Riv. Mat. Univ. Parma, Vol. **10** (2019), 99–116

ANTONELLA PERUCCA

The problem of detecting linear dependence

Abstract. Let A be an algebraic group defined over a number field K, let P be a point in $A(K)$, and let G be a finitely generated subgroup of $A(K)$. If P belongs to G, then clearly its reduction $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K (notice that we only consider those primes $\mathfrak{p}$ such that the reductions are well-defined, and are "good" reductions). The problem of detecting linear dependence asks whether the converse holds, so whether we have a local-global principle. In this survey article we also investigate the problem of detecting linear dependence for torsion points.

Keywords. Number fields, local-global principle, detecting linear dependence.

Mathematics Subject Classification (2010): Primary: 11G10; Secondary 14L10, 14K15.

Contents

Received: January 6, 2019; accepted in revised form: June 6, 2019.

1 - Introduction

This is a survey article on the problem of detecting linear dependence, which is a number theoretical problem first investigated by Schinzel in 1975 [**23**] for the multiplicative group. A more general setting was independently considered by Gajda and by Kowalski. The latter asked [**14**]:

Question 1. *Does the assertion "b is in the group generated by a" obey a local-global principle for points of an algebraic group over a number field?*

The question concerns the reductions of algebraic groups defined over a number field: if a rational point belongs to a group of rational points (this is the *global* property), then clearly the reductions of the point belong to the reductions of the group (these are the *local* properties). One can ask whether the local properties are strong enough to imply the global property, so if one has a *local-global principle*. Gajda formulated this problem for simple abelian varieties (as a question to Ribet in 2002), and the Conjecture of Detecting Linear Dependence arose:

Conjecture 2. *Let A be an abelian variety defined over a number field K. Let P be a point in $A(K)$, and let G be a subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, then P belongs to G.*

The conjecture has been open from 2002 to 2009, and it has been proven in various cases, see Section 2. Jossen and Perucca disproved the conjecture [**12**]: their counterexample and further negative results are presented in Section 3. Some open questions are listed in Section 5. Beyond several original remarks, new material can be found in Section 4, where we investigate the problem of detecting linear dependence for torsion points. In particular we complete a result by Weston and prove that the local-global principle holds for all abelian varieties with endomorphism ring $\mathbb{Z}$, see Corollary 16.

One possible application of the problem of detecting linear dependence is investigating the rank of the Mordell-Weil group of abelian varieties. Quoting [**3**]:

> One of our goals [...] is to show that the reduction maps can be used to investigate the nontorsion part of the Mordell-Weil group. Given a finite set of nontorsion points [...], one can ask whether it is possible to detect linear dependence among elements of this set by reductions.

Understanding the rank of the Mordell-Weil group (possibly making use of informations coming from the reductions) is a long-term goal and an open research direction in number theory.

2 - Positive results

In this section we consider the positive results around the following question, which asks whether the local-global principle of linear dependence holds:

Question 3. *Let A be a commutative algebraic group defined over a number field K. Let P be a point in $A(K)$, and let G be a finitely generated subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, does it follow that P belongs to G? (Notice that we only consider those primes $\mathfrak{p}$ such that the reductions are well-defined, and are "good" reductions.)*

Notice that 'for almost all primes' could either mean 'for all but finitely many primes' or 'for a set of primes having Dirichlet density 1' (it does not make a substantial difference in this context). The assumption that the group G is finitely generated ensures that its reductions are well-defined for all but finitely many primes of K.

Remark 4. Question 3 has a negative answer already for the multiplicative group over $\mathbb{Q}$ if we allow the group G to be infinitely generated (and reduce modulo p only the points of G which do not contain p in their prime factorisation). Indeed, consider the point 2 and the group generated by the odd prime numbers. The global condition clearly does not hold, but the local conditions are satisfied as a consequence of Dirichlet's theorem on arithmetic progressions.

2.1 - *The multiplicative group*

Schinzel proved that Question 3 has a positive answer for the multiplicative group (however this does not hold in general for tori, see Section 3.1):

Theorem 5 (Schinzel [**23**, Theorem 2]). *If $a_1, \ldots, a_r$, and b are non-zero elements of K and the congruence*

$$b \equiv \prod_{i=1}^{r} a_i^{x_i} \bmod \mathfrak{p}$$

in the integer variables x_i is soluble for almost all primes $\mathfrak{p}$ of K, then the corresponding equation $b = \prod_{i=1}^{r} a_i^{x_i}$ is soluble.

Proof sketch. Schinzel's proof is based on Kummer theory and several results about congruences. To highlight the proof structure we will assume $K = K(\zeta_4)$. Fix some $n \geqslant 2$, and consider the Galois group of the cyclotomic-Kummer extension $K(\zeta_n, a_1^{1/n}, \dots, a_r^{1/n})/K$. The elements in this Galois group which fix all $a_i^{1/n}$ for some choice of the n-th roots must also fix $b^{1/n}$ for some choice of the n-th root, otherwise we could easily construct a positive density of reductions for which the local condition does not hold.

Then we can apply [**23**, Lemma 6] and find integers z_i such that the equality $b^{1/n} = \prod_i a_i^{z_i/n}$ holds up to some multiple of ζ_n and up to some element of $K^\times$. We deduce that the equality $b = \prod_i a_i^{z_i}$ holds up to some element of $(K^\times)^n$. This last relation immediately translates to a set of congruences modulo n for the exponents with respect to a multiplicative basis for $K^\times$ (we can express non-zero elements of K in a unique way as a root of unity in K times a product of powers of some multiplicatively independent elements of K).

We then have a system of linear congruences which is soluble modulo n for all $n \geqslant 2$, and by a result of Skolem [**25**] the corresponding equations are also soluble. This means that the above exponents satisfy a relation that, considering the original algebraic numbers, can be written in the form $b = \prod_i a_i^{x_i}$ for some integers x_i. This concludes the proof.

