Canad. J. Math. Vol. **60** (3), 2008 pp. 532–555

Local Bounds for Torsion Points on Abelian Varieties

Pete L. Clark and Xavier Xarles

Abstract. We say that an abelian variety over a p-adic field K has anisotropic reduction (AR) if the special fiber of its Néron minimal model does not contain a nontrivial split torus. This includes all abelian varieties with potentially good reduction and, in particular, those with complex or quaternionic multiplication. We give a bound for the size of the K-rational torsion subgroup of a g-dimensional AR variety depending only on g and the numerical invariants of K (the absolute ramification index and the cardinality of the residue field). Applying these bounds to abelian varieties over a number field with everywhere locally anisotropic reduction, we get bounds which, as a function of g, are close to optimal. In particular, we determine the possible cardinalities of the torsion subgroup of an AR abelian surface over the rational numbers, up to a set of 11 values which are not known to occur. The largest such value is 72.

Introduction

In this paper we are motivated by the following problem. Let $A_{/K}$ be an abelian variety defined over a number field. What can be said about the size of the torsion subgroup of $A(K)$, as a function of K (and especially, of $d = [K:\mathbb{Q}]$) and A (and especially, of $g = \dim A$)? When $g = 1$, deep work initiated by Mazur, continued by Kamienny and brought to culmination by Merel [Me] tells us that there is a function $F = F(d)$ such that for any number field K with $[K:\mathbb{Q}] = d$ and any elliptic curve $E_{/K}$, $\#E(K)[\mathrm{tors}] \leq F(d)$.

We would like to know on the one hand "the truth" about the asymptotics of the minimal such function F. Work by Merel and Parent gives an explicit bound, but it is exponentially larger than what we suspect it should be (and certainly, than any examples we can provide). On the other hand, we would like to know that $F(d)$ extends to a function $F(g, d)$ which majorizes the order of the torsion subgroup of every g-dimensional abelian variety defined over a degree d number field.

We are not in a position to generalize either Merel's uniform boundedness theorem to higher g or the precise classification results of Mazur, Kamienny and Parent to higher d. Instead, we will give a generalization of the following fact, which can be viewed as "Step 0" of Mazur's classification of the torsion subgroups of rational elliptic curves: namely, that it would suffice to bound the order of the torsion subgroup of elliptic curves over any completion of K. Unfortunately this cannot always be done.

Received by the editors June 22, 2005.

The research of the second author was partially supported by the grant MTM2006-11391 from the Spanish MEC.

AMS subject classification: Primary: 11G10; secondary: 14K15.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

For any prime p and any positive integer N, there exists an elliptic curve $E/\mathbb{Q}_p$ with a point of exact order N. However, for sufficiently large N (depending on p), one can say a great deal about what these curves must be. Indeed, it is known that the order of $E(\mathbb{Q}_p)[\text{tors}]$ is uniformly bounded as $E/\mathbb{Q}_p$ ranges over all elliptic curves which are *not* Tate curves, *i.e.,* do not have split multiplicative reduction. This implies that the "bad elliptic curves" are restricted in moduli: they have nonintegral j-invariant. But the restriction is not only on moduli, since an elliptic curve with non-integral j-invariant can still have additive or nonsplit multiplicative reduction over its field of definition but become a Tate curve after a field extension.

It is not quite clear to whom this result should be attributed. Perhaps John Tate is a good choice, as the two key points are his work on p-adic uniformization and his algorithmic computation/classification of the special fiber of the Néron model, from which one deduces the boundedness of the component group when the reduction is not split multiplicative. In any case, it was Flexor and Oesterlé [FO] who did a serious analysis of what these bounds turn out to be, getting especially striking results in the case of additive reduction. They also observed, building on work of Frey, that the uniform boundedness of torsion on elliptic curves would follow from their local results together with the Szpiro conjecture.

We say that an abelian variety defined over a complete local field has *anisotropic reduction* (or is an AR *abelian variety*) if its Néron special fiber does not contain a copy of $\mathbb{G}_m$.[1] The Main Theorem of this paper gives explicit bounds on the torsion subgroup of a g-dimensional AR abelian variety defined over a p-adic field K, depending only on g, p and $[K:\mathbb{Q}_p]$. This includes the case in which A has potentially good reduction, and in this case the existence of a bound can be found in the literature [Sg2, Sg3].

Our results go further than what was previously known in two respects. First, as in the elliptic curve case, we require only the weaker hypothesis of anisotropic reduction. Second, following the spirit of Flexor and Oesterlé, we are interested, not just in boundedness, but in the bounds themselves. The bounds that we get are not optimal, but they are as a function of g significantly better than what was previously known even for the smaller class of abelian varieties with complex multiplication.

Indeed, at the end of the paper we give applications of the Main Theorem to classifying torsion subgroups of abelian varieties over $\mathbb{Q}$, not (alas) for all abelian varieties, but for abelian varieties which have everywhere anisotropic reduction. We hope to convince the reader that, in general, these kinds of restricted global classification results are within reach, and that by getting such classifications and comparing them to the known examples of torsion points on not necessarily AR abelian varieties, one can begin to get a sense of the true order of magnitude of $F(g,d)$. We also note what seems to be the higher-dimensional analogue of Flexor and Oesterlé's global observation: namely, that our results, together with a certain "generalized Szpiro conjecture" would imply uniform boundedness of rational torsion on all Hilbert–Blumenthal abelian varieties.

[1] Implicit in this terminology is the extension of the concept of an *anisotropic linear group*, *i.e.,* one that does not contain a split torus, to arbitrary algebraic groups. See §2 for more details.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

1 Statements of Main Results

In this paper, a *complete field* means a field K complete with respect to a discrete valuation v, and a *local field* is a complete field with finite residue field, whose characteristic we denote by p. The absolute ramification index of a local field is $e = v(p) \leq \infty$. If $A_{/K}$ is an abelian variety over a local field, then $A(K)[p^\infty]$ denotes the subgroup of p-primary torsion and $A(K)[\mathrm{tors}]'$ denotes the subgroup of torsion of order prime to p.

Recall that an abelian variety over a complete field K is said to have *potentially good reduction* if there exists a finite field extension L/K such that the base change of A to L is the generic fiber of an abelian scheme over the valuation ring of L. If R is any Dedekind domain with quotient field K, we will say that an abelian variety $A_{/K}$ has *(R)-integral moduli* if for every prime ideal v of R, the base change of A to the completion of K at v has potentially good reduction. Sometimes for brevity we shall speak of an *IM abelian variety*, which means an abelian variety defined over a number field and having $\mathcal{O}_K$-integral moduli.

For a g-dimensional variety A over a local field K, we define numerical invariants α, μ and β to be, respectively, the dimensions of the unipotent, toric and abelian parts of the special fiber of the Néron model. Relevant aspects of the structure theory of the Néron model are recalled in §2.

For a positive integer a, define

$$M(a,2) := \left\lfloor \frac{a}{2} \right\rfloor + \sum_{j=0}^{\infty} \left\lfloor \frac{a}{2^j} \right\rfloor,$$

and if p is an odd prime

$$M(a,p) := \sum_{i=0}^{\infty} \left\lfloor \frac{a}{q^i(q-1)} \right\rfloor.$$

Let $\eta(a) = \prod_p p^{M(a,p)}$, where the product extends over all primes. Let $\gamma_p(m) = \lfloor \log_p(\frac{pm}{p-1}) \rfloor$.

Main Theorem *Let K be a local field with residue cardinality $q = p^f$ and absolute ramification index e. Let $A_{/K}$ be a g-dimensional abelian variety.*

(i) *Suppose $A_{/K}$ has potentially good reduction. Then*

$$\#A(K)[\mathrm{tors}]' \leq \lfloor (1+\sqrt{q})^2 \rfloor^g. \tag{1}$$

(ii) *Suppose that K is a p-adic field and $A_{/K}$ has anistropic reduction. Then*

$$\#A(K)[\mathrm{tors}] \leq 2^{2\alpha} p^{f\alpha + 2g\gamma_p(e)} (q+1)^\mu \lfloor (1+\sqrt{q})^2 \rfloor^\beta \eta(2u).$$

and

$$\#A(K)[\mathrm{tors}]' \leq 2^\alpha (q+1)^\mu \lfloor (1+\sqrt{q})^2 \rfloor^\beta.$$

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

(iii) *Suppose K is p-adic and $A_{/K}$ has purely unipotent reduction ($\mu = \beta = 0$). Then*

$$\#A(K)[\text{tors}] \le \eta(2g) \cdot p^{2g\gamma_p(e\cdot\eta(2g))}. \tag{2}$$

In particular, if $\ell \ne p$ is a prime divisor of $\#A(K)[\text{tors}]$, then $\ell \le 2g + 1$.

(iv) *If $K = \mathbb{F}_q((T))$, then there exists a sequence of elliptic curves $(E_n)_{/K}$, all of which are ordinary with supersingular (good) reduction, such that $p^n \mid \#E_n(K)[\text{tors}]$.*

Some remarks are in order. First, since the right-hand side of (2) is at most $\lfloor(1 + \sqrt{q})^2\rfloor^g$, part (i) is a consequence of part (ii), and indeed the bound of part (i) holds for all AR abelian varieties. We have chosen to isolate part (i) because the proof uses significantly less machinery.

Since $\gamma_p(m) = 0$ for $p \gg m$, the bound in part (iii) may be viewed as being independent of p. Thus the result is, qualitatively, a generalization of work of Flexor and Oesterlé, who proved the remarkable bound $\#E(K)[\text{tors}] \le 48e$ for elliptic curves with additive reduction over p-adic fields. However, taking $g = 1$, the bound we get in part (iii) is (unfortunately) quadratic in e. In fact we suspect that for all g, one should be able to get a bound of the form $C(g)e^g$ rather than $C(g)e^{2g}$. (It will be seen that the problem is our less than complete understanding of component groups of Néron models of higher-dimensional abelian varieties.)

In contrast to the case of p-adic fields, there is not much in the literature concerning torsion groups of (even) elliptic curves over local fields of positive characteristic. Part (iv) of the main theorem shows that this case is qualitatively different from the p-adic case: we find that whereas for a locally compact field K of characteristic zero the torsion subgroup of an elliptic curve $E_{/K}$ is uniformly bounded on any affinoid subdomain of the compactified moduli space $\mathbb{P}^1_{/K}$ which does not contain the cusp ∞, in positive characteristic torsion becomes infinite not only as one approaches the boundary of the moduli space but also as one approaches a higher Newton polygon stratum. It would be interesting to explore the analogous phenomenon on the moduli space of g-dimensional abelian varieties.

