Le problème du support pour les variétés abéliennes, d'après Larsen

Olivier Wittenberg

21 novembre 2003

Résumé

Ce document contient les notes d'un exposé au séminaire Variétés rationnelles (Paris) de novembre 2003.

1 Introduction

L'histoire du problème du support commence à Banff en 1988, lorsque Paul Erdös pose la question suivante :

Question — *Que peut-on dire de deux entiers $a, b > 1$ tels que le support de $a^n - 1$ soit inclus dans celui de $b^n - 1$ pour tout $n \geqslant 1$? (On entend ici par* support *d'un entier l'ensemble de ses diviseurs premiers.) Notamment, si $a^n - 1$ et $b^n - 1$ ont même support pour tout $n \geqslant 1$, peut-on en déduire que $a = b$?*

Voici un résultat relativement élémentaire qui constitue une motivation possible pour la question d'Erdös.

Proposition 1.1 — *Si a et b sont deux entiers strictement positifs tels que $a^n - 1$ divise $b^n - 1$ pour tout $n \geqslant 1$, b est une puissance de a.*

Démonstration — Exercice. □

Le problème du support fut résolu en 1997 par Corrales-Rodrigáñez et Schoof [2].

Théorème 1.2 (Corrales-Rodrigáñez, Schoof, 1997) — *Soit k un corps de nombres. Soient $x, y \in k^\star$ tels que pour presque toute[*] place finie $\mathfrak{p}$ de k, pour tout $n \geqslant 1$ on ait l'implication*

$$x^n \equiv 1 \pmod{\mathfrak{p}} \implies y^n \equiv 1 \pmod{\mathfrak{p}}.$$

Alors y est une puissance de x.

Si l'on remplace l'implication par une équivalence dans les hypothèses de ce théorème, on conclut que l'un des trois cas suivants se présentent : $y = x$, $y = 1/x$, ou x et y sont des racines de l'unité ; ainsi la question d'Erdös admet-elle une réponse affirmative.

Un certain nombre d'auteurs ont étudié des généralisations de la proposition 1.1. Par exemple, Corvaja et Zannier [3] ont prouvé que la conclusion reste valide si l'on suppose seulement que $a^n - 1$ divise $b^n - 1$ pour une infinité de valeurs de n. Citons encore les travaux de van der Poorten [6] sur le théorème des quotients de Hadamard, vaste généralisation de la proposition 1.1. Enfin, quelques articles récents portent sur l'étude du pgcd de $a^n - 1$ et de $b^n - 1$ lorsque a et b sont multiplicativement indépendants (Bugeaud, Corvaja, Zannier, Ailon, Rudnick, etc.).

Une autre direction possible est celle consistant à généraliser le problème du support lui-même. On peut le voir comme un énoncé portant sur les points rationnels du groupe multiplicatif, d'où une question analogue pour tout groupe algébrique. Dans le cas des courbes elliptiques, Corrales-Rodrigáñez et Schoof ont encore obtenu une réponse positive.

Théorème 1.3 (Corrales-Rodrigáñez, Schoof, 1997) — *Soient k un corps de nombres, E une courbe elliptique sur k et $P, Q \in E(k)$ tels que pour presque toute place finie $\mathfrak{p}$ de k, pour tout $n \geqslant 1$ on ait l'implication*

$$nP \equiv 0 \pmod{\mathfrak{p}} \implies nQ \equiv 0 \pmod{\mathfrak{p}}.$$

Alors soit P et Q sont de torsion, soit il existe $\varphi \in \mathrm{End}_k(E)$ tel que $\varphi(P) = Q$.

[*] Dans ce document, « presque tout » signifiera toujours « tout sauf un nombre fini ».

La preuve est modelée sur celle du théorème 1.2, mais elle est nettement plus longue. Elle distingue notamment deux cas, selon que E est à multiplication complexe ou non.