We have made use of [**23**, Lemma 6]: to prove this lemma, Schinzel analyzes the Galois action on the given n-th roots as multiplication by $\zeta_n^{e_i}$ for some integers e_i. Such integers give rise to functions with abstract properties as those in [**23**, Lemma 5] and for which this other lemma applies. In turn, [**23**, Lemma 5] is a technical result about 'double congruences': the notation $v \equiv 0 \mod (M, M')$, where v is an integral vector and M, M' are square integral matrices of the same size, stands for the relation $v = wM + w'M'$ for some integral vectors w, w'. □

2.2 - *A cyclic group of points*

Question 1 is the special case of Question 3 if the group of points is cyclic. Kowalski [**14**, Theorem 3.3] proved that the answer to Question 1 is affirmative for elliptic curves, and in general we have:

Theorem 6 (Perucca [**17**, Theorem 11]). *Let A be the product of an abelian variety and a torus defined over a number field K. Let P be a point in $A(K)$, and let G be a cyclic subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, then P belongs to G.*

Perucca derives this result from Theorem 10, so we present instead the direct proof by Kowalski for elliptic curves. If K is a number field and P is a K-rational point on

an elliptic curve, then we denote by $K(n^{-1}P)$ the field extension of K obtained by adding all points on the curve (defined on an algebraic closure $\bar{K}$) such that $nQ = P$.

Proof sketch (for elliptic curves). Let P' be a generator of G, and let us focus on the main case where P and P' are points of infinite order. The local conditions imply an inclusion between Kummer extensions, namely for every $n \geqslant 1$ we have $K(n^{-1}P) \subseteq K(n^{-1}P')$. This is because for almost all primes $\mathfrak{p}$ of K we know that if $(P' \bmod \mathfrak{p})$ is an n-th power, then so is $(P \bmod \mathfrak{p})$. We deduce that P and P' cannot be independent over the ring of K-endomorphisms [**14**, Proposition 6.1] because two independent points would generate instead "large Kummer extensions" by a well-known result of Ribet [**20**, Theorem 1.2]. Then one can write a dependency relation in the form $f(P) = nP'$, where f is a K-endomorphism and n is a non-zero integer. For CM elliptic curves, by analyzing the images of the torsion points under f (and by making use of the local conditions) one finds that f is the multiplication by an integer. Finally, the smallest positive integer m such that $mP \in G$ must be 1, otherwise we can find a positive density of reductions that do not satisfy the local condition. □

2.3 - *Abelian varieties with commutative endomorphism ring*

The local-global principle of linear dependence has been established by Weston 'up to a rational torsion point' for all abelian varieties with commutative endomorphism ring:

Theorem 7 (Weston [**26**, Theorem]). *Let A be an abelian variety defined over a number field K, and suppose that $\mathrm{End}_K A$ is commutative. Let P be a point in $A(K)$, and let G be a subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, then P belongs to $G + A(K)_{\mathrm{tors}}$.*

Proof sketch. The proof investigates in detail the structure of the Mordell-Weil group as a module over the endomorphism ring. We assume that $E := \mathrm{End}_K A$ is a Dedekind domain because in this basic case one can better see the proof structure. It suffices to fix any prime number p and prove the following claim: the point P belongs to $G \otimes \mathbb{Z}_{(p)}$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ away from p.

Up to torsion, we can choose a $\mathbb{Z}$-basis for $A(K)$ such that G is generated by multiples of elements of this basis. Suppose that the claim does not hold. Then there is some integer coordinate which has less p-divisibility for the point P than for the points of G. So there is a group homomorphism $\psi_0 : A(K) \to \mathbb{Z}$ such that $\psi_0(P)$ does not belong to $\psi_0(G) + p^n\mathbb{Z}$ for all sufficiently large n. By the general algebraic result [**26**, Lemma 2.1] there is a homomorphism of E-modules $\psi : A(K) \to E$ such that $\psi(P)$ does not belong to $\psi(G) + p^n E$ for all sufficiently large n. To conclude the

proof we will contradict the last assertion, and for this we will have to choose some sufficiently large integer N.

The E-module $A(K)$ has a pre-basis, i.e. points in $A(K)$ which are E-independent and generate a subgroup of $A(K)$ of finite index. We will assume the index to be 1 (otherwise we only need to increase N to take care of this index). If we choose the pre-basis appropriately, then ψ is an integer multiple of the map to the first coordinate. We will assume that ψ equals that map (otherwise we only need to increase N to compensate this). Call B the first element of the pre-basis.

We will work with some prime $\mathfrak{q}$ of K which is of good reduction for A, is not over p, satisfies the local condition of the statement, and has the following additional properties [**26**, Lemma 3.3]. Firstly, the reduction of B modulo $\mathfrak{q}$ is not $\mathcal{P}^c$-divisible for any prime ideal $\mathcal{P}$ dividing pE, where $c > 0$ is a fixed constant: for simplicity we suppose that $c = 1$ (otherwise we could compensate this by increasing N). Secondly, the reductions modulo $\mathfrak{q}$ of all other elements of the pre-basis are p^N-divisible. Thirdly, the p^N-torsion points of the reduction of A modulo $\mathfrak{q}$ are defined over the residue field $k_{\mathfrak{q}}$.

