The strong form of Artin’s primitive root
conjecture (1927) for abelian varieties under GRH

Cristian Virdol
Department of Mathematics
Yonsei University
cristian.virdol@gmail.com

November 24, 2017

Abstract
In this paper, under GRH, we prove the strong form of Artin’s primitive
root conjecture (1927) for abelian varieties. Artin’s primitive root
conjecture (1927) states that, for any integer $a \neq \pm 1$ or a perfect
square, there are infinitely many primes $p$ for which $a$ is a primitive root (mod $p$),
and an asymptotic formula for such primes is satisfied (this conjecture
is not known for any specific $a$; not even the infinity part of Artin’s
conjecture is not known for any specific $a$). We remark that, under GRH,
the strong form of Artin’s primitive root conjecture (1927) was proved in:

(1967), 209-220.

Unconditionally the infinity part of Artin’s primitive root conjecture
(1927) for abelian varieties was proved in:

56 (2016), no. 4, 737-743.

Keywords: Abelian varieties, Artin’s conjecture, primitive-cyclic points.

1 Introduction
Let $A$ be an abelian variety defined over $\mathbb{Q}$, of conductor $N$, and of dimension
$r$, where $r \geq 1$ is an integer. Let $\Sigma_{\mathbb{Q}}$ be the set of finite places of $\mathbb{Q}$, and for $p$
a rational prime, let $\mathbb{F}_p$ be the residue field at $p$. Let $\mathcal{P}_A$ be the set of primes
$p \in \Sigma_{\mathbb{Q}}$ of good reduction for $A$, (i.e. $(p, N) = 1$). For $p \in \mathcal{P}_A$, we denote by $\bar{A}$
the reduction of $A$ at $p$.

We have that $\bar{A}(\mathbb{F}_p) \subseteq \bar{A}[m](\mathbb{F}_p) \subseteq (\mathbb{Z}/m\mathbb{Z})^{2r}$ for any positive integer $m$
satisfying $|\bar{A}(\mathbb{F}_p)||m$. Hence

$$\bar{A}(\mathbb{F}_p) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z},$$

(1.1)
where \( s \leq 2r, m_i \in \mathbb{Z}_{\geq 2}, \) and \( m_i | m_{i+1} \) for \( 1 \leq i \leq s - 1. \) Each \( \mathbb{Z}/m_i \mathbb{Z} \) is called a cyclic component of \( A(\mathbb{F}_p). \) If \( s < 2r, \) we say that \( A(\mathbb{F}_p) \) has at most \((2r - 1)\) cyclic components (thus if \( r = 1 \) this means that \( A(\mathbb{F}_p) \) is cyclic).

Assume that \( \text{rank}_A A \geq g \) where \( g \) is a positive integer, and let \( a_1, \ldots, a_g \in A(\mathbb{Q}) \) be linearly independent points (so in particular \( a_i \), for \( i = 1, \ldots, g, \) has infinite order). Let \( \bar{a}_i \), for \( i = 1, \ldots, g, \) be the reduction of \( a_i (\mod p) \), and let \( \langle \bar{a}_1, \ldots, \bar{a}_g \rangle \) be the subgroup of \( A(\mathbb{F}_p) \) generated by \( \bar{a}_1, \ldots, \bar{a}_g \). From above we know that \( A(\mathbb{F}_p) = \langle \bar{a}_1, \ldots, \bar{a}_g \rangle \) has at most \( 2r \) cyclic components. We call \( a := (a_1, \ldots, a_g) \) a primitive-cyclic tuple for \( p \) if \( A(\mathbb{F}_p) = \langle \bar{a}_1, \ldots, \bar{a}_g \rangle \) has at most \( 2r - 1 \) cyclic components.

