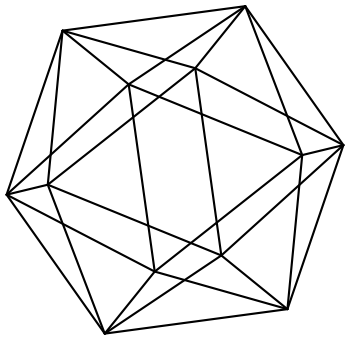
Max-Planck-Institut für Mathematik
Bonn

Local-global questions for divisibility in commutative algebraic groups

by

Roberto Dvornicich
Laura Paladino



Max-Planck-Institut für Mathematik
Preprint Series 2017 (64)

Local-global questions for divisibility in commutative algebraic groups

Roberto Dvornicich
Laura Paladino

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Università di Pisa
Dipartimento di Matematica
Largo Bruno Pontecorvo 5
56126 Pisa
Italy

Università della Calabria
Dipartimento di Matematica e Informatica
Ponte Pietro Bucci, Cubo 30B
87036 Arcavacata de Rende (CS)
Italy

MPIM 17-64

LOCAL-GLOBAL QUESTIONS FOR DIVISIBILITY IN COMMUTATIVE ALGEBRAIC GROUPS

ROBERTO DVORNICICH AND LAURA PALADINO*

Abstract. This is a survey focusing on the Hasse principle for divisibility of points in commutative algebraic groups and its relation with the Hasse principle for divisibility of elements of the Tate-Shavarevich group in the Weil-Châtelet group. The two local-global subjects arose as a generalization of some classical questions considered respectively by Hasse and Cassels. We give an overwiev of the long-established results and the ones achieved during the last fifteen years, when the questions were taken up again in a more general setting. Furthermore we give an answer to the local-global divisibility in semidirect products of a torus of dimension 1 with an elliptic curve.

1. Introduction

In 1923-1924 Hasse proved the following famous statement.

HASSE PRINCIPLE: *Let k be a number field and let $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ be a quadratic form. If F represents 0 non-trivially in k_v, for all completions k_v of k, then $F = 0$ has a non-trivial solution in k.*

The assumption that F is isotropic in k_v *for all but finitely many completions* (implying the same conclusion) gives a stronger form of the principle. Since then, many mathematicians have been concerned with similar so-called local-global problems, i.e., they have been questioning if the validity of some properties in all but finitely many local fields k_v could ensure the validity of the same properties in k. When the answer to such a problem is affirmative, one says that there is a local-global principle or a Hasse Principle.

Local-global questions have often an equivalent formulation in terms of principal homogeneous spaces under some group schemes G over k, that are classified by the first cohomology group $H^1(G, k)$ (see for example [24]). When the hypotheses require the

Date: 19-10-2017.

* Corresponding author.

validity of the assertion in *all* completions k_v, one can study the behaviour of the Tate-Shafarevich group $Ш(G,k)$ to get information about the failure of the principle. In fact, this group is the intersection of the kernels of the maps $H^1(G,k) \to H^1(G,k_v)$, as v varies in the set M_k of places of k, and its vanishing ensures a positive answer to the question. On the other hand, by answering the problem in some cases, one can get information about $Ш(G,k)$ and so check the validity of the Birch and Swinnerton-Dyer conjecture in particular instances. When the hypotheses of a local-global question require its validity in *all but finitely many* completions k_v, the group that interprets the hypotheses of the problem in the cohomological context is not exactly $Ш(G,k)$, but a similar group, i. e., the intersection of the kernels of the map $H^1(G,k) \to \prod_{v\in\Sigma} H^1(G,k_v)$, as v varies in a subset Σ of M_k containing all the places v, such that there exists a local solution in k_v. The two groups often coincide, but there are examples in which they are not equal (see for instance [39] and Section 6.2). In various cases it suffices to study the behaviour of one of them to understand the structure of the other (see Section 5).

In this paper we will be concerned with the following two local-global problems and their cohomological setting.

Problem 1. *Let k be a number field, M_k be the set of the places of k and $\mathcal{G}$ be a commutative algebraic group defined over k. Let $P \in \mathcal{G}(k)$ and let q be a positive integer. Assume that for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$. Is it possible to conclude that there exists $D \in \mathcal{G}(k)$ such that $P = qD$?*

Problem 1 was stated by the first author and Zannier in 2001 in [18] and they named it *Local-global divisibility problem.* In fact, it is a particular case of the following second local-global question.

Problem 2. *Let k be a number field, M_k be the set of the places of k and $\mathcal{G}$ be a commutative algebraic group defined over k. Let q be a positive integer and let $\sigma \in H^r(k,\mathcal{G})$. Assume that for all $v \in M_k$ there exists $\tau_v \in H^r(k_v,\mathcal{G})$ such that $q\tau_v = \sigma$. Can we conclude that there exists $\tau \in H^r(k,\mathcal{G})$, such that $q\tau = \sigma$?*

When $r = 0$ Problem 2 is nothing but Problem 1. In the present form, for all commutative algebraic groups, Problem 2 was stated in 2016 by Creutz (see [16]). In fact, when $r = 1$, the question was firstly posed by Cassels in [7] only in the case when $\mathcal{G}$ is an elliptic curve. Later on, it was considered by Bašmagov in the more general case when $\mathcal{G}$ is an abelian variety (see [3] and [4]) and recently by Çiperiani end Stix (see

[14]) too. Both problems are generally studied in the cases when $q = p^l$, with p a prime number and l a positive integer. In fact, an answer for all powers of prime numbers suffices to solve the problem for a general integer q, by using the unique factorization in $\mathbb{Z}$ and Bézout's identity.

At first we give a historical overview of the formulation of the two problems and their classical solutions. Then we describe a cohomological interpretation for Problem 1. Section 4 is dedicated to Problem 2 and Section 5 to the link between the two problems. The following Sections 6-8 are dedicated to the description of the results achieved for Problem 1, respectively in the case of elliptic curves, in the case of algebraic tori and in the case of general commutative algebraic groups. In the last section we give an answer to the local-global divisibility in semidirect products of a torus of dimension 1 with an elliptic curve. The paper ends with an Appendix in which we describe some recent results about the number fields generated by torsion points of elliptic curves.

Acknowledgments. The main part of this paper was written when the second author was a guest at the Max Planck Institute for Mathematics in Bonn. She thanks every people there for their kind hospitality. The authors are grateful to Brendan Creutz for some useful remarks about earlier versions of this paper.

2. Classical problems and classical solutions

In the case of a quadratic form X^2+rY^2, where r is a rational number, the Hasse Principle is equivalent to the statement "if a rational number is a square in K_v, for all but finitely many v, then it is a square in k". It is then natural to ask if such a principle still holds for q-powers of rational numbers, where q is a general positive integer, and not only for rational squares. The answer to such a question was given by the Grunwald-Wang Theorem (see [2, Chap. IX and Chap. X]). Here we state the theorem in its classical form, in the more general case when k is a global field. For every positive integer q, we denote by ζ_q a primitive q-th root of the unity. Furthermore, let ξ_h be a 2^h-th root of the unity such that $\xi_{h+1} = \xi_h$, and let $\eta_h := \xi_h + \xi_h^{-1}$. In particular, for every field k, there exists an integer $s_k \geq 2$ such that $\eta_{s_k} \in k$, but $\eta_{s_k+1} \notin k$.

Theorem 2.1 (Grunwald-Wang, 1933-1950)**.** *Let k be a global field, let m be a positive integer and let Σ be a set containing all but finitely many places v of k. Consider the*

group $P(m,\Sigma)$ of all $x \in k$ such that $x \in k_v^m$, for all $v \in \Sigma$. Then $P(m,\Sigma) = k^m$ except under the following conditions:

1.: *k is a number field;*

2.: *-1, $2+\eta_{s_k}$ and $-(2+\eta_{s_k})$ are non-squares in k;*

3.: *$m = 2^t m'$, where m' is odd and $t > s$;*

4.: *$v \notin \Sigma$, for all $v|2$ where $-1, 2+\eta_{s_K}$ and $-(2+\eta_{s_k})$ are non-squares in k_v.*

In this special case $P(m,\Sigma) = k^m \cup \mathfrak{a}_0 k^m$, where $\mathfrak{a}_0 = \eta_{s_k+1}^m$.

In particular, when $k = \mathbb{Q}$, the principle for q-powers of rational numbers could fail only for $q = 2^t$, with $t \geq 8$. The first example violating the principle was showed by Trost in 1934 (see [39]).

Theorem 2.2 (Trost, 1948)**.** *The equation $x^8 = 16$ has a solution in the p-adic fields $\mathbb{Q}_p$, for every $p \neq 2$, but it has no solutions in $\mathbb{Q}_2$ and in $\mathbb{Q}$.*

Similar examples can be constructed for all powers 2^t, with $t \geq 8$ and, consequently, for all integers $m = 2^t m'$, where m' is odd and $t \geq 8$, as in the statement of the theorem. Theorem 2.1 was originally proved by Grunwald in 1933, but he made a mistake, including some cases in which the answer is negative in the ones with an affirmative answer. The mistake was corrected by Wang around 1950, when he took up again Trost's example and considered some similar ones.

