TESTING LOCAL-GLOBAL DIVISIBILITY AT A SMALL SET OF PRIMES

ALEXANDER B. IVANOV AND LAURA PALADINO

Abstract. We show that the local-global divisibility in commutative algebraic groups defined over number fields can be tested on sets of primes of arbitrary small density, i.e. stable and persistent sets. We also give a new description of the cohomological group giving an obstruction to the problem. In addition, we show new examples of stable sets.

1. Introduction

Let k be a number field. Let A be a connected commutative group scheme of finite type over k. Dvornicich and Zannier investigated a local-global principle for divisibility of rational points on A:

Problem 1.1 (Local-global divisibility problem [DZ01]). *Let r be a positive integer and let $P \in A(k)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of k, we have $rD_{\mathfrak{p}} = P$ for some $D_{\mathfrak{p}} \in A(k_{\mathfrak{p}})$, where $k_{\mathfrak{p}}$ denotes the completion of k at $\mathfrak{p}$. Can one conclude that there exists $D \in A(k)$ with $rD = P$?*

Of course, one may assume that r is a power of a rational prime without loosing any generality. The solution to Problem 1.1 and to variants of it are known in many cases, in particular, for tori [DZ01, Ill08] and for elliptic curves [PRV12, PRV14, Cre16]. In elliptic curves the answer is affirmative for every power $r = p^n$, with $p > B(d)$, where $d := [k : \mathbb{Q}]$ and

$$B(d) := \begin{cases} 3 & if\ k = \mathbb{Q}; \\ (3^{\frac{d}{2}} + 1)^2 & if\ d > 1. \end{cases}$$

Observe that for $k \neq \mathbb{Q}$ the bound $B(d) = (3^{\frac{d}{2}} + 1)^2$ is the one appearing in [Oes], giving an effective version of Merel's Theorem on torsion points of an elliptic curve [Mer96], and in particular $E(k)[p] = 0$ for all primes $p > B(d)$. It is shown in [DP22b, §5] that for a *fixed* elliptic curve E, a *fixed* number field k and a *fixed* power r, Problem 1.1 admits an explicit and effective solution, that is there is an effectively computable constant $C(k, E, r) > 0$ such that to deduce global divisibility, it suffices to test the local one for all primes $\mathfrak{p}$ of k with norm $N\mathfrak{p} < C(k, E, r)$.

In this note we ask, whether in Problem 1.1 one can considerably shrink the set of primes where local divisibility is tested, simultaneously for *all* A, *all* k and *all* r. It turns out that this strengthened version of the problem admits a solution. More precisely, we show that certain sets of primes with arbitrary small Dirichlet density suffice, cf. Theorem 2.7. For clarity, let us state our main result in the case of elliptic curves, where the original Problem 1.1 is quite well-understood.

Theorem 1.1 (see Corollary 2.9 for most general statement). *For any $\varepsilon > 0$ there exists a set S of primes of $\mathbb{Q}$, such that for all number fields k, all elliptic curves E/k and all primes p one has $0 < \delta_k(S) < \varepsilon$ and the following hold:*

(1) If a point $P \in E(k)$ is locally divisible by p at any $\mathfrak{p} \in S_k$, then it is globally divisible by p in $E(k)$.

(2) Suppose that $p > B(d)$. Then for all $n \geq 1$, if a point $P \in E(k)$ is locally divisible by p^n at any $\mathfrak{p} \in S$, then it is globally divisible by p^n in $E(k)$.

Moreover, sets S as in Theorem 1.1 exist in abundance, and examples of them can be given explicitly, cf. §3.

It is well known that an obstruction to the validity of Problem 1.1 is given by the first local cohomology group (see [DZ01], [DZ07] and Equation (2.2) below). Such a group is isomorphic to some modified Tate-Shafarevich groups defined by sets S of primes of density one (see for instance [Cre12, DP22a]). If one shrinks the set S, the Tate-Shafarevich group can *a priori* become bigger. Our main point is that if we shrink S is an appropriate way, then the Tate-Shafarevich group will stay small. This is based on the properties of the so-called *stable* and *persistent* sets of primes studied in [Iva16]. In §3 we also give new examples of such sets with particularly nice properties.