For \( x \in \mathbb{R}, \) define
\[
f_{A,a}(x) = |\{ p \in \mathcal{P}_A | p \leq x, A(\mathbb{F}_p) = \langle \bar{a}_1, \ldots, \bar{a}_g \rangle \}|,
\]
and
\[
f'_{A,a}(x) = |\{ p \in \mathcal{P}_A | p \leq x, A(\mathbb{F}_p) = \langle \bar{a}_1, \ldots, \bar{a}_g \rangle \}|.
\]
Let \( \mathbb{Q}(A[m]) \) be the field obtained by adjoining to \( \mathbb{Q} \) the \( m \)-division points \( A[m] \) of \( A, \) and let \( \mathbb{Q}(A[m], m^{-1}a) := \mathbb{Q}(A[m], m^{-1}a_1, \ldots, m^{-1}a_g) \) be the field obtained by adjoining to \( \mathbb{Q} \) the \( m \)-division points \( A[m] \) of \( A, \) and \( m^{-1}a_1, \ldots, m^{-1}a_g \in A(\mathbb{Q}). \)

In this paper, in particular, we prove the following results (for all details regarding the most general results see the remarks in this introduction after the main theorems; the condition \( \mathbb{Q}(A[2]) = \mathbb{Q} \) that appears in Theorem 1.1 below is never used in this paper and so it can be removed altogether):

**Theorem 1.1.** Assume that \( \mathbb{Q}(A[2]) = \mathbb{Q}. \) Let \( A \) be an abelian variety over \( \mathbb{Q} \) of dimension \( r \geq 1. \) Assume that \( \text{rank}_A A \geq g \) where \( g \) is a positive integer, and let \( a_1, \ldots, a_g \in A(\mathbb{Q}) \) be linearly independent points. Define \( a := (a_1, \ldots, a_g). \) Assume that the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta functions of the fields \( \mathbb{Q}(A[m], m^{-1}a) := \mathbb{Q}(A[m], m^{-1}a_1, \ldots, m^{-1}a_g) \) for all integers \( m. \) Then we have
\[
f_{A,a}(x) = c_{A,a} li x + O(x^{\frac{4r+4r-g}{4r+2r}} (\log x)^{\frac{2r+4r-g}{2r+2r}}),
\]
where \( li x := \int_2^x \frac{1}{\log t} dt \), and
\[
c_{A,a} = \sum_{m=1}^{\infty} \mu(m) \frac{\mu(m)}{[\mathbb{Q}(A[m], m^{-1}a) : \mathbb{Q}]},
\]
where \( \mu(\cdot) \) is the Möbius function.

**Theorem 1.2.** Assume that \( \mathbb{Q}(A[2]) = \mathbb{Q}. \) Under the same assumptions as in Theorem 1.1, we have that \( c_{A,a} \neq 0 \) if and only if \( \mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}. \) Moreover if \( \mathbb{Q}(A[2], 2^{-1}a) = \mathbb{Q}, \) then the function \( f_{A,a}(x) \) is bounded.
Let $\mathbf{a} \in \mathbb{Z}$, $\mathbf{a} \neq 0$. Assume that $\mathbf{a}$ is linearly independent in the multiplicative group $\mathbb{Q}^\times$, i.e. that $\mathbf{a} \neq \pm 1$. For $x \in \mathbb{R}$, define

$$f_\mathbf{a}(x) := |\{p \mid p \leq x, \langle \mathbf{a} \rangle = \mathbb{F}_p^\times\}|.$$

Note that Theorem 1.1 and 1.2 are precise analogues of the following two theorems, due to Hooley [H]:

**Theorem 1.3.** Trivially $\mathbb{Q}(\pm 1) = \mathbb{Q}$. Let $\mathbf{a} \in \mathbb{Z}$, $\mathbf{a} \neq 0$. Assume that $\mathbf{a}$ is linearly independent in the multiplicative group $\mathbb{Q}^\times$, i.e. that $\mathbf{a} \neq \pm 1$. Assume that the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta functions of the fields $\mathbb{Q}(\sqrt{\mathbf{1}}, \sqrt{\mathbf{a}})$ for all positive integers $m$. Then

$$f_\mathbf{a}(x) = c_\mathbf{a} li x + O\left(\frac{x \log \log x}{\log^2 x}\right),$$

where

$$c_\mathbf{a} = \sum_{m=1}^\infty \frac{\mu(m)}{|\mathbb{Q}(\sqrt{\mathbf{1}}, \sqrt{\mathbf{a}}) : \mathbb{Q}|}.$$

