On the Titchmarsh divisor problem for abelian varieties

Cristian Virdol
Department of Mathematics
Yonsei University
cristian.virdol@gmail.com
July 3, 2017

Abstract
In this article we study Titchmarsh divisor problem in the context of abelian varieties. Under GRH, we obtain an asymptotic formula.

Keywords: Abelian varieties, Titchmarsh divisor problem, asymptotic formulas.

1 Introduction
For \( n \) a positive integer we denote by \( \tau(n) \) the number of positive divisors of \( n \). Throughout this paper \( p \) denotes a prime number. For a fixed \( a \in \mathbb{Z}_{>0} \), Titchmarsh in 1931 in [T] studied the sum

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

as \( x \to \infty \). More exactly he proved:

\textbf{Theorem 1.1.} Assume that the Generalized Riemann Hypothesis (GRH) holds for Dirichlet \( L \)-series. Then one has

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

as \( x \to \infty \).

Linnik in 1961 in [L] proved, by using his dispersion method, the above asymptotic formula unconditionally, and later, Rodriguez ([R]), and Halberstam...
proven, by using the Bombieri-Vinogradov theorem, the same formula also unconditionally. When $a = 1$ we have

$$
\sum_{p \leq x} \tau(p - 1) = \sum_{\substack{1 \leq m \leq x - 1}} \pi_1(x, m) = \sum_{m \geq 1} \pi_1(x, m),
$$

(1.1)

where $\pi_1(x, m) = |\{ p \leq x \mid p \text{ is prime and } p \equiv 1 \pmod{m}\}|$. Hence one can make the following interpretation of Titchmarsh’s result. For each positive integer $m$ and for each odd prime number $p$, one has that $p \equiv 1 \pmod{m}$ if and only if $p$ splits completely in $\mathbb{Q}(\mu_m)$, where $\mu_m$ is a primitive $m$-root of unity. Hence in (1.1) for each $m \in \mathbb{N}$, one counts the number of primes $p \leq x$ such that $p$ splits completely in $\mathbb{Q}(\mu_m)$. This interpretation of Titchmarsh’s result has lead the authors of [AG] to consider the analogue of Titchmarsh divisor problem in the context of abelian varieties, by replacing $\mathbb{Q}(\mu_m)$ above, by the fields $\mathbb{Q}(A[m])$, where $A[m]$ is the set of $m$-division points of an abelian variety $A$ over $\mathbb{Q}$. In this paper, under GRH, we study this analogue of Titchmarsh divisor problem ([T]) in the context of general abelian varieties over arbitrary number fields and obtain an asymptotic formula.

Consider $A$ an abelian variety defined over a number field $F$, of conductor $N$, and of dimension $r$, where $r \geq 1$ is an integer. Let $\Sigma_F$ be the set of finite places of $F$, and let $P_A$ be the set of primes $\wp \in \Sigma_F$ of good reduction for $A$, (i.e. $(N_F/Q\wp, N_F/QN) = 1$). For each positive integer $m$, we denote by $A[m]$ the set of $m$-torsion points of $A$.

Let $a$ be a positive integer. For $\wp \in P_A$ we define

$$
\tau_{A,a,F}(\wp) = \{ m \in \mathbb{N} \mid (m, N_F/Q\wp) = 1, \ \sigma_{\wp} \text{ acts on } A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r} \}
$$

through the scalar matrix $a \cdot I_{2r}$,

where $\sigma_{\wp}$ denotes a Frobenius element at $\wp$ in Gal($F(A[m])$/$F$).

We have that $F(\zeta_m) \subset F(A[m])$, and by using the Weil pairing on the abelian variety $A$ we get that the action of $\sigma_{\wp}$ on $F(\zeta_m)$ is given by $\zeta_m \mapsto \zeta_m^a$. Hence if $m \in \tau_{A,a,F}(\wp)$, then $N_F/Q\wp \equiv a^2 \pmod{m}$, and thus $|\tau_{A,a,F}(\wp)| < \infty$ for all $\wp \in P_A$ such that $N_F/Q\wp > a^2$ (in order to simplify our notations we assume from now on that $N_F/Q\wp > a^2$).