At the end of the paper we state a generalization of a classical question posed by Cassels about the p-divisibility of elements of the Tate-Shafarevich group and we discuss the implications of our results for such a question.

Notation. We denote by p a rational prime. We fix once and for all an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and consider all algebraic extensions of $\mathbb{Q}$ as subfields of $\overline{\mathbb{Q}}$. Unless stated otherwise, k always denote a number field of degree $d = [K : \mathbb{Q}]$. If ℓ/k is a Galois extension, we denote by $\mathrm{Gal}_{\ell/k}$ its Galois group. We denote by Σ_k the set of primes of k. If $S \subseteq \Sigma_k$ and ℓ/k is a finite extension, we write S_ℓ for the preimage of S under the natural map $\Sigma_\ell \to \Sigma_k$. We denote by $\delta_k(S) \in [0, 1]$ the Dirichlet density of a set $S \subseteq \Sigma_k$, whenever it exists. Whenever we write "density" below, we mean "Dirichlet density".

By A we denote a commutative algebraic group defined over k and by K_n the extension of k trivializing $A[p^n]$, i.e. the p^n-division field of A over k, where p is a fixed prime and n is a positive integer.

Acknowledgements. The first author was supported by a Heisenberg grant of the DFG (grant nr. IV 177/3-1), based at the Universities of Bonn and Bochum. Also he was supported by the Leibniz Universität Hannover. The second author is a member of INdAM-GNSAGA.

2. Testing local-global divisibility at a stable set

2.1. **Review of stable sets.** We recall the following definition.

Definition 2.1 ([Iva16], §2)**.** Let $\mathscr{L}/k$ be an algebraic extension, $S \subseteq \Sigma_k$ and $\lambda > 1$.

(1) A finite subextension $\mathscr{L}/K/k$ is called λ-*stabilizing* (resp. *persisting*) for S, if there exists a subset $T \subseteq S$ and some $a \in (0, 1]$ such that for all finite subextensions $\mathscr{L}/L/K$ one has $\lambda a > \delta_L(T_L) \geq a$ (resp. $\delta_L(T_L) = \delta_K(T_K) > 0$).

(2) S is λ-*stable* (resp. *persisting*) for $\mathscr{L}/k$, if it has a λ-stabilizing (resp. persisting) subextension of $\mathscr{L}/k$.

There are many natural examples of stable and persistent sets, cf. [Iva16, §3]. For example, if ℓ/k is a finite Galois extension, then for $\sigma \in \mathrm{Gal}_{\ell/k}$ the set

$$P_{\ell/k}(\sigma) = \{\mathfrak{p} \in \Sigma_k \colon \mathfrak{p} \text{ is unramified in } \ell/k \text{ and } \mathrm{Frob}_\mathfrak{p} = C(\sigma, \mathrm{Gal}_{l/k})\}, \tag{2.1}$$

where $C(\sigma, G_{\ell/k})$ denotes the conjugacy class of σ, is persistent for any algebraic extension $\mathscr{L}/k$ satisfying $C(\sigma, G_{\ell/k}) \cap \mathrm{Gal}_{\ell/\mathscr{L}\cap\ell} \neq \varnothing$, with persisting field $\mathscr{L} \cap \ell$. In §3 we give new interesting examples of persistent sets.

Stable sets generalize sets of density one in the following sense. Let ℓ/k be a finite extension. If S is a set of primes of k with density one, then any element of $\mathrm{Gal}_{\ell/k}$ is a Frobenius at S, and consequently any cyclic subgroup is a decomposition subgroup of a prime in S. Weakening the assumption on S to be p-stable for ℓ/k with stabilizing field k, destroys the claim about *elements*, but the claim about *cyclic p-subgroups* (that is, of p-power order and not just of order p) remains true:

Lemma 2.2 ([Iva16], Lemma 4.4)**.** *Let ℓ/k be a finite Galois extension, S a set of primes of k and p a rational prime such that S is p-stable for ℓ/k with p-stabilizing field k. Then any cyclic p-subgroup of $\mathrm{Gal}_{\ell/k}$ is the decomposition subgroup of a prime in S.*

2.2. p-stable sets detect local-global divisibility by p^n.

