Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 347 (2009) 709–714
COMPTES RENDUS MATHEMATIQUE

Number Theory

On a Hasse principle for Mordell–Weil groups

Grzegorz Banaszak

Department of Mathematics, Adam Mickiewicz University, 61614 Poznań, Poland

Received 7 April 2008; accepted after revision 17 March 2009

Available online 7 May 2009

Presented by Christophe Soulé

Abstract

In this Note we establish a Hasse principle concerning the linear dependence over $\mathbb{Z}$ of nontorsion points in the Mordell–Weil group of an abelian variety over a number field. ***To cite this article: G. Banaszak, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Résumé

Un principe de Hasse pour les groupes de Mordell–Weil. Dans cette Note, on démontre un principe de Hasse concernant la dépendance linéaire sur $\mathbb{Z}$ des points d'ordre infini dans le groupe de Mordell–Weil d'une variété abélienne définie sur un corps de nombres. ***Pour citer cet article : G. Banaszak, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***

Version française abrégée

Soit A une variété abélienne définie sur un corps de nombres F. Soient v un idéal premier de $\mathcal{O}_F$ et $k_v := \mathcal{O}_F/v$. Soit A_v la réduction de A pour un idéal premier v de bonne réduction. Soit,

$$r_v : A(F) \to A_v(k_v),$$

le morphisme de réduction. On pose $\mathcal{R} := \mathrm{End}_F(A)$. Soit Λ une sous-groupe de $A(F)$ et soit $P \in A(F)$. Une question naturelle est : La condition $r_v(P) \in r_v(\Lambda)$, pour presque tout idéal premier v de $\mathcal{O}_F$, implique-t-elle $P \in \Lambda$? Cette question a eté posée par W. Gajda en 2002. Le résultat fondamental de cette Note est le théorème suivant :

Théorème 0.1. *Soient $P_1, \ldots, P_r$ des éléments de $A(F)$ linéairement indépendants sur l'anneau $\mathcal{R}$. Soit P un point de $A(F)$ tel que $\mathcal{R}P$ soit un $\mathcal{R}$-module libre. Les conditions suivantes sont équivalentes* :

(1) $P \in \sum_{i=1}^{r} \mathbb{Z}P_i$;
(2) $r_v(P) \in \sum_{i=1}^{r} \mathbb{Z}r_v(P_i)$ *pour presque tout idéal premier v de $\mathcal{O}_F$.*

E-mail address: banaszak@amu.edu.pl.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2009.03.014

1. Introduction

Let A be an abelian variety over a number field F. Let v be a prime of $\mathcal{O}_F$ and let $k_v := \mathcal{O}_F/v$. Let A_v denote the reduction of A for a prime v of good reduction and let,

$$r_v : A(F) \to A_v(k_v),$$

be the reduction map. Put $\mathcal{R} := \mathrm{End}_F(A)$. Let Λ be a subgroup of $A(F)$ and let $P \in A(F)$. A natural question is whether the condition $r_v(P) \in r_v(\Lambda)$ for almost all primes v of $\mathcal{O}_F$ implies that $P \in \Lambda$. This question was posed by W. Gajda in 2002. The main result of this Note is the following theorem:

Theorem 1.1. *Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R}$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$ module. The following conditions are equivalent*:

(1) $P \in \sum_{i=1}^{r} \mathbb{Z} P_i$;
(2) $r_v(P) \in \sum_{i=1}^{r} \mathbb{Z} r_v(P_i)$ *for almost all primes v of $\mathcal{O}_F$.*

In the case of the multiplicative group $F^\times$ the problem analogous to W. Gajda's question has already been solved by 1975. Namely, A. Schinzel, [16, Theorem 2, p. 398], proved that for any $\gamma_1, \ldots, \gamma_r \in F^\times$ and $\beta \in F^\times$ such that $\beta = \prod_{i=1}^{r} \gamma_i^{n_{v,i}} \bmod v$ with $n_{v,1}, \ldots, n_{v,r} \in \mathbb{Z}$ for almost all primes v of $\mathcal{O}_F$ there are $n_1, \ldots, n_r \in \mathbb{Z}$ such that $\beta = \prod_{i=1}^{r} \gamma_i^{n_i}$. The theorem of A. Schinzel was proved again by Ch. Khare [11] using methods of C. Corralez-Rodrigáñez and R. Schoof [6]. Ch. Khare applied this theorem to prove that every family of one-dimensional strictly compatible l-adic representations comes from a Hecke character.

