A GEOMETRIC VARIANT OF TITCHMARSH DIVISOR PROBLEM

AMIR AKBARY AND DRAGOS GHIOCA

Abstract. We formulate a geometric analogue of the Titchmarsh Divisor Problem in the context of abelian varieties. For any abelian variety A defined over $\mathbb{Q}$, we study the asymptotic distribution of the primes of $\mathbb{Z}$ which split completely in the division fields of A. For all abelian varieties which contain an elliptic curve we establish an asymptotic formula for such primes under the assumption of GRH. We explain how to derive an unconditional asymptotic formula in the case that the abelian variety is a CM elliptic curve.

1. Introduction

Let $\tau(n)$ denote the number of divisors of the positive integer n and p denote a prime number. In 1931 Titchmarsh [23] studied the behaviour of

$$\sum_{a<p\leq x} \tau(p-a),$$

for a fixed positive integer a, as $x \to \infty$. He proved the following result.

Theorem 1.1. (Titchmarsh) *Under the assumption of the Generalized Riemann Hypothesis (GRH) for the Dirichlet L-functions we have*

$$\sum_{a<p\leq x} \tau(p-a) = x \prod_{p\mid a}\left(1-\frac{1}{p}\right)\prod_{p\nmid a}\left(1+\frac{1}{p(p-1)}\right)+O\left(\frac{x\log\log x}{\log x}\right),$$

as $x \to \infty$.

In 1961, Linnik [12] established the above asymptotic unconditionally by using his dispersion method. Later Rodriquez [18] and independently Halberstam [8], by a straightforward application of the Bombieri-Vinogradov theorem, proved unconditionally the Titchmarsh conjectural asymptotic formula. In the special case $a = 1$ we have

$$\sum_{p\leq x} \tau(p-1) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}x + O\left(\frac{x\log\log x}{\log x}\right),$$

where $\zeta(.)$ denotes the Riemann zeta function. It is immediate to see that

$$\sum_{p\leq x} \tau(p-1) = \sum_{1\leq m\leq x-1} \pi(x;m,1) = \sum_{m\geq 1} \pi(x;m,1), \tag{1.1}$$

where $\pi(x;m,1) = \#\{p \leq x;\ p \text{ is prime and } p \equiv 1 \pmod m\}$ is the usual counting function for primes congruent to 1 modulo m. This allows us to make the following interpretation of

2010 *Mathematics Subject Classification.* 11G35, 11G10, 11R45.

Key words and phrases. Titchmarsh divisor problem, abelian varieties, CM elliptic curves.

Research of the authors is partially supported by NSERC.

Titchmarsh classical result. For each positive integer m and for each odd prime number p, we have that $p \equiv 1 \pmod{m}$ if and only if p splits completely in the cyclotomic extension $\mathbb{Q}(\mu_m)$ (where μ_m is the set of all roots of unity of order dividing m). Also note that the prime 2 splits completely in $\mathbb{Q}(\mu_m)$ if and only if $m \in \{1, 2\}$. So, essentially, in (1.1) we are counting each prime number $p \leq x$ for each occurrence of $m \in \mathbb{N}$ such that p splits completely in $\mathbb{Q}(\mu_m)$. This interpretation of Titchmarsh's original result leads us to consider the more general problem for arbitrary families of Galois extensions.

Let $\mathcal{F} = \{\mathcal{F}_m;\ m \in \mathbb{N}\}$ be a family of finite Galois extensions of $\mathbb{Q}$. For each m, let D_m be a union of conjugacy classes of $\mathrm{Gal}(\mathcal{F}_m/\mathbb{Q})$ and let $\tau_{\mathcal{F}}(p)$ be the number of $m \in \mathbb{N}$ such that p is unramified in $\mathcal{F}_m/\mathbb{Q}$ and the Artin symbol σ_p belongs to D_m. Suppose that $\tau_{\mathcal{F}}(p) < \infty$ for each prime p. Then we have the following generalization of the Titchmarsh Divisor Problem.

Generalized Titchmarsh Divisor Problem: Study the behaviour of $\sum_{p \leq x} \tau_{\mathcal{F}}(p)$ as $x \to \infty$.

In the above generality, the problem is too unwieldy unless some constraints are imposed on the sizes of D_m, at least. Thus, for the most part, it seems reasonable to first consider the case of $D_m = \{\mathrm{Id}\}$, i.e., when $\tau_{\mathcal{F}}(p) = \#\{m \in \mathbb{N};\ p \text{ splits completely in } \mathcal{F}_m\}$. This will be the case for most of this paper (see Theorems 1.2 and 1.3). In Theorem 1.5 we will discuss a slightly more general case in which D_m is a union of conjugacy classes of $\mathrm{Gal}(\mathcal{F}_m/\mathbb{Q})$ with the property that each $\sigma \in D_m$ restricts to a given morphism on a subextension $\mathcal{E}_m \subset \mathcal{F}_m$.

Next we consider an instance of the Generalized Titchmarsh Divisor Problem, which has geometric flavour and it is also closely connected with the original Titchmarsh conjecture.

Let A be an abelian variety defined over $\mathbb{Q}$, and for each positive integer m, let $A[m]$ be the set of torsion points of A of order dividing m (for more information on abelian varieties, see Section 3). Let $\mathcal{A} = \{\mathbb{Q}(A[m]);\ m \in \mathbb{N}\}$ be the family of finite Galois extensions of $\mathbb{Q}$ and define

$$\tau_{\mathcal{A}}(p) = \#\{m \in \mathbb{N};\ p \text{ splits completely in } \mathbb{Q}(A[m])\}.$$

Since $\mathbb{Q}(\mu_m) \subset \mathbb{Q}(A[m])$ (according to [3, Lemma 1]), we know that if p splits completely in $\mathbb{Q}(A[m])$ then p splits completely in $\mathbb{Q}(\mu_m)$ and so for $p \neq 2$ we have $p \equiv 1 \pmod{m}$. For $p = 2$, clearly, p may split completely in $\mathbb{Q}(A[m])$ *only* if $m = 1, 2$ (since for $m > 2$, the prime 2 does not split completely in $\mathbb{Q}(\mu_m)$). Therefore $\tau_{\mathcal{A}}(p) < \infty$ for all primes p. So we have the following analogue of the Titchmarsh Divisor Problem for abelian varieties.

Titchmarsh Divisor Problem for Abelian Varieties Study the behaviour of $\sum_{p \leq x} \tau_{\mathcal{A}}(p)$ as $x \to \infty$.

In this paper we answer completely the above question for abelian varieties which contain a dimension one abelian subvariety E, assuming that the Generalized Riemann Hypothesis holds for the Dedekind zeta function for each number field $\mathbb{Q}(A[m])$. Note that any dimension one abelian variety is an elliptic curve. Furthermore, we show that a version of our theorem holds unconditionally when $A = E$ is an elliptic curve with complex multiplication (CM).

