COMPOSITIO MATHEMATICA

The growth of Tate–Shafarevich groups in cyclic extensions

Yi Ouyang and Jianfeng Xie

Compositio Math. **158** (2022), 2014–2032.

doi:10.1112/S0010437X22007734

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

Compositio Math. 158 (2022) 2014–2032
doi:10.1112/S0010437X22007734

The growth of Tate–Shafarevich groups in cyclic extensions

Yi Ouyang and Jianfeng Xie

Abstract

Let p be a prime number. Kęstutis Česnavičius proved that for an abelian variety A over a global field K, the p-Selmer group $\mathrm{Sel}_p(A/L)$ grows unboundedly when L ranges over the $(\mathbb{Z}/p\mathbb{Z})$-extensions of K. Moreover, he raised a further problem: is $\dim_{\mathbb{F}_p} Ш(A/L)[p]$ also unbounded under the above conditions? In this paper, we give a positive answer to this problem in the case $p \neq \mathrm{char}\, K$. As an application, this result enables us to generalize the work of Clark, Sharif and Creutz on the growth of potential Ш in cyclic extensions. We also answer a problem proposed by Lim and Murty concerning the growth of the fine Tate–Shafarevich groups.

1. Introduction

Let p be a prime number and K be a number field. There is an important result in algebraic number theory (see [Mad72, Theorem 3]):

> The p-torsion subgroup of the ideal class group of L is unbounded as L varies over $(\mathbb{Z}/p\mathbb{Z})$-extensions of K.

The first result of such a kind is due to Gauss, who proved the case $K = \mathbb{Q}$ and $p = 2$. Since the growth problems for ideal class groups and for Selmer groups of abelian varieties are closely related (see [Čes15a]), it is naturally expected that similar results hold for p-Selmer groups of abelian varieties. Based on his generalization of the Cassels–Poitou–Tate sequence, Kęstutis Česnavičius successfully proved the following result.

Theorem 1.1 [Čes17, Theorem 1.2]. *Let p be a prime number, and A be an abelian variety over a global field K. If either $A[p](\bar{K}) \neq 0$ or A is supersingular, then*

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/L)$$

is unbounded as L varies over $(\mathbb{Z}/p\mathbb{Z})$-extensions of K.

For the Tate–Shafarevich groups, when L ranges over degree p extensions of K, Clark and Sharif [CS10] proved that $\dim_{\mathbb{F}_p} Ш(A/L)[p]$ is unbounded in the case $\dim A = 1$ and $p \neq \mathrm{char}\, K$; later Creutz [Cre11] showed the unboundedness of $\dim_{\mathbb{F}_p} Ш(A/L)[p]$ when A is strongly principally polarized over a number field K and the G_K-action on the Néron–Severi group of A is trivial. Note that the extensions L/K they constructed are not necessarily Galois. When fixing a $(\mathbb{Z}/n\mathbb{Z})$-extension $K/\mathbb{Q}$, Matsuno [Mat09] proved that there exist elliptic curves $E/\mathbb{Q}$ with the

Received 15 August 2021, accepted in final form 12 July 2022, published online 4 November 2022.
2020 Mathematics Subject Classification 11G10, 14K15 (primary), 11G05, 11R34, 14K05 (secondary).
Keywords: abelian varieties, Selmer groups, Tate–Shafarevich groups, fine Tate–Shafarevich groups, twist of abelian varieties.

n-rank of $Ш(E/K)[n]$ being arbitrarily large. Based on these results, Česnavičius proposed the following problem [Čes17, Problem 1.8].

Problem 1.2. Is $\dim_{\mathbb{F}_p} Ш(A/L)[p]$ unbounded as L varies over $(\mathbb{Z}/p\mathbb{Z})$-extensions of K?

To attack this problem, one may try to generalize the methods of Clark and Sharif and of Creutz. However, we remark that these are based on the study of the period and index problem in $\mathrm{H}^1(K, A)$, whose generalization to general abelian varieties seems rather difficult.

In this paper we shall present another idea to treat Problem 1.2, which is a combination of the machinery developed by Mazur and Rubin in [MR18] and the method invented by Česnavičius in [Čes17]. Our main result is the following theorem.

Theorem 1.3. *Let A be an abelian variety over a global field K. If p is a prime number not equal to* $\operatorname{char} K$*, then there exists a sequence of $(\mathbb{Z}/p\mathbb{Z})$-extensions $\{L_i/K\}_{i=1}^{\infty}$ satisfying*

$$\operatorname{rank}_{\mathbb{Z}} A(L_i) \leq \begin{cases} \operatorname{rank}_{\mathbb{Z}}(A(K)) + 3(r_0 + 4g), & \text{if } p = 2, \\ \operatorname{rank}_{\mathbb{Z}}(A(K)) + (p-1)(r_0 + 4g), & \text{otherwise,} \end{cases}$$

and

$$\lim_{i \to \infty} \dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/L_i) = \infty,$$

where $r_0 := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/K)$ and $g := \dim A$.

This result gives a positive answer to Problem 1.2 when $p \neq \operatorname{char} K$. Indeed, by the well-known exact sequence

$$0 \to A(L)/pA(L) \to \mathrm{Sel}_p(A/L) \to Ш(A/L)[p] \to 0 \tag{1}$$

and the inequality $\dim_{\mathbb{F}_p} A(L)/pA(L) \leq \operatorname{rank}_{\mathbb{Z}} A(L) + 2\dim(A)$, we have the following result.

Theorem 1.4. *If $p \neq \operatorname{char} K$, then*

$$\dim_{\mathbb{F}_p} Ш(A/L)[p]$$

can be arbitrarily large as L ranges over $(\mathbb{Z}/p\mathbb{Z})$-extensions of K.

Remark 1.5. See Theorems 4.10 and 4.11 for a more detailed description of our main results.

The idea behind the proof of the above results is in fact rather simple. In [Čes17], Česnavičius found a method to construct a sequence of $(\mathbb{Z}/p\mathbb{Z})$-extensions $\{L_i\}_{i=1}^{\infty}$ such that

$$\lim_{i \to \infty} \dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/L_i) = \infty.$$

However, he did not bound $\operatorname{rank}_{\mathbb{Z}} A(L_i)$. We will use the tools developed by Mazur and Rubin in [MR18] to bound the Mordell–Weil ranks.

1.1 Layout of this paper

Section 2 is devoted to introducing the machinery of Mazur and Rubin. In § 3 we generalize Česnavičius's idea to construct $(\mathbb{Z}/n\mathbb{Z})$-extensions L/K with large n-rank of $\mathrm{Sel}_n(A/L)$. We prove our main result, Theorem 4.10, in § 4 and then give applications of this result in the rest of this paper. In § 5 we obtain a result on the growth of the potential Ш in cyclic extensions, which generalizes the work of Clark, Sharif and Creutz in [CS10, Cre11]. In § 6 we solve a problem raised by Lim and Murty in [LM16] concerning the growth of the fine Tate–Shafarevich groups.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

1.2 Notation and convention

- p will always be a prime number.
- A $(\mathbb{Z}/n\mathbb{Z})$-extension is a Galois extension whose Galois group is cyclic of order n, that is, isomorphic to $\mathbb{Z}/n\mathbb{Z}$.
- For a $(\mathbb{Z}/p^k\mathbb{Z})$-extension L/K and $0 \le i \le k$, $L^{(i)}$ is the unique $(\mathbb{Z}/p^i\mathbb{Z})$-subextension of K inside L. Thus $\mathrm{Gal}(L/L^{(i)}) \cong \mathbb{Z}/p^{k-i}\mathbb{Z}$ and $\mathrm{Gal}(L^{(i)}/K) \cong \mathbb{Z}/p^i\mathbb{Z}$.
- For $n \in \mathbb{Z}_{\ge 2}$, the n-rank of an abelian group H, denoted by $r_n(H)$, is the largest $r \in \mathbb{N}$ such that $(\mathbb{Z}/n\mathbb{Z})^r$ can be viewed as a subgroup of H. In particular, $r_{p^k}(H) = \dim_{\mathbb{F}_p} p^{k-1}H/p^kH$.
- If K is a global field, let $\mathcal{P}\ell_K$ denote the set of places of K.
- For any place v of a global field K, we fix a K-embedding $\sigma : \overline{K} \hookrightarrow \overline{K_v}$ and let $L_v = LK_v$ for any finite extension L of K, which is the completion of L with respect to the unique valuation extending v corresponding to the embedding $L \overset{\mathrm{id}}{\hookrightarrow} \overline{K} \overset{\sigma}{\hookrightarrow} \overline{K_v}$.
- If K is a local field, let K^{ur} denote the maximal unramified extension of K.
- For an abelian variety A over a global field K, let $\mathrm{Sel}_n(A/K)$ denote the n-Selmer group of A over K.

2. The machinery of Mazur and Rubin

Suppose K is a field and A is an abelian variety over K. In this section we introduce the machinery developed by Mazur and Rubin in [MR18], which plays a key role in our proof of bounding the Mordell–Weil ranks in $(\mathbb{Z}/p^k\mathbb{Z})$-extensions. However, in [MR18], this machinery requires A to be a simple abelian variety and p be unramified in the center of the endomorphism ring $\mathrm{End}_K(A)$ (see [MR18, § 5] for details). In order to deal with all prime numbers and arbitrary abelian varieties, we revise this machinery slightly so that our revision is closer to the treatment in [MR07]. One should keep in mind the small difference between our setting and that in [MR18]. The results in this section are analogous to those in [MR18, §§ 6–8] and can be proved similarly.