**Theorem 1.4.** Trivially $\mathbb{Q}(\pm 1) = \mathbb{Q}$. Under the same assumptions as in Theorem 1.3, we have that $c_\mathbf{a} \neq 0$ if and only if $\mathbf{a} \neq a$ a perfect square, or equivalently if and only if $\mathbb{Q}[1\{2\}, 2^{-1}a \neq \mathbb{Q}$. Moreover if $\mathbb{Q}[1\{2\}, 2^{-1}a = \mathbb{Q}$, then the function $f_\mathbf{a}(x)$ is bounded.

We prove also this theorem:

**Theorem 1.5.** If $\mathbb{Q}(A[2], 2^{-1}a) = \mathbb{Q}$, then the function $f_{A,a}(x)$ is bounded. Hence if $\mathbb{Q}(A[2], 2^{-1}a) = \mathbb{Q}$, then Theorem 5 and its Corollary of [GM] are false, and Theorems 2, 3, and 4 of [GM] are also false.

We remark that Theorem 1.1 holds true for abelian varieties $A$ defined over arbitrary number fields $F$ (so throughout Theorem 1.1 one can replace $\mathbb{Q}$ by $F$; the same is true for Theorem 1.3). Then, in Theorem 1.1 one should replace $f_{A,a}(x)$ by $f_{A,a,F}(x)$, and $c_{A,a} = \sum_{m=1}^\infty \frac{\mu(m)}{|\mathbb{Q}(A[m], m^{-1}a) : \mathbb{Q}|}$, by $c_{A,a,F} = \sum_{m=1}^\infty \frac{\mu(m)}{|\mathbb{F}(A[m], m^{-1}a,F) : \mathbb{F}|}$, to indicate the dependence of $F$. Now regarding Theorem 1.2, we remark that if $F(A[q], q^{-1}a) = F$, for some rational prime $q$, then because $c_{A,a,F} = \sum_{m=1}^\infty \frac{\mu(m)}{|\mathbb{F}(A[m], m^{-1}a,F) : \mathbb{F}|}$, which is a sum over square-free positive integers $m$, one gets trivially that $c_{A,a,F} = 0$. In general one should have $c_{A,a,F} \neq 0$ if and only if $F(A[q], q^{-1}a) \neq F$ for every rational prime $q$ (note that for $q$ sufficiently large, we have that $F(A[q], q^{-1}a) \neq F$ because $F(A[q], q^{-1}a) \supseteq F(A[q]) = F(\zeta_q)$, where $\zeta_q$ is the $q$-th root of unity (see for example Lemma 1 of [BK])). So when $F = \mathbb{Q}$ we actually have that $F(A[q], q^{-1}a) \neq F$ for any $q \geq 3$ prime, and this explains the statement of Theorem 1.2, and also of Theorem 1.4. We remark that if $\mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) = \mathbb{Q}$, then for all odd rational primes $p$ of good reduction for $A$, we have $\overline{A}[2](\overline{F}_p) \subset \overline{A}(F_p) \sim (\mathbb{Z}/2\mathbb{Z})^{2g}$, and thus in this case $f_{A,a}(x)$ is bounded.
Hence if $Q(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) = Q$, the function $f'_{A,a}(x)$ is bounded, and thus in this case $f'_{A,a}(x)$ cannot have positive density as it is FALSELY! claimed in Theorem 5 and its Corollary of [GM], and also in Theorems 2, 3, and 4 of [GM1], and we are done with the proof of Theorem 1.5 above.

Here is a brief history of Artin’s primitive root conjecture (1927), and of Artin’s primitive root conjecture (1927) for abelian varieties from this paper.