We note the following connection between the classical Titchmarsh divisor problem and our abelian varieties analogue. In both cases, one studies the asymptotic behaviour of the number of primes p which split completely in the extensions of $\mathbb{Q}$ obtained by adjoining the torsion points of order dividing m of a given algebraic group. Indeed, in the original Titchmarsh divisor problem, the algebraic group is the multiplicative group $\mathbb{G}_m$, while in our problem, the algebraic group is the abelian variety itself.

In Section 3, we show the following further connection between our question and the classical Titchmarsh divisor problem. For a prime p of good reduction for the abelian variety A, let A_p be the reduction modulo p of A. Let $i_A(p)$ be the largest positive integer m such that $A_p(\mathbb{F}_p)$ contains a subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$, where $g = \dim(A)$. In Section 3 we show that $\tau(i_A(p))$ is a natural analogue of $\tau(p-1)$; more precisely, we show that $\tau_{\mathcal{A}}(p) = \tau(i_A(p))$ for each prime number p of good reduction for A. Therefore, the Titchmarsh divisor problem for abelian varieties reduces to studying $\sum_{p\leq x}\tau(i_A(p))$.

We prove the following theorem.

Theorem 1.2. *Let A be an abelian variety defined over $\mathbb{Q}$, which contains a dimension one abelian subvariety E also defined over $\mathbb{Q}$. If GRH holds for the Dedekind zeta function of each extension $\mathbb{Q}(A[m])/\mathbb{Q}$, then*

$$\sum_{p\leq x}\tau_{\mathcal{A}}(p) = \left(\sum_{m=1}^{\infty}\frac{1}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O\left(x^{5/6}(\log x)^{2/3}\right).$$

We believe Theorem 1.2 holds in general, possibly with a less precise error term, i.e.

$$\sum_{p\leq x}\tau_{\mathcal{A}}(p) = \left(\sum_{m=1}^{\infty}\frac{1}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right), \tag{1.2}$$

as $x\to\infty$. However, we will explain in Remark 4.1 why our method of proof for Theorem 1.2 does not generalize to arbitrary abelian varieties.

In the special case that $A = E$ is a CM elliptic curve, one can prove unconditionally a slightly weaker version of Theorem 1.2; in this case we denote by

$$\tau_{\mathcal{E}}(p) := \{m\in\mathbb{N};\ p \text{ splits completely in } \mathbb{Q}(E[m])\}.$$

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ whose endomorphism ring $\mathrm{End}(E)$ is isomorphic with the ring of algebraic integers of an imaginary quadratic field K. Then*

$$\sum_{p\leq x}\tau_{\mathcal{E}}(p) = \left(\sum_{m=1}^{\infty}\frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O\left(\frac{x}{(\log x)^c}\right),$$

for any $c>1$.

In the case of elliptic curves the proof of the asymptotic for $\sum_{p\leq x}\tau_{\mathcal{E}}(p)$ is essentially the same as the proof of the asymptotic for the set of primes that never split completely in extensions $\mathbb{Q}(E[m])$. (In the latter problem the constant in the main term contains a Möbius function, instead of 1.) So the proof of Theorem 1.3 follows essentially from [15, Section 6] (see also [1]); For proving Theorem 1.3 we observe that since $\mathbb{Q}(E[m]) = K(E[m])$ for $m\geq 3$ (see [15, Lemma 6]) the study of primes of $\mathbb{Q}$ that split completely in $\mathbb{Q}(E[m])$ can be reduced to the study of prime ideals of K that split completely in $K(E[m])$. On the other hand since the extension $K(E[m])/K$ is abelian, we can use class field theory to show that the prime ideals of K which split completely in $K(E[m])$ belong to a bounded number of classes in the $\mathfrak{fm}$-ideal class group of K. Here $\mathfrak{f}$ is the conductor of the Grössencharacter associated to E and $\mathfrak{m}$ is the ideal generated by m in the ring of integers of K. Then one employs a version of the Bombieri-Vinogradov theorem for number fields to count the prime ideals in some fixed classes of the $\mathfrak{fm}$-ideal class group of K as $\mathfrak{m}$ varies. The fact that the ring of integers of K has only a finite number of units

plays a crucial role in the successful application of the Bombieri-Vinogradov theorem in a proof of Theorem 1.3.

Going in the opposite direction, one can prove easily under GRH the asymptotic for the set of primes p which *never* split completely in the extensions $\mathcal{A}_m$ (see [15, Theorems 1 and 2]).

Theorem 1.4. *Let A be an abelian variety defined over $\mathbb{Q}$, and assume the GRH holds for each extension $\mathbb{Q}(A[m])/\mathbb{Q}$. Then the number of primes $p \leq x$ which split completely in none of the extensions $\mathcal{A}_m$ is equal to*

$$\left(\sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(A[m]) : \mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right),$$

as $x \to \infty$, where $\mu(m)$ is the usual Möbius function.

We would like to point out that although Theorem 1.4 and our conjectured asymptotic (1.2) for $\sum_{p \leq x} \tau_{\mathcal{A}}(p)$ appear very similar to each other, however we are not able to adapt the proof of Theorem 1.4 to prove (1.2). This is mainly due to the fact that in Theorem 1.4 we are dealing with the estimations of sums which are taken over square-free integers and such sums are amenable to application of sieve techniques, however to establish (1.2) we need to deal with sums which are taken over integers (both square-free and non square-free) and these sums are harder to estimate. So our variant of the Titchmarsh divisor problem for abelian varieties appears to be a technically more challenging problem.

We note that our Theorem 1.4 fits into the general framework established by Murty in [15] for studying the asymptotic of the set of primes which do not split in any extension from a given family of Galois extensions. Our Theorem 1.4 also can be considered as a higher dimensional analogue of the cyclicity question for elliptic curves (see [20], [15], and [4]). Therefore, similar to the cyclicity question for elliptic curves, one may ask when is the density from our Theorem 1.4 positive, i.e.

$$\delta_A := \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(A[m]) : \mathbb{Q}]} > 0?$$

