AN ANALOGUE OF A CONJECTURE OF RASMUSSEN AND TAMAGAWA FOR ABELIAN VARIETIES OVER FUNCTION FIELDS

MENTZELOS MELISTAS

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic

University of Twente, Department of Applied Mathematics, Drienerlolaan 5, 7522 NB Enschede, The Netherlands

Abstract. Let L be a number field and let ℓ be a prime number. Rasmussen and Tamagawa conjectured, in a precise sense, that abelian varieties whose field of definition of the ℓ-power torsion is both a pro-ℓ extension of $L(\mu_\ell)$ and unramified away from ℓ are quite rare. In this paper, we formulate an analogue of the Rasmussen–Tamagawa conjecture for non-isotrivial abelian varieties defined over function fields. We provide a proof of our analogue in the case of elliptic curves. In higher dimensions, when the base field is a subfield of the complex numbers, we show that our conjecture is a consequence of the uniform geometric torsion conjecture. Finally, using a theorem of Bakker and Tsimerman we also prove our conjecture unconditionally for abelian varieties with real multiplication.

1. introduction

Let L be a number field and let ℓ be a prime number. Denote by $\tilde{L}_\ell$ the maximal pro-ℓ extension of $L(\mu_\ell)$ which is unramified away from ℓ, where μ_ℓ is the group of ℓ-th roots of unity in a fixed algebraic closure $\overline{L}$ of L. Given an integer $d \geq 1$, a prime ℓ, and a number field L, we also denote by $\mathscr{A}(L, d, \ell)$ the set of L-isomorphism classes of d-dimensional abelian varieties A/L which satisfy the following inclusion

$$L(A[\ell^\infty]) \subseteq \tilde{L}_\ell.$$

The motivation to consider the fields $\tilde{L}_\ell$ comes from Galois representations arising from $\mathbb{P}^1_{01\infty} := \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$. More precisely, let $\Phi : \mathrm{Gal}(\overline{L}/L) \longrightarrow \mathrm{Out}(\pi_1^\ell(\mathbb{P}^1_{01\infty}))$ be the natural outer Galois representation of the pro-ℓ fundamental group of $\mathbb{P}^1_{01\infty}$ and let $M := \overline{L}^{\ker(\Phi)}$ be the fixed field of its kernel. Anderson and Ihara in [2] showed the inclusion $M \subseteq \tilde{L}_\ell$. The following question, posed by Ihara in [13], is still open; For $L = \mathbb{Q}$, is it true that $M = \tilde{L}_\ell$? A natural source of sub-extensions of M comes from abelian varieties that belong to $\mathscr{A}(L, d, \ell)$. Examples of primes ℓ and abelian varieties in $\mathscr{A}(L, d, \ell)$ have been found in [2], [22], [21], and [23]. However, it seems that such examples are actually quite rare. This motivated Rasmussen and Tamagawa, in [23], to formulate the following conjecture.

Conjecture 1.1. (Rasmussen–Tamagawa) For any number field L and integer $d \geq 1$ there exists a number $N = N(L, d)$ such that $\mathscr{A}(L, d, \ell) = \emptyset$ for $\ell > N$.

Date: October 18, 2023.

For an integer $d \geq 1$ and a number field L, we define

$$\mathscr{A}(L,d) = \{([A],\ell) \; : \; A \in \mathscr{A}(L,d,\ell)\}.$$

We note that it follows from the Shafarevich conjecture, which is a theorem due to Faltings [9], that for fixed L, d, and ℓ as above the set $\mathscr{A}(L,d,\ell)$ is finite. Therefore, Conjecture 1.1 is equivalent to the following statement; For any number field L and integer $d \geq 1$ the set $\mathscr{A}(L,d)$ is finite.

Conjecture 1.1 has been proven in many cases. First, in [23], Conjecture 1.1 is proved in the case where $d = 1$ and $L = \mathbb{Q}$, as well as in the case where $d = 1$ and $L/\mathbb{Q}$ is a quadratic extension such that K is not an imaginary quadratic field of class number 1. Moreover, Rasmussen and Tamagawa [24] proved Conjecture 1.1 conditionally on the Generalized Riemann Hypothesis, unconditionally for all semi-stable abelian varieties, and unconditionally for $d = 1$ when $L/\mathbb{Q}$ has degree 2, 3, or when $L/\mathbb{Q}$ is Galois of exponent 3. Bourdon [5], for CM elliptic curves, and more generally Lombardo [16], for CM abelian varieties, proved a uniform version of Conjecture 1.1. Finally, a Drinfeld module analogue has been proven by Okumura [20].

In this paper we are interested in formulating an analogue of Conjecture 1.1 for abelian varieties over function fields. More precisely let k be a perfect field of characteristic $p \geq 0$ and let C/k be a smooth, projective, and geometrically connected curve over k. We denote by K the function field $k(C)$ of the curve C/k. We are interested in stating an analogue of Conjecture 1.1 over the field K.

Fix an algebraic closure $\overline{K}$ of K. Recall that an abelian variety A/K is called *constant* if there exists an abelian variety A_0/k such that $A \cong A_0 \times_k K$. An abelian variety A/K is called *isotrivial* if the base change $A_{\overline{K}}/\overline{K}$ of A/K to $\overline{K}$ is constant. Finally, an abelian variety A/K is called *non-isotrivial* if it is not isotrivial.

If ℓ is any prime with $\ell \neq p$, then we let $\tilde{K}'_\ell$ be the maximal pro-ℓ extension of $K(\mu_\ell)$, where μ_ℓ is the group of ℓ-th roots of unity in a fixed algebraic closure $\overline{K}$ of K. Moreover, we denote by $\mathscr{A}'(K,d,\ell)$ the set of K-isomorphism classes of d-dimensional non-isotrivial abelian varieties A/K which satisfy the following condition

$$K(A[\ell^\infty]) \subseteq \tilde{K}'_\ell.$$

Our analogue of Conjecture 1.1 is the following.

