A counterexample to the local-global principle of linear dependence for abelian varieties

Peter Jossen and Antonella Perucca

Abstract

Let A be an abelian variety defined over a number field k. Let P be a point in $A(k)$ and let X be a subgroup of $A(k)$. Gajda and Kowalski asked in 2002 whether it is true that the point P belongs to X if and only if the point $(P \bmod \mathfrak{p})$ belongs to $(X \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of k. We provide a counterexample.

Résumé

Soient k un corps de nombres, A une variété abélienne sur k, P un point de $A(k)$ et X un sous-groupe de $A(k)$. En 2002 Gajda et Kowalski ont demandé s'il est vrai que le point P appartient à X si et seulement si le point $(P \bmod \mathfrak{p})$ appartient à $(X \bmod \mathfrak{p})$ pour presque toute place finie $\mathfrak{p}$ de k. Nous donnons une réponse négative à cette question.

Let A be an abelian variety defined over a number field k. Let P be a point in $A(k)$ and let X be a subgroup of $A(k)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of k the point $(P \bmod \mathfrak{p})$ belongs to $(X \bmod \mathfrak{p})$. Is it true that P belongs to X? This question, which was formulated by Gajda and by Kowalski in 2002, was named the problem of detecting linear dependence. The problem was addressed in several papers (see the bibliography) but the question was still open. In a recent note ([Jos09a]) the first author stated that the answer to this problem is always affirmative, but this is wrong. In this note we present a counterexample.

A counterexample to the analogous statement for tori was given by Schinzel in [Sch75]. We have recently been informed that Banaszak and Krasoń found different counterexamples, which will appear in a new version of [BK09]. In his Ph.D. thesis the first author shows that for *simple* abelian varieties the answer is positive.

Let k be a number field and let E be an elliptic curve over k such that there are points P_1, P_2, P_3 in $E(k)$ which are $\mathbb{Z}$–linearly independent. Define $A := E^3$, and let $P \in A(k)$ and $X \subseteq A(k)$ be the following:

$$P := \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \qquad\qquad X := \Big\{ MP \in A(k) \;\Big|\; M \in \mathrm{Mat}(3, \mathbb{Z}), \operatorname{tr} M = 0 \Big\}$$

So the group X consists of the images of the point P via the subgroup of the endomorphisms of A consisting of the matrices with integer coefficients and trace zero. Since the points P_i are $\mathbb{Z}$–independent, the point P does not belong to X. Notice that no non-zero multiple of P belongs to X.

Claim. *Let $\mathfrak{p}$ be a prime of k where E has good reduction. The image of P under the reduction map modulo $\mathfrak{p}$ belongs to the image of X.*

For the rest of this note, we fix a prime $\mathfrak{p}$ of good reduction for E. We write κ for the residue field of k at $\mathfrak{p}$. To ease notation, we now let E denote the reduction of the given elliptic curve modulo $\mathfrak{p}$ and write P_1, P_2, P_3, P for the image of the given points under the reduction map modulo $\mathfrak{p}$.
Our aim is to find an integer matrix M of trace zero such that $P = MP$ in $A(\kappa)$.

For $i = 1, 2, 3$ call J_i the subgroup of the integers defined as follows: n belongs to J_i if and only if nP_i is in the subgroup of $E(\kappa)$ generated by the other two points. Call α_i the positive generator of J_i. There are integers m_{ij} such that

$$\begin{aligned} \alpha_1 P_1 + m_{12} P_2 + m_{13} P_3 &= O \\ m_{21} P_1 + \alpha_2 P_2 + m_{23} P_3 &= O \\ m_{31} P_1 + m_{32} P_2 + \alpha_3 P_3 &= O \end{aligned}$$

Assume that the greatest common divisor of α_1, α_2 and α_3 is 1 (we prove this assumption later). We can thus find integers a_1, a_2, a_3 such that

$$3 = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3$$

Write $m_{ii} := 1 - \alpha_i a_i$, so that in particular $m_{11} + m_{22} + m_{33} = 0$. Then we have

$$\begin{pmatrix} m_{11} & -a_1 m_{12} & -a_1 m_{13} \\ -a_2 m_{21} & m_{22} & -a_2 m_{23} \\ -a_3 m_{31} & -a_3 m_{32} & m_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}$$

Notice that the above matrix has integer entries and trace zero. Hence we are left to prove that the greatest common divisor of α_1, α_2 and α_3 is indeed 1, or in other words that the ideals J_1, J_2 and J_3 generate $\mathbb{Z}$.

