Annali di Matematica (2018) 197:1215–1225
https://doi.org/10.1007/s10231-017-0721-9

Counterexamples to the local–global divisibility over elliptic curves

Gabriele Ranieri[1]

Received: 3 May 2017 / Accepted: 6 December 2017 / Published online: 12 December 2017

Abstract Let $p \geq 5$ be a prime number. We find all the possible subgroups G of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ such that there exist a number field k and an elliptic curve $\mathcal{E}$ defined over k such that the $\mathrm{Gal}(k(\mathcal{E}[p])/k)$-module $\mathcal{E}[p]$ is isomorphic to the G-module $(\mathbb{Z}/p\mathbb{Z})^2$ and there exists $n \in \mathbb{N}$ such that the local–global divisibility by p^n does not hold over $\mathcal{E}(k)$.

Keywords Elliptic curves · Local–global · Galois cohomology

Mathematics Subject Classification 11R34 · 11G05

1 Introduction

Let k be a number field, and let $\mathcal{A}$ be a commutative algebraic group defined over k. Several papers have been written on the following classical question, known as the *Local–Global Divisibility Problem*.

PROBLEM: Let $P \in \mathcal{A}(k)$. Assume that for all but finitely many valuations v of 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 $P = qD$?

By Bézout's identity, to get answers for a general integer it is sufficient to solve it for powers p^n of a prime. In the classical case of $\mathcal{A} = \mathbb{G}_m$, the answer is positive for p odd, and negative for instance for $q = 8$ (and $P = 16$) (see for example [1,19]).

For general commutative algebraic groups, Dvornicich and Zannier gave a cohomological interpretation of the problem (see [5] and [7]) that we shall explain. Let Γ be a group and let M be a Γ-module. We say that a cocycle $Z\colon \Gamma \to M$ satisfies the local conditions if for every $\gamma \in \Gamma$, there exists $m_\gamma \in M$ such that $Z_\gamma = \gamma(m_\gamma) - m_\gamma$. The set of the classes of

Supported by Fondecyt Regular Project No. 1140946.

✉ Gabriele Ranieri
gabriele.ranieri@pucv.cl

1 Instituto de Matemáticas, Pontificia Universidad Católica de Valparaíso, Valparaiso, Chile

cocycles in $H^1(\Gamma, M)$ that satisfy the local conditions is a subgroup of $H^1(\Gamma, M)$. We call it the first local cohomology group $H^1_{\text{loc}}(\Gamma, M)$. Dvornicich and Zannier [5, Proposition 2.1] proved the following result.

Proposition 1 *Let p be a prime number, let n be a positive integer, let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. If $H^1_{\text{loc}}(\text{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n]) = 0$, then the local–global divisibility by p^n over $\mathcal{A}(k)$ holds.*

The converse of Proposition 1 is not true, but if the group $H^1_{\text{loc}}(\text{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n])$ is not trivial, we can find an extension L of k such that $L \cap k(\mathcal{A}[p^n]) = k$, and the local–global divisibility by p^n over $\mathcal{A}(L)$ does not hold (see [7, Theorem 3] for the details).

Several mathematicians got criterions for the validity of the local–global divisibility principle for various commutative algebraic groups, as algebraic tori [5] and [12], elliptic curves [3–8, 14–17], and very recently polarized abelian surfaces [9] and GL_2-type varieties [10].

In this paper, we focus on elliptic curves. Let p be a prime number, let k be a number field, and let $\mathcal{E}$ be an elliptic curve defined over k. Dvornicich and Zannier [7, Theorem 1] found a very interesting criterion for the validity of the local–global divisibility by a power of p over $\mathcal{E}(k)$, in the case when $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

In a joint work with Paladino and Viada (see [16], and Sect. 2), we refined this criterion, by proving that if k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ and $\mathcal{E}(k)$ does not admit a point of order p, then for every positive integer n, the local–global divisibility by p^n holds over $\mathcal{E}(k)$. In another joint work with Paladino and Viada [17], we improved our previous criterion and the new criterion allowed us to show that if $k = \mathbb{Q}$ and $p \geq 5$, for every positive integer n the local–global divisibility by p^n holds for $\mathcal{E}(\mathbb{Q})$.

Very recently, Lawson and Wutrich [13] found a very strong criterion for the triviality of $H^1(\text{Gal}(k(\mathcal{E}[p^n])/k), \mathcal{E}[p^n])$ (then for the validity of the local–global principle by p^n over $\mathcal{E}(k)$, see Proposition 1), but still in the case when $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

Finally, Dvornicich and Zannier [6] and Paladino [14] studied the case when $p = 2$ and Paladino [15] and Creutz [3] studied the case when $p = 3$.

Thus we have a fairly good understanding of the local–global divisibility by a power of p over $\mathcal{E}(k)$ either when $p \in \{2, 3\}$ or k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$ and $\mathcal{E}(k)$ does not admit a point of order p. In this paper we prove the following result:

Theorem 2 *Let $p \geq 5$ be a prime number, let k be a number field and let $\mathcal{E}$ be an elliptic curve defined over k. Suppose that there exists a positive integer n such that the local–global divisibility by p^n does not hold over $\mathcal{E}(k)$. Let G_1 be $\text{Gal}(k(\mathcal{E}[p])/k)$. Then one of the following holds:*

1. $p \equiv 2 \mod (3)$ *and G_1 is isomorphic to a subgroup of S_3 of order divisible by 3;*
2. *G_1 is cyclic of order dividing $p - 1$, and it is generated by an element that has an eigenvalue equal to 1;*
3. *G_1 is contained in a Borel subgroup, and it is generated by an element σ of order p and an element g of order dividing 2 such that σ and g have one common eigenvector for the eigenvalue 1.*

Moreover, for every case $i \in \{1, 2, 3\}$ there exist a number field L_i and an elliptic curve $\mathcal{E}_i$ defined over L_i, such that the $\text{Gal}(L_i(\mathcal{E}_i[p])/L_i)$-module $\mathcal{E}_i[p]$ is isomorphic to the G_1-module $\mathcal{E}[p]$ of the case i and the local–global divisibility by p^2 does not hold over $\mathcal{E}(L_i)$.