Denote by $\mathbb{G}_m$ the multiplicative group over k. Then the Grunwald-Wang Theorem holds in the commutative group $\mathbb{G}_m$ as well as in k. By questioning if its validity still holds for a general commutative algebraic group $\mathcal{G}$ instead of $\mathbb{G}_m$, we get nothing but Problem 1, i.e., the *Local-global divisibility problem in commutative algebraic groups*. In fact, in [18] the authors say that Problem 1 was motivated by a strong form of the Hasse principle considered for q-powers of numbers and not only for squares and in the more general setting of commumative algebraic groups instead of simply $\mathbb{G}_m$. So in the cases when the answer to Problem 1 is affirmative, we have a kind of a generalization of the Hasse Principle for squares of k-rational numbers. We postpone the description of the results achieved for Problem 1 since its formulation in Section 6, 7 and 8. Meanwhile, we describe the classical setting for Problem 2.

Let $\bar{k}$ be the algebraic closure of k and let G_k be the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$. As usual, we denote by $H^1(k,\mathcal{G})$ the group $H^1(G_k,\mathcal{G}(\bar{k}))$. Furthermore, for every G_k-module $\mathcal{G}$, we denote by $Ш(k,\mathcal{G})$ the Tate-Shafarevich group $Ш(G_k,\mathcal{G}(\bar{k}))$, defined by

$$Ш(k,\mathcal{G}) := \bigcap_{v\in M_k} \ker(H^1(k,\mathcal{G}) \xrightarrow{res_v} H^1(k_v,\mathcal{G})), \tag{2.1}$$

where res_v denotes, as usual, the restriction map. More generally, one can define $H^r(k,\mathcal{G}) := H^r(\mathcal{G}_k, A(\bar{k}))$ and

$$Ш^r(k,\mathcal{G}) := \bigcap_{v\in M_k} \ker(H^r(k,\mathcal{G}) \xrightarrow{res_v} H^r(k_v,\mathcal{G})). \tag{2.2}$$

Clearly $Ш(k,\mathcal{G}) = Ш^1(k,\mathcal{G})$. We will often use the second notation with the exponent 1, but we will keep the classical notation $Ш(k,\mathcal{G})$ too, especially when $\mathcal{G}$ is an abelian variety.

In 1962, Cassels stated the following question in the third of his famous series of papers *Arithmetic on curves of genus 1.* (see Problem (b) in [10] and Problem 1.2 in [9]; for the whole series of mentioned Cassels' papers see [7], [8], [9], [10], [11], [12]).

Problem 3 (**Cassels' question**). *Let k be a number field and $\mathcal{E}$ an abelian variety of dimension 1 defined over k. Are the elements of $Ш(k,\mathcal{E})$ infinitely divisible by a prime p when considered as elements of the Weil-Châtelet group $H^1(k,\mathcal{E})$ of all classes of homogeneous spaces for $\mathcal{E}$ defined over k?*

Here infinitely divisible by p means divisible by p^l, for all positive integer l. As mentioned above, Cassels' question is a particular case of Problem 2. In fact, it can be reformulated as follows.

Problem 3. *Let k be a number field and $\mathcal{E}$ an abelian variety of dimension 1 defined over k. Let p be a prime number. Assume that for all $v \in M_k$ there exists $\tau_v \in H^1(k_v,\mathcal{E})$, such that $p^l\tau_v = \sigma$, for every positive integer l. Can we conclude that there exists $\tau \in H^1(k,\mathcal{E})$, such that $p^l\tau = \sigma$, for all l?*

3. A cohomological interpretation of the local-global divisibility problem

As stated above, in the case when $\mathcal{G} = \mathbb{G}_m$, a solution of Problem 1 is given by the Grunwald-Wang Theorem. When $\mathcal{G} \neq \mathbb{G}_m$ an useful way to proceed was showed in [18], in which the authors give a cohomological interpretation to the problem.

For every positive integer q, we denote by $\mathcal{G}[q]$ the q-torsion subgroup of $\mathcal{G}$ and by $K := k(\mathcal{G}[q])$ the number field generated over k by the coordinates of the points in $\mathcal{G}[q]$. Since K is the splitting field of the q-division polynomials, then K/k is a Galois extension, whose Galois group we denote by G. Let $P \in \mathcal{G}[q]$ and let $D \in \mathcal{G}(\bar{k})$ be a q-divisor of P, i. e. $P = qD$. For every $\sigma \in G$, we have

$$q\sigma(D) = \sigma(qD) = \sigma(P) = P.$$

Thus $\sigma(D)$ and D differ by a point in $\mathcal{G}[q]$ and we can construct a cocycle $\{Z_\sigma\}_{\sigma \in G}$ of G with values in $\mathcal{G}[q]$ by

$$Z_\sigma := \sigma(D) - D. \tag{3.1}$$

Proposition 3.1. *The cocycle $\{Z_\sigma\}_{\sigma \in G}$ defined in* (3.1) *vanishes in $H^1(G, \mathcal{G}[q])$ if and only if there exists $D' \in A(k)$ such that $qD' = P$*

Proof. Assume that $\{Z_\sigma\}_{\sigma \in G}$ vanishes in $H^1(G, \mathcal{G}[q])$, then there exists $W \in \mathcal{G}[q]$ such that $\sigma(W) - W = Z_\sigma = \sigma(D) - D$, for all $\sigma \in G$. We have $\sigma(D - W) = D - W$, for all $\sigma \in G$. Thus $D' := D - W \in \mathcal{G}(k)$ and $qD' = qD - qW = qD = P$. The other implication is trivial. □

In particular, the triviality of $H^1(G, \mathcal{G}[q])$ assures an affirmative answer to the problem. The triviality of some first cohomology group often ensures an affirmative answer to this kind of problems. This is quite a standard way of proceeding in local-global questions, so we stated the proof of Proposition 3.1 for the reader's convenience. The goal in [18] is the introduction of a subgroup of $H^1(G, \mathcal{G}[q])$, whose vanishing still ensures an affirmative answer to Problem 1.

Definition 3.2. Let Σ a subset of M_k containing all but finitely many valuations, such that $v \notin \Sigma$, for all v ramified in K. For every $v \in \Sigma$, let $G_v := \mathrm{Gal}(\bar{k_v}/k_v)$, where w is

a place of K extending v. We call the *first local cohomology group* (of G with values in $\mathcal{G}[q]$) the following subgroup of $H^1(G, \mathcal{G}[q])$.

$$H^1_{\mathrm{loc}}(G, \mathcal{G}[q]) := \bigcap_{v \in \Sigma} (\ker H^1(G, \mathcal{G}[q]) \xrightarrow{res_v} H^1(G_v, \mathcal{G}[q])), \tag{3.2}$$

The first local cohomology group portrays the hypotheses of the problem in the cohomological context. In fact, the elements of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ are represented by cocycles that vanish in $H^1(G_v, \mathcal{G}[q])$, for all $v \in \Sigma$. We can say that they are *coboundaries locally*. By Proposition 3.1, then there exists a point $W_v \in \mathcal{G}(k_v)$ such that $Z_\sigma = (\sigma - 1)W_v$. Since Σ does not contain the valuations v that are unramified in K, then, by the Chebotarev Density Theorem, the local Galois group G_v varies over *all* cyclic subgroups of G as v varies in Σ. Since we can identify a cyclic subgroup with one of its generators, we can associate every $\sigma \in G$ with some $v \in \Sigma$, such that $G_v = \langle \sigma \rangle$. We can also denote by W_σ the q-torsion point W_v as above. Then we have the following equivalent definition of $H^1_{loc}(G, \mathcal{G}[q])$.

Definition 3.3. A cocycle $\{Z_\sigma\}_{\sigma \in G} \in H^1(G, \mathcal{G}[q])$ satisfies the *local conditions* if, for every $\sigma \in G$, there exists $A_\sigma \in \mathcal{G}[q]$ such that $Z_\sigma = (\sigma - 1)A_\sigma$. The subgroup of $H^1(G, \mathcal{G}[q])$ formed by all cocycles satisfying the local conditions is the first local cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$.

This second definition shows explicity the kind of cocycles that one has to check to see if they are coboundaries or not. Such a description is useful to get a solution to the problem both when the answer is affirmative and when it is negative. First of all we have the following result.

Theorem 3.4 (Dvornicich, Zannier, 2001)**.** *Let $G := \mathrm{Gal}(K/k)$. If $H^1_{loc}(G, \mathcal{G}[q]) = 0$, then the local-global divisibility by q holds in $\mathcal{G}$ over k.*

Furthermore, it is sometimes better to look at the p-Sylow subgroup G_p of G, since the authors also show that the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is equivalent to the triviality of $H^1_{\mathrm{loc}}(G_p, \mathcal{G}[q])$.