Recall the definition of the cohomology group satisfying the *local conditions* [DZ01]. Let Γ be a finite group and M a discrete Γ-module. Then

$$H^1_{\mathrm{loc}}(\Gamma, M) := \ker\left(H^1(\Gamma, M) \to \prod_{C\subseteq\Gamma} H^1(C, M)\right), \tag{2.2}$$

where the product is taken over all cyclic subgroups $C \subseteq \Gamma$, and the map is the product of restriction maps.

Lemma 2.3. *Let Γ, M be as above, and suppose that M is p-primary for a rational prime p. Then $H^1_{\mathrm{loc}}(\Gamma, M) = \ker\left(H^1(\Gamma, M) \to \prod_{C\subseteq\Gamma} H^1(C, M)\right)$, where the product is taken over all cyclic p-subgroups $C \subseteq \Gamma$.*

Proof. This follows from the fact that for any finite group H and any p-primary module M, $H^1(H, M) \to H^1(H_p, M)$ is injective, where H_p is a p-Sylow subgroup of H (see [NSW13, (1.6.10)]). □

Let $K_n^{\mathrm{ab}}(p)/k$ be the maximal abelian pro-p extension of K_n. The following generalization of [DZ01, Prop. 2.1] shows that it suffices to test local-global divisibility by p^n at a p-stable set of primes:

Proposition 2.4. *Let p be a rational prime and $n \geq 1$ an integer. Let A/k be a commutative algebraic group. Let S be a set of primes of k, which is p-stable for $K_n^{\mathrm{ab}}(p)/k$ with p-stabilizing field k. Assume that $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_n/k}, A[p^n]) = 0$. Then the following holds. Let $P \in A(k)$, such that for all $\mathfrak{p} \in S$, there is some $Q_\mathfrak{p} \in A(k_\mathfrak{p})$ with $P_\mathfrak{p} = p^n Q_\mathfrak{p}$. Then there is some $Q \in A(k)$ with $P = p^n Q$.*

Proof. Let $D \in A(\overline{\mathbb{Q}})$ be a point with $p^n D = P$ and let $\ell = k(D)$ be the corresponding extension of k. Put $F = K_n \cdot \ell$. Then F/k is Galois and ℓ/k is cyclic of p-power degree, so in particular $F \subseteq K_n(p)^{\mathrm{ab}}$. One can define a 1-cocycle $c\colon \mathrm{Gal}_{F/k} \to A[p^n]$, by $c(\sigma) := \sigma(D) - D$, for all $\sigma \in \mathrm{Gal}_{F/k}$. Its image $[c] \in H^1(\mathrm{Gal}_{F/k}, A[p^n])$ is zero if and only if $P = p^n D'$ for some $D' \in A(k)$, see [DZ01, p. 320]. Moreover, as by assumpion P is locally p^n-divisible at any $\mathfrak{p} \in S$, the same argument with cocycles show that the restriction of $[c]$ to $H^1(C, A[p^n])$ is zero, where

$C \subseteq \mathrm{Gal}_{F/k}$ is the decomposition subgroup of any prime in S. Now, as $F \subseteq K_n(p)^{\mathrm{ab}}$, by Lemma 2.2 the set of decomposition subgroups in $\mathrm{Gal}_{F/k}$ at primes in S contains the set of all cyclic p-subgroups of $\mathrm{Gal}_{F/k}$, and so by Lemma 2.3 we deduce $[c] \in H^1_{\mathrm{loc}}(\mathrm{Gal}_{F/k}, A[p^n])$. To finish the proof of Proposition 2.4 it thus remains to show that the restriction via $\mathrm{Gal}_{F/k} \twoheadrightarrow \mathrm{Gal}_{K_n/k}$ induces an isomorphism $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_n/k}, A[p^n]) \xrightarrow{\sim} H^1_{\mathrm{loc}}(\mathrm{Gal}_{F/k}, A[p^n])$. But this is done in the proof of [DZ01, Prop. 2.1]. □