Conjecture 1.2. Let k be a perfect field and let C/k be a smooth, projective, and geometrically connected curve with function field $K = k(C)$. Then for any integer $d \geq 1$ there exists a number $N = N(K,d)$ such that $\mathscr{A}'(K,d,\ell) = \emptyset$ for $\ell > N$.

We note in contrast to the number field case for each prime ℓ the set $\mathscr{A}'(K,d,\ell)$ is not necessarily finite. This is because we do not impose any ramification requirements in the definition of $\tilde{K}'_\ell$ as in the definition of $\tilde{L}_\ell$. For every prime ℓ, which is different from the characteristic of K, one could choose a place $\mathfrak{P}_\ell$ of K and require that $\tilde{K}'_\ell$ is in addition unramified away from $\mathfrak{P}_\ell$. We do not require this ramification condition in our case because in our theorem below such a restrictive condition is not necessary.

Our main theorem in this article is the following theorem, which provides proof for Conjecture 1.2 in dimension 1.

Theorem 1.3. *Let k be a perfect field and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Then we have that $\mathscr{A}'(K,1,\ell) = \emptyset$ for every $\ell > 6 + \sqrt{1 + 24g}$.*

We also produce examples (Example 2.8 and Example 2.9) which show that Theorem 1.3 is sharp when $g = 0$ and $g = 1$. In higher dimensions, we are not able to prove Conjecture 1.2 in full generality. However, when the characteristic of k is zero, we provide evidence for our conjecture by showing that the uniform geometric torsion conjecture for abelian varieties over function fields (Conjecture 2.3) implies Conjecture 1.2, see Theorem 2.4 below. We also prove the following unconditional theorem.

Theorem 1.4. *Let d be a positive integer, let k be a field, and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Then the following are true.*

- *(i) (Proposition 3.1) If k is a finite field of characteristic p and A/K is an abelian variety that belongs to $\mathscr{A}'(K, d, \ell)$ for some $\ell > 2d+1$, then A/K has semi-stable reduction at all places of K.*
- *(ii) (Theorem 2.6) Assume that k is a subfield of $\mathbb{C}$ and let $\mathscr{A}'_{RM}(K, d, \ell)$ be the set of abelian varieties A/K that belong to $\mathscr{A}'(K, d, \ell)$ and have real multiplication. Then there exists a constant $N := N(g, d)$ (depending only on g and d) such that if A/K an abelian variety that belongs to $\mathscr{A}'_{RM}(K, d, \ell)$, then we must have that $\ell < N$.*

This article is organized as follows. In Section 2 we prove Theorem 1.3 and we show that our theorem is sharp, when the genus of C/k is 0 or 1. Moreover, we prove part (ii) of Theorem 1.4 and we show that the uniform geometric torsion conjecture over function fields (Conjecture 2.3) implies Conjecture 1.2. Section 3 mostly concerns the case where the characteristic of k is positive. After proving part (i) of Theorem 1.4, we prove that Conjecture 1.2 is true for a general class of Jacobians, and then we discuss why an analogue of Conjecture 1.2 for abelian varieties over finite fields does not seem to exist. Finally, in the last section, we consider the possibility of formulating a generalization of Conjecture 1.2 by replacing the fields $K(\mu_\ell)$ with more general field extensions.

Acknowledgement. The author was supported by Czech Science Foundation (GAČR) grant 21-00420M and by Charles University Research Center program No.UNCE/SCI/022.

2. Proof of Theorem 1.3

In this section, we first prove Theorem 1.3. Then we relate Conjecture 1.2 to the uniform geometric torsion conjecture over function fields. More precisely, we show that Conjecture 2.3 implies Conjecture 1.2. Finally, we prove part (ii) of Theorem 1.4 using a Theorem of Bakker and Tsimerman from [3].

We start our discussion with a lemma that will be very useful for our results.

Lemma 2.1. *Let k be a perfect field of characteristic $p \geq 0$ and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Let $\ell \neq p$ be a prime. If the degree of the extension $K(A[\ell])/K(\mu_\ell)$ is equal to a power of ℓ, then $A_{K(\mu_\ell)}/K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point of order ℓ.*

Proof. The main tool for our proof is the following group theoretic lemma which is essentially due to Rasmussen and Tamagawa [24, Lemma 3.4] (see also [20, Lemma 5.1]).

Lemma 2.2. *Let ℓ be a prime and let G be a profinite group with a pro-ℓ open normal subgroup N. Assume that $C = G/N$ is a finite cyclic group of order dividing $\ell-1$. Let V be a vector space* *over $\mathbb{F}_\ell$ of dimension r on which G acts continuously. Fix a group homomorphism $\chi_0 : G \longrightarrow \mathbb{F}_\ell^\times$ with* $\mathrm{Ker}(\chi_0) = \mathrm{N}$. *Then there exists a filtration of vector spaces*

$$0 = V_0 \subseteq V_1 \subseteq ... \subseteq V_r = V$$

such that for every $i = 0, ..., r$ the vector space V_i is G-stable of dimension equal to i and such that for every $s = 1, ..., r$ the G-action on the quotient V_s/V_{s-1} is given by $\chi_0^{i_s}$ for some integer i_s with $0 \leq i_s \leq \#C$.