Proof By Proposition 4 and Lemma 15, we are in one of the three cases of the statement. The elliptic curves exist in case 1 by Remark 6 and Corollary 9, in case 2 by Remark 6 and Lemma 10, in case 3 by Remark 6 and Lemma 11. □

Clearly the case 2 of Theorem 2 corresponds to the case when $\mathcal{E}(k)$ has a point of order p defined over k. The cases 1 and 3 of Theorem 2 correspond to the case when $\mathbb{Q}(\zeta_p+\overline{\zeta_p}) \subseteq k$.

By the main result of [16] and Theorem 2, we have the following corollary:

Corollary 3 *Let $p \geq 5$ be a prime number, let k be a number field and let $\mathcal{E}$ be an elliptic curve defined over k. If $p \equiv 1 \mod (3)$ and $\mathcal{E}$ does not admit any point of order p over k, then for every positive integer n, the local–global divisibility by p^n holds over $\mathcal{E}(k)$. If $p \equiv 2 \mod (3)$, $\mathcal{E}$ does not admit any point of order p over k and $[k(\mathcal{E}[p]) : k]$ is not 3 or 6, then for every positive integer n the local–global divisibility by p^n holds over $\mathcal{E}(k)$.*

Proof If k does not contain $\mathbb{Q}(\zeta_p+\overline{\zeta_p})$, just apply the main result of [16]. If $p \equiv 1 \mod (3)$ and k contains $\mathbb{Q}(\zeta_p+\overline{\zeta_p})$, and if there exists $n \in \mathbb{N}$ such that the local–global divisibility by p^n does not hold over $\mathcal{E}(k)$, then either case 2 or case 3 of Theorem 2 applies. Thus $\mathcal{E}$ admits a point of order p defined over k.

If $p \equiv 2 \mod (3)$, $\mathcal{E}$ does not admit any point of order p over k, and there exists a positive integer n such that the local–global divisibility by p^n does not hold over $\mathcal{E}(k)$, then case 1 of Theorem 2 applies. Hence $k(\mathcal{E}[p])/k$ is either an extension of degree 3 or an extension of degree 6. □

2 Known results

In the following proposition, we combine the main results of [16] and [17] with results of [9].

Proposition 4 *Let k be a number field and let $\mathcal{E}$ be an elliptic curve defined over k. Let p be a prime number and, for every $m \in \mathbb{N}$, let G_m be* $\mathrm{Gal}(k(\mathcal{E}[p^m])/k)$. *Suppose that there exists $n \in \mathbb{N}$ such that $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) \neq 0$. Then one of the following cases holds:*

1. *If p does not divide $|G_1|$, then either G_1 is cyclic of order dividing $p-1$, generated by an element fixing a point of order p of $\mathcal{E}$, or $p \equiv 2 \mod (3)$ and G_1 is a group isomorphic either to S_3 or to a cyclic group of order 3;*
2. *If p divides $|G_1|$ then G_1 is contained in a Borel subgroup, and it is either cyclic of order p, or it is generated by an element of order p and an element of order 2 distinct from $-Id$.*

Proof Suppose first that p does not divide $|G_1|$. By the argument in [7, p. 29], we have that G_1 is isomorphic to its projective image. By [18, Proposition 16], then G_1 is either cyclic, or dihedral or isomorphic to one of the following groups: A_4, S_4, A_5.

Suppose that the last case holds. Then G_1 should contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and so it contains $-Id$. This contradicts the fact that G_1 is isomorphic to its projective image.

Suppose that G_1 is dihedral. Then G_1 is generated by τ and σ with σ of order 2 and $\sigma\tau = \tau^{-1}\sigma$. In particular all the elements of G_1 have determinant either 1 or -1. Suppose that there exists $i \in \mathbb{N}$ such that τ^i has order dividing $p-1$, and distinct from 1. Observe that since p does not divide $|G_1|$, we have $H^1(G_1, \mathcal{E}[p]) = 0$. Then, by [9, Theorem 2], we get that τ^i has at least an eigenvalue equal to 1. Thus, since τ^i is not the identity, it has determinant -1. Then τ^i has order 2. Since $\sigma\tau = \tau^{-1}\sigma$, we get $\sigma\tau^i = \tau^{-i}\sigma = \tau^i\sigma$, because τ^i has order 2. Then, since G_1 is not cyclic, τ^i and σ are two distinct elements of order 2 which commute. Thus, like in the previous case, G_1 contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and so it contains $-Id$. This contradicts the fact that G_1 is isomorphic to its projective image. Then τ has odd order dividing $p+1$. In particular it has two eigenvalues over $\mathbb{F}_{p^2}$: λ and λ^p. By [9, Proposition 17, Lemma 18] (or see [2, Sect. 3]), if there exists $n \in \mathbb{N}$ such that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$, then the intersection between the sets $\{1, \lambda^{p-1}, \lambda^{1-p}\}$ and $\{\lambda, \lambda^p\}$ is not trivial. It follows that τ has order 3. Then 3 divides $p+1$ and G_1 is isomorphic to S_3.