Proposition 3.5 (Dvornicich, Zannier, 2001)**.** *Let G_p be the p-Sylow subgroup of A. An element of $H^1_{loc}(\mathcal{A}, \mathcal{A}[p^l])$ is zero if and only if its restriction to $H^1_{loc}(G_p, \mathcal{A}[p^l])$ is zero.*

As we can see in the statement of Theorem 3.4 (and Theorem 3.5), it is crucial to know the extension K/k (instead of F/k), i. e. to know explicitly two generators of $\mathcal{G}[q]$. As we will see in next Theorem 3.6, the extension K/k is the one important in finding counterexamples too. Consequentely, the second author developed an interest in number fields generated by torsion points of elliptic curves and in families of elliptic curves with a small p-torsion, where p is a prime number and *small* is intended in terms of the degree of the extension K/k. We state some results about those number fields in Appendix A.

3.1. **How to find counterexamples**

The triviality of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ is not exactly a necessary condition for the local-global divisibility by q in $\mathcal{G}$ over k. In fact, the existence of a cocycle of G with values in $\mathcal{G}[q]$ that satisfies the local conditions and it is not a coboundary ensures the existence of a counterexample over a *finite extension* of k. Here is the precise statement, proved in [20].

Theorem 3.6 (Dvornicich, Zannier, 2007)**.** *Let $K := k(\mathcal{G}[q])$ and $G := \mathrm{Gal}(K/k)$. Let $\{Z_\sigma\}_{\sigma\in G}$ be a cocycle with values in $\mathcal{G}[q]$ representing a nontrivial element in $H^1_{loc}(G, \mathcal{G}[q])$. Then there exists a number field L such that $L \cap K = k$ and a point $P \in \mathcal{G}(L)$ which is divisible by q in $\mathcal{G}(L_w)$ for all unramified places w of L, but not divisible by q in $\mathcal{G}(L)$.*

Some evidence that the non-vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ implies the existence of a counterexample was firstly showed in [18] in the case of the algebraic tori and in [19] in the case of elliptic curves. We will describe the mentioned counterexamples in the following dedicated sections. In their third paper about the topic, the same authors describe the following general method to construct counterexamples and proved Theorem 3.6.

Assume that $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ is non-trivial and let $\{Z_\sigma\}_{\sigma\in G}$ be a cocycle satisfying the local conditions, that does not vanish in $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$. With such a Z_σ, we can obtain an equation (3.1), where the variables are the coordinates of D. When we know explicit equations for the group law of $\mathcal{G}$, as for instances in the case of elliptic curves, we get an explicit system of equations in the coordinates of D, as variables. For instance when $\mathcal{G}$ is an elliptic curve, we have a systems of two equations in two variables. In [20], the authors show that, as σ varies in G, that system defines an algebraic variety $\mathcal{B}$ that is isomorphic to $\mathcal{G}$ over K. Furthermore, they show that every k-rational point of $\mathcal{B}$, corresponds to a point $D \in \mathcal{E}(K)$, such that $P = qD$ is a k-rational point of $\mathcal{G}(k)$ violating the Hasse

principle for divisibility by q. That construction clarifies why in certain cases the non-vanishing of $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ is not a necessary condition; it depends on the existence of a k-rational point on the variety $\mathcal{B}$. In the case when $\mathcal{B}$ has no k-rational points, we are not able to find a counterexample over k. Anyway, Theorem 3.6 ensures the existence of an L-rational point in $\mathcal{B}$, where L is a finite extension of k, linearly disjoint from K over k.

Once we have a counterexample for p^l, the following statement (see [33]) gives a method to prove the existence of counterexamples to the local-global divisibility by p^{l+s}, for every $s \geq 0$.

Theorem 3.7 (Paladino, 2011)**.** *Let p be a prime number and let l, t be positive integers such that $t \leq l$. Suppose there exists a cocycle $\widehat{Z}$ of the group G with values in $\mathcal{G}[p^{l-t}]$, representing a nonzero element in $H^1_{\mathrm{loc}}(G, \mathcal{G}[p^l])$. Furthermore, suppose that there are no k-rational p^{t+1}-torsion points in $\mathcal{G}(k)$. Then, for all positive integers s, there exist number fields $L^{(s)}$ linearly disjoint from $k(\mathcal{G}[p^l])$ over k, and points $P_s \in \mathcal{G}(L^{(s)})$ such that P_s is locally divisible by p^{l+s} for almost all $v \in M_k$, but P_s is not divisible by p^{l+s} in $\mathcal{G}(L^{(s)})$.*

The proof is based on producing injective maps between some first local cohomology groups. The most suitable cases to apply Theorem 3.7 are for very small t. The best possibility is, of course, when $t = 0$. In this case $\mathcal{G}$ must have no k-rational p-torsion points. For every $\mathcal{G}$, that happens for infinitely many primes p. When $\mathcal{G}$ is an elliptic curve we have Merel's theorem (see Theorem 6.5) and we also have explicit bounds to the maximal order of a torsion point (see [30] and [37] and Subection 6.1). As a consequence of Theorem 3.7 we have the following result.

Corollary 3.8 (Paladino, 2011)**.** *For all but finitely many primes p, the existence of a counterexample to the local-global divisibility by p^l in $\mathcal{G}$ ensures the existence of a counterexample to the local-global divisibility by p^{l+s} in $\mathcal{G}$, for all positive integers s.* □

Theorem 3.7 can be useful only to show the existence of counterexamples, but it gives no methods to find explicitly some of them. Under the same assumptions, the next theorem shows how we can find numerical counterexamples. In particular, it shows how to find a sequence of points P_s, with $s \geq 0$, such that P_s violates the local-global divisibility by p^{n+s}.

Theorem 3.9 (Paladino, 2011). *Let l, t be positive integers such that $t \leq l$. Let $K_0 := k(\mathcal{A}[p^l])$. Suppose there exists a cocycle $\widehat{Z}$ of the group G with values in $\mathcal{A}[p^{l-t}]$, representing a nonzero element in $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^l])$. Suppose that there are no k-rational p^{t+1}-torsion points in $\mathcal{A}(k)$. Furthermore, suppose that there exists a point $D \in \mathcal{A}(K_0)$ of infinite order such that $\widehat{Z}(\sigma) = D^\sigma - D$ for all $\sigma \in G$. Then, for every positive integer s, the point $P_s := p^{l+s}D$ is divisible by p^{h+s} in $\mathcal{A}(k_v)$ for all valuations $v \in M_k$ unramified in K_0, but P_s is not divisible by p^{l+s} in $\mathcal{A}(k)$.*

Theorem 3.7 and Theorem 3.9 were applied successfully in the case of elliptic curves to produce counterexamples for 2^l and 3^l, with $l \geq 2$, respectively over $\mathbb{Q}$ and over $\mathbb{Q}(\zeta_3)$ (see Subsection 6.2 for further details).

4. Local-global divisibility of elements of the Tate-Shafarevich group in the Weil-Châtelet group

In this section we give some more information about Problem 2. As mentioned in the Introduction, Problem 2 was considered by Cassels in 1962, in the case of elliptic curves defined over number fields. It is clear that an answer for all powers of primes p gives an answer to all integers q. An affirmative answer to the local-global divisibility by p for elements in $H^1(k, \mathcal{E})$ was immediately given by the following Lemma proved by Tate (see Lemma 5.1 in [10]) and by Tate's duality.

Lemma 4.1 (Tate, 1962). *Let $\mathcal{A}$ be a G_k-module that is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then an element of $H^2(G_k, \mathcal{A})$ is trivial if it is everywhere locally trivial.*

Here *locally trivial everywhere* means the vanishing in $H^2(G_{k_v}, \mathcal{A}(\bar{k_v}))$, for all $v \in M_k$.

On the contrary, for powers p^l, with $l \geq 2$, the problem remained open for decades, even in the case of elliptic curves defined over $\mathbb{Q}$. An affirmative answer in this special case for all powers $p \geq 5$ has been lately proved. We will describe it in Section 6, since it is a direct consequence of some answers given to Problem 1 in elliptic curves.

In the more general case when $\mathcal{G}$ is an abelian variety $\mathcal{A}$, the problem was firstly considered by Bašmakov in [3] and [4]. Even if he stated the question for abelian varieties, in his papers he focuses especially on elliptic curves. Some more general results in the case of abelian varieties have recently been proved in [13], [14] and in [15]. In [15], Creutz

showed some counterexamples to the local-global divisibility by p of elements of the Tate-Shafarevich group $Ш(\mathbb{Q}, \mathcal{A})$ in the Weil-Châtelet group, where $\mathcal{A}$ is a Jacobian of a cyclic cover of the projective line.

Theorem 4.2 (Creutz, 2013)**.** *For every prime p, there exist infinitely many abelian varieties $\mathcal{A}$ defined over $\mathbb{Q}$, such that $Ш(\mathbb{Q}, \mathcal{A}) \not\subseteq pH^1(\mathbb{Q}, \mathcal{A})$.*

Theorem 4.2 is a consequence of the following result, reproved in [14] (see Proposition 14).