Let now A/K be an abelian variety of dimension d such that $[K(A[\ell]) : K(\mu_\ell)]$ is equal to a power of ℓ. We will show that $A_{K(\mu_\ell)}/K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point of order ℓ. Recall that we denote by $\tilde{K}'_\ell$ the maximal pro-ℓ extension of $K(\mu_\ell)$. Since $K(A[\ell]) \subseteq \tilde{K}'_\ell$, by applying Lemma 2.2 to the case where $G = \mathrm{Gal}(\tilde{K}'_\ell/K)$, $N = \mathrm{Gal}(\tilde{K}'_\ell/K(\mu_\ell))$, $V = A[\ell]$, and χ_0 is equal to the mod-ℓ cyclotomic character $\chi : G \longrightarrow \mathbb{F}_\ell^\times$, we obtain that there exists a basis $\{P_1, ..., P_{2d}\}$ of $A[\ell]$ with respect to which the mod-ℓ Galois representation $\rho_{A,\ell}$ of A/K has the following form

$$\begin{pmatrix} \chi^{i_1} & * & ... & * \\ 0 & \chi^{i_2} & ... & * \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & ... & \chi^{i_{2d}} \end{pmatrix}.$$

From the above matrix, it follows directly that P_1 is a $K(\mu_\ell)$-rational point of order ℓ. This proves our lemma. $\square$

In what follows when we refer to the genus of a function field K we will mean the genus of C/k, where C/k is a smooth, projective, and geometrically connected curve with function field K. We are now ready to proceed to the proof of Theorem 1.3. The key to our proof, and to the proofs of Theorems 2.4 and 2.6 below, is that $K(\mu_\ell)/K$ is a constant extension and, hence, $K(\mu_\ell)$ has the same genus K.

Proof of Theorem 1.3. Let E/K be a non-isotrivial abelian variety that belongs to $\mathscr{A}'(K, 1, \ell)$. We will show that $\ell \leq 6 + \sqrt{1 + 24g}$. First, since $K(\mu_\ell)/K$ is a constant extension, by our assumptions on C/k, it follows that the genus of $K(\mu_\ell)$ is g. Moreover, using Lemma 2.1 we find that $E_{K(\mu_\ell)}/K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point of order ℓ. Therefore, using work of Levin (see [14, Page 460]) we obtain that $\ell \leq 6 + \sqrt{1 + 24g}$. This completes the proof of our theorem. $\square$

The following conjecture, see [6, Page 228], is called the uniform geometric torsion conjecture for abelian varieties over function fields.

Conjecture 2.3. Let k be an algebraically closed field of characteristic 0 and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Then for any integer d, there exists a constant $N := N(k, g, d)$ (which depends on k, g, and d) such that for any d-dimensional abelian variety A/K containing no nontrivial isotrivial abelian subvariety the torsion subgroup $A(K)_{\mathrm{tors}}$ is contained in $A[N]$.

Following the same strategy as in the proof of Theorem 1.3, we can prove the following theorem.

Theorem 2.4. *Let k be a perfect field of characteristic 0 and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Then Conjecture 2.3 (over $\overline{k}$) implies Conjecture 1.2.*

Proof. Let A/K be a non-isotrivial abelian variety that belongs to $\mathscr{A}'(K,d,\ell)$ and we will show that ℓ is bounded. Using Lemma 2.1 we find that $A_{K(\mu_\ell)}/K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point of order ℓ. Let now $\bar{k}$ be the algebraic closure of k and let $K_{\bar{k}}$ denote the function field of $C_{\bar{k}}/\bar{k}$, which has genus g. It follows that $A_{K_{\bar{k}}}/K_{\bar{k}}$ has a $K_{\bar{k}}$-rational point of order ℓ. Therefore, using Conjecture 2.3 we obtain that $\ell \leq N$, for some constant N that depends on k, g, and d. This proves our theorem. $\square$

Recall that an abelian variety with real multiplication is an abelian variety of dimension d such that there exists an injection $\mathcal{O}_F \longrightarrow \mathrm{End}(A)$, where $\mathcal{O}_F$ is the ring of integers of a totally real number field F with $[F:\mathbb{Q}] = d$. The following theorem is due to Bakker and Tsimerman, see [3, Corollary B].

Theorem 2.5. *Fix positive integers d,g, let $k = \mathbb{C}$, and let K be the function field of a smooth, projective, and geometrically connected curve C/k of genus g. Then there exists a constant $N := N(g,d)$ such that for any d-dimensional non-isotrivial abelian variety A/K the torsion subgroup $A(K)_{tors}$ is contained in $A[N]$.*

Recall that $\mathscr{A}'_{\mathrm{RM}}(K,d,\ell)$ is the set of abelian varieties A/K that belong to $\mathscr{A}'(K,d,\ell)$ and have real multiplication.

Theorem 2.6. *Let k be a subfield of $\mathbb{C}$ and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Then there exists a constant $N := N(g,d)$ such that if A/K a d-dimensional abelian variety that belongs to $\mathscr{A}'_{RM}(K,d,\ell)$, then we must have that $\ell \leq N$.*

Proof. The proof is similar to the proof of Theorem 2.4. Assume that there exists a non-isotrivial abelian variety A/K that belongs to $\mathscr{A}'_{\mathrm{RM}}(K,d,\ell)$ and we will show that $\ell \leq N$ for some N that depends on k, g, and d. Using Lemma 2.1 we find that $A_{K(\mu_\ell)}/K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point of order ℓ. Let now $\bar{k} = \mathbb{C}$ be the algebraic closure of k and let $K_{\bar{k}}$ denote the function field of $C_{\bar{k}}/\bar{k}$, which still has genus g. It follows that $A_{K_{\bar{k}}}/K_{\bar{k}}$ has a $K_{\bar{k}}$-rational point of order ℓ. Therefore, using Theorem 2.5 we obtain that $\ell \leq N$, for some constant N that depends on k, g, and d. This proves our theorem. $\square$

The following proposition can be thought of as the converse of Lemma 4.2 for elliptic curves. We will use this proposition below to find elements of $\mathscr{A}'(K,1,\ell)$ and show that the bound provided by Theorem 1.3 is sharp when the genus of K is 0 or 1.