By the choice of $\mathfrak{q}$ we know that $(\psi(P)B \bmod \mathfrak{q})$ belongs to $(\psi(G)B \bmod \mathfrak{q})$ up to some p^N-divisible point. In other words, the point $(\psi(P - P')B \bmod \mathfrak{q})$ is p^N-divisible for some $P' \in G$. This p^N-divisibility does not come from $(B \bmod \mathfrak{q})$, so we deduce (with the help of [**26**, Lemma 2.4]) that $\psi(P)$ belongs to $\psi(G)$ up to some element in $p^N E$. Since N can be chosen to be arbitrarily large, we have found a contradiction. □

Banaszak and Krasoń extended Weston's result as follows:

T h e o r e m 8 (Banaszak and Krasoń [**4**, Theorem A]). *Let A be an abelian variety defined over a number field K. Let A be $\bar{K}$-isogenous to the product $\prod_{i=1}^{t} A_i^{e_i}$, where the A_i are geometrically simple and pairwise not $\bar{K}$-isogenous abelian varieties. Suppose that e_i does not exceed the dimension of $H_1(A_i(\mathbb{C}), \mathbb{Q})$ over $\mathrm{End}_{\bar{K}} A_i \otimes \mathbb{Q}$ for all i. Let P be a point in $A(K)$, and let G be a subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K, then P belongs to $G + A(K)_{\mathrm{tors}}$.*

P r o o f s k e t c h. Since P and G are defined over K, it suffices to prove that for some finite extension K' of K we have $P \in G + A(K')_{tors}$. In particular we may replace K by some finite extension K' (because the local conditions for P and G also hold over K'). Moreover, we may replace A by any K-isogenous abelian variety. Indeed, if $\varphi : A \to A'$ is a K-isogeny, then the local conditions also hold in A' for $\varphi(P)$ and $\varphi(G)$, and the global condition $\varphi(P) \in \varphi(G) + A'(K)_{\mathrm{tors}}$ implies $P \in G + A(K')_{tors}$ for some finite extension K' of K (where the points in the kernel of φ are defined). This allows us to work with the abelian variety $\prod_{i=1}^{t} A_i^{e_i}$ instead.

The proof then follows substantially the one of Theorem 7, which covers the case where $e_i = 1$ for all i. Thus we only explain where the assumption on e_i is used. Let $\mathcal{L}_i$ be a Riemann lattice such that $A_i(\mathbb{C}) \simeq \mathbb{C}^{g_i}/\mathcal{L}_i$, where g_i is the dimension of A_i. Fix a finite index sublattice $\mathcal{L}_i'$ of $\mathcal{L}_i$ which is a free $\mathrm{End}_K A_i$-submodule: the rank of $\mathcal{L}_i'$ is at least e_i by assumption. Let $\mathcal{O}$ be the ring of integers of K, let ℓ be a prime number, and write the prime ideal factorisation $\ell\mathcal{O} = \prod_{\lambda|\ell} \lambda^{\epsilon}$. Call $\mathcal{O}_\lambda$ the localization of $\mathcal{O}$ away from λ. For every $n \geqslant 1$ we have $A_i[\ell^n] = \bigoplus_{\lambda|\ell} A_i[\lambda^{\epsilon n}]$ and $A_i[\lambda^{\epsilon n}] \simeq \mathcal{L}_i \otimes \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L}_i \otimes \mathcal{O}_\lambda$. The information about the rank of $\mathcal{L}_i'$ ensures that we can find e_i torsion points which are independent over an appropriate endomorphism ring. This will be used to construct (with results in the style of Lemma 9) a suitable family of reductions. □

The analogous result for products of abelian varieties and tori (i.e. where one of the simple factors can be the multiplicative group) was proven by Blinkiewicz [**7**, Twierdzenie 3.1.7].

2.4 - *Free modules over the endomorphism ring*

Several theorems about the problem of detecting linear dependence are based on results about 'prescribing valuations for the order of the reductions of points' like the following lemma (for the most general results of this kind so far, see [**18**]).

Lemma 9. *Let A be the product of an abelian variety and a torus defined over a number field K. Let P_1 to P_n be points in $A(K)$ that are independent over the ring of K-endomorphisms of A. Let ℓ be a prime number, and let a_1 to a_n be non-negative integers. There exists a positive density of primes $\mathfrak{p}$ of K such that for every $i = 1, \ldots, n$ the order of $(P_i \bmod \mathfrak{p})$ has ℓ-adic valuation a_i.*

The first theorems around Question 3 obtained with this method are due to Banaszak, Gajda, and Krasoń [**1**, **3**]: crucial assumptions are that the point generates a free module over the endomorphism ring, and that the group of points is either a free module or it has group generators which generate a free module. Gajda and Górnisiewicz proved a similar result in [**8**, Theorem B]. All these results are improved by Theorem 10.

Theorem 10 (Perucca [**17**, Theorems 6 and 8]). *Let A be the product of an abelian variety and a torus defined over a number field K. The local-global principle of linear dependence holds for a point in $A(K)$ and a subgroup of $A(K)$ if the subgroup is either a free $\mathrm{End}_K A$-module or it has a set of group generators which generate a free $\mathrm{End}_K A$-module.*

Perucca's proof is based on her results about *the support problem* [**19**], which in turn are based on Lemma 9. Gajda and Górnisiewicz also proved the following result:

Theorem 11 (Gajda and Górnisiewicz [**8**, Theorem A]). *Let A be an abelian variety defined over a number field K. Let ℓ be a prime number, and suppose that the Tate module $T_\ell(A)$ is integrally semisimple. Then the local-global principle of linear dependence holds for a point in $A(K) \otimes \mathbb{Z}_\ell$ and a subgroup of $A(K) \otimes \mathbb{Z}_\ell$ if the point generates a free module and the subgroup is a free module over* $\mathrm{End}_K A \otimes \mathbb{Z}_\ell$.