It is clear that if $A[2] \subset A(\mathbb{Q})$, then $\delta_A = 0$. This fact may be seen either directly since in this case $\mathbb{Q}(A[2m]) = \mathbb{Q}(A[m])$ for all odd integers m, or by interpreting the conclusion of Theorem 1.4. The density δ_A refers to the primes p for which $A_p(\mathbb{F}_p)$ does not have $2g$ invariant factors; however, if $A[2] \subset A(\mathbb{Q})$ then for all odd primes p of good reduction for A, we have $A_p[2] \subset A_p(\mathbb{F}_p)$ and $A_p[2] \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{2g}$. Therefore, there are at most finitely many primes p satisfying the hypothesis of Theorem 1.4, which forces $\delta_A = 0$. We also note that the method of [4, Section 6] can be applied to show that if $A[2] \not\subset A(\mathbb{Q})$ then $\delta_A > 0$, assuming the image of $\mathrm{Gal}(\mathbb{Q}(A[\ell^\infty])/\mathbb{Q})$ is an open subgroup of $\mathrm{GSp}(2g, \mathbb{Z}_\ell)$ for *all* primes ℓ, and moreover, $\mathrm{Gal}(\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}) \xrightarrow{\sim} \mathrm{GSp}(2g, \mathbb{Z}_\ell)$ for all but finitely many primes ℓ. Here $A[\ell^\infty]$ is the set of all torsion points of A of order a power of the prime number ℓ, while GSp denotes the general symplectic group of matrices with respect to the Weil pairing on the polarized abelian variety A. Serre [21, Théorème 3] showed that if $\mathrm{End}(A) \xrightarrow{\sim} \mathbb{Z}$ and if $\dim(A)$ equals 2, 6 or any odd integer, then the above assumption regarding the Galois groups $\mathrm{Gal}(\mathbb{Q}(A[\ell^\infty])/\mathbb{Q})$ holds, and thus, the proof of [4, Section 6] applies to show that $\delta_A > 0$ in this case.

In order to prove Theorem 1.2, we consider the prime counting function

$$\pi_{\mathcal{A}}(x; m) = \#\{2 < p \leq x;\ p \text{ is a good prime for } A \text{ which splits completely in } \mathbb{Q}(A[m])\}, \tag{1.3}$$

and show that

$$\sum_{2<p\leq x} \tau_{\mathcal{A}}(p) = \sum_{1\leq m\leq \sqrt{x}+1} \pi_{\mathcal{A}}(x;m).$$

The proof of Theorem 1.2 comes as a result of an application of the Chebotarev density theorem (under the assumption of GRH) for small values of m and employing a suitable upper bound for $\pi_{\mathcal{A}}(x;m)$ for large values of m. In finding the suitable upper bound for $\pi_{\mathcal{A}}(x;m)$ for large values of m, we use the information that A contains a dimension one abelian subvariety. We believe that such a bound may be established for any abelian variety A. However, in Remark 4.1 we explain why our method does not apply for an arbitrary abelian variety A; so, in order to establish the conclusion of Theorem 1.2 without the extra assumption about A, one would need a new approach.

Moreover, using the same approach outlined above we can prove the following generalization of Theorem 1.2. Note that for any elliptic curve E defined over $\mathbb{Q}$, and for any $m \in \mathbb{N}$, $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ embeds naturally into $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$; we will fix such an embedding for the statement of our next result.

Theorem 1.5. *Let A be an abelian variety defined over $\mathbb{Q}$, which contains a dimension one abelian subvariety E also defined over $\mathbb{Q}$. Let δ be a real number in the interval $[0,1)$, and let a be a positive integer. For each $m \in \mathbb{N}$, we let C_m be a union of conjugacy classes in $\mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})$ such that*

(i) *$|C_m| \ll m^{\delta}$; and*
(ii) *each $\sigma \in C_m$ acts on $E[m]$ through the scalar matrix*

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

For each prime number p we define

$$\tau_{\mathcal{A},\mathcal{C}}(p) := \{m \in \mathbb{N} : \sigma_p \in C_m\},$$

where for each prime p, we denote by σ_p a lifting of the Frobenius in $\mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})$. Assuming the GRH and the Artin Holomorphy Conjecture (AHC) hold for each extension $\mathbb{Q}(A[m])/\mathbb{Q}$, then

$$\sum_{p\leq x} \tau_{\mathcal{A},\mathcal{C}}(p) = \left(\sum_{m=1}^{\infty} \frac{|C_m|}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right),$$

as $x \to \infty$. More precisely if $\delta \in [0, 2/3)$ we have

$$\sum_{p\leq x} \tau_{\mathcal{A},\mathcal{C}}(p) = \left(\sum_{m=1}^{\infty} \frac{|C_m|}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + O\left(x^{\frac{10+3\delta}{12+2\delta}} (\log x)^{\frac{4}{6+\delta}}\right),$$

and if $\delta \in [2/3, 1)$ then

$$\sum_{p\leq x} \tau_{\mathcal{A},\mathcal{C}}(p) = \left(\sum_{m=1}^{\infty} \frac{|C_m|}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + O\left((x/\log x)^{\frac{5+2\delta}{6+\delta}}\right).$$

Note that using estimate (3.1) together with the fact that $|C_m| \ll m^{\delta}$ where $\delta < 1$, we conclude that the infinite sum from Theorem 1.5 is convergent. As mentioned before, if $\mathrm{End}(A) = \mathbb{Z}$ it is expected conjecturally (and also proven in many cases by Serre) that $\mathrm{Gal}(\mathbb{Q}(A[m])/\mathbb{Q}) \xrightarrow{\sim}$

$\mathrm{GSp}(2g, \mathbb{Z}/m\mathbb{Z})$ and thus $[\mathbb{Q}(A[m]) : \mathbb{Q}] \gg m^{2g^2+g+1-\epsilon}$; in this case, we can relax condition (i) from Theorem 1.5 by asking that $|C_m| \ll m^\delta$ for some $\delta \in [0, 2)$. Also, as proved by Serre [21] (see also [2, Theorem 2.8]), there exists a positive integer D such that as long as a is relatively prime with D, then $a \cdot \mathrm{Id}_{2g}$ is contained in the image of the Galois representation for A.

We consider Theorem 1.5 as a generalization of Titchmarsh original problem of studying $\sum_{p\le x} \tau(p-a)$ for an arbitrary a. Indeed, the sum in Titchmarsh's divisor problem reduces to studying the asymptotic distribution of primes p whose corresponding Frobenius elements correspond to the map $x \mapsto x^a$ in the Galois group of the cyclotomic extension $\mathbb{Q}(\mu_m)/\mathbb{Q}$. An analogue of this condition in the geometric context of Theorem 1.5 is condition (ii). For example, using the Weil pairing on the elliptic curve E, condition (ii) yields that the action on $\mathbb{Q}(\mu_m)$ of each such σ_p is precisely $x \mapsto x^{a^2}$. In particular, each p with $\sigma_p \in C_m$ satisfies $p \equiv a^2 \pmod m$ which shows that for each prime number p, the set $\tau_{\mathcal{A},\mathcal{C}}(p)$ is finite.