Theorem 4.3 (Creutz, 2013)**.** *Let $\mathcal{A}$ be an abelian variety defined over a number field k and let $\mathcal{A}^\vee$ its dual. Let q be a positive integer. In order to have that $Ш(k, \mathcal{A}) \subseteq qH^1(k, \mathcal{A})$ it is necessary and sufficient that the image of the natural map $Ш(k, \mathcal{A}[q]) \to Ш(k, \mathcal{A})$ is contained in the maximal divisible subgroup of $Ш(k, \mathcal{A}^\vee)$*

$$\mathrm{div}(H^1(k, \mathcal{A}^\vee) := \bigcap_{q \in \mathbb{N}} qH^1(k, \mathcal{A}^\vee).$$

What really counts in proving an affirmative answer for divisibility by q of elements of $Ш(k, \mathcal{A})$ in $H^1(k, \mathcal{A})$ is to prove the triviality of $Ш(k, \mathcal{A}^\vee[q])$. In fact, the exact sequence

$$0 \longrightarrow \mathcal{A}[q] \longrightarrow \mathcal{A} \xrightarrow{[q]} \mathcal{A} \longrightarrow 0,$$

where the map $[q]$ as usual denote the multiplication by q, implies the long-exact sequence of cohomology

$$... \longrightarrow H^r(k, \mathcal{A}[q]) \longrightarrow H^r(k, \mathcal{A}) \longrightarrow H^r(k, \mathcal{A}) \xrightarrow{\delta} H^{r+1}(k, \mathcal{A}[q]) \longrightarrow ...,$$

where δ denotes the boundary map. In [16], Creutz explicitly observes that an element $\sigma \in H^r(k, \mathcal{A})$ is locally divisible by q if and only if its image under δ is in $Ш(k, \mathcal{A}[n])$ and that it is globally divisible by q if and only if $\delta(\sigma) = 0$. Then the local-global divisibility by q holds in $H^r(k, \mathcal{A})$ if and only if $Ш^{r+1}(k, \mathcal{A}[q]) = 0$. Because of Tate's duality, one gets the following statement.

Theorem 4.4 (Creutz, 2016)**.** *Assume any of the following:*

1): *$r = 0$ and $Ш^1(k, \mathcal{A}[q]) = 0$;*

2): *$r = 1$ and $Ш^1(k, \mathcal{A}[q]^\vee) = 0$;*

3): *$r \geq 2$.*

Then the local-global divisibility by q holds in $H^r(k, \mathcal{A})$.

Theorem 4.4 has an extension to the case when k has positive characteristic, that was implemented by Creutz and Voloch in [17]. When $\mathcal{A}$ is an abelian variety principally polarized, then $\mathcal{A} \simeq \mathcal{A}^\vee$ and $Ш(k, \mathcal{A})$ is a finite group. Therefore the triviality of $Ш^1(k, \mathcal{A}[q])$ is a sufficient condition to the local-global divisibility by q in $H^r(k, \mathcal{A})$, for every $r \geq 0$.

Corollary 4.5. *Let $\mathcal{A}$ be an abelian variety principally polarized defined over a number field k. If $Ш^1(k, \mathcal{A}[q]) = 0$, for some positive integer q, then the local-global divisibility by q holds in $H^r(k, \mathcal{A})$, for every $r \geq 0$.*

In [14] the authors give some sufficient conditions to have an affirmative answer to Cassels' question in the case of an abelian variety. In fact, for a fixed prime p, they show some sufficient conditions to have $Ш(k, \mathcal{A}[p^n]) = 0$, for every $n \geq 0$.

Theorem 4.6 (Çiperiani, Stix, 2015)**.** *Let $\mathcal{A}$ be an abelian variety defined over a number field k and let p be a prime number. Then*

$$Ш(k, \mathcal{A}[p^n]) = 0, \text{ for every } n \geq 1,$$

if we assume that

1): $H^1(G, \mathcal{A}[p]) = 0$ *and*

2): *the G_k-modules $\mathcal{A}[p]$ and End$(\mathcal{A}[p])$ have no common irreducible subquotient.*

In the case of elliptic curves, an answer to Cassels' question for many primes can be deduced by the results achieved for Problem 1 in the last few years, in view of the connection between the two problems that we are going to explain better in next section. In particular, in elliptic curves defined over $\mathbb{Q}$, we have an affirmative answer for all $p \geq 5$. The mentioned results to Problem 1 for elliptic curves will be presented in Section 6 and the concequence about Problem 2 will be stated in Subsection 6.1.1.

5. First local-cohomology group and Tate-Shafarevich group

The definition of $H^1_{\text{loc}}(G, \mathcal{G}[q])$ 3.4 is very similar to the classical definition of the Tate-Shafarevich group $Ш^1(k, \mathcal{G}[q])$. We describe this relation. Firstly, we recall that as a consequence of Chevalley's Theorem on the classification of the commutative algebraic

groups in characteristic zero (see [38] and also [18, §2]), we have a group isomorphism $\mathcal{G}[q] \simeq (\mathbb{Z}/q\mathbb{Z})^n$, where n is a positive integer depending only on $\mathcal{G}$. In the case when $\mathcal{G}$ is an abelian variety of dimension g, it is well-known that $n = 2g$. Therefore we have a representation of the absolute Galois group $G_k = \mathrm{Gal}(\bar{k}/k)$ in the general linear group $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$. The image of G_k in $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$ is isomorphic to G, and we still denote by G such an image. The q-torsion subgroup $\mathcal{G}[q]$ is a G_k-module as well as a G-module. By letting v vary in the whole M_k instead of Σ and considering the G_k-module $\mathcal{G}[q]$ instead of $\mathcal{G}$ in definition 3.4, we get a subgroup of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ isomorphic to the Tate-Shafarevich group $Ш^1(k, \mathcal{G}[q])$ defined in (2.1) (in view of the cited isomorphism between G and the image of G_k in $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$). The Tate-Shafarevich group was firstly defined for abelian varieties, but later the definition has been generalized to the case of an algebraic group $\mathcal{G}$. It is then clear from the definitions (3.4) and (2.1) that the Tate-Shafarevich group $Ш(k, \mathcal{G}[q])$ is isomorphic to a subgroup of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$. In particular, the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ implies the vanishing of $Ш(k, \mathcal{G}[q])$. Thus, every affirmative answer to Problem 1, obtained by showing the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{G}[q])$, gives an affimative answer to Problem 2 for divisibility by q. On the other hand, observe the Kummer exact sequence

$$0 \to \mathcal{G}(k)/q\mathcal{G}(k) \to H^1(k, \mathcal{G}[q]) \to H^1(k, \mathcal{G})[q] \to 0.$$

If $Ш(k, \mathcal{G}[q]) = 0$, then the map $H^1(k, \mathcal{G}[q]) \to H^1(k, \mathcal{G})[q])$ is injective and $\mathcal{G}(k) \simeq q\mathcal{G}(k)$ (see also [15]). Therefore, the triviality of $Ш(k, \mathcal{G}[q])$ is a sufficient condition to get an affirmative answer to Problem 1 for local-global divisibility by q in $\mathcal{G}$ over k, as well as it is a sufficient condition to get an affirmative answer to Problem 2, for $r = 1$. In the case when $\mathcal{G}$ is an abelian variety $\mathcal{A}$ principally polarized, then the vanishing of $Ш(k, \mathcal{A}[q])$ is a sufficient condition to have an affirmative answer to both Problem 1 and Problem 2, for all $r \geq 0$, accordingly to Corollary 4.5. The two groups $Ш(k, \mathcal{A}[q])$ and $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$ often coincides and are both trivial. For instance, this is the case for p sufficiently large (see [4], [3] and [16]). Anyway, in a few cases, the two groups may differ. This happens for examples in some elliptic curves, having points locally divisible by 4 in all p-adic fields $\mathbb{Q}_p$, with $p \neq 2$, but not divisible by 4 in $\mathbb{Q}$ and in $\mathbb{Q}_2$ (see [19] and Subsection 6.2).

6. **Local-global divisibility in elliptic curves**

In this section we will be concerned with the local-global divisibility in elliptic curves. In particular, we firstly describe the affirmative answers given to Problem 1 in the last

fifteen years, then we proceed by underlining the consequences of those results to Problem 2 and we finish by showing some counterexamples to Problem 1.

6.1. **Local-global divisibility of points in elliptic curves**

In the case when $\mathcal{G}$ is an elliptic curve $\mathcal{E}$, the local-global divisibility of points has been widely studied during the last fifteen years. In fact having explicit equations satisfied by torsion points of such commutative algebraic groups was useful to describe the extension K/k and the group $H^1_{\mathrm{loc}}(G, \mathcal{E}[q])$ in various examples. The problem was considered for powers of primes p. In fact, as previously underlined, by the unique factorization in $\mathbb{Z}$ and Bézout identity, an answer for $q = p^l$, with $l \geq 1$, implies an answer for all integers q. By Tate's Lemma 4.1 and the Kummer sequence showed in the previous section, the local-global divisibility by p holds in elliptic curves defined over number fields. That result was reproved in [18] and [40] too. The most interesting case for the local-global divisibility problem, is clearly when $k = \mathbb{Q}$. In fact, many results obtained over $\mathbb{Q}$ can be extended to other number fields. In 2007 the following affirmative answer in elliptic curves defined over $\mathbb{Q}$ for various powers of primes was given in [20].