Corollary 2.5. *Let p be a rational prime and $n \geq 1$ an integer. Let A/k be a commutative algebraic group. Let S be a set of primes of k, which is p-stable for $K_n^{\mathrm{ab}}(p)/k$ with p-stabilizing field k. Assume that $P \in A(k)$, such that for all $\mathfrak{p} \in S$, there is some $Q_{\mathfrak{p}} \in A(k_{\mathfrak{p}})$ with $P_{\mathfrak{p}} = p^n Q_{\mathfrak{p}}$. Then $D \in A(K_n)$, for all D such that $P = p^n D$.*

Proof. One can apply the same argument used in the proof of [DZ01, Corollary 2.3], by substituting the set of density one with the set S. □

We denote by G_k the absolute Galois group $\mathrm{Gal}_{\bar{\mathbb{Q}}/k}$ and by $G_{k_{\mathfrak{p}}}$ the absolute Galois group $\mathrm{Gal}_{\bar{k}_{\mathfrak{p}}/k_{\mathfrak{p}}}$, where $\bar{k}_{\mathfrak{p}}$ is an algebraic closure of $k_{\mathfrak{p}}$. Let S be a subset of primes of k which is p-stable at $K_n^{\mathrm{ab}}(p)/k$ with p-stabilizing field k. We define a modified Tate-Shafarevich group related to S and we will prove that it is isomorphic to $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_n/k}, A[p^n])$.

Definition 2.6. Let A be a comutative algebraic group defined over a number field k and let S be a set of primes of k, unramified in K_n, which is p-stable at $K_n^{\mathrm{ab}}(p)/k$ with p-stabilizing field k. We denote by $Ш_S(k, A[p^n])$ the subgroup of $H^1(G_k, A[p^n])$ formed by the classes of the cocycles vanishing in $k_{\mathfrak{p}}$, for all $\mathfrak{p} \in S$, i.e.

$$Ш_S(k, A[p^n]) := \bigcap_{\mathfrak{p} \in S} \ker(H^1(G_k, A[p^n]) \xrightarrow{res_{\mathfrak{p}}} H^1(G_{k_{\mathfrak{p}}}, A[p^n])) \tag{2.3}$$

Notice that in Equation (2.3) by replacing S with the set of primes of k one gets the definition of the classical Tate-Shafarevich group $Ш(k, A[p^n])$. We are going to prove that $H^1_{\mathrm{loc}}(G, A[p^n]) \simeq Ш_S(k, A[p^n])$.

Proposition 2.7. *Let p be a rational prime and $n \geq 1$ an integer. Let A/k be a commutative algebraic group. Let S be a set of primes of k, unramified in K_n, which is p-stable for $K_n^{\mathrm{ab}}(p)/k$ with p-stabilizing field k. Then $H^1_{\mathrm{loc}}(G, A[p^n]) \simeq Ш_S(k, A[p^n])$.*

Proof. Let S_{K_n} denote the set of primes $w_{\mathfrak{p}}$ of K_n extending the primes $\mathfrak{p}$ in S and by $K_{n,w_{\mathfrak{p}}}$ we denote the completion of K_n at the place $w_{\mathfrak{p}}$. Let $G_{\mathfrak{p}} := \mathrm{Gal}_{K_{n,w_{\mathfrak{p}}}/k_{\mathfrak{p}}}$ and consider the following diagram given by the inflation restrictions exact sequence

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(G, A[p^n]) & \xrightarrow{inf} & H^1(G_k, A[p^n]) & \xrightarrow{res} & H^1(G_{K_n}, A[p^n]) \\
 & & \Big\downarrow \prod res_{\mathfrak{p}} & & \Big\downarrow \prod res_{\mathfrak{p}} & & \Big\downarrow \prod res_{w_{\mathfrak{p}}} \\
0 & \longrightarrow & \prod_{\mathfrak{p} \in S} H^1(G_{\mathfrak{p}}, A[p^n]) & \xrightarrow{inf} & \prod_{\mathfrak{p} \in S} H^1(G_{k_{\mathfrak{p}}}, A[p^n]) & \xrightarrow{res} & \prod_{w_{\mathfrak{p}} \in S_{K_n}} H^1(G_{K_{n,w_{\mathfrak{p}}}}, A[p^n])
\end{array}$$

