POTENTIAL SHA FOR ABELIAN VARIETIES

BRENDAN CREUTZ

Abstract. We show that the p-torsion in the Tate-Shafarevich group of any principally polarized abelian variety over a number field is unbounded as one ranges over extensions of degree $\mathcal{O}(p)$, the implied constant depending only on the dimension of the abelian variety.

1. Introduction

Let A/k be an abelian variety over a number field k. We denote the completion of k at a prime v by k_v. The Galois cohomology group $\mathrm{H}^1(k, A)$ is known as the Weil-Châtelet group. The elements in this group can be interpreted as isomorphism classes of k-torsors under A. Such a torsor is trivial if and only if it contains a k-rational point. Since any torsor under the connected group A is locally solvable at all but finitely many primes, the image of the restriction map

$$\mathrm{res} : \mathrm{H}^1(k, A) \to \prod_v \mathrm{H}^1(k_v, A)$$

is contained in the direct sum. The Tate-Shafarevich group of A/k, denoted $Ш(A/k)$, is defined as the kernel of this restriction map. As such, a torsor represents an element of the Tate-Shafarevich group if and only if it is everywhere locally solvable. Thus, nontrivial elements in this group are counterexamples to the Hasse principle.

Conjecturally the Tate-Shafarevich group is finite. Nevertheless there are a number of results in the literature which show that this group can be arbitrarily large. The first results in this direction were due to Cassels [2] who showed that one can arrange for the 3-torsion subgroup of $Ш(E/\mathbb{Q})$ to be as large as one likes by choosing a suitable CM elliptic curve E defined over $\mathbb{Q}$. Similar results have been obtained for all $p \leq 7$ and $p = 13$ (see [1, 8, 9, 12, 14]). These results exploit the existence of elliptic curves admitting p-isogenies and, for $p = 5, 7, 13$, make use of the fact that the modular curve $X_0(p)$ parametrizing such curves has genus 0 and infinitely many $\mathbb{Q}$-points. Kloosterman and Schaefer [10, 11] have employed similar techniques when the modular curve $X_0(p)$ is of higher genus to show that the order of the p-torsion in $Ш(E/k)$ is unbounded as E/k ranges over elliptic curves defined over number fields of degree bounded by some polynomial in p.

These latter results require that both the elliptic curve and the base field be allowed to vary. Matsuno showed [15] that if k is a cyclic extension of $\mathbb{Q}$ of degree p, then the p-rank of the Tate-Shafarevich group over k of elliptic curves defined over $\mathbb{Q}$ can be arbitrarily large. In a different direction, results of Clark and Sharif explore the p-torsion in $Ш(A/\ell)$ for a fixed abelian variety A over a number field k as the extension ℓ/k is allowed to vary. Their results actually concern the subgroup

$$Ш_k(A/\ell) := \mathrm{res}_{\ell/k}(\mathrm{H}^1(k, A)) \cap Ш(A/\ell)\,,$$

which we call the *potential* Ш *of* A/k *in* ℓ.

In [3] Clark showed that the potential p-torsion in Ш of an elliptic curve E/k with full level p structure is unbounded as ℓ ranges over extensions of degree p. In [6] Clark and Sharif removed the assumption of full level p structure, thus showing that the potential p-torsion of Ш of any elliptic curve is unbounded as ℓ ranges over extensions of degree p. Clark has generalized the original result (i.e. under the assumption of full level p structure) to all strongly principally polarized abelian varieties for which the absolute Galois group G_k of k acts trivially on the Néron-Severi group [5, Theorem 9] (recall that a polarization is *strong* if it is given by a k-rational divisor). The main result of this paper is to remove the assumption of full level p structure in the higher-dimensional case as well.

Theorem 1.1. *Let A/k be a strongly principally polarized abelian variety over a number field k such that the G_k-action on the Néron-Severi group is trivial. For any prime p and any integer N, there exists a degree p extension ℓ of k for which*

$$\#Ш(A/\ell)[p] \geq \#Ш_k(A/\ell)[p] > N\,.$$

As Clark has noted (see [5, Corollary 10]), any principally polarized abelian variety of dimension g can be made to satisfy the conditions of theorem 1.1 by passing to an extension of degree at most $2^g \cdot \#\,\mathrm{GL}_{4g^2}(\mathbb{F}_3)$. As

this does not depend on p, we see that the p-torsion in the Tate-Shafarevich group of any principally polarized abelian variety A/k becomes arbitrarily large as ℓ ranges over extensions of degree $\mathcal{O}(p)$, the implied constant depending only on the dimension of the abelian variety.

Our approach to theorem 1.1 is based on the method utilized in [3, 5, 6] which relates potential Ш to the period-index problem for torsors under abelian varieties. Recall that the *period* of a torsor under A/k is its order in the Weil-Châtelet group while its *index* is the greatest common divisor of the degrees of extensions over which the torsor contains a rational point. Using weak approximation together with a result of Lang and Tate regarding period and index over local fields (theorem 2.12) one can often arrange that a torsor of degree n become everywhere locally solvable after a sufficiently ramified extension ℓ/k of degree n. If the index of such a torsor exceeds n, then it will represent a nontrivial element of $Ш(A/\ell)[n]$. Of course the difficulty lies in constructing sufficiently many such torsors and ensuring that they remain pairwise nonisomorphic over ℓ. We give a new construction of such period-index discrepancies which simultaneously generalizes [5, Theorem 8] and [6, Theorem 2].

Theorem 1.2. *Let $n \geq 2$ and A/k a strongly principally polarized abelian variety over a number field k such that the G_k-action on the Néron-Severi group is trivial. Then there exist infinitely many elements of $\mathrm{H}^1(k, A)$ of period n which cannot be split by any extension of degree n. If n is a prime power, then these torsors have index strictly larger than n.*

For the statement of the next two results, let A/k be a principally polarized abelian variety over a number field k, and let p be a prime number. Let S denote the set of primes of k that are either of bad reduction for A or lie above p, and let $T = \{v \notin S : A(k_v)[p] \neq 0\}$. Matsuno showed [15, Corollary 4.5] that for an elliptic curve $E/\mathbb{Q}$ and a cyclic extension $\ell/\mathbb{Q}$ of degree p,

$$\#Ш(E/\ell)[p] \cdot \# \left(\frac{E(\ell)}{pE(\ell)} \right) \geq p^{t-4} ,$$

where t denotes the number of primes in T which are totally ramified in ℓ. Our approach yields similar results on the potential p-torsion in terms of the ramification of the extension.

