ACTA ARITHMETICA
148.1 (2011)

On counterexamples to local-global divisibility in commutative algebraic groups

by

Laura Paladino (Pisa)

1. Introduction. Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. Let $P \in \mathcal{A}(k)$. We denote by M_k the set of the valuations $v \in k$ and by k_v the completion of k at the valuation v. In previous papers we were concerned with the following question:

Problem. Assume that for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$, where q is a positive integer. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?

This problem is known as *Local-Global Divisibility Problem*. There are known solutions in many cases, but many cases remain open too. By using the Bézout identity, it turns out that it is sufficient to solve it in the case when q is a power p^n of a prime p, to get answers for a general integer q.

The local-global divisibility problem is motivated by a strong form of the Hasse principle that says: *If a quadratic form* $ax^2 + bxy + cy^2 \in \mathbb{Q}[x, y]$ *of rank* 2 *represents* 0 *non-trivially over all but finitely many completions* $\mathbb{Q}_p$*, then it represents* 0 *non-trivially over* $\mathbb{Q}$. Then, in particular, if a rational number is a perfect square modulo all but finitely many primes p, then it is a rational square. A generalization of this fact for q-powers of k-rational numbers is the Local-Global Divisibility Problem in the case when $\mathcal{A}$ is the multiplicative group $\mathbb{G}_m$. For this algebraic group a solution is classical. The answer is affirmative for all odd prime powers q and for $q \mid 4$ (see [AT, Chap. IX, Thm. I]). On the other hand, there are counterexamples for $q = 2^t$, $t \geq 3$. The most famous of them was discovered by Trost (see [Tro]) and it is the diophantine equation $x^8 = 16$, that has a solution in $\mathbb{Q}_p$ for all primes $p \in \mathbb{Q}$ different from 2, but has no solutions in $\mathbb{Q}_2$ and in $\mathbb{Q}$.

2010 *Mathematics Subject Classification*: Primary 14H52; Secondary 11S25.
Key words and phrases: commutative algebraic groups, local-global divisibility problem, elliptic curves.

DOI: 10.4064/aa148-1-2

When $\mathcal{A} \neq \mathbb{G}_m$ a classical way to proceed is to give a cohomological interpretation to the problem. It turns out that the answer is strictly connected to the behavior of two cohomology groups. The first of them is the cohomology group $H^1(\mathrm{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n])$, where $\mathcal{A}[p^n]$ denotes the p^n-torsion subgroup of $\mathcal{A}$. The second is one of its subgroups, named $H^1_{\mathrm{loc}}(\mathrm{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n])$, that interprets the hypothesis of the problem in the cohomological context. This last group is known as the *first local cohomology group* and was defined by R. Dvornicich and U. Zannier (see [DZ1]).

Definition. Let Σ be a group and let M be a Σ-module. We say that a cocycle $[c] = [\{Z_\sigma\}] \in H^1(\Sigma, M)$ satisfies the *local conditions* if there exists $W_\sigma \in M$ such that $Z_\sigma = (\sigma - 1)W_\sigma$ for all $\sigma \in \Sigma$. We denote by $H^1_{\mathrm{loc}}(\Sigma, M)$ the subgroup of $H^1(\Sigma, M)$ formed by such cocycles.

Working with all valuations, instead of almost all, we would get the classical definition of the Shafarevich group. Modified Shafarevich groups similar to $H^1_{\mathrm{loc}}(\Sigma, M)$ appear in [San].

In 2001 R. Dvornicich and U. Zannier proved the following result (see [DZ1]).

Theorem 1.1 (Dvornicich, Zannier, 2001). *Assume that*

$$H^1_{\mathrm{loc}}(\mathrm{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n]) = 0.$$

Let $P \in \mathcal{A}(k)$ be a point locally divisible by p^n almost everywhere in the completions k_v of k. Then there exists a point $D \in \mathcal{A}(k)$ such that $P = p^n D$.

Therefore, a natural question was if the non-vanishing of the group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ could imply the existence of a counterexample to the problem. In 2007 they proved the following statement (see [DZ3]).