Fix a prime number ℓ and let us show that ℓ does not divide $\gcd(\alpha_1, \alpha_2, \alpha_3)$. Suppose on the contrary that ℓ divides $\gcd(\alpha_1, \alpha_2, \alpha_3)$. By definition of the ideals J_i, this is equivalent to saying that ℓ divides all the coefficients appearing in any linear relation between P_1, P_2 and P_3. In particular, this implies that ℓ divides the order of P_1, P_2 and P_3 in $E(\kappa)$.
Let Z denote the subgroup of $E(\kappa)$ generated by P_1, P_2 and P_3. It is well–known that the group $E(\kappa)[\ell]$ is either trivial, isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. In any case, the intersection $Z \cap E(\kappa)[\ell]$ is generated by two elements or less. Without loss of generality, let us suppose that the subgroup of Z generated by P_2 and P_3 contains $Z \cap E(\kappa)[\ell]$.
We are supposing that ℓ divides all the coefficients appearing in any linear relation of the points P_i. Let $\alpha_1 = x_1 \ell$ and write $x_1 \ell P_1 + x_2 \ell P_2 + x_3 \ell P_3 = O$ for some integers x_2 and x_3. It follows that

$$x_1 P_1 + x_2 P_2 + x_3 P_3 = T$$

for some point T in Z of order 1 or ℓ. In any case, the point T is a linear combination of P_2 and P_3. Hence also $x_1 P_1$ is a linear combination of P_2 and P_3 and this contradicts the minimality of α_1.

In our counterexample, the only requirement for the elliptic curve E is that $E(k)$ has rank at least 3. According to John Cremona's database ([Cre]), the elliptic curve given by the equation

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

has rank 3 over $\mathbb{Q}$. The three points $P_1 := [-2 : 3 : 1]$, $P_2 := [-1 : 3 : 1]$ and $P_3 := [0 : 2 : 1]$ on E given in projective coordinates are $\mathbb{Z}$–linearly independent.

References

[Ban09] G. Banaszak, *On a Hasse principle for Mordell-Weil groups*, C. R. Acad. Sci. Paris, Sér. I Math. (2009), no. 347, 709–714.

[Bar] S. Barańczuk, *On a generalization of the support problem of Erdös and its analogues for abelian varieties and K-theory*, to appear on Journal Pure Appl. Algebra.

[BGK05] G. Banaszak, W. Gajda, and P. Krasoń, *Detecting linear dependence by reduction maps*, J. Number Theory **115** (2005), no. 2, 322–342.

[BK09] G. Banaszak and P. Krasoń, *On arithmetic in Mordell–Weil groups*, arXiv:math/0904.2848, 2009.

[Cre] J. Cremona, *Elliptic Curve Data*, `http://www.warwick.ac.uk/staff/J.E.Cremona/`.

[GG09] W. Gajda and K. Górnisiewicz, *Linear dependence in Mordell–Weil groups*, J. Reine Angew. Math. **630** (2009), 219–233.

[Jos09a] P. Jossen, *Detecting linear dependence on a semiabelian variety*, arXiv:math/0903.5271, 2009.

[Jos09b] P. Jossen, *On the arithmetic of 1-motives*, Ph.D. thesis, Central European University Budapest, July 2009.

[Kha03] C. Khare, *Compatible systems of mod p Galois representations and Hecke characters*, Math. Res. Lett. **10** (2003), 71–83.

[Kow03] E. Kowalski, *Some local–global applications of Kummer theory*, Manuscripta Math. **111** (2003), no. 1, 105–139.

[Per08] A. Perucca, *On the problem of detecting linear dependence for products of abelian varieties and tori*, arXiv:math/0811.1495, 2008.

[Sch75] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.

[Wes03] T. Weston, *Kummer theory of abelian varieties and reduction of Mordell-Weil groups*, Acta Arith. **110** (2003), 77–88.

Peter Jossen
NWF I - Mathematik, Universität Regensburg
D-93040 Regensburg, Germany
`peter.jossen@gmail.com`

Antonella Perucca
Section des Mathématiques, École Polytechnique Fédérale de Lausanne
EPFL Station 8, 1015 Lausanne, Switzerland
`antonella.perucca@epfl.ch`