It was Gauss who in a section of *Disquisitiones Arithmeticae*, considered the problem of determining the primes $p$ for which a given number $a$ is a primitive root, modulo $p$, for the particular case $a = 10$. On September 27, 1927, according to Helmut Hasse’s diary, Emil Artin formulated his celebrated conjecture. This conjecture was proved in 1967, under GRH, by Hooley ([H]), in its strong form for all integers $a \neq \pm 1$ or a perfect square (see Theorems 1.3 and 1.4 above). Unconditionally Artin’s conjecture is not known to be true for any specific $a$.

Now let’s describe the results in the literature about Artin’s primitive root conjecture (1927) for abelian varieties. With the same notations as above, assume that $A = E$ is an elliptic curve curve defined over $\mathbb{Q}$, and assume also that $g = 0$. In 1976, Serre proved (see Theorem 1.1 of [S], and also Theorem 2 of [MU]), under GRH, that if $E$ is a non-CM elliptic curve, then

$$f_{E,\mathbb{Q}}(x) := f_{E,\mathbb{Q},a}(x) = c_E \text{li} x + o\left(\frac{x}{\log x}\right),$$

where $c_E := c_{E,a}$. Moreover, Serre proved that $c_E > 0$ if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. In 2004, the error term in Serre’s estimate was improved by Cojocaru and Murty in Theorem 1.1 of [CM], where they obtained the formula

$$f_{E,\mathbb{Q}}(x) = c_E \text{li} x + O\left(x^{5/6}(\log x)^{2/3}\right).$$

Moreover, when $E$ is a CM elliptic curve in Theorem 1.2 of [CM] it was obtained a better asymptotic formula:

$$f_{E,\mathbb{Q}}(x) = c_E \text{li} x + O\left(x^{3/4}(\log x)^{1/2}\right).$$

The results from [CM] were extended in [AG] and [FM] to the very particular case when our abelian variety $A$ defined over $\mathbb{Q}$ contains an abelian subvariety $E$ of dimension one also defined over $\mathbb{Q}$ (see Theorem 2 of [AG], and also the last sentence of §1.1 of [FM] where the authors say that they can prove their results only for ”abelian varieties defined over $\mathbb{Q}$ which have a one-dimensional subvariety which is also defined over $\mathbb{Q}$”). Finally, the results regarding Serre’s cyclicity question from [S], [CM], [AG], and [FM] were extended to arbitrary abelian varieties defined over number fields in [V1]. As in Theorem 1.1 of [V1], one can prove in Theorem 1.1 above the following asymptotic formula (so the assumption $\mathbb{Q}(A[2]) = \mathbb{Q}$ that appear in Theorem 1.1 is never used):

$$f_{A,a}(x) = c_{A,a} \text{li} x + O\left(x^{5/6}(\log x)^{2/3}\right).$$
In order to prove Theorem 1.1, we make use of Chebotarev density theorem, Lemmas 2.1, 2.2, 2.3, 2.4, 2.5, the principle of inclusion-exclusion (i.e. formula 4.1), the decomposition 4.2, and of the inequality (4.4). In order to prove Theorem 1.2 we make use of the main Theorem of [V], i.e. of Lemma 2.6 below, in which we proved unconditionally the infinity part of Artin’s primitive root conjecture for abelian varieties, and of the asymptotic formula from Theorem 1.1. So the best possible error term that we could prove in Theorem 1.1 for general abelian varieties is $O\left(\frac{x^{5/6} (\log x)^{2/3}}{}\right)$ for $g \geq 0$ (as in Theorem 1.1 of [V1] where we made use of Lemmas 2.5, 2.6, and 2.7 of [V1], and a similar proof as in §4 of [V1] goes through), or $O\left(x^{\frac{4r+4g+8}{2gr+r-1}} (\log x)^{\frac{2gr+r-1}{2gr+r-1}}\right)$ for $g \geq 1$ as we proved in this paper making use of Lemma 2.5 and of the inequality (4.5). We remark that because of formula (4.1) below, Artin’s primitive root conjecture for abelian varieties can be considered as the infinite version of Chebotarev Density Theorem, hence one can expect that for general abelian varieties as in the case of Riemann Hypothesis, the best possible error term in Theorem 1.1 should be (see for example the Conjecture on page 16 of [MON])

$$f_{A,a}(x) = c_{A,a}x \log x + O\left(x^{\frac{1}{2}}(\log x)^{B}\right),$$

for any $B > -1$, but we are not able to prove this result in this paper. The same remark holds for Theorem 1.3.