Proposition 2.7. *Let K be a field of characteristic $p \geq 0$, let ℓ be prime with $\ell \neq p$, and let E/K be an elliptic curve. If the base change $E_{K(\mu_\ell)}/K(\mu_\ell)$ of E/K to $K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point of order ℓ, then $K(E[\ell^\infty]) \subseteq \tilde{K}'_\ell$.*

Proof. Assume that $E_{K(\mu_\ell)}/K(\mu_\ell)$ has a $K(\mu_\ell)$-rational point P of order ℓ. We first show, using an idea from [5, Lemma 3], that $[K(E[\ell]):K(\mu_\ell)]$ is either 1 or ℓ. By choosing a basis $\{P,Q\}$ of $E[\ell]$ and considering the mod-ℓ Galois representation with respect to this basis we find that the Galois group $\mathrm{Gal}(K(E[\ell])/K(\mu_\ell))$ is isomorphic to the group H generated by the matrix $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ inside the group $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, for some $a \in \mathbb{F}_\ell$. On the other hand, the group H has cardinality either 1 or ℓ. Therefore, the degree $[K(E[\ell]):K(\mu_\ell)]$ is either 1 or ℓ.

In order to complete our proof it is enough to show that $K(E[\ell^n])/K(E[\ell])$ is an extension of degree a power of ℓ, for every integer $n \geq 2$. We now show this. Recall that for every n we have a natural injective group homomorphism

$$\mathrm{Gal}(K(E[\ell^{n+1}])/K(E[\ell^n])) \longrightarrow \mathrm{Aut}(E[\ell^{n+1}]/E[\ell^n]),$$

where the group on the right is the group of automorphisms of $E[\ell^{n+1}]$ which fix $E[\ell^n]$ pointwise. Therefore, the order of the group $\mathrm{Gal}(K(E[\ell^{n+1}])/K(E[\ell^n]))$ divides the order of the group $\mathrm{Aut}(E[\ell^{n+1}]/E[\ell^n])$. Since $\ell \neq p$, we know that $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ and, hence, the group $\mathrm{Aut}(E[\ell^{n+1}]/E[\ell^n])$ has order a power of ℓ. This proves that $K(E[\ell^{n+1}])/K(E[\ell^n])$ is an extension of degree equal to a power of ℓ. This proves our proposition. □

Let k be a perfect field of characteristic $p \geq 0$. We now show that the bound provided by Theorem 1.3 is sharp when $K = k(C)$, where C/k is a smooth, projective, and geometrically connected curve of genus either 0 or 1. Let ℓ_0 be the largest prime such that $\mathscr{A}'(K, 1, \ell_0) \neq \emptyset$. One may then wonder how large can ℓ_0 be. It follows from Theorem 1.3 that $\ell_0 \leq 7$ if $g = 0$ and that $\ell_0 \leq 11$ if $g = 1$. Using Proposition 2.7 we find that if E/K is an elliptic curve with a K-rational point of order $\ell \neq p$, then E/K belongs to $\mathscr{A}'(K, 1, \ell)$. Therefore, in order to show that Theorem 1.3 is sharp when $g = 0$ or 1, then we just need to find examples of elliptic curves with a K-rational point of order 7 and 11, respectively. We do so in the following two examples, using (well-known) explicit equations for modular curves.

Example 2.8. Let k be a perfect field of characteristic $p \neq 7$, let $K = k(t)$, and let $f \in K$ be a non-constant rational function. Consider the elliptic curve E_f/K given by the following Weierstrass equation

$$E_f : \; y^2 + (1 - f(f-1))xy - f^2(f-1)y = x^3 - f^2(f-1)x^2.$$

The discriminant of the above equation is

$$\Delta_f = f^7(f-1)^7(f^3 - 8f^2 + 5f + 1).$$

Since Δ_f is non-zero in K, we see that indeed E_f/K is an elliptic curve. The c_4-invariant of E_f/K is

$$c_4 = (f^2 - f + 1)(f^6 - 11f^5 + 30f^4 - 15f^3 - 10f^2 + 5f + 1).$$

Moreover, the curve E_f/K is non-isotrvial because the j-invariant of E_f/K is $j_{E_f} = \frac{c_4^3}{\Delta_f}$ is non-constant. Finally, since the point $(0,0)$ is a K-rational point of order 7 of E_f/K (see [12, Section 4.4]), it follows that the curve E_f/K belongs to $\mathscr{A}'(K, 1, 7)$.

Example 2.9. (see [27] and [18, Page 64]) Let k be a perfect field of characteristic $p \neq 11$. Consider the modular curve $X_1(11)/k$ which parametrizes elliptic curves with torsion points of order 11. The curve $X_1(11)/k$ is an elliptic curve which can be given by the following affine equation

$$u^2 + (t^2 + 1)u + t = 0.$$

We note that the above equation is not the standard short Weierstrass equation that one can find in the LMFDB database [15], but it is an equation optimized for computations [27]. Another equation for $X_1(11)/k$ can be found in [25, Example III.1.1.3]. Let $K = k(X_1(11)) = k(t, u)$ and consider, for every $n \geq 0$, the elliptic curve E_n/K given by the following Weierstrass equation

$$E_n : \; y^2 + (1-a)^{p^n} - b^{p^n}y = x^3 - b^{p^n}x^2,$$

where $a = -(u+1)t - u^2 - u + 1$ and $b = a(ut+1)$. For every $n \geq 0$ it follows that E_n/K has a K-rational point of order 11, namely $(0,0)$. Therefore, when E_n/K is non-isotrivial, it belongs to $\mathscr{A}'(K, 1, 11)$.