Theorem 6.1 (Dvornicich, Zannier, 2007)**.** *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic curve and let $P \in \mathcal{E}(\mathbb{Q})$ a point which is locally divisible by p^l in $\mathcal{E}(\mathbb{Q}_v)$, for all but finitely many $v \in M_{\mathbb{Q}}$, where v is a prime number and $l \geq 1$. If*

$$p \notin S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\},$$

then P is divisible by p^l in $\mathcal{E}(\mathbb{Q})$.

Theorem 6.1 is particularly interesting for its generalization to many number fields k. In fact, with mild hypotheses on k (see [34] and [35]), the same proof gives the following statement (see [20]).

Theorem 6.2. *Let p be a prime. Let $\mathcal{E}$ be an elliptic curve defined over a number field k which does not contain the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where ζ_p is a primitive pth root of the unity. If $\mathcal{E}$ does not admit any k-rational isogeny of degree p, then the local-global principle holds for divisibility by p^l in $\mathcal{E}$ over k, for every positive integer l.*

When $k = \mathbb{Q}$, Mazur's famous theorem on rational isogenies of prime degrees (see [28]) produces the set S as above. Stronger conditions have been given in [35] and [36]. We summarize the results of the main statements of those two papers in the next theorem.

Theorem 6.3 (Paladino, Ranieri, Viada, 2012-2014)**.** *Let p be a prime number. Let $\mathcal{E}$ be an elliptic curve defined over a number field k that does not contain the field $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Suppose that at least one of the following conditions holds:*

(1) *$\mathcal{E}$ has no k-rational torsion points of exact order p;*
(2) *$k(\mathcal{E}[p]) \neq k(\zeta_p)$;*
(3) *there does not exist any cyclic k-isogeny of degree p^3 between two elliptic curves defined over k that are k-isogenous to $\mathcal{E}$.*

Then, the local-global principle for divisibility by p^l holds for $\mathcal{E}$ over k and for all positive integers l.

Observe that when $k = \mathbb{Q}$, in view of Mazur's Theorem on the possible subgroups $\mathcal{E}_{tors}(\mathbb{Q})$ of rational torsion points of elliptic curves (see [28]), condition (1) implies that the local-global divisibility by p^l, with $l \geq 1$ holds for $\mathcal{E}$ over $\mathbb{Q}$ and for all $p > 7$. Furthermore, Merel proved that an equality as $\mathbb{Q}(\mathcal{E}[p]) \neq \mathbb{Q}(\zeta_p)$ implies $p \in \{2, 3, 5\}$ or $p > 1000$ (see Appendix A for further details). Then condition (2) implies that the local-global divisibility by p^l, with $l \geq 1$, holds for $\mathcal{E}$ over $\mathbb{Q}$ and for all $p > 5$. Finally, in [25] Kenku proved that condition (3) is impossible for $p = 5$, by showing that the modular curve $Y_0(125)$ has no rational points. Then Theorem 6.3 implies that the local-global divisibility by p^l, with $l \geq 1$, holds for $\mathcal{E}$ over $\mathbb{Q}$, for all $p \geq 5$.

Corollary 6.4 (Paladino, Ranieri, Viada, 2012-2014)**.** *Let $\mathcal{E}$ be an elliptic curve defined over k and let $p \geq 5$. Then local-global divisibility by p^l, with $l \geq 1$, holds in $\mathcal{E}$ over $\mathbb{Q}$.*

This result is best possible, since for powers p^l, with $p \in \{2, 3\}$ and $l \geq 2$, there are counterexamples, as we will see in next subsection.

For a general k, condition (1) is also very interesting in view of Merel's Theorem on torsion points of elliptic curves (see [29]). Here we recall its statement.

Theorem 6.5 (Merel, 1994)**.** *For every positive integer d, there exists a constant $B(d) \geq 0$ such that for all elliptic curves $\mathcal{E}$ over a number field k, with $[k : \mathbb{Q}] = d$, we have*

$$|E_{tors}(k)| \leq B(d)|.$$

Thus Theorem 6.3, combined with Theorem 6.5, implies the next interesting fact.

Corollary 6.6. *Let $\mathcal{E}$ be an elliptic curve defined over a number field k. Then there exists a constant $C([k:\mathbb{Q}])$, depending only on the degree of k over $\mathbb{Q}$, such that the local-global principle holds for divisibility by every power p^l of primes $p > C([k:\mathbb{Q}])$. In addition $C([k:\mathbb{Q}]) \leq (3^{[k:\mathbb{Q}]/2}+1)^2$.*

Remark 6.7. Observe that the statement of Corollary 6.6 holds for all k and not only for number fields that do not contain $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. In fact the number $C([k:\mathbb{Q}])$ can be chosen as the maximum $\max\{p_0, B([k:\mathbb{Q}])\}$, where p_0 is the largest prime such that k contains the field $\mathbb{Q}(\zeta_{p_0} + \overline{\zeta_{p_0}})$. In his very cited but unpublished paper [30], Oesterlé showed that Merel's constant $B([k:\mathbb{Q}])$ can be taken as $\leq (3^{[k:\mathbb{Q}]/2}+1)^2$. Since $p_0 \leq 2[k:\mathbb{Q}]+1$, then $C([k:\mathbb{Q}]) \leq (3^{[k:\mathbb{Q}]/2}+1)^2$.

The hypothesis that k does not contain the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is necessary, for all the conditions (1), (2), (3) in Theorem 6.3, as showed by an example constructed in [36, Section 6].

6.1.1. *Consequent results about Cassel's question.* As explained in Section 5, the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{E}[q])$ implies the triviality of $Ш(k, \mathcal{E}[q])$. Then, in view of Theorem 4.4, Theorem 6.3 assures an affirmative answer to Cassels' question (i.e. Problem 3) over $\mathbb{Q}$ for all prime numbers $p \geq 5$. We have also an affirmative answer to Problem 2, for all $r \geq 0$, for every $q = p^l$, with $p \geq 5$ and $l \geq 1$. Furthermore, for a general number field k, Theorem 6.3, combined with Corollary 6.6, imply an affirmative answer to Cassels' question (respectively to Problem 2, for all r) in elliptic curves over k, for every $p > (3^{[k:\mathbb{Q}]/2}+1)^2$ (resp. for all powers p^l of a prime $p > (3^{[k:\mathbb{Q}]/2}+1)^2$).

6.2. **Counterexamples**

The first paper dedicated exclusively to the local-global divisibility of points of elliptic curves is [19]. As stated above, in that article the authors construct an explicit counterexamples to the local-global divisibility by 4 in some elliptic curves over $\mathbb{Q}$. They use equation (3.1) and the method explained in Subsection 3.1. One of the counterexamples is given by the curve $y^2 = (x+15)(x-5)(x-10)$, with its rational point $P = (1561/12^2, 19459/12^3)$, that is locally divisible by 4 in $\mathbb{Q}_p$, for all $p \neq 2$, but it is not divisible by 4 in $\mathbb{Q}$ and in $\mathbb{Q}_2$. Similar counterexamples appear in [31] and in [16]. In [19]

the authors also show an example in which the local divisibility by 4 holds in all $\mathbb{Q}_p$ and the global divisibility fails, i. e. the curve $y^2 = (x + 2795)(x - 1365)(x - 1430)$ and the point $P = (5086347841/1848^2, -35496193060511/1848^3)$. In [33], by applying Theorem 3.9 it is showed that the cited counterexamples to the divisibility by 4 can be raised to counterexamples to the local-global divisibility by 2^l, for all $l \geq 2$. In particular, the point $2^{l-2}P$ gives a counterexample to the divisibility by 2^l.

The first counterexamples to the local-global divisibility by 3^l, for some $l \geq 2$, where produced in [32]. They are counterexamples to the local-global divisibility by 3^2, but the points giving the counterexamples have rational abscissas only, whereas the ordinates are not rational and are defined over $\mathbb{Q}(\zeta_3)$. In [33] again, Theorem 3.9 is used to raise those counterexamples to the local-global divisibility by 3^2 to counterexamples to the local-global divisibility by 3^l, for all $l \geq 2$ in elliptic curves over $\mathbb{Q}(\zeta_3)$. In 2016 Creutz produced the first explicit counterexamples to the local-global divisibility by 3^l, for all $l \geq 2$ in elliptic curves over $\mathbb{Q}$ (see [16]). Those examples are given by the elliptic curve $\mathcal{E} : x^3 + y^3 + 30z^3 = 0$ defined over $\mathbb{Q}$, (with distinguished point $P_0 = (1 : -1 : 0)$ and the rational point $P = (1523698559 : -2736572309 : 826803945)$. For every $n \geq 2$, the point $3^{n-1}P$ is locally divisible by 3^n in all p-adic fields $\mathbb{Q}_p$ but it is not divisible by 3^n in $\mathbb{Q}$.

