove Theorems 1.6 and 1.7. The type I case is already covered by Theorems 1.4 and 1.5. In [4], Chen and the authors proved the independence property for Galois representations from a pair of GL_2-type abelian varieties and established an Erdős–Kac analogue for the invariant $|A_v(k_v)| + 1$. In the present setting of surfaces, we refine the invariant to $|A_v(k_v)|$ via explicit computations, thereby obtaining the result for

the type II case (cf. [4, Remark 4.15]). Next, we prove the independence result for a pair of abelian surfaces with quaternionic multiplication and settle the type III case. Finally, we add a remark on the CM-type case, for which we can only obtain a univariate distribution result for now.

The proofs for all cases proceed in parallel with that for generic varieties. For an abelian surface A of any given type, we always let $G(\ell)$ denote the image of its mod-ℓ representation, and let $C(\ell)$ be the conjugacy-invariant subset of $G(\ell)$ determined by the invariant $|A_v(k_v)|$. While treating a pair of surfaces A_1, A_2, we similarly define $G(\ell,\ell)$ and $C(\ell,\ell)$. Setting $g(\ell) = |C(\ell)|/|G(\ell)|$ and $g(\ell,\ell) = |C(\ell,\ell)|/|G(\ell,\ell)|$, and assuming the independence condition, it then suffices to verify that conditions **C4** and **C5** hold with $\sigma_{12} = \sigma_{21} = 0$ in **C4** and $c_1 = c_2 = 1$ in **C5**. More precisely, to prove Theorems 1.6 and 1.7, we only need to verify that the following holds.

(a) As $T > 0$ goes to infinity, there exists $c \in \mathbb{R}$ such that

$$\sum_{\ell > T} g^2(\ell) = O\left(\frac{1}{\log T}\right) \text{ and } \sum_{\ell \le T} g(\ell) = \log\log T + c + O\left(\frac{1}{\log T}\right);$$

(b) As $T > 0$ goes to infinity,

$$\sum_{\ell \le T} g(\ell,\ell) < \infty.$$

5.1. **GL_2-type surfaces.** Let A/K be an abelian surface of GL_2-type, i.e., its endomorphism algebra $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ is a real quadratic field E. Ribet [22] proved that for almost all ℓ, the image of $\rho_{A,\ell}$ is

$$\mathcal{A}_{\ell^\infty} = \{x \in \mathrm{GL}_2(\mathcal{O}_E \otimes \mathbb{Z}_\ell) : \det x \in \mathbb{Z}_\ell^\times\},$$

and so for almost all ℓ, the image of $\overline{\rho}_{A,\ell}$ is

$$G(\ell) = \{x \in \mathrm{GL}_2(\mathcal{O}_E \otimes \mathbb{Z}_\ell/\ell) : \det x \in \mathbb{F}_\ell^\times\}.$$

Under Theorem 3.1, the invariant $|A_v(k_v)|$ corresponds to the conjugacy-invariant subset

$$C(\ell) = \{x \in G(\ell) : \overline{\mathrm{Norm}}_\ell(\det(1-x)) = 0\},$$

where $\overline{\mathrm{Norm}}_\ell : \mathcal{O}_E \otimes \mathbb{Z}_\ell/\ell \to \mathbb{F}_\ell$ is the norm map induced from $\mathrm{Norm}_{E/\mathbb{Q}}$.

Lemma 5.1. *Let ℓ be an odd prime number that is unramified in the quadratic field E.*

(1) *If ℓ splits in E, then $|G(\ell)| = \ell^2(\ell-1)^3(\ell+1)^2$ and $|C(\ell)| = 2\ell^6 - \ell^5 - 7\ell^4 + 3\ell^3 + 6\ell^2$;*
(2) *If ℓ is inert in E, then $|G(\ell)| = \ell^2(\ell-1)^2(\ell+1)(\ell^2+1)$ and $|C(\ell)| = \ell^5 - \ell^4 + \ell^3 - 2\ell^2$.*

