Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Some remarks on almost rational torsion points

par John Boxall et David Grant

Introduction

Let G be a commutative algebraic group defined over a perfect field k. Let $\overline{k}$ be an algebraic closure of k and Γ_k be the Galois group of $\overline{k}$ over k. Following Ribet ([1], [19], see also [7]), we say a point $P \in G(\overline{k})$ is *almost rational over* k if whenever $\sigma, \tau \in \Gamma_k$ are such that $\sigma(P) + \tau(P) = 2P$, then $\sigma(P) = \tau(P) = P$. We denote the almost rational points of G over k by G_k^{ar}. Let G_{tors} denote the torsion subgroup of $G(\overline{k})$ and G'_{tors} the subgroup of points of order prime to the characteristic of k. Let $G_{\mathrm{tors},k}^{\mathrm{ar}} = G_k^{\mathrm{ar}} \cap G_{\mathrm{tors}}$ and $G_{\mathrm{tors},k}^{\mathrm{ar},\prime} = G_k^{\mathrm{ar}} \cap G'_{\mathrm{tors}}$. For any $N \geq 1$, we let $G[N]$ denote the subgroup of G_{tors} consisting of points of order dividing N, and O denote the origin of G.

Using unpublished results of Serre [22], Ribet showed that if K is a number field and G is an abelian variety over K, then $G_{\mathrm{tors},K}^{\mathrm{ar}}$ is a finite set [1], [19]. Let C be a nonsingular projective curve of genus at least 2 over K, and $\phi_Q : C \to J$ an Albanese embedding of C into its Jacobian J with a K-rational point Q as base point. Then for any $P \in C(\overline{K})$ which is not a hyperelliptic Weierstrass point, $\phi_Q(P) \in J_K^{\mathrm{ar}}$. Hence Ribet's result gives a new proof of the Manin-Mumford conjecture, originally proved by Raynaud [18], that the torsion packet $\phi_Q(C) \cap J_{\mathrm{tors}}$ is finite. In [7], Calegari determined all the possibilities for the $\mathbb{Q}$-almost rational torsion points on a semi-stable elliptic curve over $\mathbb{Q}$.

In [4] and [5] the authors defined and studied the notion of the set of *singular torsion points* E_{sing} on an elliptic curve E over a field of characteristic different from 2, which is an analogue of torsion packets for elliptic curves. Since singular torsion points of order at least 3 are almost rational, Ribet's result also shows that E_{sing} is a finite set when E is defined over a field of characteristic 0.

The purpose of this paper is to prove a number of properties of almost rational torsion points on various classes of commutative algebraic groups over fields of arithmetic interest. Our first topic concerns uniform bounds

---

1991 *Mathematics Subject Classification.* 11G30, 14H25.
Key words and phrases. Elliptic curves, torsion, almost rational.
The first author was enjoying the hospitality of the University of Colorado at Boulder while working on the paper.

for the orders of points of $G^{\mathrm{ar}}_{\mathrm{tors},K}$ for certain G defined over number fields K. In § 2 we show that for given integers g and d, there exists an integer $U_{d,g}$ such that for all tori M of dimension at most g over number fields K of degree at most d, we have $M^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq M[U_{d,g}]$. In § 3 we likewise show that for given d and g, there exists an integer $V_{d,g}$ such that if A is an abelian variety of dimension at most g with (potential) complex multiplication, and A is defined over a number field K of degree at most d, then $A^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq A[V_{d,g}]$ This implies that for a given $g > 1$ and d, if C is a curve of genus g defined over a number field K of degree d and $Q \in C(K)$, and if the Jacobian J of C has (potential) complex multiplication, then there is an integer $W_{d,g}$ such that $\phi_Q(C) \cap J_{\mathrm{tors}} \subseteq J[W_{d,g}]$. Coleman has a sharp bound for the order of this torsion packet that depends on the reduction type of C and the ramification in K [8].

In § 4 we show that a folklore conjecture concerning the action of Γ_K on torsion points of elliptic curves without complex multiplication implies that for a given d, there is an integer X_d with the property that for all one dimensional commutative group varieties G defined over number fields K of degree at most d, we have $G^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq G[X_d]$. We also mention a number of related unconditional results for elliptic curves. The proofs rely on general properties of almost rational points as recalled in § 1, and use methods similar to those of our previous paper [5]. We note that writing our proofs in greater detail would yields explicit values of $U_{d,g}$, $V_{d,g}$, and $W_{d,g}$.

Our second topic concerns whether $A^{\mathrm{ar}}_{\mathrm{tors},K}$ is infinite or not when A is an abelian variety defined over a field K which is a finite extension of $\mathbb{Q}_p$ (which we will refer to as a *p-adic field*). We give an example in § 6 where $A^{\mathrm{ar}}_{\mathrm{tors},K}$ is finite, and show that there is always a finite extension L of K, of degree bounded only in terms of the dimension of A, such that $A^{\mathrm{ar}}_{\mathrm{tors},L}$ is infinite.

This is achieved by passing to an extension where A has semistable reduction, and by using a simple argument to lift almost rational torsion from the reduction of A to almost rational torsion defined over the maximal unramified extension of K. This forces us in § 5 to make a careful study of whether $G^{\mathrm{ar},\prime}_{\mathrm{tors},k}$ is infinite or not when G is a semi-abelian variety and k is a finite field. In § 5 we show that $G^{\mathrm{ar},\prime}_{\mathrm{tors},k}$ is infinite except in a finite number of cases that are listed explicitly in Proposition 11.

1. Almost rational points

Let G be a commutative algebraic group defined over a perfect field k. We begin by bringing together some of the simpler properties of G^{ar}_k (see [5] and [7]). It is clear that $G(k) \subseteq G^{\mathrm{ar}}_k$, that if K is an extension field of k, then $G^{\mathrm{ar}}_k \subseteq G^{\mathrm{ar}}_K$, and that G^{ar}_k is Γ_k-stable. Note that it is not true in general that G_k^{ar} is a group. For a counterexample, see the example after Theorem 1.2 in [7].

Lemma 1. *Let P, $Q \in G(\overline{k})$, and suppose that the normal closures of $k(P)$ and $k(Q)$ are linearly disjoint over k. If $P + Q \in G_k^{\text{ar}}$, then $P, Q \in G_k^{\text{ar}}$.*

Proof. By symmetry it suffices to show that $P \in G_k^{\text{ar}}$. Suppose $P + Q$ is almost rational, and let σ, $\tau \in \Gamma_k$ be such that $\sigma(P) + \tau(P) = 2P$. By hypothesis, there exist σ', $\tau' \in \Gamma_k$ such that $\sigma'(P) = \sigma(P)$ and $\sigma'(Q) = Q$, $\tau'(P) = \tau(P)$ and $\tau'(Q) = Q$. Then $\sigma'(P + Q) + \tau'(P + Q) = 2(P + Q)$, so $\sigma'(P + Q) = \tau'(P + Q) = P + Q$. But then $\sigma(P) = P$ and $\tau(P) = P$, hence P is almost rational. □

Remarks. 1) In practice, we apply Lemma 1 to torsion points. If $P \in G[M]$ and $Q \in G[N]$ for integers M and N such that $k(G[M])$ and $k(G[N])$ are linearly disjoint over k, then if $P + Q \in G_k^{\text{ar}}$, the components P, Q are in G_k^{ar} as well.