Plusieurs auteurs ont récemment établi des énoncés analogues au théorème 1.3 en remplaçant E par une variété abélienne. Soient k un corps de nombres et A une variété abélienne sur k. Notons $\overline{k}$ une clôture algébrique de k. Soient $P, Q \in A(k)$ tels que pour presque toute place finie $\mathfrak{p}$ de k, pour tout $n \geqslant 1$ on ait l'implication

$$nP \equiv 0 \pmod{\mathfrak{p}} \implies nQ \equiv 0 \pmod{\mathfrak{p}}.$$

Théorème 1.4 (Khare, Prasad, 2002) — *Supposons que* $\mathrm{End}_{\overline{k}}(A) = \mathbf{Z}$ *et que* $\dim A$ *soit impair ou égal à* 2 *ou à* 6. *Alors soit* P *et* Q *sont de torsion, soit il existe* $\varphi \in \mathrm{End}_k(A)$ *tel que* $\varphi(P) = Q$.

Banaszak, Gajda et Krasón établissent dans [1] la même conclusion dans un certain nombre d'autres cas définis par des hypothèses très techniques sur A. Leurs résultats présentent l'avantage de s'énoncer dans un cadre plus général que celui des variétés abéliennes, ce qui leur permet d'obtenir par exemple un analogue des théorèmes 1.2 et 1.3 pour la K-théorie de Quillen de k.

Plus récemment, Larsen a prouvé, sans aucune hypothèse sur A :

Théorème 1.5 (Larsen, 2003, [5]) — *Il existe* $s \in \mathbf{N}^\star$ *et* $\varphi \in \mathrm{End}_k(A)$ *tels que* $\varphi(P) = sQ$.

Proposition 1.6 — *On ne peut pas toujours choisir* $s = 1$ *dans le théorème précédent.*

Ceci résout essentiellement la question du problème du support pour les variétés abéliennes. C'est à la preuve du théorème 1.5 que la troisième section de ce document sera consacrée.

Démontrons tout de suite la proposition 1.6. Soient k un corps de nombres et E une courbe elliptique sur k sans multiplication complexe (i.e. telle que $\mathrm{End}_{\overline{k}}(E) = \mathbf{Z}$), de rang non nul, et dont les points de 2-torsion soient k-rationnels. Notons T_1 et T_2 deux points distincts d'ordre 2 de $E(k)$ et $R \in E(k)$ un point d'ordre infini. On vérifie facilement que les hypothèses du théorème sont satisfaites avec $A = E \times_k E$, $P = (R, R + T_1)$ et $Q = (R, R + T_2)$, mais qu'il n'existe pas de $\varphi \in \mathrm{End}_k(A) = \mathcal{M}_2(\mathbf{Z})$ tel que $\varphi(P) = Q$. Pour trouver explicitement une telle courbe elliptique, on peut procéder comme suit. Partons d'une équation de Weierstrass sous la forme de Legendre, soit

$$E\colon y^2 = x(x-1)(x-\lambda)$$

avec $\lambda \in \mathbf{Q}^\star \setminus \{1\}$. Les points de 2-torsion sont évidemment $\mathbf{Q}$-rationnels. Pour assurer que E n'a pas de multiplication complexe, il suffit de choisir λ de telle sorte que l'invariant j ne soit pas entier ; par exemple $\lambda = 5$ convient. Il ne reste plus qu'à choisir k assez grand pour que $E(k)$ soit infini.

Ce contre-exemple soulève une dernière question : peut-on toujours choisir $s = 1$ si l'on suppose la variété abélienne A simple[†] ?

2 Ingrédients

Commençons par rappeler quelques théorèmes sur les représentations ℓ-adiques des variétés abéliennes utilisés dans [1], [4], [5], ou dans la suite de ce texte.

Soit ℓ un nombre premier. Si B est un groupe (resp. groupe algébrique) commutatif et N un entier, $B[N]$ désigne le noyau de la multiplication par N dans B. On note $T_\ell(A) = \varprojlim A[\ell^n](\overline{k})$ le module de Tate ℓ-adique de la variété abélienne A ; c'est un $\mathbf{Z}_\ell$-module libre de rang $2\dim A$. L'action naturelle du groupe de Galois absolu $G = \mathrm{Gal}(\overline{k}/k)$ sur $T_\ell(A)$ fournit un morphisme continu $\rho\colon G \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(A))$.