2.1 Twists of abelian varieties

We recall some basic knowledge about twists of abelian varieties. This conception was first discussed by Milne in [Mil72], and later generalized by Mazur and Rubin to the case of commutative algebraic groups in [MRS07].

Suppose $k \ge 1$ and L/K is a $(\mathbb{Z}/p^k\mathbb{Z})$-extension. Recall that $L^{(i)}$ is the unique $(\mathbb{Z}/p^i\mathbb{Z})$-subextension of K inside L. Denote $G := \mathrm{Gal}(L/K)$. We have the following definition in the sense of [MRS07, Definition 1.1].

Definition 2.1. The (L/K)-twist A_L of A is the abelian variety

$$A_L := \mathrm{Ker}\left(\mathbb{Z}[G] \to \mathbb{Z}[\mathrm{Gal}(L^{(k-1)}/K)]\right) \otimes A$$

over K. More concretely, by [MRS07, Theorem 5.8], $A_L = \mathrm{Ker}\left(\mathrm{Res}^L_K A \to \mathrm{Res}^{L^{(k-1)}}_K A\right)$. We also set $A_K = A$.

Remark 2.2. From now on in this paper, A_L always means the (L/K)-twist of A, not to be confused with $A \times_K L$, the base change of A to L.

Notation 2.3. Set

$$\mathbb{Z}_L := \mathbb{Z}[G]/\mathcal{N}\mathbb{Z}[G], \quad \text{where } \mathcal{N} := \sum_{\sigma \in \mathrm{Gal}(L/L^{(k-1)})} \sigma \in \mathbb{Z}[G],$$

which is a free $\mathbb{Z}$-module of rank $\varphi(p^k) = p^{k-1}(p-1)$. Set $\mathbb{Z}_K = \mathbb{Z}$.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

By fixing an isomorphism $G \cong \mu_{p^k}$, we have $\mathbb{Z}_L \cong \mathbb{Z}[\mu_{p^k}]$ and we identify these two through this isomorphism, which gives an inclusion $\mathbb{Z}_L \hookrightarrow \mathbb{Q}(\mu_{p^k})$. Let $\mathfrak{p}_L$ be the unique prime ideal of $\mathbb{Z}_L$ above p. Let $\mathfrak{p}_K = (p)$.

Theorem 2.4. *There is an isomorphism of $\mathbb{Z}[G_K]$-modules*

$$A[p] \cong A_L[\mathfrak{p}_L].$$

Proof. The case where A is an elliptic curve was proved in [MR07, Proposition 4.1]. The proof for the general case is essentially the same. One can also deduce the isomorphism by a similar argument to that in [MR18, Corollary 6.4]. □

2.2 Local conditions

In this subsection we suppose K is a local field whose residue field is $\mathbb{F}_q$ with $p \neq \operatorname{char} \mathbb{F}_q$. Let A be an abelian variety over K. Let L/K be a $(\mathbb{Z}/p^k\mathbb{Z})$-extension, $k \geq 0$.

Notation 2.5. The group $\mathcal{H}(L/K)$ is the subgroup of $\mathrm{H}^1(K, A[p])$ given by

$$\mathcal{H}(L/K) := \operatorname{Im}\left(A_L(K)/\mathfrak{p}_L A_L(K) \hookrightarrow \mathrm{H}^1(K, A_L[\mathfrak{p}_L]) \cong \mathrm{H}^1(K, A[p])\right),$$

where the first inclusion is the Kummer map and the second isomorphism is induced by the isomorphism $A_L[\mathfrak{p}_L] \cong A[p]$ of G_K-modules. In particular, $\mathcal{H}(K) = \mathcal{H}(K/K)$ is the image of the Kummer map

$$\mathcal{H}(K) = \mathcal{H}(K/K) := \operatorname{Im}\left(A(K)/pA(K) \hookrightarrow \mathrm{H}^1(K, A[p])\right).$$

Recall that if $p \neq \operatorname{char} \mathbb{F}_q$ and A/K has good reduction, the unramified subgroup of $\mathrm{H}^1(K, A[p])$ is given by

$$\mathrm{H}^1_{\mathrm{ur}}(K, A[p]) := \ker(\mathrm{H}^1(K, A[p]) \to \mathrm{H}^1(K^{\mathrm{ur}}, A[p])) = \mathrm{H}^1(K^{\mathrm{ur}}/K, A[p]).$$

We have the following basic facts about the subgroups $\mathcal{H}(L/K)$ and $H^1_{\mathrm{ur}}(K, A[p])$ of $\mathrm{H}^1(K, A[p])$.

Lemma 2.6. *Suppose $p \neq \operatorname{char} \mathbb{F}_q$. Then the following assertions hold.*

(1) $\dim_{\mathbb{F}_p} \mathcal{H}(L/K) = \dim_{\mathbb{F}_p} A(K)[p]$.
(2) *If A/K has good reduction, and $\phi \in G_K$ is an element whose restriction in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ is the Frobenius, then*

$$\dim_{\mathbb{F}_p} \mathcal{H}(L/K) = \dim_{\mathbb{F}_p} A[p]/(\phi - 1)A[p].$$

Proof. See [MR18, Lemma 7.2]. □

Lemma 2.7. *Suppose $p \neq \operatorname{char} \mathbb{F}_q$, L/K is unramified, and A/K has good reduction.*

(1) *If $\phi \in G_K$ is an element that restricts to Frobenius in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$, then evaluation of cocycles at ϕ gives an isomorphism*

$$H^1_{\mathrm{ur}}(K, A[p]) \simeq A[p]/(\phi - 1)A[p].$$

(2) *The twist A_L has good reduction over K, and*

$$\mathcal{H}(L/K) = H^1_{\mathrm{ur}}(K, A[p]).$$

Thus under these assumptions $\mathcal{H}(L/K)$ is independent of L.

Proof. See [MR18, Lemma 7.3]. □

Proposition 2.8. *Suppose $p \neq \operatorname{char} \mathbb{F}_q$, L/K is nontrivial and totally ramified, and A/K has good reduction. Recall that $L^{(1)}$ is the unique $(\mathbb{Z}/p\mathbb{Z})$-extension of K contained in L.*

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

(1) *The map*
$$A_L(K)/\mathfrak{p}_L A_L(K) \to A_L(L^{(1)})/\mathfrak{p}_L A_L(L^{(1)})$$
induced by the inclusion $A_L(K) \hookrightarrow A_L(L^{(1)})$ *is the zero map.*
(2) $\mathcal{H}(L/K) = \mathrm{Hom}(\mathrm{Gal}(L^{(1)}/K), A(K)[p])$.

Proof. The first assertion is essential for the proof of the second, which plays an important role in the proof of Theorem 4.10. One can refer to [MR18, Lemma 7.4] for the proof of (1). Assertion (2) was implied in the proof of [MR18, Proposition 7.8], but, because of its importance, we include its proof here.

Consider the following commutative diagram.
$$\begin{array}{ccccc} A_L(K)/\mathfrak{p}_L A_L(K) & \hookrightarrow & \mathrm{H}^1(K, A_L[\mathfrak{p}_L]) & \xrightarrow{\sim} & \mathrm{H}^1(K, A[p]) \\ \downarrow a & & \downarrow b & & \downarrow c \\ A_L(L^{(1)})/\mathfrak{p}_L A_L(L^{(1)}) & \hookrightarrow & \mathrm{H}^1(L^{(1)}, A_L[\mathfrak{p}_L]) & \xrightarrow{\sim} & \mathrm{H}^1(L^{(1)}, A[p]) \end{array}$$

We have $a = 0$ by the first assertion, thus
$$\mathcal{H}(L/K) \subset \ker c = \mathrm{Hom}(\mathrm{Gal}(L^{(1)}/K), A(K)[p]).$$
According to Lemma 2.6, we obtain
$$\dim_{\mathbb{F}_p} \mathcal{H}(L/K) = \dim_{\mathbb{F}_p} A(K)[p] = \dim_{\mathbb{F}_p} \mathrm{Hom}(\mathrm{Gal}(L^{(1)}/K), A(K)[p]),$$
so $\mathcal{H}(L/K) = \mathrm{Hom}(\mathrm{Gal}(L^{(1)}/K), A(K)[p])$. □

2.3 Relative Selmer groups

In this subsection we fix a $(\mathbb{Z}/p^k\mathbb{Z})$-extension L/K of global fields with $p \neq \mathrm{char}\, K$, and we allow the case $L = K$.

Definition 2.9. The *relative Selmer group* $\mathrm{Sel}(L/K, A[p])$ is the subgroup of $\mathrm{H}^1(K, A[p])$ defined by the exact sequence
$$0 \longrightarrow \mathrm{Sel}(L/K, A[p]) \longrightarrow \mathrm{H}^1(K, A[p]) \longrightarrow \prod_{v \in \mathcal{P}\ell_K} \frac{\mathrm{H}^1(K_v, A[p])}{\mathcal{H}(L_v/K_v)},$$
where (in our notation) L_v is the completion of L at some place of L above v. Note that $\mathrm{Sel}(K/K, A[p])$ is nothing more than $\mathrm{Sel}_p(A/K)$.