Remark 6.8. The most interesting case for counterexample is when $k = \mathbb{Q}$, since a counterexample over $\mathbb{Q}$ gives also a counterexample over all but finitely many number fields k. In fact, assume that P is a point giving a counterexample to the local-global divisibility by q in $\mathcal{E}$ over k and let D be a q-divisor of P, i. e. $P = qD$. Consider the extension $F(D) = k(\mathcal{E}[q])(D)$ of k, generated by the coordinates of D and the ones of the points in $k(\mathcal{E}[q])$. Since two different q-divisors of the same point differ for a q-torsion point in $\mathcal{E}$, then L/k is a Galois extension. If L is linearly disjoint form $F(D)$ over k, then P is locally divisible by q in all but finitely many completions L_v, with $v \in M_L$ (because it is locally divisible by q in all but finitely many p-adic field $\mathbb{Q}_p$), but it is not divisible by q in L (since the coordinates of the q-divisors of P lie in $F(D)$).

Remark 6.9. All the mentioned counterexamples in particular show that Problem 2 has a negative answer for $r = 0$ in elliptic curves over $\mathbb{Q}$, when $q = p^l$, with $p \in \{2, 3\}$ and $l \geq 2$.

Remark 6.10. When the question about the local-global divisibility is restricted only to the torsion points of an elliptic curve, the set of primes for which the answer is affirmative can be enlarged to all odd primes p, as recently proved in [21]. On the contrary, for powers of 2 there are counterexamples even in this case.

7. Local-global divisibility of points in algebraic tori

The study of the local-global divisibility on the algebraic tori was initiated in [18]. In particular the authors proved the following statement.

Theorem 7.1 (Dvornicich, Zannier, 2001)**.** *Let $\mathcal{T}$ be an algebraic k-torus of dimension*

$$n \leq \max\{3, 2(p-1)\}.$$

Then the local-global divisibility by p holds in T over k.

That result was improved in [26].

Theorem 7.2 (Illengo, 2008)**.** *Let $\mathcal{T}$ be an algebraic k-torus of dimension*

$$n < 3(p-1).$$

Then the local-global divisibility by p holds in T over k.

Illengo also shows that his bound is best possible, since for all $n \geq 3(p-1)$ there are counterexamples.

Theorem 7.3 (Illengo, 2008)**.** *Let $p \neq 2$ be a prime and let $n \geq 3(p-1)$. Let $\mathbb{F}_p$ be the field with p elements. There exists a p-group G in $\mathrm{SL}_n(\mathbb{Z})$ such that the map $H^1(G, \mathbb{F}_p^n) \to \prod H^1(C, \mathbb{F}_p^n)$, where the product is taken on all cyclic subgroups C of G, is not injective.*

In [18] too, the authors produce a counterexample to the local-global divisibility by p in algebraic tori. They show that for every number field k and for every prime p there exists a torus with a point locally divisible by p over k_v, for all but finitely many $v \in M_k$, but not divisible by p over k. It is especially interesting that the counterexamples appearing in [18] to the local-global divisibility on the torus are given by torsion points.

For divisibility by powers of p^l, with $l \geq 2$, the question is open.

8. **Local-global divisibility in other commutative algebraic groups**

We have seen that the local-global divisibility by p holds when $\mathcal{G}$ is a torus isomorphic to $\mathbb{G}_m$ and when $\mathcal{G}$ is an elliptic curve. This is not true in general for other commutative algebraic groups $\mathcal{G}$ (as showed for example by the results presented in the previous section about the tori of dimension $n > 1$), and it seems to depend on the dimension of $\mathcal{G}[p]$ as a vector space over $\mathbb{F}_p$. Even for abelian varieties of dimension higher than 1 it is not true in general that the local-global divisibility by a prime p holds. In [18] the authors show some examples of p-groups Γ formed by matrices either in $\mathrm{GL}_3(p)$ or in $\mathrm{GL}_4(p)$, pointing out that if the p-Sylow subgroup of some Galois group $\mathrm{Gal}(k(\mathcal{G}[p])/k)$ is isomorphic to such a Γ, then $H^1_{\mathrm{loc}}(G_p, \mathcal{G}[p]) \neq 0$. Anyway, there are no explicit examples of commutative algebraic groups $\mathcal{G}$ over a number field k having such a p-Sylow subgroup of G, and so the situation is not completely clear yet. A recent result, not published yet, gives certain conditions on $\mathcal{G}[p]$ ensuring the validity of the local-global divisibility by p. A precise statement is the following.

Theorem 8.1 (Paladino, 2017)**.** *Let $p > 3$ be a prime number. Let k be a number field. Let $\mathcal{G}$ be a commutative algebraic group defined over k, such that $\mathcal{G}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Assume that $\mathcal{G}[p]$ is an irreducible G_k-module or a direct product of irreducible G_k-modules. Then*

- **1):** *for every $n \leq 12$, the local-global divisibility by p holds in $\mathcal{G}$ over k;*
- **2):** *for every $n > 12$, there exist a prime p_n, depending only on n, such that the local-global divisibility by p holds in $\mathcal{G}$ over k, for all $p > p_n$.*

Observe that 1) holds in particular for abelian varieties of dimension $g \leq 6$. A direct consequence of Theorem 8.1 is the following statement that can be considered as a weak generalization of Theorem 6.2 to all commutative algebraic groups for the local-global divisibility by p.

Corollary 8.2. *Let p be a prime number. Let $\mathcal{G}$ be a commutative algebraic group defined over k, such that $\mathcal{G}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. For every n, there exists a prime p_n, depending only on n, such that if $\mathcal{G}$ does not admit a k-rational isogeny of degree p^α, with $1 \leq \alpha \leq n-1$, then the local-global divisibility by p holds in $\mathcal{G}(k)$, for all $p \geq p_n$. In particular we can take $p_n = 3$, for all $n \leq 12$.*

Furthermore, we have the following result concerning Problem 2.

Corollary 8.3. *Let p be a prime number. Let $\mathcal{A}$ be an abelian variety defined over k of dimension g, principally polarized and such that $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$. For every g, there exists a prime p_g, depending only on g, such that if $p > p_g$, then $Ш(k, \mathcal{A}[p]) = 0$ and $Ш(k, \mathcal{A}) \subseteq pH^r(k, \mathcal{A})$, for all positive integers r. In particular we can take $p_g = 3$, for all $g \leq 6$.*

The proof of Theorem 8.1 in particular show all possible Galois groups G for which the local-global divisibility may fail in $\mathcal{G}$ and $Ш(k, \mathcal{G}[p])$ can be nontrivial.

When $\mathcal{G}$ is an abelian variety $\mathcal{A}$ of dimension 2, we have some more information about Problem 1, proved by Gillibert and Ranieri in [22].

Theorem 8.4 (Gillibert, Ranieri, 2017)**.** *Let $\mathcal{A}$ be a principally polarized abelian variety defined over a number field k. Let $p > 3840$ be a prime number that does not divide the degree of the polarization and such that $k \cap \mathbb{Q}(z_p) = \mathbb{Q}$. If there exists l such that $H^1_{loc}(G, \mathcal{A}[p^l]) \neq 0$, then there exists a finite extension $\tilde{k}/k$ of degree $d \leq 24$ such that $\mathcal{A}$ is $\tilde{k}$-isogenous to an abelian surface with a $\tilde{k}$-rational torsion point of order p.*

Furthermore, when Problem 1 is restricted only to the torsion points of an abelian variety $\mathcal{A}$ of GL_2-type, the same authors obtained the following result in [21].

Theorem 8.5 (Gillibert, Ranieri, 2016)**.** *Let $\mathcal{A}$ be an abelian variety of GL_2-Type defined over a number field k. Let E be a number field of degree $\dim(A)$ such that there exists an embedding $\phi : E \hookrightarrow End_k(\mathcal{A}) \otimes \mathbb{Q}$ and let $\mathcal{O}_E$ the ring of integers of E. Let $R = E \cap \phi^{-1}(End_k(\mathcal{A}) \otimes \mathbb{Z})$ and assume that p is a prime that does not divide $[\mathcal{O}_E : R]$ and that splits completely in E. Then the local-global divisibility by p^l, $l \geq 1$ holds for the torsion points of $\mathcal{A}$.*

9. Local-global divisibility in $\mathbb{G}_m \rtimes \mathcal{E}$

We consider the special case when $\mathcal{G}$ is isomorphic to a semidirect product of the multiplicative group $\mathbb{G}_m$ and an elliptic curve $\mathcal{E}$. This case was never treated in the literature before. We show a complete answer to the local-global divisibility for these particular commutative algebraic groups. We recall that by Chevalley's Theorem on the classification of the commutative algebraic groups in characteristc 0 (see for example [38] and also [18]), for every $\mathcal{G}$ there exist positive integers r, s and an abelian variety $\mathcal{B}$, such that we have an exact sequence

$$0 \longrightarrow \mathbb{G}_m^r \times \mathbb{G}_a^s \longrightarrow \mathcal{G} \longrightarrow \mathcal{B} \longrightarrow 0,$$

where $\mathbb{G}_a$ is the additive group over k.