2) There is a complement to Lemma 1, which says that if $P, Q \in G_k^{\text{ar}}$ are such that the subgroups G_P and G_Q of $G(\overline{k})$ generated respectively by all the Γ_k-conjugates of P and of Q satisfy $G_P \cap G_Q = \{O\}$, then also $P + Q \in G_k^{\text{ar}}$. In particular, if M, N are relatively prime integers, and $P, Q \in G_k^{\text{ar}}$ are of order M and N respectively, then $P + Q \in G_k^{\text{ar}}$.

Proposition 2. *Let Ω be a finite set of primes and let G_Ω be the subgroup of G_{tors} consisting of points whose order is divisible only by primes in Ω. If ℓ is a prime, set $\ell' = \ell$ if ℓ is odd and $\ell' = 4$ if $\ell = 2$. Let $L = \prod_{\ell \in \Omega} \ell'$ and let $k' = k(G[L])$. Suppose that there exists an integer M, divisible only by primes in Ω, such that $G(k') \cap G_\Omega \subseteq G[M]$. Then $G_{\text{tors},k}^{\text{ar}} \cap G_\Omega \subseteq G[M]$.*

This is Proposition C of [5]. Note that the hypothesis about M is satisfied whenever k is a field having the property that for every finite extension K of k, $G_{\text{tors}}(K)$ is a finite group. In particular, this is the case when k is a finite field, a p-adic field, or a number field.

The explicit bound $B(r)$ in the following Lemma appears in several applications.

Lemma 3. *For any integer $r \geq 1$, let*

$$B(r) = \left((r-1)(r-2) + r\sqrt{r^2 - 6r + 17}\right)^2/4.$$

If p is any prime such that $p > B(r)$, then for every $a \geq 1$, there is a point $(x_a, y_a) \in ((\mathbb{Z}/p^a\mathbb{Z})^*)^2$ on the curve $x^r + y^r = 2$ satisfying $x_a^r \neq 1$, $y_a^r \neq 1$.

Proof. It is easy to see that $B(r) > r$, so that if $p > B(r)$, the projective curve $X^r + Y^r = 2Z^r$ is smooth in characteristic p, and its genus is $(r-1)(r-2)/2$. The case $a = 1$ now follows from standard applications of the Weil bounds. The case $a > 1$ then follows from Hensel's Lemma (see for example [2], Chapter I §5.2). □

2. Tori over number fields

As a simple application of the above, we consider tori. First we need a Lemma.

Lemma 4. *Let K be a number field of degree at most d, and $B(d)$ as in Lemma 3. For every $g \geq 1$, if $p > B(d)$, then p does not divide the order of any almost rational torsion point of $(\mathbb{G}_m)^g$ over K.*

Proof. Suppose there is an almost rational torsion point Q of $(\mathbb{G}_m)^g$ over K of order N divisible by a prime $p > B(d)$. Since $p > B(d) > d$, we have $p > d$ and p odd. Decompose $Q = Q_p + Q'$, where Q' is of order prime to p, and Q_p is of precise order p^a for some $a \geq 1$. Let $\mathfrak{p}$ be a prime of K above p, and I the inertia group of any prime of $K(Q_p)$ above $\mathfrak{p}$. Then I is a subgroup of finite index s in $(\mathbb{Z}/p^a\mathbb{Z})^\times$ for some $s \leq d < p$. Since $(\mathbb{Z}/p^a\mathbb{Z})^\times$ is cyclic, I is just the group of s-th powers in $(\mathbb{Z}/p^a\mathbb{Z})^\times$. If we can find $x, y \in (\mathbb{Z}/p^a\mathbb{Z})^\times$ such that $x^s + y^s = 2$, but $x^s \neq 1$ and $y^s \neq 1$, then since I acts trivially on Q', Q cannot be almost rational over K. It is easy to see that $B(r+1) > B(r)$ for all $r \geq 1$, so $p > B(s)$ and we can apply Lemma 3 to find such x and y. □

Proposition 5. *Let K be a number field of degree at most d. Then there is an explicitly computable integer R_d such that for every $g \geq 1$, every almost rational torsion point on $\mathbb{G}_m^g$ over K is of order dividing R_d.*

Proof. This follows almost immediately from Lemma 4 by applying Proposition 2, taking Ω to be the set of all primes less than or equal to $B(d)$. To conclude the proof, we need to check that the integer M appearing in Proposition 2 depends only on d. But L depends only on $B(d)$, and hence only on d. Then $K' = K((\mathbb{G}_m)^g[L]) = K(\mathbb{G}_m[L])$ is a Galois extension of K whose Galois group embeds into $(\mathbb{Z}/L\mathbb{Z})^\times$, whose order is therefore bounded only in terms of d. It follows that the degree of K' is bounded only in terms of d. But the Nth-cyclotomic polynomial is irreducible over $\mathbb{Q}$ and has degree tending to ∞ with N. This implies that the number of roots of unity in K' is bounded only in terms of d. □

Theorem 6. *Let $d \geq 1$, $g \geq 1$ be integers. Then there exists an explicitly computable integer $U_{d,g}$ such that for all tori M of dimension at most g defined over number fields K of degree at most d, we have $M^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq M[U_{d,g}]$.*

Proof. By Proposition 5, it suffices to reduce to the case of split tori. To do this, we show that given an integer g, there exists an integer N_g such that if M is a torus of dimension g defined over a perfect field k, then M splits over a Galois extension of degree at most N_g of k. This is well-known, and we briefly recall the proof. By definition, there exists a finite Galois extension L of k and an isomorphism $\phi : \mathbb{G}_m^g \to M$ defined over L. Since all automorphisms of $\mathbb{G}_m^g$ are defined over k, we have a homomorphism $\rho : \mathrm{Gal}(L/k) \to \mathrm{Aut}(\mathbb{G}_m^g) \cong GL_g(\mathbb{Z})$ defined by $\rho(\sigma) = \phi^{-1} \circ \phi^{\sigma}$. Then ϕ is defined over the fixed field F of the kernel of ρ, so M splits over F and $\mathrm{Gal}(F/k)$ is isomorphic to the image of ρ. Finally, according to a well-known result in group theory, the order of any finite subgroup of $GL_g(\mathbb{Z})$ divides $(2g)!$ (see for example [14] page 175), which gives us what we want. □