Theorem 1.3. *Assume A is strongly principally polarized and that the G_k-action on the Néron-Severi group is trivial. Let $\{\ell_i\}$ be any sequence of degree p extensions of k such that for every prime v in T, there exists an integer n such that for every $i \geq n$, v is totally ramified in ℓ_i. Then $\lim_{i\to\infty} \#Ш_k(A/\ell_i)[p] = \infty$*

Theorem 1.4. *Let ℓ/k be any extension of degree p. Let t be the number of primes in T which are totally ramified in ℓ. Then*

$$\#Ш_k(A/\ell)[p^\infty] \leq \#Ш(A/k)[p^\infty] \cdot p^{g[k:\mathbb{Q}]+2g(t+\#S)} .$$

Remark: The reader will note that theorem 1.4 makes no assumptions on either the principal polarization or the G_k-module structure of the Néron-Severi group. The proofs of theorems 1.1–1.3 rely on a theorem of Clark (2.5 below) whose proof does require such assumptions.

The existence of an upper bound as in theorem 1.4 was alluded to by Clark and Sharif in [6, Section 3.8]. They also ask if the size of $Ш(E/\ell)[p]$ necessarily approaches infinity with the number of primes ramifying in ℓ. Theorems 1.3 and 1.4 show that for the potential Ш it is only the ramification in T that plays any role. In a sense this is quite natural. One can show that every torsor V/k of p-powered period is locally solvable at all primes outside $S \cup T$.

2. The obstruction map for abelian varieties

Here we collect various results related to the *obstruction map* utilized by Clark to study the period-index problem for abelian varieties in [5]. We are indebted to him for having laid a comfortable foundation for forays in this direction. His results generalize those of O'Neil who developed the obstruction map for elliptic curves [20]. The only possibly new material here is contained in propositions 2.4 and 2.9. The first relates the obstruction map to the Tate pairing. The second uses this to compute the image of the obstruction map over p-adic fields. These results were to be expected, if not already well known.

Let (A, L) be a polarized abelian variety over a field K. Recall that the polarization is given by a line bundle $L \in \mathrm{Pic}(\bar{A})$ that is ample, base point free and algebraically equivalent to each of its Galois conjugates. The last condition means that L gives rise to a G_K-invariant class in the Néron-Severi group. One says that the polarization is *strong* if $L \in \mathrm{Pic}(A)$ (i.e. if L can be represented by a K-rational divisor on A). One says that L is *symmetric* if $L \simeq [-1]^* L$. Corresponding to L is an isogeny $\varphi_L : A \to A^\vee$, given by $\varphi_L(x) = \tau_x^* L \otimes L^{-1}$,

where τ_x denotes translation by x on A. We denote the kernel of φ_L by $A[\varphi_L]$ and let n be the exponent of $A[\varphi_L]$. We assume that n is not divisible by the characteristic of K.

2.1. **The result of Zarkhin.** Let $\mathcal{G}_L$ denote the theta group associated to L (e.g. [18], [5, Section 5.1], [25, Chapter 8]). This is a central extension of $A[\varphi_L]$,

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{G}_L \longrightarrow A[\varphi_L] \longrightarrow 0\,, \tag{1}$$

which gives rise to a nondegenerate symplectic form

$$e^L : A[\varphi_L] \times A[\varphi_L] \longrightarrow \mathbb{G}_m\,. \tag{2}$$

For $Q, R \in A[\varphi_L]$ the pairing is given by taking the commutator of any choice of lifts of Q and R to $\mathcal{G}_L$. Since the possible lifts differ only by central elements the pairing is well-defined. Since $A[\varphi_L]$ is commutative, the pairing takes values in the center of $\mathcal{G}_L$. The fact that $\mathbb{G}_m$ is the center of $\mathcal{G}_L$ implies that the pairing is nondegenerate.

The pairing may be composed with the cup product to obtain a pairing

$$\cup_{e^L} : \mathrm{H}^1(K, A[\varphi_L]) \times \mathrm{H}^1(K, A[\varphi_L]) \xrightarrow{\cup} \mathrm{H}^2(K, A[\varphi_L] \otimes A[\varphi_L]) \xrightarrow{e^L} \mathrm{H}^2(K, \mathbb{G}_m)\,.$$

On the other hand, the central extension (1) leads to an exact sequence (of pointed sets) coming from nonabelian Galois cohomology. The following relation between the connecting map

$$\Delta_L : \mathrm{H}^1(K, A[\varphi_L]) \to \mathrm{H}^2(K, \mathbb{G}_m) = \mathrm{Br}(K) \tag{3}$$

and the cup product pairing was established by Zarkhin in [26].

Theorem 2.1 (Zarkhin)**.** *For any $\xi, \eta \in \mathrm{H}^1(K, A[\varphi_L])$ one has*

$$\xi \cup_{e^L} \eta = \Delta_L(\xi + \eta) - \Delta_L(\xi) - \Delta_L(\eta)\,.$$

If L is symmetric, then in addition $\Delta_L(a\xi) = a^2\Delta_L(\xi)$ for any integer a. In particular, Δ_L is quadratic and is a quadratic form if L is symmetric.

We record here the following elementary lemma for later use.