Lemma 2.10. *The isomorphism* $H^1(K, A[p]) \cong H^1(K, A_L[\mathfrak{p}_L])$ *identifies the standard* $\mathfrak{p}_L$*-Selmer group* $\mathrm{Sel}_{\mathfrak{p}_L}(A_L/K)$ *of* A_L *with* $\mathrm{Sel}(L/K, A[p])$*, that is, there exists an isomorphism* ϕ *making the following diagram commutative.*
$$\begin{array}{ccc} \mathrm{Sel}(L/K, A[p]) & \hookrightarrow & \mathrm{H}^1(K, A[p]) \\ \downarrow \phi & & \downarrow \simeq \\ \mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) & \hookrightarrow & \mathrm{H}^1(K, A_L[\mathfrak{p}_L]) \end{array}$$

Proof. This follows almost verbatim from the argument to prove [MR18, Lemma 8.4]. □

The important fact that enables us to bound the Mordell–Weil ranks in $(\mathbb{Z}/p^k\mathbb{Z})$-extensions is that there is an isogeny (see [MRS07, Theorem 4.5])
$$\bigoplus_{i=0}^{k} A_{L^{(i)}} \to \mathrm{Res}^L_K A$$

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

over K. Then, taking K-rational points, we get

$$\operatorname{rank}_{\mathbb{Z}}(A(L)) = \operatorname{rank}_{\mathbb{Z}}(A(K)) + \sum_{i=1}^{k} \operatorname{rank}_{\mathbb{Z}} A_{L^{(i)}}(K). \tag{2}$$

By Lemma 2.10 one can use the relative Selmer groups to bound the ranks of $A_{L^{(i)}}(K)$, which gives the following theorem.

THEOREM 2.11. *Suppose L/K is a nontrivial $(\mathbb{Z}/p^k\mathbb{Z})$-extension, and let $L^{(i)}$ denote the extension of K of degree p^i inside L. Then*

$$\operatorname{rank}_{\mathbb{Z}}(A(L)) \leq \operatorname{rank}_{\mathbb{Z}}(A(K)) + \sum_{i=1}^{k} \varphi(p^i) \dim_{\mathbb{F}_p}(\operatorname{Sel}(L^{(i)}/K, A[p])). \tag{3}$$

Proof. The proof is very close to that of [MR18, Proposition 8.8]. By Lemma 2.10, the Kummer map induces an inclusion

$$A_{L^{(i)}}(K) \otimes (\mathbb{Z}_{L^{(i)}}/\mathfrak{p}_{L^{(i)}}) \hookrightarrow \operatorname{Sel}(L^{(i)}/K, A[p]).$$

Note also that $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_{L^{(i)}}/\mathfrak{p}_{L^{(i)}}\mathbb{Z}_{L^{(i)}}$. Thus,

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}} A_{L^{(i)}}(K) &= \varphi(p^i) \operatorname{rank}_{\mathbb{Z}_{L^{(i)}}} A_{L^{(i)}}(K) \\ &\leq \varphi(p^i) \dim_{\mathbb{F}_p} A_{L^{(i)}}(K) \otimes (\mathbb{Z}_{L^{(i)}}/\mathfrak{p}_{L^{(i)}}) \\ &\leq \varphi(p^i) \dim_{\mathbb{F}_p}(\operatorname{Sel}(L^{(i)}/K, A[p])). \end{aligned}$$

The above inequality combined with (2) completes the proof. □

3. Growth of n-Selmer ranks in degree n cyclic extensions

In this section, let $n \geq 2$ be a fixed integer and A be an abelian variety over a global field K with $\operatorname{char} K = 0$ or $\operatorname{char} K \nmid n$. Based on Česnavičius's idea in [Čes17], we explain how to construct $(\mathbb{Z}/n\mathbb{Z})$-extensions L/K with large $r_n(\operatorname{Sel}_n(A/L))$. The following results hold in a more general setting, but the special case is enough for our applications. One can refer [Čes17, §§ 4 and 5] for more general statements.

THEOREM 3.1 [Čes17, Theorem 4.2]. *Let S be a finite subset of $\mathcal{P}\ell_K$ containing the places above $n\infty$ or where A has bad reduction, and $(\cdot)^*$ denote the Pontryagin dual of $(\cdot)$. Then there is an exact sequence*

$$\begin{aligned} 0 \to \operatorname{Sel}_n(A/K) \to H^1(\operatorname{Gal}(K^S/K), A[n]) \to \bigoplus_{v\in S} \frac{H^1(K_v, A[n])}{\mathcal{H}(K_v)} \to \operatorname{Sel}_n(A^\vee/K)^* \\ \to H^1(\operatorname{Gal}(K^S/K), A[n]) \to \bigoplus_{v\in S} H^2(K_v, A[n]), \end{aligned}$$

where K^S is the maximal extension of K unramified outside S.

Remark 3.2. The fppf cohomology was used in the original statement of [Čes17, Theorem 4.2]. Here we rephrase it in the language of Galois cohomology, due to the canonical isomorphism

$$\mathrm{H}^i_{\mathrm{fppf}}(U, \mathcal{A}[n]) \cong \mathrm{H}^i(\operatorname{Gal}(K^S/K), A[n])$$

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

(see [Čes15b, p. 1661, equation (1)]), where $U := X - S$, $\mathcal{A}$ is the Néron model of A and

$$X := \begin{cases} \operatorname{Spec} O_K, & \text{if } \operatorname{char} K = 0; \\ C_K, & \text{if } \operatorname{char} K > 0, \end{cases}$$

with C_K the proper smooth curve over a finite field whose function field is K.

We also note that if K is a global function field, the condition 'above $n\infty$' is an empty one.

From now on, we shall use the following notation.

Notation 3.3. The set Σ is a fixed finite subset of $\mathcal{P}\ell_K$ such that:

(1) $\{v \in \mathcal{P}\ell_K \mid A \text{ has bad reduction at } v \text{ or } v \mid n\infty\} \subset \Sigma$;
(2) the primes in Σ generate the class group of K.

For a $(\mathbb{Z}/n\mathbb{Z})$-extension L/K, define

$$S_L := \{v \in \mathcal{P}\ell_K \mid v \notin \Sigma \text{ is totally ramified in } L, \text{ and splits completely in } K(A[n])\}.$$

The following result is based on Česnavičius's idea presented in the proof of [Čes17, Theorem 5.2].

Theorem 3.4. *For any $(\mathbb{Z}/n\mathbb{Z})$-extension L/K, let $X_L := \operatorname{res}_{L/K}(H^1(K, A[n])) \cap \operatorname{Sel}_n(A/L)$. Then there exists a constant $c > 0$ independent of L such that*

$$r_n(X_L) \geq |S_L| - c.$$

Proof. Let Σ be as in Notation 3.3, $S := \Sigma \cup S_L$, and S' (respectively, Σ') be the set of places of L above S (respectively, Σ). According to [Čes16, Proposition 2.5(d)], for all $v \in S_L$, $\mathcal{H}(K_v) = \mathrm{H}^1_{\mathrm{ur}}(K_v, A[n])$. Thus by Theorem 3.1, we have a commutative diagram with exact rows as follows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Sel}_n(A/K) & \longrightarrow & \mathrm{H}^1(\mathrm{Gal}(K^S/K), A[n]) & \xrightarrow{d_L} & \left(\bigoplus_{v\in\Sigma} \frac{\mathrm{H}^1(K_v, A[n])}{\mathcal{H}(K_v)}\right) \oplus \left(\bigoplus_{v\in S_L} \frac{\mathrm{H}^1(K_v, A[n])}{\mathrm{H}^1_{\mathrm{ur}}(K_v, A[n])}\right) & \longrightarrow & \operatorname{Sel}_n(A^\vee/K)^* \\
 & & \downarrow{\scriptstyle a_L} & & \downarrow{\scriptstyle b_L} & & \downarrow{\scriptstyle c_L} & & \\
0 & \longrightarrow & \operatorname{Sel}_n(A/L) & \longrightarrow & \mathrm{H}^1(\mathrm{Gal}(L^{S'}/L), A[n]) & \longrightarrow & \left(\bigoplus_{v\in\Sigma'} \frac{\mathrm{H}^1(L_v, A[n])}{\mathcal{H}(L_v)}\right) \oplus \left(\bigoplus_{v\in S'_L} \frac{\mathrm{H}^1(L_v, A[n])}{H^1_{\mathrm{ur}}(L_v, A[n])}\right) & \longrightarrow & \operatorname{Sel}_n(A^\vee/L)^*
\end{array}$$

Then the snake lemma yields the exact sequence

$$\operatorname{Ker} b_L \to \operatorname{Ker}(c_L|_{\operatorname{Im} d_L}) \xrightarrow{h_L} \operatorname{Coker} a_L \xrightarrow{j_L} \operatorname{Coker} b_L. \tag{4}$$

Note that $\operatorname{Ker} b_L \subset \ker(\mathrm{H}^1(K, A[n]) \to \mathrm{H}^1(L, A[n])) = \mathrm{H}^1(\mathrm{Gal}(L/K), A[n](L))$, whose order is bounded by a constant independent of L. Along with (4), this implies

$$r_n(\operatorname{Im} h_L) \geq r_n(\operatorname{Ker}(c_L|_{\operatorname{Im} d_L})) - c_1 \tag{5}$$

for some constant c_1 independent of L.