Théorème 2.7 (Faltings) — *Le* $\mathbf{Q}_\ell[G]$*-module* $T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ *est semi-simple. De plus, l'application naturelle* $\mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \to \mathrm{End}_{\mathbf{Z}_\ell[G]}(T_\ell(A))$ *est bijective.*

Le théorème suivant nous sera utile dans la preuve du théorème 1.5, bien qu'il n'apparaisse dans aucun des trois articles [1], [4] et [5]. On peut en trouver une preuve dans [7]. La cohomologie dont il est question est bien entendu celle des $\rho(G)$-modules topologiques (par opposition aux $\rho(G)$-modules discrets).

Théorème 2.8 (Serre) — *Pour tout* $n \in \mathbf{N}$, *le groupe* $H^n(\rho(G), T_\ell(A))$ *est un* ℓ*-groupe fini.*

[†]Mise à jour au 01/01/2004 : C. Khare et D. Prasad ont récemment apporté une réponse positive à cette dernière question. La preuve sera incluse dans la version publiée de [4].

Il existe des conjectures profondes très précises sur l'image de ρ, qui est un groupe de Lie ℓ-adique, et notamment sur ce que doit être son adhérence pour la topologie de Zariski. Nous nous bornerons ici à mentionner quelques théorèmes qui s'énoncent en termes élémentaires.

Si A est une courbe elliptique sans multiplication complexe, Serre a prouvé que ρ est surjectif pour ℓ assez grand. En dimension supérieure, on ne peut espérer un tel résultat. En effet, l'accouplement de Weil et le choix d'une polarisation sur A déterminent une forme bilinéaire alternée $e\colon T_\ell(A)\times T_\ell(A)\to \mathbf{Z}_\ell(1)$, non dégénérée pour ℓ assez grand. Cette forme est de plus G-équivariante, de sorte que ρ se factorise par le groupe $\mathrm{GSp}(T_\ell(A))$ des similitudes symplectiques de $(T_\ell(A), e)$. On a cependant :

Théorème 2.9 (Serre) — *Si* $\mathrm{End}_{\overline{k}}(A)=\mathbf{Z}$ *et si la dimension de* A *est impaire ou égale à* 2 *ou à* 6*, l'image de* ρ *est* $\mathrm{GSp}(T_\ell(A))$ *pour* ℓ *assez grand.*

C'est de là que viennent les hypothèses du théorème 1.4.

Théorème 2.10 (Bogomolov) — *Quel que soit le nombre premier* ℓ*,* $\rho(G)$ *contient un ouvert du groupe des homothéties.*

Le théorème de Bogomolov ne concerne que les homothéties mais présente l'avantage de n'être soumis à aucune hypothèse. On est cependant encore loin de la conjecture de Lang, selon laquelle pour ℓ assez grand, $\rho(G)$ doit contenir *toutes* les homothéties.

3 Preuve du théorème 1.5

Toutes les notations introduites ci-dessus (notamment k, $\overline{k}$, G, A, ρ, P et Q) sont conservées. Le nombre premier ℓ est fixé, par exemple par $\ell=2$. Lorsque S est une partie de $A(\overline{k})$, on notera $k(S)$ le sous-corps de $\overline{k}$ formé des éléments laissés invariants par tous les $g\in G$ qui agissent trivialement sur S. Si S est finie (resp. stable par G), l'extension $k(S)/k$ est finie (resp. galoisienne). Si M est un groupe abélien, on note $M[\ell^\infty]$ la partie ℓ-primaire de M. Soient $K=k(A(\overline{k})[\ell^\infty])$ et $G_K=\mathrm{Gal}(\overline{k}/K)=\mathrm{Ker}(\rho)$.

Pour tout $n\in\mathbf{N}$, la suite de Kummer

$$0\longrightarrow A[\ell^n]\longrightarrow A\xrightarrow{\ell^n} A\longrightarrow 0$$

induit par passage aux points k-rationnels une injection $A(k)\otimes_{\mathbf{Z}}\mathbf{Z}/\ell^n\mathbf{Z}\hookrightarrow H^1(k,A[\ell^n])$. Comme $A(k)$ est un groupe abélien de type fini, on en déduit une injection $A(k)\otimes_{\mathbf{Z}}\mathbf{Z}_\ell\hookrightarrow \varprojlim H^1(k,A[\ell^n])$. De plus, $H^0(k,A[\ell^n])$ est un groupe fini pour tout $n\in\mathbf{N}$, de sorte que[‡] l'on a $\varprojlim H^1(k,A[\ell^n])=H^1(k,T_\ell(A))$. Composons l'injection $A(k)\otimes_{\mathbf{Z}}\mathbf{Z}_\ell\hookrightarrow H^1(k,T_\ell(A))$ ainsi obtenue avec l'homomorphisme de restriction $H^1(k,T_\ell(A))\to H^1(K,T_\ell(A))=\mathrm{Hom}_{\mathrm{cont}}(G_K,T_\ell(A))=\mathrm{Hom}_{\mathrm{cont}}(G_K^{\mathrm{ab}},T_\ell(A))$, où G_K^{ab} désigne le quotient de G_K par l'adhérence de son sous-groupe dérivé, et notons