Proof. If ℓ splits in E, then $\mathcal{O}_E \otimes \mathbb{Z}_\ell/\ell \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$, so

$$G(\ell) = \{x \in \mathrm{GL}_2(\mathbb{F}_\ell \oplus \mathbb{F}_\ell) : \det x \in \mathbb{F}_\ell^\times\}.$$

We naturally identify $G(\ell)$ with the set

$$\{(u_1, u_2) \in \mathrm{GL}_2(\mathbb{F}_\ell) \times \mathrm{GL}_2(\mathbb{F}_\ell) : \det(u_1) = \det(u_2)\},$$

and thus

$$|G(\ell)| = (\ell-1) \cdot |\mathrm{SL}_2(\mathbb{F}_\ell)|^2 = \ell^2(\ell-1)^3(\ell+1)^2.$$

Now

$$C(\ell) = \{(u_1, u_2) \in G(\ell) : \det(1-u_1) = 0 \text{ or } \det(1-u_2) = 0\}.$$

Consider $H := \{u \in \mathrm{GL}_2(\mathbb{F}_\ell) : \det(1-u) = 0\}$, i.e., the set of matrices with eigenvalue 1. We classify elements of H by the description of the conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_q)$ (See for example [8, Chap.4, §5.2]):

- The identity matrix: 1 element;
- Diagonalizable matrices with eigenvalues 1 and λ ($\lambda \in \mathbb{F}_\ell^\times$, $\lambda \neq 1$): For each λ, the conjugacy class size is $\ell(\ell+1)$, and there are $\ell-2$ choices of λ, contributing $(\ell-2)\ell(\ell+1)$ elements;
- Non-diagonalizable matrices with eigenvalue 1: The conjugacy class has size ℓ^2-1, contributing ℓ^2-1 elements.

Thus

$$|H| = 1 + (\ell-2)\ell(\ell+1) + (\ell^2-1) = \ell^3 - 2\ell.$$

It is easy to see that

$$\begin{aligned} |C(\ell)| &= \sharp\{(u_1,u_2) \in G(\ell) : \ u_1 \in H \text{ or } u_2 \in H\} \\ &= 2|G_1| - |G_{1,2}|, \end{aligned}$$

where $G_1 = \{(u_1,u_2) \in G(\ell) : u_1 \in H\}$ and $G_{1,2} = \{(u_1,u_2) \in G(\ell) : u_1 \in H,\ u_2 \in H\}$.

For fixed $u_1 \in H$ with $\det(u_1) = d$, the number of u_2 with $\det(u_2) = d$ is $|\mathrm{SL}_2(\mathbb{F}_\ell)|$. Hence

$$|G_1| = |H| \cdot |\mathrm{SL}_2(\mathbb{F}_\ell)| = \ell^2(\ell^2-1)(\ell^2-2).$$

We compute $|G_{1,2}|$ by partition according to the common determinant d. Let $H_d = \{u \in H : \det(u) = d\}$. It follows from the description of elements of H that $H_1 = \ell^2$ and $H_d = \ell(\ell+1)$ for $d \in \mathbb{F}_\ell^\times, d \neq 1$. Then

$$|G_{1,2}| = \sum_{d \in \mathbb{F}_\ell^\times} |H_d|^2 = \ell^4 + (\ell-2)\ell^2(\ell+1)^2.$$

Hence

$$\begin{aligned} |C(\ell)| &= 2\ell^2(\ell^2-1)(\ell^2-2) - \left[\ell^4 + \ell^2(\ell-2)(\ell+1)^2\right] \\ &= 2\ell^6 - \ell^5 - 7\ell^4 + 3\ell^3 + 6\ell^2 \end{aligned}$$

and (1) follows.