The motivation for our paper comes in part from [10, Section 3], where Kowalski studied the asymptotic behaviour of $\sum_{p\le x} i_E(p)$ (the sum is over the primes of good reduction for E) for an elliptic curve E; and also our motivation comes in part from the paper of Murty [15] where a related question is considered for families of Galois extensions. Our proof of Theorem 1.2 was inspired by the method employed by Cojocaru and Murty in [4]. We also found enlightening the papers of Duke and Tóth [6] and Duke [5] which study the primes p which split completely in $\mathbb{Q}(E[m])$. The plan of our paper is as follows. In Section 2, we introduce our notation. In Section 3 we present more background on abelian varieties and set up our problem, and then in Section 4 we prove Theorem 1.2. We conclude our paper by proving Theorem 1.5 in Section 5.

Acknowledgments. The authors thank Ram Murty and the referee for many useful suggestions. Also, the second author thanks David Masser for a conversation regarding the size of the Galois groups for division fields associated to abelian varieties.

2. Notation

The identity of any group G will be denoted simply by 1. For the cardinality of any finite set S, we will use alternatively the notation $\#S$, or $|S|$. For any $a \in \mathbb{N}$, we denote by $\varphi(a)$ the Euler totient function.

For any abelian variety A, always a sum $\sum_p f_A(p)$ (for some function f_A associated to A) represents a sum over all primes p of good reduction for A.

For two functions $f(x)$ and $g(x) \neq 0$, we use the notation $f(x) = O(g(x))$, or alternatively $f(x) \ll g(x)$, if $|f(x)/g(x)|$ is uniformly bounded as $x \to \infty$. Sometimes we will use the notation $f(x) \ll_t g(x)$, or alternatively $f(x) = O_t(g(x))$ to denote the dependence of the O-constant *only* on the parameter t. On the other hand we use the notation $f(x) = o(g(x))$ if $\lim_{x\to\infty} |f(x)/g(x)| = 0$. We also use the notation $\mathrm{Li}(x)$ for $\int_2^x dt/\log t$.

3. The Setup of our Problem for Abelian Varieties

We describe in detail our abelian varieties analogue of the Titchmarsh divisor problem. We start with preliminaries regarding abelian varieties (for a comprehensive treatment of abelian varieties see [14]).

An abelian variety is a projective connected algebraic group. From now on, we assume A is an abelian variety defined over $\mathbb{Q}$; for any number field K, we denote by $A(K)$ the set of K-points of the abelian variety A.

For any positive integer m, let $A[m]$ be the kernel of the multiplication-by-m endomorphism of A. If $\dim(A) = g \geq 1$, then $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$, and so $\#A[m] = m^{2g}$. Then $\mathcal{A}_m := \mathbb{Q}(A[m])$ is a finite Galois extension of $\mathbb{Q}$ and moreover $\mathbb{Q}(\mu_m) \subset \mathcal{A}_m$ (according to [3, Lemma 1]). We will use the following result of Masser [13] (see also [9, Théorème 1.1]).

Theorem 3.1. (Masser) *Let A be an abelian variety of dimension g defined over a number field K_0. Then for every nontrivial finite extension K of K_0, the size of the torsion subgroup $A(K)_{\mathrm{tor}}$ of $A(K)$ is bounded above by $C(A)[K : \mathbb{Q}]^g(\log[K : \mathbb{Q}])^g$, for some absolute constant $C(A)$ depending only on A.*

We claim that Theorem 3.1 yields the following lower bound for the degrees of our extensions

$$[\mathcal{A}_m : \mathbb{Q}] \gg_{\epsilon,A} m^{2-\epsilon} \text{ for any } \epsilon > 0. \tag{3.1}$$

Indeed, according to Theorem 3.1, $|A(\mathcal{A}_m)_{\mathrm{tor}}| \leq C(A)[\mathcal{A}_m : \mathbb{Q}]^g(\log[\mathcal{A}_m : \mathbb{Q}])^g$. On the other hand, clearly $|A(\mathcal{A}_m)_{\mathrm{tor}}| \geq m^{2g}$. Therefore $m^{2g} \leq C(A)[\mathcal{A}_m : \mathbb{Q}]^g(\log[\mathcal{A}_m : \mathbb{Q}])^g$, which immediately yields $[\mathcal{A}_m : \mathbb{Q}] \gg_{\epsilon,A} m^{2-\epsilon}$, for any $\epsilon > 0$, as claimed by (3.1).

Now, since A is defined over $\mathbb{Q}$, there exists an abelian scheme $\tilde{A}$ over an open subset of $\mathrm{Spec}(\mathbb{Z})$ such that the generic fiber of $\tilde{A}$ is A (see for example the proof of [7, Claim 3.3]). Therefore, for all but finitely many primes p, there exists a canonical reduction A_p of A modulo p, which is an abelian variety defined over $\mathbb{F}_p$ of the same dimension as the dimension of A. Each such p is called a prime of good reduction; if a prime is not of good reduction, then we say that it is of bad reduction. Since there are only finitely many primes p of bad reduction, it suffices to prove Theorem 1.2 by restricting the sum $\sum_{p \leq x} \tau_{\mathcal{A}}(p)$ over the odd primes of good reduction for A. We exclude $p = 2$ since later we will employ the condition that the prime p splits completely in $\mathbb{Q}(\mu_m)$ if and only if $p \equiv 1 \pmod{m}$, which holds as long as $p > 2$. Hence, from now on, implicitly all our sums over primes p are restricted to the odd primes of good reduction for the abelian variety A.

For a prime of good reduction p, we have that for all integers m such that $p \nmid m$, the torsion subgroup $A_p[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$. On the other hand, $\#A_p[p] \leq p^g$. By [22, Proposition 4.1(a), Ch. 7], the only possible ramified primes p for the extension $\mathcal{A}_m/\mathbb{Q}$ which are of good reduction for A are the primes dividing m. Actually, the proof from [22] is only for elliptic curves, but the same proof goes through for arbitrary abelian varieties - the main ingredient of the proof there is [22, Proposition 3.1, Ch. 7], while for this last statement, one uses [22, Proposition 3.2(b), Ch. 4] (which is a general statement about formal groups).

