The Artin’s conjecture for CM abelian varieties

Cristian Virdol
Department of Mathematics
Yonsei University
cristian.virdol@gmail.com
July 4, 2017

Abstract
Consider $A$ a CM abelian variety of dimension $r$, defined over $\mathbb{Q}$, such that $\text{End}_F A \otimes \mathbb{Q} = \text{End}_{\overline{\mathbb{Q}}} A \otimes \mathbb{Q}$, for some arbitrary finite abelian extension $F$ of $\mathbb{Q}$. 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 (so in particular $a_1, \ldots, a_g$ have infinite order, and if $g = 0$, then the set $\{a_1, \ldots, a_g\}$ is empty). For a rational prime of good reduction for $A$, let $\bar{A}$ be the reduction of $A$ at $p$, let $\bar{a}_i$ for $i = 1, \ldots, g$, be the reduction of $a_i$ (modulo $p$), and let $\langle \bar{a}_1, \ldots, \bar{a}_g \rangle$ be the subgroup of $\bar{A}(\mathbb{F}_p)$ generated by $\bar{a}_1, \ldots, \bar{a}_g$. Assume that $\mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) \neq \mathbb{Q}$. Then, in this paper we show that the number of primes $p$, for which $\bar{A}(\mathbb{F}_p) \langle \bar{a}_1, \ldots, \bar{a}_g \rangle$ has at most $2r - 1$ cyclic components is infinite. This result is the right generalization of the classical Artin’s primitive root conjecture (1927) in the context of CM abelian varieties, i.e. this result is an unconditional proof of Artin’s conjecture for CM abelian varieties. Artin’s conjecture 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 $p$) (this conjecture is not known for any specific $a$). Similar results hold true for CM abelian varieties $A$ defined over arbitrary finite abelian extensions $F'$ of $\mathbb{Q}$.

Keywords: CM 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 $P_A$ be the set of rational primes $p$ of good reduction for $A$, (i.e. $(p, N) = 1$). For $p \in P_A$, 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

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

(1.1)
where \( s \leq 2r, m_i \in \mathbb{Z}_{\geq 2}, \) and \( m_i | m_{i+1} \) for \( 1 \leq i < s - 1. \) 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 \( \text{rank}_Q A \geq g, \) where \( g \geq 0 \) is an integer, and let \( a_1, \ldots, a_g \in A(\mathbb{Q}) \) be linearly independent points (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 \( a_i \) (modulo \( p \)), 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 \( \frac{A(p)}{\langle \bar{a}_1, \ldots, \bar{a}_g \rangle} \) has at most \( 2r \) cyclic components. We call \( a := (a_1, \ldots, a_g) \) a primitive-cyclic tuple for \( p \) if \( \frac{A(p)}{\langle a_1, \ldots, a_g \rangle} \) has at most \( 2r - 1 \) cyclic components.

For \( x \in \mathbb{R}, \) define

\[
f_{A,a,Q}(x) = |\{ p \in \mathcal{P}_A | p \leq x, \frac{A(p)}{\langle a_1, \ldots, a_g \rangle} \text{ has at most } (2r-1) \text{ cyclic components} \}|
\]

In this paper, in particular, we prove the following result (for the case of abelian varieties over number fields see Remark 4.1 below):

**Theorem 1.1.** Let \( A \) be an abelian variety over \( \mathbb{Q} \) of dimension \( r \geq 1, \) such that \( \text{End}_F A \otimes \mathbb{Q} = \text{End}_F \mathbb{Q} \otimes \mathbb{Q}, \) for some arbitrary finite abelian extension \( F \) of \( \mathbb{Q}. \) Assume that \( \text{End}_F A \otimes \mathbb{Q} = K \) is a CM number field, such that \( |K : \mathbb{Q}| = 2r. \) Assume that \( \text{rank}_Q A \geq g, \) where \( g \geq 0 \) is an integer, and let \( a_1, \ldots, a_g \in A(\mathbb{Q}) \) be linearly independent points. Assume that \( \mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) \neq \mathbb{Q}. \) Then we have