Finally suppose that G_1 is cyclic. If G_1 is generated by an element of order dividing $p-1$, by [9, Theorem 2] we have that such an element has an eigenvalue equal to 1. On the other hand if the generator of G_1 has order not dividing $p-1$, again by [9, Proposition 17, Lemma 18] (see the dihedral case) we get that such an element has order 3 and 3 divides $p+1$.

Suppose now that p divides $|G_1|$. Since p divides the order of G_1, by [18, Proposition 15] and the fact that G_1 is isomorphic to its projective image, we have that G_1 is contained in a Borel subgroup. In particular the p-Sylow subgroup N of G_1 is normal. Suppose that G_1/N is not cyclic. Then G_1 is not isomorphic to its projective image. Thus G_1 is generated by an element σ of order p, which generates N, and an element g of order dividing $p-1$. Suppose that 1 is not an eigenvalue for g. Then by [9, Theorem 2] (in particular notice that, by [9, Remark 16], the hypothesis $H^1(G_1, \mathcal{E}[p]) = 0$ is not necessary), we have $H^1_{\text{loc}}(G_m, \mathcal{E}[p^m]) = 0$ for every $m \in \mathbb{N}$ and so we get a contradiction. Then g has an eigenvalue equal to 1. Suppose that g has order ≥ 3. Then its determinant has order ≥ 3 and so, since the determinant is the pth cyclotomic character, k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Then if g and σ do not fix the same point of order p, by [16, Theorem 1] we get a contradiction. On the other hand, since p divides the order of G_1, we have $k(\mathcal{E}[p]) \neq k(\zeta_p)$. Then by [17, Theorem 3], we get a contradiction.

We conclude that G_1 is either cyclic of order p, or it is generated by an element g of order 2 distinct from $-Id$ and an element of order p (which generates a normal subgroup of G_1). □

We now recall some properties of the Galois action over the torsion points on an elliptic curve over a number field. In [8] we proved the following Lemma, which is a direct consequence of very interesting results of Greicius [11] and Zywina [20].

Lemma 5 *Given a prime number p, a positive integer n and a subgroup G of* $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$*, there exists a number field k and an elliptic curve $\mathcal{E}$ defined over k such that there are an isomorphism* $\phi\colon \mathrm{Gal}(k(\mathcal{E}[p^n])/k) \to G$ *and a $\mathbb{Z}/p^n\mathbb{Z}$-linear homomorphism* $\tau\colon \mathcal{E}[p^n] \to (\mathbb{Z}/p^n\mathbb{Z})^2$ *such that, for all* $\sigma \in \mathrm{Gal}(k(\mathcal{E}[p^n])/k)$ *and $v \in \mathcal{E}[p^n]$, we have* $\phi(\sigma)\tau(v) = \tau(\sigma(v))$.

Proof See [8, Lemma 11]. □

Remark 6 Given a prime number p, a positive integer n and a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, if we suppose $H^1_{\text{loc}}(G, (\mathbb{Z}/p^n\mathbb{Z})^2) \neq 0$, then by Lemma 5, there exist a number field k and an elliptic curve $\mathcal{E}$ defined over k such that $H^1_{\text{loc}}(G_n, \mathcal{E}[p^n]) \neq 0$. Hence, by [7, Theorem 3], there exists a finite extension L of k such that $L \cap k(\mathcal{E}[p^n]) = k$ and the local–global divisibility by p^n does not hold over $\mathcal{E}(L)$.

3 Auxiliary results in the prime to p case

Let $p \equiv 2 \mod (3)$ be a prime number. In [9, Sect. 5] we already found a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ such that $H^1_{\text{loc}}(G, (\mathbb{Z}/p^2\mathbb{Z})^2) \neq 0$ and the quotient of G by the subgroup

H of the elements congruent to the identity modulo p is a cyclic group of order 3. We use the following remark and the following proposition to extend the example to a group G' containing G such that G'/H is isomorphic to S_3.

Remark 7 Let p be a prime number, let m be a positive integer, let V be $(\mathbb{Z}/p^2\mathbb{Z})^{2m}$, let G be a subgroup of $\mathrm{GL}_{2m}(\mathbb{Z}/p^2\mathbb{Z})$ and let H be the subgroup of G of the elements congruent to the identity modulo p. Then we have the following inflation–restriction exact sequence:

$$0 \to H^1(G/H, V[p]) \to H^1(G, V[p]) \to H^1(H, V[p])^{G/H} \to H^2(G/H, V[p]). \tag{3.1}$$

Moreover, the exact sequence

$$0 \to V[p] \to V \to V[p] \to 0$$

(the first map is the inclusion and the second map the multiplication by p) induces the following exact sequence:

$$H^0(G, V[p]) \to H^1(G, V[p]) \to H^1(G, V) \to H^1(G, V[p]). \tag{3.2}$$

Proposition 8 *Let p be a prime number, let m be a positive integer, let V be $(\mathbb{Z}/p^2\mathbb{Z})^{2m}$, let G be a subgroup of $\mathrm{GL}_{2m}(\mathbb{Z}/p^2\mathbb{Z})$, and let H be the subgroup of G of the elements congruent to the identity modulo p. Suppose that:*

1. *G has an element δ not fixing any element of V;*
2. *H is isomorphic, as an G/H-module, to a non-trivial G/H-submodule of $V[p]$;*
3. *For every $h \in H$ distinct from the identity, the endomorphism $h - Id\colon V/V[p] \to V/V[p]$ is an isomorphism;*
4. *G/H has order not divisible by p.*

Then $H^1_{\mathrm{loc}}(G, V) \neq 0$.