Note that $\operatorname{Ker} c_L / \operatorname{Ker}(c_L|_{\operatorname{Im} d_L}) \hookrightarrow \operatorname{Coker} d_L \hookrightarrow \operatorname{Sel}_n(A^\vee/K)^*$, whose order is finite and independent of L. This implies that

$$r_n(\operatorname{Ker}(c_L|_{\operatorname{Im} d_L})) \geq r_n(\operatorname{Ker} c_L) - c_2 \tag{6}$$

for some constant c_2 independent of L.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

Let $\pi_L : \mathrm{Sel}_n(A/L) \longrightarrow \mathrm{Coker}\, a_L$ be the projection. Then one can easily check that

$$\mathrm{Ker}\,(j_L \circ \pi_L) \subset X_L. \tag{7}$$

Note that $\pi_L : \mathrm{Ker}\,(j_L \circ \pi_L) \twoheadrightarrow \mathrm{Ker}\, j_L$ is surjective, so we have

$$r_n(\mathrm{Ker}\,(j_L \circ \pi_L)) \geq r_n(\mathrm{Ker}\, j_L) = r_n(\mathrm{Im}\, h_L). \tag{8}$$

Applying (5)–(8), we then have

$$r_n(X_L) \geq r_n(\mathrm{Ker}\,(j_L \circ \pi_L)) \geq r_n(\mathrm{Im}\, h_L) \geq r_n(\mathrm{Ker}\, c_L) - c$$

for some constant c independent of L. It remains to show the following claim.

Claim. $r_n(\mathrm{Ker}\, c_L) \geq |S_L|$.

Note that for $v \in S_L$, $A[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$ over K_v. So $\mathrm{H}^1(K_v, \mathbb{Z}/n\mathbb{Z})$ is a direct factor of $\mathrm{H}^1(K_v, A[n])$, and

$$\mathrm{H}^1(K_v, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(G_{K_v}, \mathbb{Z}/n\mathbb{Z}) \supset \mathrm{H}^1_{\mathrm{ur}}(K_v, \mathbb{Z}/n\mathbb{Z}).$$

Since L_v/K_v is a totally ramified $(\mathbb{Z}/n\mathbb{Z})$-extension, $I_{K_v}/I_{L_v} \cong \mathbb{Z}/n\mathbb{Z}$. Choose a continuous homomorphism $f : G_{K_v}/I_{L_v} \to \mathbb{Z}/n\mathbb{Z}$ whose restriction on I_{K_v}/I_{L_v} is an isomorphism to $\mathbb{Z}/n\mathbb{Z}$. Let $\bar{f}$ be its image in $\mathrm{H}^1(K_v, \mathbb{Z}/n\mathbb{Z})/\mathrm{H}^1_{\mathrm{ur}}(K_v, \mathbb{Z}/n\mathbb{Z})$. Then

$$0 \neq \bar{f} \in \mathrm{H}^1(K_v, \mathbb{Z}/n\mathbb{Z})/\mathrm{H}^1_{\mathrm{ur}}(K_v, \mathbb{Z}/n\mathbb{Z}),\ 0 = \bar{f}|_{G_{L_v}} \in \mathrm{H}^1(L_v, \mathbb{Z}/n\mathbb{Z})/\mathrm{H}^1_{\mathrm{ur}}(L_v, \mathbb{Z}/n\mathbb{Z}).$$

Thus $0 \neq \bar{f} \in \mathrm{Ker}\, c_L$. We check that the order of $\bar{f}$ is exactly n. Let $g \in I_{K_v}/I_{L_v}$ be the preimage of $1 \in \mathbb{Z}/n\mathbb{Z}$. Then, for $1 \leq m < n$, $(mf)(g) = m \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$, hence $m\bar{f} \neq 0$.

Such a construction is valid for every $v \in S_L$, so we obtain a set of $|S_L|$ nonzero elements of order n in $\mathrm{Ker}\, c_L$, each lying in different direct summand hence $(\mathbb{Z}/n\mathbb{Z})$-linearly independent. Thus we have $r_n(\mathrm{Ker}\, c_L) \geq |S_L|$. This completes the proof. □

4. Bounding the Mordell–Weil ranks in $(\mathbb{Z}/p^k\mathbb{Z})$-extensions

In this section we always assume K is a global field with $p \neq \mathrm{char}\, K$.

If L/K is a $(\mathbb{Z}/p^k\mathbb{Z})$-extension with large $|S_L|$, then Theorem 3.4 implies that $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/L)$ is also large. However, it could be possible that $\mathrm{rank}_{\mathbb{Z}}(A(L))$ is very large, which leads to small $Ш(A/L)[p]$. By Theorem 2.11, we can bound $\mathrm{rank}_{\mathbb{Z}}(A(L))$ by the relative Selmer groups $\mathrm{Sel}(L^{(i)}/K, A[p])$. So the $(\mathbb{Z}/p^k\mathbb{Z})$-extensions we need are those L/K with

$$\text{large } |S_L| \text{ and also small } \mathrm{Sel}(L^{(i)}/K, A[p]).$$

We give a method for finding such extensions in this section, which enables us to prove our main result.

4.1 $(\mathbb{Z}/p^k\mathbb{Z})$-extensions of global fields with given completions at local places

In [MR18], Mazur and Rubin defined the so-called T-ramified, Σ-split extensions and showed the existence of such extensions. Under mild hypotheses, they proved that, if T is chosen properly, then any T-ramified, Σ-split extension L/K satisfies

$$\mathrm{Sel}(L/K, A[\lambda]) = 0 \quad (\text{thus } \mathrm{rank}_{\mathbb{Z}} A(K) = \mathrm{rank}_{\mathbb{Z}} A(L)),$$

in which $A[\lambda]$ is a subgroup scheme of $A[p]$ defined in [MR18, Definition 6.2].

However, these mild hypotheses may not hold in general. As one will see in the proof of Theorem 4.10, in order to seek L/K with small $\dim_{\mathbb{F}_p} \mathrm{Sel}(L/K, A[p])$ and large $|S_L|$, only requiring L/K to be T-ramified, Σ-split seems insufficient, and we need to require more: that L should

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

have given completions at all $v \in T \setminus \{v_1, v_n\}$, in which $T = \{v_1, v_2, \dots, v_n\}$ with v_1, v_n two special elements in T. This leads to the following discussion in this subsection, and our main result is Lemma 4.6.

Definition 4.1. Let Σ' be the set of all places of $K' := K(\mu_{p^k})$ above those in Σ. Suppose Σ and Σ' satisfy the respective conditions in Notation 3.3. Denote

$$\mathcal{P} := \left\{ v \in \mathcal{P}\ell_K \mid v \notin \Sigma, v \text{ splits completely in } K'(\sqrt[p^k]{O^\times_{K',\Sigma'}}) \right\}. \tag{9}$$

Suppose T is a non-empty finite subset of $\mathcal{P}$. A $(\mathbb{Z}/p^k\mathbb{Z})$-extension L/K is called T-ramified and Σ-split if:

(1) L/K is totally ramified at $v \in T$ and unramified outside T;
(2) L/K splits completely at $v \in \Sigma$.

For $v \in \mathcal{P}$, let

$$Y_v := K^\times (O_v^\times)^{p^k} \prod_{w \in \Sigma} K_w^\times \prod_{w \notin \Sigma \cup \{v\}} O_w^\times. \tag{10}$$

Then we have a surjective map $O_v^\times \twoheadrightarrow \mathbf{A}_K^\times / Y_v$, which induces isomorphisms

$$\mathbb{Z}/p^k\mathbb{Z} \cong O_v^\times/(O_v^\times)^{p^k} \cong \mathbf{A}_K^\times / Y_v$$

by the definition of $\mathcal{P}$. Let

$$K(v) := \text{ the abelian extension of } K \text{ corresponding to } Y_v. \tag{11}$$

Then by class field theory we see that $K(v)/K$ is a $\{v\}$-ramified, Σ-split $(\mathbb{Z}/p^k\mathbb{Z})$-extension.

Theorem 4.2. *Suppose $T = \{v_1, \dots, v_n\} \subset \mathcal{P}$. If L/K is a $(\mathbb{Z}/p^k\mathbb{Z})$-extension which is T-ramified and Σ-split, then $L \subset K(v_1) \cdots K(v_n)$. In particular, for every $v \in \mathcal{P}$, $K(v)$ is the only $(\mathbb{Z}/p^k\mathbb{Z})$-extension which is $\{v\}$-ramified and Σ-split.*

Proof. Let Y_L be the norm group of $\mathbf{A}_K^\times$ corresponding to L. By class field theory, since L/K is unramified outside T,

$$(\cdots, 1, O_v^\times, 1, \cdots) \subset Y_L \quad \text{for all } v \notin T;$$

since $L_v = K_v$ for $v \in \Sigma$,

$$(\cdots, 1, K_v^\times, 1, \cdots) \subset Y_L \quad \text{for all } v \in \Sigma;$$

since L/K is a $(\mathbb{Z}/p^k\mathbb{Z})$-extension,

$$\prod_{i=1}^n (O_{v_i}^\times)^{p^k} \subset Y_L.$$

Combining these facts yields

$$Y = K^\times \prod_{i=1}^n (O_{v_i}^\times)^{p^k} \prod_{v \in \Sigma} K_v^\times \prod_{v \notin \Sigma \bigcup T} O_v^\times \subset Y_L.$$

Note that Y is exactly the norm group corresponding to $K(v_1) \cdots K(v_n)$. Thus

$$L \subset K(v_1) \cdots K(v_n).$$

□

If $\mu_{p^k} \subset K$, then by Kummer theory, every $(\mathbb{Z}/p^k\mathbb{Z})$-extension L/K can be written as $L = K\left(\sqrt[p^k]{a}\right)$ for some $a \in K^\times$. We have the following lemma.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