Theorem 1.2 (Dvornicich, Zannier, 2007). *Let $K_0 := k(\mathcal{A}[p^n])$ and let $G := \mathrm{Gal}(k(\mathcal{A}[p^n])/k)$. Let $\{Z_\sigma\}_{\sigma \in G}$ be a cocycle of G representing a non-trivial element in $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$. Then there exists a number field L such that $L \cap K_0 = k$ and a point $P \in \mathcal{A}(L)$ which is divisible by p^n in $\mathcal{A}(L_w)$ for all unramified places w of L but is not divisible by p^n in $\mathcal{A}(L)$.*

It is possible to find a suitable field L and a suitable point P by proceeding in the following way. Consider the restriction of scalars $\mathcal{H} := R^K_k(\mathcal{A})$ of $\mathcal{A}$ from K to k. It is well known that $\mathcal{H}$ is isomorphic over K to the product $\mathcal{H}_K := \prod_{\sigma \in G} \mathcal{A}^\sigma$ (see [Ser]), where $\mathcal{A}^\sigma$ is now simply $\mathcal{A}$, but viewed over K. Consider the points $D \in \mathcal{A}$ satisfying

$$D^\sigma - D = Z_\sigma.$$

The map $D \mapsto D^\sigma := D + Z_\sigma$ is a K-isomorphism between $\mathcal{A}$ and a subvariety $\mathcal{B}$ of $\mathcal{H}$ (see [DZ3, Proof of Prop. 1]). Clearly $\mathcal{B}$ depends on Z. Every L-rational point $\{D^\sigma\}_{\sigma \in G}$ over $\mathcal{B}$ corresponds to a point $D \in \mathcal{A}(LK)$. The

point $P := p^n D$ is an L-rational point of $\mathcal{A}$, locally divisible by p^n for all primes of L unramified in LK, but not globally (see [DZ3, Prop. 1 and proof of Thm. 3]).

In this paper, we will prove two generalizations of Theorem 1.2 (see Theorem 2.1 and Theorem 3.1).

Later, R. Dvornicich and U. Zannier investigated particularly the case when $\mathcal{A}$ is an elliptic curve. They proved that for these algebraic groups we have an affirmative answer to the problem when q is a prime (see [DZ1] and [Won]), and when q is a power of a prime and

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

(see [DZ3, Thm. 1]). An interesting open question is if there exists a counterexample for $q = p^n$, for all $p \in S$ and $n > 1$. There are known counterexamples only to the local-global divisibility by 4 (see [DZ2] and [Pal1]) and by 9 (see [Pal1]). In this paper we will prove the existence of counterexamples to the local-global divisibility by 2^n (see [DZ2] and [Pal1]) and by 3^n, for every $n \geq 2$.

2. On counterexamples to local-global divisibility. We will prove that for almost all primes $p \in \mathbb{N}$ the existence of a counterexample to the local-global divisibility by p^n in $\mathcal{A}$ ensures the existence of a counterexample to the local-global divisibility by p^{n+s} in $\mathcal{A}$ for all positive integers s. The following theorem shows that in many cases the hypotheses of Theorem 1.2 are sufficient to prove that conclusion. As in the statement of Theorem 1.2 let $K_0 := k(\mathcal{A}[p^n])$ and $G := \mathrm{Gal}(k(\mathcal{A}[p^n])/k)$.

THEOREM 2.1. *Let n, t be positive integers such that $t \leq n$. Suppose there exists a cocycle $\widehat{Z}$ of the group G with values in $\mathcal{A}[p^{n-t}]$, representing a nonzero element in $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$. Furthermore, suppose there are no k-rational p^{t+1}-torsion points in $\mathcal{A}(k)$. Then, for all positive integers s, there exist number fields $L^{(s)}$ linearly disjoint from K_0 over k, and points $P_s \in \mathcal{A}(L^{(s)})$ such that P_s is locally divisible by p^{n+s} for almost all $v \in M_k$, but P_s is not divisible by p^{n+s} in $\mathcal{A}(L^{(s)})$.*