3. Abelian varieties over fields of positive characteristic

In this section, we first show that if an abelian variety A/K belongs to $\mathscr{A}'(K,d,\ell)$ for $\ell > 2d+1$, then it must have semi-stable reduction at all places of K. We then prove that Conjecture 1.2 is true for a general class of Jacobians. Finally, we consider the situation in the case where K is a finite field, instead of a function field.

Before we proceed we need to recall a few basic facts concerning reduction of abelian varieties. Let $\mathcal{O}_{K_v}$ be a discrete valuation ring with valuation v, fraction field K_v, and perfect residue field k_v. Let A/K_v be an abelian variety of dimension d with Néron model $\mathcal{A}/\mathcal{O}_{K_v}$ (see [4] or [17] for the definition as well as the basic properties of Néron models). The special fiber $\mathcal{A}_{k_v}/k_v$ of $\mathcal{A}/\mathcal{O}_{K_v}$ is a smooth commutative group scheme. We denote by $\mathcal{A}^0_{k_v}/k_v$ the connected component of the identity of $\mathcal{A}_{k_v}/k_v$. By a theorem of Chevalley (see [8, Theorem 1.1]) we have a short exact sequence

$$0 \longrightarrow T\times U \longrightarrow \mathcal{A}^0_{k_v} \longrightarrow B \longrightarrow 0,$$

where T/k_v is a torus, U/k_v is a unipotent group, and B/k_v is an abelian variety. We say that A/K_v has semi-stable reduction if $\dim(U)=0$. If now k is a finite field of characteristic p and $K=k(C)$, where C/k is a smooth, projective, and geometrically connected curve, then we will say that A/K has semi-stable reduction at a place v if A_{K_v}/K_v has semi-stable reduction. Here K_v is the completion of K at v. Moreover, we will say that A/K is semi-stable if it has semi-stable reduction at every place v of K.

Proposition 3.1. *Let k be a finite field of characteristic p and let C/k be a smooth, projective, and geometrically connected curve with function field $K=k(C)$. If A/K is an abelian variety that belongs to $\mathscr{A}'(K,d,\ell)$ for some $\ell > 2d+1$, then A/K is semi-stable.*

Proof. Let A/K be an abelian variety that belongs to $\mathscr{A}'(K,d,\ell)$, for some $\ell > 2d+1$, and we will show that it has semi-stable reduction at every finite place v of K. Since $K(\mu_\ell)/K$ is a constant extension, then it is an everywhere unramified extension. Moreover, since an everywhere unramified base extension does not affect whether an abelian variety is semi-stable, by considering the base change $A_{K(\mu_\ell)}/K(\mu_\ell)$ of A/K to $K(\mu_\ell)$, we can assume from now on that $K(\mu_\ell)=K$ and that $K(A[\ell])/K$ is a field extension of degree equal to a power of ℓ.

Let v be a place of K and let K_v be the completion of K at v. We also denote by K_v^{unr} the maximal unramified extension of K_v. Since $K(A[\ell])/K$ is a Galois extension, we find that the degree of the extension $K_v^{unr}(A[\ell])/K_v^{unr}$ divides the degree of the extension $K(A[\ell])/K$. Therefore, since $K(A[\ell])/K$ is a field extension of degree equal to a power of ℓ, we find that the same is true for $K_v^{unr}(A[\ell])/K_v^{unr}$. It follows from a theorem due to Raynaud [1, Proposition 4.7] that the base change $A_{K_v^{unr}(A[\ell])}/K_v^{unr}(A[\ell])$ of A/K to $K_v^{unr}(A[\ell])$ has semi-stable reduction. On the other hand, by [17, Theorem 3.8] there exists a minimal extension $K_{A_{K_v^{unr}}}/K_v^{unr}$ over which $A_{K_v^{unr}}/K_v^{unr}$ acquires semi-stable reduction. Moreover, every prime that divides the degree of $K_{A_{K_v^{unr}}}/K_v^{unr}$ is at most $2d+1$, see [7, Theorem 6.8]. By the minimality of $K_{A_{K_v^{unr}}}/K_v^{unr}$ we must have that

$$K_{A_{K_v^{unr}}} \subseteq K_v^{unr}(A[\ell]).$$

By comparing the degrees of the extensions $K_{A_{K_v^{unr}}}/K_v^{unr}$ and $K_v^{unr}(A[\ell])/K_v^{unr}$ we find that $K_{A_{K_v^{unr}}} = K_v^{unr}$. This proves that the variety A_K/K has semi-stable reduction at v. $\square$

Remark 3.2. Let L be a number field and let A/L be an abelian variety that belongs to the set $\mathscr{A}(L,g,\ell)$, for some prime number ℓ. If $L(\mu_\ell)=L$ and $\ell > 2d+1$, then exactly the same argument as in the proof of Proposition 3.1 proves that A/L has everywhere semi-stable reduction.

We now prove for a general class of Jacobians over $\mathbb{F}_q(t)$ that if they belong to $\mathscr{A}'(\mathbb{F}_q(t), d, \ell)$, then $\ell = 2$, thus providing additional evidence for Conjecture 1.2 over $\mathbb{F}_q(t)$. Let d be a positive integer, let q be a odd prime power and let $f(x) \in \mathbb{F}_q[x]$ be a monic square-free polynomial of degree $2d$. Consider the hyperelliptic curve $C/\mathbb{F}_q(t)$ given by the following affine equation

$$C : y^2 = (t - x)f(x)$$

and denote by $J_C/\mathbb{F}_q(t)$ the Jacobian of the curve $C/\mathbb{F}_q(t)$, which is a d-dimensional abelian variety. The following proposition is a consequence of a Theorem of Hall [11], originally due to Jiu-Kang Yu.