Similar questions were considered in [GM] and [GM1] which were based on a short paper [LT] of Lang and Trotter from 1977, where the authors were able to prove in Theorem 1 of [GM] an asymptotic formula as in Theorems 1.1 and 1.3 above for the very particular case of CM elliptic curves $E$ defined over $\mathbb{Q}$ and ONLY for the ordinary primes of $E$. The methods of [GM] cannot be used to obtain an asymptotic form of Theorem 1 of [GM] for any non-CM elliptic curve, or for any simple abelian variety of dimension at least 2; moreover, the condition $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ imposed in Theorem 2 of [GM] (see also the subsequent remark) is necessary (in the classical Artin’s conjecture we have trivially that $\mathbb{Q}(\pm 1) = \mathbb{Q}$). These limitations arise from the fact that the statement considered in [GM] is not the correct analogue of Artin’s conjecture, despite numerous claims to the contrary (e.g., see page 63 of [MU1], the introduction of [C], the ‘elliptic Artin’ section of [MO], the introduction of [AGM], etc.). By contrast, as in Theorem 1.1 of [V], in Theorem 1.1 and Theorem 1.2 one does not have to assume that $g \geq 1$, and (at the expense of changing the error term) one can replace the assumption $\mathbb{Q}(A[2]) = \mathbb{Q}$ and $\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$ with the assumption $\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$ contains a nontrivial abelian extension of $\mathbb{Q}$’ as in Remark 3.1 of [V].

So this is the statement of Artin’s primitive root conjecture: in the case of the multiplicative group we have a cyclic component that we want to kill with an element $a \neq \pm 1$, or a perfect square, and in the case of abelian varieties of dimension $r$ we have $2r$ cyclic components and we want to kill one of them with an element $a \neq \pm 1$, or a perfect square; and this is what we are doing in our paper! We have Kummer theory for the multiplicative group and also for general abelian varieties, we have RH for the multiplicative group and also for general abelian varieties, we have BSD for elliptic curves and also for general
abelian varieties, and we have Artin’s conjecture for the multiplicative group
and also for general abelian varieties, and this is EXACTLY what we prove,
under GRH, in this paper! We remark that there is a paper [HE] with the title:
”Artin’s conjecture for primitive roots” in which the author does not prove
Artin’s conjecture for any specific $a$.

2 General abelian varieties

In this section we follow very closely [V]. For $F$ a number field, we denote
$G_F := \text{Gal}(\bar{F}/F)$. Let $A$ be an abelian variety over $\mathbb{Q}$, of dimension $r \geq 1$, and
of conductor $N$. Let $\mathcal{P}_A$ be the set of primes $p \in \Sigma_\mathbb{Q}$ of good reduction for $A$
(i.e. $(p, N) = 1$). For $m \geq 1$ an integer, let $A[m]$ be the $m$-division points of $A$
in $\bar{\mathbb{Q}}$. Let $\mathbb{Q}(A[m])$ is the field obtained by adjoining to $\mathbb{Q}$ the elements of $A[m]$. We have

$$A[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2r}.$$ 

Assume that $\text{rank}_{\mathbb{Q}} A \geq g$ where $g$ is a positive integer, and let $a_1, \ldots, a_g \in A(\mathbb{Q})$ be linearly independent points. Throughout this paper we denote
$a := (a_1, \ldots, a_g)$, and $\mathbb{Q}(A[m], m^{-1}a) := \mathbb{Q}(A[m], m^{-1}a_1, \ldots, m^{-1}a_g)$. Then we have natural injections

$$\Phi_m : \text{Gal}(\mathbb{Q}(A[m])/\mathbb{Q}) \hookrightarrow \text{Aut}(A[m]) \cong \text{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}),$$

and

$$\Phi_{a,m} : \text{Gal}(\mathbb{Q}(A[m], m^{-1}a)/\mathbb{Q}) \hookrightarrow \text{Aut}(A[m]) \cong \text{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}) \rtimes ((\mathbb{Z}/m\mathbb{Z})^{2r})^g.$$ 