Proof By Hypothesis 4, we know that the groups $H^1(G/H, \mathcal{A}[p])$ and $H^2(G/H, \mathcal{A}[p])$ in (3.1) are trivial, and hence the restriction map is an isomorphism. Since the action of H over $V[p]$ is trivial and H is an abelian group of exponent p, we have that $H^1(H, V[p])^{G/H}$ is isomorphic to $\mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[G/H]}(H, V[p])$. By Hypothesis 2, there exists $\phi\colon H \to V[p]$ an injective homomorphism of $\mathbb{Z}/p\mathbb{Z}[G/H]$-modules. Let $[Z]$ be in $H^1(G, V[p])$ such that its image in $H^1(H, V[p])^{G/H}$ is the class of ϕ. In particular, we have $[Z] \neq 0$ because ϕ is injective and the restriction map is an isomorphism.

Now observe that $H^0(G, V[p]) = 0$ by Hypothesis 1. Then, by Remark 7, we have the following exact sequence of G-modules

$$0 \to H^1(G, V[p]) \to H^1(G, V) \to H^1(G, V[p]).$$

Let us call $[W] \in H^1(G, V)$ the image of $[Z] \in H^1(G, V[p])$ defined above by the injective map $H^1(G, V[p]) \to H^1(G, V)$. Since $[Z] \neq 0$, the same holds for $[W]$. Moreover, since G/H is not divisible by p, the restriction $H^1(G, V) \to H^1(H, V)$ is injective. We conclude because by Hypothesis 3, the image of $[W]$ under this map is in $H^1_{\mathrm{loc}}(H, V)$. □

Corollary 9 *Let p be an odd prime such that $p \equiv 2 \mod (3)$. Let G be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ generated by*

$$\tau = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}$$

(which has order 3*), by an element* σ *of order* 2 *such that* $\sigma\tau\sigma^{-1} = \tau^2$ *and by*

$$H = \left\{ \begin{pmatrix} 1 + p(a - 2b) & 3p(b - a) \\ -pb & 1 - p(a - 2b) \end{pmatrix},\ a, b \in \mathbb{Z}/p^2\mathbb{Z} \right\}.$$

Then $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/p^2\mathbb{Z})^2) \neq 0$.

Proof It suffices to show that the conditions of Proposition 8 hold for G. Conditions 1 and 4 are clear and condition 3 holds by [9, Sect. 5]. Observe that G/H is isomorphic to S_3 and recall that S_3 has a unique irreducible representation of dimension 2 over $\mathbb{F}_p$. To prove condition 2 we equivalently prove that H is stable by the conjugation by τ and σ. In [9, Sect. 5] we proved that the conjugation by τ sends H to H.

Let us show that $\sigma H \sigma^{-1} = H$. A straightforward computation shows that if $\overline{\sigma}$ has order 2 in G/H and $\overline{\sigma\tau\sigma}^{-1} = \overline{\tau}^2$, then there exists $\alpha, \beta \in \mathbb{F}_p$ such that

$$\overline{\sigma} = \begin{pmatrix} \alpha - 2\beta & 3(\beta - \alpha) \\ \beta & 2\beta - \alpha \end{pmatrix}.$$

Let

$$W = \left\{ \begin{pmatrix} 1 + pc & pd \\ pe & 1 - pc \end{pmatrix},\ c, d, e \in \mathbb{Z}/p^2\mathbb{Z} \right\}.$$

It is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ and a $\mathbb{F}_p$-vector space of dimension 3. Observe that W is the subgroup of the group of the matrices congruent to the identity modulo p and having trace 2. Since the trace is invariant under conjugation, we have that $\sigma W \sigma^{-1} = W$. Let ϕ_σ be the automorphism of W such that, for every $w \in W$, $\phi_\sigma(w) = \sigma w \sigma^{-1}$. Observe that since σ has order 2, and it is distinct from Id and $-Id$, ϕ_σ has an eigenspace W_1 of dimension 1 for the eigenvalue 1, which is generated by the element $h_1 \in H$ with $a = \alpha$, $b = \beta$, and an eigenspace W_2 of dimension 2 for the eigenvalue -1. Let h be in H and $h \notin W_1$. Then $h \in W$ and, since $W = W_1 \bigoplus W_2$, there exist $r \in \mathbb{Z}$ and $h_2 \in W_2$ distinct from the identity such that $h = h_1^r h_2$. Thus $h_2 = h h_1^{-r} \in H$. Since h_1 and h_2 are linearly indipendent, they generate H. Moreover, $\phi_\sigma(h_2) = h_2^{-1} \in H$. Then $\phi_\sigma(H) = \sigma H \sigma^{-1} = H$. □

Lemma 10 *Let* p *be a prime number and let* V *be* $(\mathbb{Z}/p^2\mathbb{Z})^2$. *Let* $\lambda \in (\mathbb{Z}/p^2\mathbb{Z})^*$ *be of order dividing* $p - 1$ *and let* G *be the following subgroup of* $\mathrm{GL}_2(V)$*:*

$$G = \left\langle g = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, h(1,0) = \begin{pmatrix} 1 + p & 0 \\ 0 & 1 - p \end{pmatrix}, h(0,1) = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Then $H^1_{\mathrm{loc}}(G, V) \neq 0$.