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

Theorem 1.1 is the right generalization of the classical Artin’s primitive root conjecture in the context of CM abelian varieties (the Kummer number fields \( \mathbb{Q}(A,g), q^{-1}a), \) for \( q \) rational prime, that appear in the statements of Lemmas 2.2 and 2.3 below are the analogous of the Kummer splitting fields \( \mathbb{Q}(\sqrt{T}, \sqrt{a}) \) of \( x^q - a = 0 \) which occur in the classical Artin’s conjecture (see [H] for details). Also the assumption that \( a_1, \ldots, a_g \in A(\mathbb{Q}) \) are linearly independent and \( \mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) \neq \mathbb{Q} \) corresponds exactly to the assumption “\( a \neq \pm 1 \) or a perfect square” or to the equivalent assumption that \( a \neq \pm 1 \) and “\( \mathbb{Q}(\pm 1, \sqrt{a}) \neq \mathbb{Q} \)” from the classical Artin’s primitive root conjecture. So in this paper we consider an element \( a := (a_1, \ldots, a_g) \) such that \( a_1, \ldots, a_g \in A(\mathbb{Q}) \) are linearly independent, and \( a \) is not a perfect square, and we prove that the number of primes \( p \) for which \( \frac{A(p)}{\langle a_1, \ldots, a_g \rangle} \) has at most \( 2r - 1 \) cyclic components is infinite. We remark that in 1977 Lang and Trotter in [LT] formulated a so-called “analogous conjecture” for elliptic curves (actually they did not formulate any conjecture) but that is not Artin’s conjecture for elliptic curves as many people, including the authors of [GM1], believe. 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 \( \bar{A}[2](\mathbb{F}_p) \subset \frac{A(p)}{\langle a_1, \ldots, a_g \rangle} \) and \( A[2](\mathbb{F}_p) \simeq (\mathbb{Z}/2)^{2r}, \) and thus in this case \( f_{A,a,Q}(x) \) is bounded. Therefore the condition \( \mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) \neq \mathbb{Q} \) imposed in Theorem 1.1 is necessary.
We remark that one can prove Theorem 1.1 for abelian varieties $A$ over any non-trivial abelian extension $F'$ of $Q$, provided that $F'(A[q], q^{-1}a_1, \ldots, q^{-1}a_g) \neq F'$ for any rational prime $q$ (see Remark 4.1 below).

2 General abelian varieties

We follow very closely [V]. For a number field $M$ we denote $\Gamma_M := \text{Gal}(\bar{Q}/M)$. Let $A$ be an abelian variety over $Q$, of dimension $r \geq 1$, and of conductor $N$. Let $\mathcal{P}_A$ be the set of rational primes $p$ 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 $\bar{Q}$. Assume that $\text{rank}_Q A \geq g$, where $g \geq 0$ is an integer, and let $a_1, \ldots, a_g \in A(Q)$ be linearly independent points. Throughout this paper we denote $a := (a_1, \ldots, a_g)$, and $Q(A[m], m^{-1}a) := Q(A[m], m^{-1}a_1, \ldots, m^{-1}a_g)$. We have

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

If $Q(A[m])$ is the field obtained by adjoining to $Q$ the elements of $A[m]$, then we have natural injections

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

and

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

For a rational prime $l$, let

$$T_l(A) = \varprojlim_{n} [\text{Aut}(A[m])],$$

and $V_l(A) = T_l(A) \otimes Q$. The Galois group $\Gamma_Q$ 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 $V_l(A) \cong Q_l^{2r}$, and we obtain a representation

$$\rho_{A,l} := \varprojlim_{n} \Phi_{a} : \Gamma_Q \rightarrow \text{Aut}(T_l(A)) \cong \text{GL}_{2r}(\mathbb{Z}_l) \subset \text{Aut}(V_l(A)) \cong \text{GL}_{2r}(Q_l),$$