The kernel of the vertical map on the left is $H^1_{\mathrm{loc}}(G, A[p^n])$ by assumption on S and by Lemma 2.2 and the kernel of the central vertical map is $Ш_S(k, A[p^n])$. The vertical map on the right is injective because of G_{K_n} acting trivially on $A[p^n]$ and because of $G_{K_{n,w}}$ varying over all cyclic subgroups of G_{K_n} as w varies in S_{K_n} by Lemma 2.2. Therefore $H^1_{\mathrm{loc}}(G, A[p^n]) \simeq \text{Ш}_S(k, A[p^n])$. ☐

At cost of slightly strengthening the assumption on S, we can eliminate the dependence on the particular algebraic group A in Proposition 2.4. For an integer $M > 0$, consider the class $\mathfrak{C}_{\leq M}(k)$ of all commutative algebraic groups over k, such that $\dim_{\mathbb{F}_p} \# A[p](\overline{\mathbb{Q}}) \leq M$. Moreover, for a set $\mathbb{P} \subseteq \Sigma_{\mathbb{Q}}$ of rational primes, let $k(\mathbb{P})$ be the compositum of all finite extensions of k whose orders are products of elements of $\mathbb{P}$.

Corollary 2.8. *Let p be a rational prime and let $M > 0$. Let S be a set of primes of k. Assume that S is p-stable with p-stabilizing field k for the extension $k(\mathbb{P}(M))/k$, where $\mathbb{P}(M)$ is the set of all prime divisors of $\# \mathrm{GL}_{M'}(\mathbb{F}_p)$ for all $M' \leq M$. Then for any $A \in \mathfrak{C}_{\leq M}(k)$, such that $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_n/k}, A[p^n]) = 0$, the following holds.*

Let $P \in A(k)$, such that for all $\mathfrak{p} \in S$, there is some $Q_{\mathfrak{p}} \in A(k_{\mathfrak{p}})$ with $P_{\mathfrak{p}} = p^n Q_{\mathfrak{p}}$. Then there is some $Q \in A(k)$ with $P = p^n Q$.

For example, if one restricts further to the class of elliptic curves one can take $M = 2$ and $\mathbb{P}$ the set of prime divisors of $p, p \pm 1$. For abelian varieties of dimension $\leq g$, one can take $M = 2g$.

Proof of Corollary 2.8. We have to show that for a particular $A \in \mathfrak{C}_M(k)$, the assumptions of Proposition 2.4 hold, i.e., that $K_n(p)^{\mathrm{ab}} \subseteq k(\mathbb{P}(M))$. As $p \in \mathbb{P}(M)$, it suffices to show that $K_n \subseteq k(\mathbb{P}(M))$. Also as K_n/K_1 is a p-extension, it suffices to show that $K_1/k \subseteq k(\mathbb{P}(M))$. But $\mathrm{Gal}_{K_1/k} \subseteq \mathrm{GL}(A[p])$, which is a subgroup of $\mathrm{GL}_{M'}(\mathbb{F}_p)$ for some $M' \leq M$. ☐

Strengthening assumptions on S even further, Corollary 2.8 immediately gives the following:

Corollary 2.9. *Fix a prime p. Let S be a set of primes of k, which is persistent for $\overline{\mathbb{Q}}/k$ with persisting field k. For any commutative algebraic group A/k and any $n > 0$, if $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_n/k}, A[p^n]) = 0$, the following holds.*

Let $P \in A(k)$, such that for all $\mathfrak{p} \in S$, there is some $Q_{\mathfrak{p}} \in A(k_{\mathfrak{p}})$ with $P_{\mathfrak{p}} = p^n Q_{\mathfrak{p}}$. Then there is some $Q \in A(k)$ with $P = p^n Q$.