Proof Observe that the subgroup H of G of the elements congruent to the identity modulo p is the group generated by $h(1,0)$ and $h(0,1)$. Since G/H has order not divisible by p, $H^1(G/H, V[p]) = 0$ and $H^2(G/H, V[p]) = 0$. Then, from the exact sequence (3.1) in Remark 7, we get an isomorphism from $H^1(G/H, V[p])$ to $H^1(H, V[p])^{G/H}$. Since H acts like the identity over $V[p]$ and since the groups $V[p]$ and H are abelian with exponent p, we have $H^1(H, V[p])^{G/H} = \mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[G/H]}(H, V[p])$. Observe that $gh(0,1)g^{-1} = h(0,1)^\lambda$ and $g(p,0) = \lambda(p,0)$. Then we can define a non-trivial $\mathbb{Z}/p\mathbb{Z}[G/H]$ homomorphism ϕ from H to $V[p]$ by sending $h(0,1)$ to $(p,0)$ and $h(1,0)$ to $(0,0)$ and extending it by linearity. Let Z be a cocycle representing the class $[Z]$ in $H^1(G, V[p])$ corresponding to ϕ. By (3.2) of Remark 7, we have an homomorphism from $H^1(G, V[p])$ to $H^1(G, V)$. Let $[W]$ be the image of $[Z]$ for such homomorphism. Let us show that $[W] \in H^1_{\mathrm{loc}}(G, V)$

and $[W] \neq 0$. Since G/H has order not divisible by p, it is sufficient to prove that the image of $[W]$ under the restriction to $H^1(H, V)$ is in $H^1_{\text{loc}}(H, V)$. For all integers a, b define $h(a, b) := ah(1, 0) + bh(0, 1)$. Then, by the definition of $[Z]$, we have that $h(a, b)$ is sent to $(bp, 0)$. An easy calculation shows that for every a, b, there exist x, y in $\mathbb{Z}/p^2\mathbb{Z}$ such that $(h - Id)(x, y) = (bp, 0)$. This proves that $[W] \in H^1_{\text{loc}}(G, V)$.

Finally observe that for every x, y in $\mathbb{Z}/p^2\mathbb{Z}$ such that $(h(1, 0) - Id)(x, y) = (0, 0)$, we have $x \equiv 0 \mod (p)$ and $y \equiv 0 \mod (p)$. On the other hand, for every x, y in $\mathbb{Z}/p^2\mathbb{Z}$ such that $(h(1, 0) - Id)(x, y) = (p, 0)$, we have $y \equiv 1 \mod (p)$. Thus $[W] \neq 0$. □

4 Auxiliary results in the p-dividing case

In this section we first prove the following result.

Lemma 11 *Let V be $(\mathbb{Z}/p^2\mathbb{Z})^2$ and let G be the following subgroup of* $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$*:*

$$G = \left\langle g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma = \begin{pmatrix} 1+p & 1 \\ 2p & 1+p \end{pmatrix}, h = \begin{pmatrix} 1+p & 0 \\ 0 & 1-p \end{pmatrix} \right\rangle.$$

Then $H^1_{\text{loc}}(G, V) \neq 0$.

Proof Let H be the subgroup of G of the elements congruent to 1 modulo p. Let $\overline{g}$ and $\overline{\sigma}$ be the classes of g and σ modulo H. We have that $H^1(G/H, V[p]) \neq 0$. In fact we can define a cocycle $Z\colon G/H \to V[p]$, which is not a coboundary, by sending, for every integer i_1, i_2, $Z_{\overline{g}^{i_1}\overline{\sigma}^{i_2}}$ to $(pi_2(i_2-1)/2, (-1)^{i_1} pi_2)$. Since H is normal, we have an injective homomorphism (the inflation) from $H^1(G/H, V[p])$ to $H^1(G, V[p])$. By abuse of notation we still call Z a cocycle representing the image of the class of Z in $H^1(G, V[p])$. Moreover, see Remark 7 and in particular the sequence (3.2), we have a homomorphism from $H^1(G, V[p])$ to $H^1(G, V)$. It maps the class of Z in $H^1(G, V[p])$ to some class $[W] \in H^1(G, V)$. We shall prove that $[W] \in H^1_{\text{loc}}(G, V)$ and $[W] \neq 0$.

First of all let us observe that for every $a, b, c, d \in \mathbb{Z}/p^2\mathbb{Z}$, we have

$$\begin{pmatrix} 1+ap & 1+bp \\ cp & 1+dp \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

To verify this write

$$\begin{pmatrix} 1+ap & 1+bp \\ cp & 1+dp \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} ap & 1+bp \\ cp & dp \end{pmatrix}$$

and observe that

$$\begin{pmatrix} ap & 1+bp \\ cp & dp \end{pmatrix}^2 \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \mod (p), \quad \begin{pmatrix} ap & 1+bp \\ cp & dp \end{pmatrix}^4 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus the subgroup H of G of the elements congruent to the identity modulo p is

$$H = \left\langle \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1+p & 0 \\ 0 & 1-p \end{pmatrix} \right\rangle.$$

Now observe that, since H and $\langle \sigma, H \rangle$ are normal in G, for every $\tau \in G$ there exist integers i_1, i_2, i_3 and $h \in H$ such that $\tau = g^{i_1}\sigma^{i_2}h^{i_3}$. If W is a representant for $[W]$, we have $W_\tau = (p(i_2 - 1), (-1)^{i_1} pi_2)$. If $i_2 \equiv 0 \mod (p)$, then clearly $W_\tau = (0, 0)$ and so $W_\tau =$

$(\tau - Id)((0,0))$. Then we can suppose $i_2 \not\equiv 0 \mod (p)$. It is simple to prove by induction on i_2 that

$$\sigma^{i_2} = \begin{pmatrix} 1+ap & i_2+bp \\ 2i_2p & 1+cp \end{pmatrix}$$

holds for some $a, b, c \in \mathbb{Z}/p^2\mathbb{Z}$. Moreover $\sigma^{i_2}h^{i_3}$ has again the top right entry congruent to i_2 modulo p and the bottom left entry equal to $2i_2p$. From these remarks is an easy exercise to prove that there exist α and $\beta \in \mathbb{Z}/p^2\mathbb{Z}$ such that $W_\tau = (\tau - Id)((\alpha, p\beta))$. Then $[W]$ is in $H^1_{\text{loc}}(G, V)$.