A free $\mathbb{Z}_\ell$-module T with the continuous action of $\mathrm{Gal}(\bar{K}/K)$ is called *integrally semisimple* if for every Galois subrepresentation T' of $T \otimes \mathbb{Q}_\ell$ the following exact sequence of $\mathbb{Z}_\ell[\mathrm{Gal}(\bar{K}/K)]$-modules splits:

$$0 \longrightarrow T \cap T' \longrightarrow T \longrightarrow T/(T \cap T') \longrightarrow 0\,.$$

The Tate module $T_\ell(A)$ is integrally semisimple for almost all ℓ. Moreover, it is integrally semisimple for all ℓ for at least one abelian variety in every K-isogeny class. These results are due to Larsen and Schoof [**15**] and can be found in [**8**, Section 3]. The proof of Theorem 11 uses this theory of integrally semisimple Galois modules, but also results of Kummer theory and Galois cohomology [**8**, Section 2] which provide an assertion similar to Lemma 9.

The following result does not require additional assumptions, and its proof is also based on Lemma 9:

Theorem 12 (Perucca [**17**, Theorem 6]). *Let A be the product of an abelian variety and a torus defined over a number field K. Let P be a point in $A(K)$, and let G be a subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, then there exists a non-zero integer m (depending on A and K, and the rank of G) such that mP belongs to the* $\mathrm{End}_K A$*-module generated by G.*

2.5 - *Geometrically simple abelian varieties*

Jossen proved that the local-global principle of linear dependence holds for all geometrically simple abelian varieties, and in particular for all elliptic curves:

Theorem 13 (Jossen [**10**, Main Theorem]). *Let A be a geometrically simple abelian variety defined over a number field K. Let P be a point in $A(K)$, and let G be a subgroup of $A(K)$. If the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, then P belongs to G.*

Jossen's proof makes use of 1-motives, but these are not really necessary because one could phrase everything in terms of Galois modules. To avoid misunderstandings we point out that a previous and more general version of this result [**11**] was incorrect.

Proof sketch. Let S be a set of primes of K having density 1 and for which the local condition in the statement holds. Then for any subgroup X of $A(K)$ define

the group

$$\bar{X} := \{Q \in A(K) \mid (Q \bmod \mathfrak{p}) \in (X \bmod \mathfrak{p}) \quad \forall\, \mathfrak{p} \in S\}\,.$$

We have to prove that $\bar{G} = G$, and for this it suffices to show that $\bar{X}/X$ is torsion free for every finite index subgroup X of $A(K)$ containing G. Indeed, the quotient $\bar{X}/X$ is trivial (being torsion free and finite), so we have $\bar{G} \subseteq \bar{X} = X$. Thus $\bar{G}$ is contained in all finite index subgroups of $A(K)$ containing G, and hence $\bar{G} = G$ because $A(K)$ is finitely generated.

We now prove that $\bar{X}/X$ is torsion free for every subgroup X of $A(K)$. It suffices that for any prime number ℓ the group $(\bar{X}/X) \otimes \mathbb{Z}_\ell$ is torsion free.

Let Γ be the absolute Galois group of K, and let $T_\ell M$ be the Tate module of the 1-motive encoding the group X. In simpler terms, $T_\ell M$ is the generalisation of the Tate module to points other than the zero point, and it is constructed by similarly considering the tree of ℓ-division points; it is in particular a finitely generated and free $\mathbb{Z}_\ell$-module with a continuous Galois action. Then define the group $H^1_S(\Gamma, T_\ell M)$ as the kernel of the map

$$H^1(\Gamma, T_\ell M) \longrightarrow \prod_{\mathfrak{p} \in S} H^1(\Gamma_\mathfrak{p}, T_\ell M)\,,$$

where $\Gamma_\mathfrak{p}$ is the absolute Galois group of the residue field at $\mathfrak{p}$, and where we consider the family of restriction maps. The group $(\bar{X}/X) \otimes \mathbb{Z}_\ell$ can be embedded in $H^1_S(\Gamma, T_\ell M)$ [**10**, Proposition 1.11] and hence it suffices to prove that the latter group is torsion free. One technical detail: we may replace S so that the primes over ℓ are excluded.

By the Chebotarev Density Theorem (considering the topologically cyclic subgroups generated by the Frobenius maps) we find that $H^1_S(\Gamma, T_\ell M)$ is isomorphic to the group $H^1_*(\Gamma, T_\ell M)$ [**10**, Proposition 1.15], which is defined as the kernel of the map

$$H^1(\Gamma, T_\ell M) \longrightarrow \prod_{C} H^1(C, T_\ell M)\,,$$

where C varies over all topologically cyclic subgroups of Γ, and where we consider the family of restriction maps. Moreover, we may replace Γ by its image in the group of automorphisms of $T_\ell M$, i.e. we may work with the smallest Galois extension of K where for each n the ℓ^n-division points over the points of G are defined [**10**, Proposition 1.16]. This is straight-forward but important because Γ is then an ℓ-adic Lie group.

Finally, the proof that $H^1_*(\Gamma, T_\ell M)$ is torsion free is achieved through a general result [**10**, Key Lemma 4.1] about a finitely generated and free $\mathbb{Z}_\ell$-module with the continuous action of an ℓ-adic Lie group, whose assumptions hold for a geometrically simple abelian variety [**10**, Corollary 4.5]. □

3 - Negative results

3.1 - *A counterexample for tori*

Schinzel gave a counterexample to the local-global principle of detecting linear dependence for tori [**23**, p.419-420]. The counterexample is for the square of the multiplicative group over $\mathbb{Q}$. Consider the point $P := \begin{pmatrix}1\\2\end{pmatrix}$, and the group G which is generated by the following three points:

$$P_1 := \begin{pmatrix}2\\1\end{pmatrix} \qquad P_2 := \begin{pmatrix}3\\2\end{pmatrix} \qquad P_3 := \begin{pmatrix}1\\3\end{pmatrix}.$$