Lemma 2.2. *Let m be an odd number, V a $\mathbb{Z}/m\mathbb{Z}$-module and $Q : V \to \mathbb{Z}/m\mathbb{Z}$ a quadratic form whose associated bilinear form B is symmetric and non-degenerate. Suppose there exists an isotropic element $u \in V$ of order m (i.e. such that $u \neq 0$ and $2Q(u) = B(u,u) = 0$). Then $Q(V) = \mathbb{Z}/m\mathbb{Z}$.*

Proof: Let $a \in \mathbb{Z}/m\mathbb{Z}$. We will show that $a \in Q(V)$. Let u be isotropic and of order m. The map $B(u, \cdot) : V \to \mathbb{Z}/m\mathbb{Z}$ is surjective (since u has order m and B is nondegenerate). Thus we can find w such that $B(u,w) = 1/2 \in \mathbb{Z}/m\mathbb{Z}$. Set $b = a - B(w,w)$. Consider $v = bu + w$. We have

$$\begin{aligned} 2Q(v) &= B(bu + w, bu + w) \\ &= 2\left(2bB(u,w) + B(w,w) + b^2B(u,u)\right) \\ &= 2\left(a - B(w,w) + B(w,w)\right) = 2a\,. \end{aligned}$$

Since 2 is invertible we have $Q(v) = a$. □

2.2. **The Weil pairing.** Let $\lambda : A \to B$ be an isogeny of abelian varieties. One has the dual isogeny $\lambda^\vee : B^\vee \to A^\vee$ and standard duality theorems (e.g. [25, Theorem 7.5]) give an isomorphism of group schemes $\beta : B^\vee[\lambda^\vee] \simeq \mathrm{Hom}(A[\lambda], \mathbb{G}_m)$. The rule $(x,y) \mapsto \beta(y)(x)$ defines a pairing

$$e_\lambda : A[\lambda] \times B^\vee[\lambda^\vee] \to \mathbb{G}_m\,. \tag{4}$$

In the particular case $\lambda = n : A \to A$, this gives a pairing

$$e_n : A[n] \times A^\vee[n] \to \mu_n\,, \tag{5}$$

known as the *Weil pairing*. In the situation considered above, one has an isogeny $\varphi_L : A \to A^\vee$. So $A[\varphi_L] = A[\varphi_L^\vee]$, and this gives rise to a pairing

$$e_{\varphi_L} : A[\varphi_L] \times A[\varphi_L] \to \mathbb{G}_m\,. \tag{6}$$

The following proposition gives the connection between this and the commutator pairing in (2).

Proposition 2.3. $e^L = e_{\varphi_L}$.

Proof: This appears to be well known. It is alluded to in [26] and proven in [25, Theorem 11.20]. □

2.3. **The Tate pairing.** Together with the cup product, the Weil pairing e_n induces a symmetric bilinear pairing

$$T_n : \mathrm{H}^1(K, A[n]) \times \mathrm{H}^1(K, A^\vee[n]) \to \mathrm{H}^2(K, \mu_n) = \mathrm{Br}(K)[n]\,. \tag{7}$$

Recall that for any n indivisible by the characteristic of K, we have a Kummer sequence

$$0 \longrightarrow A(K)/nA(K) \xrightarrow{\delta} \mathrm{H}^1(K, A[n]) \longrightarrow \mathrm{H}^1(K, A)[n] \longrightarrow 0\,. \tag{8}$$

If $V \in \mathrm{H}^1(K, A)[n]$ is a torsor under A of period dividing n, then any lift to $\mathrm{H}^1(K, A[n])$ will be called a *Kummer lift of* V. Tate has shown (e.g. [17, Section I.3]) that T_n descends to give a symmetric bilinear pairing

$$\tilde{T}_n : \frac{A(K)}{nA(K)} \times \mathrm{H}^1(K, A^\vee)[n] \to \mathrm{Br}(K)[n]\,, \tag{9}$$

which is compatible with T_n and the Kummer sequences of A and $A^\vee$. Namely $\tilde{T}_n(R, V) = T_n(\delta(R), \tilde{V})$ where $\delta(R)$ is the image of R in $\mathrm{H}^1(K, A[n])$ under the connecting homomorphism and $\tilde{V}$ is any Kummer lift of V.

2.4. **The case of a principal polarization.** Suppose now that (A, P) is a principally polarized abelian variety over K, and consider the isogeny φ_n associated to the line bundle $L = nP$. Upon identification of $A^\vee[n]$ and $A[n]$ using the principal polarization, the isogeny φ_n is multiplication by n. Using the same identification, we can interpret the pairings T_n and $\tilde{T}_n$ as being defined on $\mathrm{H}^1(K, A[n]) \times \mathrm{H}^1(K, A[n])$ and $A(K)/nA(K) \times \mathrm{H}^1(K, A)[n]$, respectively. For simplicity we denote the corresponding connecting map Δ_L in (3) by Δ_n.

Proposition 2.4. *Let A/K be a principally polarized abelian variety over a field K of characteristic not dividing n. Then the bilinear form associated to Δ_n is T_n.*

Proof: By Zarkhin's result we know that the bilinear form associated to Δ_n is the cup product associated to the commutator pairing e^{nP} for the theta group of $A[n]$. By proposition 2.3 this coincides with the pairing $e_{\varphi_{nP}}$ associated to the isogeny φ_{nP}. As φ_{nP} is multiplication by n on $A \simeq A^\vee$, we see that $e_{\varphi_{nP}}$ is the Weil pairing $e_n : A[n] \times A[n] \to \mu_n$. The cup product induced by this is equal to T_n. □

For a principally polarized abelian variety, the map

$$\Delta_n : \mathrm{H}^1(K, A[n]) \longrightarrow \mathrm{Br}(K)\,,$$

will be referred to as the *obstruction map*. Clark gives two other equivalent definitions of the obstruction map which allow him to use Δ_n to study the period-index problem for torsors under A. Rather than giving details, we encourage the reader to consult [5, Section 5]. The following theorem gives the crucial connection between this map and the index of a torsor.