The finite group $A_p(\mathbb{F}_p)$ has $\prod_{i=1}^{2g} \mid 1 - \xi_i \mid$ elements, where the $\{\xi_i\}_{1 \leq i \leq 2g}$ are the eigenvalues of the Frobenius corresponding to $\mathbb{F}_p$ seen as an endomorphism of A_p. Since for each i, we have $|\xi_i| \leq \sqrt{p}$ (see [14, Theorem 1.1(b), Ch. 2]), we conclude that

$$\#A_p(\mathbb{F}_p) \leq (1 + \sqrt{p})^{2g}. \tag{3.2}$$

Let $e_A(p)$ be the exponent of the finite group $A_p(\mathbb{F}_p)$; then $A_p(\mathbb{F}_p) \subset A_p[e_A(p)]$. Therefore, $A_p(\mathbb{F}_p)$ is a subgroup of a group isomorphic to $(\mathbb{Z}/e_A(p)\mathbb{Z})^{2g}$, since $A_p[e_A(p)]$ is itself isomorphic with a subgroup of $(\mathbb{Z}/e_A(p)\mathbb{Z})^{2g}$. Let $i_A(p)$ be the largest positive integer m such that there exists a subgroup of $A_p(\mathbb{F}_p)$ isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$. In particular, this means that there exist

positive integers $i_1 \mid i_2 \mid \cdots \mid i_{2g}$ such that $A_p(\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/i_1\mathbb{Z} \times \mathbb{Z}/i_2\mathbb{Z} \times \cdots \times \mathbb{Z}/i_{2g}\mathbb{Z}$; we have that $i_A(p) = i_1$ and $e_A(p) = i_{2g}$. Since

$$i_A(p)^{2g} \mid \#A_p(\mathbb{F}_p),$$

inequality (3.2) yields that

$$i_A(p) \leq \sqrt{p} + 1. \tag{3.3}$$

The following result establishes a close connection between the primes that split completely in $\mathcal{A}_m$ and the divisors of $i_A(p)$ (the analogue of this statement for elliptic curves is well-known - see [15] and [6]).

Lemma 3.2. *Let A be an abelian variety defined over $\mathbb{Q}$, let p be an odd prime of good reduction for A. Then $m \mid i_A(p)$ if and only if p splits completely in $\mathcal{A}_m$.*

Proof. If $m \mid i_A(p)$, then we first note that p is unramified in $\mathcal{A}_m$ since it is a prime of good reduction, and also because $p \nmid m$ (since $\#A_p[m] = m^{2g}$ because $m \mid i_A(p)$). Secondly, we note that the Frobenius corresponding to $\mathbb{F}_p$ acts trivially on $A_p[m]$, which means that the identity of the Galois group $\mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})$ is a lifting of the Frobenius corresponding to $\mathbb{F}_p$. Therefore p splits completely in $\mathcal{A}_m$ by [17, Page 367, Corollary 1].

Conversely, assume now that p splits completely in $\mathcal{A}_m$. Since p is unramified in $\mathcal{A}_m$, we get that $p \nmid m$ (recall that p is odd and $\mathbb{Q}(\mu_m) \subset \mathcal{A}_m$, which means that all odd primes dividing m ramify in $\mathcal{A}_m$). If $\mathfrak{p} \in \mathrm{Spec}\,(\mathfrak{O}_{\mathcal{A}_m})$ lies above the prime $p \in \mathrm{Spec}(\mathbb{Z})$, then the reduction of each element of $A[m]$ modulo $\mathfrak{p}$ belongs to $A_p(\mathbb{F}_p)$. However, since p is a prime of good reduction for A which does not divide m, then the entire torsion subgroup $A[m]$ goes injectively through the reduction map modulo $\mathfrak{p}$ (by a similar argument as in the proof of [22, Proposition 3.1, Ch. 7]). Hence $A_p[m] \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{2g}$ is a subgroup of $A_p(\mathbb{F}_p)$; this can only happen if $m \mid i_A(p)$. □

Lemma 3.2 shows that our Titchmarsh Divisor Problem for Abelian Varieties is equivalent to the asymptotic study of the sum $\sum_{p \leq x} \tau(i_A(p))$. We use the prime counting function $\pi_{\mathcal{A}}(x; m)$ defined as in (1.3), and so, according to Lemma 3.2, we have

$$\sum_{2<p\leq x} \tau(i_A(p)) = \sum_{2<p\leq x} \left(\sum_{m \mid i_A(p)} 1 \right) = \sum_{1\leq m\leq \sqrt{x}+1} \pi_{\mathcal{A}}(x; m).$$

Note that in the above equality, we used the fact that $i_A(p) \leq \sqrt{x} + 1$ for $p \leq x$ (see inequality (3.3)), and thus all divisors $m \mid i_A(p)$ are also at most $\sqrt{x} + 1$.

Let σ_p be the conjugacy class in $G_m = \mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})$ of a lifting of the Frobenius associated to the prime p. As noted before, p splits completely in $\mathcal{A}_m$ if and only if $\sigma_p = 1$ (see [17, Page 367, Corollary 1]). So, $\pi_{\mathcal{A}}(x; m)$ counts the number of primes $p \leq x$ for which their lifting of the Frobenius in G_m equals the identity of this Galois group. This fact will allow us to employ in our proofs an effective version of the Chebotarev Density Theorem (see [11, Theorem 1.1] and [19, Theorem 4] for a proof of the first part, and [16, Corollary 3.7] for a proof of the second part).

Proposition 3.3. (Effective Chebotarev) *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G. Let $C \subset G$ be closed under conjugation, and assume the GRH for $K/\mathbb{Q}$. Define*

$$\Pi_C(x, K/\mathbb{Q}) := \#\{p \leq x;\ p \text{ is a prime of } \mathbb{Q} \text{ unramified in } K \text{ such that } \sigma_p \subseteq C\}$$

where σ_p is the Frobenius conjugacy class corresponding to p in $\mathrm{Gal}(K/\mathbb{Q})$. Then

$$\Pi_C(x, K/\mathbb{Q}) = \frac{|C|}{|G|}\mathrm{Li}\ x + O\left(|C|x^{1/2}\log\left(|G|\left(\prod_{p\in P(K/\mathbb{Q})} p\right)x\right)\right),$$

where $P(K/\mathbb{Q})$ is the set of rational primes which ramify in K, and the constant appearing in the O-notation is absolute and effectively computable.

Moreover if we assume that both GRH and AHC hold for $K/\mathbb{Q}$, then we have the following version of the above asymptotic with the improved error term.

$$\Pi_C(x, K/\mathbb{Q}) = \frac{|C|}{|G|}\mathrm{Li}\ x + O\left(|C|^{1/2}x^{1/2}\log\left(|G|\left(\prod_{p\in P(K/\mathbb{Q})} p\right)x\right)\right),$$

where $P(K/\mathbb{Q})$ is defined above, and the constant appearing in the O-notation is absolute.

We will use Proposition 3.3 for the extensions $\mathcal{A}_m/\mathbb{Q}$ and for the conjugacy class of the identity from $\mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})$ (which obviously has only one element in it). Moreover, since we know that the only primes which may ramify in $\mathcal{A}_m$ are either the primes dividing m, or the (finitely many) primes which are not of good reduction for A, we derive the following result.

Corollary 3.4. *With the above notation and under the assumption of GRH,*

$$\pi_{\mathcal{A}}(x; m) = \frac{1}{[\mathcal{A}_m : \mathbb{Q}]}\cdot \mathrm{Li}(x) + O_A\left(x^{1/2}\log(mx)\right).$$

Proof. The conclusion follows immediately from Proposition 3.3 once we note that $\mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})$ embeds naturally into $\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$ (by identifying each $\sigma \in \mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})$ with its action on $A[m]$); therefore $|\mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})| \ll m^{4g^2}$. □

Using Corollary 3.4 we establish the following result.