Theorem 9.1. *Let $q = p^l$, where p is a prime number and l is a positive integer. Let $\mathcal{G}$ be a commutative algebraic group defined over k, isomorphic to the semidirect product $\mathbb{G}_m \rtimes \mathcal{E}$, where $\mathcal{E}$ is an elliptic curve. The local-global divisibility by q holds in $\mathcal{G}$ if and only if it holds both in $\mathbb{G}_m$ and in $\mathcal{E}$.*

Proof. Let $\varphi : \mathcal{E} \to \mathrm{A}ut(\mathbb{G}_m)$ and assume that $\mathbb{G} \simeq \mathbb{G}_m \rtimes_\varphi \mathcal{E}$. The group $\mathrm{Aut}(\mathbb{G}_m)$ is formed by the identity and the automorphism that maps an element g in $\mathbb{G}_m$ to g^{-1}. Let $*$ be the operation of the group $\mathbb{G}_m \rtimes_\varphi \mathcal{E}$ and let $(g_1, P_1), (g_2, P_2) \in \mathbb{G}_m \rtimes_\varphi \mathcal{E}$. Then we have two possibilities for $(g_1, P_1) * (g_2, P_2)$: if $\varphi(P_1)$ is the identity, then $(g_1, P_1) * (g_2, P_2) = (g_1 g_2, P_1 + P_2)$; if $\varphi(P_1)$ is the automorphism mapping g to g^{-1}, then $(g_1, P_1) * (g_2, P_2) = (g_1 g_2^{-1}, P_1 + P_2)$. Assume now that $Q = (g, P) \in \mathcal{G}$ is a point locally divisible by a positive integer q. For all but finitely many places v of k, we have that there exists $R_v \in \mathcal{G}(k_v)$ such that $qR_v = Q = (g, P)$. Let $R_v = (g_v, D_v)$. The condition $R_v \in \mathcal{G}(k_v)$ implies that both g_v and D_v are k_v-rational. As above, we have two possibilities for $q(g_v, D_v)$. If $\varphi(D_v)$ is the identity over $\mathbb{G}_m$, then $q(g_v, D_v) = (g_v^q, qD_v)$. In that case $g = g_v^q$ and $P = qD_v$. If the local-global divisibility by q holds both in $\mathbb{G}_m(k)$ and $\mathcal{E}(k)$, then there exist $d \in \mathbb{G}_m(k)$ and $D \in \mathcal{E}(k)$ such that $g = d^q$ and $P = qD$. We have a k-rational point (d, D) of $\mathcal{G}$ such that $q(d, D) = Q$ and an affirmative answer to the local-global divisibility in $\mathcal{G}$. Otherwise, if we have a counterexample to the local-global divisibility by q in at least one between $\mathbb{G}_m$ and $\mathcal{E}$, then we have a counterexample in $\mathcal{G}$ too. If $\varphi(D_v)$ is the automorphism of order 2 of $\mathbb{G}_m$, then it maps g_v to g_v^{-1}. If p is an odd prime, then $Q = q(g_v, D_v) = (g_v, qD_v)$. For all but finitely many $v \in M_k$, $g = g_v \in k_v$ and $P = qD_v$. If the local-global divisibility by q holds in $\mathcal{E}(k)$, then there exist $D \in \mathcal{E}(k)$ such that $P = qD$. Therefore $q(g, D) = Q$ and Q has the k-rational q-divisor (g, D). If the local-global divisibility by q does not hold in $\mathcal{E}(k)$, then we have a counterexample in $\mathcal{G}$ too. Finally, if $p = 2$, then $Q = q(g_v, D_v) = (1, qD_v)$. As in the case of odd primes, Q is divisible by q over k if and only if P is divisible by q in $\mathcal{E}(k)$. We can conclude that the local-global divisibility by q holds in $\mathcal{G}$ if and only if it holds both in $\mathbb{G}_m$ and in $\mathcal{E}$.

□

Appendix A. Number fields generated by torsion points of elliptic curves

Let $\mathcal{E}$ be an elliptic curve defined over a number field k. As above, let q denote a positive integer and p denote a prime. In this appendix we recall some results obtained about the generating sets of the field $k(\mathcal{E}[q])$ and about the families of elliptic curves defined over $\mathbb{Q}$ with a small p-torsion subgroup (small here is intended in terms of degree of the extension $\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q}$).

If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two q-torsion points of $\mathcal{E}$ forming a basis of $\mathcal{E}[q]$, then $k(\mathcal{E}[q]) = k(x_1, x_2, y_1, y_2)$. Because of Artin's primitive element theorem one knows that the extension $k(\mathcal{E}[q])/k$ is monogeneous and in principle one can find a single generator by combining the above coordinates. Anyway, in some cases to find such a generator is neither easy, nor useful for applications. On the other hand, observe that, by the properties of the Weil pairing e_q, we have that $\zeta_q := e_q(P_1, P_2) \in k(\mathcal{E}[q])$ is a primitive q-th root of the unity. In [5] and [6], the second author and Bandini underline that ζ_q could be used as an important generator of $k(\mathcal{E}[q])/k$ and they show some sets of generators contained in $\{x_1, x_2, y_1, y_2, \zeta_q\}$, that are minimal (i.e., with the smallest number of elements) for infinitely many q. First of all $k(\mathcal{E}[q]) = k(x_1, x_2, \zeta_q, y_2)$, for every q. Furthermore, for all odd q (and sometimes for even q too) that generating set could be further restricted as follows.

Theorem A.1. *Let $\mathcal{E}$ be an elliptic curve defined over a field k with $char(k) \neq 2, 3$. Let $q \geqslant 4$ a positive integer and let ζ_q a primitive qth root of the unity.*

1): *If q is an odd number, then*

$$K(\mathcal{E}[q]) = K(x_1, \zeta_q, y_2).$$

2): *If m is an even number, then either $K(\mathcal{E}[q]) = K(x_1, \zeta_q, y_2)$ or $[K(\mathcal{E}[q]) : K(x_1, \zeta_q, y_2)] = 2$ and its Galois group is generated by the element sending P_2 to $\frac{q}{2}P_1 + P_2$. In particular, if q is even then $K_{\frac{q}{2}} \subseteq K(x_1, \zeta_q, y_2)$.*

Note that **1)** holds in particular when q is an odd prime number. Such a generating set could be useful for many applications, even in analytic number theory. For example the discriminant of the field $k(\mathcal{E}[q])$ could be more easily calculated in many cases. Observe that, since the p-th division polynomial has degree $\frac{p^2-1}{2}$ and $[K(x_1, \zeta_p) : K(x_1)] \leqslant p-1$, then

$$[k(x_1, \zeta_p, y_2) : k] \leqslant \frac{p^2-1}{2} \cdot (p-1) \cdot 2p = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|.$$

By Serre's Open Image Theorem, if $\mathcal{E}$ has no complex multiplication, then $[k(x_1, \zeta_p, y_2) : k] = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$, for almost all but finitely many prime numbers p, and the generating set $\{x_1, \zeta_p, y_2\}$ of $k(\mathcal{E}[p])/k$ is minimal among those contained in $\{x_1, x_2, y_1, y_2, \zeta_p\}$. A recent bound on exceptional primes for which the Galois representation $\rho_{\mathcal{E},p}$ of G in $\mathrm{GL}_2(\mathcal{E}[p])$ is not surjective was proved for instance in [27]. When $\rho_{\mathcal{E},p}$ is not surjective the set $\{x_1, \zeta_p, y_2\}$ can be often reduced to $\{\zeta_p, y_2\}$ as a generating set for $\mathcal{E}[p]$ (see [6] for further details). In [6] there is also a classification of all possible number fields $k(\mathcal{E}[q])/k$ in terms of explicit generators, degree and Galois groups, for $q \in \{3, 4\}$ (see also [5] for an explicit classification of $\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}$).

Another interesting question that arose in this context was about the elliptic curves defined over $\mathbb{Q}$ such that $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$. Because of the mentioned property of the Weil Pairing one always has $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\mathcal{E}[p])$. In [29] Merel proved that if an equality $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$ holds, then $p \in \{2, 3, 5\}$ (or $p > 1000$). When $p = 2$ the question is trivial, since the elliptic curves with $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}$ are the curves of the family $y^3 = (x-\alpha)(x-\beta)(x-\gamma)$, with $\alpha, \beta, \gamma \in \mathbb{Q}$ and $\alpha+\beta+\gamma = 0$. When $p = 3$ the problem was solved in [32].

Theorem A.2 (Paladino, 2010)**.** *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where $b, c \in \mathbb{Q}$. Its 3-torsion subgroup $\mathcal{E}[3]$ is such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ if and only if $\mathcal{E}$ belongs to the family*

$$\mathcal{F}_{\beta,h}: \quad y^2 = x^3 + b_{\beta,h}x + c_{\beta,h} \qquad \beta, h \in \mathbb{Q} \setminus \{0\}, \tag{A.1}$$

with $b_{\beta,h} = -27\,\frac{\beta^4}{h^4} + 18\,\frac{\beta^3}{h^2} - 9\,\frac{\beta^2}{2} + 3\,\frac{\beta h^2}{2} - 3\,\frac{h^4}{16}$,

$$c_{\beta,h} = 54\,\frac{\beta^6}{h^6} - 54\,\frac{\beta^5}{h^4} + 45\,\frac{\beta^4}{2h^2} - 15\,\frac{\beta^2 h^2}{8} - 3\,\frac{\beta h^4}{8} - \frac{1}{32h^6}. \quad \square$$

When $p = 5$ the problem was lately solved in [23].