Proof. By [DZ3, Thm. 3] we have the conclusion when $s = 0$. Now, suppose $s \geq 1$. Let $K_s := k(\mathcal{A}[p^{n+s}])$, let G_s be the Galois group $\mathrm{Gal}(K_s/k)$ and let H_s be the Galois group $\mathrm{Gal}(K_s/K_0)$. We have $G \cong G_s/H_s$. We consider the map

$$\alpha : H^1(G, \mathcal{A}[p^n]) \to H^1(G_s, \mathcal{A}[p^{n+s}])$$

defined by

$$(\alpha(Z))(\sigma) := Z(\sigma H_s) \quad \text{for all } \sigma \in G_s.$$

We will prove that α is a homomorphism and that its restriction to the first cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ induces a homomorphism

$$\alpha : H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n]) \to H^1_{\mathrm{loc}}(G_s, \mathcal{A}[p^{n+s}])$$

that is injective on the elements in $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ represented by cocycles with values in $\mathcal{A}[p^{n-t}]$. Let $Z \in H^1(G, \mathcal{A}[p^n])$ and let $\sigma, \tau \in G_s$. We have

$$(\alpha(Z))(\sigma\tau) = Z(\sigma\tau H_s) = Z(\sigma H_s \tau H_s) = Z(\sigma H_s) + \sigma(Z(\tau H_s)).$$

Since $Z(\tau H_s) \in \mathcal{A}[p^n]$, it is fixed by H_s. Thus

$$Z(\sigma H_s) + \sigma(Z(\tau H_s)) = (\alpha(Z))(\sigma) + \sigma((\alpha(Z))(\tau))$$

and $\alpha(Z)$ is a cocycle.

We will show that the image of a coboundary under α is again a coboundary. Let $Z \in H^1(G, \mathcal{A}[p^n])$ be such that $Z(\sigma) = (\sigma - 1)A$ with $A \in \mathcal{A}[p^n]$. Therefore

$$(\alpha(Z))(\sigma) = Z(\sigma H_s) = (\sigma H_s - H_s)A = (\sigma - 1)A.$$

Since H_s fixes $\mathcal{A}[p^n]$, we have $(\alpha(Z))(\sigma) = (\sigma - 1)A$, with $A \in \mathcal{A}[p^n] \leq \mathcal{A}[p^{n+s}]$. Therefore α is well defined. It is clearly a homomorphism.

Remark. Let $\mathcal{A}[p^{n+s}]^{H_s}$ be the set of p^{n+s}-torsion points of $\mathcal{A}$ fixed by H_s. When $\mathcal{A}[p^{n+s}]^{H_s} = \mathcal{A}[p^n]$, then α is the *inflation* and it is injective.

Now, we are going to prove that $\alpha(H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])) \subseteq H^1_{\mathrm{loc}}(G_s, \mathcal{A}[p^{n+s}])$. Let $Z \in H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$. Then, for all $\sigma \in G$, we have

$$Z(\sigma) = (\sigma - 1)A_\sigma \quad \text{with } A_\sigma \in \mathcal{A}[p^n].$$

Let $\sigma \in G_s$. Therefore

$$(\alpha(Z))(\sigma) = Z(\sigma H_s) = (\sigma H_s - H_s)A_\sigma = (\sigma - 1)A_\sigma.$$

Since $A_\sigma \in \mathcal{A}[p^n] \leq \mathcal{A}[p^{n+s}]$, we can conclude $\alpha(Z) \in H^1_{\mathrm{loc}}(G, \mathcal{A}[p^{n+s}])$. Furthermore, we observe that if $h \in H_s$, then $(\alpha(Z))(h) = O$, where O is the zero point in $\mathcal{A}$.

Remark. We have already noticed that if $\mathcal{A}[p^{n+s}]^{H_s} = \mathcal{A}[p^n]$, then α is injective. In this case, by using [DZ3, Thm. 3], we immediately get the conclusion.

Now, let $\widetilde{Z}$ be a cocycle with values in $\mathcal{A}[p^{n-t}]$, representing an element in $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$. Suppose that $\alpha(\widetilde{Z})$ is a coboundary. Therefore, for all $\sigma \in G_s$ we have

$$\widetilde{Z}(\sigma H_s) = (\alpha(\widetilde{Z}))(\sigma) = (\sigma - 1)\widetilde{A} \quad \text{with } \widetilde{A} \in \mathcal{A}[p^{n+s}].$$