Theorem 1.1 strengthens the results of [2,8,19]. Namely T. Weston [19] obtained a result analogous to Theorem 1.1 with coefficients in $\mathbb{Z}$ for $\mathcal{R}$ commutative. T. Weston did not assume that $P_1, \ldots, P_r$ are linearly independent over $\mathcal{R}$, however there was some torsion ambiguity in the statement of his result. In [2], together with W. Gajda and P. Krasoń, we proved Theorem 1.1 for elliptic curves without CM and more generally for a class of abelian varieties with $\mathrm{End}_{\overline{F}}(A) = \mathbb{Z}$. We also got a general result for all abelian varieties [2, Theorem 2.9], in the direction of Theorem 1.1. However in Theorem 2.9 [2], the coefficients associated with points $P_1, \ldots, P_r$ are in $\mathcal{R}$ and the coefficient associated with the point P is in the set of positive integers $\mathbb{N}$. W. Gajda and K. Górnisiewicz [8, Theorem 5.1], strengthened Theorem 2.9 of [2] by implementing some techniques of M. Larsen and R. Schoof [12]. They proved that the coefficient associated with the point P is equal to 1. Nevertheless the coefficients associated with points $P_1, \ldots, P_r$ in [8, Theorem 5.1], are still in $\mathcal{R}$. Recently A. Perucca [13, Corollary 5], has proven Theorem 5.1 of [8] using her l-adic support problem result. At the end of this paper we reprove Theorem 5.1 of [8] by arguments presented in the proof of Theorem 1.1.

Although not explicitly presented in our proofs, this paper essentially applies results on Kummer Theory for abelian varieties, originally developed by K. Ribet [15], and results of F. Bogomolov [5], G. Faltings [7], J.-P. Serre and J. Tate [17], A. Weil [18], J. Zarhin [20] and other important results about abelian varieties. The application of these results comes by referring to [1,2,4,14] where Kummer Theory and the results of [5,7,17,18,20] are key ingredients.

2. Proof of Theorem 1.1

Let L/F be an extension of number fields. Let S_l be the following set of primes w in $\mathcal{O}_L$.

$$S_l := \{w:\ w|l\} \cup \{w:\ w|v \text{ for a prime } v \text{ of bad reduction for } A/F\}.$$

Let G_l denote the l-torsion part of an abelian group G. The reduction map,

$$r_w : A(L)_l \to A_w(k_w)_l,$$

is injective for every $w \notin S_l$ [10] pp. 501–502, [9] Theorem C.1.4 p. 263.

The following lemma is a result of S. Barańczuk which is a refinement of Theorem 3.1 of [2] and Proposition 2.2 of [3]. This is also a result of R. Pink [14, Corollary 4.3]. Recall [13, Proposition 2.2], that a nontorsion point $Q \in A(F)$ is independent over $\mathcal{R}$ if and only if the subgroup $\mathbb{Z}Q$ is Zariski dense in A.

Lemma 2.1. *([4], Th. 5.1, [14], Cor. 4.3.) Let l be a prime number. Let $m_1, \dots, m_s \in \mathbb{N} \cup \{0\}$. Let L/F be a finite extension and let $Q_1, \dots, Q_s \in A(L)$ be independent over $\mathcal{R}$. There is a family of primes w of $\mathcal{O}_L$ of positive density such that $r_w(Q_i)$ has order l^{m_i} in $A_w(k_w)_l$ for all $1 \leqslant i \leqslant s$.*

The following corollary follows also from [14], Theorem 4.1:

Corollary 2.2. *Let $m \in \mathbb{N}$. Let $Q_1, \dots, Q_s \in A(F)$ be independent over $\mathcal{R}$ and let $T_1, \dots, T_s \in A[l^m]$. Let $L := F(A[l^m])$. There is a family of primes w of $\mathcal{O}_L$ of positive density such that for the prime v of $\mathcal{O}_F$ below w:*

(1) $r_w(T_1), \dots, r_w(T_s) \in A_v(k_v) \subset A_w(k_w)$,
(2) $r_w(T_i) = r_v(Q_i)$ *in* $A_v(k_v)_l$ *for all* $1 \leqslant i \leqslant s$.