Proposition 3.3. *If the abelian variety $J_C/\mathbb{F}_q(t)$ belongs to $\mathscr{A}'(\mathbb{F}_q(t), d, \ell)$, then $\ell = 2$.*

Proof. Assume that $\ell > 2$. It follows from [11, Theorem 4.1] that the extension $K(J_C[\ell])/K(\mu_\ell)$ has Galois group $\mathrm{Sp}(2g, \mathbb{F}_\ell)$. On the other hand, we know that the group $\mathrm{Sp}(2d, \mathbb{F}_\ell)$ has order equal to $\ell^{d^2} \prod_{i=1}^{d} (\ell^{2i} - 1)$. Therefore, the field extension $K(J_C[\ell])/K(\mu_\ell)$ cannot have order a power of ℓ and, hence, the variety J_C/K does not belong to $\mathscr{A}'(\mathbb{F}_q(t), d, \ell)$. This proves our proposition. □

We end this section by discussing why a similar analogue of the Rasmussen Tamagawa conjecture does not seem to exist for abelian varieties over finite fields. Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p. We fix an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$ and for every integer $m \geq 1$ we denote by $\mathbb{F}_{q^m}$ the unique subfield of $\overline{\mathbb{F}_q}$ that has q^m elements.

We first recall some necessary background on abelian varieties over finite fields. The reader is referred to [19, Chapter II] for more information. Let $A/\mathbb{F}_q$ be a d-dimensional abelian variety and denote by ϕ the Frobenius endomorphism of $A/\mathbb{F}_q$. Recall that the characteristic polynomial of ϕ, denoted by $P_\phi(x)$, is a monic polynomial of degree $2d$ which belongs in $\mathbb{Z}[x]$. Write $P_\phi(x) = \prod_{i=1}^{2d}(x - \alpha_i)$, where $\alpha_1, ..., \alpha_{2d} \in \mathbb{C}$ are the roots of $P_\phi(x)$ (not necessarily distinct). For every integer $m \geq 1$ we know the following equality

$$\#A(\mathbb{F}_{q^m}) = \prod_{i=1}^{2d}(1 - \alpha_i^m). \tag{1}$$

If $A/\mathbb{F}_q$ is an abelian variety and $\ell \neq p$, then, using an argument similar to the second paragraph of the proof of Proposition 2.7, we find that $\mathbb{F}_q(A[\ell^\infty])$ is contained in the maximal pro-ℓ extension of $\mathbb{F}_q$ if and only if the field extension $\mathbb{F}_q(A[\ell])/\mathbb{F}_q(\mu_\ell)$ has degree a power of ℓ. Let now f be the smallest integer such that $q^f \equiv 1 \pmod{\ell}$. The degree of the extension $\mathbb{F}_q(\mu_\ell)/\mathbb{F}_q$ is equal to f and, hence, we have that $\mathbb{F}_q(\mu_\ell) = \mathbb{F}_{q^f}$. For every $e \geq 0$, let $\mathbb{F}_{q^{f\ell^e}}$ be the unique subfield of $\overline{\mathbb{F}_q}$ such that the extension $\mathbb{F}_{q^{f\ell^e}}/\mathbb{F}_{q^f}$ has degree ℓ^e. We now want to examine when $[\mathbb{F}_q(A[\ell]) : \mathbb{F}_q(\mu_\ell)] = \ell^e$, for some $e \geq 0$, i.e., when $\mathbb{F}_q(A[\ell]) = \mathbb{F}_{q^{f\ell^e}}$. Using Equation (1), we find that

$$A(\mathbb{F}_{q^{f\ell^e}}) = \prod_{i=1}^{2d}(1 - \alpha_i^{f\ell^e}).$$

Since ℓ^2 divides $\#A(\mathbb{F}_q(A[\ell]))$, if $A(\mathbb{F}_q(A[\ell])) = A(\mathbb{F}_{q^{f\ell^e}})$ for some $e \geq 0$, then we find that ℓ^2 must divide the product $\prod_{i=1}^{2d}(1 - \alpha_i^{f\ell^e})$. Therefore, whether $\mathbb{F}_q(A[\ell^\infty])$ is contained in the maximal pro-ℓ extension of $\mathbb{F}_q$ depends on the solutions to the characteristic polynomial of the Frobenius endomorphism of $A/\mathbb{F}_q$.

To be more concrete, assume that $q = p \geq 5$ is a prime, that $\ell > p$, and that our abelian variety is a supersingular elliptic curve which we denote by $E/\mathbb{F}_p$. In this case, the polynomial $P_\phi(x)$ is a quadratic polynomial with roots α_1 and α_2. Since $E/\mathbb{F}_p$ is supersingular , we have that $\#E(\mathbb{F}_p) = p + 1$ and, hence, using Equation (1) (or [26, Theorem V.2.3.1]) we find that $\alpha_1 = -\alpha_2$. This implies, by [26, Theorem V.2.3.1], that

$$\#E(\mathbb{F}_{p^{f\ell^e}}) = \begin{cases} p^{f\ell^e} + 1, & \text{if } f \text{ is odd} \\ (p^{\frac{f\ell^e}{2}} - (-1)^{\frac{f\ell^e}{2}})^2, & \text{if } f \text{ is even} \end{cases}$$

We now show that in this case, whether $\mathbb{F}_p(E[\ell^\infty])$ is contained in the maximal pro-ℓ extension of $\mathbb{F}_p$ depends on f. It follows from the Weil pairing, see [28, Proposition 1.11] for a self-contained proof, that if ℓ divides $\#E(\mathbb{F}_{p^{f\ell^e}})$, for some $e \geq 0$, then the extension $\mathbb{F}_p(E[\ell)/\mathbb{F}_{q^f}$ has degree equal to a power of ℓ. Therefore, using a similar argument as in the second paragraph of the proof of Proposition 2.7 we find that if ℓ divides $\#E(\mathbb{F}_{p^{f\ell^e}})$, then $\mathbb{F}_p(E[\ell^\infty])$ is contained in the maximal pro-ℓ extension of $\mathbb{F}_p$.