The proof of parts (i)–(iii) of the Main Theorem in the case of potentially good reduction is obtained by combining several techniques and concepts that are certainly well known to the experts: the Chevalley decomposition of an algebraic group, the functorial properties of the Néron model and the base-changing map, the structure of the component group, the group of rational points of an algebraic group over a finite field, and the torsion subgroup of the formal group. In the general case we need to work in a more general context: we use Raynaud's extension of the notion of a Néron model to *semi* abelian varieties together with an analytic uniformization result which reduces the general case to the potentially good reduction case together with an analysis of the case of linear tori.

We have chosen to present an account, in some detail, of each of these topics (§2). In particular, we get a three-step filtration on $A(K)[\text{tors}]$. Separate bounds for the orders (or at least, the exponents) of the successive graded quotients occur in §3.1–3.4, and then these bounds are used to get the proof of the theorem in §3.5.

One consequence of the Main Theorem is that totally indefinite quaternionic Shimura varieties with $\Gamma_1(N)$-level structure will, for sufficiently large N, fail to have

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

points rational over any given p-adic field. Because it is somewhat technical to make precise the moduli problem corresponding to a $\Gamma_1(N)$-level structure in the higher-dimensional case, we will content ourselves here with the case of Shimura curves over $\mathbb{Q}$, in which case a careful description of the moduli problem may be found in [Bu].

Given $D > 1$ a squarefree positive integer, let $B = B_D$ be the indefinite rational quaternion algebra with discriminant D. For any positive integer N prime to D, we let $X_1^D(N)_{/\mathbb{Q}}$ be the Shimura curve associated to the group $B^\times$ and the congruence subgroup $\Gamma_1(N)$.

Theorem 1.1 *For each prime number p and a positive integer $d \geq 1$, there exists a constant $N_0 = N_0(p,d)$ with the following property: for any p-adic field $K/\mathbb{Q}_p$ with $[K\colon\mathbb{Q}_p] \leq d$ and any integer $N \geq N_0$, $X_1^D(N)(K) = \varnothing$.*

Note that the integer N_0 does *not* depend upon the quaternionic discriminant D.

Proof For $N \geq 4$ and $F/\mathbb{Q}$ any field of characteristic zero, to a point $P \in X_1^D(N)(F)$ we can associate A/F an abelian surface, $\iota\colon B \hookrightarrow \operatorname{End}_F(A) \otimes \mathbb{Q}$ a quaternionic multiplication (QM) structure, and $x \in A(F)$ a point of exact order N. Now suppose K is a local field and $P = (A, \iota, x) \in X_1^D(N)(K)$.

Claim A QM surface necessarily has potentially good reduction. Indeed, any d-dimensional abelian variety admitting as a subring of endomorphisms an order $\mathcal{O}$ in a $2d$-dimensional division algebra has potentially good reduction (note that this also includes the CM case).

To see this, by a theorem of Grothendieck, after a finite base change there is no additive part. Moreover, the character group, if nontrivial, would be the underyling $\mathbb{Z}$-module of a (necessarily faithful) representation of $\mathcal{O}$, but its dimension is at most d, whereas any nontrivial representation of $\mathcal{O}$ has dimension at least $2d$. This proves the claim.

Thus the result follows immediately from the Main Theorem. ■

The remainder of the paper pursues applications of the Main Theorem to bounding torsion on certain abelian varieties over number fields. An immediate consequence is the following.

Corollary 1.2 *Let $A_{/K}$ be of dimension g and defined over K with $[K\colon\mathbb{Q}] = d$.*

(i) *Assume that A has anisotropic reduction at places v_2, v_3 of K over 2 and 3. Then $\#A(K)[\text{tors}] \leq B(g,d) := \lfloor (1+2^{\frac{d}{2}})^2 \rfloor^g \lfloor (1+3^{\frac{d}{2}})^2 \rfloor^g$.*

(ii) *Assume that A has potentially good reduction at a place v_2 of K over 2.*

Then the maximum prime order of a torsion point is $\lfloor (1+2^{\frac{d}{2}})^2 \rfloor^g$.

Proof For part (i), let $\iota_2\colon A(K)[\text{tors}] \to A(K_{v_2})[\text{tors}]'$ be the composite of the natural embedding of the global torsion points into the local torsion points with projection onto the prime-to-2-torsion, and define $\iota_3\colon A(K)[\text{tors}] \to A(K_{v_3})[\text{tors}]'$ similarly. Then the product map

$$\iota_2 \times \iota_3\colon A(K)[\text{tors}] \to A(K_{v_2})[\text{tors}]' \times A(K_{v_3})[\text{tors}]'$$

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

is evidently an injection, so the result follows from the Main Theorem (ii). Injecting the odd order torsion into $A(K_{v_2})[\mathrm{tors}]'$ gives part (ii). ■

Remark. The existence of a strong bound on torsion for IM varieties is due to Alice Silverberg [Sg2, Sg3]. She gives the bound:

$$\#A(K)[\mathrm{tors}] \leq \lfloor (1 + 2^{\#GL_{2g}(\mathbb{Z}/3\mathbb{Z})d/2})(1 + 3^{\#GL_{2g}(\mathbb{Z}/4\mathbb{Z})d/2}) \rfloor^{2g}.$$

As an example of the improvement that the present results provide, in the case of abelian surfaces over $\mathbb{Q}$, Corollary 2 gives $\#A(\mathbb{Q}) \leq 1225$, while Silverberg's bound is approximately $4.0262 \times 10^{1275357349}$.

But the bound of Corollary 1.2 is still visibly far from the truth: because we are double counting the prime-to-6 torsion, we will in practice get much better bounds by applying part (i) of the Main Theorem prime by prime and collating the results. The point that we want to emphasize is that, at least when d is small, this collation process leads to *short lists* of possible orders for the torsion subgroup, *i.e.,* it becomes feasible to give serious individual consideration to each of the elements on the list as to whether or not they actually arise globally.

We give one instance where our methods can be used to give a classification result, and one instance where we are tantalizingly close to a classification.

Theorem 1.3 *Let $E/\mathbb{Q}$ be an elliptic curve with everywhere anistropic reduction (*i.e., *has no prime of split multiplicative reduction). Then $E(\mathbb{Q})[\mathrm{tors}]$ is one of the following groups:*

$$0, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Conversely, all such groups occur among elliptic curves $E/\mathbb{Q}$ with $j = 0$ and $j = 1728$.

Remark. Theorem 1.3 extends a result of Gerhard Frey [Fr], which itself extends a result of Loren Olson [Ol]. Olson's paper gives a complete classification of the possible torsion subgroups of CM elliptic curves over $\mathbb{Q}$ (in fact a separate classification for each of the 13 j-invariants). Frey's theorem extends the classification to elliptic curves with integral j-invariant. What is notable is that the purely local methods of the Main Theorem rule out all extraneous possibilities except for $\mathbb{Z}/5\mathbb{Z}$.

Theorem 1.3 is proved in Section 4.

In the next result (and in Section 5) we use the interval notation $[a, b]$ to mean the set of all integers x such that $a \leq x \leq b$.

Theorem 1.4 *Let $A/\mathbb{Q}$ be an abelian surface with everywhere anisotropic reduction. Then the order of the torsion subgroup $\#A(\mathbb{Q})[\mathrm{tors}]$ lies in the following set:*

$$[1, 16] \cup [18, 20] \cup \{22, 24, 25, 28, 30, 36, 48, 60, 72\}. \tag{3}$$

Conversely, every value in the set $[1, 10] \cup \{12, 16, 18, 19, 20, 24, 36\}$ is known to occur.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

Remark. Note well that Theorem 1.4 leaves us with 11 numbers N for which we do not know whether there exists an AR abelian surface $A/\mathbb{Q}$ with $A(\mathbb{Q})[\text{tors}] = N$. This is nevertheless a substantial improvement over what was previously known even in the special case of CM abelian surfaces, *cf.* [Sg1, VanM].

Section 4 is devoted to the proof of Theorem 2.1. The upper bounds are purely local but use more than the Weil bound (1), which is far from being sharp for higher-dimensional abelian varieties over $\mathbb{F}_2$ and $\mathbb{F}_3$.

We end this introduction with some further remarks comparing our function $B(g, d)$ to the "true function" $F(g, d)$, *i.e.*, the supremum over all $\#A(K)[\text{tors}]$ where $\dim(A) = g$, $[K:\mathbb{Q}] = d$. As $F(g, d)$ is not even known to be finite for $g > 1$, some of these remarks are necessarily speculative.

Notice that the behavior of the function $B(g, d)$ is essentially symmetric in g and d: when either variable is fixed, it is exponential in the other variable. Clearly the bound must be exponential in g: as above, there exists a CM elliptic curve $E/\mathbb{Q}$ with $\#E(\mathbb{Q})[\text{tors}] = 6$, so the g-dimensional abelian variety $A/\mathbb{Q} = E^g$ has $\#A(\mathbb{Q})[\text{tors}] = 6^g$. Unfortunately we do not have the right exponential $B(g, 2) = 35^g$ which is surely too large. More reasonable (but still not optimal, by Theorem 1.3) is $B(g, 1)[\text{odd}] = 5^g$.

On the other hand, being exponential in d is probably very far from the truth. The main theorem of [HS] gives $\#E(K)[\text{tors}] \leq 1977408 d \log d$ for all elliptic curves with integral moduli. For the class of CM elliptic curves, [Sg1, Sg2, PY] show that the exponent of the torsion group is at most $d \log \log d$. On the other hand, choosing a fixed CM elliptic curve and trivializing its p-torsion for successively large primes p gives fields K with $E(K)[\text{tors}] \geq C'(E) d \sqrt{\log \log d}$, so that the above upper bounds are quite close to being sharp. We see no reason to expect better lower bounds for $d \gg 0$.

2 Some Background

In this section we will briefly recall some key definitions and results about Néron–Raynaud) models of semiabelian varieties as well as the Serre–Tate theory of abelian varieties with potentially good reduction.

