Artin's conjecture for abelian varieties

Cristian Virdol

Abstract Consider A an abelian variety of dimension r defined over $\mathbb{Q}$. Assume that $\operatorname{rank}_{\mathbb{Q}} A \geq g$, 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 p 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 $\mathbb{Q}(A[2]) = \mathbb{Q}$ and $\mathbb{Q}(A[2], 2^{-1}a_1, \ldots, 2^{-1}a_g) \neq \mathbb{Q}$. (Note that this particular assumption $\mathbb{Q}(A[2]) = \mathbb{Q}$ forces the inequality $g \geq 1$, but we can take care of the case $g = 0$, under the right assumptions, also.) Then in this article, in particular, we show that the number of primes p for which $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1, \ldots, \bar{a}_g \rangle}$ has at most $(2r-1)$ cyclic components is infinite. This result is the right generalization of the classical Artin's primitive root conjecture in the context of general abelian varieties; that is, this result is an unconditional proof of Artin's conjecture 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 $(\operatorname{mod} p)$. (This conjecture is not known for any specific a.)

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 $\mathcal{P}_A$ be the set of rational primes p 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 $\bar{A}(\mathbb{F}_p) \subseteq \bar{A}[m](\bar{\mathbb{F}}_p) \subseteq (\mathbb{Z}/m\mathbb{Z})^{2r}$ for any positive integer m satisfying $|\bar{A}(\mathbb{F}_p)| \mid m$. Hence,

$$\bar{A}(\mathbb{F}_p) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}, \tag{1.1}$$

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

Assume that $\operatorname{rank}_{\mathbb{Q}} A \geq g$, 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_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 $\bar{A}(\mathbb{F}_p)$ generated by $\bar{a}_1, \ldots, \bar{a}_g$. From above we

Kyoto Journal of Mathematics, Vol. 56, No. 4 (2016), 737–743
DOI 10.1215/21562261-3664896,
Received December 25, 2014. Revised September 17, 2015. Accepted September 24, 2015.
2010 Mathematics Subject Classification: Primary, 11G10, 11G15.
The author's research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2015R1D1A1A01056643).

know that $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ has at most $2r$ cyclic components. We call $a := (a_1,\ldots,a_g)$ a *primitive-cyclic* tuple for p if $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ has at most $(2r-1)$ cyclic components. For $x \in \mathbb{R}$, define

$$f_{A,a,\mathbb{Q}}(x) = \left|\left\{p \in \mathcal{P}_A \;\middle|\; p \le x, \frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle} \text{ has at most } (2r-1) \text{ cyclic components}\right\}\right|.$$

In this article, in particular, we prove the following result.

THEOREM 1.1

Let A be an abelian variety over $\mathbb{Q}$. Assume that $\operatorname{rank}_{\mathbb{Q}} A \ge g$, where $g \ge 0$ 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 that $\mathbb{Q}(A[2], 2^{-1}a_1,\ldots,2^{-1}a_g) \ne \mathbb{Q}$. Then we have

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

We remark that the assumption $\mathbb{Q}(A[2]) = \mathbb{Q}$ in Theorem 1.1 corresponds to the trivial fact $\mathbb{Q}(\pm 1) = \mathbb{Q}$ from the classical Artin's primitive root conjecture, and that the assumption that $a_1,\ldots,a_g \in A(\mathbb{Q})$ are linearly independent and $\mathbb{Q}(A[2], 2^{-1}a_1,\ldots,2^{-1}a_g) \ne \mathbb{Q}$ corresponds *exactly* to the assumption that "$a \ne \pm 1$ or a perfect square" or to the equivalent assumption that $a \ne \pm 1$ and "$\mathbb{Q}(\pm 1, \sqrt{a}) \ne \mathbb{Q}$" from the classical Artin's primitive root conjecture. (Actually in Theorem 1.1 one does not necessarily have to assume that $\mathbb{Q}(A[2]) = \mathbb{Q}$ (see Remark 3.1 below), but we prefer to leave Theorem 1.1 in this classical form.) Theorem 1.1 is the right generalization of the classical Artin's primitive root conjecture in the context of abelian varieties. (The fields $\mathbb{Q}(A[q], q^{-1}a)$, for q rational prime, that appear in the statements of Lemmas 2.2 and 2.3 below are the analogues of the splitting fields $\mathbb{Q}(\sqrt[q]{1}, \sqrt[q]{a})$ of $x^q - a = 0$ which occur in the classical Artin's conjecture (see [6] for details).) We remark that in 1977 Lang and Trotter [8] formulated an analogous conjecture for elliptic curves, but that is not Artin's conjecture for elliptic curves as some people, including the authors of [4], 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 $\bar{A}[2](\bar{\mathbb{F}}_p) \subset \frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ and $\bar{A}[2](\bar{\mathbb{F}}_p) \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$, and thus, in this case $f_{A,a,\mathbb{Q}}(x)$ is finite. Therefore, the condition $\mathbb{Q}(A[2], 2^{-1}a_1,\ldots,2^{-1}a_g) \ne \mathbb{Q}$ imposed in Theorem 1.1 is necessary.