Assume that f is even. We will show that if $f \equiv 0 \pmod 4$, then ℓ does not divide $\#E(\mathbb{F}_{p^{f\ell^e}})$ and that if $f \equiv 2 \pmod 4$, then ℓ does divide $\#E(\mathbb{F}_{p^{f\ell^e}})$. Since f is even, we see that $\#E(\mathbb{F}_{p^{f\ell^e}}) = (p^{\frac{f\ell^e}{2}} - (-1)^{\frac{f\ell^e}{2}})^2$. Therefore, we have that

$$\#E(\mathbb{F}_{p^{f\ell^e}}) \equiv ((p^{\ell^e})^{\frac{f}{2}} - ((-1)^{\ell^e})^{\frac{f}{2}})^2 \equiv (p^{\frac{f}{2}} - (-1)^{\frac{f}{2}})^2 \pmod{\ell}.$$

On the other hand, since f is the smallest integer such that $p^f \equiv 1 \pmod{\ell}$, we find that $p^{\frac{f}{2}} \equiv -1 \pmod{\ell}$. Consequently, if $f \equiv 2 \pmod 4$, then $\#E(\mathbb{F}_{p^{f\ell^e}}) \equiv (-1+1)^2 \equiv 0 \pmod{\ell}$. On the other hand, if $f \equiv 0 \pmod 4$, then $\#E(\mathbb{F}_{p^{f\ell^e}}) \equiv (-1-1)^2 \equiv 4 \pmod{\ell}$ and, hence, ℓ does not divide $\#E(\mathbb{F}_{p^{f\ell^e}})$.

Finally we show that if f is odd, then ℓ does not divide $\#E(\mathbb{F}_{p^{f\ell^e}})$. Indeed, since f is odd, we see that $\#E(\mathbb{F}_{p^{f\ell^e}}) = p^{f\ell^e} + 1$. Therefore, we have that

$$\#E(\mathbb{F}_{p^{f\ell^e}}) \equiv (p^{\ell^e})^f + 1 \equiv p^f + 1 \equiv 2 \pmod{\ell},$$

where the last congreunce is true because $p^f \equiv 1 \pmod{\ell}$.

4. A POSSIBLE GENERALIZATION

Let k be a perfect field of characteristic $p \geq 0$ and let C/k be a smooth, projective, and geometrically connected curve with function field $K = k(C)$. One may wonder whether we can replace the extensions $K(\mu_\ell)/K$ with more general (possibly ramified) extensions in Conjecture 1.2. More precisely, for every prime $\ell \neq p$ let M_ℓ/K be a finite extension and for each M_ℓ consider the maximal pro-ℓ extension $K_{M_\ell}^{\text{pro}-\ell}$ of M_ℓ. One may now wonder for which M_ℓ would the statement of Conjecture 1.2 still make sense after replacing $\tilde{K}_\ell'$ with $K_{M_\ell}^{\text{pro}-\ell}$.

As an example, we show below that if for every ℓ we take M_ℓ/K to be a Galois extension of degree dividing $\ell - 1$, then we still have that the variant of Conjecture 1.2 is true for elliptic curves.

Theorem 4.1. *Let k be a perfect field and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. Let E/K be a non-isotrivial elliptic curve, let ℓ be a prime number, and let L/K be a Galois extension of degree dividing $\ell - 1$. If the degree of the extension $K(E[\ell])/L$ is a power of ℓ, then $\ell \leq 49\max\{1, g\}$.*

Proof. Let K be as in the theorem and let E/K be a non-isotrivial elliptic curve. We will show that if the degree of the extension $K(E[\ell])/L$ is a power of ℓ, then $\ell \leq 49\max\{1,g\}$. The main tool in our proof is the following lemma.

Lemma 4.2. *The $\mathbb{F}_\ell$-vector space $E[\ell]$ has a cyclic Gal(K^{sep}/K)-stable subgroup.*

Proof of the lemma. The strategy for the proof of the lemma is inspired by the arguments of the proof of [23, Lemma 3]. We include all the relevant details in order to make our proof self-contained.

Let $G = \mathrm{Gal}(K(E[\ell])/K)$, let $N = \mathrm{Gal}(K(E[\ell])/L)$, and let $\Delta = G/N = \mathrm{Gal}(L/K)$. By assumption, the group N is a finite ℓ-group. Therefore, each of the orbits of $E[\ell]$ under N must have order equal to a power of ℓ. This implies that the subspace $E[\ell]^N$ of fixed points of $E[\ell]$ under the action of N is not equal to $\{0\}$. Indeed, if $E[\ell]^N = \{0\}$, then we would have that ℓ divides $\#E[\ell] - 1$ which is not possible.

If $\Delta = G/N$ is trivial, which occurs when $L = K$, then we have that $E[\ell]^G = E[\ell]^N \neq \{0\}$. Therefore, either the action of G on $E[\ell]$ is trivial or $E[\ell]^G$ is a subspace of dimension 1. Hence, either the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[\ell]$ is trivial or $E[\ell]^{\mathrm{Gal}(K^{\mathrm{sep}}/K)} = E[\ell]^G$ is a subspace of dimension 1. This proves our lemma in the case where Δ is trivial. Therefore, we can assume from now on that $\Delta \neq \{0\}$.