3. Abelian varieties with complex multiplication

Let A be an abelian variety of dimension g over the number field K, let $\mathrm{End}(A)$ denote the endomorphism ring of A over $\overline{K}$, and $\mathrm{End}_{\mathbb{Q}}(A)$ denote $\mathrm{End}\, A \otimes \mathbb{Q}$. Then A is $\overline{K}$-isogenous to a product $\prod_{j=1}^{n} A_j^{r_j}$ where the A_j, $1 \le j \le n$, are mutually non-$\overline{K}$-isogenous simple abelian varieties. We say that A has complex multiplication if for each j, $\mathrm{End}_{\mathbb{Q}}(A_j)$ is a CM field F_j and $[F_j : \mathbb{Q}] = 2 \dim A_j$.

Theorem 7. *Let $d \ge 1$, $g \ge 1$ be integers. There exists an explicitly computable integer $V_{d,g}$ such that for all abelian varieties A of dimension at most g, with complex multiplication, and defined over number fields K of degree at most d, $A^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq A[V_{d,g}]$.*

Proof. We first show how to reduce to the case where $\mathrm{End}(A)$ is defined over K, all of the absolutely simple factors of A are defined over K, A is isogenous over K to the product of these simple factors, and A has everywhere good reduction over K. The following lemma follows from Theorem 4.1 of [24], but for the convenience of the reader we include a quick direct proof.

Lemma 8. *Let g be an integer. Then there exists a constant N_g such that for any abelian variety B of dimension g defined over a perfect field k, there exists an extension k' of k of degree at most N_g, such that all the endomorphisms and absolutely simple factors of B are defined over k', and B is isogenous over k' to the product of its simple factors.*

Proof. Recall that $\mathrm{End}\, B$ is a free abelian group of rank at most $4g^2$, and Γ_k acts on $\mathrm{End}\, B$. Fixing a $\mathbb{Z}$-basis $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of $\mathrm{End}\, B$, we obtain a homomorphism $\rho : \Gamma_k \to GL_n(\mathbb{Z})$ by letting $\rho(\sigma)$ be the matrix of $\big(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)\big)$ with respect to $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. As in the proof of Theorem 6, the image of ρ is a finite subgroup of $GL_n(\mathbb{Z})$ whose order bounded only in terms of n and hence only in terms of g. Thus $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is defined over the finite extension k' fixed by the kernel of ρ, so the same must be true of each element α_i. Since $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a basis of $\mathrm{End}\, B$, we conclude the all the elements of $\mathrm{End}\, B$ are defined over k'. By Poincaré's irreducibility theorem, the simple factors of B are images of B under integral multiples of suitable idempotents in $\mathrm{End}_{\mathbb{Q}} B$, so the simple factors of B are defined over k' and B is isogenous over k' to the product of its simple factors. □

Proof of Theorem 7. By Lemma 8, we may suppose that A is K-isogenous to a product $\prod_{j=1}^{n} A_j^{r_j}$, where the A_j, $1 \le j \le n$, are absolutely simple mutually non-isogenous abelian varieties over K, and for each j, $\mathrm{End}_{\mathbb{Q}} A_j$ is a CM field F_j with $[F_j : \mathbb{Q}] = 2\dim A_j$. In addition, A acquires semistable reduction over $K(A[12])$ (see for example [25]), which is again an extension of K of degree bounded by the order of $GL_{2g}(\mathbb{Z}/12\mathbb{Z})$, which depends only on g. On the other hand, since each A_j has CM, it acquires everywhere good reduction over a finite extension of K ([10], page 100). This implies that A actually has everywhere good reduction over $K(A[12])$. Thus, replacing K by $K(A[12])$ if necessary, we now suppose A has everywhere good reduction over K. Then each A_j also has everywhere good reduction over K. Let K^{ab} denote the maximal abelian extension of K.

For each j, A_j has a polarization defined over K, so we can apply the main theorems of complex multiplication to study the action of $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ on $(A_j)_{\mathrm{tors}}$. Let ℓ be any prime, and $T_\ell(A_j)$ the Tate module. Let I_K denote the idele group of K, H the Hilbert class field of K, and $\mathcal{O}$ the ring of integers of K. Then the composite of the inclusion $(\mathcal{O}\otimes\mathbb{Z}_\ell)^* \to I_K$ and the Artin map $I_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ sends $(\mathcal{O}\otimes\mathbb{Z}_\ell)^*$ into $\mathrm{Gal}(K^{\mathrm{ab}}/H)$. Let ρ be the composite map

$$(\mathcal{O}\otimes\mathbb{Z}_\ell)^* \to \mathrm{Gal}(K^{ab}/H) \to \mathrm{End}(T_\ell(A_j)) \to \mathrm{End}(F_j\otimes\mathbb{Z}_\ell),$$

where the center arrow is the Galois representation on $T_\ell(A_j)$, and the righthand arrow is the map induced from the identification of $T_\ell(A_j)\otimes\mathbb{Q}_\ell$ with $F_j\otimes\mathbb{Z}_\ell$. The proof of Theorem 2.8 of Chapter 4 in [10] shows that ρ is the reflex norm. In particular, if $\alpha\in\mathbb{Z}_\ell^*$, then there is an element $\sigma_\alpha\in\mathrm{Gal}(K^{ab}/H)$ that acts on $T_\ell(A_j)$ via the homothety which is multiplication by $\alpha^{[K:\mathbb{Q}]/2}$. Since this holds for all j, σ_α also acts on $T_\ell(\prod_{j=1}^{n}(A_j)^{r_j})$ via multiplication by $\alpha^{[K:\mathbb{Q}]/2}$. Note that the action of homotheties on Tate modules is preserved by isogenies (see e.g. [6] Prop. 1.8(e)), so σ_α also acts on $T_\ell(A)$ via the homothety $\alpha^{[K:\mathbb{Q}]/2}$. Since A has everywhere good reduction over K, σ_α actually belongs to the subgroup I^ℓ of $\mathrm{Gal}(K^{ab}/H)$ generated by the inertia groups of places of K lying above ℓ. By the Néron-Ogg-Shafarevich criterion, I^ℓ acts trivially on the points of A_{tors} of order prime to ℓ. Using Lemma 3, it follows as in the proof of Lemma 4, that if $\ell > B([K:\mathbb{Q}]/2)$, ℓ does not divide the order of a point of $A^{\mathrm{ar}}_{\mathrm{tors},K}$. We deduce that the orders of points of $A^{\mathrm{ar}}_{\mathrm{tors},K}$ can only be divisible by a finite set of primes Ω that depends only on d and g.