For (2), assume that ℓ is inert, then $\mathcal{O}_E \otimes \mathbb{Z}_\ell/\ell \cong \mathbb{F}_{\ell^2}$, and

$$\begin{aligned} |G(\ell)| &= \sharp\{u \in \mathrm{GL}_2(\mathbb{F}_{\ell^2}) : \ \det(u) \in \mathbb{F}_\ell^\times\} \\ &= \ell^2(\ell-1)^2(\ell+1)(\ell^2+1). \end{aligned}$$

Consider

$$C(\ell) = \{u \in G(\ell) : \ \det(1-u) = 0\}.$$

For $u \in C(\ell)$, $\det(1-u) = 0$ implies that 1 is an eigenvalue of u, and so the eigenvalues of u are 1 and $\lambda = \det(u) \in \mathbb{F}_\ell^\times$. Again by counting conjugacy classes, we have

$$|C(\ell)| = \ell^4 + (\ell-2)\cdot\ell^2(\ell^2+1) = \ell^5 - \ell^4 + \ell^3 - 2\ell^2.$$

The lemma follows. □

Next, we check the condition (a) holds for $g(\ell) = |C(\ell)|/|G(\ell)|$. By the above Lemma,

$$g(\ell) = \begin{cases} 2/\ell + O(1/\ell^2) & \text{if } \ell \text{ splits in } E, \\ O(1/\ell^2) & \text{if } \ell \text{ is inert.} \end{cases}$$

The first equation in (a) holds obviously. Denote by Δ the discriminant of E. It is well-known that there exists a subgroup J of index 2 in $(\mathbb{Z}/|\Delta|\mathbb{Z})^\times$ such that an odd prime ℓ splits in the real quadratic field E if and only if $\ell \bmod \Delta \in J$. The Mertens' theorem for arithmetic progressions [30] says that, for any integer $m \geq 1$ and integer a with $\gcd(a, m) = 1$, there exists a constant $c_{m,a}$ such that

$$\sum_{\ell \leq x, \ell \equiv a (\bmod m)} \frac{1}{\ell} = \frac{1}{\varphi(m)} \log\log x + c_{m,a} + O\left(\frac{1}{\log x}\right), \tag{5.1}$$

where $\varphi(m)$ is the Euler's totient function. Therefore

$$\begin{aligned}\sum_{\ell \leq x} g(\ell) &= \sum_{a \in J} \sum_{\ell \leq x, \ell \equiv a (\bmod \Delta)} \frac{2}{\ell} + c' + O\left(\frac{1}{\log x}\right) \\ &= \frac{\phi(\Delta)}{2} \frac{2}{\phi(\Delta)} \log\log x + \sum_{a \in J} c_{\Delta,a} + c' + O\left(\frac{1}{\log x}\right) \\ &= \log\log x + c + O\left(\frac{1}{\log x}\right).\end{aligned}$$

So the second equation in (a) holds.

Let A_1/K and A_2/K be abelian surfaces of GL_2-type with real multiplication by E_1 and E_2 respectively. Assume that A_1 and A_2 are not isogenous over $\overline{K}$. The independence property [4, Theorem 1.4] implies that the product representation $\overline{\rho}_{A_1,\ell} \times \overline{\rho}_{A_2,\ell}$ has image

$$G(\ell, \ell) = \{(u_1, u_2) \in \mathrm{GL}_2(\mathcal{O}_{E_1} \otimes \mathbb{Z}_\ell/\ell) \times \mathrm{GL}_2(\mathcal{O}_{E_2} \otimes \mathbb{Z}_\ell/\ell) : \ \det(u_1) = \det(u_2) \in \mathbb{F}_\ell^\times\}.$$

By [4, Lemma 4.6], we have $|G(\ell, \ell)| = \ell^{13} + O(\ell^{12})$.

We need to consider the subset

$$C(\ell, \ell) = \{(u_1, u_2) \in G(\ell, \ell) : \ \overline{\mathrm{Norm}}_{1,\ell}(\det(1 - u_1)) = 0 \text{ or } \overline{\mathrm{Norm}}_{2,\ell}(\det(1 - u_2)) = 0\},$$

where $\overline{\mathrm{Norm}}_{i,\ell} : \mathcal{O}_{E_i} \otimes \mathbb{Z}_\ell/\ell \to \mathbb{F}_\ell$ is the norm map induced from $\mathrm{Norm}_{E_i/\mathbb{Q}}$ for $i = 1, 2$. To check the condition (b), it suffices to show $C(\ell, \ell) = O(\ell^{11})$. We verify it only when ℓ splits in both E_1 and E_2 and the verification for other cases follows similarly.