Finally let us observe that W is not a coboundary. Let $\alpha, \beta \in \mathbb{Z}/p^2\mathbb{Z}$ be such that $W_\sigma = (0, p) = (\sigma - Id)((\alpha, \beta))$. Then $\alpha \not\equiv 0 \mod (p)$. On the other hand, let $h \in H$ be such that

$$h = \begin{pmatrix} 1+p & 0 \\ 0 & 1-p \end{pmatrix}.$$

Then $W_h = (0,0)$ and so for every $\alpha, \beta \in \mathbb{Z}/p^2\mathbb{Z}$ such that $(h - id)((\alpha, \beta)) = (0,0)$, we have $\alpha \equiv 0 \mod (p)$. Hence W is not a coboundary. □

Remark 12 For every $a, b, c, d \in \mathbb{Z}/p^2\mathbb{Z}$, we have

$$\begin{pmatrix} 1+ap & 1+bp \\ cp & 1+dp \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

In a similar way, for every integer $m \geq 2$, and every $a_m, b_m, c_m, d_m \in \mathbb{Z}/p^m\mathbb{Z}$, we have

$$\begin{pmatrix} 1+a_mp & 1+b_mp \\ c_mp & 1+d_mp \end{pmatrix}^{p^{m-1}} = \begin{pmatrix} 1 & p^m \\ 0 & 1 \end{pmatrix}.$$

Corollary 13 *Let V be $(\mathbb{Z}/p^2\mathbb{Z})^2$ and let G be the following subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$:*

$$\widetilde{G} = \left\langle \sigma = \begin{pmatrix} 1+p & 1 \\ 2p & 1+p \end{pmatrix}, h = \begin{pmatrix} 1+p & 0 \\ 0 & 1-p \end{pmatrix} \right\rangle.$$

Then $H^1_{\text{loc}}(\widetilde{G}, V) \neq 0$

Proof Observe that $\widetilde{G}$ is a subgroup of index 2 of the group G of Lemma 11. Since $p \neq 2$, the restriction $H^1_{\text{loc}}(G, V) \to H^1_{\text{loc}}(\widetilde{G}, V)$ is injective and the result follows. □

Before proving the last result of this section, we need a result of linear algebra.

Lemma 14 *Let $n \in \mathbb{N}$ and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Let H be the subgroup of G of the elements congruent to the identity modulo p. Suppose that G/H is contained in a Borel subgroup, and it is generated by an element g of order 2 and an element σ of order p such that σ and g do not fix the same element of order p. Let τ be in H and let $\sigma_n \in G$ be such that σ_n is sent to σ by the projection of G over G/H. Then there exist $\tau_d, \tau_l \in H$, $\lambda \in \mathbb{N}$, such that τ_d is diagonal, τ_l is lower unitriangular and $\tau = \tau_d\tau_l\sigma_n^{p\lambda}$. In other words H is generated by its subgroups of the diagonal matrices, its subgroup of the lower unitriangular matrices and σ_n^p.*

Proof Fix a basis of $(\mathbb{Z}/p^n\mathbb{Z})^2$ such that

$$\sigma_n \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod (p).$$

Then, since g has order 2 and p is odd, there exists an element g_n of G such that

$$g_n = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We remark that $\sigma_n^p \in H$. In fact $\sigma_n^p \equiv Id \mod (p)$.

We first show that every $\tau \in H$ can be written as a product of a lower triangular matrix $\tau_L \in H$ and a power of σ_n^p. Since $\tau \in H$, $\tau \equiv Id \mod (p)$ and so there exist $e, g, m, r \in \mathbb{Z}/p^n\mathbb{Z}$ such that

$$\tau = \begin{pmatrix} 1+pe & pg \\ pm & 1+pr \end{pmatrix}.$$

We prove by induction that for every integer $i \geq 1$, there exists $\lambda_i \in \mathbb{Z}/p^n\mathbb{Z}$ such that

$$\tau\sigma_n^{p\lambda_i} = \begin{pmatrix} 1+pe_i & p^i g_i \\ pm_i & 1+pr_i \end{pmatrix}, \tag{4.1}$$

for some $e_i, g_i, m_i, r_i \in \mathbb{Z}/p^n\mathbb{Z}$. If $i = 1$ then for $\lambda_1 = 0$ the relation (4.1) is satisfied. Suppose that (4.1) is satisfied for an integer $i \geq 1$. Then there exists $\lambda_i \in \mathbb{Z}/p^n\mathbb{Z}$ such that

$$\tau\sigma_n^{p\lambda_i} = \begin{pmatrix} 1+pe_i & p^i g_i \\ pm_i & 1+pr_i \end{pmatrix},$$

for some $e_i, g_i, m_i, r_i \in \mathbb{Z}/p^n\mathbb{Z}$. Choose an element λ_{i+1} of $\mathbb{Z}/p^n\mathbb{Z}$ such that $p\lambda_{i+1} = p\lambda_i - p^i g_i$. Observe that this element exists because $i \geq 1$. By Remark 12 we have

$$\begin{aligned} \sigma_n^{-p^i g_i} &= \begin{pmatrix} 1+p^{i+1}a_{i+1} & p^i + p^{i+1}b_{i+1} \\ p^{i+1}c_{i+1} & 1+p^{i+1}d_{i+1} \end{pmatrix}^{-g_i} \\ &= \begin{pmatrix} 1+p^{i+1}a'_{i+1} & -p^i g_i + p^{i+1}b'_{i+1} \\ p^{i+1}c'_{i+1} & 1+p^{i+1}d'_{i+1} \end{pmatrix}, \end{aligned}$$

for some $a'_{i+1}, b'_{i+1}, c'_{i+1}, d'_{i+1} \in \mathbb{Z}/p^n\mathbb{Z}$. By a short computation