which is unramified outside $lN$. If $p \in \mathcal{P}_A$, let $\sigma_p$ be the Artin symbol of $p$ in $\Gamma_Q$, and let $l$ be a rational prime satisfying $(l, p) = 1$. We denote by $P_{A,p}(X) = X^{2r} + a_1A(p)X^{2r-1} + \cdots + a_{2r-1}A(p)X + p^r \in \mathbb{Z}[X]$ the characteristic polynomial of $\sigma_p$ on $T_l(A)$. Then $P_{A,p}(X)$ is independent of $l$. We know (Riemann Hypothesis) that $P_{A,p}(X) = (X - x_{1,p})(X - x_{2,p}) \cdots (X - x_{r,p})(X - x_{r,p})$, where $|x_{i,p}| = p^{\frac{1}{2}}$ for $i = 1, \ldots, r$. One can identify $T_l(A)$ with $T_l(A)$, where $A$ 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 $A$ on $T_l(A)$.
Also for each rational prime \( l \), one has a representation
\[
\rho_{A,a,l} := \lim_{n \to \infty} \Phi_a,l^n : \Gamma_Q \to \Aut(T_l(A)) \times (T_l A)^g \cong \GL_{2r} / \Z_l^2 \times (\Z_l^2)^g.
\]

We know (see for example Proposition 9 of [LTA], Lemma 1 of [BK], Lemma 4 and its Corollary from Chapter III of [CF]):

**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 \( g \geq 0 \) is an integer, and let \( a_1, \ldots, a_g \in A(\Q) \) be linearly independent points. Let \( a := (a_1, \ldots, a_g) \). Then
1. the extensions \( \Q(A[m])/\Q \) and \( \Q(A[m],m^{-1}a)/\Q \) are ramified only at places dividing \( mN \),
2. \( \Q(\zeta_m) \subseteq \Q(A[m]) \), and hence if a rational prime \( p \) splits completely in \( \Q(A[m]) \), then \( mp - 1 \).

We know (Lemma 2.2 of [V]):

**Lemma 2.2.** Let \( A \) be an abelian variety over \( \Q \), of dimension \( r \), of conductor \( N \). Assume that \( \text{rank} \, \Q A \geq g \), where \( g \geq 0 \) is an integer, let \( a_1, \ldots, a_g \in A(\Q) \) be linearly independent points, and let \( a := (a_1, \ldots, a_g) \). Let \( p \in \mathcal{P}_A \), and let \( q \neq p \) be a rational prime. Then \( \overline{A}(\F_p)^{\langle \overline{a}_1, \ldots, \overline{a}_g \rangle} \) contains a \((q,\ldots,q)\)-type subgroup (\( q \) appears \( 2r \)-times), i.e. a subgroup isomorphic to \( \Z/q \Z \times \cdots \times \Z/q \Z \), if and only if \( p \) splits completely in \( \Q(A[q], q^{-1}a) \).

We know (Lemma 2.3 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 \( g \geq 0 \) is an 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 \( \overline{A}(\F_p)^{\langle \overline{a}_1, \ldots, \overline{a}_g \rangle} \) 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 (Lemma 2.4 of [V]):

**Lemma 2.4.** Let \( A \) be an abelian variety over \( \Q \), of dimension \( r \), of conductor \( N \). Let \( p \in \mathcal{P}_A \), and let \( q \neq p \) be a rational prime. If \( p \) splits completely in \( \Q(A[q]) \), then \( \frac{\alpha_1}{\alpha_2} - 1 \) is an algebraic integer for any \( i = 1, \ldots, r \).