Proof. Observe that the points $Q_1 - T_1, \dots, Q_s - T_s$ are linearly independent over $\mathcal{R}$ in $A(L)$. Hence it follows by Lemma 2.1 that there is a family of primes w of $\mathcal{O}_L$ of positive density such that $r_w(Q_i - T_i) = 0$ in $A_w(k_w)_l$. Since $Q_1, \dots, Q_s \in A(F)$, it follows that $r_w(Q_i - T_i) = r_w(Q_i) - r_w(T_i) = r_v(Q_i) - r_w(T_i)$ for the prime v of $\mathcal{O}_F$ below w. Hence we get $r_w(T_i) = r_v(Q_i) \in A_v(k_v)_l$ for all $1 \leqslant i \leqslant s$. □

Proof of Theorem 1.1. It is enough to prove that (2) implies (1). By Theorem 2.9 [2] there is an $a \in \mathbb{N}$ and elements $\alpha_1, \dots, \alpha_r \in \mathcal{R}$ such that

$$aP = \sum_{i=1}^{r} \alpha_i P_i. \tag{1}$$

Step 1. Assume that $\alpha_i \in \mathbb{Z}$ for all $1 \leqslant i \leqslant r$. We will show (cf. the proof of Theorem 3.12 of [2]) that $P \in \sum_{i=1}^{r} \mathbb{Z} P_i$. Let l^k be the largest power of l that divides a. Lemma 2.1 shows that for any $1 \leqslant i \leqslant r$ there are infinitely many primes v such that $r_v(P_1) = \cdots = r_v(P_{i-1}) = r_v(P_{i+1}) = \cdots = r_v(P_r) = 0$ and $r_v(P_i)$ has order equal to l^k in $A_v(k_v)_l$. By (1) we obtain $ar_v(P) = \alpha_i r_v(P_i)$. Moreover by assumption (2) of the theorem, $r_v(P) = \beta_i r_v(P_i)$ for some $\beta_i \in \mathbb{Z}$. Hence

$$(\alpha_i - a\beta_i) r_v(P_i) = 0$$

in $A_v(k_v)_l$. This implies that l^k divides α_i for all $1 \leqslant i \leqslant r$. So by (1) we obtain:

$$\frac{a}{l^k} P = \sum_{i=1}^{r} \frac{\alpha_i}{l^k} P_i + T, \tag{2}$$

for some $T \in A(F)[l^k]$. Again, by Lemma 2.1 there are infinitely many primes v in $\mathcal{O}_F$ such that $r_v(P_i) = 0$ in $A_v(k_v)_l$ for all $1 \leqslant i \leqslant r$. In addition $r_v(P) \in \sum_{i=1}^{r} \mathbb{Z} r_v(P_i)$ for almost all v. So (2) implies that $r_v(T) = 0$, for infinitely many primes v. This contradicts the injectivity of r_v, unless $T = 0$. Hence,