Corollary 3.5. *Let $\eta \in (1/4, 1/2)$, and let $h(x)$ be any function satisfying*

$$x^{\eta} \ll h(x) \ll x^{1/2}/(\log x)^3.$$

Then, working with the above notation and under the assumption of GRH, we have

$$\sum_{1\le m\le h(x)} \pi_{\mathcal{A}}(x; m) = \left(\sum_{m=1}^{\infty}\frac{1}{[\mathcal{A}_m : \mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O_{A,\eta}\left(h(x)x^{1/2}\log x\right). \tag{3.4}$$

Proof. Applying Corollary 3.4 for the range $1 \le m \le h(x)$, and also using estimate (3.1), we obtain (3.4). Indeed, the sum from the left hand side in (3.4) equals

$$\begin{aligned}
&\left(\sum_{1\le m\le h(x)}\frac{1}{[\mathcal{A}_m : \mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O_A\left(h(x)x^{1/2}\log x\right)\\
=\ &\left(\sum_{m=1}^{\infty}\frac{1}{[\mathcal{A}_m : \mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O_{\epsilon,A}\left(\frac{x}{\log x}x^{-\eta(1-\epsilon)}\right) + O_A\left(h(x)x^{1/2}\log x\right)\\
=\ &\left(\sum_{m=1}^{\infty}\frac{1}{[\mathcal{A}_m : \mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O_{A,\eta}\left(h(x)x^{1/2}\log x\right).
\end{aligned}$$

In the above computation, we may choose $\epsilon = \frac{4\eta-1}{2\eta}$ since $\eta \in \left(\frac{1}{4}, \frac{1}{2}\right)$. □

4. Proof of Theorem 1.2

We continue with the notation as in Section 3.

Proof of Theorem 1.2. Using $h(x) = x^{1/3}/(\log x)^{1/3}$ in Corollary 3.5, we obtain

$$\sum_{1\leq m\leq x^{1/3}/(\log x)^{1/3}} \pi_{\mathcal{A}}(x;m) = \left(\sum_{m=1}^{\infty} \frac{1}{[\mathcal{A}_m:\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O_A\left(x^{5/6}(\log x)^{2/3}\right).$$

We will show that

$$\sum_{x^{1/3}/(\log x)^{1/3}<m\leq \sqrt{x}+1} \pi_{\mathcal{A}}(x;m) = O_A\left(x^{5/6}(\log x)^{2/3}\right), \tag{4.1}$$

which will conclude the proof of Theorem 1.2. For proving estimate (4.1) we will use the fact that A contains a one dimensional abelian subvariety E defined over $\mathbb{Q}$. As noted before, E is an elliptic curve.

Now, if the prime p splits completely in $\mathcal{A}_m$ (for some positive integer m), then p also splits completely in $\mathcal{E}_m := \mathbb{Q}(E[m])$. Furthermore, we may assume that p is a prime of good reduction for both A and E. Indeed, there are finitely many primes of bad reduction for A or E, and thus for m large (as in the sum from (4.1)), no prime of bad reduction for either A or E splits completely in $\mathbb{Q}(E[m])$ because then p would split completely in $\mathbb{Q}(\mu_m)$ (which may only happen if $p \equiv 1 \pmod m$ for odd p, or if $m \leq 2$ for $p = 2$). Therefore $\pi_{\mathcal{A}}(x;m) \leq \pi_{\mathcal{E}}(x;m)$ (where $\pi_{\mathcal{E}}(x;m)$ is the prime counting function associated to E), and thus, in order to prove (4.1), it suffices to show that

$$\sum_{x^{1/3}/(\log x)^{1/3}<m\leq \sqrt{x}+1} \pi_{\mathcal{E}}(x;m) = O\left(x^{5/6}(\log x)^{2/3}\right). \tag{4.2}$$

We prove (4.2) using the method employed in [4]. So, using Lemma 3.2 for the one dimensional abelian variety E, we conclude that if $p \leq x$ splits completely in $\mathbb{Q}(E[m])$ then $m \mid i_E(p)$, and in particular, $m^2 \mid \#E_p(\mathbb{F}_p)$ (where E_p is the reduction of the elliptic curve E modulo the prime p of good reduction for E). Using [14, Theorem 1.1, Ch. 2] for the one-dimensional abelian variety E, we conclude that $\#E_p(\mathbb{F}_p) = p + 1 - a_E(p)$, where

$$|a_E(p)| \leq 2\sqrt{p} \leq 2\sqrt{x}.$$

Furthermore, since $\mathbb{Q}(\mu_m) \subset \mathcal{E}_m$, we obtain that if the odd prime p splits completely in $\mathcal{E}_m$, then $p \equiv 1 \pmod m$ (since p must also split completely in $\mathbb{Q}(\mu_m)$). Since $p \equiv a_E(p) - 1 \pmod{m^2}$ and also $p \equiv 1 \pmod m$, then $a_E(p) \equiv 2 \pmod m$, and thus we have the following inequality:

$$\pi_{\mathcal{E}}(x;m) \leq \sum_{\substack{|c|\leq 2\sqrt{x}\\ c\equiv 2 \pmod m}} N(x;m,c), \tag{4.3}$$

where for each integer c, we let $N(x;m,c)$ be the set of primes $p \leq x$ satisfying $p \equiv c - 1 \pmod{m^2}$. By the trivial upper bound for the number of primes in an arithmetic progression we

have $N(x;m,c) \leq \frac{x}{m^2}+1$. Since we employ this estimate for $N(x;m,c)$ only when $m \leq \sqrt{x}+1$, we conclude that

$$N(x;m,c) \ll \frac{x}{m^2}.$$

Applying this bound for $N(x;m,c)$ in (4.3) yields

$$\begin{aligned} \pi_{\mathcal{E}}(x;m) &\leq \sum_{\substack{|c|\leq 2\sqrt{x} \\ c\equiv 2 \pmod m}} N(x;m,c) \\ &\ll \frac{x^{3/2}}{m^3}, \end{aligned} \tag{4.4}$$

for $m \leq \sqrt{x}+1$. Therefore, using (4.4) with $x^{1/3}/(\log x)^{1/3} < m \leq \sqrt{x}+1$, we obtain

$$\begin{aligned} \sum_{x^{1/3}/(\log x)^{1/3}<m\leq\sqrt{x}+1} \pi_{\mathcal{E}}(x;m) &\ll \sum_{x^{1/3}/(\log x)^{1/3}<m\leq\sqrt{x}+1} \frac{x^{3/2}}{m^3} \\ &= O\left(x^{5/6}(\log x)^{2/3}\right), \end{aligned}$$