2. General abelian varieties

Let $G_{\mathbb{Q}} := \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let A be an abelian variety over $\mathbb{Q}$, of dimension $r \ge 1$, 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 $m \ge 1$ an integer, let $A[m]$ be the m-division points of A in $\bar{\mathbb{Q}}$. Assume that $\operatorname{rank}_{\mathbb{Q}} A \ge g$, where $g \ge 0$ is an integer, and let $a_1,\ldots,a_g \in A(\mathbb{Q})$ be linearly independent points. Throughout this article we denote $a :=$

$(a_1,\dots,a_g)$, and $\mathbb{Q}(A[m],m^{-1}a) := \mathbb{Q}(A[m],m^{-1}a_1,\dots,m^{-1}a_g)$. We have

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

If $\mathbb{Q}(A[m])$ is the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the elements of $A[m]$, then we have a natural injection

$$\Phi_m : \mathrm{Gal}\big(\mathbb{Q}\big(A[m]\big)/\mathbb{Q}\big) \hookrightarrow \mathrm{Aut}\big(A[m]\big) \simeq \mathrm{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}).$$

For a rational prime l, let

$$T_l(A) = \varprojlim_n A[l^n],$$

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

$$\rho_{A,l} := \varprojlim_n \Phi_{l^n} : G_\mathbb{Q} \to \mathrm{Aut}\big(T_l(A)\big) \simeq \mathrm{GL}_{2r}(\mathbb{Z}_l) \subset \mathrm{Aut}\big(V_l(A)\big) \simeq \mathrm{GL}_{2r}(\mathbb{Q}_l),$$

which is unramified outside lN. If $p \in \mathcal{P}_A$, then let σ_p be the Artin symbol of p in $G_\mathbb{Q}$, and let l be a rational prime satisfying $(l,p) = 1$. We denote by $P_{A,p}(X) = X^{2r} + a_{1,A}(p)X^{2r-1} + \cdots + a_{2r-1,A}(p)X + p^r \in \mathbb{Z}[X]$ the characteristic polynomial of σ_p on $T_l(A)$. Then $P_{A,p}(X)$ is independent of l. We know (Riemann hypothesis) that $P_{A,p}(X) = (X - x_{1,p})(X - \bar{x}_{1,p})\cdots(X - x_{r,p})(X - \bar{x}_{r,p})$, where $|x_{i,p}| = p^{1/2}$, for $i = 1,\dots,r$. 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 σ_p on $T_l(A)$ is the same as the action of the Frobenius π_p of $\bar{A}$ on $T_l(\bar{A})$.

We know (see, e.g., [7, Proposition 9], [1, Lemma 1], [2, Chapter III, Lemma 4 and its corollary], [10], and [3]) the following.