To conclude the proof we apply Proposition 2. Again, $L = \prod_{\ell\in\Omega}\ell'$ depends only on d and g, and so $[K' : \mathbb{Q}]$ is bounded only in terms of d and

g, where $K' = K(A[L])$. Since A has everywhere good reduction, applying the Weil bounds at places of K' above 2 and 3 shows that the orders of points of $A_{\text{tors}}(K')$ are bounded only in terms of $[K' : \mathbb{Q}]$ and g. □

4. Elliptic curves without complex multiplication

We now assume that E is an elliptic curve defined over a number field K that does not have complex multiplication. For any prime ℓ, let $\rho_\ell : \Gamma_K \to GL_2(\mathbb{F}_\ell)$ be the representation obtained from the action of Γ_K on $E[\ell]$. Similarly, let $\rho_{\ell^\infty} : \Gamma_K \to GL_2(\mathbb{Z}_\ell)$ be the representation giving the action of Γ_K on $T_\ell(E)$, and let $\rho : \Gamma_K \to GL_2(\hat{\mathbb{Z}}) = \prod_{\ell \text{ prime}} GL_2(\mathbb{Z}_\ell)$ be that obtained from the action of Γ_K on E_{tors}.

The main theorem of Serre in [21] is that the image of ρ is of finite index in $GL_2(\hat{\mathbb{Z}})$. The Proposition on page IV-19 of [20] shows that this is equivalent to the existence of an integer $n(E,K)$ such that for all primes $\ell > n(E,K)$, the image of ρ_ℓ contains $SL_2(\mathbb{F}_\ell)$.

Proposition 9. *Suppose $\ell \geq 7$. If the image of ρ_ℓ contains $SL_2(\mathbb{F}_\ell)$, then ℓ cannot divide the order of an almost rational torsion point of E over K.*

Proof. Lemma 5 on page IV-26 of [20] states that if S is the finite set of primes containing 2, 3, and 5, and all primes $\ell \geq 7$ such that the image of ρ_ℓ does not contain $SL_2(\mathbb{F}_\ell)$, then if $X = \prod_{\ell \notin S} SL_2(\mathbb{Z}_\ell)$ as a subgroup of the full product $SL_2(\hat{\mathbb{Z}})$, then $\rho(\Gamma_K) \supseteq X$. Let L the extension of K such that $\rho(\Gamma_L) = X$. Then by Lemma 1, it suffices to show that there is no almost rational torsion point R of E over L with R of ℓ-power order. Suppose such an R exists. By construction, $\rho_{\ell^\infty}(\Gamma_L) = SL_2(\mathbb{Z}_\ell)$. Let $\sigma \in \Gamma_L$ be such that $\rho_{\ell^\infty}(\sigma)$ is a transvection in $SL_2(\mathbb{Z}_\ell)$. Then $(\sigma - 1)^2 R = (\sigma + \sigma^{-1} - 2)\sigma(R) = O$, and since R is almost rational over L, $\sigma(R) = R$. But the only element of $\mathbb{Z}_\ell^2$ fixed under multiplication by all the transvections in $SL_2(\mathbb{Z}_\ell)$ is the origin, so $R = O$. □

The Proposition says that if ℓ is a prime dividing the order of a point of $E^{\text{ar}}_{\text{tors},K}$, then $\ell \leq \max(5, n(E,K))$. Note that applying Proposition 2, taking Ω to be the set of all primes $\ell \leq \max(5, n(K,E))$, we again deduce the finiteness of $E^{\text{ar}}_{\text{tors},K}$. Combining this with Theorem 7, we again conclude that there are only finitely-many almost rational torsion points on an elliptic curve over a number field. Recall that in [21], page 299, Serre asks whether there exists an integer $n(K)$, depending only on K, such that $n(E,K) \leq n(K)$ for all elliptic curves E over K without complex multiplication. It seems like a reasonable question to ask whether, given any integer $d \geq 1$, there is an integer n_d such that for all elliptic curves E without complex multiplication defined over number fields K of degree at most d, $n(E,K) \leq n_d$.

Corollary 10. *Suppose for every $d \geq 1$ there is an integer n_d such that for all elliptic curves E without complex multiplication defined over number fields K of degree at most d, $\rho_\ell(\Gamma_K) \supseteq SL_2(\mathbb{F}_\ell)$ for all primes $\ell > n_d$. Then for every $d \geq 1$ there is an integer $X_d \geq 1$ such that for all one-dimensional commutative algebraic groups G over number fields K of degree at most d, $G^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq G[X_d]$.*

Proof. When $G = \mathbb{G}_a$, there is nothing to prove. The case of a torus follows from Theorem 6. In view of Theorem 7, it suffices to consider elliptic curves E without complex multiplication. By Proposition 9, only primes $\ell \leq \max(5, n_d)$ can divide the order of a point of $E^{\mathrm{ar}}_{\mathrm{tors},K}$. We apply Proposition 2, taking Ω to be this set of primes. We deduce that there exists an extension K'/K, of degree bounded only in terms of d, such that $E^{\mathrm{ar}}_{\mathrm{tors},K} \subseteq E(K')_{\mathrm{tors}}$. A well-known result of Merel [13], [16] gives that $E(K')_{\mathrm{tors}}$ is bounded only in terms of d. □

Remarks. 1) For general K and E, the best known upper bound on $n(E, K)$ is that of Masser-Wüstholz [11]. They prove that there exist absolute constants c and γ, such that if E is an elliptic curve without complex multiplication over a number field K of degree d, and if h is the absolute logarithmic Weil height of $j(E)$, then $\rho_\ell(\Gamma_K) \supseteq SL_2(\mathbb{F}_\ell)$ provided $\ell > c\big(\max(d, h)\big)^\gamma$. For more recent work, see [17] and [27]. Since there are elliptic curves over $\mathbb{Q}$ with a rational 5-torsion point, $5 \leq c\big(\max(d, h)\big)^\gamma$, so we get that if ℓ divides the order of a point of $E^{\mathrm{ar}}_{\mathrm{tors},K}$, then $\ell \leq c\big(\max(d, h)\big)^\gamma$.

2) Recall that Mazur [12] proved that if E is a semistable elliptic curve over $\mathbb{Q}$, then $\rho_\ell(\Gamma_\mathbb{Q}) = GL_2(\mathbb{F}_\ell)$ for all $\ell \geq 11$. Since there are no elliptic curves over $\mathbb{Q}$ with everywhere good reduction, there are no semistable elliptic curves over $\mathbb{Q}$ that have complex multiplication. Using Proposition 9, we get that if E is a semistable elliptic curve over $\mathbb{Q}$, and if ℓ is a prime dividing the order of a point of $E^{\mathrm{ar}}_{\mathrm{tors},\mathbb{Q}}$, then $\ell \leq 7$. This recovers Corollary 2.2 of [7].