$$\frac{a}{l^k} P = \sum_{i=1}^{r} \frac{\alpha_i}{l^k} P_i. \tag{3}$$

Repeating the above argument for primes dividing $\frac{a}{l^k}$ shows that condition (1) holds.
Step 2. Fix an embedding of F into $\mathbb{C}$. Assume $\alpha_i \notin \mathbb{Z}$ for some i. Observe that α_i is an endomorphism of the Riemann lattice $\mathcal{L}$, such that $A(\mathbb{C}) \cong \mathbb{C}^g / \mathcal{L}$. To make the notation simple, we will denote again by α_i the endomorphism $\alpha_i \otimes 1$ acting on $T_l(A) \cong \mathcal{L} \otimes \mathbb{Z}_l$. Let $P(t) := \det(t\,\mathrm{Id}_{\mathcal{L}} - \alpha_i) \in \mathbb{Z}[t]$, be the characteristic polynomial of α_i acting on $\mathcal{L}$. Let K be the splitting field of $P(t)$ over $\mathbb{Q}$. We take l such that it splits in K and l does not divide primes of bad reduction. Since $P(t)$ has all roots in $\mathcal{O}_K$ and is also the characteristic polynomial of α_i on $T_l(A)$, we see that $P(t)$ has all roots in $\mathbb{Z}_l$ by the assumption on l. If $P(t)$ has at least two different roots in $\mathcal{O}_K$, we easily find a vector $u \in T_l(A)$ which is not an eigenvector of α_i on $T_l(A)$. If $P(t)$ has a single root $\lambda \in \mathcal{O}_K$ then $P(t) = (t - \lambda)^{2g}$ and we must have $\lambda \in \mathbb{Z}$ because we are in characteristic 0. Hence $P(t) = (t - \lambda)^{2g}$ is the characteristic polynomial of α_i as an endomorphism of $\mathcal{L}$. Since $\alpha_i \notin \mathbb{Z}$ we find easily $u \in \mathcal{L}$ such that u is not an eigenvector of α_i acting on $T_l(A)$. In any case there is $u \in T_l(A)$ which is not an eigenvector of α_i acting on $T_l(A)$. Rescaling if necessary, we can assume that u is not divisible by l in $T_l(A)$. Hence for $m \in \mathbb{N}$ and m big enough we can see that the coset $u + l^m T_l(A)$ is not

an eigenvector of α_i acting on $T_l(A)/l^m T_l(A)$. Indeed, if $\alpha_i u \equiv c_m u \mod l^m T_l(A)$ for $c_m \in \mathbb{Z}/l^m$ for each $m \in \mathbb{N}$, then $c_{m+1} u \equiv c_m u \mod l^m T_l(A)$. Because u is not divisible by l in $T_l(A)$, this implies that $c_{m+1} \equiv c_m \mod l^m$ for each $m \in \mathbb{N}$. But this contradicts the fact that u is not an eigenvector of α_i acting on $T_l(A)$. Consider the natural isomorphism of Galois and $\mathcal{R}$ modules $T_l(A)/l^m T_l(A) \cong A[l^m]$. We put $T \in A[l^m]$ to be the image of the coset $u + l^m T_l(A)$ via this isomorphism. Put $L := F(A[l^m])$. By Corollary 2.2 we choose a prime v below a prime w of $\mathcal{O}_L$ such that

(i) $r_w(T) \in A_v(k_v)_l$,
(ii) $r_v(P_j) = 0$ for all $j \neq i$ and $r_v(P_i) = r_w(T)$ in $A_v(k_v)_l$.

From (1) and (ii) we get $ar_v(P) = \alpha_i r_v(P_i) = \alpha_i r_w(T)$ in $A_v(k_v)_l$. Hence for the prime w in $\mathcal{O}_L$ over v we get in $A_w(k_w)_l$ the following equality:

$$ar_w(P) = \alpha_i r_w(P_i) = \alpha_i r_w(T). \tag{4}$$

By assumption (2) and (ii) there is $d \in \mathbb{Z}$, such that $ar_v(P) = adr_v(P_i) = adr_w(T)$ in $A_v(k_v)_l$. Hence, for the prime w in $\mathcal{O}_L$ over v, we get in $A_w(k_w)_l$ the following equality:

$$ar_w(P) = adr_w(P_i) = adr_w(T). \tag{5}$$

Since r_w is injective, the equalities (4) and (5) give:

$$\alpha_i T = adT \quad \text{in } A\big[l^m\big].$$

But this contradicts the fact that T is not an eigenvector of α_i acting on $A[l^m]$. It proves that $\alpha_i \in \mathbb{Z}$ for all $1 \leqslant i \leqslant r$, but this case has already been taken care of in step 1 of our proof. □

Corollary 2.3. *Let A be a simple abelian variety. Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R}$. Let P be a nontorsion point of $A(F)$. The following conditions are equivalent*:

(1) $P \in \sum_{i=1}^r \mathbb{Z} P_i$,
(2) $r_v(P) \in \sum_{i=1}^r \mathbb{Z} r_v(P_i)$ *for almost all primes v of $\mathcal{O}_F$.*

Proof. This is an immediate consequence of Theorem 1.1. Indeed, for a nontorsion point P the $\mathcal{R}$-module $\mathcal{R}P$ is a free $\mathcal{R}$-module since $D = \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra because A is simple. □

Corollary 2.4. *Let A be a simple abelian variety. Let P and Q be nontorsion elements of $A(F)$. The following conditions are equivalent*:

(1) $P = mQ$ *for some $m \in \mathbb{Z}$,*
(2) $r_v(P) = m_v r_v(Q)$ *for some $m_v \in \mathbb{Z}$ for almost all primes v of $\mathcal{O}_F$.*

Proof. This is an immediate consequence of Corollary 2.6 because $\mathcal{R}Q$ is a free $\mathcal{R}$-module since A is simple. □

The following proposition is Theorem 5.1 of [8]. We give a new proof of this theorem using arguments presented in the proof of Theorem 1.1.