Theorem 2.5 (Clark)**.** *Let A/K be a strongly principally polarized abelian variety over a field K of characteristic not dividing n. Assume A has G_K-invariant Néron-Severi group and let $V \in \mathrm{H}^1(K, A)[n]$. If $\Delta_n(\xi) \neq 0$ for every Kummer lift ξ of V, then V cannot be split over any degree n field extension. If n is a prime power, we have moreover that the index of V exceeds n.*

Proof: See [5, Theorem 31]. The proof there uses the assumption that the principal polarization is strong and that the Néron-Severi group is trivial as a Galois module. □

2.5. **Local results.** We now specialize to the case that A/k is a principally polarized abelian variety defined over a number field k. The definition of the obstruction map is functorial in the base field. In particular it commutes with restriction maps. For a completion k_v of k at a prime v, we we will use $\Delta_{n,v}$ to denote the corresponding 'local obstruction map' $\Delta_{n,v} : \mathrm{H}^1(k_v, A[n]) \to \mathrm{Br}(k_v)$. Similarly the local versions of the Tate pairings T_n and $\tilde{T}_n$ will be denoted by $T_{n,v}$ and $\tilde{T}_{n,v}$, respectively.

We recall the following important theorem of Tate (see [17, I.3.4]).

Theorem 2.6 (Tate)**.** *For any nonarchimedean prime v, the pairings $T_{n,v}$ and $\tilde{T}_{n,v}$ are nondegenerate.*

The Brauer group of k_v embeds in $\mathbb{Q}/\mathbb{Z}$. Thus these pairings establish Pontryagin duality between the finite groups appearing in their domains. In the nonarchimedean case, one can determine the size of these groups by using the fact that $A(k_v)$ contains a finite index subgroup isomorphic to $\dim(A)$ copies of the maximal ideal in the ring of integers of k_v.

Lemma 2.7. *Let v be a nonarchimedean prime of k above the rational prime q, and let n be a positive integer. Then*

$$\#\,\mathrm{H}^1(k_v, A)[n] = \#A(k_v)/nA(k_v) = q^{\dim(A)\cdot \mathrm{ord}_q(n)\cdot[k_v:\mathbb{Q}_q]} \cdot \#A(k_v)[n]\,.$$

PROOF: The first equality follows from the nondegeneracy of $\tilde{T}_{n,v}$. For the second see [21, Proposition 3.9]. □

Using the Kummer sequence (8) one easily determines the size of $\mathrm{H}^1(k_v, A[n])$. The following lemma is also useful.

Lemma 2.8. *Let v be a nonarchimedean prime, and let n be a positive integer. Then the exponent of $\mathrm{H}^1(k_v, A[n])$ is equal to the exponent of $A(k_v)/nA(k_v)$.*

PROOF: Let m be the exponent of $A(k_v)/nA(k_v)$ and let $n' = n/m$. By Tate's duality theorem m is also the exponent of $\mathrm{H}^1(k_v, A)[n]$. Consider the commutative diagram (with exact rows, but non-exact columns)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{A(k_v)}{nA(k_v)} & \longrightarrow & \mathrm{H}^1(k_v, A[n]) & \longrightarrow & \mathrm{H}^1(k_v, A)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle m_*} & & \downarrow{\scriptstyle m} & & \\
0 & \longrightarrow & \frac{A(k_v)}{n'A(k_v)} & \xrightarrow{\delta_{n'}} & \mathrm{H}^1(k_v, A[n']) & \longrightarrow & \mathrm{H}^1(k_v, A)[n'] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle i_*} & & \downarrow & & \\
0 & \longrightarrow & \frac{A(k_v)}{nA(k_v)} & \xrightarrow{\delta_n} & \mathrm{H}^1(k_v, A[n]) & \longrightarrow & \mathrm{H}^1(k_v, A)[n] & \longrightarrow & 0
\end{array}$$

Here δ_n and $\delta_{n'}$ denote the connecting homomorphisms in the Kummer sequences for n and n', respectively. The maps i_* and m_* are induced by $A[n'] \xhookrightarrow{i} A[n]$ and $A[n] \xrightarrow{m} A[n']$, respectively. The composition of the middle column gives multiplication by m in the group $\mathrm{H}^1(k_v, A[n])$. Our assumption is that both maps labelled m in the diagram are the zero map. A diagram chase then shows that $i_* \circ m_* = 0$ as well. So $\mathrm{H}^1(k_v, A[n])$ has exponent dividing m. □

Proposition 2.9. *Let v be a nonarchimedean prime and n a positive integer. If $A(k_v)/nA(k_v)$ is nontrivial, then $\Delta_{n,v}$ is not the zero map. If the exponent m of $A(k_v)/nA(k_v)$ is odd and the principal polarization is symmetric, then $\Delta_{n,v}\left(\mathrm{H}^1(k_v, A[n])\right) = \mathrm{Br}(k_v)[m]$.*

Applying the Chebotarëv density theorem to the extension $k(A[n])/k$ and using lemma 2.7, the first statement yields the following corollary.

Corollary 2.10. *Let A/k be a principally polarized abelian variety over a number field and $n \geq 2$. There are infinitely many primes v of k for which $\Delta_{n,v}$ is not the zero map.*

PROOF: For the first statement recall that the bilinear form associated to $\Delta_{n,v}$ is $T_{n,v}$, which by Tate's theorem is nondegenerate. The assumption implies that $\mathrm{H}^1(k_v, A[n]) \neq 0$, so the result is clear. For the second, lemma 2.8 shows that the exponent of $\mathrm{H}^1(k_v, A[n])$ is equal to that of $A(k_v)/nA(k_v)$. By Zarkhin's result, $\Delta_{n,v}$ is a quadratic form on the finite dimensional $\mathbb{Z}/m\mathbb{Z}$-module $\mathrm{H}^1(k_v, A[n])$. Since m is odd, the image of $\Delta_{n,v}$ is contained in the m-torsion subgroup of $\mathrm{Br}(k_v) \simeq \mathbb{Q}/\mathbb{Z}$ (this is a general property of quadratic maps; see [5, Lemma 42]). We are thus in a position to apply lemma 2.2. We need to show that $\mathrm{H}^1(k_v, A[n])$ contains an isotropic element of order m. The compatibility of $T_{n,v}$ and $\tilde{T}_{n,v}$ shows that the image of any element in $A(k_v)/nA(k_v)$ under the connecting homomorphism is isotropic with respect to $T_{n,v}$. By assumption on the exponent there is such an element of order m. □

The (middle third of) the Poitou-Tate exact sequence for $A[n]$ (see [24, Section II.6]) and the fundamental exact sequence for the Brauer group of k give rise to the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
 & & \mathrm{H}^1(k, A[n]) & \xrightarrow{\mathrm{res}} & \prod{}' \mathrm{H}^1(k_v, A[n]) & \xrightarrow{\phi} & \mathrm{H}^1(k, A[n])^* & & \\
 & & \downarrow{\scriptstyle \Delta_n} & & \downarrow{\scriptstyle \prod \Delta_{n,v}} & & & & \\
0 & \longrightarrow & \mathrm{Br}(k) & \xrightarrow{\mathrm{res}} & \bigoplus \mathrm{Br}(k_v) & \xrightarrow{\Sigma} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0
\end{array}$$

The product is the restricted product with respect to unramified subgroups. For all but finitely many primes, the unramified subgroups are exact annihilators with respect to the Tate pairing, so the vertical map in the middle is well-defined.