We are assuming $\widetilde{Z}(\sigma H_s) \in \mathcal{A}[p^{n-t}]$, thus

$$0 = p^{n-t}\widetilde{Z}(\sigma H_s) = p^{n-t}((\sigma - 1)\widetilde{A}) = p^{n-t}\sigma(\widetilde{A}) - p^{n-t}\widetilde{A} = \sigma(p^{n-t}\widetilde{A}) - p^{n-t}\widetilde{A}.$$

Therefore $p^{n-t}\widetilde{A} \in \mathcal{A}(k)$. Since $\widetilde{A}$ is a p^{n+s}-torsion point, we have $p^{n-t}\widetilde{A} \in \mathcal{A}[p^{s+t}]$. By hypothesis there are no k-rational p^{t+1}-torsion points, which implies there are no k-rational p^{t+s}-torsion points for every $s \geq 1$. So $p^{n-t}\widetilde{A} \in \mathcal{A}[p^t]$, yielding $\widetilde{A} \in \mathcal{A}[p^n]$. It follows that $\widetilde{Z}$ is a coboundary. Thus, the restriction of α to $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ is injective on the cocycles with values in $\mathcal{A}[p^{n-t}]$. Let $\widehat{Z}$ be as in the statement of the theorem. Then $\alpha(\widehat{Z})$ is a nonzero element in $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^{n+s}])$. By applying [DZ3, Thm. 3], we have the conclusion. ∎

Clearly, the best cases to apply Theorem 2.1 are when t is very small. The most suitable possibility is when $t = 0$. In this case, the algebraic group $\mathcal{A}$ must have no k-rational p-torsion points. In fact, for every $\mathcal{A}$, this happens for infinitely many primes p. When $\mathcal{A}$ is an elliptic curve and $k = \mathbb{Q}$, the famous Mazur's Theorem ensures that there are no rational torsion points of order $p \geq 11$. For completeness, we recall the statement of this theorem.

THEOREM 2.2 (Mazur). *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$. Then its subgroup $\mathcal{E}_{\mathrm{tors}}$, formed by the rational torsion points of $\mathcal{E}$, is isomorphic to one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z} && \text{for } m = 1, 2, 3, \ldots, 10, 12, \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} && \text{for } m = 2, 4, 6, 8. \end{aligned}$$

Now, we consider the more general case when $\mathcal{A}$ is a commutative algebraic group defined over a number field k. For every integer m, the m-torsion subgroup of $\mathcal{A}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{n_{\mathcal{A}}}$ for a certain integer $n_{\mathcal{A}}$, depending only on $\mathcal{A}$ (see for instance [DZ1, §2]). Therefore, if $\mathcal{A}$ is a linear algebraic group, we can deduce from [Jar, Thm. B] that the torsion part of $\mathcal{A}$ over k is finite. If $\mathcal{A}$ is an abelian variety, we can use the Mordell–Weil Theorem (see [Wei, VIII, Thm. 6.7]) to get the same conclusion. Thus, the torsion part of a commutative algebraic group over a number field k is finite (see for instance [Sha, III, §4, Thm. C]).

Then, for every $\mathcal{A}$, there exists a prime $p_{\mathcal{A},k}$, depending on $\mathcal{A}$ and k, such that for all primes $p \geq p_{\mathcal{A},k}$, we can choose $t = 0$ to apply Theorem 2.1. When $k = \mathbb{Q}$, we will denote $p_{\mathcal{A},k}$ simply by $p_{\mathcal{A}}$. For every elliptic curve $\mathcal{E}$, we have already observed that $p_{\mathcal{E}} \leq 11$.

By Theorem 1.1, the existence of a counterexample to the local-global divisibility by p^n in $\mathcal{A}(k)$ is a sufficient condition to the non-vanishing of the group $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$. Therefore, in particular we have proved the following statement.