$$f\colon A(k)\otimes_{\mathbf{Z}}\mathbf{Z}_\ell\longrightarrow \mathrm{Hom}_{\mathrm{cont}}(G_K,T_\ell(A))^{\mathrm{Gal}(K/k)}$$

la flèche qui en résulte.

Supposons dans un premier temps que $\mathrm{Ker}(f(P))\subset\mathrm{Ker}(f(Q))$. Il existe donc une unique application $\mathbf{Z}$-linéaire γ_0 rendant le diagramme suivant commutatif :

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ker}(f(P)) & \longrightarrow & G_K^{\mathrm{ab}} & \xrightarrow{f(P)} & \mathrm{Im}(f(P)) \longrightarrow 0 \\ & & & & \downarrow{\scriptstyle f(Q)} & \swarrow{\scriptstyle \gamma_0} & \\ & & & & T_\ell(A) & & \end{array}$$

Munissons le groupe $\mathrm{Im}(f(P))$ de la topologie induite par $T_\ell(A)$, de sorte que $f(P)$ soit continue. Comme G_K^{ab} est compact, $\mathrm{Im}(T_\ell(A))$ est un sous-groupe fermé de $T_\ell(A)$; c'en est donc un sous-$\mathbf{Z}_\ell$-module. Pour que γ_0 soit $\mathbf{Z}_\ell$-linéaire, il suffit que ce soit une application continue, et pour cela il suffit que l'application $G_K^{\mathrm{ab}}\to\mathrm{Im}(f(P))$ soit ouverte (une application surjective et ouverte est un épimorphisme strict dans la

[‡]Pour tout système projectif (M_n) indexé par $\mathbf{N}$ de G-modules topologiques, on a pour tout $i\in\mathbf{N}$ une suite exacte

$$0\longrightarrow \varprojlim{}^1 H^i(G,M_n)\longrightarrow H^{i+1}(G,\varprojlim M_n)\longrightarrow \varprojlim H^{i+1}(G,M_n)\longrightarrow 0,$$

où $\varprojlim^1$ désigne le premier foncteur dérivé à droite de $\varprojlim$.

catégorie des espaces topologiques). Cette dernière condition est bien vérifiée : tout morphisme continu et surjectif entre groupes profinis est ouvert. (Preuve : comme les sous-groupes ouverts forment une base de voisinages du neutre dans un groupe profini, il suffit de voir que l'image d'un sous-groupe ouvert est ouvert ; or l'image d'un tel sous-groupe est fermée (compacité) et d'indice fini.)

Comme $f(P)$ est une application $\mathrm{Gal}(K/k)$-équivariante, $\mathrm{Im}(f(P))$ est stable sous G et est donc un sous-$\mathbf{Z}_\ell[G]$-module de $T_\ell(A)$. Le théorème de Faltings assure que c'en est presque un facteur direct : il existe un entier naturel n et une application $\mathbf{Z}_\ell[G]$-linéaire $\gamma_1 \colon T_\ell(A) \to \mathrm{Im}(f(P))$ tels que la composée de l'inclusion $\mathrm{Im}(f(P)) \subset T_\ell(A)$ et de γ_1 soit la multiplication par ℓ^n sur $\mathrm{Im}(f(P))$.

Posons $\gamma = \gamma_0 \circ \gamma_1$. C'est un $\mathbf{Z}_\ell[G]$-endomorphisme de $T_\ell(A)$; le théorème de Faltings garantit qu'il provient d'un $\varphi \in \mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$. On vérifie tout de suite que $\gamma \circ (f(P)) = f(\ell^n Q)$. De plus, il découle immédiatement de la fonctorialité de la suite de Kummer que $\gamma \circ (f(P)) = f(\varphi(P))$, $\varphi(P)$ désignant ici l'élément de $A(k) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ image de P par φ. Ainsi, $\varphi(P) - \ell^n Q \in \mathrm{Ker}(f)$.