Proposition 2.5. *Let A be an abelian variety over F. Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R}$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$ module. The following conditions are equivalent*:

(1) $P \in \sum_{i=1}^r \mathcal{R} P_i$;
(2) $r_v(P) \in \sum_{i=1}^r \mathcal{R} r_v(P_i)$ *for almost all primes v of $\mathcal{O}_F$.*

Proof. Again we need to prove that (2) implies (1). Let us assume (2). By [2], Theorem 2.9 there is an $a \in \mathbb{N}$ and elements $\alpha_1, \ldots, \alpha_r \in \mathcal{R}$ such that equality (1) holds. Let l be a prime number such that $l^k || a$ for some $k > 0$. Put

$L := F(A[l^k])$ and take arbitrary $T \in A[l^k]$. By Corollary 2.2 we can choose a prime v below a prime w of $\mathcal{O}_L$ such that

(i) $r_w(T) \in A_v(k_v)_l$,
(ii) $r_v(P_j) = 0$ for all $j \neq i$ and $r_v(P_i) = r_w(T)$ in $A_v(k_v)_l$.

From (1) and (ii) we get $ar_v(P) = \alpha_i r_v(P_i) = \alpha_i r_w(T)$ in $A_v(k_v)_l$. Hence we have the following equality in $A_w(k_w)_l$:

$$ar_w(P) = \alpha_i r_w(P_i) = \alpha_i r_w(T). \tag{6}$$

By assumption (2) and (ii) there is $\delta \in \mathcal{R}$, such that $ar_v(P) = a\delta r_v(P_i) = a\delta r_w(T) = 0$ in $A_v(k_v)_l$. Hence we have the following equality in $A_w(k_w)_l$:

$$ar_w(P) = a\delta r_w(P_i) = a\delta r_w(T) = 0. \tag{7}$$

By injectivity of r_w, the equalities (6) and (7) imply:

$$\alpha_i T = 0 \quad \text{in } A\big[l^k\big].$$

This shows that α_i maps to zero in $\mathrm{End}_{G_F}(A[l^k])$. It is easy to observe that the natural map,

$$\mathcal{R}/l^k\mathcal{R} \to \mathrm{End}_{G_F}\big(A\big[l^k\big]\big),$$

is an embedding for every prime number l and every $k \in \mathbb{N}$. Recall [20, Corollary 5.4.5], that this map is an isomorphism for $l \gg 0$ and all $k \in \mathbb{N}$ cf. the proof of Lemma 2.2 of [2]. It follows that $\alpha_i \in l^k\mathcal{R}$ for all $1 \leqslant i \leqslant r$. So

$$\frac{a}{l^k} P = \sum_{i=1}^{r} \beta_i P_i + T', \tag{8}$$

where $T' \in A(F)[l^k]$ and $\beta_i \in \mathcal{R}$ for all $1 \leqslant i \leqslant r$. By Lemma 2.1 there are infinitely many primes v in $\mathcal{O}_F$ such that $r_v(P_i) = 0$ in $A_v(k_v)_l$ for all $1 \leqslant i \leqslant r$. In addition $r_v(P) \in \sum_{i=1}^{r} \mathcal{R} r_v(P_i)$ for almost all v. So (8) implies that $r_v(T') = 0$, for infinitely many primes v. Hence $T' = 0$ by the injectivity of r_v [10] pp. 501–502, [9] Theorem C.1.4 p. 263. Hence

$$\frac{a}{l^k} P = \sum_{i=1}^{r} \beta_i P_i. \tag{9}$$

Repeating the above argument for primes dividing $\frac{a}{l^k}$ finishes the proof of the proposition. □