THEOREM 2.3. *For all but finitely many primes $p \in \mathbb{N}$, the existence of a counterexample to the local-global divisibility by p^n in $\mathcal{A}$ ensures the existence of a counterexample to the local-global divisibility by p^{n+s} in $\mathcal{A}$ for all positive integers s.* ∎

The case of elliptic curves when $p \in \{2,3\}$. In [DZ2], [Pal1] and [Pal2] there are counterexamples to the local-global divisibility by 4 and by 9 in elliptic curves defined over $\mathbb{Q}$. We will use Theorem 2.1 to get the existence of counterexamples to the local-global divisibility by 2^n and 3^n, for all $n \geq 2$. We have the following result:

COROLLARY 2.4. *For every integer $n \geq 2$, there exist counterexamples to the local-global divisibility by 2^n and 3^n in elliptic curves.*

Proof. In [DZ2] and [Pal1] there are given elliptic curves such that $H^1_{\mathrm{loc}}(\mathrm{Gal}(\mathcal{E}[4]/\mathbb{Q}), \mathcal{E}[4]) \neq 0$, and [Pal2] features elliptic curves such that $H^1_{\mathrm{loc}}(\mathrm{Gal}(\mathcal{E}[9]/\mathbb{Q}), \mathcal{E}[9]) \neq 0$. Since those curves have a rational point of order respectively 2 or 3, we cannot apply Theorem 2.1 with $t = 0$. But in the same numerical examples, the cocycles representing non-zero elements in the first local cohomology group have values in $\mathcal{E}[p]$, where p is respectively 2 or 3. Therefore, we may try to apply Theorem 2.1 with $t = 1$. We only have to prove that the relevant elliptic curves have no rational p^2-torsion points. One can verify that by calculating the rational points of finite order of those curves by using the software PARI. The command is elltors($\mathcal{E}$). ∎

Some remarks about the first local cohomology groups. In the proof of Theorem 2.1 we have shown that for commutative algebraic groups $\mathcal{A}(k)$ with no k-rational torsion points of order p, there is an injective map α between $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ and $H^1_{\mathrm{loc}}(G_s, \mathcal{A}[p^{n+s}])$ for every positive integer s. In particular, there is an injective map from $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ to $H^1_{\mathrm{loc}}(G_1, \mathcal{A}[p^{n+1}])$. Therefore, the first local cohomology groups form an increasing sequence

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n]) \leq H^1_{\mathrm{loc}}(G_1, \mathcal{A}[p^{n+1}]) \leq \cdots \leq H^1_{\mathrm{loc}}(G_s, \mathcal{A}[p^{n+s}]) \leq \cdots$$

when n varies in $\mathbb{N}$.

Now, we are going to prove that there also exists an injective map φ from $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n])$ to $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^{n+1}]^{H_1})$. Then the first local cohomology groups $H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n]^{H_s})$ also form an increasing sequence

$$H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n]) \leq H^1_{\mathrm{loc}}(G, \mathcal{A}[p^{n+1}]^{H_1}) \leq \cdots \leq H^1_{\mathrm{loc}}(G, \mathcal{A}[p^{n+s}]^{H_s}) \leq \cdots$$

when n varies in $\mathbb{N}$.

PROPOSITION 2.5. *Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. Let p be a prime and suppose there are no k-rational torsion points of order p in $\mathcal{A}$. Then there exists an injective map $\varphi : H^1_{\mathrm{loc}}(G, \mathcal{A}[p^n]) \to H^1_{\mathrm{loc}}(G, \mathcal{A}[p^{n+1}]^{H_1})$ such that the following diagram commutes:*

$$\begin{array}{ccc} H^1_{\mathrm{loc}}(G,\mathcal{A}[p^n]) & \xrightarrow{\alpha} & H^1_{\mathrm{loc}}(G_1,\mathcal{A}[p^{n+1}]) \\ & \searrow^{\varphi} & \uparrow{\scriptstyle \iota} \\ & & H^1_{\mathrm{loc}}(G,\mathcal{A}[p^{n+1}]^{H_1}) \end{array}$$

where ι is the restriction of the inflation map to $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^{n+1}]^{H_1})$.