The group G consists of all points of the form $\begin{pmatrix}2^x3^y\\2^y3^z\end{pmatrix}$ for some integers x, y, z. Since 2 and 3 are multiplicative independent integers, the point P does not belong to G (in fact, no non-trivial multiple of P does). Nevertheless, for every prime number $p \neq 2, 3$ the reduction of P modulo p belongs to the reduction of G modulo p. Indeed, calling a and b the index of $(2 \bmod p)$ and $(3 \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, we only need to find integers x, y, z satisfying

$$\begin{cases} xa + yb \equiv 0 \pmod{p-1} \\ ya + zb \equiv a \pmod{p-1}. \end{cases}$$

For any integer t the numbers $x := -tb/(a,b)$ and $y := ta/(a,b)$ satisfy the first congruence. It then suffices to take for t and z a solution of the following linear diophantine equation (which can be easily checked to be solvable):

$$t\frac{a^2}{(a,b)} + zb = a\,.$$

We may consider the reductions modulo any prime p by working with $\mathbb{Z}/p\mathbb{Z}$ rather than $(\mathbb{Z}/p\mathbb{Z})^\times$, provided that we exclude those points for which the reduction is not well-defined (e.g. the reduction of P_1^{-1} modulo 2 is not well-defined). In the above example, by choosing $P := \begin{pmatrix}1\\4\end{pmatrix}$ instead (as done by Schinzel), one gets a counterexample where the local condition is satisfied for all prime numbers.

Remark 14. In Schinzel's counterexample the numbers 2 and 3 can be replaced by any other prime number pair, and hence one has infinitely many counterexamples. By putting such counterexamples together, one can fix any positive integer n and construct two finitely generated and torsion free groups of points $G' \subset G$ such that for all prime numbers p we have $(G \bmod p) = (G' \bmod p)$, and such that the ranks of G and G' differ by n. In the same way one could construct groups G and G'

that satisfy the above local conditions and such that the quotient G/G' is not finitely generated. Analogously, one could consider two groups G and G' having a small intersection (i.e. the difference between the ranks of G and $G \cap G'$ can be made arbitrarily large, and similarly for G') and such that for all prime numbers p we have $(G \bmod p) = (G' \bmod p) = (G \cap G' \bmod p)$: some examples of this kind (easy adaptations of the counterexamples in this section) can be found in [**2**, Section 3] by Banaszak and Blinkiewicz.

3.2 - *A counterexample for abelian varieties*

Jossen and Perucca [**12**] gave a counterexample to Conjecture 2 for the third power of an elliptic curve without complex multiplication[1]. Consider the elliptic curve (Cremona label 5077a1)

$$E:\ y^2 + y = x^3 - 7x + 6\,.$$

This curve is without CM, and its $\mathbb{Q}$-points $P_1 := (-2, 3)$, $P_2 := (-1, 3)$, and $P_3 := (0, 2)$ are $\mathbb{Z}$–linearly independent. For the problem of detecting linear dependence, consider the abelian variety E^3 over $\mathbb{Q}$, and the following point and group:

$$P := \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \qquad G := \left\{ MP \in E^3(\mathbb{Q}) \;\middle|\; M \in \mathrm{Mat}(3, \mathbb{Z}), \operatorname{tr} M = 0 \right\}.$$

The group G consists of the images of the point P under all those endomorphisms of E^3 which, considered as 3×3 matrices, have trace zero. The point P has three coordinates which are $\mathbb{Z}$-linearly independent, and therefore it does not belong to G. However, for all primes $p \neq 5077$ the point $(P \bmod p)$ belongs to $(G \bmod p)$ because we can find a matrix M with trace zero such that $(MP \bmod p) = (P \bmod p)$, see [**12**]. This is because the $\mathbb{Z}/p\mathbb{Z}$-points of E form a group which is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^2$ for some integer $n \geqslant 1$, and hence any three such points are 'dependent'.

3.3 - *A counterexample for abelian surfaces*

Banaszak and Krasoń gave a counterexample to Conjecture 2 for the square of an elliptic curve with complex multiplication. Consider the following elliptic curve (Cremona label 18496i2):

$$E:\ y^2 = x^3 - 34^2 x\,.$$

[1] Jossen had reasons to believe that the conjecture was false and thus Perucca, who was previously trying to prove the conjecture, produced the first counterexample.

This curve has complex multiplication by $\mathbb{Z}[i]$, and the points $Q_1 := (-16, 120)$ and $Q_2 := (-2, 48)$ are independent over the endomorphism ring $\mathbb{Z}[i]$. For the problem of detecting linear dependence consider the abelian variety E^2 over $\mathbb{Q}(i)$, whose endomorphism ring consists of the 2×2 matrices with entries in $\mathbb{Z}[i]$. Take as point $P := \begin{pmatrix} 0 \\ Q_1 \end{pmatrix}$, and take as group G the $\mathbb{Z}[i]$-module generated by the following three points:

$$P_1 := \begin{pmatrix} Q_1 \\ 0 \end{pmatrix} \qquad P_2 := \begin{pmatrix} Q_2 \\ Q_1 \end{pmatrix} \qquad P_3 := \begin{pmatrix} 0 \\ Q_2 \end{pmatrix}.$$

The group G is closed under multiplication by scalar matrices, but not by all matrices. It does not contain the point P (nor any non-zero multiple of P). For all primes $\mathfrak{p}$ of $\mathbb{Q}(i)$ which lie over a prime number $p \neq 2, 17$ the group of $k_\mathfrak{p}$-points of E (where $k_\mathfrak{p}$ is the residue field at $\mathfrak{p}$) is a cyclic $\mathbb{Z}[i]$-module, and one can show that the point $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$, see [**4**, Section 6]. It is because of the above cyclicity that this counterexample works as the one in Section 3.1.