We show in Proposition 3.1 below that sets S satisfying the requirements of the corollary exist in abundance. Using this along with existing results on the original form of Problem 1.1, Corollary 2.9 specializes to the case of elliptic curves:

Proof of Theorem 1.1. Pick a set $S \subseteq \Sigma_{\mathbb{Q}}$ as constructed in Proposition 3.1. Let E/k be an elliptic curve. By Corollary 2.9 it suffices to show that $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_p/k}, E[p]) = 0$ for all p, resp. that $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_{p^n}/k}, E[p^n]) = 0$ for all $p > B(d)$ and all $n > 1$. The first case is easy, as was observed in [DZ01, beginning of §3]: $\mathrm{Gal}_{K_p/k}$ is then a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, which implies that the p-Sylow subgroup of $\mathrm{Gal}_{K_p/k}$ is cyclic and so $H^1_{\mathrm{loc}}(\mathrm{Gal}_{K_p/k}, E[p]) = 0$. In the second case we may apply [PRV12, Theorem 1' (on p. 8)] (see also Corollary 2 of *loc. cit.*) and [PRV14]. ☐

3. New examples of stable sets

It is easy to give examples of stable sets S with arbitrary small density in the whole tower $\mathscr{L}/k$, when $\mathscr{L}$ is some reasonably small subextension of $\overline{\mathbb{Q}}/k$. However, those examples will often not be stable for other towers $\mathscr{L}'/k$. Consider, for example, $S = P_{\ell/k}(\sigma)$ as in (2.1). If $\sigma = 1$, then S will be stable –even persistent– for any extension $\mathscr{L}/k$, but if $\mathscr{L} \supseteq \ell$, the persisting field is ℓ and $\delta_\ell(S_\ell) = 1$, that is S_ℓ eventually becomes "big". On the other hand, if $\sigma \neq 1$, then $\delta_{\ell'}(S_{\ell'}) = 0$ for any finite ℓ'/ℓ, and hence S is not stable for $\mathscr{L}/k$ whenever $\mathscr{L} \supseteq \ell$. With this in mind, we now produce now many examples of sets persistent for $\overline{\mathbb{Q}}/k$ with persisting field k and arbitrary small positive density.

Proposition 3.1. *For any number field k and any $\varepsilon > 0$, there exists a set S of primes of k satisfying*

$$0 < \delta_k(S) = \delta_\ell(S_\ell) < \varepsilon$$

for all finite extensions ℓ/k. In particular, S is persistent for $\overline{\mathbb{Q}}/k$ with persisting field k.

Proof. Let p be a prime such that $\frac{1}{p-1} < \varepsilon$. Let k_∞/k be a $\mathbb{Z}_p$-extension (e.g. the cyclotomic one) with Galois group identified with $\mathbb{Z}_p$. For $n \geq 1$, choose $a_n \in \mathbb{F}_p^\times$ and consider the set

$$A = \bigcup_{n\geq 1} \left(a_n p^{n-1} + p^n\mathbb{Z}_p\right) \subseteq \mathbb{Z}_p.$$

We put

$$S = P_{k_\infty/k}(A),$$

the set of all primes unramified in k_∞/k, whose Frobenius lies in A. Clearly, A is open in $\mathbb{Z}_p$ and one computes $\overline{A} = A \cup \{0\}$. Equip $\mathbb{Z}_p$ with the invariant Haar measure μ normalized such that $\mu(\mathbb{Z}_p) = 1$. Then the boundary $\overline{A} \smallsetminus A^\circ = \{0\}$ of A has measure 0, and the infinite Chebotarev theorem [Ser68, I.2.2 Corollary 2b)] (which we may apply as k_∞/k is ramified at most in the finitely many primes above p and ∞) then shows that S has a density and that it is equal to