For $x \in \mathbb{R}$ we define

$$
f_{A,a,F}(x) := \sum_{\substack{\wp \in P_A \mid N_{F/Q\wp} \leq x}} |\tau_{A,a,F}(\wp)|.
$$

In this paper we prove the following result:

**Theorem 1.2.** Let $A$ be an abelian variety over a number field $F$ of dimension $r \geq 1$. Let $a$ be a positive integer. Assume that the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta functions of the division fields for $A$. Then we have

$$
f_{A,a,F}(x) = c_{A,F}li(x + O(x^{5/6}(\log x)^{2/3})�,\)
where
\[ c_{A,F} = \sum_{m=1}^{\infty} \frac{1}{[F(A[m]) : F]}. \]

Theorem 1.2 is the analog of Titchmarsh divisor problem in the context of abelian varieties (see the beginning of this Introduction and also [AG]). The asymptotic formula from Theorem 1.2 above represents an improvement of the main asymptotic formulas of [AG] where only the very particular case of abelian varieties defined over \( \mathbb{Q} \) that contain elliptic curves defined over \( \mathbb{Q} \) was considered. Also Theorem 1.2 is an improvement of the main theorems of [V], i.e. of Theorems 1.1, 1.2, and 1.3 of [V]: the asymptotic formulas from Theorem 1.2 above and Theorem 1.1 of [V] coincide only when \( r = 1 \), the asymptotic formulas from Theorem 1.2 above and from Theorem 1.2 of [V] coincide only when \( h = 1 \) (see Theorem 1.2 of [V] for the definition of \( h \)), and the asymptotic formula from Theorem 1.2 above and first asymptotic formula from Theorem 1.3 of [V] coincide only when \( h = 1 \) (see Theorem 1.3 of [V] for the definition of \( h \)). In order to prove Theorem 1.2, and improve the results from [AG] and [V], we make use of the Lemmas 2.3, 2.4, and 2.5, and of Chebotarev density theorem.

We remark that in Theorem 1.3 of [V] in some cases, i.e. when \( h = e = 1 \) (see Theorem 1.3 of [V] for notations), one obtains by a different method a better asymptotic formula than in Theorem 1.2 above. One can expect, as in the case of the error term from Riemann Hypothesis, that the best possible error term in Theorem 1.2 above should be \( O(x^{1/2} \log x^A) \), for some \( A > 0 \), but we are not able to prove this result in this paper!

## 2 General abelian varieties

For \( F \) a number field, we denote \( G_F := \text{Gal}({\overline{F}}/F) \). Let \( A \) be an abelian variety over \( F \) of dimension \( r \geq 1 \), and of conductor \( \mathcal{N} \). Let \( \Sigma_F \) be the set of finite places of \( F \), and for \( \wp \) a prime of \( F \), let \( \mathbb{F}_\wp \) be the residue field at \( \wp \). Let \( \mathcal{P}_A \) be the set of primes \( \wp \in \Sigma_F \) of good reduction for \( A \), (i.e. \( (N_F/Q\wp, N_F/Q\mathcal{N}) = 1 \)). For \( \wp \in \mathcal{P}_A \), we denote by \( \bar{A} \) the reduction of \( A \) at \( \wp \). For \( m \geq 1 \) an integer, let \( A[m] \) be the \( m \)-division points of \( A \) in \( \bar{F} \). Then
\[
A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}.
\]

If \( F(A[m]) \) is the field obtained by adjoining to \( F \) the elements of \( A[m] \), then we have a natural injection
\[
\Phi_m : \text{Gal}(F(A[m])/F) \hookrightarrow \text{Aut}(A[m]) \simeq \text{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}).
\]

We denote \( G_m := \text{Im} \Phi_m(\text{Gal}(F(A[m])/F)) \). Define
\[
n(m) := |G_m| = [F(A[m]) : F].
\]
For a rational prime $l$, let

$$T_l(A) = \lim_{m \to \infty} A[l^m],$$

and $V_l(A) = T_l(A) \otimes \mathbb{Q}$. The Galois group $G_F$ acts on

$$T_l(A) \simeq \mathbb{Z}_l^{2r},$$

where $\mathbb{Z}_l$ is the $l$-adic completion of $\mathbb{Z}$ at $l$, and also on $V_l(A) \simeq \mathbb{Q}_l^{2r}$, and we obtain a representation

$$\rho_{A,l} : G_F \to \text{Aut}(T_l(A)) \simeq \text{GL}_{2r}(\mathbb{Z}_l) \subset \text{Aut}(V_l(A)) \simeq \text{GL}_{2r}(\mathbb{Q}_l),$$

which is unramified outside $lN_{F/\mathbb{Q}}N$. If $\wp \in \mathcal{P}_A$, let $\sigma_{\wp}$ be the Artin symbol of $\wp$ in $G_F$, and let $l$ be a rational prime satisfying $(l, N_{F/\mathbb{Q}}\wp) = 1$. We denote by $P_{A,\wp}(X) = X^{2r} + a_1 A(\wp)X^{2r-1} + \ldots + a_{2r-1} A(\wp)X + N_{F/\mathbb{Q}}\wp^r \in \mathbb{Z}[X]$ the characteristic polynomial of $\sigma_{\wp}$ on $T_l(A)$. Then $P_{A,\wp}(X)$ is independent of $l$.