Clark asked ([5, Question 45]) if $\Delta_n\left(\mathrm{H}^1(k, A[n])\right) = \mathrm{Br}(k)[n]$ when A/k is a strongly principally polarized abelian variety over a number field. The analysis above shows that this is not the case in general (or even generically; see the remark below). If there is some $\sigma \in G_k$ which acts on $A[n]$ with no nontrivial fixed points, then by Chebotarëv's density theorem there are infinitely many primes v for which $A(k_v)/nA(k_v)$, $\mathrm{H}^1(k_v, A)[n]$ and $\mathrm{H}^1(k_v, A[n])$ are all trivial (cf. lemma 2.7). The diagram above shows that every element in the image of Δ_n must be trivial at these primes. One might still ask the following.

Question 2.11. *Consider an abelian variety A/k over a number field k with a (symmetric) principal polarization. Let $D \in \mathrm{Br}(k)$ be such that the local invariant $\mathrm{inv}_v(D)$ has order dividing the exponent of $A(k_v)/nA(k_v)$ for every prime v. Is D in the image of the obstruction map Δ_n?*

It seems unlikely that this is the whole story, since exactness of the Poitou-Tate sequence should place additional restrictions on the image of Δ_n. The results of the next section (e.g. corollary 3.2) show at least that, given D as in the question, there exist elements in the image of Δ_n whose local invariants coincide with D on an arbitrarily large finite sets of primes.

Remark: By a result of Serre [23] (see also [16, Corollary 2.1.7]) there exists an integer $d = d(A/k)$ such that for any $n \geq 1$, all d-th powers in $(\mathbb{Z}/n\mathbb{Z})^\times$ arise as homotheties via the action of G_k on $A[n]$. In particular, for any n sufficiently large, there exists $\sigma \in G_k$ which acts on $A[n]$ with no nontrivial fixed points.

We close this section with the following theorem of Lang and Tate [13, Corollary 1 to Theorem 1, p. 676] which gives a simple criterion for determining splitting fields of torsors over local fields.

Theorem 2.12 (Lang-Tate)**.** *Let v be a prime of k above the rational prime q. Suppose that A has good reduction at v, that n is prime to q and that $V \in \mathrm{H}^1(k_v, A)[n]$ is a torsor under A/k_v of exact period n. Then for any finite field extension K_v/k_v, $V(K_v) \neq \emptyset$ if and only if n divides the ramification index of K_v/k_v.*

3. Weak approximation

Let A/k be a principally polarized abelian variety over a number field k. Under the assumption of full level n structure, one has $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ as G_k-modules (where $g = \dim A$) and $\mu_n \subset k$. Consequently the cohomology group $\mathrm{H}^1(k, A[n])$ splits as $2g$ copies of $k^\times/k^{\times n}$. The Grunwald-Wang theorem (or rather a slight variation thereof [19, Theorems 9.1.11, 9.2.3]) implies that the restriction map in the following diagram is injective and has dense image in the product of the discrete topologies.

$$\begin{array}{ccc} \mathrm{H}^1(k, A[n]) & = & (k^\times/k^{\times n})^{2g} \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ \prod_v \mathrm{H}^1(k_v, A[n]) & = & \prod_v (k_v^\times/k_v^{\times n})^{2g} \end{array} \tag{10}$$

This, together with the fact that one can interpret the obstruction map Δ_n in terms of norm residue symbols in this case seems to be responsible for 'most' of the period-index discrepancies constructed (see for example, [3, Proposition 7], [6], or [5]).

Another approach used by Clark (e.g. [4, Proof of theorem 1]) is to make use of the fact [17, Theorem I.6.26(b)] that for any abelian variety A/k over a number field with $Ш(A/k)[p^\infty]$ finite, there is an exact sequence

$$Ш(A/k)[p^\infty] \to \mathrm{H}^1(k, A)[p^\infty] \xrightarrow{\mathrm{res}} \bigoplus \mathrm{H}^1(k_v, A)[p^\infty] \to A(k)^{\vee\wedge *}\,, \tag{11}$$

the last term being the Pontryagin dual of the pro-p completion of the Mordell-Weil group of the dual abelian variety. If one is willing to assume that $Ш(A/k)$ and $A(k)$ are finite, one again gets very satisfactory control over the restriction map. But at present, this limits us to elliptic curves of analytic rank zero over $\mathbb{Q}$. When applied to abelian varieties (i.e. taking $M = A[n]$) the *weak weak approximation theorem* below gives a finite level version of (11) which requires no assumption on either the Mordell-Weil or Tate-Shafarevich groups.

For the statement we need the following notation. For any G_k-module M and any set of primes S of k, let $Ш^1(k, M; S)$ denote the kernel of the restriction map

$$\mathrm{H}^1(k, M) \to \prod_{v \notin S} \mathrm{H}^1(k_v, M)\,.$$

This is the subgroup of cocycle classes that are trivial outside S. We use S^c to denote the complement of S.

Theorem 3.1 (weak weak approximation)**.** *Let M be a finite G_k-module and S the finite set of primes where $M^\vee$ is ramified. Then the map*

$$\mathrm{res}_{S^c} : Ш^1(k, M; S^c) \to \prod_{v \notin S} \mathrm{H}^1(k_v, M)$$

has dense image in the product of the discrete topologies.