LEMMA 4.3. *Suppose $\mu_{p^k} \subset K$ and $v \in \mathcal{P}$. Let $\Sigma_0 \not\ni v$ be any finite subset of $\mathcal{P}\ell_K$ which generates the class group of K. Then there exists $a \in O^\times_{K,\Sigma_0\cup\{v\}}$ such that $K(v) = K(\sqrt[p^k]{a})$.*

Proof. Suppose $K(v) = K\big(\sqrt[p^k]{b}\big)$ for some $b \in K^\times$. Then, for every place $w \neq v$, we have $p^k \mid \mathrm{ord}_w(b)$ since $K(v)/K$ is unramified outside $\{v\}$, and $\mathrm{ord}_w(b) = 0$ for almost all places. Denote

$$\{w_1, \dots, w_n\} := \{w \neq v, w \notin \Sigma_0 \mid \mathrm{ord}_w(b) \neq 0\}.$$

For each w_i, the sequence

$$O^\times_{K,\Sigma_0\cup\{w_i\}} \xrightarrow{\mathrm{ord}_{w_i}} \mathbb{Z} \to 0$$

is exact since Σ_0 generates the class group of K. Let $\beta_i \in O^\times_{K,\Sigma_0\cup\{w_i\}}$ such that $\mathrm{ord}_{w_i}(b) = 1$. Write $\mathrm{ord}_{w_i}(b) = p^k k_i$. Then

$$a := \frac{b}{\beta_1^{p^k k_1} \cdots \beta_n^{p^k k_n}} \in O^\times_{K,\Sigma_0\cup\{v\}} \quad \text{and} \quad K(v) = K\big(\sqrt[p^k]{a}\big). \qquad \square$$

Recall that $(\cdot,\cdot)_v$ is the Hilbert symbol, and $(\frac{\cdot}{\cdot})_{p^k}$ is the p^kth power residue symbol, whose definitions and properties can be found in [Neu13, Chapter V, § 3].

LEMMA 4.4. *Suppose $\mu_{p^k} \subset K$ and $p^k \neq 2$. Let $\{v_1, v_2\} \subset \mathcal{P}$ such that $K(v_i) = K(\sqrt[p^k]{a_i})$ with p, a_1 and a_2 relatively prime. Then:*

(1) $(\frac{a_1}{a_2})_{p^k} = (\frac{a_2}{a_1})_{p^k}$;
(2) $(\frac{a_1}{v_2})_{p^k} = 1 \Leftrightarrow (\frac{a_2}{v_1})_{p^k} = 1$.

Consequently, v_1 splits completely in $K(v_2)$ if and only if v_2 splits completely in $K(v_1)$.

Proof. (1) According to the reciprocity law of the p^kth power residue (see [Neu13, Chapter VI, Theorem 8.3]), we have

$$\left(\frac{a_1}{a_2}\right)_{p^k}\left(\frac{a_2}{a_1}\right)^{-1}_{p^k} = \prod_{v\mid p\infty} (a_1, a_2)_v.$$

If $v \mid \infty$, then v must be a complex place by our assumption, so $(a_1, a_2)_v = 1$; if $v \mid p$, then $a_1 \in O_v^\times$ and $K(\sqrt[p^k]{a_2})/K$ is unramified at v, so $a_1 \in \mathbf{Nm}\ K_v(\sqrt[p^k]{a_2})$, which implies that $(a_1, a_2)_v = 1$. Thus,

$$\left(\frac{a_1}{a_2}\right)_{p^k}\left(\frac{a_2}{a_1}\right)^{-1}_{p^k} = 1.$$

(2) As $K(v_i)$ is totally ramified at v_i and unramified outside v_i, $(a_i) = v_i^{k_i} I_i^{p^k}$ with $p \nmid k_i \in \mathbb{Z}$ and I_i a fractional ideal relatively prime to $(p)v_i$. If $(\frac{a_1}{v_2})_{p^k} = 1$, then $(\frac{a_1}{a_2})_{p^k} = 1$ and by (1) we get $1 = (\frac{a_2}{a_1})_{p^k} = (\frac{a_2}{v_1})^{k_1}_{p^k}$. Thus we have $(\frac{a_2}{v_1})_{p^k} = 1$ since $p \nmid k_1$. The converse is similar. $\square$

LEMMA 4.5. *Suppose $\mu_{p^k} \subset K$ and $T = \{v_1, \dots, v_n\} \subset \mathcal{P}$. Then any T-ramified and Σ-split $(\mathbb{Z}/p^k\mathbb{Z})$-extension of K has the form*

$$L = K\big(\sqrt[p^k]{a_1^{x_1} \cdots a_n^{x_n}}\big)$$

where $x_i \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ and $a_i \in K^\times$ such that $K(v_i) = K(\sqrt[p^k]{a_i})$.

Proof. This is clear from Theorem 4.2. $\square$

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

Lemma 4.6. *Suppose $n \geq 2$, $T = \{v_1, \dots, v_n\} \subset \mathcal{P}$ and $p^k \neq 2$. Let $v_{n+1} \in \mathcal{P} \setminus T$ be a place splitting completely in $K(v_2) \cdots K(v_n)$ and $T_1 = T \cup \{v_{n+1}\}$. If L/K is a T-ramified and Σ-split $(\mathbb{Z}/p^k\mathbb{Z})$-extension, then there exists a $(\mathbb{Z}/p^k\mathbb{Z})$-extension L_1/K such that:*

(1) *L_1/K is T_1-ramified and Σ-split;*
(2) *$(L_1)_{v_i} = L_{v_i}$ for $2 \leq i \leq n$.*

Proof. For convenience, we denote $K_i := K(v_i)$ for $1 \leq i \leq n+1$. Let $K' := K(\mu_{p^k})$, $L' := LK'$ and $d := [K' : K]$. Let Σ' be the set of primes of K' above Σ. By definition of $\mathcal{P}$, the place v_i splits completely in K'. Let v_i^j $(1 \leq j \leq d)$ be the primes of K' above v_i. The sets of primes in K' above T, v_{n+1} and T_1 are

$$T' = \{v_i^j \mid 1 \leq i \leq n, 1 \leq j \leq d\}, \quad \Pi = \{v_{n+1}^j \mid 1 \leq j \leq d\} \quad \text{and} \quad T_1' = T' \cup \Pi,$$

respectively. Then L'/K' is T'-ramified and Σ'-split.

Choosing finite pairwise disjoint sets of primes $\Sigma_{v'}$ $(v' \in T_1')$ of K' which generate the class group of K' and contain no prime above p, and then applying Lemma 4.3, we obtain $a_{v'} \in O_{K',\Sigma_{v'}}$ such that

- $K'(v') = K'(\sqrt[p^k]{a_{v'}})$, p and all $a_{v'}$ are pairwise coprime.

Let $a_{(i-1)d+j} = a_{v_i^j}$ for $1 \leq i \leq n+1$ and $1 \leq j \leq d$.

By Lemma 4.5, $L' = K'\left(\sqrt[p^k]{a_1^{x_1} \cdots a_{nd}^{x_{nd}}}\right)$ with $x_i \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ for each i. Note that $K'K_{n+1}/K'$ is Π-ramified and Σ'-split. Then $K_{n+1}K' = K'\left(\sqrt[p^k]{a_{nd+1}^{x_{nd+1}} \cdots a_{(n+1)d}^{x_{(n+1)d}}}\right)$. Let

$$L_1' := K'\left(\sqrt[p^k]{a_1^{x_1} \cdots a_{nd}^{x_{nd}} a_{nd+1}^{x_{nd+1}} \cdots a_{(n+1)d}^{x_{(n+1)d}}}\right).$$

Then $L_1' \subset K_1 \cdots K_n K_{n+1} K'$ is T_1'-ramified and Σ'-split. Since v_{n+1} splits completely in K_i for $i \geq 2$, we have

$$\left(\frac{a_{(i-1)d+j}}{v_{n+1}^{j'}}\right)_{p^k} = 1 \implies \left(\frac{a_{nd+j'}}{v_i^j}\right)_{p^k} = 1$$

by Lemma 4.4. This implies

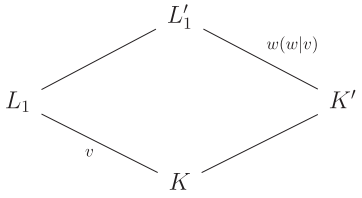
$$(L_1')_{v_i^j} = L_{v_i^j}' = L_{v_i}, \quad 2 \leq i \leq n, \ 1 \leq j \leq d. \tag{12}$$

For any nonempty subset $I \subset [n+1] = \{1, \dots, n+1\}$, let $K_I = \prod_{i \in I} K_i$. By considering the ramification of primes we see that $K_I \cap K_J = K$ if $I \cap J = \emptyset$ and $K_I \cap K' = K$. Now by induction we have the canonical isomorphisms

$$\mathrm{Gal}(K_I/K) \cong \prod_{i \in I} \mathrm{Gal}(K_i/K), \quad \mathrm{Gal}(K_I K'/K') \cong \mathrm{Gal}(K_I/K),$$
$$\mathrm{Gal}(K_I K'/K) \cong \mathrm{Gal}(K_I/K) \times \mathrm{Gal}(K'/K).$$