Proposition 3.11 — *Le noyau de f est un ℓ-groupe fini.*

Démonstration — Comme la flèche $A(k) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \to H^1(k, T_\ell(A))$ intervenant dans la définition de f est injective, $\mathrm{Ker}(f)$ est inclus dans le noyau de l'homomorphisme de restriction $H^1(k, T_\ell(A)) \to H^1(K, T_\ell(A))$, dont la suite exacte d'inflation-restriction montre qu'il est canoniquement isomorphe à $H^1(\rho(G), T_\ell(A))$. Le théorème 2.8 permet de conclure. □

Il existe donc $N \in \mathbf{N}$ tel que $\ell^{n+N} Q = \ell^N \varphi(P)$ dans $A(k) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$. Autrement dit, en notant φ_j un endomorphisme de A congru à φ modulo ℓ^j, on a $\ell^{n+N} Q \equiv \ell^N \varphi_j(P) \pmod{\ell^j}$ pour tout $j \in \mathbf{N}$. L'image de $\ell^{n+N} Q$ dans le groupe B quotient de $A(k)$ par $\{\psi(P) \,;\, \psi \in \mathrm{End}_k(A)\}$ est donc divisible par des puissances arbitrairement grandes de ℓ. Le groupe B étant abélien de type fini, ceci signifie que l'image de $\ell^{n+N} Q$ dans B est de torsion, ce qui est exactement la conclusion recherchée.

Il reste à traiter le cas où $\mathrm{Ker}(f(P)) \not\subset \mathrm{Ker}(f(Q))$. Pour $R \in \{P, Q\}$, soit $R_\infty = (R_n)_{n \in \mathbf{N}}$ une famille de $\overline{k}$-points de A vérifiant $R_0 = R$ et $\ell R_{n+1} = R_n$. Il n'est pas difficile d'expliciter $f(R)$: pour $\sigma \in G_K$, on a $f(R)(\sigma) = \sigma(R_\infty) - R_\infty$. L'hypothèse se traduit ainsi par l'existence d'un $\sigma \in G_K$ tel que $\sigma(P_\infty) = P_\infty$ mais $\sigma(Q_\infty) \neq Q_\infty$. Fixons $n \in \mathbf{N}$ tel que $\sigma(Q_n) \neq Q_n$.

Proposition 3.12 — *Il existe $N \geqslant n$ et $\tau \in G$ tels que $\tau(P_n) = P_n$, $\tau(Q_n) \neq Q_n$ et $\rho(\tau) \in 1 + \ell^N \mathbf{Z}_\ell^\star$, i.e. τ agit sur $T_\ell(A)$ par une homothétie congrue à 1 modulo ℓ^N mais non congrue à 1 modulo ℓ^{N+1}.*

Démonstration — D'après le théorème de Bogomolov, il existe $g \in G$ tel que $\rho(g) \in 1 + \ell \mathbf{Z}_\ell$ mais $\rho(g) \neq 1$. Soit $m \in \mathbf{N}^\star$ tel que g^m agisse trivialement sur P_n et sur $\sigma(Q_n)$ (prendre par exemple pour m le degré de l'extension galoisienne $k(P_n, \sigma(Q_n), A[\ell^n](\overline{k}))/k)$. Soit k un entier. Posons $\tau = g^{m\ell^k} \sigma$. Il existe un unique $N \in \mathbf{N}$ tel que $\rho(\tau) \in 1 + \ell^N \mathbf{Z}_\ell^\star$ (rappel : $\rho(\sigma) = 1$) ; si k est assez grand, on aura $N \geqslant n$ et τ conviendra bien. □