Let

$$G_m := \Phi_m(\text{Gal}(\mathbb{Q}(A[m])/\mathbb{Q})), 
\quad G_{a,m} := \Phi_{a,m}(\text{Gal}(\mathbb{Q}(A[m], m^{-1}a)/\mathbb{Q})).$$

Define

$$n(m) := |G_m| = [\mathbb{Q}(A[m]) : \mathbb{Q}],$$

and

$$n_{a}(m) := |G_{a,m}| = [\mathbb{Q}(A[m], m^{-1}a) : \mathbb{Q}].$$

For a rational prime $l$, let

$$T_l(A) = \lim_{\leftarrow n} A[l^n],$$

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

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

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

$$\rho_{A,l} := \lim_{\leftarrow n} \Phi_{l^n} : G_\mathbb{Q} \to \text{Aut}(T_l(A)) \cong \text{GL}_{2r}(\mathbb{Z}_l) \subset \text{Aut}(V_l(A)) \cong \text{GL}_{2r}(\mathbb{Q}_l),$$
which is unramified outside \( lN \). If \( p \in \mathcal{P}_A \), let \( \sigma_p \) be the Artin symbol of \( p \) in \( G_Q \), and let \( l \) be a rational prime satisfying \( (l, p) = 1 \). We denote by \( P_{A, p}(X) = X^{2r} + a_{1, A}(p)X^{2r-1} + \ldots + a_{2r-1, A}(p)X + p^r \in \mathbb{Z}[X] \) the characteristic polynomial of \( \sigma_p \) on \( T_l(A) \). Then \( P_{A, p}(X) \) is independent of \( l \). We know (Riemann Hypothesis) that \( P_{A, p}(X) = (X - x_{1, p}) \ldots (X - x_{2r, p}) \), where \( |x_{i, p}| = p^\frac{1}{2} \). One can identify \( T_l(A) \) with \( T_l(\bar{A}) \), where \( \bar{A} \) is the reduction of \( A \) at \( p \), and the action of \( \sigma_p \) on \( T_l(A) \) is the same as the action of the Frobenius \( \pi_p \) of \( \bar{A} \) on \( T_l(\bar{A}) \).

Also for each rational prime \( l \), one has a representation

\[
\rho_{A, a, l} := \lim_{n \to \infty} \Phi_{a, l^n} : G_Q \to \text{Aut}(T_l(A)) \ltimes (T_lA)^g \simeq \text{GL}_{2r}(\mathbb{Z}_l) \ltimes (\mathbb{Z}_l^{2r})^g.
\]

We know (see for example Proposition 9 of [LTA], and [SI], and [CW]):

**Lemma 2.1.** Let \( A \) be an abelian variety defined over \( Q \), of dimension \( r \), of conductor \( N \), and let \( m \) be a positive integer. Assume that \( \text{rank}_Q A \geq g \) where \( g \) is a positive integer, and let \( a_1, \ldots, a_g \in A(Q) \) be linearly independent points. Then the extensions \( Q(A[m])/Q \) and \( Q(A[m], m^{-1}a)/Q \) are ramified only at places dividing \( mN \).

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

**Lemma 2.2.** Let \( A \) be an abelian variety defined over \( Q \), of dimension \( r \), and let \( m \) be a positive integer. Assume that \( \text{rank}_Q A \geq g \), where \( g \) is a positive integer. Let \( \epsilon > 0 \). Then, we have

\[
|G_m| \gg m^{2-\epsilon},
\]

and obviously

\[
m^{4r^2+2rg} \gg |G_{a, m}|.
\]

We know (Lemma 2.2 of [V]):