$$\begin{aligned} \tau\sigma_n^{p\lambda_{i+1}} &= \tau\sigma_n^{p\lambda_i}\sigma_n^{-p^i g_i} \\ &= \begin{pmatrix} 1+pe_i & p^i + p^i g_i \\ pm_i & 1+pr_i \end{pmatrix} \begin{pmatrix} 1+p^{i+1}a'_{i+1} & -p^i g_i + p^{i+1}b'_{i+1} \\ p^{i+1}c'_{i+1} & 1+p^{i+1}d'_{i+1} \end{pmatrix} \\ &= \begin{pmatrix} 1+pe_{i+1} & +p^{i+1}g_{i+1} \\ pm_{i+1} & 1+pr_{i+1} \end{pmatrix}, \end{aligned}$$

for some $e_{i+1}, g_{i+1}, m_{i+1}, r_{i+1} \in \mathbb{Z}/p^n\mathbb{Z}$. Then (4.1) is verified for λ_{i+1} that satisfies $p\lambda_{i+1} = p\lambda_i - p^i g_i$. In particular for $i = n$ we have

$$\tau\sigma_n^{p\lambda_n} = \begin{pmatrix} 1+pe_n & 0 \\ pm_n & 1+pr_n \end{pmatrix}.$$

Then, setting $\tau_L = \tau\sigma_n^{p\lambda_n}$ and $\lambda = -\lambda_n$, we have shown that τ can be written as a product of a lower triangular matrix $\tau_L \in H$ and the power $\sigma_n^{p\lambda}$ of σ_n^p.

Observe that, to conclude the proof, it is sufficient to show that τ_L can be written as the product of a diagonal matrix $\tau_d \in H$ and a lower unitriangular matrix $\tau_l \in H$. Since H is normal in G, $g_n\tau_L g_n^{-1} \in H$. Then $g_n\tau_L g_n^{-1}\tau_L^{-1} \in H$. Moreover, by a simple computation, we have

$$g_n\tau_L g_n^{-1}\tau_L^{-1} = \begin{pmatrix} 1 & 0 \\ -2pm_n/(pe_n+1) & 1 \end{pmatrix}.$$

Thus

$$(g_n\tau_L g_n^{-1}\tau_L^{-1})^{-(pe_n+1)/2(pr_n+1)} = \begin{pmatrix} 1 & 0 \\ pm_n/(pr_n+1) & 1 \end{pmatrix} \in H.$$

Call such a matrix τ_l and observe that

$$\tau_L = \begin{pmatrix} 1+pe_n & 0 \\ 0 & 1+pr_n \end{pmatrix}\begin{pmatrix} 1 & 0 \\ pm_n/(pr_n+1) & 1 \end{pmatrix}.$$

Call the diagonal matrix τ_d. Since $\tau_L, \tau_l \in H$, also $\tau_d \in H$, proving the statement. □

Lemma 15 *Under the assumptions and with the notation of Lemma 14, let V_n be $(\mathbb{Z}/p^n\mathbb{Z})^2$. Then $H^1_{\mathrm{loc}}(G, V_n) = 0$.*

Proof By replacing V with V_n, by observing that $H^0(G, V_n[p^{n-1}]) = 0$ because the group generated by g and σ do not fix any element of $V_n[p^{n-1}]$, and by using the Remark 7, we get the following exact sequence

$$0 \to H^1(G, V_n[p]) \to H^1(G, V_n) \to H^1(G, V_n[p^{n-1}]). \tag{4.2}$$

Suppose that $H^1_{\mathrm{loc}}(G, V_n) \neq 0$. Then $H^1_{\mathrm{loc}}(G, V_n)[p] \neq 0$ and so let Z be a cocycle representing a non-trivial class $[Z] \in H^1_{\mathrm{loc}}(G, V_n)[p]$. Let us observe that $[Z]$ is in the kernel of the map $H^1(G, V_n) \to H^1(G, V_n[p^{n-1}])$ (here we generalize the proof of [9, Lemma 13]). Since $[Z]$ has order p, then pZ is a coboundary and so there exists $v \in V_n$ such that, for every $\tau \in G$, $pZ_\tau = \tau(v) - v$. Let us observe that $v \in V_n[p^{n-1}]$. Since for every τ we have $\tau(v) - v \in V_n[p^{n-1}]$, and we get that $v \in \cap_{\tau\in G} \ker(p^{n-1}(\tau - Id))$. Since G does not fix any element of order p, the unique possibility is that $v \in V_n[p^{n-1}]$. Then (see the sequence (4.2)) $[Z]$ is in the image of $H^1(G, V_n[p]) \to H^1(G, V_n)$. By abuse of notation we call $[Z]$ the class in $H^1(G, V_n[p])$ sent to $[Z]$.

Consider now the inflation–restriction sequence

$$0 \to H^1(G/H, V_n[p]) \to H^1(G, V_n[p]) \to H^1(H, V_n[p])^{G/H}. \tag{4.3}$$