Theorem A.3 (González-Jiménez, Lozano-Robledo, 2016)**.** *The elliptic curves defined over $\mathbb{Q}$ with Weierstrass form $y^2 = x^3 + bx + c$, $b, c \in \mathbb{Q}$, having full 5-torsion over $\mathbb{Q}(\zeta_5)$ are the following elliptic curves*

1): *the elliptic curves curves parametrized by the non-cuspidal points of the modular curve $X(5)$ with Weierstrass model*

$$y^2 = x^3 - \frac{t^{20} - 228t^{15} + 494t^{10} + 228t^5 + 1}{48}x + \frac{t^{30} + 522t^{25} - 10005t^{20} - 10005t^{10} - 522t^5 + 1}{864},$$

with $t \in \mathbb{Q}$;

2): *the quadratic twists of the curves $\mathcal{E}$ in 1) except the quadratic twist $\mathcal{E}^5$;*

3): *the curves of the family*

$$y^2 = x^3 + \frac{(t^2 + 5t + 5)(t^4 + 5t^2 + 25)(t^4 + 5t^3 + 20t^2 + 25t + 25)}{4 \cdot 1728}x + q,$$

with $t \in \mathbb{Q}$ and $q \in \mathbb{Q}$ satisfying the equation of the j-invariant $j = 1728(4p^3)/(4p^3 + 27q^2)$,

where

$$p = (t^2 + 5t + 5)(t^4 + 5t^2 + 25)(t^4 + 5t^3 + 20t^2 + 25t + 25)$$

and

$$j = \frac{(t^2 + 5t + 5)^3(t^4 + 5t^2 + 25)^3(t^4 + 5t^3 + 20t^2 + 25t + 25)^3}{t^5(t^4 + 5t^3 + 15t^2 + 25t + 25)^5}.$$

Furthermore González-Jiménez and Lozano-Robledo proved that if $\mathbb{Q}(\mathcal{E}[q]) = \mathbb{Q}(\zeta_q)$, for any integer q, then $q \in \{2, 3, 4, 5\}$. They also describe in [23] the family of elliptic curves such that $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\zeta_4)$. Finally, they study some properties of the extension $\mathbb{Q}(\mathcal{E}[q])/\mathbb{Q}$ in the case when it is abelian. In particular they describe all possible abelian Galois groups $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[q])/\mathbb{Q})$ and prove the following statements.

Theorem A.4 (González-Jiménez, Lozano-Robledo, 2016)**.** *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let q be a positive integer. Assume that $\mathbb{Q}(\mathcal{E}[q])/\mathbb{Q}$ is abelian. Then $n \in \{2, 3, 4, 5, 6, 8\}$.*

Corollary A.5. *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let q be a positive integer. If $q \geq 9$, then the image of the Galois representation*

$$\rho_{\mathcal{E},q} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$$

is non-abelian.

References

[1] Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math., bf 76 (1984), 469-514.

[2] Artin E., Tate J., *Class field theory*, Benjamin, Reading, MA, 1967.

[3] Bašmakov M. I., *On the divisibility of principal homogeneous spaces over Abelian varieties*, Izv. Akad. Nauk SSSR Ser. Mat., **28** (1964), 661-664.

[4] Bašmakov M. I., *The cohomology of abelian varieties over a number field*, Russian Math. Surveys., **27** (1972) (English Translation), 25-70.

[5] Bandini A., Paladino L., *Number fields generated by the 3-torsion points of an elliptic curve.*, Monatsh. Math., **168** no. 2 (2012), 157-181.

[6] Bandini A., Paladino L., *Fields generated by torsion points of elliptic curves.*, J. Number Theory, **169** (2016), 103-133.

[7] Cassels J. W. S., *Arithmetic on curves of genus 1. I. On a conjecture of Selmer.*, J. Reine Angew. Math., **202** (1959), 52-99.

[8] Cassels J. W. S., *Arithmetic on curves of genus 1. II. A general result.*, J. Reine Angew. Math. **203** (1960), 174-208.

[9] Cassels J. W. S., *Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups.*, Proc. London Math. Soc., **12** (1962), 259-296.

[10] Cassels J. W. S., *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung.*, J. Reine Angew. Math. **211** (1962), 95-112.

[11] Cassels J. W. S., *Arithmetic on curves of genus 1. V. Two counterexamples.*, J. London Math. Soc., **38** (1963), 244-248.

[12] Cassels J. W. S., *Corrigendum: Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups.*, Proc. London Math. Soc., **13** no. 3 (1963), 768.

[13] Çiperiani M., Stix J., *Weil-Châtelet divisible elements in Tate-Shafarevich groups I: The Bašmakov problem for elliptic curves over $\mathbb{Q}$.*, Compos. Math., **149** no. 5 (2013), 729-753.

[14] Çiperiani M., Stix J., *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels.*, J. Reine Angew. Math., **700** (2015), 175-207.

[15] Creutz B., *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. London Math. Soc., **45** (2013), 935-942.

[16] Creutz B., *On the local-global principle for divisibility in the cohomology of elliptic curve*, Math. Res. Lett., **23** no. 2 (2016), 377-387.

[17] Creutz B., Voloch, *Local-global principle for Weil-Chătelet divisibility in positive characteristic*, Mathematical Proceedings of the Cambridge Philosophical Society **163** no. 2 (2017) pp. 357-367.

[18] Dvornicich R., Zannier U., *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France, **129** (2001), 317-338.

[19] Dvornicich R., Zannier U., *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.

[20] Dvornicich R., Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., no. **39** (2007), 27-34.

[21] Gillibert F., Ranieri G., *On the local-global divisibility of torsion points on elliptic curves and GL_2 -type varieties*, J. Number Theory, **174** (2017), 202âĂŞ220.

[22] Gillibert F., Ranieri G., *On the local-global divisibility over abelian varieties*, https://arxiv.org/pdf/1612.00058.pdf

[23] González-Jiménez E., Lozano-Robledo Á, *Elliptic curves with abelian division fields*, Math. Z., **283** no. 3-4 (2016), 835âĂŞ859.

[24] Harbater D., Hartmann J., Krashen D., *Local-global principle for torsors over arithmetic curves*, American Journal of Mathematics, to appear.

[25] Kenku M. A., *On the modular curves $X_0(125), X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** no. 3 (1981), 415-427.

[26] Illengo M., *Cohomology of integer matrices and local-global divisibility on the torus*, Le Journal de Théorie des Nombres de Bordeaux, no. **20** (2008), 327-334.

[27] E. Larson and D. Vaintrob, On the surjectivity of Galois representations associated to elliptic curves over number fields, *Bull. Lond. Math. Soc.* **46**, no. 1 (2014), 197–209.

[28] Mazur B., *Rational isogenies of prime degree (with an appendix of D. Goldfeld)*, Invent. Math., **44** (1978), 129-162.

[29] Merel L., *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437-449.
[30] Oesterlé J., *Torsion des courbes elliptiques sur les corps de nombres*, preprint.
[31] Paladino L., *Local-global divisibility by 4 in elliptic curves defined over* $\mathbb{Q}$, Annali di Matematica Pura e Applicata, no. **189.1**, (2010), 17-23.
[32] Paladino L., *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by 9*, Le Journal de Théorie des Nombres de Bordeaux, Vol. **22** no. 1 (2010), 138-160.
[33] Paladino L., *On counterexamples to local-global divisibility in commutative algebraic groups*, Acta Arithmetica, **148** no. 1, (2011), 21-29.
[34] Paladino L., Ranieri G., Viada E., *Local-global divisibility by* p^2 *in elliptic curves*, Preprint, 2011, arXiv:1103.4963.
[35] Paladino L., Ranieri G., Viada E., *On Local-Global Divisibility by* p^n *in elliptic curves*, Bulletin of the London Mathematical Society, **44** no. 5 (2012), 789-802.
[36] Paladino L., Ranieri G., Viada E., *On minimal set for counterexamples to the local-global principle*, Journal of Algebra, **415** (2014), 290-304.
[37] Parent P., *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. (French) [Effective bounds for the torsion of elliptic curves over number fields]*, J. Reine Angew. Math., **506** (1999), 85-116.
[38] Serre J-P., *Algebraic groups and class fields*, Springer-Verlag, Heidelberg, 1988.
[39] Trost E., *Zur theorie des Potenzreste*, Nieuw Archief voor Wiskunde, no. **18** (2) (1948), 58-61.
[40] Wong S., *Power residues on abelian variety*, Manuscripta Math., no. **102** (2000), 129-137.

Roberto Dvornicich

Università di Pisa

Dipartimento di Matematica

Largo Bruno Pontecorvo, 5

56126 Pisa

Italy

e-mail address: roberto.dvornicoch@unipi.it

Laura Paladino

Università della Calabria

Dipartimento di Matematica e Informatica

Ponte Pietro Bucci, Cubo 30B

87036 Arcavacata di Rende (CS)

Italy

e-mail address: paladino@mat.unical.it