We know (Lemma 2.5 of [V]):

**Lemma 2.5.** With the same notations as in Lemma 2.4, if \( p \) splits completely in \( \Q(A[q]) \), then we have
\[
q^2rp + a_1.A(p) + r.
\]

We know (Lemma 2.6 of [V]):

**Lemma 2.6.** We have
\[
|a_1.A(p)| \leq 2rp^2.
\]
3 Abelian varieties of CM type

Let $A$ be an abelian variety of dimension $r$, defined over $\mathbb{Q}$, such that $\text{End}_{F} A \otimes \mathbb{Q} = \text{End}_{\mathbb{Q}} A \otimes \mathbb{Q}$, for some arbitrary finite abelian extension $F$ of $\mathbb{Q}$. Assume that $\text{End}_{F} (A) \otimes \mathbb{Q} = K$, where $K$ is a CM number field such that $[K : \mathbb{Q}] = 2r$.

Lemma 3.1. Let $A$ be an abelian variety over $\mathbb{Q}$, as above. Then $\text{Im} \rho_{A,1} | \Gamma_{F}$ is abelian for any prime number $l$, and hence the Galois extension $F(A[m]) / F$ is abelian for any positive integer $m$.

Proof: Because $\text{End}_{F} A \otimes \mathbb{Q} = K$, from Corollary 2 of §4 of [ST], we know that $\text{Im} \rho_{A,1} | \Gamma_{F} \subseteq U_{l}(O_{K})$, where $U_{l}(O_{K})$ is the group of invertible elements of $O_{K} \otimes \mathbb{Z}_{l}$. Since the group $U_{l}(O_{K})$ is abelian we are done. ■

Lemma 3.2. Assume that $\mathbb{Q}(A[2]) \neq \mathbb{Q}$. Then $\mathbb{Q}(A[2])$ contains a nontrivial abelian extension of $\mathbb{Q}$.

Proof: If $\mathbb{Q}(A[2]) \cap F \neq \mathbb{Q}$, we are done because $F$ is an abelian extension of $\mathbb{Q}$. If $\mathbb{Q}(A[2]) \cap F = \mathbb{Q}$, then $\text{Gal}(\mathbb{Q}(A[2]) / \mathbb{Q}) \simeq \text{Gal}(F(A[2]) / F)$, and hence, from Lemma 3.1, we get that $\mathbb{Q}(A[2])$ is a non-trivial abelian extension of $\mathbb{Q}$, and we are done with the proof of Lemma 3.2. ■

Lemma 3.3. Let $A$ be an abelian variety over $\mathbb{Q}$, as above. Let $S_{r}(x)$ be the set of primes $p \in \mathbb{P}_{A}$ such that $p \leq x$, and all odd prime divisors of $p - 1$ are distinct and $\geq x^{1/4 + \epsilon}$, and $p$ does not split completely in $\mathbb{Q}(A[2], 2^{-1}a)$. If $\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$, then there exists an $\epsilon > 0$ such that

$$|S_{r}(x)| \gg \frac{x}{(\log x)^{2}}.$$ 

Proof: If $\mathbb{Q}(A[2]) \neq \mathbb{Q}$, then from Lemma 3.2 we know that $\mathbb{Q}(A[2])$ contains a nontrivial abelian extension of $\mathbb{Q}$. If $\mathbb{Q}(A[2]) = \mathbb{Q}$, and $\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$, then the field $\mathbb{Q}(A[2], 2^{-1}a)$ is a non-trivial abelian extension of $\mathbb{Q}$. Hence, if $\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$, then the field $\mathbb{Q}(A[2], 2^{-1}a)$ contains a non-trivial abelian extension of $\mathbb{Q}$, and the same proof as in Lemma 3 of [GM] goes through. ■

4 The proof of Theorem 1.1

We follow very closely [V]. Consider $\epsilon > 0$ satisfying Lemma 3.3. For each $c \in \mathbb{Z}$, such that $|c| \leq 2r x^{1/4}$, we define

$$S_{r,c}(x) := \{p \in S_{r}(x) | a_{1,A}(p) = c\}.$$ 

From Lemma 2.6, we know that $|a_{1,A}(p)| \leq 2r x^{1/4}$, and thus $S_{r}(x)$ is a disjoint union of $S_{r,c}(x)$. For each $c$ as above, we want to count the number of $p \in S_{r,c}(x)$ for which $\frac{A(p, \overline{\mathbb{Q}})}{\langle \alpha_{1}, \ldots, \alpha_{g} \rangle}$ does not have at most $2r - 1$ cyclic components. If $\frac{A(p, \overline{\mathbb{Q}})}{\langle \alpha_{1}, \ldots, \alpha_{g} \rangle}$ does not have at most $(2r - 1)$-cyclic components, then $(\mathbb{Z}/q\mathbb{Z})^{2r} \subset \frac{A(p, \overline{\mathbb{Q}})}{\langle \alpha_{1}, \ldots, \alpha_{g} \rangle}$ for