2.1 The Chevalley Decomposition

Assume for the moment that K is any perfect field, and let $G_{/K}$ be a smooth, geometrically connected commutative algebraic group over K. Then there is a (unique and functorial) short exact sequence, the *Chevalley decomposition*:

$$0 \to T \oplus U \to G \to B \to 0,$$

where $T_{/K}$, $U_{/K}$, and $B_{/K}$ are respectively a linear torus, a commutative unipotent group and an abelian variety [BLR]. We consistently use the following notation: $\mu = \dim T$ (the toric rank), $\alpha = \dim U$ (the unipotent rank) and $\beta = \dim B$ (the abelian rank). In the extremal cases $G = T$, U, or B, we say that G is purely toric, purely unipotent or purely abelian. If $\alpha = 0$, one says that G is *semiabelian*; if $\mu = 0$, we may say that G is *atoric*.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

2.2 Tori

By definition, a (linear) torus $T_{/K}$ is an algebraic group such that $T^{\mathrm{sep}}_{/K} \cong \mathbb{G}_m^r$ for some r. To every torus we associate its character group

$$X(T) = \mathrm{Hom}(T(K^{\mathrm{sep}}), \mathbb{G}_m(K^{\mathrm{sep}})),$$

which is a free abelian group of rank r endowed with the structure of a $\mathfrak{g}_K$-module. The association $T \mapsto X(T)$ gives an antiequivalence from the category of tori over K to the category of $\mathbb{Z}[\mathfrak{g}_K]$-modules which are finitely generated and torsion-free as abelian groups. Moreover, the association $T \mapsto X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ gives an antiequivalence from the isogeny category of tori to the category of finite-dimensional representations of $\mathfrak{g}_K$ on $\mathbb{Q}$-vector spaces which are continuous, *i.e.*, have finite image. In particular, tori up to isogeny form a semisimple category.

We say that a torus is *split* if it is isomorphic to $\mathbb{G}_m^r$ already over K. Let $X(T)^{\mathfrak{g}}$ denote, as usual, the submodule of $\mathfrak{g}$-invariants (which is always $\mathbb{Z}$-torsion free), and let $X(T)_{\mathfrak{g}}$ be maximal torsion-free quotient of $X(T)$ on which $\mathfrak{g}$ acts trivially, *i.e.*, the usual coinvariants divided out by the torsion subgroup. Then the maps $X(T)^{\mathfrak{g}} \to X(T)$ and $X(T) \to X(T)_{\mathfrak{g}}$ give rise to, respectively, the maximal split quotient torus and the maximal split subtorus of T. These tori are isogenous, and we denote by s their common rank, the *split toric rank*. If $s = 0$, we say T is *anisotropic*.

If $G_{/K}$ is now any smooth commutative algebraic group, we can define $X(G)$ to be the character group of its toric part; the assignment $G \mapsto X(G)$ is (co-)functorial in G. In particular, we can speak of $G_{/K}$ being anisotropic, *i.e.*, $X(G)^{\mathfrak{g}} = 0$.

2.3 Néron Models of Semiabelian Varieties

Now let G_K be a commutative algebraic group over a complete (always discretely valued) field K. A *Néron–Raynaud* model for G is a smooth, separated group scheme $G_{/R}$ whose generic fiber is isomorphic to G_K and which satisfies the Néron mapping property: if X is any smooth R-scheme, then every morphism $u_K \colon X_K \to G_K$ of the generic fibers extends uniquely to a morphism $u \colon X \to G$. As this is a universal mapping property, the Néron–Raynaud model for G_K, if it exists, is unique up to a unique isomorphism.

It is a famous (and difficult) theorem of Néron that such a model exists when $G = A$ is an abelian variety. Not quite as well known is Raynaud's generalization of Néron's existence theorem to the case of semi-abelian varieties. (Conversely, since K is perfect, if $G_{/K}$ admits a Néron model, then it has no unipotent part.) There is one caveat in the passage to the semiabelian case: the group scheme $G_{/R}$ need not be of finite type. In particular, the special fiber $G_{/k}$ is a *locally algebraic group*, *i.e.*, of the form

$$0 \to G^0_{/k} \to G_{/k} \to \Phi_{/k} \to 0,$$

where $G^0_{/k}$ is a geometrically connected algebraic group and $\Phi_{/k}$ is a possibly infinite étale group scheme. We will identify Φ with the $\mathfrak{g}_k$-module $\Phi(k^{\mathrm{sep}})$ and also write $\Phi' = \Phi/\Phi[p^\infty]$, where p is the characteristic of the residue field. (If k has characteristic zero, we mean that $\Phi' = \Phi$.) Then $G_{/R}$ is of finite type if and only if $\Phi(k^{\mathrm{sep}})$

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

is finite if and only if $G_{/K^{\mathrm{unr}}}$ is anisotropic, where K^{unr} is the maximal unramified extension of K. For proofs of all these facts, see [BLR].

In particular, if $G = A$ is an abelian variety, then the Néron special fiber is an algebraic group $G_{/k}$, hence is the extension of a finite étale group scheme $\Phi_{/k}$, the *component group*, by a smooth geometrically connected algebraic group $G^0_{/k}$. The Néron component group of an abelian variety is quite mysterious; despite much effort and interesting work, we are, except in the case of elliptic curves (or of Jacobians of curves with rational points), very far from a complete understanding of its structure. In contrast, in the purely toric case the finitely generated component group Φ is a purely cohomological quantity and is accordingly much better understood.

Theorem 2.1 **([Xa])** *Let $T_{/K}$ be a torus defined over a complete field K with perfect residue field k. Let $I = \mathfrak{g}_{K^{\mathrm{unr}}} \subset \mathfrak{g}_K$ be the inertia subgroup, and Φ the component group of the Néron special fiber of T. Then there is an exact sequence of $\mathfrak{g}_k$-modules*

$$0 \longrightarrow \operatorname{Hom}(H^1(I, X(T)), \mathbb{Q}/\mathbb{Z}) \longrightarrow \Phi \longrightarrow \operatorname{Hom}(X(T)^I, \mathbb{Z}) \longrightarrow 0.$$

Note that $H^1(I, X(T))$, being a Galois cohomology group with coefficients in a Galois module which is finitely generated as an abelian group, is finite [Se1]. Moreover $\operatorname{Hom}(X(T)^I, \mathbb{Z})$ is a $\mathfrak{g}_K$-module whose underlying abelian group has rank equal to the split rank of $T_{/K^{\mathrm{unr}}}$. It follows that $\Phi(k) \cong \mathbb{Z}^s \oplus (H^1(I, X(T))^{\mathfrak{g}_k})^\vee$, where s is the split toric rank of the Néron special fiber of $T_{/K}$; here the "$\vee$" denotes the Pontrjagin dual of a finite abelian group.

Corollary 2.2 *Let $T_{/R}$ be the Néron model of a torus $T_{/K}$ defined over a complete field K, with valuation ring R and with perfect residue field. There is an exact sequence*

$$0 \longrightarrow T^0(R)[\mathrm{tors}] \longrightarrow T(K)[\mathrm{tors}] \longrightarrow (H^1(I, X(T))^{\mathfrak{g}_k})^\vee.$$

Proof This follows immediately from the previous theorem, using the equality $T(R) = T(K)$ (guaranteed by the Néron mapping property) and the fact that

$$T(R)/T^0(R) = T(k)/T^0(k)$$

(because the kernel of reduction is contained in $T^0(R)$). ■

The alert reader may be wondering why we are considering Néron models of tori in order to bound torsion on abelian varieties. The explanation is the following result, which allows us to reduce the anisotropic reduction case to the case of potentially good reduction and to the case of tori.

Theorem 2.3 **(Uniformization Theorem)** *Let $A_{/K}$ be a g-dimensional abelian variety over a complete field. Then there exists a semiabelian variety $S_{/K}$ of dimension g, whose abelian part has potentially good reduction, a $\mathfrak{g}_K$-module M whose underlying abelian group is torsion free of rank equal to the toric rank of S and an exact sequence of $\mathfrak{g}_K$-modules*

$$0 \longrightarrow M \longrightarrow S(K^{\mathrm{sep}}) \longrightarrow A(K^{\mathrm{sep}}) \longrightarrow 0. \tag{4}$$

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

Moreover $\mathrm{rk}_{\mathbb{Z}} M^{\mathfrak{g}_K} = s$, *the split toric rank of the Néron special fiber of* A. *For every finite extension* L/K, *the identity components of the Néron special fibers of* $S_{/L}$ *and* $A_{/L}$ *are isomorphic.*

Proof The theorem is a direct consequence of some of the main results of [BX]. Indeed, the exactness of the sequence follows from [BX, Theorem 1.3], using the fact that exactness of a sequence of rigid K-analytic étale sheaves is equivalent to the exactness of the sequence of points over K^{sep}. Next, the proof of [BX, Proposition 5.1] shows that the ranks of $M_K^{\mathfrak{g}}$ and $X(S)_K^{\mathfrak{g}}$ coincide, so both quantities are equal to the split toric rank of S_k. The last sentence follows from [BX, Theorem 2.3]. ■

2.4 Potentially Good Reduction

Let $A_{/K}$ be an abelian variety over a complete field. If the residue field of K is algebraically closed, then Serre and Tate showed that there is a unique minimal field extension L/K over which A acquires potentially good reduction. This extension is given explicitly as $L = K(A[N])$, the field obtained by trivializing the Galois action on the N division points, for any N which is at least 3 and prime to the residue characteristic p of K.

It follows from this (and the fact that formation of the Néron model commutes with étale base change, which is immediate from its defining property) that if K is any complete field and $A_{/K}$ has potentially good reduction, then $A_{/K(A[N])}$ has good reduction for $N \geq 3$ and prime to p.

Similarly, the numbers μ, α, β associated to $A_{/K}$ are invariant under unramified base extensions. Since A has bad reduction if and only if $\max(\mu, \alpha) > 0$, it is evident that if $A_{/K}$ has potentially good, but bad, reduction, then any extension over which it acquires good reduction must have some ramification. If K is a local field, one can choose (noncanonically) a totally ramified extension L/K over which A acquires good reduction [ST, p. 498].

Proposition 2.4 *For any abelian variety* A *over a local field* K, *the invariants* μ *and* β *of the Néron special fiber are nondecreasing under arbitrary finite base extensions. In particular, if* $A_{/K}$ *has potentialy good reduction,* $\mu = 0$.