4 - Torsion points

We now investigate Question 3 for a split semiabelian variety (i.e. the product of a variety and a torus) if P is a torsion point, or if G is finite. The local-global principle of linear dependence holds if G is finite because the reductions of two distinct points cannot coincide for infinitely many reductions. So the interesting case is the following: P is a torsion point and G is infinite. Some of the results in Section 2 allow P to be a torsion point. Moreover, we may strengthen Theorem 10:

Theorem 15. *Let A be the product of an abelian variety and a torus defined over a number field K. The local-global principle of linear dependence holds for a torsion point $P \in A(K)$ and a group $G \subseteq A(K)$ if the torsion free part of G (by which we mean any complement to the torsion subgroup) is contained in a free $\mathrm{End}_K A$-module.*

Proof. Write $P = \sum_\ell P_\ell$ where ℓ varies over the prime divisors of the order of P, and where P_ℓ is a torsion point of order a power of ℓ. Since P_ℓ is a multiple of P, the local conditions also hold for P_ℓ, and we are left to show that $P_\ell \in G$. Write $G = G' + G_{\mathrm{tors}}$, where G_{tors} is the torsion subgroup of G. By assumption G' is contained in some free $\mathrm{End}_K A$-module, whose generators are as in Lemma 9 (there choose $a_i = 0$). We then find infinitely many primes $\mathfrak{p}$ of K such that $(P_\ell \bmod \mathfrak{p})$ belongs to $(G_{\mathrm{tors}} \bmod \mathfrak{p})$, which ensures that P_ℓ belongs to the finite group G_{tors}. □

We are then able to complete Weston's result (Theorem 7) for all abelian varieties whose endomorphism ring is $\mathbb{Z}$:

Corollary 16. *Let A be an abelian variety defined over a number field K, and whose ring of K-endomorphisms is $\mathbb{Z}$. Then the local-global principle of linear dependence holds for A.*

Proof. We use the notation of Theorem 7. Because of this result we know that $P + T \in G$ for some point $T \in A(K)_{\mathrm{tors}}$. We deduce that $(T \bmod \mathfrak{p}) \in (G \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. By applying Theorem 15 we find that $T \in G$ and hence $P \in G$. □

The following examples show that, even supposing that P is a torsion point, the local-global principle of linear dependence in general does not hold (neither for tori nor for abelian varieties).

Example 17. Consider the square of the multiplicative group over $\mathbb{Q}$, the torsion point $P := \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, and the group G which is generated by the two points

$$P_0 := \begin{pmatrix} 1 \\ 2 \end{pmatrix} \qquad P_1 := \begin{pmatrix} 2 \\ -1 \end{pmatrix}.$$

The point $(P \bmod 2)$ coincides with the reduction modulo 2 of the neutral element of G. For a prime number $p \neq 2$, if the order of $(2 \bmod p)$ is odd, then there is an odd multiple of $(P_1 \bmod p)$ which equals $(P \bmod p)$, while if the order of $(2 \bmod p)$ is even, then there is a multiple of $(P_0 \bmod p)$ which equals $(P \bmod p)$. Thus for all prime numbers p the point $(P \bmod p)$ belongs to $(G \bmod p)$, although P does not belong to G.

We now construct a similar counterexample where the order of P is any integer $m > 1$. Notice that we denote by ζ_N a root of unity of order N. Set $P := \begin{pmatrix} 1 \\ \zeta_m \end{pmatrix}$ and, considering the prime factorization $m = \prod_{\ell | m} \ell^n$, take the group G which is generated by all points $\begin{pmatrix} 1 \\ \ell \end{pmatrix}$ and $\begin{pmatrix} \ell^{\ell^{n-1}} \\ \zeta_{\ell^n} \end{pmatrix}$.

Example 18. Consider the elliptic curve $y^2 = x^3 - 34^2 x$ (Cremona label 18496i2) over its field of complex multiplication $K := \mathbb{Q}(i)$. On this curve take the following points: the zero point O; the points of infinite order $Q := (-16, 120)$ and iQ; the torsion points $T_1 := (0, 0)$ and $T_2 := (34, 0)$ of order 2. Then consider, on the square of the elliptic curve, the torsion point $P := \begin{pmatrix} O \\ T_1 \end{pmatrix}$, and the group G which is generated by the following points:

$$P_1 := \begin{pmatrix} Q \\ T_1 \end{pmatrix} \qquad P_2 := \begin{pmatrix} O \\ T_2 \end{pmatrix} \qquad P_3 := \begin{pmatrix} O \\ Q \end{pmatrix} \qquad P_4 := \begin{pmatrix} O \\ iQ \end{pmatrix}.$$

For a prime $\mathfrak{p}$ of K of good reduction for E the following holds: If the order of $(Q \bmod \mathfrak{p})$ is odd, then $(P \bmod \mathfrak{p})$ is an odd multiple of $(P_1 \bmod \mathfrak{p})$. If the order of $(Q \bmod \mathfrak{p})$ is even, then this point has a multiple of the form $(T \bmod \mathfrak{p})$ for some point T of order 2: since T_1 is a combination of the points T, iT, and T_2, the point $(P \bmod \mathfrak{p})$ is in the group generated by the reductions modulo $\mathfrak{p}$ of P_2, P_3, and P_4.

5 - Research directions

5.1 - *Extending the known results*

It may be possible to find further classes of abelian varieties for which the local-global principle holds, for example: the square of an elliptic curve without complex multiplication; simple abelian varieties; products of pairwise non-isogenous (geometrically) simple abelian varieties. Notice that removing the torsion ambiguity in the results of Section 2.3 amounts to proving the local-global principle under the assumption that P is a torsion point. One could also investigate the constant of Theorem 12, for example answering the following question:

Question 19. *Is is true in general that the local conditions of Question 3 imply that P belongs to the $\mathrm{End}_K A$-module generated by G?*

As suggested by the referee, one could consider Question 3 for non-split semi-abelian varieties which are extensions by tori of dimension one (this seems to be the most natural, still unsettled case).