5
some prime \( q \), and from Lemma 2.2 and from the definition of \( S_{c}(x) \), we deduce that \( q \) is odd and \( p \) splits completely in \( \mathbb{Q}(A[q], q^{-1}a) \). From Lemma 2.1, we get that
\[
q | p - 1,
\]
and from Lemma 2.5 we know that
\[
q^{2} | rp + a_{1,A}(p) + r = rp + c + r,
\]
and thus \( q | c + 2r \). We have that \( c \neq -2r \), because otherwise \( q^{2} | r(p - 1) \) (we already know that \( q | p - 1 \), and from the definition of \( S_{c}(x) \), for \( x \) large enough one can assume that \( (q, r) = 1 \), and hence \( q^{2} | r(p - 1) \) would imply that \( q^{2} | p - 1 \) which is a contradiction with the definition of \( S_{c}(x) \)). Since \( q \geq x^{\frac{1}{2}+\varepsilon} \), and since \( |c| \leq 2rx^{\frac{1}{2}} \), for \( x \) sufficiently large, \( q \) is determined by \( c \). If \( p \in S_{c,c}(x) \), is such that \( \frac{\bar{A}(F_{p})}{(a_{1},...,a_{g})} \) does not have at most \((2r - 1)\)-cyclic components, then from above we get that
\[
rp \equiv - c - r \mod q^{2},
\]
and hence the number of such \( p \) is
\[
< \frac{x}{q^{2}} + O(1) \ll x^{\frac{1}{2}-2\varepsilon}.
\]
Thus we proved that the number of \( p \in S_{c}(x) \), for which \( \frac{\bar{A}(F_{p})}{(a_{1},...,a_{g})} \) does not have at most \((2r - 1)\)-cyclic components, is
\[
x^{\frac{1}{2}-2\varepsilon}x^{\frac{1}{2}} = o\left(\frac{x}{(\log x)^{2}}\right),
\]
and we are done with the proof of Theorem 1.1. \( \blacksquare \)

**Remark 4.1.** We remark that Theorem 1.1 holds true for abelian varieties \( A \) defined over arbitrary finite abelian extensions \( F' \) of \( \mathbb{Q} \), and \( a_{1},...,a_{g} \in A(F') \), provided that \( F'(A[q], q^{-1}a_{1},...,q^{-1}a_{g})' \neq F' \) for any \( q \) rational prime, where \( F'(A[q], q^{-1}a_{1},...,q^{-1}a_{g})' \) is the maximal abelian field contained in the field \( F'(A[q], q^{-1}a_{1},...,q^{-1}a_{g}) \). The reason is that if one looks at the rational primes \( p \) that split completely in \( F' \), then \( \bar{A}(F_{p}) = \bar{A}(F_{v}) \) for any place \( v \) of \( F' \) over \( p \), and one still gets \( \gg \frac{x}{\log x} \) places \( v \) of \( F' \) such that \( N_{F'/\mathbb{Q}} < x \) and \( \frac{\bar{A}(F_{v})}{(a_{1},...,a_{g})} \) has at most \( 2r - 1 \) cyclic components. This is true because since \( F' \) is abelian the primes that split completely in \( F' \) are well-distributed in arithmetic progressions, and this is equivalent to putting additional conditions on the primes so that the theorem of Fourey and Iwaniec of sieve theory from [FI] can be used without change (see also §6 of [GM]).

**References**