Results of this kind are well known. The statement here is a rather simple generalization of [19, 9.2.2–9.2.3] or [17, I.9.8]. As we were unable to locate the specific formulation needed for our present application in the literature, we offer the reader [7, Theorem 1.6]. We remark that in general it is necessary to exclude the primes in S. The (now) standard counterexample led to the correct formulation of the Grunwald-Wang theorem; the map $\mathrm{H}^1(\mathbb{Q}, \mathbb{Z}/8\mathbb{Z}) \to \mathrm{H}^1(\mathbb{Q}_2, \mathbb{Z}/8\mathbb{Z})$ is not surjective. Applying the theorem to $M = A[n]$ and using the criterion of Néron-Ogg-Shafarevich one obtains the following corollary (the second result is obtained from the first by use of the Kummer sequence).

Corollary 3.2. *Let A/k be an abelian variety over a number field, n an integer and S the finite set of primes containing all primes of bad reduction for $A^\vee$ and all primes dividing n. Then the restriction maps*

$$Ш^1(k, A[n]; S^c) \to \prod_{v \notin S} \mathrm{H}^1(k_v, A[n])\,, \text{ and}$$
$$Ш^1(k, A; S^c)[n] \to \prod_{v \notin S} \mathrm{H}^1(k_v, A)[n]$$

have dense images.

4. Proofs of the main theorems

It follows from the theorem of Lang and Tate (2.12) that any finite collection of torsors of period n that are locally solvable at all 'bad primes' can be turned into a finite collection of elements of $Ш(A/\ell)[n]$ over a sufficiently ramified extension ℓ/k of degree n. The difficulty is in showing that one can choose the torsors in such a way that they yield distinct, and in particular nontrivial, elements of $Ш(A/\ell)$. One way of achieving this is to rig the torsors (and their differences) to have index strictly larger than n. This is the motivation behind [6, Theorem 2], which we generalize to the higher-dimensional situation with the following theorem. This proves theorem 1.2.

Theorem 4.1. *Let $n > 1$ be an integer, A/k a strongly principally polarized abelian variety over a number field k whose Néron-Severi group is trivial as a G_k-module and S any finite set of primes. There exists a sequence $\{V_i\}_{i=0}^{\infty} \subset \mathrm{H}^1(k, A)[n]$ of torsors such that*

1. *$V_0(k) \neq \emptyset$.*
2. *for all $i \geq 0$, $V_i \in Ш^1(k, A; S^c)[n]$.*
3. *for all $i \neq j$, $V_i - V_j$ cannot be split by any extension of degree n.*

If n is a prime power, then the sequence may be chosen so that for all $i \neq j$, the index of $V_i - V_j$ exceeds n.

Proof: By enlarging S if necessary we may assume S contains all primes of bad reduction for A, all primes dividing n and all archimedean primes. Choose representatives $Q_1, \ldots, Q_R \in A(k)$ for the finitely many classes in $A(k)/nA(k)$ (Mordell-Weil Theorem), and denote their images in $\mathrm{H}^1(k, A[n])$ under the connecting homomorphism in the Kummer sequence by $q_1, \ldots, q_R$. We will define the sequence inductively. The base of induction is established by setting $V_0 = A$. So assume we have torsors $V_0, \ldots, V_{N-1}$ satisfying the three conditions in the theorem, and let $\{\eta_0, \ldots, \eta_{N-1}\} \subset \mathrm{H}^1(k, A[n])$ denote a set of Kummer lifts of the V_i.

Corollary 2.10 guarantees that there are infinitely many primes v of k for which $\Delta_{n,v} : \mathrm{H}^1(k_v, A[n]) \to \mathrm{Br}(k_v)$ is not the zero map. We may choose $N \cdot R$ distinct such primes, none of which lie in S. Arrange these primes into N sets $\{v_{i,r}\}_{r=1}^{R}$ of size R (so $0 \leq i < N$). For each $v_{i,r}$, let $\xi_{i,r} \in \mathrm{H}^1(k_{v_{i,r}}, A[n])$ be a class such that $\Delta_{n,v_{i,r}}(\xi_{i,r}) \neq 0$.

By corollary 3.2 there exists a class $\eta_N \in Ш^1(k, A[n]; S^c) \subset \mathrm{H}^1(k, A[n])$ such that for $0 \leq i < N$ and $1 \leq r \leq R$, we have $\mathrm{res}_{v_{i,r}}(\eta_N) = \xi_{i,r} + \mathrm{res}_{v_{i,r}}(\eta_i - q_r)$. Let V_N be the image of η_N in $\mathrm{H}^1(k, A)[n]$. Then

$V_N \in Ш^1(k, A; S^c)[n]$. Let $i \in \{0, \dots, N-1\}$ and consider $V_N - V_i$. Any Kummer lift of $V_N - V_i$ is of the form $\eta_N - \eta_i + q_r$ for some $r \in \{1, \dots, R\}$. The restriction of this lift at the prime $v_{i,r}$ is equal to $\xi_{i,r}$. Our choice was such that $\Delta_{n,v_{i,r}}(\xi_{i,r}) \neq 0$. Compatibility of the obstruction map with the restriction maps shows that $\Delta_n(\eta_N - \eta_i + q_r) \neq 0$. This is the case for every Kummer lift of $V_N - V_i$, so the result follows from theorem 2.5. □

Remark: The reader will note that it is only in the final application of theorem 2.5 that we make use of the assumptions that the polarization is strong and that the Néron-Severi group is trivial as a G_k-module.

Proof of Theorems 1.1 and 1.3: First note that theorem 1.3 implies theorem 1.1. We can deduce theorem 1.3 from theorem 4.1 as follows. Let S be the finite set consisting of all primes of bad reduction for A, all primes above p and all archimedean primes. Let T be the set of primes outside S where $A(k_v)[p] \neq 0$, and let $\{\ell_j\}$ be a sequence of extensions as in the statement of theorem 1.3. Let $N \geq 1$ and let $\{V_i\}_{i=0}^{\infty}$ be the sequence of torsors given by theorem 4.1 (applied with $n = p$). By construction $V_0, \dots, V_N \in Ш(k, A, S^c)[p]$ and their differences cannot be split by any extension of degree p. So for all $j \geq 1$, their images in $\mathrm{H}^1(\ell_j, A)[p]$ are distinct. It is enough to show that when j is sufficiently large, their images lie in the subgroup $Ш(A/\ell_j)[p]$.