Proof. Let α be the homomorphism defined in Theorem 2.1. Define

$$\varphi : H^1_{\mathrm{loc}}(G,\mathcal{A}[p^n]) \to H^1_{\mathrm{loc}}(G,\mathcal{A}[p^{n+1}]^{H_1})$$

by $(\varphi(Z))(\sigma) := Z(\sigma)$ for all $\sigma \in G$. Clearly φ is a well defined homomorphism. Now, we show that the preimage of a coboundary is a coboundary. Suppose $(\varphi(Z))(\sigma) = (\sigma-1)\widetilde{A}$ with $\widetilde{A} \in \mathcal{A}[p^{n+1}]^{H_1}$ for all $\sigma \in G$. Therefore, by definition, $Z(\sigma) = (\sigma-1)\widetilde{A}$. Since $Z \in H^1_{\mathrm{loc}}(G,\mathcal{A}[p^n])$, we have $Z(\sigma) = (\sigma-1)A_\sigma$ with $A_\sigma \in \mathcal{A}[p^n]$ for all $\sigma \in G$. We get

$$(\sigma-1)A_\sigma = (\sigma-1)\widetilde{A} \quad \text{for all } \sigma \in G.$$

Thus $\sigma(\widetilde{A}-A_\sigma) = \widetilde{A}-A_\sigma$. Hence we have $p^n(\sigma(\widetilde{A}-A_\sigma)) = p^n(\widetilde{A}-A_\sigma)$, i.e. $\sigma(p^n\widetilde{A}-p^nA_\sigma) = p^n\widetilde{A}-p^nA_\sigma$. Since A_σ is a point of order p^n, we obtain

$$\sigma(p^n\widetilde{A}) = p^n\widetilde{A} \quad \text{for all } \sigma \in G.$$

We are assuming $\widetilde{A} \in \mathcal{A}[p^{n+1}]^{H_1}$. If $\widetilde{A}$ has order p^{n+1}, then $p^n\widetilde{A}$ has order p and we have a contradiction with the hypothesis that $\mathcal{A}$ has no k-rational points of order p. Therefore $\widetilde{A} \in \mathcal{A}[p^n]$ and φ is injective. Now, we consider the map

$$\iota : H^1_{\mathrm{loc}}(G,\mathcal{A}[p^{n+1}]^{H_1}) \to H^1_{\mathrm{loc}}(G_1,\mathcal{A}[p^{n+1}]),$$

defined by $(\iota(Z))(\sigma) := Z(\sigma H_1)$, which is simply the restriction of the *inflation* to $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^{n+1}]^{H_1})$. Clearly, $\varphi \circ \iota = \alpha$. ∎

3. Numerical examples. As we have seen, we can use Theorem 2.1 to prove the existence of counterexamples to the local-global divisibility in many cases. But Theorem 2.1 gives no method to find numerical examples. Under the same assumptions, the next theorem shows how we can find a sequence of points P_s violating the local-global divisibility by p^{n+s} for every $s \in \mathbb{N}$.

THEOREM 3.1. *Let n, t be positive integers such that $t \le n$. Suppose there exists a cocycle $\widehat{Z}$ of the group G with values in $\mathcal{A}[p^{n-t}]$, representing a nonzero element in $H^1_{\mathrm{loc}}(G,\mathcal{A}[p^n])$. Suppose there are no k-rational p^{t+1}-torsion points in $\mathcal{A}(k)$. Furthermore, suppose 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 $P_s := p^{n+s}D$ is divisible by p^{n+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^{n+s} in $\mathcal{A}(k)$.*

Proof. Let $v \in M_k$ be unramified in K_0. By [DZ3, Thm. 3 and its proof], the point $P_0 := p^n D$ is divisible by p^n in $\mathcal{A}(k_v)$. Therefore, there exists a point $D_v \in \mathcal{A}(k_v)$ such that $P_0 = p^n D_v$. Let $P_s := p^{n+s} D$. We have

$$P_s = p^{n+s} D = p^s P_0 = p^{n+s} D_v.$$

Thus P_s is divisible by p^{n+s} in $\mathcal{A}(k_v)$ for all valuations $v \in M_k$ unramified in K_0. Now, we will prove that P_s is not divisible by p^{n+s} over k. Suppose there exists $D_* \in \mathcal{A}(k)$ such that $P_s = p^{n+s} D_*$. Then $D = D_* + T$ with $T \in \mathcal{A}[p^{n+s}]$. Let α be the homomorphism defined in the proof of Theorem 2.1. We have shown that $\alpha(\widehat{Z})$ is a nonzero element in $H^1_{\mathrm{loc}}(G_s, \mathcal{A}[p^{n+s}])$. Suppose $\sigma \in G_s$. Then

$$(\alpha(Z))(\sigma) = Z(\sigma H_s) = D^\sigma - D.$$

The last equality follows because $D \in \mathcal{A}(K_0)$, then it is fixed by H_s, for every positive integer s. In fact, if $h \in H_s$, we have $\overline{0} = (\alpha(\widehat{Z}))(h) = Z(H_s) = D - D$, as required. Thus, for all $\sigma \in G_s$, we have

$$(\alpha(Z))(\sigma) = D^\sigma - D = (D_* + T)^\sigma - (D_* + T) = D_*^\sigma - D_* + T^\sigma - T = T^\sigma - T.$$