Considérons maintenant l'extension finie galoisienne $L = k(P_n, Q_n, A[\ell^{N+1}](\overline{k}))$ de k. Le théorème de Čebotarev fournit une place finie $\mathfrak{p}$ de k de bonne réduction pour A, ne divisant pas ℓ, non ramifiée dans L, et telle que l'image de τ dans $\mathrm{Gal}(L/k)$ soit le Frobenius en une place $\mathfrak{P}$ de L au-dessus de $\mathfrak{p}$. Notons $D \subset \mathrm{Gal}(L/k)$ le sous-groupe de décomposition en $\mathfrak{P}$, $\kappa(\mathfrak{p})$ (resp. $\kappa(\mathfrak{P})$) le corps résiduel de $\mathfrak{p}$ (resp. $\mathfrak{P}$), et A_0 la variété abélienne sur $\kappa(\mathfrak{p})$ qui se déduit de A par réduction modulo $\mathfrak{p}$. On dispose d'un morphisme de réduction D-équivariant $r \colon A(L) \to A_0(\kappa(\mathfrak{P}))$ dont la restriction à la partie ℓ-primaire est injective puisque $\mathfrak{p}$ ne divise pas ℓ. En particulier, comme toute la ℓ^{N+1}-torsion de A est L-rationnelle, $A_0(\kappa(\mathfrak{P}))$ contient un sous-groupe isomorphe à $(\mathbf{Z}/\ell^{N+1}\mathbf{Z})^{2 \dim A}$. Pour une raison de cardinalité, ce sous-groupe est nécessairement égal à $A_0(\kappa(\mathfrak{P}))[\ell^{N+1}]$. Comme le Frobenius agit trivialement sur $A_0(\kappa(\mathfrak{P}))[\ell^N]$ et par une homothétie non triviale sur $A_0(\kappa(\mathfrak{P}))[\ell^{N+1}]$, on en déduit que la partie ℓ-primaire de $A_0(\kappa(\mathfrak{p}))$ est exactement $A_0(\kappa(\mathfrak{P}))[\ell^N]$. Il existe donc un groupe fini B tel que

$$A_0(\kappa(\mathfrak{p})) \approx (\mathbf{Z}/\ell^N \mathbf{Z})^{2 \dim A} \times B.$$

Notons b l'ordre de B. Le Frobenius agit trivialement sur $r(P_n)$; $r(P)$ est donc divisible par ℓ^n dans $A_0(\kappa(\mathfrak{p}))$. Ce n'est en revanche pas le cas de $r(Q)$. En effet, étant donné que $A_0(\kappa(\mathfrak{P}))[\ell^n] \subset A_0(\kappa(\mathfrak{p}))$, cela forcerait $r(Q_n)$ à être $\kappa(\mathfrak{p})$-rationnel. L'hypothèse sur les ordres de $r(P)$ et de $r(Q)$ est maintenant contredite, puisque $b\ell^{N-n} P \equiv 0 \pmod{\mathfrak{p}}$ mais $b\ell^{N-n} Q \not\equiv 0 \pmod{\mathfrak{p}}$. Ceci termine la preuve du théorème 1.5.

Remarque — La preuve donnée dans [5] fait appel à un théorème de Serre selon lequel l'indice de $\rho(G) \cap \mathbf{Z}_\ell^\star$ dans $\mathbf{Z}_\ell^\star$, fini d'après Bogomolov, est borné indépendamment de ℓ (cours au Collège de France, 1985-1986). La démonstration qu'en donne Serre n'est malheureusement qu'une esquisse. La preuve exposée ci-dessus est inspirée d'un article en préparation de Larsen et Schoof, dans lequel une variante du théorème 1.5 est démontrée.

Bibliographie

[1] G. Banaszak, W. Gajda, P. Krasón, Support problem for the intermediate Jacobians of l-adic representations, *J. Number Theory* **100** (2003), no. 1, 133–168.

[2] C. Corrales-Rodrigáñez, R. Schoof, The support problem and its elliptic analogue, *J. Number Theory* **64** (1997), no. 2, 276–290.

[3] P. Corvaja, U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Math. (N.S.)* **9** (1998), no. 3, 317–332.

[4] C. Khare, D. Prasad, Reduction of homomorphisms mod p and algebraicity, à paraître au *J. Number Theory*.

[5] M. Larsen, The support problem for abelian varieties, *J. Number Theory* **101** (2003), no. 2, 398–403.

[6] A. J. van der Poorten, Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, *C. R. Acad. Sci. Paris Sér. I Math.* **306** (1988), no. 3, 97–102.

[7] J-P. Serre, Sur les groupes de congruence des variétés abéliennes II, *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 731–737.