LEMMA 2.1

Let A be an abelian variety defined over $\mathbb{Q}$, of dimension r, and of conductor N, and let m be a positive integer. Assume that $\mathrm{rank}_\mathbb{Q}\, A \geq g$, *where $g \geq 0$ is an integer, and let $a_1,\dots,a_g \in A(\mathbb{Q})$ be linearly independent points. Let $a := (a_1,\dots,a_g)$. Then the following statements hold:*

1. *the extensions $\mathbb{Q}(A[m])/\mathbb{Q}$ and $\mathbb{Q}(A[m],m^{-1}a)/\mathbb{Q}$ are ramified only at places dividing mN;*
2. *$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(A[m])$, and hence, if a rational prime p splits completely in $\mathbb{Q}(A[m])$, then $m \mid p-1$.*

LEMMA 2.2

Let A be an abelian variety over $\mathbb{Q}$, of dimension r, and of conductor N. Assume that $\mathrm{rank}_\mathbb{Q}\, A \geq g$, *where $g \geq 0$ is an integer, let $a_1,\dots,a_g \in A(\mathbb{Q})$ be linearly independent points, and let $a := (a_1,\dots,a_g)$. Let $p \in \mathcal{P}_A$, and let $q \neq p$ be a rational prime. Then $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\dots,\bar{a}_g\rangle}$ contains a $(q,\dots,q)$-type subgroup (q appears $2r$ times),*

that is, a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \times \cdots \times \mathbb{Z}/q\mathbb{Z}$*, if and only if* p *splits completely in* $\mathbb{Q}(A[q], q^{-1}a)$*.*

Proof
Since $(p, Nq) = 1$, from Lemma 2.1 we know that p is unramified in $\mathbb{Q}(A[q], q^{-1}a)$. Then when

$$\pi_p : \bar{A}(\bar{\mathbb{F}}_p) \to \bar{A}(\bar{\mathbb{F}}_p)$$

is the Frobenius endomorphism, we have that

$$\mathrm{Ker}(\pi_p - 1) = \bar{A}(\mathbb{F}_p).$$

But $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1, \ldots, \bar{a}_g \rangle}$ contains a $(q, \ldots, q)$-type subgroup if and only if $\bar{A}(\bar{\mathbb{F}}_p)[q] \subset \bar{A}(\mathbb{F}_p)$, and there exists a $\bar{b}_i \in \bar{A}(\mathbb{F}_p)$, for $i = 1, \ldots, g$, such that $q \cdot \bar{b}_i = \bar{a}_i$. Hence, we get that $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1, \ldots, \bar{a}_g \rangle}$ contains a $(q, \ldots, q)$-type subgroup if and only if $\bar{A}(\bar{\mathbb{F}}_p)[q] \subset \mathrm{Ker}(\pi_p - 1)$ and p has a first-degree factor in $\mathbb{Q}(q^{-1}a)$, which is equivalent to the splitting of p in $\mathbb{Q}(A[q], q^{-1}a)$. □

LEMMA 2.3

Let A *be an abelian variety over* $\mathbb{Q}$*, of dimension* r*, and of conductor* N*. Assume that* $\mathrm{rank}_{\mathbb{Q}} A \geq g$*, where* $g \geq 0$ *is an integer, let* $a_1, \ldots, a_g \in A(\mathbb{Q})$ *be linearly independent points, and let* $a := (a_1, \ldots, a_g)$*. Let* $p \in \mathcal{P}_A$*. Then* $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1, \ldots, \bar{a}_g \rangle}$ *contains at most* $(2r - 1)$ *cyclic components if and only if* p *does not split completely in* $\mathbb{Q}(A[q], q^{-1}a)$ *for any rational prime* $q \neq p$*.*

Proof
We know that $\bar{A}(\mathbb{F}_p) \subseteq \bar{A}(\bar{\mathbb{F}}_p)[m] \subseteq \mathbb{Z}/m\mathbb{Z} \times \cdots \times \mathbb{Z}/m\mathbb{Z}$ ($\mathbb{Z}/m\mathbb{Z}$ appears $2r$ times) for any positive integer m such that $|\bar{A}(\mathbb{F}_p)| \mid m$. But the p-primary part of $\bar{A}(\bar{\mathbb{F}}_p)[m]$ has at most $(2r - 1)$ cyclic components (actually at most r cyclic components; see, e.g., [9, Chapter II, Section 4]). Hence, we get that $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1, \ldots, \bar{a}_g \rangle}$ has at most $(2r - 1)$ cyclic components if and only if it does not contain a $(q, \ldots, q)$-type (q appears $2r$ times) subgroup for any rational prime $q \neq p$. From Lemma 2.2, we deduce that this is equivalent to the fact that p does not split completely in $\mathbb{Q}(A[q], q^{-1}a)$ for any rational prime $q \neq p$. □