Remark. This fact is certainly well known to the experts, and the second statement can be found (without proof) in the original paper of Serre and Tate [ST, p. 500]. We will sketch the proof here, for completeness, but also because it is a prototype of a certain kind of argument about Néron models (namely, use of the base-changing map) that we will see again in the proof of part (iii) of the Main Theorem.

Proof If L/K is a finite field extension, let R and S be the valuation rings of K and L, let $(A_R)/S$ be the base change of the Néron model of A_K to S, and let A_S be the Néron model of A_L. Since $(A_R)/S$ is smooth, the universal property of the Néron model A_S furnishes us with a morphism $u_S \colon (A_R)/S \to A_S$, the *base change map*, and in particular a morphism of the geometric special fibers $u_{k^{\mathrm{sep}}} : A_R(k^{\mathrm{sep}}) \to A_S(k^{\mathrm{sep}})$. A drop in either the toric or the abelian rank means that this map kills some nontrivial ℓ-torsion point for some (indeed, every) $\ell \neq p$. But since $[\ell]$ is an étale endomorphism of A_R and of A_S, such an ℓ-torsion point lifts uniquely to an ℓ-torsion point in

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

$A(L^{\mathrm{unr}}) = A_S(S^{\mathrm{unr}})$ which would then have lie in the kernel of the reduction map. But again, the fact that $A_S[\ell]$ is étale means that the reduction map is an isomorphism on ℓ-torsion; this gives a contradiction. ■

2.5 The Kernel of Reduction

If $G_{/R}$ is a smooth group scheme over the valuation ring of a complete field K, the completion $\widehat{G}_{/R}$ of G along the identity section is a formal Lie group over R, *i.e.*, given by a formal group law $F = (F_1, \dots, F_d), F_i \in R[[X_1, \dots, X_d, Y_1, \dots, Y_d]]$. Let $\mathcal{R}\colon G(R) \to G(k)$ be the reduction map. The kernel of reduction is an open K-analytic subgroup of $G(K)$; as a space, it is the open unit polydisk $\mathfrak{m}^{\dim G}$ (where $\mathfrak{m}$ is the maximal ideal of R); the group law is simply

$$x + y = (x_1, \dots, x_d) + (y_1, \dots, y_d) = (F_1(x, y), \dots, F_d(x, y)).$$

We write $G^1 = \operatorname{Ker}(\mathcal{R})$ for this structure, referred to in [Se3] as a "standard analytic group."

3 Proof of the Main Theorem

From the results of the preceding section, we know that if $A_{/K}$ is an abelian variety over a complete field K with valuation ring R, there exists a filtration

$$0 = \mathrm{Fil}^3 \subset \mathrm{Fil}^2 \subset \mathrm{Fil}^1 \subset \mathrm{Fil}^0 = A(K)$$

on the group of K-rational points $A(K) = A(R)$; namely $\mathrm{Fil}^1 \subset A(R)$ is the subgroup of points reducing to the identity component of the Néron model and $\mathrm{Fil}^2 \subset A(R)$ is the kernel of reduction. Let $\mathrm{Fil}^i(T) = \mathrm{Fil}^i \cap A(K)[\mathrm{tors}]$ be the induced filtration on the torsion subgroup, and write $H^i = \mathrm{Fil}^{i+1}(T)/\,\mathrm{Fil}^{i+2}(T)$ for the successive quotients. We have canonical injections $H^1 \hookrightarrow \Phi(k)$, $H^2 \hookrightarrow A^0(\mathbb{F}_q)$ and $H^3 \hookrightarrow A^1(R)[\mathrm{tors}]$. Thus one can get a bound on $A(K)[\mathrm{tors}]$ by giving separate bounds on these three latter quantities.

We can also get away with a bit less: if one has bounds on just the exponents of these three quantities, say $\exp(\Phi(k)) \leq c_1$, $\exp(A^0(\mathbb{F}_q)) \leq c_2$, $\exp(A^1(R)[\mathrm{tors}]) \leq c_3$, then clearly we have $\exp(A(K)[\mathrm{tors}]) \leq c_1c_2c_3$, and from this it follows that $\#A(K)[\mathrm{tors}] \leq (c_1c_2c_3)^{2g}$. What will actually occur is a mixture of these two arguments. We will get bounds on the order of $A^0(\mathbb{F}_q)$; our bounds for the order of $A^1(R)[\mathrm{tors}]$ are those which *come* from bounds on the exponent by raising to the $(2g)$-th power, and we will have bounds only on the exponent of $\Phi(k)$.

In Section 3.1 we bound the torsion in formal groups associated to abelian varieties in terms of e and g; there is also some discussion of what happens when $e = \infty$. In Section 3.2 we bound the number of $\mathbb{F}_q$-rational points on a connected algebraic group $G_{/\mathbb{F}_q}$ in terms of its invariants α, μ, β. In Section 3.3 we come to the heart of the matter, which is bounding the exponent of $\Phi(k)$. In the case of potentially good reduction, the bounds come directly from work of McCallum and Edixhoven–Liu–Lorenzini. (In this case the bounds apply to the geometric component group

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

$\Phi(\overline{k})$.) In the general case of anisotropic reduction, we use the uniformization theorem to bound the exponent of the component group $\Phi(k)$ of A in terms of the component group of an abelian variety with potentially good reduction and the component group of an anisotropic torus. Thus we must provide bounds on the component group of an anistropic torus, and this turns out to a be a straightforward piece of Galois cohomology.

All these bounds are put together in Section 3.4 to prove the first three parts of the Main Theorem. Part (iv) is proved in Section 3.5.

3.1 Bounds for the Torsion Subgroup of a Formal Group

Recall our notation $\gamma_p(m) = \lfloor \log_p(\frac{pm}{p-1}) \rfloor$.

Proposition 3.1 *Let $F(X,Y)$ be a d-dimensional formal group law over the valuation ring R of K, with associated "standard" K-analytic Lie group $G^1 = F(\mathfrak{m})$. Let $H \subset G^1$ be any finite subgroup. Then the exponent of H divides $p^{\gamma_p(e)}$.*

Proof This is well known when $g = 1$, *e.g.,* [Si1, Theorem 6.1]. The proof works verbatim in the higher-dimensional case provided we have a formal power series identity of the form

$$[p](T_1,\dots,T_g) = p\left((T_1,\dots,T_g) + \varphi(T_1,\dots,T_g)\right) + \psi(T_1,\dots,T_g),$$

where the lowest-degree form of φ has degree at least 2 and the lowest-degree form of ψ has degree at least p. But precisely this is shown in [Se3, § II.IV.7-9].

An immediate consequence is that if $p > e + 1$, there is no torsion in the formal group. This special case is much better known, as there is then a "pure thought" proof available: if $0 \neq P \in A(K)[\text{tors}]$, apply Raynaud's theory of finite flat group schemes to the schematic closure of $\langle P \rangle$ in the Néron model to conclude that the reduction of P still generates a constant group scheme of order N in the special fiber. ■

Remark. When $e = \infty$, *i.e.,* when K has positive characteristic, the proposition asserts nothing. We have instead the following result, whose proof was supplied to us by Bjorn Poonen.

Proposition 3.2 *Let K be a complete local field of equal characteristic $p > 0$, and $A_{/K}$ an abelian variety. Then the torsion subgroup of the kernel of reduction is finite.*

Proof Let $G^1 \subset A(K)$ be the kernel of reduction and let $(G^i)_{i\geq 1}$ be the standard decreasing filtration on G^1. Then G^i consists of g-tuples of elements of K whose valuation is at least i. Note that we have $\cap_i G^i = 0$; moreover, $G_i/G_{i+1} \cong (k,+)$ is a group of exponent p. Since $G^1 \subset A(K)$ we have $\#G^1[p] \leq p^g$, so $G^1[p]$ is a finite group. It follows that $G^n[p] = 0$ for all sufficiently large n, and if $G^N[p] = 0$, then $G^1[\text{tors}] = G^1[p^N]$ is a group of order at most p^{gN}. ■

Remark. That the p-power torsion in the kernel of reduction of an elliptic curve over $\mathbb{F}_q((T))$ can be arbitrarily large follows from part (iv) of the Main Theorem, as the bounds on H_2 and H_1 are valid in positive characteristic. Thus Proposition 3.2 is the best possible positive characteristic analogue of Proposition 3.1.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

3.2 Bounds for the Identity Component of the Néron Special Fiber

Let $G_{/\mathbb{F}_q}$ be a smooth, commutative geometrically connected algebraic group. Evidently $\#G(\mathbb{F}_q)$ is finite, as for any variety over a finite field. In order to get precise (and uniform) bounds on $\#G(\mathbb{F}_q)$, the Chevalley decomposition reduces us to separate consideration of the cases in which G is purely unipotent, purely toric, or purely abelian. Here is the result.

Proposition 3.3 *Let $G_{/\mathbb{F}_q}$ be a smooth, geometrically connected algebraic group of dimension g.*

(i) *If $G = U$ is unipotent, $\#G(\mathbb{F}_q) = q^g$.*
(ii) *If $G = T$ is toric, $\#G(\mathbb{F}_q) \leq (q+1)^g$.*
(iii) *If $G = B$ is abelian, $\#G(\mathbb{F}_q) \leq \lfloor (1+\sqrt{q})^2 \rfloor^g$.*

For each prime power q and positive integer g, all three bounds can be attained.

Proof We begin by noting that isogenous algebraic groups over a finite field $\mathbb{F}_q$ have the same number of $\mathbb{F}_q$-rational points. Part (i) follows immediately from this and from the fact that a commutative unipotent group over a perfect field is isogenous to a product of finite Witt-vector groups [Se2, p. 176].