5. Semi-abelian varieties over finite fields

Let k be a finite field with q elements, and let G be a semi-abelian variety over k. We shall prove that $G^{\mathrm{ar},\prime}_{\mathrm{tors},k}$ is typically infinite, but is finite in certain prescribed cases.

The template for our proof is the case where $G = \mathbb{G}_m$. Then if $n \in \mathbb{N}$, any primitive $(q^n - 1)$-st root of unity ζ is almost rational over k. Indeed, $\{\zeta^{q^a} \mid 0 \leq a \leq n-1\}$ is a complete set of Γ_k-conjugates of ζ. If $\zeta^{q^a}\zeta^{q^b} = \zeta^2$ with $0 \leq a, b \leq n-1$, then $q^a + q^b \equiv 2 \mod q^n - 1$. Since $q \geq 2$, we have $q^a + q^b \leq q^n$, so $a = b = 0$. Hence $(\mathbb{G}_m)^{\mathrm{ar}}_{\mathrm{tors},k}$ is infinite.

To generalize this argument, we need to recall some basic facts about the action of Γ_k on G'_{tors} for any semi-abelian variety defined over k. By definition, G is an extension of an abelian variety A by a torus M, and both A and M are defined over k. Let σ be the Frobenius generator of Γ_k, and let χ_G be the characteristic polynomial of σ acting on $T_\ell(G)$ for any prime ℓ prime to q, and define χ_A and χ_M similarly for A and M. Then χ_G, χ_A, and χ_M are monic polynomials with integer coefficients that are independent of ℓ, and since $T_\ell(G)$ is an extension of $T_\ell(A)$ by $T_\ell(M)$, we have $\chi_G = \chi_A\chi_M$. Hence $\chi_G(\sigma)(P) = 0$ for all $P \in G'_{\mathrm{tors}}$, and corresponding assertions hold for A and M. If we view G'_{tors} as a module over the polynomial ring $\mathbb{Z}[t]$ by letting $f \in \mathbb{Z}[t]$ act as $f(\sigma)$, then the annihilating ideal I of G'_{tors} contains χ_G. Let $m_G \neq 0$ be an element of I of minimal degree and let μ be the greatest common divisor of the coefficients of m_G. Since G'_{tors} is divisible, m_G/μ belongs to I, and so we can suppose $\mu = 1$. Since m_G divides χ_G in $\mathbb{Q}[t]$, χ_G/m_G actually has coefficients in $\mathbb{Z}$ by Gauss's lemma, so that, after multiplying m_G by ± 1, we can suppose that m_G is monic. Since m_G has minimal degree among the non-zero elements of I, m_G generates I. We call m_G the minimal polynomial of σ, and define m_A and m_M similarly.

It is well known (see for example [26]) that if $\prod_{i=1}^{v} g_i^{d_i}$ is the factorization of χ_A into distinct irreducibles in $\mathbb{Z}[t]$, then there is a k-isogeny

$$\omega : \prod_{i=1}^{v} \mathcal{A}_i^{d_i} \to A, \tag{1}$$

where the $\mathcal{A}_i$ are mutually non-k-isogenous k-simple abelian varieties, and where for each i, $g_i = \chi_{\mathcal{A}_i}$. Also the action of σ is semisimple, so $m_A = \prod_{i=1}^{v} g_i$.

The corresponding results hold for tori. Let $M^* = \mathrm{Hom}(M, \mathbb{G}_m)$ be the character group of the torus M. Recall (see for example [15]) that the action of Γ_k on M^* is semisimple, and the k-isogeny class of M is determined by the structure of $M^* \otimes \mathbb{Q}$ as a Γ_k-module, hence by the characteristic polynomial $h(t)$ of σ acting on M^*. Since the action of Γ_k on M^* factors through a finite quotient, $h(t)$ as a product of irreducibles in $\mathbb{Z}[t]$ is of the form $\prod_{j=1}^{w} \Phi_{\nu_j}^{e_j}$, where Φ_ν is the ν-th cyclotomic polynomial, $\nu_j \neq \nu_\ell$ if $j \neq \ell$, and $\sum_{j=1}^{w} e_j\phi(\nu_j) = d$, where d is the dimension of M and ϕ is Euler's function. For each ν there is a torus M_ν over k such that the characteristic polynomial of σ acting on $(T_\nu)^*$ is Φ_ν, so M is k-isogenous to $\prod_{j=1}^{w} M_{\nu_j}^{e_j}$, and the M_{ν_j} are mutually non-k-isogenous k-simple tori. Further, $M'_{\mathrm{tors}} = M(\overline{k}) = \mathrm{Hom}(M^*, \overline{k}^*)$, so $\chi_M = q^d h(t/q)$, and hence $m_M(t) = \prod_{j=1}^{w} m_{M_{\nu_j}}(t)$, where $m_{M_\nu}(t) = q^{\phi(\nu)}\Phi_\nu(t/q)$.

Recall that, by the Riemann hypothesis for function fields, every complex root λ of χ_A satisfies $|\lambda| = q^{1/2}$ while every complex root μ of χ_M satisfies $|\mu| = q$. It follows that the sets of roots of χ_A and of χ_M are disjoint, so $m_G = m_A m_M$. Write $R = \mathbb{Z}[t]/m_G$ and $L = R \otimes \mathbb{Q}$. Since m_G is monic, R embeds into L. Also $L = \mathbb{Q}[t]/m_G = \mathbb{Q}[t]/m_A \times \mathbb{Q}[t]/m_M$ is a product of number fields $L = \prod_{i=1}^{v+w} L_i$, where $L_i = \mathbb{Q}[t]/g_i$ if $i \leq v$ and $L_i = \mathbb{Q}[t]/m_{M_{\nu_{i-v}}}$ if $i \geq v+1$. Let $\mathcal{O}_i$ be the ring of integers of L_i, and $\mathcal{O} = \prod \mathcal{O}_i$. Let π be the image of t in $\mathcal{O}$ under the canonical map $\mathbb{Z}[t] \to R \subseteq \mathcal{O}$.

