Mathematical Research Letters **3**, 787–791 (1996)

INTEGRALITY OF TORSION POINTS ON ABELIAN VARIETIES OVER p-ADIC FIELDS

José Felipe Voloch

A classical result of Lutz and Nagell states that the rational torsion points of an elliptic curve given by a Weierstrass equation with integer coefficients are integral points. This is actually a p-adic result and can be proved one prime at a time. This was extended by Cassels to other local fields and in the case the field is ramified over $\mathbb{Q}_p$, he showed that the coordinates of torsion points have bounded denominators and are integral unless their order is a power of p. The purpose of this paper is to discuss extensions of these results to abelian varieties.

J. Tate and the author made the following conjecture in [TV]: Let A be a semiabelian variety over $\mathbb{C}_p$ and X a closed subvariety. There is a lower bound $c > 0$ for the p-adic distance (in the sense of [S]) of torsion points on A, not in X, to X. If X is an ample divisor, the conjecture implies that the torsion points of A in $A \setminus X$ have bounded (p-adic) denominators for any affine embedding of $A \setminus X$. For a linear torus, the conjecture was proved in [TV]. If $A/\bar{\mathbb{Q}}_p$ has good reduction and the Frobenius endomorphism of the reduction lifts to an endomorphism of A, Buium [Bu2] has proved the weaker version of this conjecture in which one considers only those torsion points fixed by some power of the lift of Frobenius. In this note, we will show that the conjecture holds in the case that $A/\bar{\mathbb{Q}}_p$ has good reduction and the Frobenius endomorphism of the reduction lifts to an endomorphism of A, by reducing the statement to the result proved by Buium. The reduction will be accomplished by modifying a method of Boxall [B1,2], to prove the weaker version of the conjecture in which one considers only those torsion points in the formal group of A but with no assumption on A (but we will actually need a version of this which is uniform on the degree of X, see theorem 1).

We note that Raynaud ([R]), for curves and Boxall and Hrushovski ([B3],[H]), in general have proved that is a lower bound $c > 0$ for the

Received October 25, 1996.

p-adic distance of prime-to-p torsion points on A, not in X, to X, assuming only that A has good reduction. Buium ([Bu1]) extended Raynaud's result for curves by allowing all torsion points in an unramified extension of $\mathbb{Q}_p$. Unfortunately, we need the existence of the lift of Frobenius in another step of our proof, so we are not able to use these more general results. Hopefully, they might lead to a proof of the full conjecture in the future.

Theorem 1. *Let A be a semiabelian variety defined over a p-adic field of bounded ramification K, with a given polarization and X a closed subvariety of A defined over K. Then there exists $c > 0$ depending only on the degree of X (with respect to the polarization) such that, for every torsion point Q of the formal group of A, either $d(Q, X) \geq c$ or Q belongs to a finite set of order bounded solely in terms of the degree of X.*

Proof. We proceed by induction on the dimension of X. If X has dimension zero, then X consists of a finite set of points defined over a finite extension F/K. If Q is of large p-power order in the formal group then $d(Q, 0)$ is close to, but smaller than, 1 by lemma 1 below. On the other hand, the values of $d(S, 0)$, for S in $A(F)$ which are smaller than 1 are smaller than some c, $0 < c < 1$. It follows that, for any $S \in A(F)$, $d(S, 0)$ is different from $d(Q, 0)$ if the order of Q is large enough. Hence by the ultrametric inequality $d(Q, S) = \max\{d(S, 0), d(Q, 0)\} \geq d(Q, 0) \geq c$, say.

By taking the quotient of A by the connected component of 0 of the stabilizer of X, if this stabilizer is positive dimensional, we reduce the problem to a lower dimensional variety so we may assume that X has finite stabilizer. By [B1], lemma 4, the stabilizer of X has order bounded in terms of the degree of X. Suppose Q is a torsion point of large order in the formal group of A close to X, then Q is of p-power order and we may find, by lemma 2 below, an element s of the absolute Galois group of K, such that $s(Q) - Q \in A[p^r] \setminus A[p^{r-1}]$, where r is chosen large enough so that $A[p^r] \setminus A[p^{r-1}]$ does not contain any element of the stabilizer of X. Now Q close to X implies that $s(Q)$ is also close to X. Writing $s(Q) = s(Q) - Q + Q$ we get Q close to $X - (s(Q) - Q)$. Therefore Q is close to the intersection of X and $X - (s(Q) - Q)$ which is a variety of smaller dimension, whose degree is bounded in terms of the degree of X and the theorem follows by induction.