Recall from Section 2.2 that the isogeny category of tori over $\mathbb{F}_q$ is antiequivalent to the category of representations of $\mathfrak{g}_{\mathbb{F}_q}$ on finite-dimensional $\mathbb{Q}$-vector spaces. Since $\mathfrak{g}_{\mathbb{F}_q} = \widehat{\mathbb{Z}}$ is procyclic, the isogeny class of a torus $T_{/\mathbb{F}_q}$ can be read off from the factorization of the characteristic polynomial of σ acting on $X(T) \otimes \mathbb{Q}$. Then T is isogenous to $\mathbb{G}_m^r \times \prod_{i=1}^N T_a$, where the T_a are *norm tori*. That is, for each field extension $\mathbb{F}_{q^a}$ of $\mathbb{F}_q$ there is an anisotropic torus T_a, defined as the kernel of the norm map $N\colon \operatorname{Res}_{\mathbb{F}_{q^a}/\mathbb{F}_q}(\mathbb{G}_m) \to \mathbb{G}_m$; evidently $\#T_a(\mathbb{F}_q) = \frac{q^a-1}{q-1}$. It is now easily checked that the largest number of rational points on a g-dimensional torus $T_{/\mathbb{F}_q}$ is $(q+1)^d$, attained by the d-th power of the norm torus T_2 corresponding to a quadratic extension.

Now let $B_{/\mathbb{F}_q}$ be a g-dimensional abelian variety. Then $\#B(\mathbb{F}_q)$ can be read off from the action of Fr on any ℓ-adic Tate module ($\ell \neq p$):

$$\#B(\mathbb{F}_q) = \#\operatorname{Ker}(1 - Fr) = \det(1 - Fr \mid T_\ell B) = \prod_{i=1}^{2d}(1 - \omega_i),$$

where for $1 \leq i \leq 2d$, ω_i are the characteristic roots of Frobenius. The bound that we want is a small refinement on the Weil bound following from an improvement due to Serre: namely,

$$\left|\sum_{i=1}^{2g} \omega_i\right| \leq g\lfloor 2\sqrt{q} \rfloor, \tag{5}$$

whereas Weil's bound is $\lfloor 2g\sqrt{q} \rfloor$. We may order the roots ω_i such that $\omega_{i+g} = \overline{\omega_i} = q/\omega_i$ for $i = 1, \dots, g$; writing $\rho_i = \omega_i + \overline{\omega_i}$, we have

$$P(X) = \prod_{i=1}^{g}(X^2 - \rho_i X + q).$$

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

Note that $\rho_i \le 2\sqrt{q}$, so that $q+1-\rho_i$ is a positive real number. Thus

$$\begin{aligned}\#B(k) &= \prod_{i=1}^{g}(q+1-\rho_i) \le \Big(\frac{1}{g}\sum_{i=1}^{g}(q+1-\rho_i)\Big)^g\\ &= \Big(q+1-\frac{1}{g}\sum_{i=1}^{g}\rho_i\Big)^g \le (q+1+\lfloor 2\sqrt{q}\rfloor)^g,\end{aligned}$$

where the latter inequality is Serre's bound (5), and the former inequality is obtained by replacing a geometric mean by the corresponding arithmetic mean.

As for the sharpness of the bound, it is enough to know that there exists an elliptic curve $E_{/\mathbb{F}_q}$ with $\#E(\mathbb{F}_q) = q+1+\lfloor 2\sqrt{q}\rfloor$, and this is a case of the Deuring–Waterhouse theorem [Wa, Theorem 4.1]. ■

3.3 Bounds for the Component Group of an Abelian Variety with Potentially Good Reduction

In this section all our bounds will be on the geometric component group, so for brevity, we write $\Phi = \Phi(\overline{k})$, and $\Phi' = \Phi(\overline{k})/(\Phi(\overline{k})[p^\infty])$.

The bounds on Φ and Φ' are given in terms of two auxiliary functions which measure the size of a finite abelian group in slightly different ways. For H any finite abelian group, we define (following [LO]) the *Lenstra–Oort delta function*

$$\delta_{\mathrm{LO}}(H) = \sum_{\ell \text{ prime}} (\ell-1)\operatorname{ord}_\ell(\#H)$$

and (following [Lo1, Lo2, Ed]) the *Lorenzini delta function*

$$\delta_{\mathrm{LE}}(\oplus_{i=1}^{d}\mathbb{Z}/\ell_i^{a_i}\mathbb{Z}) = \sum_{i=1}^{d}(\ell_i^{a_i}-1).$$

The following properties characterize δ_{LO}, δ_{LE} and the connection between them.

(δ0) For any prime number ℓ, $\delta_{\mathrm{LO}}(\mathbb{Z}/\ell\mathbb{Z}) = \delta_{\mathrm{LE}}(\mathbb{Z}/\ell\mathbb{Z}) = \ell-1$.
(δ1) If $0 \to H' \to H \to H'' \to 0$ is exact, then $\delta_{\mathrm{LO}}(H) = \delta_{\mathrm{LO}}(H_1) + \delta_{\mathrm{LO}}(H_2)$.
(δ2) $\delta_{\mathrm{LO}}(H) = \min_{\{H' \mid \#H' = \#H\}} \delta_{\mathrm{LE}}(H')$; in particular $\delta_{\mathrm{LO}}(H) \le \delta_{\mathrm{LE}}(H)$.

Moreover, one easily verifies that the following properties hold for *either* δ function:

(δ3) If $H \subset G$, $\delta(H) \le \delta(G)$.
(δ4) $\delta(H_1 \oplus H_2) = \delta(H_1) + \delta(H_2)$.
(δ5) If $\delta(H) \le N$, $\#H \le 2^N$.

Theorem 3.4 **(Edixhoven, [Ed, Corollary 3.4])** *Let K be a complete field with residue characteristic $p \ge 0$. Suppose that $A_{/K}$ is an atoric abelian variety. Then $\delta_{\mathrm{LE}}(\Phi') \le 2u$, where $u(A) \le \dim(A)$ is the unipotent rank.*

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

It follows that $\delta_{\mathrm{LO}}(\Phi') \leq 2u$. On the other hand, it is rather easier to prove this latter bound directly than to prove Edixhoven's theorem. Indeed, the δ_{LO} bound was shown by Lenstra–Oort in the purely unipotent case and extended by Lorenzini to the general atoric case (see [Lo2, Theorem 2.15]). Because of (δ2), the Lenstra–Oort bound gives the same information about the *order* of Φ' as Edixhoven's bound, but Edixhoven's bound can give more information on the *exponent* of Φ'. The following result is well known, and immediate from either bound using (δ5).

Corollary 3.5 *Let $A_{/K}$ be a g-dimensional atoric abelian variety over a local field. Then $\#\Phi' \leq 2^{2u} \leq 2^{2g}$.*

Theorem 3.6 (**[ELL]**) *Let $A_{/K}$ be an abelian variety with potentially good reduction over a local field. Let L/K^{unr} be the (unique, minimal, Galois) extension over which $A^{\mathrm{unr}}_{/K}$ acquires good reduction. Then Φ is killed by $[L{:}K^{\mathrm{unr}}]$.*

Because good reduction can be obtained by trivializing the Galois action on either the 3- or the 4-torsion subgroup, Theorem 3.6 leads to a bound on the exponent of Φ. Since any finite subgroup of the group of K-rational points on a g-dimensional abelian variety requires at most $2g$ generators, a bound on the exponent is all we need in order to bound the torsion. (In fact one does not need any information about the component groups of abelian varieties to prove a qualitative version of the Main Theorem, but the bounds would be worse.)

Theorem 3.7 (**Minkowski, [Mi]**) *Let G be a finite group. Suppose that for all sufficiently large prime numbers ℓ, there exists a monomorphism of groups $G \hookrightarrow GL_a(\mathbb{F}_l)$. Then $\#G \mid \eta(a)$. Especially, if a prime number p divides #G, then $p \leq a+1$.*

From these results we draw the following consequence, which is known to experts in an equivalent form [Lo1, Proposition 3.1].

Corollary 3.8 *Let $A_{/K}$ be an abelian variety over a complete field with residue characteristic p. Suppose A has potentially good reduction, and let u be the unipotent rank of the Néron special fiber. Then the degree of the field extension L/K^{unr} cut out by the action of the inertia group on any ℓ-adic Tate module ($\ell \neq p$) divides $\eta(2u)$.*

Proof Choose any $\ell > 2g+1$ and prime to p, so by the Serre–Tate theory recalled in Section 2.4 the field L is contained in $K^{\mathrm{unr}}(A[\ell])$. Let $G = \mathrm{Gal}(L/K^{\mathrm{unr}})$, and observe that G acts faithfully on the $\mathbb{F}_\ell$-vector space $A[\ell]/A[\ell](K^{\mathrm{unr}})$. Since $\ell \neq p$, $A[\ell](K^{\mathrm{unr}})$ is canonically isomorphic, under the reduction map, to $A[\ell](\overline{k})$. By Theorems 3.6 and 3.7, since $\ell > 2g+1$ the component group has no ℓ-torsion. Neither is there any ℓ-torsion coming from the unipotent part, so we conclude that $\dim_{\mathbb{F}_l} A[\ell](K^{\mathrm{unr}}) = 2\beta$. In other words, for all sufficiently large ℓ, the finite group G admits a faithful $\mathbb{F}_\ell$-representation of dimension $2g - 2\beta = 2u$, so $\#G \mid \eta(2u)$ by Theorem 3.7. ■

In summary, if $A_{/K}$ is a g-dimensional abelian variety with potentially good reduction over a locally compact field of residue characteristic p and unipotent rank u, then we have $\#\Phi'(\overline{k}) \leq 2^{2u}$ and $\exp \Phi(\overline{k}) \mid \eta(2u)$.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

3.4 Bounds for the Component Group of an Anisotropic Torus

Recall from Section 3.3 that if $T_{/K}$ is an anistropic torus, $\Phi(k) \cong (H^1(I, X(T))^{\mathfrak{g}_K})^\vee$. Thus the following simple cohomological result will give a bound on $\Phi(k)$.

Lemma 3.9 *Let G be a finite solvable group and M a $\mathbb{Z}[G]$-module whose underlying abelian group is torsion-free of finite rank g. Let r be the $\mathbb{Z}$-rank of the submodule M^G. Then $\delta_{\text{LO}}(H^1(G, M)) \leq g - r$.*

Proof See [BX, p. 483]. What is there called $\tilde{\delta}$ is our δ_{LO}. ■

Corollary 3.10 *If $T_{/K}$ is a g-dimensional anisotropic torus over a p-adic field, then $\#\Phi(k) \leq 2^{\alpha(T)} \leq 2^g$.*

Proof Recall that the dimension of the unipotent part of the Néron special fiber of a torus $T_{/K}$ is equal to the rank of the largest anisotropic subtorus of $T_{/K^{\text{unr}}}$ [Xa]. In other words, $\alpha(T) = g - r(T_{K^{\text{unr}}})$, so we may apply the lemma with G equal to the inertia group $I = \mathfrak{g}_{K^{\text{unr}}}$ (which is well known to be prosolvable, *e.g.*, [Se1]) and $M = X(T)$ together with the bound (δ5). ■

3.5 The Proof of Parts (i)–(iii) of the Main Theorem

We have now introduced all the techniques and bounds necessary to strongly bound the torsion subgroup of an anistropic abelian variety over a p-adic field. In fact we can now do this in several different ways.