as desired. □

Remark 4.1. We expect that for any abelian variety A over $\mathbb{Q}$

$$\sum_{p\leq x} \tau_{\mathcal{A}}(p) = \left(\sum_{m=1}^{\infty} \frac{1}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right),$$

as $x \to \infty$. The difficulty in establishing this asymptotic lies in estimation of the sum $\sum_m \pi_{\mathcal{A}}(x;m)$ on a range containing large values of m. It is plausible that a bound of the form

$$\pi_{\mathcal{A}}(x;m) \ll \frac{x^{g+1/2}}{m^{2g+1}} \tag{4.5}$$

may hold for any abelian variety of dimension g. From such a bound and from Corollary 3.5 applied for $h(x) = \frac{x^{g/(2g+1)}}{(\log x)^{1/(2g+1)}}$, one deduces that

$$\sum_{p\leq x} \tau_{\mathcal{A}}(p) = \left(\sum_{m=1}^{\infty} \frac{1}{[\mathbb{Q}(A[m]):\mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + O\left(x^{\frac{4g+1}{4g+2}}(\log x)^{\frac{2g}{2g+1}}\right).$$

The difficulty in establishing bound (4.5) for any arbitrary abelian variety A lies in the fact that $\#A_p(\mathbb{F}_p) = p^g - a_A(p) + 1$, where $\mid a_A(p) \mid \leq (2g-1)p^{g-1/2} + (4^g - 2g - 1)p^{g-1} + 1$ (see [14, Theorem 1.1, Ch. 2]). Therefore, our approach through congruences to estimate the tail of the series similar to (4.2) would not work for $g > 1$ since then the range for a in (4.3) would be too large.

5. Proof of Theorem 1.5

In order to prove Theorem 1.5 we employ the same strategy as in our proof of Theorem 1.2; however the key ingredient in this case will be the more refined error term in the Chebotarev

density theorem as proved by Murty, Murty and Saradha [16] (see the second part of our Proposition 3.3). So, similarly as in the proof of Theorem 1.2, for each $m \in \mathbb{N}$ we define

$$\pi_{\mathcal{A},\mathcal{C}}(x;m) = \{p \leq x : p \text{ is a prime of good reduction such that } \sigma_p \in C_m\},$$

where C_m is a conjugacy class in $\mathrm{Gal}(\mathcal{A}_m/\mathbb{Q})$ satisfying conditions (i)-(ii) from Theorem 1.5. It suffices to prove that

$$\sum_{1\leq m\leq x} \pi_{\mathcal{A},\mathcal{C}}(x;m) = \left(\sum_{m=1}^{\infty} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O\left((x/\log x)^{\frac{4+3\delta+2\epsilon}{6+\delta}}\right) + O\left(x^{\frac{10+3\delta}{12+2\delta}}(\log x)^{\frac{4}{6+\delta}}\right),$$

for any $\epsilon > 0$. Indeed, as observed before, condition (ii) of Theorem 1.5 yields that $p \equiv a^2 \pmod m$ and thus $m \leq x$ as long as $x > a^2$; this justifies the range of the above sum. We will see later that actually we can reduce the above summation to the range $m \leq 2\sqrt{x}$.

For the range $1 \leq m \leq h(x) = (x/\log x)^{\frac{2}{\delta+6}}$, we use the second part of Proposition 3.3 (see also Corollary 3.4) and conclude

$$\pi_{\mathcal{A},\mathcal{C}}(x;m) = \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\cdot \mathrm{Li}(x) + O\left(x^{1/2}\log(mx)\cdot |C_m|^{1/2}\right). \tag{5.1}$$

We sum (5.1) for all m in the above range and get

$$\sum_{1\leq m\leq h(x)} \pi_{\mathcal{A},\mathcal{C}}(x;m) = \left(\sum_{1\leq m\leq h(x)} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O\left(x^{1/2}\log x \sum_{1\leq m\leq h(x)} |C_m|^{1/2}\right). \tag{5.2}$$

Now, we use condition (i) from Theorem 1.5 and therefore conclude that

$$\sum_{1\leq m\leq h(x)} |C_m|^{1/2} \ll h(x)^{\frac{\delta}{2}+1} \ll \left(\frac{x}{\log x}\right)^{\frac{2+\delta}{6+\delta}}.$$

Therefore the error term in (5.2) is bounded by

$$x^{\frac{1}{2}}\log x\cdot\left(\frac{x}{\log x}\right)^{\frac{2+\delta}{6+\delta}} = x^{\frac{10+3\delta}{12+2\delta}}(\log x)^{\frac{4}{6+\delta}}. \tag{5.3}$$

On the other hand, using (3.1) we know that

$$[\mathcal{A}_m:\mathbb{Q}] \gg m^{2-\epsilon} \text{ for any } \epsilon > 0.$$

So, $\frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]} \ll m^{-2+\delta+\epsilon}$, and thus

$$\sum_{1\leq m\leq h(x)} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]} = \sum_{m=1}^{\infty} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]} + O\left(h(x)^{-1+\delta+\epsilon}\right).$$

Therefore

$$\left(\sum_{1\leq m\leq h(x)} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) = \left(\sum_{m=1}^{\infty} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\right)\cdot \mathrm{Li}(x) + O\left((x/\log x)^{\frac{4+3\delta+2\epsilon}{6+\delta}}\right). \tag{5.4}$$

In conclusion, (5.2) together with estimates (5.3) and (5.4) yield

(5.5)
$$\sum_{1\leq m\leq h(x)}\pi_{\mathcal{A},\mathcal{C}}(x;m)=\left(\sum_{m=1}^{\infty}\frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\right)\cdot \mathrm{Li}(x)+O\left((x/\log x)^{\frac{4+3\delta+2\epsilon}{6+\delta}}\right)+O\left(x^{\frac{10+3\delta}{12+2\delta}}(\log x)^{\frac{4}{6+\delta}}\right).$$

Next we show that

$$\sum_{h(x)<m\leq x}\pi_{\mathcal{A},\mathcal{C}}(x;m)=O\left(x^{\frac{10+3\delta}{12+2\delta}}(\log x)^{\frac{4}{6+\delta}}\right). \tag{5.6}$$