Let $H = \mathrm{Gal}(K_{[n+1]}K'/L_1')$ and $L_1 = K_{[n+1]}^H$. Then one can check that $L_1' = L_1K'$ and L_1/K is a T_1-ramified and Σ-split $(\mathbb{Z}/p^k\mathbb{Z})$-extension.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press



$$w \text{ is totally ramified (respectively, unramified, splits completely)} \Rightarrow$$
$$v \text{ is totally ramified (respectively, unramified, splits completely)}$$

Moreover, (12) implies that for $2 \le i \le n$, we have

$$L_{v_i} = (L_1')_{v_i} = (L_1)_{v_i}(K')_{v_i} = (L_1)_{v_i}.$$

This completes the proof. □

Remark 4.7. It is natural to ask whether, for each $v_i \in T$, given a totally ramified $(\mathbb{Z}/p^k\mathbb{Z})$-extension $\mathcal{L}_i/K_{v_i}$, there exists a global $(\mathbb{Z}/p^k\mathbb{Z})$-extension L/K which is T-ramified, Σ-split and $L_{v_i} = \mathcal{L}_i$ for $v_i \in T$. The famous Grunwald–Wang theorem [NSW08, Theorem 9.2.8] asserts that there does exist an extension L/K such that $L_{v_i} = \mathcal{L}_i$ for $1 \le i \le n$; however, it may be ramified at some $v \notin T$. And one can prove that an extension which is T-ramified, Σ-split and $L_{v_i} = \mathcal{L}_i$ may not exist in general.

4.2 Bounding the Mordell–Weil ranks in $(\mathbb{Z}/p^k\mathbb{Z})$-extensions

Now fix an abelian variety A over K. We denote

$$F := K(A[p], (O_{K,\Sigma}^{\times})^{1/p^k}),$$
$$T_F := \{v \in \mathcal{P}\ell_K \mid v \notin \Sigma, v \text{ splits completely in } F/K\},$$
$$S_L := \{v \in \mathcal{P}\ell_K \mid v \notin \Sigma, v \text{ splits completely in } K(A[p]) \text{ and is totally ramified in } L\}.$$

Obviously we have $T_F \subset \mathcal{P}$ and the density theorem ensures that T_F has positive density.

Definition 4.8. Suppose that $T = \{v_1, \dots, v_n\} \subset \mathcal{P}$ and, for each v_i, $\mathcal{L}_i/K_{v_i}$ is a totally ramified $(\mathbb{Z}/p^k\mathbb{Z})$-extension. Let $W_i := \mathcal{H}(\mathcal{L}_i/K_{v_i})$ and $\mathcal{W}_n := \prod_{1\le i\le n} W_i$. The *artificial Selmer group* $\mathrm{Sel}(W_1 \times \cdots \times W_n, A[p]) = \mathrm{Sel}(\mathcal{W}_n, A[p])$ is defined by the exact sequence

$$0 \longrightarrow \mathrm{Sel}(\mathcal{W}_n, A[p]) \longrightarrow \mathrm{H}^1(K, A[p]) \longrightarrow \prod_{i=1}^{n} \frac{\mathrm{H}^1(K_{v_i}, A[p])}{W_i} \prod_{v\notin T} \frac{\mathrm{H}^1(K_v, A[p])}{\mathcal{H}(K_v)}.$$

For $v_i \in T$, the strict Selmer group $\mathrm{Sel}(\mathcal{W}_n, A[p])_{v_i}$ at v_i is the group

$$\mathrm{Sel}(\mathcal{W}_n, A[p])_{v_i} := \ker(\mathrm{Sel}(\mathcal{W}_n, A[p]) \longrightarrow \mathrm{H}^1(K_{v_i}, A[p])).$$

One can deduce the finiteness of $\mathrm{Sel}(\mathcal{W}_n, A[p])$ from the finiteness of $\mathrm{Sel}(K, A[p])$.

Lemma 4.9. *Let T be a finite subset of $\mathcal{P}$, and L/K be a $(\mathbb{Z}/p^k\mathbb{Z})$-extension which is T-ramified and Σ-split. If $K \subsetneq L' \subset L$, then*

$$\mathrm{Sel}(L'/K, A[p]) = \mathrm{Sel}(L/K, A[p]).$$

Proof. See [MR18, Lemma 9.16]. □

Theorem 4.10. *Suppose K is a global field, $p \neq \mathrm{char}\, K$. Let A be an abelian variety of dimension g over K and $r_0 = \dim_{\mathbb{F}_p} \mathrm{Sel}_p(A/K)$. Then there exists a sequence of $(\mathbb{Z}/p^k\mathbb{Z})$-extensions $\{L_i\}_{i=1}^{\infty}$*

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

such that:

(1) $|S_{L_i}| \geq i$;

(2) $\operatorname{rank}_{\mathbb{Z}}(A(L_i)) \leq \begin{cases} \operatorname{rank}_{\mathbb{Z}}(A(K)) + 3(r_0+4g), & \text{if } p^k = 2, \\ \operatorname{rank}_{\mathbb{Z}}(A(K)) + (p^k-1)(r_0+4g), & \text{if otherwise.} \end{cases}$

Proof. We shall construct by induction a set of primes $\{v_i\}_{i=1}^{\infty} \subset T_F$ and a sequence of $(\mathbb{Z}/p^k\mathbb{Z})$-extensions $\{L_i\}_{i=1}^{\infty}$ of K such that the following assertions hold.

(i) L_i is T_i-ramified and Σ-split, where $T_i := \{v_1, \dots, v_i\}$; in particular, $S_{L_i} \supseteq T_i$ and $|S_{L_i}| \geq i$.
(ii) If $i > 2$, then v_i splits completely in $K_2 \cdots K_{i-1}$ and is inert in K_1, where $K_i := K(v_i)$;
(iii) v_2 is inert in K_1.
(iv) The inequalities

$$r_i \leq r_0 + s_i \leq r_0 + 2g \tag{13}$$

are always satisfied, where

$$\begin{aligned} W_i &:= \mathcal{H}((L_i)_{v_i}/K_{v_i}), \quad \mathcal{W}_i := W_1 \times \cdots \times W_i, \\ r_i &:= \dim_{\mathbb{F}_p} \operatorname{Sel}(\mathcal{W}_i, A[p]), \\ t_{i+1} &:= \dim_{\mathbb{F}_p} \operatorname{Im}\left(\operatorname{Sel}(\mathcal{W}_i, A[p]) \to H^1_{\mathrm{ur}}(K_{v_{i+1}}, A[p])\right), \\ s_i &:= \dim_{\mathbb{F}_p} \operatorname{Im}\left(\operatorname{Sel}(\mathcal{W}_i, A[p]) \to \mathcal{H}(L_{v_i}/K_{v_i})\right). \end{aligned}$$

Note that $s_i, t_i \leq 2g$, so only the first inequality in (13) needs to be addressed.

For the base step, choose an arbitrary $v_1 \in T_F$ and let $L_1 := K(v_1) = K_1$. One can deduce from the exact sequence (18) below that

$$r_1 = r_0 - t_1 + s_1 \leq r_0 + s_1.$$

Assume that we have already constructed $\{v_i\}_{i=1}^n$ and $\{L_i\}_{i=1}^n$, $n \geq 1$.

If $s_n = 0$, we choose an arbitrary $v_{n+1} \in T_F$ which splits completely in $K_2 \cdots K_n$ and is inert in K_1.

If $s_n \geq 1$, let $L_{1,n}$ be the unique $(\mathbb{Z}/p\mathbb{Z})$-extension of K_{v_n} contained in $(L_n)_{v_n}$. Then, by Proposition 2.8,

$$\mathcal{H}((L_n)_{v_n}/K_{v_n}) = \operatorname{Hom}(\operatorname{Gal}(L_{1,n}/K_{v_n}), A(K_{v_n})[p]).$$

Let $\bar{\sigma}$ be a generator of $\operatorname{Gal}(L_{1,n}/K_{v_n})$. So we can pick linearly independent $c_{n,1}, \dots, c_{n,s_n} \in \operatorname{Sel}(\mathcal{W}_n, A[p])$ such that

$$c_{n,1}(\bar{\sigma}), \dots, c_{n,s_n}(\bar{\sigma}) \subset A[p] \text{ are linear independent over } \mathbb{F}_p. \tag{14}$$

Note that by the induction assumption, we have:

- $(K_1)_{v_n}/K_{v_n}$ is nontrivial and unramified;
- $(K_n)_{v_n}/K_{v_n}$ is totally ramified;
- $(K_2 \cdots K_{n-1})_{v_n} = K_{v_n}$.

Thus, there exists a pre-image $\sigma \in G_{K_{v_n}} = G_{F_{v_n}} \subset G_F$ of $\bar{\sigma}$ such that

$$\sigma|_{K_1} \neq 1, \quad \sigma|_{K_2 \cdots K_n} = 1 \text{ (if } n \geq 2).$$

One should note that if $n = 1$, then we only require $\sigma|_{K_1} \neq 1$. Denote $d_{n,j} := c_{n,j}|_F$ for $1 \leq j \leq s_n$. Choose a Galois extension N/K such that

$$G_N \subset \bigcap_{i=1}^{s_n} \ker(d_{n,i}) \quad \text{and} \quad FK_1 \cdots K_n \subset N.$$

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

By the Chebotarev density theorem, there exists $v_{n+1} \notin T_n \cup \Sigma$ such that

v_{n+1} is unramified in N/K and $\mathrm{Frob}_{v_{n+1}}|_N = \sigma|_N$.