Assume from now on that Δ is not trivial. Since N is a normal subgroup of G, it follows that $E[\ell]^N$ is G-stable (as a set). Consequently, there is a well defined action of $\Delta = G/N$ on $E[\ell]^N$. Fix a basis of $E[\ell]^N$ and consider the associated representation $\rho : \Delta \longrightarrow \mathrm{GL}(E[\ell]^N)$. If δ is a generator of Δ, since $\delta^{\ell-1} = 1$, we have that $\rho(\delta)^{\ell-1} = I$. Therefore, the minimal polynomial of $\rho(\delta)$ splits completely over $\mathbb{F}_\ell$ and, hence, the matrix $\rho(\delta)$ has an eigenvalue λ in $\mathbb{F}_\ell^\times$. Let W be the subspace generated by an eigenvector with respect to λ. Then Δ fixes W (as a set), and since $W \subseteq E[\ell]^N$, we see that W is G-stable. This proves that W is a $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-stable subgroup of $E[\ell]$. This proves the lemma. ☐

We are now ready to complete our proof. By Lemma 4.2 we have that there exists a cyclic, $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-stable subgroup of E which has order ℓ. However, since E/K is non-isotrivial and $\ell \neq p$ by assumption, it follows from [10, Proposition 6.5] that $\ell \leq 49\max\{1,g\}$, where g is the genus of the curve C/k. This proves our theorem. ☐

Corollary 4.3. *Let k be a perfect field and let C/k be a smooth, projective, and geometrically connected curve of genus g with function field $K = k(C)$. For every prime ℓ let M_ℓ/K be a Galois extension of degree dividing $\ell - 1$ and consider the set $\mathscr{A}'_{M_\ell}(K,1,\ell)$ which consists of all non-isotrivial elliptic curves E/K such that $K(E[\ell^\infty]) \subseteq K_{M_\ell}^{pro-\ell}$. Then we have that $\mathscr{A}'_{M_\ell}(K,1,\ell) = \emptyset$ for $\ell > 49\max\{1,g\}$.*

References

[1] *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin-New York, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. 7

[2] G. Anderson and Y. Ihara. Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units. *Ann. of Math. (2)*, 128(2):271–293, 1988. 1

[3] B. Bakker and J. Tsimerman. The geometric torsion conjecture for abelian varieties with real multiplication. *J. Differential Geom.*, 109(3):379–409, 2018. 3, 5

[4] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990. 7

[5] A. Bourdon. A uniform version of a finiteness conjecture for CM elliptic curves. *Math. Res. Lett.*, 22(2):403–416, 2015. 2, 5

[6] A. Cadoret and A. Tamagawa. On a weak variant of the geometric torsion conjecture. *J. Algebra*, 346:227–247, 2011. 4

[7] B. Conrad. Semistable reduction for abelian varieties. `http://math.stanford.edu/~conrad/DarmonCM/2011Notes/Sem` [Online; accessed 14 October 2022]. 7

[8] B. Conrad. A modern proof of Chevalley's theorem on algebraic groups. *J. Ramanujan Math. Soc.*, 17(1):1–18, 2002. 7

[9] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. 2

[10] R. Griffon and F. Pazuki. Isogenies of Elliptic Curves Over Function Fields. *Int. Math. Res. Not. IMRN*, 2022(19):14697–14740, 06 2021. 10

[11] C. Hall. Big symplectic or orthogonal monodromy modulo l. *Duke Math. J.*, 141(1):179–203, 2008. 8

[12] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. 6

[13] Y. Ihara. Profinite braid groups, Galois representations and complex multiplications. *Ann. of Math. (2)*, 123(1):43–106, 1986. 1

[14] M. Levin. On the group of rational points on elliptic curves over function fields. *Amer. J. Math.*, 90:456–462, 1968. 4

[15] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2019. [Online; accessed 12 October 2022]. 6

[16] D. Lombardo. On the uniform Rasmussen-Tamagawa conjecture in the CM case. *Math. Res. Lett.*, 25(6):1893–1910, 2018. 2

[17] D. J. Lorenzini. Néron models. *Eur. J. Math.*, 3(2):171–198, 2017. 7

[18] R. J. S. McDonald. *Torsion subgroups of elliptic curves over function fields*. PhD thesis, University of Connecticut, 2019. 6

[19] J. S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/. 8

[20] Y. Okumura. A function field analogue of the Rasmussen-Tamagawa conjecture: the Drinfeld module case. *Kyushu J. Math.*, 73(2):295–316, 2019. 2, 3

[21] M. Papanikolas and C. Rasmussen. On the torsion of Jacobians of principal modular curves of level 3^n. *Arch. Math. (Basel)*, 88(1):19–28, 2007. 1

[22] C. Rasmussen. On the fields of 2-power torsion of certain elliptic curves. *Math. Res. Lett.*, 11(4):529–538, 2004. 1

[23] C. Rasmussen and A. Tamagawa. A finiteness conjecture on abelian varieties with constrained prime power torsion. *Math. Res. Lett.*, 15(6):1223–1231, 2008. 1, 2, 10

[24] C. Rasmussen and A. Tamagawa. Arithmetic of abelian varieties with constrained torsion. *Trans. Amer. Math. Soc.*, 369(4):2395–2424, 2017. 2, 3

[25] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 6

[26] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 9

[27] A. V. Sutherland. Optimized equations for $X_1(N)$ in raw form for N $\leq$ 100. `https://math.mit.edu/~drew/X1_optcurves.html`. [Online; accessed 12 October 2022]. 6

[28] A. L. Van Tuyl. The field of N-torsion points of an elliptic curve over a finite field. Master's thesis, Queen's Univesity, 1997. 9