Let U be the finite set of primes v such that for some $i \leq N$, $V_i(k_v) = \emptyset$. If ℓ/k is any degree p extension totally ramified at all primes of U, then, by the theorem of Lang and Tate (2.12), $V_0, \dots, V_N$ represent classes in $Ш(A/\ell)[p]$. On the other hand, lemma 2.7 shows that $U \subset T$. So by assumption the extension ℓ_j/k is totally ramified at all primes of U, whenever j is sufficiently large. This completes the proof. □

Proof of Theorem 1.4: Let ℓ/k be an extension of degree p and let V/k be an element of $\mathrm{H}^1(k, A)$. Assume $\mathrm{res}_{\ell/k}(V) \in Ш(A/\ell)[p^\infty]$. In other words, $\mathrm{res}_{\ell/k}(V)$ is an arbitrary element of $Ш_k(A/\ell)[p^\infty]$. Let S be the set of primes v such that A has bad reduction at v or such that v lies above p, and set

$$T = \{v \notin S \,:\, A(k_v)[p] \neq 0\},$$
$$U = S \cup \{v \in T \,:\, \text{ } v \text{ is totally ramified in } \ell \,\}.$$

Since $\mathrm{res}_{\ell/k}(V)$ has p-powered period, it also has p-powered index. As ℓ/k is of degree p, we see that $V \in \mathrm{H}^1(k, A)[p^\infty]$. We claim that the image of V under the map

$$\mathrm{res} = \prod_v \mathrm{res}_v : \mathrm{H}^1(k, A)[p^\infty] \to \bigoplus_v \mathrm{H}^1(k_v, A)[p^\infty]$$

lands in the subgroup

$$G := \prod_{v \in U} \mathrm{H}^1(k_v, A)[p] \times \prod_{v \notin U} \{0\}.$$

To prove the claim first note that for all primes v, the period and the index of $\mathrm{res}_v(V)$ divide p (since V becomes everywhere locally solvable after an extension of degree p). On the other hand, the Lang-Tate result implies that the period and the index of $\mathrm{res}_v(V)$ are equal to 1 at all nonarchimedean primes $v \notin U$. Now suppose v is archimedean and w is a prime of ℓ above v. The only nontrivial situation is when $\ell_w \neq k_v$, which can only occur when v is real and ramified, hence in U. This establishes the claim.

The bound will be obtained by computing the size of the preimage of G under res. First note that for the archimedean primes in U we have $\#\,\mathrm{H}^1(\mathbb{R}, A)[2] = \#\pi_0(A(\mathbb{R})) \leq \#A(\mathbb{R})[2]$ (see [17, I.3.7]). For nonarchimedean primes the size of $\mathrm{H}^1(k_v, A)[p]$ is given by lemma 2.7 and theorem 2.6. From this we get

$$\begin{aligned}
\#G &= \prod_{v \in U} \#\,\mathrm{H}^1(k_v, A)[p] \\
&= \left(\prod_{v|p} \#\,\mathrm{H}^1(k_v, A)[p] \right) \cdot \left(\prod_{U \ni v \nmid p} \#\,\mathrm{H}^1(k_v, A)[p] \right) \\
&= \left(\prod_{v|p} p^{g[k_v:\mathbb{Q}_p]} \#A(k_v)[p] \right) \cdot \left(\prod_{U \ni v \nmid p} \#A(k_v)[p] \right) \\
&= p^{g[k:\mathbb{Q}]} \cdot \prod_{v \in U} \#A(k_v)[p] \\
&\leq p^{g([k:\mathbb{Q}]+2\cdot\#U)} = p^{g[k:\mathbb{Q}]+2g(\#T+\#S)}.
\end{aligned}$$

On the other hand, the kernel of res is the p-primary part of $Ш(A/k)$. This gives the result. □

5. Examples

We maintain the notation above. Consider the mod p representation $G_k \to \mathrm{GL}(A[p]) \simeq \mathrm{GL}_{2g}(\mathbb{F}_p)$ associated to A/k, where $g = \dim(A)$. If $\sigma_v \in \mathrm{GL}_{2g}(\mathbb{F}_p)$ denotes the image of the Frobenius element at some prime $v \notin S$, then $v \in T$ if and only if σ_v has 1 as an eigenvalue. It is well known (see the remark following question 2.11) that if p is sufficiently large, then the image of the mod p representation contains nontrivial scalar matrices. When this is the case, Chebotarëv's density theorem gives a positive density set of primes outside of T. For elliptic curves without complex multiplication, an earlier result of Serre gives that the mod p representation is surjective for all but finitely many p. In this case T has density

$$\frac{\#\{g \in \mathrm{GL}_2(\mathbb{F}_p) \,:\, 1 \text{ is an eigenvalue of } g\,\}}{\#\,\mathrm{GL}_2(\mathbb{F}_p)} = \frac{(p^2-2)}{(p^2-1)(p-1)}\,,$$

which approaches 0 as p goes to ∞. This is of some interest since theorems 1.3 and 1.4 are stronger when T is small. On the other extreme, if $A(k)[p] \neq \emptyset$, one has that every prime outside S lies in T.