Assume that ℓ splits in both E_1 and E_2, then

$$\begin{aligned}|C(\ell, \ell)| &= \sharp\{(u_1, u_2) \in C(\ell) \times C(\ell) : \ \det(u_1) = \det(u_2)\} \\ &= \sum_{u_1 \in C(\ell)} \sharp\{u_2 \in C(\ell) : \ \det(u_2) = \det(u_1)\}.\end{aligned}$$

Note that for $d \in \mathbb{F}_\ell^\times$,

$$\sharp\{u_2 \in C(\ell) : \ \det(u_2) = d\} = 2|H_d||\mathrm{SL}_2(\mathbb{F}_\ell)| - |H_d|^2 = O(\ell^5).$$

Thus $|C(\ell, \ell)| = |C(\ell)| \cdot O(\ell^5) = O(\ell^{11})$. Since conditions (a) and (b) hold, we obtain the type II case of Theorems 1.6 and 1.7.

5.2. **QM surfaces.** Let A/K be an abelian surface such that $R = \mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$ is an order in an indefinite quaternion algebra D over $\mathbb{Q}$, and let Δ be the discriminant of R. The following result gives a description of the Galois representations attached to A. For details see [1, Theorem 5.4] and [16, Section 5].

Theorem 5.2 (cf. [1, 16]). *If ℓ is larger than $b(2[K:\mathbb{Q}],4,2h(A))^{1/2}$, does not divide Δ, and is unramified in K, then the following hold.*

1. *The Tate module $T_\ell(A)$ admits a G_K-equivariant decomposition $T_\ell(A) \cong W_{\ell^\infty} \oplus W_{\ell^\infty}$, where W_{ℓ^∞} is a free $\mathbb{Z}_\ell$-module of rank 2. The representation $\rho_{A,\ell} : G_K \to \mathrm{Aut}(T_\ell(A))$ is therefore equivalent to two copies of the representation on a single factor $\rho^W_{A,\ell} : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(W_{\ell^\infty}) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$.*
2. *The determinant of $\rho^W_{A,\ell}(g)$ is the ℓ-adic cyclotomic character $\chi_\ell(g)$.*
3. *The image of the representation $\rho_{A,\ell}$, which we identify with the image of $\rho^W_{A,\ell}$, is the full group $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Here $b(d,g,h) = \left((14g)^{64g^2} d \max(h, \log d, 1)^2\right)^{2^{10}g^3}$ and $h(A)$ is the semistable Faltings height of A as in [16, Definition 1.2].

We apply an argument similar to [16, Lemma 4.21 and Theorem 4.22] to prove an explicit large image result for products of abelian surfaces with quaternionic multiplication. The main tool is the following explicit isogeny theorem proved by Gaudron and Rémond [9, Theorem 1.4].

Theorem 5.3 (cf. [9]). *For every abelian variety A/K and for every abelian variety A^*/K that is K-isogenous to A, there exists a K-isogeny $A^* \to A$ with degree bounded by $b([K:\mathbb{Q}], \dim A, h(A))$.*

Proposition 5.4. *Let A_1/K and A_2/K be two abelian surfaces such that $\mathrm{End}_K(A_i) = \mathrm{End}_{\overline{K}}(A_i) = R_i$, where R_i is an order in an indefinite quaternion algebra D_i over $\mathbb{Q}$ for $i = 1,2$. Denote by Δ_i the discriminant of R_i. Assume that A_1 and A_2 are not isogenous over $\overline{K}$. If ℓ is strictly large than $M(K,A_1,A_2) = b(2[K:\mathbb{Q}],4,2\max(h(A_1),h(A_2)))^{1/2}$, does not divide $\Delta_1\Delta_2$, and is unramified in K, then the image S of the product representation*

$$\rho_{A_1,\ell} \times \rho_{A_2,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is the subgroup

$$\{(u_1,u_2) \in \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell) \mid \det u_1 = \det u_2\}.$$

Proof. Note that $M(K,A_1,A_2) \geq b(2[K:\mathbb{Q}],4,2h(A_i))^{1/2}$ for $i = 1,2$. So by Theorem 5.2, our assumption on ℓ implies that the representation $\rho_{A_i,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective for $i = 1,2$.