Let us observe that $H^1(G/H, V_n[p]) = 0$. Let $W\colon G/H \to V_n[p]$ be a cocycle. Since σ and g are contained in a Borel subgroup, g has order 2, and g and σ do not fix any nonzero element of $V_n[p^{n-1}]$, we can choose a basis of V_n such that $(p^{n-1}, 0)$ is fixed by σ, $g((p^{n-1}, 0)) = (-p^{n-1}, 0)$ and $(0, p^{n-1})$ is sent to (p^{n-1}, p^{n-1}) by σ and fixed by g. Observe that, since summing a coboundary to W does not change its class, we can suppose that $W_\sigma = (0, p^{n-1})$. Then, for every integer i, we have $W_{\sigma^i} = (p^{n-1}i(i-1)/2, p^{n-1}i)$. Observe that since g has order 2, we have $W_{g^2} = W_g + gW_g = (0, 0)$. In particular there exists $a \in \mathbb{Z}/p^n\mathbb{Z}$ such that $W_g = (p^{n-1}a, 0)$, and which is fixed by σ. Thus $W_{g\sigma g^{-1}} = gW_\sigma = (p^{n-1}, -p^{n-1})$. On the other hand, $g\sigma g^{-1} = \sigma^{-1}$ and so $W_{\sigma^{-1}} = (-p^{n-1}, -p^{n-1})$. We then get a contradiction. Thus, by the sequence (4.3), to every class of $H^1(G, V_n[p])$ we can associate a class in $H^1(H, V_n[p])^{G/H}$. Since H acts as the identity over $V_n[p]$, we have that $H^1(H, V_n[p])^{G/H}$ is a subgroup of $\mathrm{Hom}(H, V_n[p])$. In particular, we can associate with $[Z] \in H^1(G, V[p])$ defined above a homomorphism from H to $V_n[p]$. By Lemma 14, for every $\tau \in H$ there exist $\tau_l \in H$ a lower unitriangular matrix, $\tau_D \in H$ a diagonal matrix and $\lambda \in \mathbb{Z}$ such that $\tau = \tau_l\tau_D\sigma_n^{\lambda p}$. Consider the homorphism associated with $[Z] \in H^1(G, V_n[p])$. Since the cocycle Z has values in $V_n[p]$, in particular $Z_{\sigma_n} \in V_n[p]$ and, by the cocycle property, $Z_{\sigma_n^p} = (0, 0)$. On the other hand, since $g_n\tau_D g_n^{-1} = \tau_D$, there exists $b \in \mathbb{Z}/p^n\mathbb{Z}$ such that $Z_{\tau_D} = (0, p^{n-1}b)$. If $p^{n-1}b$ is distinct from 0, then $(0, p^{n-1}b)$ generates $V[p]$ as an G/H-module. Since $g_n\tau_l g_n^{-1} = \tau_l^{-1}$, there exists $a \in \mathbb{Z}/p^n\mathbb{Z}$ such that $Z_{\tau_l} = (p^{n-1}a, 0)$. Observe that for every $(\alpha, \beta) \in V_n$, we have that $(\tau_l - Id)(\alpha, \beta) = (p^{n-1}a, 0)$ only if $p^{n-1}a = 0$. Then if the image of Z satisfies the local conditions over V_n, the homomorphism associated with Z is trivial, and so Z is a coboundary. □

References

1. Artin, E., Tate, J.: Class Field Theory. Benjamin, Reading (1967)
2. Ciperiani, M., Stix, J.: Weil–Châtelet divisible elements in Tate–Shafarevich groups II: on a question of Cassels. J. Für Die Reine und Angew. Math. **700**, 175–207 (2015)
3. Creutz, B.: Locally trivial torsors that are not Weil–Châtelet divisible. Bull. Lond. Math. Soc. **45**, 935–941 (2013)
4. Creutz, B.: On the local-global principle for divisibility in the cohomology of elliptic curves. Math. Res. Lett. **23**(2), 377–387 (2016)
5. Dvornicich, R., Zannier, U.: Local-global divisibility of rational points in some commutative algebraic groups. Bull. Soc. Math. France **129**, 317–338 (2001)
6. Dvornicich, R., Zannier, U.: An analogue for elliptic curves of the Grunwald–Wang example. C. R. Acad. Sci. **338**, 47–50 (2004)
7. Dvornicich, R., Zannier, U.: On local-global principle for the divisibility of a rational point by a positive integer. Bull. Lond. Math. Soc. **39**, 27–34 (2007)
8. Gillibert, F., Ranieri, G.: On the local-global divisibility of torsion points on elliptic curves and GL_2-type varieties. J. Number Theory **174**, 202–220 (2017)
9. Gillibert, F., Ranieri, G.: On the local-global divisibility over abelian varieties, arXiv:1612.00058, to appear in the Ann. Institut Fourier
10. Gillibert, F., Ranieri, G.: On the local-global divisibility over GL_2-type varieties, arXiv:1703.06235, submitted
11. Greicius, A.: Elliptic curve with surjective adelic Galois representation. Exp. Math. **19**(4), 495–507 (2010)
12. Illengo, M.: Cohomology of integer matrices and local-global divisibility on the torus. Le J. de Théorie des Nombres de Bordeaux **20**(2), 327–334 (2008)
13. Lawson, T., Wuthrich, C.: *Vanishing of Some Galois Cohomology Groups of Elliptic Curves*, Preprint, arXiv:1505.02940v1
14. Paladino, L.: Local-global divisibility by 4 in elliptic curves defined over $\mathbb{Q}$. Annali di Matematica Pura e Appl. **189**(1), 17–23 (2010)
15. Paladino, L.: Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9. Le J. de Théorie des Nombres de Bordx. **22**(1), 138–160 (2010)
16. Paladino, L., Ranieri, G., Viada, E.: Local-global divisibility by p^n in elliptic curves, arXiv:1104.4762v2
17. Paladino, L., Ranieri, G., Viada, E.: On the minimal set for counterexamples to the local-global divisibility principle. J. Algebra **415**, 290–304 (2014)
18. Serre, J.-P.: Proprietés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
19. Trost, E.: Zur theorie des Potenzreste. Nieuw Archief voor Wiskunde **18**(2), 58–61 (1948)
20. Zywina, D.: Elliptic curves with maximal Galois action on their torsion points. Bull. Lond. Math. Soc. **42**(5), 811–826 (2010)