5.2 - *Considering the ℓ-part of the reductions*

Khare proved the following statement for the multiplicative group:

Theorem 20 (Khare [**13**, Proposition 3]). *Let K be a number field, let $P \in K^\times$, and let G be a finitely generated subgroup of $K^\times$. If for almost all primes $\mathfrak{p}$ of K the point $(n_\mathfrak{p} P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ for some integer $n_\mathfrak{p}$ which is coprime to ℓ (and that may depend on $\mathfrak{p}$), then nP belongs to G for some integer n that is coprime to ℓ.*

Perucca proved [**17**, Lemma 7] for products of abelian varieties and tori that Khare's local assumptions imply the existence of a non-zero integer n such that nP belongs to the $\mathrm{End}_K A$-module generated by G. It is also possible to say something about the ℓ-adic valuation of n, namely that $v_\ell(n) \leqslant v_\ell(m)$ where m only depends on A, K and the rank of G (in particular, the bound does not depend on ℓ and hence, for almost all ℓ, n is coprime to ℓ).

R e m a r k 21. If A is the product of an abelian variety and a torus defined over a number field K, then Khare's result holds for A, if we suppose that the torsion free part of G is a free $\mathrm{End}_K A$-module or it has a set of group generators that generate a free $\mathrm{End}_K A$-module (e.g. if A is K-simple and G is infinite cyclic, or if $\mathrm{End}_K A = \mathbb{Z}$). Here is a sketch of proof: We apply [**17**, Lemma 10] to a multiple of P and G (such that G torsion free) and find that $nP+T \in G$ for some torsion point $T \in A(K)$ having order a power of ℓ, and where n is an integer coprime to ℓ; Khare's local conditions hold for T and G and hence by Theorem 15 we can remove the torsion ambiguity.

One can ask if such results can be improved, for example if Khare's theorem extends to all simple abelian varieties.

5.3 - *Making the results effective*

Let A be an algebraic group defined over a number field K. If P is a point in $A(K)$, and G is a subgroup of $A(K)$, what can we say about the set of primes $\mathfrak{p}$ of K such that $(P \bmod \mathfrak{p})$ belongs to $(G \bmod \mathfrak{p})$ [**10**, Question 2]? In terms of effectivity, for how many reductions do we have to check the local condition of Question 3 before we can be sure that $P \in G$? Some general investigation of the effectivity can be found in [**2**, **4**, **7**] by Banaszak, Blinkiewicz, and Krasoń: the key idea is using an effective version of Chebotarev Density Theorem whenever this result needs to be applied. More precise results for elliptic curves over $\mathbb{Q}$ can be found in [**22**] by Sadek, and in [**24**] by Sha and Shparlinski. Given a group G of rational points, one may consider those rational points which are x-pseudolinearly dependent of G, i.e. whose reduction modulo p belongs to $(G \bmod p)$ for all primes p of good reduction up to x. In [**24**] there are bounds for the canonical height of such pseudodependent points: as noted by the authors, some of their results would hold in greater generality as soon as the theorems they rely upon can be extended. As an example of result, Sha and Shparlinski proved:

T h e o r e m 22 (Sha and Shparlinski [**24**, Theorem 5]). *Let E be an elliptic curve defined over $\mathbb{Q}$ of rank $r \geqslant 2$, and let G be a subgroup of $E(\mathbb{Q})$ of positive rank $s < r$. Then for any sufficiently large x there is a rational point $Q \in E(\mathbb{Q})$ of canonical height*

$$\hat{h}(Q) \leqslant \exp\Big(\frac{4}{s+2}x + O(x/\log x)\Big)$$

such that Q is x-pseudolinearly dependent of G.

5.4 - *Changing the setting*

Rzonsowski generalized some of the results on the problem of detecting linear dependence to abelian varieties over a finitely generated (possibly non algebraic) extension of $\mathbb{Q}$, see [**21**, Theorem 7.2 and Proposition 7.3]. One could ask whether further results hold in this setting. Alternatively, one could consider algebraic groups over function fields and their reductions. Another possibility is working abstractly with Mordell-Weil systems as done by Banaszak, Gajda, and Krasoń in [**3**] (they axiomatized the properties of Mordell-Weil groups of abelian varieties). Some further results of this kind have been obtained by Barańczuk and Górnisiewicz [**5**, **6**] for the K-theory of number fields, and for the étale and Quillen K-theory of curves.

5.5 - *Comparing two groups*

Let A be an algebraic group defined over a number field K, and consider two subgroups G and G' of $A(K)$. We may wish to know whether $G' \subseteq G$. The condition that $(G' \bmod \mathfrak{p}) \subseteq (G \bmod \mathfrak{p})$ holds for almost all primes $\mathfrak{p}$ of K gives nothing new with respect to Question 3 (just consider one by one group generators for G'). In [**2**] Banaszak and Blinkiewicz investigated local conditions that are equivalent to the following:

1. Suppose that for almost all primes $\mathfrak{p}$ of K we have
$$(G + G' \bmod \mathfrak{p}) \subseteq ((G \cap G') + A(K)_{\mathrm{tors}} \bmod \mathfrak{p}) .$$
2. Fix some integer $c \geqslant 1$, and suppose that for almost all primes $\mathfrak{p}$ of K the index
$$(G + G' \bmod \mathfrak{p})/(G \cap G' \bmod \mathfrak{p})$$
divides c.