We first show that the image $\bar{S}$ of $\bar{\rho}_{A_1,\ell} \times \bar{\rho}_{A_2,\ell}$ contains $\mathrm{SL}_2\,\mathbb{F}_\ell \times \mathrm{SL}_2\,\mathbb{F}_\ell$. Assume the contrary, then by [24, Lemme 8], there exists an isomorphism $f : \mathbb{F}_\ell^2 \to \mathbb{F}_\ell^2$ and a character $\epsilon : S \to \{\pm 1\}$, such that $u_2 = \epsilon((u_1,u_2)) f u_1 f^{-1}$ for all $(u_1,u_2) \in \bar{S}$. Assume first that ϵ is trivial. Define

$$\Gamma = \{(x_1,y_1,x_2,y_2) \in W_{1,\ell} \oplus W_{1,\ell} \oplus W_{2,\ell} \oplus W_{2,\ell} \cong A_1[\ell] \oplus A_2[\ell] :\ x_2 = fx_1, y_1 = y_2 = 0\},$$

where $T_\ell(A_i) \cong W_{i,\ell^\infty} \oplus W_{i,\ell^\infty}$ and $W_{i,\ell} = W_{i,\ell^\infty}/\ell W_{i,\ell^\infty}$. As $u_2 = f u_1 f^{-1}$, $\Gamma \subset A_1 \times A_2$ is G_K-invariant. The quotient $A^* := A_1 \times A_2/\Gamma$ is defined over K. Let $\pi : A := A_1 \times A_2 \to A^*$ be the canonical projection. By Theorem 5.3, there exists an isogeny $\psi : A^* \to A$ with degree $\leq b([K:\mathbb{Q}],4,h(A_1)+h(A_2))$. It is clear that the composition $e := \psi \circ \pi$ annihilates Γ. On the other hand, since A_1 and A_2 are not isogenous, $e = (e_1,e_2) \in \mathrm{End}(A) \subset$

$\mathcal{O}_{D_1} \oplus \mathcal{O}_{D_2}$, where $\mathcal{O}_{D_i}$ is a maximal order of D_i that contains R_i for $i = 1, 2$. Therefore $e_1 \in \ell\mathcal{O}_{D_1}$ and $e_2 \in \ell\mathcal{O}_{D_2}$. We have

$$\ell^4 \mid \deg(e_1) \cdot \deg(e_2) = \deg(\psi \circ \pi) = \ell^2 \deg(\psi) \leq \ell^2 b([K : \mathbb{Q}], 4, h(A_1) + h(A_2)),$$

which gives

$$\ell \leq b([K : \mathbb{Q}], 4, h(A_1) + h(A_2))^{1/2} \leq M(K, A_1, A_2),$$

a contradiction. If ϵ is not trivial, then the kernel of $G_K \to S \xrightarrow{\epsilon} \{\pm 1\}$ defines a quadratic extension K' of K. Replacing K by K' and repeating the above argument, we have

$$\ell \leq b(2[K : \mathbb{Q}], 4, h(A_1) + h(A_2))^{1/2} \leq M(K, A_1, A_2),$$

also a contradiction.

Since $\bar{S}$ contains $\mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$, by [24, Lemme 10], we have that S contains $\mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{SL}_2(\mathbb{Z}_\ell)$. Since furthermore the map $\det \circ \rho_{A_i,\ell} : G_K \to \mathbb{Z}_\ell^\times$ is surjective by (2) of Theorem 5.2 and [16, Lemma 2.1], we conclude that

$$S = \{(u_1, u_2) \in \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell) \mid \det u_1 = \det u_2\}.$$

The proposition follows. □

Combining the above proposition, Theorem 5.2 and [15, Theorem 1.2.3], we obtain the independent result for Galois representations.