First we note that by a similar reasoning as in the proof of Theorem 1.2, using condition (ii) of Theorem 1.5, it suffices to prove

$$\sum_{h(x)<m\leq x}\pi_{\mathcal{E},a}(x;m)=O\left(x^{\frac{10+3\delta}{12+2\delta}}(\log x)^{\frac{4}{6+\delta}}\right), \tag{5.7}$$

where $\pi_{\mathcal{E},a}(x;m)$ is the set of all primes $p\leq x$ such that their lifting of the Frobenius in $\mathrm{Gal}(\mathcal{E}_m/\mathbb{Q})$ corresponds to the scalar multiple $a\cdot \mathrm{Id}_2$ under an embedding of $\mathrm{Gal}(\mathcal{E}_m/\mathbb{Q})$ into $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Now, as proved in [6, Formula (2-2)] (see also [5, Formula (6)]), we have

$$4p=a_E(p)^2-\Delta_E(p)b_E(p)^2, \tag{5.8}$$

where $\Delta_E(p)$ is the discriminant of the ring of endomorphisms of the reduced elliptic curve E_p over the finite field $\mathbb{F}_p$. Furthermore, $a_E(p)$ is (as before) the unique integer satisfying

$$\#E_p(\mathbb{F}_p)=p+1-a_E(p),$$

and $b_E(p)$ is also an integer. Moreover, using [6, Theorem 2.1], if $\sigma_p=a\cdot \mathrm{Id}_2$ then

$$b_E(p)\equiv 0 \pmod m \text{ and } a_E(p)\equiv 2a \pmod m. \tag{5.9}$$

In particular, using also (5.8) we obtain that

$$m^2 \mid (4p-a_E(p)^2).$$

Since $|a_E(p)|\leq 2\sqrt{p}$ and $p\leq x$, we conclude that $m\leq 2\sqrt{x}$. This allows us to restrict the summation from both (5.7) and (5.6) over the smaller range $h(x)<m\leq 2\sqrt{x}$. Using (5.8) and (5.9) we conclude that

$$\sum_{h(x)<m\leq 2\sqrt{x}}\pi_{\mathcal{E},a}(x;m)\leq \sum_{h(x)<m\leq 2\sqrt{x}}\sum_{\substack{|c|\leq 2\sqrt{x}\\ c\equiv 2a \pmod m}} L(x;m,c),$$

where $L(x;m,c)$ counts the primes $p \le x$ such that $4p \equiv c^2 \pmod{m^2}$. Since $m \le 2\sqrt{x}$, we may employ the trivial bound $L(x;m,c) \ll \frac{x}{m^2}$ and thus conclude that

$$\begin{aligned}
&\sum_{h(x)<m\le 2\sqrt{x}} \pi_{\mathcal{E},a}(x;m) \\
\ll &\sum_{h(x)<m\le 2\sqrt{x}} \sum_{\substack{|c|\le 2\sqrt{x} \\ c\equiv 2a \pmod m}} \frac{x}{m^2} \\
\ll &\sum_{h(x)<m\le 2\sqrt{x}} \frac{x^{3/2}}{m^3} \\
\ll &\frac{x^{\frac{3}{2}}}{h(x)^2} = x^{\frac{10+3\delta}{12+2\delta}} (\log x)^{\frac{4}{6+\delta}}.
\end{aligned}$$

as desired for (5.6). Estimates (5.6) and (5.5) imply that

$$\sum_{1\le m\le x} \pi_{\mathcal{A},\mathcal{C}}(x;m) = \left(\sum_{m=1}^{\infty} \frac{|C_m|}{[\mathcal{A}_m:\mathbb{Q}]}\right) \cdot \mathrm{Li}(x) + O\left((x/\log x)^{\frac{4+3\delta+2\epsilon}{6+\delta}}\right) + O\left(x^{\frac{10+3\delta}{12+2\delta}} (\log x)^{\frac{4}{6+\delta}}\right),$$

for $\epsilon > 0$. Now if $\delta \in [0, 2/3)$ we choose $0 < \epsilon \le (2-3\delta)/4$ and if $\delta \in [2/3, 1)$ we choose $\epsilon = (1-\delta)/2$. In the former case (latter case) the second (first) error term is dominant. This finishes the proof of Theorem 1.5.

References

[1] A. Akbary and V. K. Murty, *An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p*, Indian J. Pure Appl. Math. **41** (1) (2010), 25–37.

[2] M. H. Baker and K. A. Ribet, *Galois theory and torsion points on curves*, Les XXIIèmes Journées Arithmetiques (Lille, 2001). J. Théor. Nombres Bordeaux **15** (2003), no. 1, 11–32.

[3] A. Brumer and K. Kramer, *Non-existence of certain semistable abelian varieties*. Manuscripta Math. **106** (2001), 291–304.

[4] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*. Math. Ann. **330** (2004), no. 3, 601–625.

[5] W. Duke, *Almost all reductions modulo p of an elliptic curve have a large exponent*, C. R. Acad. Sci. Paris, Ser. I **337** (2003), 689–692.

[6] W. Duke and Á. Tóth, *Splitting of primes in division field of elliptic curves*, Experiment. Math. **11** (2003), 555–565.

[7] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell-Lang problem*, J. Number Theory **129** (2009), 1392–1403.

[8] H. Halberstam, *Footnote to the Titchmarsh-Linnik divisor problem*, Proc. Amer. Math. Soc. **18** (1967), 187–188.

[9] M. Hindry and N. Ratazzi, *Torsion dans un produit de courbes elliptiques*, J. Ramanujan Math. Soc. **25** (2010), no. 1, 81–111.

[10] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006) 19–114.

[11] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem,* Algebraic Number Fields, A. Fröhlich (ed.), 1977, 409–464.

[12] J. V. Linnik, *The dispersion method in binary additive problems*, (Leningrad 1961), Transl. Math. monographs, Vol. 4, Amer. Math. Soc., Providence, R. I., 1963; Chapter 8.

[13] D. Masser, *Lettre à Daniel Bertrand du 10 novembre 1986.*

[14] J. Milne, *Abelian varieties*. Lecture notes available online at `http://www.jmilne.org/math/CourseNotes/AV.pdf`.

[15] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168.
[16] M. R. Murty, V. K. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, American J. Math. **110** (1988), 253-281.
[17] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers, third edition*, Springer, 2004.
[18] G. Rodriquez, *Sul problema dei divisori di Titchmarsh*, Boll. Un. Mat. Ital. (1965), 358–366.
[19] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. math. I. H. E. S. **54** (1981), 123–201.
[20] J.-P. Serre, *Résumé des cours de 1977–1978*, Ann. Collège de France (1978), 67–70, in Collected Papers, Vol. III, Springer, 1986.
[21] J.-P. Serre, *Résumé des cours de 1985–1986*, Ann. Collège de France (1986), 95–99, in Collected Papers, Vol. IV, Springer, 2000.
[22] J. H. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag, New York, 1986.
[23] E. C. Titchmarsh, *A divisor problem*, Rend. di. Palermo **54** (1931), 414–429.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada
E-mail address: amir.akbary@uleth.ca

Department of Mathematics, 1984 Mathematics Road, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
E-mail address: dghioca@math.ubc.ca