In particular, $\mathrm{Frob}_{v_{n+1}}|_F = \sigma|_F = 1$ and thus $v_{n+1} \in T_F$. By our choice,

$$c_{n,i}(\mathrm{Frob}_{v_{n+1}}) = d_{n,i}(\mathrm{Frob}_{v_{n+1}}) = d_{n,i}(\sigma) = d_{n,i}(\bar{\sigma}) = c_{n,i}(\bar{\sigma}), \quad 1 \le i \le s_n.$$

Thus, by (14) we conclude that

$$c_{n,1}(\mathrm{Frob}_{v_{n+1}}), \dots, c_{n,s_n}(\mathrm{Frob}_{v_{n+1}}) \subset A[p] \text{ are linearly independent over } \mathbb{F}_p. \tag{15}$$

According to our choice, v_{n+1} splits completely in $K_2 \cdots K_n$ and is inert in K_1, so by Lemma 4.6, there exists a $(\mathbb{Z}/p^k\mathbb{Z})$-extension L_{n+1}/K which is T_{n+1}-ramified, Σ-split and

$$(L_{n+1})_{v_i} = (L_n)_{v_i}, \quad 2 \le i \le n. \tag{16}$$

Since the restrict map

$$\mathbf{loc}_{v_{n+1}} : \mathrm{Sel}(\mathcal{W}_n, A[p]) \to H^1_{\mathrm{ur}}(K_{v_{n+1}}, A[p])$$

can be regarded as the evaluation of cocycles at $\mathrm{Frob}_{v_{n+1}}$, (15) implies that

$$t_{n+1} = \dim_{\mathbb{F}_p} \mathrm{Im}\,(\mathbf{loc}_{v_{n+1}}) \ge s_n. \tag{17}$$

Observe the following diagram with exact rows.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}(\mathcal{W}_{n+1}, A[p])_{v_{n+1}} & \longrightarrow & \mathrm{Sel}(\mathcal{W}_{n+1}, A[p]) & \xrightarrow{\mathbf{loc}'_{v_{n+1}}} & \mathcal{H}(L_{v_{n+1}}/K_{v_{n+1}}) \\ & & \| & & & & \\ 0 & \longrightarrow & \mathrm{Sel}(\mathcal{W}_n, A[p])_{v_{n+1}} & \longrightarrow & \mathrm{Sel}(\mathcal{W}_n, A[p]) & \xrightarrow{\mathbf{loc}_{v_{n+1}}} & H^1_{\mathrm{ur}}(K_{v_{n+1}}, A[p]) \end{array} \tag{18}$$

Recall that $s_{n+1} = \dim_{\mathbb{F}_p} \mathrm{Im}\,\mathbf{loc}'_{v_{n+1}}, t_{n+1} = \dim_{\mathbb{F}_p} \mathrm{Im}\,\mathbf{loc}_{v_{n+1}}$, thus

$$r_{n+1} - s_{n+1} = \dim_{\mathbb{F}_p} \mathrm{Sel}(\mathcal{W}_{n+1}, A[p])_{v_{n+1}} = \dim_{\mathbb{F}_p} \mathrm{Sel}(\mathcal{W}_n, A[p])_{v_{n+1}} = r_n - t_{n+1},$$

which implies that

$$r_{n+1} = r_n - t_{n+1} + s_{n+1}.$$

Using the induction assumption and (17), we obtain

$$r_{n+1} = r_n - t_{n+1} + s_{n+1} \le r_0 + s_n - t_{n+1} + s_{n+1} \le r_0 + s_{n+1}.$$

This completes our construction. We claim that for all $m \ge 1$,

$$\mathrm{rank}_{\mathbb{Z}}(A(L_m)) \le \mathrm{rank}_{\mathbb{Z}}(A(K)) + (p^k - 1)(r_0 + 4g).$$

By (16), we have

$$W_i = \mathcal{H}((L_i)_{v_i}/K_{v_i}) = \mathcal{H}((L_m)_{v_i}/K_{v_i}), \quad 2 \le i \le m. \tag{19}$$

Consider the following diagram with exact rows.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}(\mathcal{W}_m, A[p])_{v_1} & \longrightarrow & \mathrm{Sel}(\mathcal{W}_m, A[p]) & \longrightarrow & W_1 \\ & & \| & & & & \\ 0 & \longrightarrow & \mathrm{Sel}(L_m/K, A[p])_{v_1} & \longrightarrow & \mathrm{Sel}(L_m/K, A[p]) & \longrightarrow & \mathcal{H}(L_{m,v_1}/K_{v_1}) \end{array} \tag{20}$$

in which (19) gives the vertical equality. Thus, we have

$$\dim_{\mathbb{F}_p} \mathrm{Sel}(L_m/K, A[p]) \le \dim_{\mathbb{F}_p} \mathrm{Sel}(\mathcal{W}_m, A[p])_{v_1} + 2g \le r_0 + 4g.$$

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

Recall that by Lemma 4.9,

$$\mathrm{Sel}(L_m^{(i)}/K, A[p]) = \mathrm{Sel}(L_m/K, A[p]).$$

It follows from Theorem 2.11 that

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}}(A(L_m)) &\le \mathrm{rank}_{\mathbb{Z}}(A(K)) + \sum_{i=1}^{k} \varphi(p^i) \dim_{\mathbb{F}_p} \mathrm{Sel}(L_m^{(i)}/K, A[p]) \\ &\le \mathrm{rank}_{\mathbb{Z}}(A(K)) + (p^k - 1)(r_0 + 4g).\end{aligned}$$

The proof of theorem is completed except the case $p^k = 2$.

As for the case $p^k = 2$, by previous discussion we can find $(\mathbb{Z}/2^2\mathbb{Z})$-extensions $\{L_i/K\}_{i=1}^{\infty}$ such that:

(i) $|S_{L_i}| \ge i$;
(ii) $\mathrm{rank}_{\mathbb{Z}} A(L_i) \le \mathrm{rank}_{\mathbb{Z}}(A(K)) + 3(r_0 + 4g)$.

Furthermore, by our construction, for all $v \in S_{L_i}$, v is totally ramified in L_i/K, thus v is totally ramified in $L_i^{(1)}/K$. Then $\{L_i^{(1)}/K\}_{i=1}^{\infty}$ is the sequence of quadratic extensions we require. □

Theorem 4.11. *Let $n \ge 2$ be an integer. If K is a global field such that* $\mathrm{char}\, K = 0$ *or* $\mathrm{char}\, K \nmid n$, *then*

$$r_n(Ш(A/L))$$

can be arbitrarily large as L ranges over $(\mathbb{Z}/n\mathbb{Z})$-extensions of K.

Proof. We first treat the case $n = p^k$. In this case, the result follows from Theorem 4.10, Theorem 3.4 and the exact sequence (1).

Next suppose $n = \prod_{i=1}^{t} p_i^{k_i}$ is the prime decomposition of n. By the first step we can find a $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$-extension L_i/K for each i such that

$$r_{p_i^{k_i}}(Ш(A/L_i)) \ge m.$$

Let $L = L_1 \cdots L_t$. Note that the p_i-primary part of

$$\mathrm{Ker}\,(\mathrm{H}^1(L_i, A) \to \mathrm{H}^1(L, A)) = \mathrm{H}^1(\mathrm{Gal}(L/L_i), A(L))$$

is zero, then the restriction homomorphism

$$Ш(A/L_i)[p_i^{k_i}] \to Ш(A/L)$$

is injective. This implies

$$r_{p_i^{k_i}}(Ш(A/L)) \ge r_{p_i^{k_i}}(Ш(A/L_i)[p_i^{k_i}]) \ge m, \quad 1 \le i \le t.$$

Then L/K is a $(\mathbb{Z}/n\mathbb{Z})$-extension we require. □

5. Growth of potential Ш

In this section we fix an abelian variety A defined over a global field K. We study the growth of n-rank of the potential Ш of A over K, whose definition we now recall.

Definition 5.1. Let L/K be a finite extension of global fields. The potential Ш of A/K in L is

$$Ш_K(A/L) := \mathrm{res}_{L/K}(\mathrm{H}^1(K, A)) \cap Ш(A/L).$$

Clark and Sharif proved the following result.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

Theorem 5.2 [CS10, Theorem 3]. *Let E/K be an elliptic curve and n be an positive integer such that* $\operatorname{char} K = 0$ *or* $\operatorname{char} K \nmid n$. *Then, for any positive integer r, there exists a field extension L/K of degree n such that*

$$r_n(Ш_K(A/L)) \geq r.$$

Creutz later considered the case of abelian varieties. He proved the following result.

Theorem 5.3 [Cre11, Theorem 1]. *Let A be a strongly principally polarized abelian variety over a number field K such that the G_K-action on the Néron–Severi group is trivial. Then, for any prime p and any integer N, there exists a degree p extension L/K for which*

$$r_p(Ш_K(A/L)) > N.$$

The method used to prove the above theorems is closely related to the study of the period and index problem in the Weil–Châtelet group. Here we apply a different method, which can treat high-dimensional abelian varieties, to generalize the above two results.