Theorem 5.5. *Let A_1/K and A_2/K be two abelian surfaces such that $\mathrm{End}_K(A_i) = \mathrm{End}_{\overline{K}}(A_i)$ is an order in an indefinite quaternion algebra over $\mathbb{Q}$ for $i = 1, 2$. Assume that A_1 and A_2 are not isogenous over $\overline{K}$. Then there exists a positive number N such that for each $\ell \in \Lambda_N$, the representations $\rho_{A_1,\ell}$ and $\rho_{A_2,\ell}$ are independent up to determinant (cf.* [4, Definition 1.3]*) and the system $\{\rho_{A_1,\ell} \times \rho_{A_2,\ell}\}_{\ell \in \Lambda_N}$ is independent.*

Note that $\ell \mid |A_v(k_v)| = \det(I_2 - \rho_{A,\ell}^W(\mathrm{Frob}_v))^2$ if and only if $\ell \mid \det(I_2 - \rho_{A,\ell}^W(\mathrm{Frob}_v))$. Then the type III case of Theorems 1.6 and 1.7 follows from the following computations, where we keep the notation H and $G_{1,2}$ from the previous subsection.

$$|G(\ell)| = |\,\mathrm{GL}_2(\mathbb{F}_\ell)| = \ell(\ell+1)(\ell-1)^2.$$

$$|C(\ell)| = \sharp\{u \in \mathrm{GL}_2(\mathbb{F}_\ell) : \det(1-u) = 0\} = |H| = \ell^3 - 2\ell.$$

$$|G(\ell,\ell)| = \sharp\{(u_1, u_2) \in \mathrm{GL}_2(\mathbb{F}_\ell) \times \mathrm{GL}_2(\mathbb{F}_\ell) : \det(u_1) = \det(u_2)\} = \ell^2(\ell-1)^3(\ell+1)^2.$$

$$|C(\ell,\ell)| = \sharp\{(u_1, u_2) \in G(\ell,\ell) : u_1 \in H,\ u_2 \in H\} = |G_{1,2}| = \ell^4 + (\ell-2)\ell^2(\ell+1)^2.$$

5.3. **CM-type surfaces.** In her work [29], Weng computed the image $G(\ell)$ of the mod-ℓ Galois representations for abelian surfaces of CM-type and the size of the subset of matrices with eigenvalue 1 of $G(\ell)$, which she used to study the divisibility properties of the group order of rational points on CM-type abelian surfaces over finite fields. Combining her calculations [29, Lemma 3.8] and a variant [29, Theorem 4.2] of equation (5.1) precisely yields the condition (a) and hence yields the type IV case of Theorem 1.6. However, for a pair of non-isogenous CM-type surfaces, we do not know whether a bivariate distribution result such as Theorem 1.7 holds.

Remark 5.6. It is not difficult to state Theorem 4.3 for three or more systems of Galois representations and state Theorems 1.5 and 1.7 for three or more abelian varieties. We omit the details as there is little difference between the general case and the two systems case.

References

[1] G. M. Banaszak, W. Gajda and P. Krasoń, On the image of l-adic Galois representations for abelian varieties of type I and II, Doc. Math. **2006**, Extra Vol., 35–75; MR2290584

[2] S. Bloom, Almost prime values of the order of abelian varieties over finite fields, arXiv:1803.03698, 2018.