3. Remark on Mordell–Weil $\mathcal{R}$ systems

Let $\mathcal{R}$ be a ring with identity. In the paper [1] the Mordell–Weil $\mathcal{R}$ systems have been defined. In [2] we investigated Mordell–Weil $\mathcal{R}$ systems satisfying certain natural axioms $A_1 - A_3$ and $B_1 - B_4$. We also assumed that $\mathcal{R}$ was a free $\mathbb{Z}$-module. Let us consider Mordell–Weil $\mathcal{R}$ systems which are associated to families of l-adic representations $\rho_l : G_F \to GL(T_l)$ such that $\rho_l(G_F)$ contains an open subgroup of homotheties. Since Theorem 2.9 of [2] and Theorem 5.1 of [4] were proven for Mordell–Weil $\mathcal{R}$ systems, then Proposition 2.8 and its proof generalize for the Mordell–Weil $\mathcal{R}$ systems. This shows that Theorem 2.9 of [2], which is stated for Mordell–Weil $\mathcal{R}$ systems, holds with $a = 1$. Let us also assume that there is a free $\mathbb{Z}$-module $\mathcal{L}$ such that $\mathcal{R} \subset \mathrm{End}_{\mathbb{Z}}(\mathcal{L})$ and for each l there is an isomorphism $\mathcal{L} \otimes \mathbb{Z}_l \cong T_l$ such that the action of $\mathcal{R}$ on T_l comes from its action on $\mathcal{L}$. Abelian varieties are principal examples of Mordell–Weil $\mathcal{R}$ systems satisfying all the requirements stated above with $\mathcal{R} = \mathrm{End}_F(A)$. Then Theorem 1.1 generalizes also for Mordell–Weil $\mathcal{R}$ systems satisfying the above assumptions because we can apply again Theorem 2.9 of [2] and Theorem 5.1 of [4].

Acknowledgements

The author would like to thank the referees for valuable comments and suggestions. The research was partially financed by the research grant N N201 1739 33 of the Polish Ministry of Science and Education and the grant MRTN-CT-2003-504917 of the Marie Curie Research Training Network "Arithmetic Algebraic Geometry".

References

[1] G. Banaszak, W. Gajda, P. Krasoń, Support problem for the intermediate Jacobians of l-adic representations, J. Number Theory 100 (1) (2003) 133–168.

[2] G. Banaszak, W. Gajda, P. Krasoń, Detecting linear dependence by reduction maps, J. Number Theory 115 (2) (2005) 322–342.

[3] G. Banaszak, W. Gajda, P. Krasoń, On reduction map for étale K-theory of curves, in: Proceedings of Victor's Snaith 60th Birthday Conference, Homology Homotopy Appl. 7 (3) (2005) 1–10.

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

[5] F.A. Bogomolov, Sur l'algébricité des représentations l-adiques, C. R. Acad. Sci. Paris Sér. A-B 290 (1980) A701–A703.

[6] C. Corralez-Rodrigáñez, R. Schoof, Support problem and its elliptic analogue, J. Number Theory 64 (1997) 276–290.

[7] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983) 349–366.

[8] W. Gajda, K. Górnisiewicz, Linear dependence in Mordell–Weil groups, J. Reine Angew. Math., in press.

[9] M. Hindry, J.H. Silverman, Diophantine Geometry an Introduction, Graduate Texts in Math., vol. 201, Springer, 2000.

[10] N.M. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981) 481–502.

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

[12] M. Larsen, R. Schoof, Whitehead's lemmas and Galois cohomology of abelian varieties, preprint.

[13] A. Perucca, The l-adic support problem for abelian varieties, preprint, 2007.

[14] R. Pink, On the order of the reduction of a point on an abelian variety, Math. Ann. 330 (2004) 275–291.

[15] K.A. Ribet, Kummer theory on extensions of abelian varieties by tori, Duke Math. J. 46 (4) (1979) 745–761.

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

[17] J.-P. Serre, J. Tate, Good reduction of abelian varieties, Ann. of Math. 68 (1968) 492–517.

[18] A. Weil, Variétés Abélienne et Courbes Algébriques, Hermann, Paris, 1948.

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

[20] J.G. Zarhin, A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction, Invent. Math. 79 (1985) 309–321.