One can identify $\mathbb{Z}_l$ with $\mathbb{Z}_{l^G}$, and we get that $T_l(A)$ is the same as the action of the Frobenius $\pi_{\wp}$ of $A$ on $T_l(A)$. We know (Riemann Hypothesis) that $P_{A,\wp}(X) = (X - x_{1,\wp})(X - x_{1,\wp})\cdots (X - x_{r,\wp})(X - x_{r,\wp})$, where $|x_{i,\wp}| = N_{F/\mathbb{Q}}\wp^{1/2}$ for $i = 1, \ldots, r$.

We know (see for example page 195 of [SI], and Lemma 1 of [BK]):

**Lemma 2.1.** Let $A$ be an abelian variety defined over a number field $F$, of dimension $r$, of conductor $N$, and let $a$ and $m$ be positive integers. Then

1. The extension $F(A[m])/F$ is ramified only at places dividing $mN$.
2. $F(\zeta_m) \subseteq F(A[m])$. Hence if $\sigma_{\wp}$, for $\wp \in \mathcal{P}_A$ such that $(N_{F/\mathbb{Q}}\wp, m) = 1$, acts on $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}$ through the scalar matrix $a \cdot I_{2r}$, from the Weil pairing we get that $m|N_{F/\mathbb{Q}}\wp - a^2$.

We know (see (3.1) of [AG]):

**Lemma 2.2.** Let $A$ be an abelian variety defined over a number field $F$. Let $\epsilon > 0$. Then, with the same notations as above, we have

$$|G_m| \gg m^{2-\epsilon}.$$

**Lemma 2.3.** Let $A$ be an abelian variety over a number field $F$, of conductor $N$. Let $\wp \in \mathcal{P}_A$, and let $p$ be the rational prime below $\wp$. Let $m$ be an integer relatively prime to $p$, and let $a$ be a positive integer. If $\sigma_{\wp}$ acts on $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}$ through the scalar matrix $a \cdot I_{2r}$, then $\frac{x_{i,\wp} - a}{m}$ is an algebraic integer for any $i = 1, \ldots, r$.

**Proof:** Let $l|m$ be a rational prime, and let $m(l)$ be the largest natural number such that $l^{m(l)}|m$. Since $\sigma_{\wp}$ acts on $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}$ through the scalar matrix $a \cdot I_{2r}$, we know that $A(F(\wp))[m] \subset \text{Ker}(\pi_{\wp} - a)$. Hence in particular $A(F(\wp))[l^{m(l)}] \subset \text{Ker}(\pi_{\wp} - a)$, and we get that $\rho_{A,l}(\sigma_{\wp}) = aI_{2r} + l^{m(l)}B_l$, where $B_l \in M_{2r}(\mathbb{Z}_l)$. Thus $(mX - (x_{1,\wp} - a))(mX - (x_{1,\wp} - a))\cdots (mX - (x_{r,\wp} - a))$, and

$$...$$
$(x_{r,p} - a) = P_{A,p}(mX + a) = \det((mX + a)I_{2r} - \rho_{A,p}(\sigma_p)) = \det(mXI_{2r} - \frac{1}{r}m(I)B_1)$, and we get trivially that $(X - \frac{r_{1,p} - a}{m})(X - \frac{r_{2,p} - a}{m})\cdots(X - \frac{r_{r,p} - a}{m})) = Z[X]$, and hence $x_{i,a} = \frac{a}{m}$ is an algebraic integer for any $i = 1, \ldots, r$. 

We define $y_{i,p,a} := \frac{x_{i,p} - a}{m}$, for $i = 1, \ldots, r$. Then, if $\sigma_p$ acts on $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}$ through the scalar matrix $a \cdot I_{2r}$, from the proof of Lemma 2.3, we know that $(X - y_{1,p,a})(X - y_{1,p,a})\cdots(X - y_{r,p,a})(X - \bar{y}_{r,p,a}) \in \mathbb{Z}[X]$. Hence $N_{F/Q}\psi = x_{i,p}\bar{x}_{i,p} = (a + my_{i,p,a})(a + \bar{y}_{i,p,a}) = a^2 + am(y_{i,p,a} + \bar{y}_{i,p,a}) + m^2y_{i,p,a}\bar{y}_{i,p,a}$. Thus

$$rN_{F/Q}\psi = a^2r + amb_{1,A}(\psi)_{m,a} + m^2b_{2,A}(\psi)_{m,a},$$

where $b_{1,A}(\psi)_{m,a} := \sum_{i=1}^{r}(y_{i,p,a} + \bar{y}_{i,p,a}) \in \mathbb{Z}$, and $b_{2,A}(\psi)_{m,a} := \sum_{i=1}^{r}y_{i,p,a}\bar{y}_{i,p,a} \in \mathbb{Z}$.