[3] W. Castryck, A. Folsom, H. Hubrechts and A. V. Sutherland, The probability that the number of points on the Jacobian of a genus 2 curve is prime, Proc. Lond. Math. Soc. (3) **104** (2012), no. 6, 1235–1270; MR2946086

[4] J. Chen, C. Cheng and Y. Cui, The independence of Galois representations from abelian varieties of GL_2-type. `http://maths.nju.edu.cn/~ccheng/Research/GL2type.pdf`

[5] P. Deligne, La conjecture de Weil. I, Inst. Hautes Études Sci. Publ. Math. No. 43 (1974), 273–307; MR0340258

[6] D. El-Baz, D. Loughran and E. Sofos, Multivariate normal distribution for integral points on varieties, Trans. Amer. Math. Soc. **375** (2022), no. 5, 3089–3128; MR4402657

[7] P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. Math. **62** (1940), 738–742; MR0002374

[8] W. Fulton and J. D. Harris, *Representation theory*, Graduate Texts in Mathematics Readings in Mathematics, 129 , Springer, New York, 1991; MR1153249

[9] É. Gaudron and G. Rémond, Polarisations et isogénies, Duke Math. J. **163** (2014), no. 11, 2057–2108; MR3263028

[10] A. J. Granville and K. Soundararajan, Sieving and the Erdős-Kac theorem, in *Equidistribution in number theory, an introduction*, 15–27, NATO Sci. Ser. II Math. Phys. Chem., 237, Springer, Dordrecht, 2007; MR2290492

[11] C. J. Hall, An open-image theorem for a general class of abelian varieties, Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711; MR2820155

[12] M. Hindry and N. Ratazzi, Points de torsion sur les variétés abéliennes de type GSp, J. Inst. Math. Jussieu **11** (2012), no. 1, 27–65; MR2862374

[13] K. Lee, A counting formula about the symplectic similitude group, Bull. Austral. Math. Soc. **63** (2001), no. 1, 15–20; MR1812305

[14] Y.-R. Liu, Prime analogues of the Erdős-Kac theorem for elliptic curves, J. Number Theory **119** (2006), no. 2, 155–170; MR2250042

[15] D. Loeffler, Images of adelic Galois representations for modular forms, Glasg. Math. J. **59** (2017), no. 1, 11–25; MR3576325

[16] D. Lombardo, Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties, J. Algebra **460** (2016), 26–59; MR3510393

[17] J. Mayle and T. Wang, An effective open image theorem for products of principally polarized abelian varieties, J. Number Theory **274** (2025), 140–179; MR4875533

[18] D. B. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, 5, Tata Inst. Fund. Res., Bombay, 1970 Oxford Univ. Press, London, 1970; MR0282985

[19] M. R. Murty and V. P. Murty, An analogue of the Erdős-Kac theorem for Fourier coefficients of modular forms, Indian J. Pure Appl. Math. **15** (1984), no. 10, 1090–1101; MR0765015

[20] O. T. O'Meara, *Symplectic groups*, Mathematical Surveys, No. 16, Amer. Math. Soc., Providence, RI, 1978; MR0502254

[21] R. Pink, l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture, J. Reine Angew. Math. **495** (1998), 187–237; MR1603865

[22] K. A. Ribet, Galois action on division points of Abelian varieties with real multiplications, Amer. J. Math. **98** (1976), no. 3, 751–804; MR0457455

[23] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968; MR0263823

[24] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331; MR0387283

[25] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Études Sci. Publ. Math. No. 54 (1981), 123–201; MR0644559

[26] J.-P. Serre, *Œuvres. Collected papers. IV*, Springer, Berlin, 2000; MR1730973
[27] J.-P. Serre, Un critère d'indépendance pour une famille de représentations ℓ-adiques, Comment. Math. Helv. **88** (2013), no. 3, 541–554; MR3093502
[28] W. Wang and C. Cheng, Distinguishing newforms by the prime divisors of their Fourier coefficients, J. Number Theory **255** (2024), 148–165; MR4648487
[29] A. Weng, On the order of abelian surfaces of CM-type over finite prime fields, Quaest. Math. **38** (2015), no. 6, 771–787; MR3435951
[30] K. S. Williams, Mertens' theorem for arithmetic progressions, J. Number Theory **6** (1974), 353–359; MR0364137

School of Mathematics, Nanjing University, Nanjing 210093, China
Email address: cxcheng@nju.edu.cn

School of Mathematics, Nanjing University, Nanjing 210093, China
Email address: ydc@smail.nju.edu.cn