Since $\alpha(\widehat{Z})$ is a nonzero element in $H^1_{\mathrm{loc}}(G_s, \mathcal{A}[p^{n+s}])$, there is a contradiction. We conclude that P_s is not divisible by p^{n+s} over k. ∎

Numerical examples for 2^n. The numerical examples that appear in [DZ2] and [Pal1] satisfy every assumption of Theorem 3.1, except the infinite order of the point D, which we have to prove. It suffices to prove that the point $P = 4D$ has infinite order. Since $P \in \mathcal{E}(\mathbb{Q})$ and its coordinates are not integers, by the Nagell–Lutz theorem it has infinite order. Therefore, for every integer $n \geq 2$, the point $2^{n-2}P = 2^n D$ gives a numerical counterexample to the local-global divisibility by 2^n over $\mathbb{Q}$.

For completeness, we recall the cited numerical examples that appear respectively in [DZ2] and [Pal1]:

$$\mathcal{E}: \quad y^2 = x(x+15)(x-5)(x+10),$$

$$D = (7 + 4\sqrt{-1}, -4 + 22\sqrt{-1}), \qquad P = 4D = \left(\frac{1561}{12^2}, -\frac{19459}{13^3}\right),$$

and

$$\mathcal{E}: \quad y^2 = x(x+93)(x-31)(x-62) = x^3 - 6727x + 178746,$$

$$D = \left(-\frac{403}{2} - \frac{31}{2}\sqrt{-31}, 1922 - 434\sqrt{-31}\right),$$

$$P = 4D = \left(\frac{5006244481}{16646400}, -\frac{341996266999871}{67917312000}\right).$$

By using PARI one can calculate $2^{n-2}P = 2^n D$ for every $n \geq 2$. The command is ellpow$(\mathcal{E}, P, 2^{n-2})$.

Acknowledgements. I would like to thank R. Dvornicich and the referee for their precious remarks about this paper.

References

[AT] E. Artin and J. Tate, *Class Field Theory*, Benjamin, Reading, MA, 1967.

[DZ1] R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France 129 (2001), 317–338.

[DZ2] —, —, *An analogue for elliptic curves of the Grunwald–Wang example*, C. R. Math. Acad. Sci. Paris 338 (2004), 47–50.

[DZ3] —, —, *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. London Math. Soc. 39 (2007), 27–34.

[Jar] M. Jarden, *Torsion in linear algebraic groups over large algebraic fields*, Arch. Math. (Basel) 32 (1979), 445–451.

[Pal1] L. Paladino, *Local-global divisibility by 4 in elliptic curves defined over* $\mathbb{Q}$, Ann. Mat. Pura Appl. 189 (2010), 17–23.

[Pal2] —, *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by 9*, J. Théor. Nombres Bordeaux 22 (2010), 139–160.

[San] J.-J. Sansuc, *Groupe de Brauer et arithméthique des groupes linéaires sur un corps de nombres*, J. Reine Angew. Math. 327 (1981), 12–80.

[Ser] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[Sha] I. R. Shafarevich, *Basic Algebraic Geometry 1*, 2nd ed., Springer, Berlin, 1994.

[Tro] E. Trost, *Zur Theorie des Potenzreste*, Nieuw Arch. Wiskunde 18 (1948), 58–61.

[Wei] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. 52 (1929), 281–315.

[Won] S. Wong, *Power residues on abelian variety*, Manuscripta Math. 102 (2000), 129–137.

Laura Paladino
Department of Mathematics
University of Pisa
Largo Bruno Pontecorvo 5
56127 Pisa, Italy
E-mail: paladino@mail.dm.unipi.it

Received on 17.6.2009
and in revised form on 27.6.2010 (6062)