**Lemma 2.4.** With the same notations as in Lemma 2.3, if $\sigma_p$ acts on $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r}$ through the scalar matrix $a \cdot I_{2r}$, then

$$m^2|rN_{F/Q}\psi| > a \cdot a_{1,A}(\psi) + a^2r.$$

**Proof:** From above we know that

$$m^2|rN_{F/Q}\psi| > a^2r - amb_{1,A}(\psi)_{m,a} = rN_{F/Q}\psi + a \cdot a_{1,A}(\psi) + a^2r. \blacksquare$$

**Lemma 2.5.** We have

$$|a_{1,A}(\psi)| \leq 2rN_{F/Q}\psi^{\frac{1}{2}}.$$

**Proof:** Since $a_{1,A}(\psi) = \sum_{i=1}^{r}(x_{i,p} + \bar{x}_{i,p})$, and $|x_{i,p}| = N_{F/Q}\psi^{\frac{1}{2}}$, for $i = 1, \ldots, r$, we are done. \(\blacksquare\)

### 3 Chebotarev density theorem

Let $L/F$ be a Galois extension of number fields, with Galois group $G$. We denote by $n_L$ and $d_L$ the degree and the discriminant of $L/Q$, and by $d_F$ the discriminant of $F/Q$. Let $\mathcal{P}(L/F)$ be the set of rational primes $p$ which lie below places of $F$ which ramify in $L/F$.

We know (see page 130 of [S]):

**Lemma 3.1.** If $L/F$ is Galois extension of number fields, then

$$\log d_L \leq |G| \log d_F + n_L(1 - \frac{1}{|G|}) \sum_{p \in \mathcal{P}(L/F)} \log p + n_L \log |G|.$$
Using the same assumptions as above, let $C$ be a conjugacy class in $G$. For a positive real number $x$, let

$$\pi_C(x, L/F) := \left| \{ \wp \in \Sigma_{F} \mid N_{F/Q} \wp \leq x, \ \wp \text{ unramified in } L/F, \ \sigma_{\wp} \in C \} \right|,$$

where $\sigma_{\wp}$ is a Frobenius element at $\wp$. The Chebotarev density theorem says that

$$\pi_C(x, L/F) \sim \frac{|C|}{|G|} \log x,$$

and moreover we know (see Theorem 4 from page 144 of [S]):

**Lemma 3.2.** Let $L/F$ be a Galois extension of number fields. If the Dedekind zeta function of $L$ satisfies the GRH, then

$$|\pi_C(x, L/F) - \frac{|C|}{|G|} \log x| \ll \frac{|C|}{|G|} x^{\frac{1}{2}} (\log x + \frac{1}{|G|} \log |d_L|),$$

for every $x \geq 2$, where the implied $O$-constant is absolute.

### 4 The proof of Theorem 1.2

We want to estimate the sum

$$f_{A,a,F}(x) := \sum_{\wp \in \mathcal{P}_A \mid N_{F/Q} \wp \leq x} |\tau_{A,a,F}(\wp)|.$$

If $m \in \tau_{A,a,F}(\wp)$, then $m^{2r}|P_{A,\wp}(a) < (1 + a)^{2r}x^r$. Hence it is sufficient to consider only positive integers $m$ satisfying $m \leq (1 + a)x^{\frac{1}{2}}$.

Thus

$$\sum_{\wp \in \mathcal{P}_A \mid N_{F/Q} \wp \leq x} |\tau_{A,a,F}(\wp)| = \sum_{1 \leq m \leq (1 + a)x^{\frac{1}{2}}} \pi_a(x, F(A[m])/F),$$

where

$$\pi_a(x, F(A[m])/F) := \left| \{ \wp \in \mathcal{P}_A \mid N_{F/Q} \wp \leq x, \ (m, N_{F/Q} \wp) = 1, \ \sigma_{\wp} \text{ acts on } A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r} \text{ through the scalar matrix } a \cdot I_{2r} \} \right|,$$