$$\delta_k(S) = \mu(A) = \sum_{n\geq 1}^{\infty} p^{-n} = \frac{1}{p-1}.$$

Now, let ℓ/k be a finite extension. Then there is some $m \geq 0$ such that $\ell \cap k_\infty = k_m := (k_\infty)^{p^m\mathbb{Z}_p}$. Let $\ell_\infty = k_\infty.\ell$. Via $\mathrm{Gal}_{\ell_\infty/\ell} \cong \mathrm{Gal}_{k_\infty/k_m}$, we may identify $\mathrm{Gal}_{\ell_\infty/\ell}$ with $p^m\mathbb{Z}_p \subseteq \mathbb{Z}_p$. Let $\mathrm{Spl}_{\ell/k}$ denotes the set of primes of ℓ, which are split (and unramified) over k. Then

$$S_\ell \cap \mathrm{Spl}_{\ell/k} = P_{\ell_\infty/\ell}(A \cap p^m\mathbb{Z}_p), \tag{3.1}$$

where we ignore the finitely many primes of ℓ which ramify in ℓ_∞/k. Now, $\Sigma_\ell \smallsetminus \mathrm{Spl}_{\ell/k}$ consists of primes of ℓ, which are not split over $\mathbb{Q}$, so it has density 0. In particular, $\delta_\ell(S_\ell)$ exists if and only if $\delta_\ell(S_\ell \cap \mathrm{Spl}_{\ell/k})$ exists, in which case both agree. On the other hand, the argument using infinite Chebotarev applied above to compute $\delta_k(S)$ applies also to $P_{\ell_\infty/\ell}(A \cap p^m\mathbb{Z}_p)$, giving $\delta_\ell(P_{\ell_\infty/\ell}(A \cap p^m\mathbb{Z}_p)) = \frac{1}{p-1}$. Combining the two computations, we get $\delta_\ell(S_\ell) = \delta_\ell(P_{\ell_\infty/\ell}(A \cap p^m\mathbb{Z}_p)) = \frac{1}{p-1}$, finishing the proof. □

Remark 3.2. One has to be careful in the above proof, as the Dirichlet density does not satisfy σ-additivity: suppose that $T_n \subseteq \Sigma_k$ $(n \geq 1)$ is a collection of mutually disjoint subsets, such that $\delta_k(T_n)$ exists. Let $T = \bigcup_n T_n$. Then it might happen that $\delta_k(T)$ does not exist, and even if it exists, it might happen that $\delta_k(T) \neq \sum_{n\geq 1} \delta_k(T_n)$ (it is enough to consider singletons $T_n = \{\mathfrak{p}_n\}$ for any n). However, by the argument in the proof of Proposition 3.1, the density of the set S, which is in fact a disjoint union of infinitely many Chebotarev sets, exists and is equal to the sum of densities of these Chebotarev sets.

4. On a question posed by Cassels

In addition Problem 1.1 is strongly related to the following question stated by Cassels in 1962 that remained open for 50 years (see [DP22a] for further details).

Cassels' question. *Let k be a number field and E be an elliptic curve defined over k. Are the elements of $Ш(k, E)$ infinitely divisible by a prime p when considered as elements of the Weil-Châtelet group $H^1(G_k, A)$ of all classes of principal homogeneous spaces for E defined over k?*

An affirmative answer for $p > B(d)$ is implied by [Cre13, Theorem 3] and the results in [PRV12, PRV14]. Since 1972 this question was considered in abelian varieties of every dimension by various authors [Baš72, Cre13, ÇS15]. In particular, Creutz showed sufficient and necessary conditions to get an affirmative answer and the existence of counterexamples for every p in infinitely many abelian varieties [Cre13]. [Cre16]. Moreover, Çiperiani and Stix also showed sufficient conditions to get an affirmative answer [ÇS15].

In the spirit of this article, we can pose the following more general question.

Problem 4.1. *Let k be a number field and A an abelian variety defined over k. Let S be an infinite set of places of k and let*

$$Ш_S(k, A) := \bigcap_{\mathfrak{p}\in S} \ker(H^1(G_k, A[p^n]) \xrightarrow{res_{\mathfrak{p}}} H^1(G_{k_{\mathfrak{p}}}, A[p^n])).$$

Are the elements of $Ш_S(k, A)$ infinitely divisible by a prime p when considered as elements of the Weil-Châtelet group $H^1(G_k, A)$?