The first condition clearly implies the second. Banaszak and Blinkiewicz showed [**2**, Propositions 2.1 and 2.2] that again we do not have anything new with respect to Question 3. Indeed, Property (1) implies the inclusion $(G+G') \subseteq (G \cap G')+A(K)_{\mathrm{tors}}$ if and only if for Question 3 we can prove that $P \in G+A(K)_{\mathrm{tors}}$. Moreover, Property (2) implies the finiteness of the group $(G + G')/(G \cap G')$ if and only if for Question 3 we can prove that $nP \in G$ for some non-negative integer n. A new question could be:

Question 23. *If for almost all primes* $\mathfrak{p}$ *of* K *the two groups* $(G \bmod \mathfrak{p})$ *and* $(G' \bmod \mathfrak{p})$ *have a non-trivial intersection, does it follow that* G *and* G' *have a non-trivial intersection?*

The counterexamples in Section 3 provide a negative answer to the above question. Nevertheless the answer could be affirmative, say, for cyclic groups of points of the multiplicative group or an elliptic curve. We conclude by remarking that there are several open questions in number theory concerning the reductions of algebraic groups, but to describe them goes beyond the purpose of this note. Just to mention one example, in a work by Hall and Perucca [**9**] the following result is proven (for simplicity, we state the result for elliptic curves):

Theorem 24. *Let E/K be an elliptic curve defined over a number field K, and suppose that the rank of $E(K)$ is positive. Then the size of the group $(E(K) \bmod \mathfrak{p})$ by varying $\mathfrak{p}$ in a set of primes of K (of good reduction for E) having density 1 determines E up to K-isogeny.*

Acknowledgments. The author would like to sincerely thank the referee for their improvements to the paper.

References

[**1**] G. BANASZAK, *On a Hasse principle for Mordell-Weil groups*, C. R. Math. Acad. Sci. **347** (2009), 709–714.

[**2**] G. BANASZAK and D. BLINKIEWICZ, *Commensurability in Mordell-Weil groups of abelian varieties and tori*, Funct. Approx. Comment. Math. **58** (2018), 145–156.

[**3**] G. BANASZAK, W. GAJDA and P. KRASOŃ, *Detecting linear dependence by reduction maps*, J. Number Theory **115** (2005), 322–342.

[**4**] G. BANASZAK and P. KRASOŃ, *On arithmetic in Mordell-Weil groups*, Acta Arith. **150** (2011), 315–337.

[**5**] S. BARAŃCZUK, *On reduction maps and support problem in K-theory and abelian varieties*, J. Number Theory **119** (2006), 1–17.

[**6**] S. BARAŃCZUK and K. GÓRNISIEWICZ, *On reduction maps for the étale and Quillen K-theory of curves and applications*, J. K-Theory **2** (2008), 103–122.

[**7**] D. BLINKIEWICZ, *Zasada lokalno-globalna dla rozmaitości semiabelowych*, Ph.D. thesis, Adam Mickiewicz University, Poznań, 2017.

[**8**] W. GAJDA and K. GÓRNISIEWICZ, *Linear dependence in Mordell-Weil groups*, J. Reine Angew. Math. **630** (2009), 219–233.

[**9**] C. HALL and A. PERUCCA, *Characterizing abelian varieties by the reduction of the Mordell-Weil group*, Pacific J. Math. **265** (2013), 427–440.

[**10**] P. JOSSEN, *Detecting linear dependence on an abelian variety via reduction maps*, Comment. Math. Helv. **88** (2013), 323–352.

[**11**] P. JOSSEN, *On the arithmetic of 1-motives*, Ph.D. thesis, Central European University Budapest, July 2009.

[**12**] P. JOSSEN and A. PERUCCA, *A counterexample to the local-global principle of linear dependence for abelian varieties*, C. R. Math. Acad. Sci. Paris **348** (2010), 9–10.

[**13**] C. KHARE, *Compatible systems of mod p Galois representations and Hecke characters*, Math. Res. Lett. **10** (2003), 71–83.

[**14**] E. KOWALSKI, *Some local-global applications of Kummer theory*, Manuscripta Math. **111** (2003), 105–139.

[**15**] M. LARSEN and R. SCHOOF, *Whitehead's lemma and Galois cohomology of abelian varieties*, preprint, 2003.

[**16**] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2013, `http://www.lmfdb.org`, [Online; accessed 16 September 2013].

[**17**] A. PERUCCA, *On the problem of detecting linear dependence for products of abelian varieties and tori*, Acta Arith. **142** (2010), 119–128.

[**18**] A. PERUCCA, *On the reduction of points on abelian varieties and tori*, Int. Math. Res. Not. IMRN **2011** (2011), 293–308.

[**19**] A. PERUCCA, *Two variants of the support problem for products of abelian varieties and tori*, J. Number Theory **129** (2009), 1883–1892.

[**20**] K. A. RIBET, *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. **46** (1979), 745–761.

[**21**] P. RZONSOWSKI, *Linear relations and arithmetic on abelian schemes*, Funct. Approx. Comment. Math. **52** (2015), 83–107.

[**22**] M. SADEK, *On dependence of rational points on elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **38** (2016), 75–84.

[**23**] A. SCHINZEL, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.

[**24**] M. SHA and I. E. SHPARLINSKI, *Effective results on linear dependence for elliptic curves*, Pacific J. Math. **295** (2018), 123–144.

[**25**] TH. SKOLEM, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Avh. Norske Vid. Akad. Oslo **1937** (1937), no. 12, 1–16.

[**26**] T. WESTON, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups*, Acta Arith. **110** (2003), 77–88.

ANTONELLA PERUCCA
University of Luxembourg
Mathematics Research Unit
6, av. de la Fonte
4364, Esch-sur-Alzette, Luxembourg
e-mail: antonella.perucca@uni.lu