**Lemma 2.3.** Let \( A \) be an abelian variety over \( Q \), of dimension \( r \), of conductor \( N \). Assume that \( \text{rank}_Q A \geq g \) where \( g \) is a positive integer, let \( a_1, \ldots, a_g \in A(Q) \) be linearly independent points, and let \( a := (a_1, \ldots, a_g) \). Let \( p \in \mathcal{P}_A \). Let \( q \neq p \) be a rational prime. Then \( \frac{A(\overline{\mathbb{F}_p})}{(a_1, \ldots, a_g)} \) contains a \((q, \ldots, q)\)-type subgroup \((q \text{ appears } 2r \text{-times})\), i.e. a subgroup isomorphic to \( \mathbb{Z}/q\mathbb{Z} \times \ldots \times \mathbb{Z}/q\mathbb{Z} \), if and only if \( p \) splits completely in \( Q(A[q], q^{-1}a) \).

We know (Lemma 2.3 of [V]):

**Lemma 2.4.** Let \( A \) be an abelian variety over \( Q \), of dimension \( r \), of conductor \( N \). Assume that \( \text{rank}_Q A \geq g \), where \( g \) is a positive integer, let \( a_1, \ldots, a_g \in A(Q) \) be linearly independent points, and let \( a := (a_1, \ldots, a_g) \). Let \( p \in \mathcal{P}_A \). Then \( \frac{A(\overline{\mathbb{F}_p})}{(a_1, \ldots, a_g)} \) contains at most \((2r - 1)\)-cyclic components if and only if \( p \) does not split completely in \( Q(A[q], q^{-1}a) \) for any rational prime \( q \neq p \).

We know (see Lemma 14 of [GM]):

7
Lemma 2.5. Let $A$ be an abelian variety over $\mathbb{Q}$, of conductor $N$. Assume that $\text{rank}_\mathbb{Q}A \geq g$ where $g$ is a positive integer, and let $a_1, \ldots, a_g \in A(\mathbb{Q})$ be linearly independent points. Then, we have

$$\left| \{ p \in \mathcal{P}_A \mid |\langle \overline{a}_1, \ldots, \overline{a}_g \rangle| < y \} \right| = O(y^{\frac{g+2}{2}}).$$

(We remark that a little stronger estimate with $O(y^{\frac{g+2}{2}})$ replaced by $O(y^{\frac{g+2}{2} \log y})$ is stated in Proposition 5.4 of [AGM]).

We know (see Theorem 1.1 of [V]; and also Remark 3.1 of [V] for a more general result):

Lemma 2.6. Let $A$ be an abelian variety over $\mathbb{Q}$. Assume that $\text{rank}_\mathbb{Q}A \geq g$, where $g \geq 0$ is an integer, and let $a_1, \ldots, a_g \in A(\mathbb{Q})$ be linearly independent points. Assume that $\mathbb{Q}(A[2]) = \mathbb{Q}$, and $\mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) \neq \mathbb{Q}$. Then we have

$$f_{A,a}(x) \gg \frac{x (\log x)^2}{\log \log x}.$$ 

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 $L/\mathbb{Q}$, and by $d_F$ the discriminant of $F/\mathbb{Q}$. 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

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

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

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

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

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

for every $x \geq 2$, where the implied $O$-constant is absolute.
4 The proofs of Theorems 1.1 and 1.2

From Lemma 2.4 we get

$$f_{A,a}(x) = \sum_{m=1}^{\infty} \mu(m)\pi_1(x, \mathbb{Q}(A|m), m^{-1}a)/\mathbb{Q}), \quad (4.1)$$

where the sum is over square-free positive integers. If $p \leq x$ splits completely in $\mathbb{Q}(A|m), m^{-1}a)$, then from Lemma 2.3 and from the fact that (Riemann hypothesis) $|x_{i,p}| = \frac{p}{2} \leq x^{\frac{1}{2}}$ for each root $x_{i,p}$ of $P_{A,p}(X)$, we get that $m^{2r}||P_{A,p}(1)| < 2^{2r}x^{r}$. Hence in (4.1) it is sufficient to consider only positive square-free integers $m$ satisfying $m \leq 2x^{\frac{1}{2}}$.