As a consequence of Proposition 2.7, in the case of elliptic curves curves Problem 4.1 has an affirmative answer for all $p > B(d)$, for every sets S which is p-stable for $\cup_{n\in\mathbb{N}} K_n^{ab}(p)/k$ with p-stabilizing field k.

Corollary 4.1. *Let k be a number field and E an elliptic curve over k. Let S be a set of places of k which is p-stable for $\cup_{n\in\mathbb{N}} K_n^{ab}(p)/k$ with stabilizing field k. Then the elements of $Ш_S(k, E)$ are infinitely divisible by every $p > B(d)$ when considered as elements of $H^1(G_k, E)$.*

Proof. By the results in [PRV12] and [PRV14], we have $H^1_{\mathrm{loc}}(G, E[p^n]) = 0$, for all $p > B(d)$ and all $n \geq 1$. By Proposition 2.7, we have $Ш_S(k, E[p^n]) = 0$, for all $p > B(d)$ and all $n \geq 1$. The conclusion is then implied by [Cre13, Theorem 3]. □

Observe that by Proposition 3.1 there are many sets S of primes satisfying the assumtpions of Corollary 4.1.

References

[Baš72] M. I. Bašmakov, *Cohomology of Abelian varieties over a number field*, Uspehi Mat. Nauk **27** (1972), no. 6(168), 25–66. MR 0399110

[Cre12] Brendan Creutz, *A Grunwald-Wang type theorem for abelian varieties*, Acta Arith. **154** (2012), no. 4, 353–370. MR 2949874

[Cre13] ———, *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. Lond. Math. Soc. **45** (2013), no. 5, 935–942. MR 3104985

[Cre16] ———, *On the local-global principle for divisibility in the cohomology of elliptic curves*, Math. Res. Lett. **23** (2016), no. 2, 377–387. MR 3512890

[ÇS15] Mirela Çiperiani and Jakob Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, J. Reine Angew. Math. **700** (2015), 175–207. MR 3318515

[DP22a] Roberto Dvornicich and Laura Paladino, *Local-global questions for divisibility in commutative algebraic groups*, Eur. J. Math. **8** (2022), no. suppl. 2, S599–S628. MR 4507256

[DP22b] ———, *On the division fields of an elliptic curve and an effective bound to the hypotheses of the local-global divisibility*, Int. J. Number Theory **18** (2022), no. 7, 1567–1590. MR 4439046

[DZ01] R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001), no. 3, 317–338.

[DZ07] Roberto Dvornicich and Umberto Zannier, *On a local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lond. Math. Soc. **39** (2007), no. 1, 27–34. MR 2303515

[Ill08] Marco Illengo, *Cohomology of integer matrices and local-global divisibility on the torus*, J. Théor. Nombres Bordeaux **20** (2008), no. 2, 327–334. MR 2477506

[Iva16] A. Ivanov, *Stable sets of primes in number fields*, Algebra & Number Theory **10** (2016), no. 1, 1–36.

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

[NSW13] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, second ed., Springer, 2013.

[Oes] J. Oesteré, *Torsion des courbes elliptiques sur les corps de nombres*, preprint.

[PRV12] L. Paladino, G. Ranieri, and E. Viada, *On local-global divisibility by p^n in elliptic curves*, Bull. Lon. Math. Soc. **44** (2012), no. 5, 789–802.

[PRV14] Laura Paladino, Gabriele Ranieri, and Evelina Viada, *On the minimal set for counterexamples to the local-global principle*, J. Algebra **415** (2014), 290–304. MR 3229518

[Ser68] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, New York, Benjamin Publ., 1968.

Alexander Ivanov, Ruhr-Universität Bochum, Fakultät für Mathematik, IB 2/153, Universitätsstrasse 150, D-44780 Bochum

Email address: alexander.ivanov@ruhr-uni-bochum.de

Laura Paladino, Università della Calabria, Ponte Bucci, Cubo 30B, 87075, Rende (CS), Italy

Email address: laura.paladino@unical.it