Proposition 11. *Let E_1, E_2, and E_3 denote respectively the curves over k with equations $y^2 + (x+1)y = x^3 + x^2$, $y^2 + y = x^3 + x$, and $y^2 + y = x^3$, and let M_ν be as above.*

(*i*) *If $q = 2$ and G is an abelian variety over k which is k-isogenous to some power of E_1 or E_2, then $G^{\mathrm{ar},\prime}_{\mathrm{tors},k} = G'_{\mathrm{tors}}(k)$.*

(*ii*) *If $q = 2$ or 4, and if G is an abelian variety over k which is k-isogenous to a power of E_3, then $G^{\mathrm{ar},\prime}_{\mathrm{tors},k} = G'_{\mathrm{tors}}(\mathbb{F}_4)$.*

(*iii*) *If $q = 2$ and if G is a torus over k which is k-isogenous to some power of M_2, then $G^{\mathrm{ar},\prime}_{\mathrm{tors},k} = G'_{\mathrm{tors}}(k)$.*

Proof. Consider first the case when $q = 2$ and G is isogenous to some power of E_1. Then $\chi_{E_1}(t) = m_{E_1}(t) = t^2 + t + 2$, and so $m_G(t) = t^2 + t + 2$ and this divides $t^3 + t - 2$. Therefore $\pi^3 P + \pi P = 2P$ for all $P \in G'_{\mathrm{tors}}$. But if $P \notin G'_{\mathrm{tors}}(k)$, then $\pi P \neq P$, so P cannot be almost rational. The other cases are treated similarly, using the fact that $m_{E_2}(t) = t^2 + 2t + 2$, which divides $t^3 + t^2 - 2$; $m_{E_3}(t) = t^2 + 2$ over $\mathbb{F}_2$, which divides $t^4 + t^2 - 2$; $m_{E_3}(t) = t + 2$ over $\mathbb{F}_4$, which divides $t^2 + t - 2$; and $m_{M_2}(t) = t + 2$ over $\mathbb{F}_2$, which again divides $t^2 + t - 2$. □

Theorem 12. *Let G be a semi-abelian variety over a finite field k with q elements. Then $G^{\mathrm{ar},\prime}_{\mathrm{tors},k}$ is finite if and only if G is of one of the types listed in Proposition 11.*

The proof will follow the argument given for $\mathbb{G}_m$ at the beginning of the section. First we need a few technical lemmas. Let p denote the characteristic of k.

Lemma 13. *Let N be an integer divisible by p and by the index of R in $\mathcal{O}$. If $\mathfrak{a}$ is any ideal of $R[1/N]$, there exists a $P \in G'_{\mathrm{tors}}$ of order prime to N whose annihilator ideal in $R[1/N]$ is $\mathfrak{a}$.*

Proof. (John: Since $p|N$, should we rephrase as a Lemma for G_{tors} instead of G'_{tors}?) From the ring decomposition $R = \mathbb{Z}[T]/m_G \cong \mathbb{Z}[T]/m_T \times \mathbb{Z}[T]/m_A$, we get corresponding splittings $G'_{\mathrm{tors}} \cong T'_{\mathrm{tors}} \times A'_{\mathrm{tors}}$ and $\mathfrak{a} \cong \mathfrak{a}_T \times \mathfrak{a}_A$ that reduce the proof of the lemma to the cases where $G = T$ and $G = A$. The two cases are handled similarly, so we assume for sake of exposition that $G = A$, so now $R = \mathbb{Z}[T]/m_A$ and $\mathfrak{a} = \mathfrak{a}_A$. By the choice of N, $R[1/N]$ is a product of Dedekind domains $\mathcal{O}_i[1/N]$,

$1 \leq i \leq v$. If E is an $R[1/N]$-module, we write E_i for the $\mathcal{O}_i[1/N]$-component of E. Since G'_{tors} is an R-module, $G'_{\text{tors}} \otimes \mathbb{Z}[1/N]$, the torsion of G of order prime to N, is an $R[1/N]$-module. It suffices to show for every $1 \leq i \leq v$ that there is a $P_i \in (G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i$ whose annihilator ideal in $\mathcal{O}_i[1/N]$ is $\mathfrak{a}_i$. If $Q_1, Q_2 \in (G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i$ have relatively prime annihilators ideals $\mathfrak{b}_1, \mathfrak{b}_2$ in $\mathcal{O}_i[1/N]$, then the annihilator ideal of $Q_1 + Q_2$ is $\mathfrak{b}_1\mathfrak{b}_2$, so it suffices to show the result when $\mathfrak{a}_i$ is $\mathfrak{p}_i^\epsilon$ for a prime ideal $\mathfrak{p}_i$ of $\mathcal{O}_i[1/N]$ and $\epsilon \geq 1$. The result will hold in this case unless $(G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i[\mathfrak{p}_i^\epsilon] = (G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i[\mathfrak{p}_i^{\epsilon-1}]$, which would imply that $(G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i[\mathfrak{p}_i^\infty] = (G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i[\mathfrak{p}_i^{\epsilon-1}]$, which is absurd. Indeed, via (1), we get that $(G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i = \omega((\mathcal{A}_i^{d_i})'_{\text{tors}} \otimes \mathbb{Z}[1/N])$ (restricting ω to the i^{th}-factor), so $(G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i[\mathfrak{p}_i^\infty]$ is infinite, while $(G'_{\text{tors}} \otimes \mathbb{Z}[1/N])_i[\mathfrak{p}_i^{\epsilon-1}]$ is finite.

□

For $r \geq 1$, write $S(r) = \pi^{r-1} + \pi^{r-2} + \cdots + \pi + 1$. Then $S(r)_i \in \mathcal{O}_i$ for all i.

Lemma 14. *There are infinitely many integers $r \geq 1$ such that $S(r)_i$ is relatively prime to N for all i.*

Proof. Since $\mathcal{O}/N\mathcal{O}$ is a finite ring, there exist s and $t \geq 1$ such that the images of $S(s+t)$ and $S(t)$ in $\mathcal{O}/N\mathcal{O}$ coincide. Since

$$S(s+t) = \pi^t S(s) + S(t), \tag{2}$$

we have $\pi^t S(s) \in N\mathcal{O}$, so $(\pi S(s))^t \in N\mathcal{O}$. But since $S(s+1) = \pi S(s) + 1$ we get that $(S(s+1) - 1)^t \in N\mathcal{O}$, so $S(s+1)_i$ is prime to N for all i. Setting $r = s+1$ and taking s as large as we please in (2) concludes the proof. □

Let $[\cdot]$ denote the greatest integer function.

Lemma 15. *Let $r \geq 15$, and suppose that $\pi^c + \pi^d - 2\pi^e = \alpha(\pi^r - 1)$ for some $\alpha \in \mathcal{O}$ with $0 \leq c \leq r-1$, $0 \leq d, e \leq [r/2]$. Then $\alpha = 0$.*

Proof. Let λ be a complex root of $m_G(t)$. Since m_G is monic, λ is an algebraic integer and there is a unique $\mathbb{Q}$-algebra homomorphism $\sigma_\lambda : L \to \mathbb{C}$ such that $\sigma_\lambda(\pi) = \lambda$.