First, it is quite elementary that $\#A(K)[\text{tors}]' \leq \lfloor (1+\sqrt{q})^2 \rfloor^g$ in the case of potentially good reduction. Namely, as recalled in Section 2.4, we can make a totally ramified base extension L/K such that A/L has good reduction, and then

$$A(K)[\text{tors}]' \subset A(L)[\text{tors}]' \subset A(\mathbb{F}_q)[\text{tors}]' \subset A(\mathbb{F}_q),$$

where $\mathbb{F}_q$ is the common residue field of K and L. The claim now follows from Proposition 11(iii).

Similarly, one get can a strong bound on $A(K)[\text{tors}]$ just by injecting it into $A(L)[\text{tors}]$; we then use Proposition 3.1 to bound the torsion in the formal group, which for A/L has order at most $p^{2g\gamma_p(e_L)}$, where by Corollary 3.8 $e_L \leq e \cdot \eta(2u) \leq e \cdot \eta(2g)$. In particular, if $p \gg e$, then we will still have no torsion in the formal group even over L. This gives part (i) of the Main Theorem. Note that this argument makes no mention of component groups or even of Néron models and as such is much more elementary than the improvements which follow.

The general, *i.e.*, anisotropic, case can be reduced to the case of potentially good reduction using the uniformization theorem (Theorem 2.3) and Corollary 3.8. Let us first fix notation: let

$$0 \to S^1 \to S \to S^2 \to 0$$

be the Chevalley decomposition for the uniformizing K-group scheme S of Theorem 2.3, so S^1 is linear torus and S^2 is an abelian variety with potentially good reduction. For $i = 1, 2$, let α_i, μ_i, β_i denote the dimensions of the unipotent, toric and abelian

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

parts of the Néron special fiber of S^i. We have $\alpha_1 + \alpha_2 = \alpha$, and $\mu_1 + \mu_2 = \mu$; note that $\beta_1 = 0$, so $\beta = \beta_2$. Taking Galois cohomology of the uniformization sequence (4), we get

$$0 \longrightarrow M^{\mathfrak{g}} \longrightarrow S(K) \longrightarrow A(K) \longrightarrow H^1(\mathfrak{g}, M).$$

Moreover, since A has anisotropic reduction, Theorem 2.3 gives $M^{\mathfrak{g}} = 0$, so by Corollary 3.10 we have $\#A(K)[\text{tors}] \leq \#S(K)[\text{tors}] \cdot \#H^1(\mathfrak{g}, M) \leq 2^{\alpha_1} \cdot \#S(K)[\text{tors}]$. Applying the three-step filtration Fil^i to $\#S(K)[\text{tors}]$, we get

$$\#S(K)[\text{tors}] \leq p^{2g\gamma_p(e)} \cdot \#S(\mathbb{F}_q) \cdot \#\Phi_{S^1}(k) \cdot \#H^1(S^2),$$

where $H^1(S^2) \hookrightarrow \Phi_{S^2}(k)$ and it has at most $2(\alpha_2 + \mu_2) = 2\dim(S^2)$ generators, begin a subquotient of S^2. We know from the uniformization theorem that the identity components of the Néron special fibers of S and A coincide, so

$$\#S(\mathbb{F}_q) = \#A(\mathbb{F}_q) \leq q^{\alpha}(q+1)^{\mu}\lfloor(1+\sqrt{q})^2\rfloor^{\beta}.$$

Applying Corollary 3.10 again, we have $\#\Phi_{S^1}(k) \leq 2^{\alpha_1}$; from Section 3.3 we have that $\Phi_{S^2}(k)$ is killed by $\eta(2\alpha_2)$. We conclude

$$\#A(K)[\text{tors}] \leq 2^{2\alpha_1} p^{f\alpha+2g\gamma_p(e)}(q+1)^{\mu}\lfloor(1+\sqrt{q})^2\rfloor^{\beta}\eta(2\alpha_2)^{2\alpha_2+\mu_2)},$$

giving the first bound of part (ii) of the Main Theorem.

Assume now that $A_{/K}$ has purely unipotent reduction. Then the reduction map induces an injection $A(K)[\text{tors}]' \hookrightarrow \Phi(k)'$ (in fact, since k is finite, it is an isomorphism, so we conclude from Theorem 3.7 that every prime $\ell \neq p$ dividing $A(K)[\text{tors}]$ satisfies $\ell \leq 2g+1$. To get a bound on $A(K)[\text{tors}]$ depending only on e and g, let L/K be a finite extension over which A acquires semiabelian reduction. By an argument using the base-change map as in Section 2.4, we conclude that under the natural map $A(K) \hookrightarrow A(L)$, $\operatorname{Fil}^1(A(K)[\text{tors}])$ maps to $\operatorname{Fil}^2(A(L)[\text{tors}])$. In other words, all torsion points reducing to the identity component in the Néron special fiber of A_K reduce to the identity of the Néron special fiber of A_L. Thus we get

$$\#A(K)[\text{tors}] \leq \#H^1(A_K)\#\operatorname{Fil}^2(A(L)[\text{tors}]) \leq \eta(2g)^{2g}p^{2g\gamma_p(e_L)} \leq \eta(2g)^{2g}p^{2g\gamma_p(e\cdot\eta(2g))},$$

which is part (iii) of the Main Theorem.

3.6 The Proof of Part (iv) of the Main Theorem

Our result will be deduced readily from the following theorem of Igusa.

Theorem 3.11 **(Local monodromy theorem)** *Let $K = \mathbb{F}_q((T))$, let $j_0 \in \mathbb{F}_q$ be a supersingular j-invariant, and let $E_{/K}$ be an elliptic curve with j-invariant $j(E) = T + j_0$, so E is ordinary with good supersingular reduction. Consider*

$$\rho\colon \operatorname{Gal}_K \longrightarrow \operatorname{Aut}(T_p(E)) \cong \mathbb{Z}_p^{\times},$$

the Galois representation on the étale part of the p-adic Tate module of E, Then the restriction of ρ to $\operatorname{Gal}_{\overline{\mathbb{F}_q}((T))}$ is surjective.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

Remark. Recall that there is always at least one supersingular j-invariant $j_0 \in \mathbb{F}_p$. In particular elliptic curves $E_{/K}$ as in Igusa's theorem always exist.

It follows that if $E_{/K}$ is such an elliptic curve, then for all n, $L_n = K(E(\overline{K}[p^n]))$ is a totally ramified extension of K. By definition of L we have that $p^n \mid \#E(L_n)$. However, since L/K is totally ramified, by the classification of locally compact fields of positive characteristic, L must be (non-canonically!) isomorphic to $\mathbb{F}_q((T))$. In other words, there exists a change of variables $T \mapsto f_n(T)$, with respect to which we can view E/L_n as an elliptic curve E_n/K with j-invariant $f_n(T) + j_0$, and such that $p^n \mid \#E(K)$. This completes the proof of part (iv) of the Main Theorem.

4 The Proof of Theorem 1.3

Let $E/\mathbb{Q}$ be a rational elliptic curve with anisotropic reduction at every prime number. In particular, applying the Main Theorem to $E/\mathbb{Q}_2$ we get that the odd-order torsion in $E(\mathbb{Q})$ is a group of order at most $\lfloor (1+\sqrt{2})^2 \rfloor = 5$, so is either trivial, or $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z}$. Applying the Main Theorem to $E/\mathbb{Q}_3$ we get that the prime-to-3 torsion injects into a group of order at most $\lfloor (1+\sqrt{3})^2 \rfloor = 7$, so is trivial, or is $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z}$. Finally, considering $E/\mathbb{Q}_5$ we get that the prime-to-5-torsion injects into a group of order at most $\lfloor (1+\sqrt{5})^2 \rfloor = 10$. Collating this information and comparing with the statement of Theorem 1.3, we see that what remains to be shown is that there cannot exist a rational 5-torsion point.

To recover Frey's Theorem we need to show the nonexistence of a 5-torsion point in the special case of integral moduli. This is easier and we present, "just for fun," the following quick proof. Namely, by a well-known result of Tate, $E/\mathbb{Q}$ does not have good reduction everywhere. Moreover, we claim that it is not possible for it to have good reduction except possibly at $p = 5$. Otherwise the conductor of E would have to divide 25, but since $X_0(25)$ has genus zero, there are (by the elliptic modularity theorem) no such elliptic curves. Thus we get a prime $p \neq 5$ of bad, so necessarily additive reduction, and part (iii) of the Main Theorem applies to show that $E(\mathbb{Q}_p)[5] = 0$.

For the general case we will show that an elliptic curve $E/\mathbb{Q}$ endowed with a rational 5-torsion point must have a prime of split multiplicative reduction by a direct computation with the modular curve $X_1(5)$. The following calculation uses the fact that $\mathbb{Q}(X_1(N)) = \mathbb{Q}(t)$, *i.e.,* that $N \leq 12$ and is not 11, as well as the fact that $X_1(N)$ is a fine moduli space, *i.e.,* that $N \geq 5$.

Indeed, these two facts imply that there is a universal (generalized) elliptic curve $E \to X_1(5)$. Following Kubert [Kub], for a suitable choice of parameter $t \in \mathbb{Q}(X_1(N))$ we get the equation $E_t : Y^2 + (1-t)XY - tY = X^3 - tX^2$. We record some of the basic invariants:

$$\Delta(t) = t^7 - 11t^6 - t^5, \qquad c_4(t) = t^4 - 12t^3 + 14t^2 + 12t + 1,$$

$$c_6(t) = -t^6 + 18t^5 - 75t^4 - 75t^2 - 18t - 1, \qquad \gamma(t) = -\frac{c_4(t)}{c_6(t)}.$$

From the equation for Δ, we see that the fiber over $t = 0$ corresponds to the cuspidal points, *i.e.,* the semistable singular curves needed to compactify the moduli space.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

The fibers over $t = \pm 1$ are isomorphic to $E = X_0(11)$, which has split multiplicative reduction at 11. For any other value of $t \in \mathbb{Q}$ there exists some prime number p dividing either the numerator or the denominator of t.