Theorem 5.4. *Let $n \geq 2$ be a positive integer and K be a global field with* $\operatorname{char} K = 0$ *or* $\operatorname{char} K \nmid n$. *Then, for an abelian variety A over K and an arbitrary positive integer m, there exists a $(\mathbb{Z}/n\mathbb{Z})$-extension L/K such that*

$$r_n(Ш_K(A/L)) \geq m.$$

Proof. First consider the case $n = p^k$. By Theorems 4.10 and 3.4, there exists a $(\mathbb{Z}/p^k\mathbb{Z})$-extension L/K such that

$$r_{p^k}(X_L) \geq M + 2g + m \quad \text{and} \quad r := \operatorname{rank}_{\mathbb{Z}} A(L) \leq M,$$

where $X_L = \operatorname{res}_{L/K}(\mathrm{H}^1(K, A[n])) \cap \mathrm{Sel}_n(A/L)$. Denote $\psi_L : \mathrm{H}^1(L, A[p^k]) \to \mathrm{H}^1(L, A)[p^k]$. Then $\operatorname{Ker} \psi_L = A(L)/p^k A(L)$. Since $r \leq M$, we have $r_{p^k}(\psi_L(X_L)) \geq m$. So it suffices to show that $\psi_L(X_L) \subset Ш_K(A/L)$. Since $X_L \subset \mathrm{Sel}_{p^k}(A/L)$, from the exact sequence

$$0 \to A(L)/p^k A(L) \to \mathrm{Sel}_{p^k}(A/L) \to Ш(A/L)[p^k] \to 0$$

we obtain $\psi_L(X_L) \subset Ш(A/L)$. Consider the following commutative diagram.

$$\begin{array}{ccc} \mathrm{H}^1(K, A[p^k]) & \xrightarrow{\psi_K} & \mathrm{H}^1(K, A)[p^k] \\ \downarrow{\scriptstyle \operatorname{res}'_{L/K}} & & \downarrow{\scriptstyle \operatorname{res}_{L/K}} \\ \mathrm{H}^1(L, A[p^k]) & \xrightarrow{\psi_L} & \mathrm{H}^1(L, A)[p^k] \end{array}$$

The fact that $X_L \subset \operatorname{Im} \operatorname{res}'_{L/K}$ implies that $\psi_L(X_L) \subset \operatorname{res}_{L/K}(\mathrm{H}^1(K, A)[p^k])$. Thus

$$\psi_L(X_L) \subset Ш_K(A/L).$$

The general case follows by replacing $Ш(A/L)$ by $Ш_K(A/L)$, and applying the same argument as in the proof of Theorem 4.11. □

6. Growth of fine Selmer groups and fine Tate–Shafarevich groups

The aim of this section is to solve a problem raised by Lim and Murty in [LM16]. Our answer also generalizes their results about the growth of fine Selmer groups in $(\mathbb{Z}/p\mathbb{Z})$-extensions.

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

Definition 6.1. Let A be an abelian variety over a number field K, and recall that

$$\mathrm{Sel}_{p^k}(A/K) := \mathrm{Ker}\left(\mathrm{H}^1(K, A[p^\infty])\right) \to \bigoplus_{v\in\mathcal{P}\ell_K} \mathrm{H}^1(K_v, A)[p^\infty]).$$

The p^k-fine Selmer group $R_{p^k}(A/K)$ of A over K is defined by the exact sequence

$$0 \to R_{p^k}(A/K) \to \mathrm{Sel}_{p^k}(A/K) \to \bigoplus_{v|p} H^1(K_v, A[p^k]).$$

Similarly the p^∞-fine Selmer group $R_{p^\infty}(A/K)$ is defined by the exact sequence

$$0 \to R_{p^\infty}(A/K) \to \mathrm{Sel}_{p^\infty}(A/K) \to \bigoplus_{v|p} H^1(K_v, A[p^\infty]).$$

In [Wut07], Wuthrich introduced the fine Tate–Shafarevich groups, which we now recall.

Definition 6.2. The fine Mordell–Weil group $M_{p^k}(A/K)$ is defined by the exact sequence

$$0 \to M_{p^k}(A/K) \to A(K)/p^kA(K) \to \bigoplus_{v|p} A(K_v)/p^kA(K_v).$$

Then the fine Tate–Shafarevich group $Ш_{p^k}(A/K)$ is defined by

$$0 \to M_{p^k}(A/K) \to R_{p^k}(A/K) \to Ш_{p^k}(A/K) \to 0.$$

One can similarly define $M_{p^\infty}(A/K)$ and $Ш_{p^\infty}(A/K)$.

Lim and Murty proved the following result in [LM16].

Theorem 6.3 [LM16, Theorem 6.3]. *Let A be an abelian variety over a number field K. Suppose that $A(K)[p] \neq 0$. Then*

$$\sup\{r_p(R_{p^\infty}(A/L)) \mid L/K \text{ is a cyclic extension of degree } p\} = \infty.$$

Furthermore, they posed the following problem.

Problem 6.4. Retaining the assumptions of above theorem, do we also have

$$\sup\{r_p(Ш_{p^\infty}(A/L)) \mid L/K \text{ is a cyclic extension of degree } p\} = \infty?$$

Based on Theorem 4.11, we give a positive answer to the problem above in a more general setting.

Wuthrich has already observed that $Ш_p(A/L)$ is a subgroup of $Ш(A/L)$ with finite index, and later Kundu observed that this index has a uniform upper bound independent of L, as a result of which we have the following proposition.

Proposition 6.5 [Kun21, Proposition 4.7]. *Let A be an abelian variety over a number field K, varying over all $(\mathbb{Z}/p\mathbb{Z})$-extensions L/K. Then $Ш_p(A/L)$ is unbound if and only if $Ш(A/L)$ is unbounded.*

Since the unboundedness of $Ш(A/L)$ is proved by Theorem 4.11, we obtain the following result.

Theorem 6.6. *Let A be an abelian variety defined over a number field K. Then*

$$\sup\{r_p(Ш_p(A/L)) \mid L/K \text{ is a } (\mathbb{Z}/p\mathbb{Z})\text{-extension}\} = \infty.$$

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press

Note that $Ш_p(A/L)$ (respectively, $Ш_{p^\infty}(A/L)$) is a quotient group of $R_p(A/L)$ (respectively, $R_{p^\infty}(A/L)$), so we also get the unboundedness of fine Selmer group, which generalizes the result of Lim and Murty mentioned above by removing the condition $A(K)[p] \neq 0$.

Corollary 6.7. *Let A be an abelian variety over a number field K. Then*

$$\sup\{r_p(R_p(A/L)) \mid L/K \text{ is a cyclic extension of degree } p\} = \infty,$$
$$\sup\{r_p(R_{p^\infty}(A/L)) \mid L/K \text{ is a cyclic extension of degree } p\} = \infty.$$

Acknowledgements

The authors would like to thank the anonymous referees heartily for their invaluable comments and suggestions which greatly improved this paper. In particular, their suggestion to prove a stronger unboundedness result in Theorem 3.4 than the original version enabled us to simplify and improve the presentation in § 5. We also thank Kęstutis Česnavičius for helpful correspondence.

This work is partially supported by the Innovation Program for Quantum Science and Technology (grant no. 2021ZD0302904) and the Anhui Initiative in Quantum Information Technologies (grant no. AHY150200).

References

Čes15a K. Česnavičius, *Selmer groups and class groups*, Compos. Math. **151** (2015), 416–434.

Čes15b K. Česnavičius, *Poitou-Tate without restrictions on the order*, Math. Res. Lett. **22** (2015), 1621–1666.

Čes16 K. Česnavičius, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31** (2016), 31–61.

Čes17 K. Česnavičius, *p-Selmer growth in extensions of degree p*, J. Lond. Math. Soc. (2) **95** (2017), 833–852.

CS10 P. L. Clark and S. Sharif, *Period, index and potential* III, Algebra Number Theory **4** (2010), 151–174.

Cre11 B. Creutz, *Potential Sha for abelian varieties*, J. Number Theory **131** (2011), 2162–2174.

Kun21 D. Kundu, *Growth of p-fine Selmer groups and p-fine Shafarevich-Tate groups in $\mathbb{Z}/p\mathbb{Z}$-extension*, J. Ramanujan Math. Soc. **1** (2021), 1–9.

LM16 M. F. Lim and V. K. Murty, *The growth of fine Selmer groups*, J. Ramanujan Math. Soc. **31** (2016), 79–94.

Mad72 M. L. Madan, *Class groups of global fields*, J. Reine Angew. Math. **252** (1972), 171–177.

Mat09 K. Matsuno, *Elliptic curves with large Tate-Shafarevich groups over a number field*, Math. Res. Lett. **16** (2009), 449–461.

MR07 B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), 579–612.

MR18 B. Mazur and K. Rubin, *Diophantine stability, with an appendix by M. Larsen*, Amer. J. Math. **140** (2018), 571–616.

MRS07 B. Mazur, K. Rubin and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), 419–438.

Mil72 J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

Neu13 J. Neukirch, *Algebraic number theory*, Grundl. Math. Wissen., vol. 322 (Springer, 2013).

NSW08 J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Grundl. Math. Wissen., vol. 323, second edition (Springer, 2008).

Wut07 C. Wuthrich, *The fine Tate-Shafarevich group*, Math. Proc. Cambridge Philos. Soc. **142** (2007), 1–12.

The growth of Tate–Shafarevich groups in cyclic extensions

Yi Ouyang yiouyang@ustc.edu.cn
School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China

and

Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China

Jianfeng Xie xjfnt@mail.ustc.edu.cn
School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China

https://doi.org/10.1112/S0010437X22007734 Published online by Cambridge University Press