Lemma 1. *Let $\mathcal{F}$ be a formal group over $\mathbb{C}_p$ and $\mathcal{M}$ the maximal ideal of the ring of integers of $\mathbb{C}_p$. If P_r is a point of order p^r of $\mathcal{F}$ with coordinates in $\mathcal{M}$, for $r \geq 1$, then the maximum of the absolute values of the coordinates of P_r tends to 1 (from below) as r tends to infinity.*

Proof. Let n be the dimension of $\mathcal{F}$. Normalize the distance of $P \in \mathcal{M}^n$ to 0 by $d(P, 0) = |P| = \max\{|x_i|\}$, where $P = (x_1, \ldots, x_n)$ and the absolute value is normalized by $|p| = 1/p$. Now, multiplication by p in $\mathcal{F}$ is given by power series $g_1, \dots, g_n$ in the variables $x_1, \dots, x_n$, with $g_i = px_i + \cdots$ and g_i congruent modulo p to a power series in $x_1^p, \dots, x_n^p$, because multiplication by p factors through Frobenius in characteristic p. It follows from this the inequality $|[p]P| \le \max\{|P|/p, |P|^p\}$ and when $|P| < p^{-1/(p-1)}$ we actually get $|[p]P| = |P|/p$. It follows first that, in the disk $|P| < p^{-1/(p-1)}$, there are no torsion points. Outside this disk, we get $|[p]P| \le |P|^p$. So if P_r is a sequence with $[p]P_r = P_{r-1}$ and $|P_1| \ge p^{-1/(p-1)}$ (say, P_1 is p-torsion) then it follows that $|P_r| \ge |P_1|^{1/p^r}$ which tends to 1 as r tends to infinity.

The next lemma is similar to lemma 1 of [B1,2] and its proof is based on a proof of Boxall's result shown to me by R. Coleman.

Lemma 2. *Let A be a semiabelian variety defined over a field K of characteristic different from p and let $F = K(A[p^r])$, where r is a positive integer and $r \neq 1$ if $p = 2$. Suppose P is a point in A is of p-power order but is not defined over F. Then there exists s in the absolute Galois group of F such that $s(P) - P \in A[p^r] \setminus A[p^{r-1}]$.*

Proof. Suppose $p^nP \in A(F)$ and n is minimal. Let $P_i = p^{n-i-r+1}P$ and choose s_1 in $\mathrm{Gal}(\bar{F}/F)$ with $s_1(p^{n-1}P) \neq p^{n-1}P$, which exists by definition of n. Let also $s_i = s_1^{p^{i-1}}$ and $Q_i = s_i(P_i) - P_i$. We will prove by induction on i that $Q_i \in A[p^r] \setminus A[p^{r-1}]$. Then s_{n-r+1} will prove our lemma, since $P_{n-r+1} = P$. For $i = 1, p^rQ_1 = s_1(p^nP) - p^nP = 0$ and $p^{r-1}Q_1 = s_1(p^{n-1}P) - p^{n-1}P \neq 0$, by construction. Now let $i > 1$. First we will show that $s_i^j(P_i) - P_i = jQ_i, j \ge 1$. This holds for $j = 1$ by definition and assuming it holds for j we get:

$$s_i^{j+1}(P_i) - P_i = s_i^{j+1}(P_i) - s_i(P_i) + s_i(P_i) - P_i = s_i(jQ_i) + Q_i = (j+1)Q_i,$$

as claimed. For $j = p$ this gives $s_i^p(P_i) - P_i = pQ_i \in A[p^{r-1}]$, by the induction hypothesis. Now, $pQ_{i+1} = p(s_{i+1}(P_{i+1}) - P_{i+1}) = s_i^p(P_i) - P_i \in A[p^{r-1}]$, since $pP_{i+1} = P_i$ and $s_i^p = s_{i+1}$. So Q_{i+1} is in $A[p^r]$. Now, define $R_i = s_i(P_{i+1}) - P_{i+1}, S_i = s_i(R_i) - R_i$. Then, $pR_i = Q_i$ and $pS_i = s_i(Q_i) - Q_i = 0$. It follows by induction on j that $s_i^j(R_i) = R_i + jS_i$. Hence, for p odd,

$$\sum_{j=0}^{p-1} s_i^j(R_i) = pR_i + \frac{p(p-1)}{2}S_i = pR_i = Q_i.$$

On the other hand,

$$\sum_{j=0}^{p-1} s_i^j(R_i) = \sum_{j=0}^{p-1} s_i^j(s_i(P_{i+1}) - P_{i+1}) = s_i^p(P_{i+1}) - P_{i+1}$$
$$= s_{i+1}(P_{i+1}) - P_{i+1} = Q_{i+1},$$

that is, $Q_i = Q_{i+1}$. The lemma now follows by induction on i, as mentioned above, if p is odd. For $p = 2$ a similar argument applies.