Assume first that p divides the numerator of t. Then the displayed Weierstrass equation has $\mathbb{Z}_p$-integral coefficients and has $v_p(c_4(t)) = 0 < 4$, so that the equation is minimal [Si1, Remark VII.1.1]. Since $v_p(\Delta(t)) > 0$ and $v_p(c_4(t)) = 0$, the reduction is multiplicative [Si1, Proposition VII.5.1]. Moreover, we claim that $\gamma(t)$ is a square in $\mathbb{Q}_p^\times$. Indeed, since $\gamma(t)$ lies in the group $U_1 \subset \mathbb{Z}_p^\times$ of units congruent to 1 modulo p, this is clear for odd p. For the case $p = 2$, it suffices to calculate that

$$\gamma(2t) \equiv 1 - 4t + 4t^2 \pmod{8\mathbb{Z}_2[[t]]}$$

and observe that this latter polynomial is congruent to 1 mod 8 for all integers t. Thus by the theory of Tate curves [Si2, § V.2], E_t has split multiplicative reduction at p.

If $v_p(t) = n < 0$, then rescaling the Weierstrass equation by

$$(x, y) = (p^{-2n}x', p^{-3n}y'),$$

we get back to the first case.

That all these groups occur already among elliptic curves $E/\mathbb{Q}$ with j-invariant 0 or 1728 is a very classical fact, which can readily be reestablished by looking at the Weierstrass equations $y^2 = x^3 + Dx$ ($j = 0$) and $y^2 = x^3 + D$ ($j = 1728$). This completes the proof of Theorem 1.3.

Remark. We were hoping for the opposite result, *i.e.,* for an anisotropic elliptic curve $E/\mathbb{Q}$ with a rational 5-torsion point. This would have implied that the bound $A(\mathbb{Q})[\text{odd}] \leq 5^g$ coming from Corollary 1.2 was sharp.

5 The Proof of Theorem 1.4

5.1 Bounds Obtained from the Main Theorem

Let $A/\mathbb{Q}$ be an abelian surface with everywhere anisotropic reduction. As usual, applying part (i) of the Main Theorem prime by prime leads to a short list of possible orders of torsion groups. Indeed, in this case, the odd order torsion injects into a group of order at most $\#A(\mathbb{F}_2) \leq \lfloor (1 + \sqrt{2})^2 \rfloor^2 = 25$ and the prime-to-3 torsion injects into a group of order at most $\#A(\mathbb{F}_3) \leq \lfloor (1 + \sqrt{3})^2 \rfloor^2 = 49$. This implies that the the possible orders of torsion groups are of the form $2^a \cdot y$, where $0 \leq a \leq 5$ and y lies in the set

(6) $$1, 3, 5, 7, 3^2, 11, 13, 3 \cdot 5, 17, 19, 3 \cdot 7, 23, 5^2.$$

5.2 Some Tate-Honda Theory

Suppose one wishes to enumerate all the possible values of $\#A(\mathbb{F}_q)$, where $A_{/\mathbb{F}_q}$ is a d-dimensional abelian variety. Recall that for two abelian varieties A_1, A_2 over $\mathbb{F}_q$, the

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

following are equivalent: (i) that they are isogenous, (ii) that their Frobenius characteristic polynomials coincide, (iii) that they have the same number of rational points over every finite field extension. Thus, to perform the enumeration, it is enough to know the set of all Frobenius polynomials $P(T)$ of d-dimensional $A_{/\mathbb{F}_q}$: just evaluate at $T = 1$.

This problem, namely, which polynomials arise as Frobenius polynomials, is addressed by the theory of Tate and Honda. The definitive introduction to this theory is still to be found in Waterhouse's thesis [Wa]. Here we will just give an "explicit formula" for $\#A(\mathbb{F}_p)$ where A is an abelian surface.

Proposition 5.1 *There are three types of abelian surface $A/\mathbb{F}_p$, whose Frobenius polynomials are as follows:*

(i) *Type I: $P_A(T) = (T^2 - a_1T + p)(T^2 - a_2T + p)$, where a_1, a_2 are integers such that $|a_1|,\ |a_2| < 2\sqrt{p}$; $\#A(\mathbb{F}_p) = (p + 1 - a_1)(p + 1 - a_2)$.*

(ii) *Type II: $P_A(T) = (T^2 - p)^2$; $\#A(\mathbb{F}_p) = (p - 1)^2$.*

(iii) *Type III: $P_A(T) = T^4 - 2aT^3 + (a^2 + 2p - 2db^2)T^2 - 2apT + p^2$, where $d > 1$ is a squarefree integer, $a, b \in \frac{1}{2}\mathbb{Z}$ are such that $a + b\sqrt{d}$ is in the ring of integers of $\mathbb{Q}(\sqrt{d})$, $b \neq 0$ and $|a| + |b|\sqrt{d} < 2\sqrt{p}$; $\#A(\mathbb{F}_p) = (p + 1)^2 + (a - 1)^2 - 2ap - db^2 - 1$.*

Sketch of the Proof The Frobenius polynomial $P_A(t)$ of any abelian surface $A_{/\mathbb{F}_q}$ is a quartic Weil q-polynomial, *i.e.,* a polynomial with integral coefficients whose roots have norm $\sqrt{q}$ under every Archimedean valuation. Moreover, either $A \sim_{\mathbb{F}_q} E_1 \times E_2$ or A is $\mathbb{F}_q$-simple. The former case is precisely Type I, so it suffices to consider the $\mathbb{F}_q$-simple surfaces. Henceforth we will abbreviate $\mathbb{F}_q$-simple to "simple" (although we warn the reader that it is more standard to use "simple" to mean "geometrically simple").

If $A_{/\mathbb{F}_q}$ is a simple abelian surface, $P_A(t)$ is either irreducible or is of the form $Q(T)^2$ for $Q(T)$ an irreducible quadratic. Over a general finite field $\mathbb{F}_q$, it is somewhat intricate to describe which Weil polynomials of the second type correspond to abelian surfaces, but over $\mathbb{F}_p$, this can only happen if the field $\mathbb{Q}(\pi)$ generated by a Frobenius root π is real, *i.e.,* $\pi = (\pm)\sqrt{p}$. This is Type II. Otherwise $\mathbb{Q}(\pi)$ is a quartic CM field which is best understood in terms of the real quadratic subfield $\mathbb{Q}(\beta)$, where $\beta = \pi + \frac{p}{\pi}$. Indeed, the condition on β that it be "the β" of some quartic Weil p-number π is just that it be an irrational real quadratic integer $\beta = a + b\sqrt{d}$ which has norm strictly less than $2\sqrt{p}$ in both Archimedean valuations, *i.e.,* $|a| + |b|\sqrt{d} < 2\sqrt{p}$. The corresponding π is then a solution of $T^2 - \beta T + p = 0$. This is Type III.

5.3 Compiling the Bounds

Using Proposition 5.1, we record $\#A(\mathbb{F}_p)$ for $p = 2, 3, 5$.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

Fact 5.2 *Let $A/\mathbb{F}_p$ be an abelian surface over the finite field $\mathbb{F}_p$, $p \leq 5$. Then*

$$\#A(\mathbb{F}_2) \in [1,16] \cup [19,20] \cup [25],$$
$$\#A(\mathbb{F}_3) \in [1,16] \cup [18,25] \cup [28,30] \cup [34,36] \cup [42] \cup [49],$$
$$\#A(\mathbb{F}_5) \in [4] \cup [6,50] \cup [52,56] \cup [58,64] \cup [69,72] \cup [79,81] \cup [90] \cup [100].$$

Note the sparsity for $p = 2$ and $p = 3$. By the time we get to $p = 5$ there is such an enormous interval of assumed values that nothing further is ruled out.[2]

Working prime by prime, we now use Fact 5.2 to eliminate many of the values from the list $2^a \cdot y$, $1 \leq a \leq 5$, y in the list (6) *e.g.*, we can in fact take $a \leq 4$, and in doing so we arrive at the list (3) of Theorem 1.4.

5.4 Some Attained Values of N

Let us discuss which values of the list (3) we know do arise.

If $E_{1/\mathbb{Q}}$, $E_{2/\mathbb{Q}}$ are two everywhere AR elliptic curves, then $A := E_1 \times E_{2/\mathbb{Q}}$ is an everywhere AR abelian surface, and $A(\mathbb{Q})[\mathrm{tors}] = E_1(\mathbb{Q})[\mathrm{tors}] \times E_2(\mathbb{Q})[\mathrm{tors}]$. Thus, using Theorem 1.3, the orders of $A(\mathbb{Q})[\mathrm{tors}]$ arising in this way are:

$$1\text{–}4,\ 6,\ 8,\ 9,\ 12,\ 18,\ 24,\ 36.$$

If $E_{/K}$ is an IM elliptic curve over a quadratic field, then $A := \mathrm{Res}_{K/\mathbb{Q}}(E)$, the Weil restriction of E from K to $\mathbb{Q}$, is an IM abelian surface with $A(\mathbb{Q})[\mathrm{tors}] = E(K)[\mathrm{tors}]$. To fully implement this observation, we use the complete classification of torsion subgroups on IM elliptic curves over quadratic fields, due to [MSZ]; one can get all orders less than or equal to 12 except 11. Thus to the previous list we can add the orders $5, 7, 10$.

The next two results were discovered by A. Ogg more than 30 years ago. Nowadays, it is straightforward to confirm them using standard software packages.

The abelian surface $J_1(13)/\mathbb{Q}$, *i.e.*, the Jacobian of the modular curve $X_1(13)$, has integral moduli and $J_1(13)(\mathbb{Q})[\mathrm{tors}] \cong \mathbb{Z}/19\mathbb{Z}$ [MT, Theorem, §4]. Thus 19 arises.

The abelian surface $J_1(16)/\mathbb{Q}$ has integral moduli and $J_1(16)(\mathbb{Q})[\mathrm{tors}] \cong \mathbb{Z}/2 \times \mathbb{Z}/10$. Thus 20 arises.