LEMMA 2.4

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

Proof
Since p splits completely in $\mathbb{Q}(A[q])$, we know that $\bar{A}(\bar{\mathbb{F}}_p)[q] \subset \mathrm{Ker}(\pi_p - 1)$. Therefore, we have that $\rho_{A,q}(\sigma_p) = I_{2r} + qB_q$, where $B_q \in M_{2r}(\mathbb{Z}_q)$. Thus, $(qX - (x_{1,p} - 1))(qX - (\bar{x}_{1,p} - 1)) \cdots (qX - (x_{r,p} - 1))(qX - (\bar{x}_{r,p} - 1)) = P_{A,p}(qX + 1) = \det((qX + 1)I_{2r} - \rho_{A,q}(\sigma_p)) = \det(qXI_{2r} - qB_q)$, and we get trivially that $(X -$

$(\frac{x_{1,p}-1}{q}))(X-(\frac{\bar{x}_{1,p}-1}{q}))\cdots(X-(\frac{x_{r,p}-1}{q}))(X-(\frac{\bar{x}_{r,p}-1}{q}))\in\mathbb{Z}[X]$. Hence, $\frac{x_{i,p}-1}{q}$ is an algebraic integer for any $i=1,\ldots,r$. □

We define $y_{i,p}:=\frac{x_{i,p}-1}{q}$, for $i=1,\ldots,r$. Then, when p splits completely in $\mathbb{Q}(A[q])$, from the proof of Lemma 2.4 we know that $(X-y_{1,p})(X-\bar{y}_{1,p})\cdots(X-y_{r,p})(X-\bar{y}_{r,p})\in\mathbb{Z}[X]$. Hence, $p=x_{i,p}\bar{x}_{i,p}=(1+qy_{i,p})(1+q\bar{y}_{i,p})=1+q(y_{i,p}+\bar{y}_{i,p})+q^2y_{i,p}\bar{y}_{i,p}$. Thus,

$$rp=r+qb_{1,A}(p)_q+q^2b_{2,A}(p)_q,$$

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

LEMMA 2.5

With the same notation as in Lemma 2.4, if p splits completely in $\mathbb{Q}(A[q])$, then we have

$$q^2\mid rp+a_{1,A}(p)+r.$$

Proof

From above we know that

$$q^2\mid rp-r-qb_{1,A}(p)_q=rp+a_{1,A}(p)+r.$$ □

LEMMA 2.6

We have

$$\left|a_{1,A}(p)\right|\le 2rp^{1/2}.$$

Proof

Since $a_{1,A}(p)=-\sum_{i=1}^r(x_{i,p}+\bar{x}_{i,p})$ and $|x_{i,p}|=p^{1/2}$, for $i=1,\ldots,r$, we are done. □

LEMMA 2.7

Let A be an abelian variety over $\mathbb{Q}$. Let $S_\epsilon(x)$ be the set of primes $p\in\mathcal{P}_A$ such that $p\le x$, all odd prime divisors of $p-1$ are distinct and greater than or equal to $x^{1/4+\epsilon}$, and p does not split completely in $\mathbb{Q}(A[2],2^{-1}a)$. If $\mathbb{Q}(A[2])=\mathbb{Q}$ and $\mathbb{Q}(A[2],2^{-1}a)\neq\mathbb{Q}$, then there exists an $\epsilon>0$ such that

$$\left|S_\epsilon(x)\right|\gg\frac{x}{(\log x)^2}.$$

Proof

Since $\mathbb{Q}(A[2])=\mathbb{Q}$ and $\mathbb{Q}(A[2],2^{-1}a)\neq\mathbb{Q}$, we have that the field $\mathbb{Q}(A[2],2^{-1}a)$ is a nontrivial abelian extension of $\mathbb{Q}$. Hence, the same proof as that for [5, Lemma 3] goes through. □