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

$$f_{A,a}(x) = \sum_{m \leq 2x^{\frac{1}{2}}} \mu(m)\pi_1(x, \mathbb{Q}(A|m), m^{-1}a)/\mathbb{Q})$$

$$= \sum_{m \leq y} \mu(m)\pi_1(x, \mathbb{Q}(A|m), m^{-1}a)/\mathbb{Q}) + \sum_{y < m \leq 2x^{\frac{1}{2}}} \mu(m)\pi_1(x, \mathbb{Q}(A|m), m^{-1}a)/\mathbb{Q})$$

$$= \text{main} + \text{error.} \quad (4.2)$$

From Lemmas 3.2, 3.1, 2.1 and 2.2, under GRH, we get

$$\text{main} = \sum_{m \leq y} \frac{\mu(m)}{n_a(m)} \cdot \text{li} \cdot x + \sum_{m \leq y} O(x^{\frac{1}{2}} \log(mx))$$

$$= \sum_{m \leq y} \frac{\mu(m)}{n_a(m)} \cdot \text{li} \cdot x + O(yx^{\frac{1}{2}} \log(Nx)), \quad (4.3)$$

where $n_a(m) := [\mathbb{Q}(A|m), m^{-1}a) : \mathbb{Q}]$.

Now we estimate the error. If $p$ splits completely in $\mathbb{Q}(A|m), m^{-1}a)$, then

$$|\langle \bar{a}_1, \ldots, \bar{a}_g \rangle| \leq \frac{2^{2r}x^{r}}{m^{2r}}, \quad (4.4)$$

and from Lemma 2.5 we obtain

$$\text{error} \ll \sum_{y < m \leq 2x^{\frac{1}{2}}} \frac{x^{\frac{1}{2}+2r}}{m^{\frac{1}{2}+2r}}$$

$$\ll \frac{x^{\frac{1}{2}+2r}}{y^{\frac{1}{2}+2r-1}}. \quad (4.5)$$

From (4.2), (4.3), and (4.5) we get

$$f_{A,a}(x) = \sum_{m \leq y} \frac{\mu(m)}{n_a(m)} \cdot \text{li} \cdot x + O(yx^{\frac{1}{2}} \log x) + O(\frac{x^{\frac{1}{2}+2r}}{y^{\frac{1}{2}+2r-1}}).$$
We choose \( y \) such that \( x^2 y \log x = \frac{x^{1+2}}{y^{2r-2}} \), i.e.

\[
y := \frac{x^{2r+4r-g}}{(\log x)^{2gr-4r}}.
\]

Then

\[
f_{A,a}(x) = \sum_{m \leq y} \frac{\mu(m)}{n_a(m)} \log x + O(x^{\frac{4g+8r-g}{4g+8r}} (\log x)^{\frac{2g+4r-g}{2gr-4r}}).
\]

From Lemma 2.2, with \( \epsilon > 0 \), we obtain

\[
\sum_{m > y} \frac{1}{n_a(m)} \ll \sum_{m > y} \frac{1}{m^{2-\epsilon}} \ll \frac{1}{y^{1-\epsilon}}.
\]

Since \( y := \frac{x^{2r+4r-g}}{(\log x)^{2gr-4r}} \), for \( \epsilon > 0 \) small enough, we get

\[
f_{A,a}(x) = c_{A,a} \log x + O(x^{\frac{4g+8r-g}{4g+8r}} (\log x)^{\frac{2g+4r-g}{2gr-4r}}),
\]

(4.6)

and Theorem 1.1 is proved.

Now, if \( \mathbb{Q}(A[2], 2^{-1}a) = \mathbb{Q} \), then we proved in the Introduction that \( f_{A,a}(x) \) is bounded, and because of the asymptotic formula (4.6) we get that \( c_{A,a} = 0 \).

If \( \mathbb{Q}(A[2]) = \mathbb{Q} \) and \( \mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q} \), then \( c_{A,a} \neq 0 \), because the error term in the asymptotic formula of Theorem 1.1 is smaller than the term \( \frac{x}{(\log x)^2} \) which appears in the statement of Lemma 2.6, and we are done with the proof of Theorem 1.2.

\[\blacksquare\]

**References**