Remark. It is not hard to see that if $E_{/K}$ is an everywhere AR elliptic curve defined over a quadratic number field, then $\mathrm{Res}_{K/\mathbb{Q}}\, E$ is an everywhere AR abelian surface. There are several values N of $\#E(K)[\mathrm{tors}]$ which are permitted by our bounds to arise for everywhere AR elliptic curves but are known by the work of [MSZ] not to arise for IM elliptic curves, namely, $14, 16, 18, 24$ and 36. Thus it is conceivable that one could get an everywhere AR abelian surface $A_{/\mathbb{Q}}$ with 14 torsion points in this way. Since $X_1(14)$ is a fine moduli space of genus one, the search for an elliptic curve defined over a quadratic field $E_{/K}$ with the desired properties amounts to a study of all quadratic points on a fixed rational elliptic curve, a rather daunting prospect.

[2] In [DH], one finds evidence that the smaller size of the *central interval* $I_{d,q}$, (*i.e.*, the largest symmetric interval I centered at $q^d + 1$ such that if $N \in I$, then there exists $A_{/\mathbb{F}_q}$ of dimension d with $\#A(\mathbb{F}_q) = N$) for $q = 2$ and 3 than for other prime powers is a general phenomenon.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

6 A Higher-Dimensional Szpiro Conjecture

As we have already mentioned, Flexor and Oesterlé (following Frey) used their work on torsion points defined over local fields to show that the size of the torsion subgroups of elliptic curves over a fixed number field K is uniformly bounded, assuming that the Szpiro conjecture is true. It may be of some interest to note that this implication has a kind of higher-dimensional analogue: we can show that the uniform boundedness of torsion points on g-dimensional Hilbert–Blumenthal abelian varieties $A_{/K}$ follows from a certain higher-dimensional Szpiro conjecture.

For $A/\mathbb{Q}$ an abelian variety, denote by $\mathfrak{f}_{A_{/K}}$ its conductor, an ideal of K. We also define its *pseudo-discriminant* $\mathcal{D}_{A_{/K}}$ to be the ideal $\prod_{v|\mathfrak{f}} v^{\exp(\Phi_v)}$, where Φ_v denotes the component group of the fiber at v of the Néron model. It follows from Ogg's formula [Si2, IV.11.1] that $\mathcal{D}$ is the discriminant in the usual sense if $E_{/K}$ is a semistable elliptic curve. If $E_{/K}$ is any elliptic curve, then $\mathcal{D}$ can be viewed as the discriminant defined by a simplified version of Ogg's formula in which we have taken only the highest order term. Consider now the following.

Conjecture 6.1 *Let K be a number field and g be a positive integer. There exists a constant $\beta = \beta(K, g)$ such that if $A_{/K}$ is any g-dimensional abelian variety,*

$$\log(N_{K/\mathbb{Q}}(\mathcal{D})) \leq \beta \log(N_{K/\mathbb{Q}}(\mathfrak{f})).$$

Using the boundedness of the conductor exponents and of component groups of anisotropic elliptic curves $E_{/K}$, it is easy to see that when $g = 1$ this is equivalent to a weak form of the Szpiro conjecture [FO, Conjecture 2].

Now suppose that $A_{/K}$ is a Hilbert–Blumenthal abelian variety, *i.e.,* there exists a totally real number field M of degree g over $\mathbb{Q}$ together with an embedding $M \hookrightarrow \mathrm{End}_K(A) \otimes \mathbb{Q}$. This condition imposes restrictions on the structure of the Néron fiber A_{k_v} at v (for any finite place v). Indeed, as in the proof of Theorem 1.1, since the representation of M on the rational character group $X(A_{k_v}) \otimes \mathbb{Q} \cong \mathbb{Q}^\mu$ is a unital homomorphism of rings, we have either $\mu = 0$ or $\mu = g$. In other words, the reduction is either atoric or purely toric. In the former case a similar argument, using the fact that the degree g totally real field M does not act as an algebra of endomorphisms on any abelian variety of dimension less than g, shows that the reduction is either purely unipotent or good. Because part (iii) of the Main Theorem bounds the torsion subgroup in the purely unipotent case (independently of the residue characteristic), we may assume that $A_{/K}$ is semistable with purely toric reduction at every prime dividing $\mathfrak{f}$. The interested reader may now check that using Conjecture 6.1 in place of the Szpiro conjecture, the argument of [FO] goes through *mutatis mutandis*: especially, we have taken the exponent instead of the order of the component group in our definition of $\mathcal{D}$ so that [FO, Proposition 4] remains valid (for the proof, one replaces the Tate curve $\mathbb{G}_m/\langle q\rangle$ with the v-adically uniformized abelian variety $\mathbb{G}_m^g/\Lambda$).

Remark. While there are very good reasons to believe in the Szpiro conjecture (for instance, its truth in the function field case), we are not at all sure what to make of our Conjecture 6.1, which is motivated only by a crude sort of generalization of Ogg's formula. It seems fair to say that even people who believe in the Szpiro conjecture do

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

not expect an easy proof: it implies, among other wondrous things, the ABC conjecture. Obviously Conjecture 6.1 is even harder to prove (and, what is worse, almost as hard to disprove). Nevertheless it seems to give us some small reason to believe in the uniform boundedness of torsion points on all Hilbert–Blumenthal abelian varieties, which is perhaps more than could be said before.

Acknowledgements Some of this material (especially Theorem 1.1) appeared in Chapter 5 of the first author's thesis [Cl] on Shimura curves. The first author gratefully acknowledges the support of Harvard University and the guidance of his thesis advisor, Barry Mazur. He also thanks the second author for graciously agreeing to jointly write the present paper, which includes significantly stronger local results than those appearing in [Cl]. The second author thanks Bas Edixhoven and Dino Lorenzini for several conversations on this subject during these last years. He also thanks the first author for convincing him to jointly write the present paper.

References

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

[BX] S. Bosch and X. Xarles, *Component groups of Néron models via rigid uniformization.* Math. Ann. **306**(1996), no. 3, 459–486.

[Bu] K. Buzzard, *Integral models of certain Shimura curves.* Duke Math. J. **87**(1997), no. 3, 591–612.

[Cl] P. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves.* Thesis, Harvard University, 2003.

[DH] S. DiPippo and E. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields.* J. Number Theory **73**(1998), no. 2, 426–450.

[Ed] S. Edixhoven, *On the prime-to-p part of the groups of connected components of Néron models.* Compositio Math. **97**(1995), no. 1-2, 29–49.

[ELL] S. Edixhoven, Q. Liu, and D. Lorenzini, *The p-part of the group of components of a Néron model.* J. Algebraic Geom. **5**(1996), no. 4, 801–813.

[FO] M. Flexor and J. Oesterlé, *Sur les points de torsion des courbes elliptiques.* In: Séminaire sur les Pinceaux de Courbes Elliptiques, Astérisque 1990 no. 193, pp. 25–36.

[Fr] G. Frey, *Some remarks concerning points of finite order on elliptic curves over global fields.* Ark. Mat. *15*(1977), no. 1, 1–19.

[HS] M. Hindry and J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique.* C. R. Acad. Sci. Paris Sér. I Math. **329**(1999), no. 2, 97–100.

[Kub] D. Kubert, *Universal bounds on the torsion of elliptic curves.* Proc. London Math. Soc. **33**(1976), no. 2, 193–237.

[LO] H. W. Lenstra, Jr. and F. Oort, *Abelian varieties having purely additive reduction.* J. Pure Appl. Algebra **36**(1985), no. 3, 281–298.

[Lo1] D. Lorenzini, *Jacobians with potentially good ℓ-reduction.* J. Reine Angew. Math. **430**(1992), 151–177.

[Lo2] ———, *On the group of components of a Néron model.* J. Reine Angew. Math. **445**(1993), 109–160.

[MT] B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves.* Invent. Math. **22**(1973/74), 41–49.

[Me] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. **124**(1996), no. 1-3, 437–449.

[Mi] H. Minkowski, *Zur Theorie der positiven quadratische Formen.* J. Reine Angew. Math. **101**(1887), 196–202.

[MSZ] H. Müller, H. Ströher, and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic felds.* J. Reine Angew. Math. **397**(1989), 100–161.

[Ol] L. Olson, *Points of finite order on elliptic curves with complex multiplication.* Manuscripta Math. **14**(1974), 195–205.

[PY] D. Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves.* C. R. Math. Acad. Sci. Soc. R. Can. **23**(2001), no. 1, 1–5.

[Se1] J.-P. Serre. *Corps locaux*, Hermann, Paris, 1962.

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press

[Se2] ———, *Algebraic Groups and Class Fields.* Graduate Texts in Mathematics 117, Springer-Verlag, New York, 1988.

[Se3] ———, *Lie Algebras and Lie Groups.* Lecture Notes in Mathematics 1500, Springer-Verlag, Berlin, 1992.

[ST] J.-P. Serre and J. Tate, *Good reduction of abelian varieties.* Ann. of Math. **88**(1968), 492–517.

[Sg1] A. Silverberg, *Torsion points on abelian varieties of CM-type.* Compositio Math. **68**(1988), no. 3, 241–249.

[Sg2] ———, *Points of finite order on abelian varieties*. Contemp. Math. **133**(1992), 175–193.

[Sg3] ———, *Open questions in arithmetic algebraic geometry.* In: Arithmetic Algebraic Geometry. IAS/Park City Math. Ser. 9, American Mathematical Society, Providence, RI, 2001, pp. 83–142.

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[Si2] ———, *Advanced Topics in The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.

[VanM] P. Van Mulbregt, *Torsion-points on low-dimensional abelian varieties with complex multiplication*. Contemp. Math. **133**(1992), 205–210,

[Wa] W. C. Waterhouse, *Abelian varieties over finite fields.* Ann. Sci. École Norm. Sup. **2**(1969), 521–560.

[Xa] X. Xarles, *The scheme of connected components of the Néron model of an algebraic torus.* J. Reine Angew. Math. **437**(1993), 167–179.

Department of Mathematics, University of Georgia, Athens, GA 30602, U.S.A.
e-mail: pete@math.uga.edu

Departament de Matemátiques, Universitsat Autónoma de Barcelona, Catahunya, Spain
e-mail: xarles@mat.uab.es

https://doi.org/10.4153/CJM-2008-026-x Published online by Cambridge University Press