3. The proof of Theorem 1.1

Let $\epsilon > 0$ satisfy Lemma 2.7. For each $c \in \mathbb{Z}$ such that $|c| \leq 2rx^{1/2}$, we define

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

From Lemma 2.6, we know that $|a_{1,A}(p)| \leq 2rx^{1/2}$, and thus, $S_\epsilon(x)$ is a disjoint union of $S_{\epsilon,c}(x)$. For each c as above, we want to count the number of $p \in S_{\epsilon,c}(x)$ for which $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ does not have at most $(2r-1)$ cyclic components. If $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ does not have at most $(2r-1)$ cyclic components, then $(\mathbb{Z}/q\mathbb{Z})^{2r} \subset \frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ for some prime q, and from Lemma 2.2 and from the definition of $S_\epsilon(x)$, 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

$$q \mid p-1,$$

and from Lemma 2.5, we know that

$$q^2 \mid rp + a_{1,A}(p) + r = rp + c + r.$$

Thus, $q \mid c + 2r$. We have that $c \neq -2r$, because otherwise $q^2 \mid r(p-1)$. (We already know that $q \mid p-1$, and from the definition of $S_\epsilon(x)$, for x large enough one can assume that $(q,r) = 1$, and hence $q^2 \mid r(p-1)$ would imply that $q^2 \mid p-1$, which is a contradiction with the definition of $S_\epsilon(x)$.) Since $q \geq x^{1/4+\epsilon}$ and $|c| \leq 2rx^{1/2}$, for x sufficiently large, q is determined by c. If $p \in S_{\epsilon,c}(x)$ is such that $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ does not have at most $(2r-1)$ cyclic components, then from above we get that

$$rp \equiv -c - r \bmod q^2.$$

Hence, the number of such p's is less than

$$\frac{x}{q^2} + O(1) \ll x^{1/2-2\epsilon}.$$

Thus, we proved that the number of $p \in S_\epsilon(x)$ for which $\frac{\bar{A}(\mathbb{F}_p)}{\langle \bar{a}_1,\ldots,\bar{a}_g\rangle}$ does not have at most $(2r-1)$ cyclic components is

$$x^{1/2-2\epsilon}x^{1/2} = o\Big(\frac{x}{(\log x)^2}\Big).$$

This completes the proof of Theorem 1.1. □

REMARK 3.1

We remark that Theorem 1.1 and Lemma 2.7 are true if one replaces the assumption "$\mathbb{Q}(A[2]) = \mathbb{Q}$ and $\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$" by the assumption "$\mathbb{Q}(A[2], 2^{-1}a) \neq \mathbb{Q}$ contains a nontrivial abelian extension of $\mathbb{Q}$" (which is satisfied, for example, when A is an elliptic curve over $\mathbb{Q}$).

References

[1] A. Brumer and K. Kramer *Non-existence of certain semistable abelian varieties*, Manuscripta Math. **106** (2001), 291–304. MR 1869222. DOI 10.1007/PL00005885.

[2] J. W. S. Cassels and A. Fröhlich, eds., *Algebraic Number Theory*, 2nd ed., London Math. Soc., London, 2010. MR 0215665.

[3] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251. MR 0463176.

[4] R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compos. Math. **58** (1986), 13–44. MR 0834046.

[5] ———, *Cyclicity and generation of points* mod p *on elliptic curves*, Invent. Math. **101** (1990), 225–235. MR 1055716. DOI 10.1007/BF01231502.

[6] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR 0207630.

[7] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684. MR 0106226.

[8] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **83** (1977), 289–292. MR 0427273.

[9] D. Mumford, *Abelian Varieties*, Tata Inst. Fundam. Res. Stud. Math. **5**, Hindustan Book Agency, New Delhi, 2008. MR 2514037.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, Dordrecht, 2009. MR 2514094. DOI 10.1007/978-0-387-09494-6.

Department of Mathematics, Yonsei University, Seoul, South Korea;
cristian.virdol@gmail.com