Theorem 2. *Let A be a semiabelian variety over $\mathbb{C}_p$ and X a closed subvariety of A. Assume that the Frobenius endomorphism of the reduction lifts to an endomorphism of A. Then there exists $c > 0$ such that, for every torsion point P of A, either $P \in X$ or $d(P, X) \geq c$.*

Proof. Let A be a semiabelian variety defined over a p-adic field with a lift of Frobenius and let T be the set of Teichmuller points, in the sense of [Bu2]. That is, T is the set of points in A fixed by a power of the Frobenius. The reduction map induces an isomorphism between T and the torsion points in the reduction of A. Let X be a subvariety of A.

Suppose P is a torsion point in A close to X, write $P = Q + R$, with Q of p-power order in the formal group of A and $R \in T$. This can be done since, by hypothesis, Frobenius lifts. Let K be a field where the points of T are defined, X is defined and assume that K has bounded ramification (we can always do that). It follows that Q is close to $X - R$ and since the degree of $X - R$ is the degree of X, we conclude by theorem 1 that either $d(P, X) = d(Q, X - R)$ is bounded below or Q belongs to a finite set. We can then apply Buium's result ([Bu2]) to bound $d(P, X) = d(R, X - Q)$ from below, for each of the finitely many remaining Q, proving the theorem.

Remarks. (i) One may ask whether a global version of the conjecture holds, namely whether torsion points are integral points over the algebraic closure of $\mathbb{Q}$, for some embedding of an open subset of an abelian variety A. The answer is “no” for $\dim A > 1$. Indeed, if X is the divisor at infinity, then X will have many points modulo p, for large p, and those points will lift to torsion points not integral at p. This example does not preclude the possibility that the exponent of p in the denominators of the coordinates of torsion points is bounded independently of p and one might conjecture that this is indeed the case.

(ii) Theorem 2 can be used to answer, for abelian varieties with a lift of Frobenius, a question posed by Tate [T] and studied by Boxall [B3]. Define $\lambda(P, X) = -\log d(P, X)$, for an ample divisor X on an abelian variety A over $\mathbb{C}_p$ of dimension g. Assume that the Frobenius endomorphism of the reduction lifts to an endomorphism of A. Then

$$\lim_{N \to \infty} \frac{1}{N^{2g}} \sum_{P \in A[N] \setminus X} \lambda(P, X) = 0.$$

Boxall proved this if N is not divisible by p. Essentially the same proof applies once we know that $\lambda(P, X)$ is bounded above, which is what theorem 2 gives.

Acknowledgements

The author would like to thank J. Boxall, A. Buium, R. Coleman and J. Tate for helpful discussions.

References

[B1] J. Boxall, *Autour d'un problème de Coleman*, C. R. Acad. Sci. Paris **315** (1992), 1063–1066.

[B2] ______, *Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini in Number Theory, Paris 1992–3,*, S. David (eds.), London Math. Soc. lecture note series **215** (1995), Cambridge Univ. Press, 69–89.

[B3] ______, *Une propriété des hauters locales de Néron-Tate sur les variétés abéliennes*, J. de Théorie des Nombres de Bordeaux **7** (1995), 111–119.

[Bu1] A. Buium, *Geometry of p-jets*, Duke Math. J. **82** (1996), 349–367.

[Bu2] ______, *An approximation property for Teichmüller points*, Math. Res. Lett. **3** (1996), 453–457.

[H] E. Hrushovski, *The Manin-Mumford conjecture and the model theory of difference fields*, preprint (1996).

[R] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), 207–235.

[S] J. H. Silverman, *Arithmetic distance functions and height functions in Diophantine geometry*, Math. Ann. **279** (1987), 193–216.

[T] J. Tate, *Letter to J-P. Serre*, June 21st, 1968.

[TV] J. Tate and J. F. Voloch, *Linear forms in p-adic roots of unity*, Internat. Math. Res. Notices **12** (1996), 589–601.

Department of Mathematics, University of Texas, Austin, TX 78712
E-mail address: voloch@math.utexas.edu