Suppose that $\alpha \neq 0$. Then there exists a root λ of $m_G(t)$ such that $\sigma_\lambda(\alpha) \neq 0$. Furthermore, since $\sigma_\lambda(\alpha)$ is an algebraic integer, we can choose λ in such a way that $|\sigma_\lambda(\alpha)| \geq 1$. Fix such a choice of λ, and if $\gamma \in \mathcal{O}$, we write $|\gamma|$ for $|\sigma_\lambda(\gamma)|$ to simplify notation. Writing $x = |\pi|$ we have:

$$x^r - 1 \leq |\pi^r - 1| \leq |\alpha(\pi^r - 1)| = |\pi^c + \pi^d - 2\pi^e| \leq x^c + x^d + 2x^e \leq x^{r-1} + 3x^{[r/2]}.$$

Since $x \geq \sqrt{2}$, a calculation shows $x^r > x^{r-1} + 4x^{[r/2]} > x^{r-1} + 3x^{[r/2]} + 1$ when $r \geq 15$, a contradiction. Thus $\alpha = 0$. □

Proof of Theorem 12. Let $r \geq 15$ be one of the infinitely many integers specified in Lemma 14. By Lemma 13, there exists a $P \in G'_{\mathrm{tors}}$ of order prime to N whose annihilator ideal in $R[1/N]$ is the ideal generated by $S(r)$. Furthermore, considering π as an endomorphism of G, it is not separable, so the degree of π is divisible by p, and therefore that of $1-\pi$ is prime to p. It follows that $1-\pi$ is a separable endomorphism of G and therefore that there exists $Q \in G_{\mathrm{tors}}$ such that $(1-\pi)Q = P$. If we write $Q = Q_p + Q'$, where Q_p is of p-power order and $Q' \in G'_{\mathrm{tors}}$, then since $P \in G'_{\mathrm{tors}}$, $(1-\pi)Q_p = O$, so without loss of generality we can take $Q \in G'_{\mathrm{tors}}$. We will show that given the hypotheses in the statement of the theorem, either Q is almost rational over k or G is of one of the types listed in Proposition 11.

Since $S(r)$ annihilates P, $\pi^r - 1$ annihilates Q, so since σ acts as multiplication by π, $\{\pi^a Q \mid 0 \leq a \leq r-1\}$ contains a complete set of Γ_k-conjugates of Q. Thus it suffices to show that either G is of one the exceptional types, or if a, $b \in \{0, 1, \dots, r-1\}$ are such that $\pi^a Q + \pi^b Q = 2Q$, then $a = b = 0$. We consider two cases, according as to whether at least one of a or b is less than $[r/2]$ or not.

Case 1. Suppose either a or $b \leq [r/2]$. Since $\pi^a Q + \pi^b Q = 2Q$, we have $(\pi^a + \pi^b - 2)Q = O$ and so $(S(a) + S(b))P = O$. By hypothesis, there exists $\alpha \in \mathcal{O}[1/N]$ such that $S(a) + S(b) = \alpha S(r)$. Since $S(r)_i$ and N are relatively prime for all i, in fact $\alpha \in \mathcal{O}$. Therefore $\pi^a + \pi^b - 2 = \alpha(\pi^r - 1)$ with $\alpha \in \mathcal{O}$.

By Lemma 15, $\alpha = 0$, so we have $\pi^a + \pi^b = 2$. Hence by the definition of R, $m_G(t)$ divides $t^a + t^b - 2$ in $\mathbb{Z}[t]$. Suppose that $(a, b) \neq (0, 0)$. If one of a or b was zero the constant term of $m_G(t)$ would divide 1, which is impossible by the Riemann hypothesis for function fields. Now if $a \geq 1$ and $b \geq 1$, the constant coefficient of each irreducible factor of $m_G(t)$ must divide 2, so must be ± 1 or ± 2, The possibility ± 1 is again excluded by the Riemann hypothesis. Hence $m_G(t)$ is irreducible, and this means that G is either a torus or an abelian variety. If G is a torus, then necessarily $m_G(t) = t \pm 2$, and $q = 2$. Since $t - 2$ cannot divide $t^a + t^b - 2$, we must have $m_G(t) = t + 2$, and G is isogenous to a power of M_2. When G is an abelian variety, then either $q = 4$ and $m_G(t)$ is linear, or $m_G(t)$ is an irreducible quadratic and $q = 2$. In the former case, $m_G(t) = t + 2$. Over $\mathbb{F}_4$, $\chi_{E_3}(t) = (t+2)^2$ so $\chi_G(t) = (t+2)^{2 \dim G} = \chi_{E_3^{\dim G}}(t)$, and G is $\mathbb{F}_4$-isogenous to $E_3^{\dim G}$. In the latter case, the Riemann hypothesis show that $m_G(t) = t^2 + ct + 2$ with $|c| \leq 2$. Since $(a, b) \neq (0, 0)$, $t^2 - t + 2$ and $t^2 - 2t + 2$ do not divide $t^a + t^b - 2$, so G must be isogenous over $\mathbb{F}_2$ to a power of E_1 or E_2 or E_3.

Case 2. Suppose that a and $b > [r/2]$. Let $c = a + [r/2] - r$, $d = b + [r/2] - r$, so that $0 \leq c, d < [r/2]$. Since $(\pi^a + \pi^b - 2)Q = O$ and $\pi^r Q = Q$, $(\pi^c + \pi^d - 2\pi^{[r/2]})Q = O$ and, arguing as in Case 1, one sees that there exists a $\beta \in \mathcal{O}$ such that $\pi^c + \pi^d - 2\pi^{[r/2]} = \beta(\pi^r - 1)$. Again

Lemma 15 shows that $\beta = 0$. As in Case 1, this implies that $m_G(t)$ divides $t^c + t^d - 2t^{[r/2]}$ in $\mathbb{Z}[t]$. Since c, $d < [r/2]$, this violates the Riemann hypothesis. □

6. Abelian varieties over p-adic fields

We can now apply the results of the last section to study almost rational torsion points on an abelian variety A over a p-adic field K. Unlike the case of number fields, $A^{\mathrm{ar}}_{\mathrm{tors},K}$ can be finite or infinite. Let K^{ur} denote that maximal unramified extension of K. Let q be the number of elements in the residue field k of K.

Proposition 16. *Let E be the elliptic curve defined by $y^2 + y = x^3$ over $\mathbb{Q}_2$. Then $E^{\mathrm{ar}}_{\mathrm{tors},\mathbb{Q}_2}$ is finite.*

Proof. Since E reduces mod 2 to a supersingular curve $\tilde{E}$, $\mathbb{Q}_2(E[2^\infty])/\mathbb{Q}_2$ is a totally ramified extension, so by the Néron-Ogg-Shafarevich criterion is linearly disjoint from $\mathbb{Q}_2(R)/\mathbb{Q}_2$ for any $R \in E_{\mathrm{tors}}$ of odd order. Hence by Lemma 1, if we decompose any $P \in E^{\mathrm{ar}}_{\mathrm{tors},\mathbb{Q}_2}$ as $P_2 + P'$, where P_2 is of 2-power order and P' is of odd order, then $P_2, P' \in E^{\mathrm{ar}}_{\mathrm{tors},\mathbb{Q}_2}$. By Proposition 2, there are only finitely many such P_2. Now $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ur}}/\mathbb{Q}_2)$ and $\Gamma_{\mathbb{F}_2}$ are isomorphic, so again by the Néron-Ogg-Shafarevich criterion, reduction modulo 2 puts points of $E^{\mathrm{ar}}_{\mathrm{tors},\mathbb{Q}_2}$ of odd order in one-to-one correspondence with $\tilde{E}^{\mathrm{ar}}_{\mathrm{tors},\mathbb{F}_2}$. Since $\tilde{E}$ is what we called E_3 in Proposition 11, there are only finitely many such P' as well. □

Theorem 17. *For any abelian variety A of dimension g over the p-adic field K, there is a finite extension L of K of degree bounded only in terms of g, such that A has infinitely many almost rational torsion points over L.*

Proof. By Raynaud's criterion for semistable reduction (SGA 7, expose IX, Proposition 4.7, see [25] for more recent results), replacing K by $K(A[12])$ if necessary, we can assume that A has semistable reduction, so the connected component A_0 of the special fibre of the Néron model of A is a semi-abelian variety over k. Likewise, replacing K by its unramified extension of degree 2 or 3 if necessary, we can assume that $q \neq 2, 4$. Theorem 12 shows that $(A_0)^{\mathrm{ar},\prime}_{\mathrm{tors},k}$ is infinite. Let $A'_{\mathrm{tors}}(K^{\mathrm{ur}})$ denote the torsion points of A of order prime to q defined over K^{ur}. Proposition 3 on page 179 of [3] shows that the reduction map $\rho : A'_{\mathrm{tors}}(K^{\mathrm{ur}}) \to (A_0)'_{\mathrm{tors}}$ is a bijection. Again, since $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ and Γ_k are isomorphic, ρ restricts to a bijection between $A^{\mathrm{ar}}_{\mathrm{tors},K} \cap A'_{\mathrm{tors}}(K^{\mathrm{ur}})$ and $(A_0)^{\mathrm{ar},\prime}_{\mathrm{tors},k}$, which is all we need. □

Remark. As in Proposition 16, if M is the torus over $\mathbb{Q}_2$ which is the non-trivial twist of $\mathbb{G}_m$ over the unramified quadratic extension of $\mathbb{Q}_2$, then

$M^{\mathrm{ar}}_{\mathrm{tors},\mathbb{Q}_2}$ is finite. In addition, an argument similar to that in Theorem 17 shows that for any torus M over a p-adic field K that is split over an unramified extension of K, that replacing K by its unramified quadratic extension if necessary, M has infinitely many almost rational torsion points over K.

References

[1] M. H. Baker, K. A. Ribet. *Galois theory and torsion points on curves*. Journal de Théorie des Nombres de Bordeaux **15** (2003), 11–32.

[2] Z. I. Borevich, I. R. Shafarevich. *Number Theory*. Academic Press, New York, San Francisco and London, (1966).

[3] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **21**. Springer-Verlag, Berlin, 1990.

[4] J. Boxall, D. Grant. *Theta functions and singular torsion on elliptic curves*, in *Number Theory for the Millenium*, Bruce Berndt, et. al. editors. A K Peters, Natick, (2002), 111–126.

[5] J. Boxall, D. Grant. *Singular torsion points on elliptic curves*. Math. Res. Letters **10** (2003), 847–866.

[6] J. Boxall, D. Grant. *Examples of torsion points on genus two curves*. Trans. AMS **352** (2000), 4533–4555.

[7] F. Calegari. *Almost rational torsion points on semistable elliptic curves*. Intern. Math. Res. Notices (2001), 487–503.

[8] R. Coleman. *Torsion points on curves and p-adic abelian integrals*. Ann. of Math. (2) **121** (1985), no. 1, 111–168.

[9] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry*. Graduate Texts in Mathematics **150**. Springer-Verlag, New York, 1995.

[10] S. Lang. *Complex Multiplication*. Springer-Verlag, New York, (1983).

[11] D. Masser, G. Wüstholz. *Galois properties of division fields*. Bull. London Math. Soc. **25** (1993), 247–254.

[12] B. Mazur. *Rational isogenies of prime degree*. Invent. Math. **44** (1978), 129–162.

[13] L. Merel. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. **124** (1996), 437-449.

[14] M. Newman. *Integral matrices*. Academic Press, New York and London (1972).

[15] T. Ono. *Arithmetic of algebraic tori*. Ann. Math. **74** (1961), 101–139.

[16] P. Parent. *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*. J. reine angew. Math. **506** (1999), 85–116.

[17] F. Pellarin. *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques*. Acta Arith. **100** (2001), 203–243.

[18] M. Raynaud. *Courbes sur une variété abélienne et points de torsion*. Invent. Math. **71** (1983), 207–233.

[19] K. Ribet, M. Kim. *Torsion points on modular curves and Galois theory*. Notes of a series of talks by K. Ribet in the Distinguished Lecture Series, Southwestern Center for Arithmetic Algebraic Geometry, May 1999. arXiv:math.NT/0305281

[20] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. Benjamin, New York (1968).

[21] J.-P. Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), 259–332.

[22] J.-P. Serre. *Algèbre et géométrie*. Ann. Collège de France (1985–1986), 95–100.

[23] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Iwanami Shoten Publishers and Princeton University Press (1971).

[24] A. Silverberg. *Fields of definition for homomorphisms of abelian varieties*. J. Pure and Applied Algebra **77** (1992), 253–272.

[25] A. Silverberg and Yu. G. Zarhin. *Étale cohomology and reduction of abelian varieties*. Bull. Soc. Math. France. **129** (2001), 141–157.

[26] J. Tate. *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2** (1966), 134–144.

[27] E. Viada. *Bounds for minimal elliptic isogenies*. Preprint.

Laboratoire de Mathématiques Nicolas Oresme, CNRS – UMR 6139, Université de Caen, boulevard Maréchal Juin, BP 5186, 14032 Caen cedex, France
E-mail : boxall@math.unicaen.fr

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395 USA
E-mail : grant@boulder.colorado.edu