If $y = y(x)$ is a real number with $y \leq (1 + a)x^{\frac{1}{2}}$ ($y$ will be chosen later), then

$$f_{A,a,F}(x) = \sum_{m \leq (1 + a)x^{\frac{1}{2}}} \pi_a(x, F(A[m])/F) = \sum_{m \leq y} \pi_a(x, F(A[m])/F) + \sum_{y < m \leq (1 + a)x^{\frac{1}{2}}} \pi_a(x, F(A[m])/F).$$
= main + error.  \hspace{1cm} (4.1)

From Lemmas 3.2 and 2.1, under GRH, we get

\[
\begin{align*}
\text{main} &= \sum_{m \leq y} \frac{1}{\nu(m)} \text{li} \ x + \sum_{m \leq y} O(x^{1/2} \log(mN_{F/Q}N_{x})) \\
&= \sum_{m \leq y} \frac{1}{\nu(m)} \text{li} \ x + O(yx^{1/2} \log(N_{F/Q}N_{x})). \\
\end{align*}
\]

(4.2)

Now we estimate the error. For each \( b \in \mathbb{Z} \), with \(|b| \leq 2rx^{1/2}\), and for each positive integer \( m \) we define

\[ S_{b,a}(m) := \{ \wp \in \mathcal{P}_A \mid N_{F/Q}\wp \leq x, \ a_{1,A}(\wp) = b, \]
\[ \sigma_\wp \text{ acts on } A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2r} \text{ through the scalar matrix } a \cdot I_{2r} \}. \]

Then, because from Lemma 2.5 we know that \(|a_{1,A}(\wp)| \leq 2rx^{1/2}\), we obtain

\[
\text{error} \leq \sum_{y < m \leq (1+\alpha)x^{1/2}} \sum_{b \in \mathbb{Z}} |S_{b,a}(m)|. 
\]

From Lemma 2.4 we know that for each \( \wp \in S_{b,a}(m) \) we have \( m^2|\sigma_\wp|N_{F/Q}\wp + a \cdot a_{1,A}(\wp) + a^2r \), and from Lemma 2.1 we know that for each \( \wp \in S_{b,a}(m) \) we have \( m|N_{F/Q}\wp - a^2 \), and hence we get also that for each \( \wp \in S_{b,a}(m) \) we have \( m|a \cdot a_{1,A}(\wp) + 2a^2r \). Therefore

\[
\sum_{y < m \leq (1+\alpha)x^{1/2}} \sum_{b \in \mathbb{Z}} |S_{b,a}(m)| \
\leq \sum_{y < m \leq (1+\alpha)x^{1/2}} \sum_{b \in \mathbb{Z}} \sum_{|b| \leq 2rx^{1/2}} \sum_{\wp \in \mathcal{P}_A \atop N_{F/Q}\wp \leq x, a_{1,A}(\wp) = b} m^2|\sigma_\wp|N_{F/Q}\wp + a^2r + a \cdot a_{1,A}(\wp) \
\ll \sum_{y < m \leq (1+\alpha)x^{1/2}} \sum_{|b| \leq 2rx^{1/2}} (\frac{x}{m^2} + 1) \
\ll \sum_{y < m \leq (1+\alpha)x^{1/2}} (\frac{x}{m^2} + 1)(\frac{\sqrt{x}}{m} + 1) \
\ll \frac{x^{3/2}}{y^2}. 
\]
From above we get

\[ f_{A,a,F}(x) = \sum_{m \leq y} \frac{1}{n(m)} \text{li} x + O(y x^{\frac{2}{3}} \log x) + O\left(\frac{x^{\frac{3}{2}}}{y}\right). \]

We choose \( y \) such that \( x^{\frac{2}{3}} y \log x = \frac{x^{\frac{3}{2}}}{y^2} \), i.e.

\[ y := \frac{x^{\frac{4}{3}}}{(\log x)^\frac{2}{3}}. \]

Then

\[ f_{A,a,F}(x) = \sum_{m \leq y} \frac{1}{n(m)} \text{li} x + O(x^{\frac{5}{6}} (\log x)^{\frac{3}{2}}). \]

From Lemma 2.2, with \( \epsilon = \frac{1}{2} \), we obtain

\[ \sum_{m > y} \frac{1}{n(m)} \ll \sum_{m > y} \frac{1}{m^{\frac{3}{2}}} \ll \frac{1}{y^{\frac{1}{2}}}. \]

Since \( y := \frac{x^{\frac{4}{3}}}{(\log x)^\frac{2}{3}} \), we get

\[ f_{A,a,F}(x) = c_{A,F} \text{li} x + O(x^{\frac{5}{6}} (\log x)^{\frac{3}{2}}), \]

and Theorem 1.2 is proved. ■

References