For a concrete example consider the elliptic curve $E/\mathbb{Q}$ of conductor 11 with minimal model $y^2 + y = x^3 - x^2 - 10x - 20$. For $p = 3$, the bad primes are $S = \{3, 11\}$. The mod 3 representation is surjective so T has density 7/16. The first few primes in T are 29, 53, 67, 71, 79, 83, 89, ... One easily checks that $E(\mathbb{Q}_3)[3] = E(\mathbb{Q}_{11})[3] = 0$, so the group G in the proof of 1.4 reduces to $\mathrm{H}^1(\mathbb{Q}_3, E)[3] \times \prod_{q\neq 3}\{0\}$, which has order 3. A 3-descent (implemented in MAGMA, see [22]) shows that $Ш(E/\mathbb{Q})[3^\infty] = 0$ (in fact, deeper results prove that $Ш(E/\mathbb{Q}) = 0$). Thus, there are at most 3 elements in $\mathrm{H}^1(\mathbb{Q}, E)$ which restrict into G. In fact, there are exactly 3; the inverse pair of nontrivial trivial torsors are represented by the plane cubic

$$C : -4x^3 + 3x^2z - 6xy^2 - 30xyz - 27xz^2 - 11y^3 - 9y^2z - 12yz^2 + 8z^3 = 0\,,$$

which is locally solvable at all primes $q \neq 3$. It follows that if ℓ is any cubic number field which is not totally ramified at any primes of T, we have

$$\#Ш_{\mathbb{Q}}(E/\ell)[3^\infty] = \begin{cases} 3 & \text{if } C(\ell) = \emptyset, \text{ but } C(\ell_w) \neq \emptyset \text{ for all } w \mid 3, \\ 1 & \text{otherwise.} \end{cases}$$

At the same time, theorem 1.3 gives that $\#Ш_{\mathbb{Q}}(E/\ell)[3]$ is unbounded as ℓ runs through the fields $\mathbb{Q}(\sqrt[3]{29})$, $\mathbb{Q}(\sqrt[3]{29\cdot 53})$, $\mathbb{Q}(\sqrt[3]{29\cdot 53\cdot 67})$, ...

On the other hand, $E(\mathbb{Q})$ is generated by the 5-torsion point $(5, 5) \in E(\mathbb{Q})$. So, for $p = 5$, we have $T = S^c$. For cyclic extensions $\ell/\mathbb{Q}$, Matsuno's result [15, Corollary 4.5] shows that $\dim_{\mathbb{F}_5} Ш(E/\ell)[5] + \mathrm{rank}(E(\ell))$ grows linearly in the number of ramified primes. Our upper bound for $\dim_{\mathbb{F}_5} Ш_{\mathbb{Q}}(E/\ell)[5]$ also grows linearly with the number of totally ramified primes, and one would expect that this is true of $\dim_{\mathbb{F}_5} Ш_{\mathbb{Q}}(E/\ell)[5]$ itself. However, theorem 1.3 only applies to a sequence of extensions which is eventually totally ramified at *almost every* prime of k. This deficiency ultimately traces back to the use of theorem 3.1, itself a consequence of Poitou-Tate duality which is ineffective as an existence theorem.

References

[1] R. Bölling, Die Ordnung der Schafarewitsch-Tate Gruppe kann beliebig groß werden, Math. Nachr. 67 (1975) 157–179.
[2] J.W.S. Cassels, Arithmetic on curves of genus 1, VI. The Tate-Šafarevič group can be arbitrarily large, J. Reine Angew. Math. 214–215 (1964) 65–70.
[3] P.L. Clark, The period-index problems in WC-groups I: elliptic curves, J. Number Theory 114 (2005) 193–208.
[4] P.L. Clark, There are genus one curves of every index over every number field, J. Reine Angew. Math. 594 (2006) 201–206.
[5] P.L. Clark, Period-index problems in WC-groups II: abelian varieties, (preprint) arXiv:math/0406135v1.
[6] P.L. Clark and S. Sharif, Period, index and potential Ш, Algebra and Number Theory 4 (2010) 151–174.
[7] B. Creutz, A Grunwald-Wang type theorem for abelian varieties, (preprint) arXiv:math/1009.3546v2.
[8] S. Donnelly, Elements of given order in Tate-Shafarevich groups of elliptic curves, PhD Thesis (2003) University of Georgia.
[9] T. Fisher, Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$, J. Eur. Math. Soc. 3 (2001) 169–201.
[10] R. Kloosterman, The p-part of Tate-Shafarevich groups of elliptic curves can be arbitrarily large, J. Théor. Nomb. Bordeaux 17 (2005) 787–800.
[11] R. Kloosterman and E.F. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, J. Number Theory 99 (2003) 148–163.
[12] K. Kramer, A family of semistable elliptic curves with large Tate-Shararevitch groups, Proc. Amer. Math. Soc., 89 (1983) 379–386.
[13] S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties, Amer. J. Math. 80 (1958) 659-684.
[14] K. Matsuno, Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups, Manuscripta Math. 122 (2007) 289–304.

[15] K. Matsuno, Elliptic curves with large Tate-Shafarevich groups over a number field, Math. Res. Lett. 16 (2009) 449–461.
[16] M. McQuillen, Division points on semi-abelian varieties, Invent. Math. 120 (1995) 143-159.
[17] J.S. Milne, Arithmetic duality theorems, Perspectives in Mathematics 1, Academic Press, Boston, 1986.
[18] D. Mumford, On the equations defining abelian varieties. I, Invent. Math. 1 (1966) 287–354.
[19] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields (second edition), Grundlehren Math. Wiss. 323, Springer-Verlag, Berlin, 2008.
[20] C.H. O'Neil, The period-index obstruction for elliptic curves, J. Number Theory 95 (2002) 329–339.
[21] E.F. Schaefer, Class groups and Selmer groups, J. Number Theory 56 (1996) 79–114.
[22] E.F. Schaefer and M. Stoll, How to do a p-descent on an elliptic curve, Trans. Amer. Math. Soc. 356 (2004) 1209-1231.
[23] J-P. Serre, Quelques propriétés des groupes algébriques commutatifs, Appendix in Astérisque 69-70 (1979) 191-202.
[24] J-P. Serre, Galois cohomology (second printing), Springer Monogr. Math., Springer-Verlag Berlin Heidelberg New York, 2002.
[25] G. van der Geer and B. Moonen, Abelian varieties, available at: http://staff.science.uva.nl/∼bmoonen/boek/BookAV.html
[26] Yu.G. Zarkhin, Noncommutative cohomologies and Mumford groups, Math. Notes 15 (1974) 241–244. Translated from Mat. Zametki 15 (1974) 415–419.

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia