JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 25, Number 1, January 2012, Pages 245–269
S 0894-0347(2011)00710-8
Article electronically published on July 12, 2011

RANDOM MAXIMAL ISOTROPIC SUBSPACES AND SELMER GROUPS

BJORN POONEN AND ERIC RAINS

1. Introduction

1.1. **Selmer groups.** D. R. Heath-Brown [HB93, HB94], P. Swinnerton-Dyer [SD08], and D. Kane [Kan11] obtained the distribution for the nonnegative integer $s(E)$ defined as the $\mathbb{F}_2$-dimension of the 2-Selmer group $\mathrm{Sel}_2 E$ minus the dimension of the rational 2-torsion group $E(\mathbb{Q})[2]$, as E varies over quadratic twists of certain elliptic curves over $\mathbb{Q}$. The distribution was the one for which

$$\mathrm{Prob}\,(s(E)=d)=\left(\prod_{j\geq 0}(1+2^{-j})^{-1}\right)\left(\prod_{j=1}^{d}\frac{2}{2^j-1}\right).$$

In [HB94], it was reconstructed from the moments of $2^{s(E)}$; in [SD08] and [Kan11], it arose as the stationary distribution for a Markov process.

Our work begins with the observation that this distribution coincides with a distribution arising naturally in combinatorics, namely, the limit as $n\to\infty$ of the distribution of $\dim(Z\cap W)$, where Z and W are random maximal isotropic subspaces inside a hyperbolic quadratic space of dimension $2n$ over $\mathbb{F}_2$. Here it is essential that the maximal isotropic subspaces be isotropic not only for the associated symmetric bilinear pairing, but also for the quadratic form; otherwise, one would obtain the wrong distribution. That such a quadratic space might be relevant is suggested already by the combinatorial calculations in [HB94].

Is it just a coincidence, or is there some direct relation between Selmer groups and intersections of maximal isotropic subgroups? Our answer is that $\mathrm{Sel}_2 E$ is naturally the intersection of two maximal isotropic subspaces in an *infinite-dimensional* quadratic space V over $\mathbb{F}_2$. The fact that it could be obtained as an intersection of two subspaces that were maximal isotropic for a pairing induced by a Weil pairing is implicit in standard arithmetic duality theorems.

To make sense of our answer, we use the theory of quadratic forms on locally compact abelian groups as introduced by A. Weil in [Wei64]. The locally compact abelian group V in the application is the restricted direct product of the groups $\mathrm{H}^1(\mathbb{Q}_p, E[2])$ for $p\leq\infty$ with respect to the subgroups of unramified classes. The

Received by the editors September 21, 2010 and, in revised form, April 20, 2011, and May 20, 2011.

2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 11G05, 11G30, 14G25, 14K15.

Key words and phrases. Selmer group, Shafarevich-Tate group, maximal isotropic, quadratic space, Weil pairing, theta characteristic.

The first author was partially supported by NSF grant DMS-0841321.

©2011 American Mathematical Society
Reverts to public domain 28 years from publication

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

quadratic form Q is built using D. Mumford's Heisenberg group, using ideas of Yu. Zarhin [Zar74, §2]. Then arithmetic duality theorems are applied to show that the images of the compact group $\prod_{p\le\infty} E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ and the discrete group $\mathrm{H}^1(\mathbb{Q}, E[2])$ are maximal isotropic in (V, Q). Their intersection is $\mathrm{Sel}_2 E$.

1.2. **Conjectures for elliptic curves.** This understanding of the structure of $\mathrm{Sel}_2 E$ suggests the following, in which we replace 2 by p and generalize to global fields:

Conjecture 1.1. *Fix a global field k and a prime p.*

(a) *As E varies over all elliptic curves over k,*

$$\mathrm{Prob}\left(\dim_{\mathbb{F}_p} \mathrm{Sel}_p E = d\right) = \left(\prod_{j\ge 0}(1+p^{-j})^{-1}\right)\left(\prod_{j=1}^{d}\frac{p}{p^j-1}\right).$$

(For the sake of definiteness, we define the probability by considering the finitely many elliptic curves $y^2 = x^3 + ax + b$ where $a, b \in k$ have height $\le B$, and looking at the limit of the probability as $B \to \infty$; use a long Weierstrass equation if $\mathrm{char}\, k$ *is* 2 *or* 3*.)*

(b) *The average of $\#\mathrm{Sel}_p E$ over all E/k is $p+1$.*

(c) *For $m \in \mathbb{Z}_{\ge 0}$, the average of $(\#\mathrm{Sel}_p E)^m$ over all E/k is $\prod_{i=1}^{m}(p^i+1)$.*

Several results in the direction of Conjecture 1.1 are known:

- When $p = 2$, Heath-Brown [HB94, Theorem 2] proved the analogue of Conjecture 1.1 for the family of quadratic twists of $y^2 = x^3 - x$ over $\mathbb{Q}$, with the caveat that the distribution of $\dim \mathrm{Sel}_2 E$ is shifted by $+2$ to account for the contribution of $E[2]$ (cf. Remark 4.17). Swinnerton-Dyer [SD08] and Kane [Kan11] generalized this result to the family of quadratic twists of any fixed elliptic curve $E/\mathbb{Q}$ with $E[2] \subseteq E(\mathbb{Q})$ and no rational cyclic subgroup of order 4.
- For the family of all elliptic curves $E/\mathbb{Q}$ with $E[2] \subset E(\mathbb{Q})$, G. Yu [Yu06, Theorem 1] built upon Heath-Brown's approach to prove that the average size of $\mathrm{Sel}_2 E$ is finite. (Strictly speaking, if the limit defining the average does not exist, the result holds with a lim sup.) See also [Yu05] for results for other families of elliptic curves over $\mathbb{Q}$.
- For the family of all elliptic curves over $\mathbb{F}_q(t)$ with $3 \nmid q$, A. J. de Jong [dJ02] proved that the average size of $\mathrm{Sel}_3 E$ (in the lim sup sense) is at most $4 + O(1/q)$, where the $O(1/q)$ is an explicit rational function of q. In fact, de Jong speculated that the truth was 4, and that the same might hold for number fields.
- For the family of all elliptic curves over $\mathbb{Q}$, M. Bhargava and A. Shankar proved that the average size of Sel_2 is 3 [BS10a] and the average size of Sel_3 is 4 [BS10b].
- For E over a number field k with a real embedding and with $E[2](k) = 0$, B. Mazur and K. Rubin [MR10] and Z. Klagsbrun showed how to twist judiciously to obtain lower bounds on the number of quadratic twists of E (up to a bound) with prescribed $\dim \mathrm{Sel}_2$.

As has been observed by Bhargava, since $\mathrm{rk}\, E(k) \le \dim_{\mathbb{F}_p} \mathrm{Sel}_p E$, Conjecture 1.1(b) would imply that $\mathrm{Prob}(\mathrm{rk}\, E(k) \ge 2)$ is at most $(p+1)/p^2$. If we assume

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

this for an infinite sequence of primes p, we conclude that asymptotically 100% of elliptic curves over k have rank 0 or 1.

A priori, the average rank could still be greater than 1 if there were rare curves of very high rank, but Conjecture 1.1(b) for an infinite sequence of primes p implies also that the elliptic curves of rank ≥ 2 contribute nothing to the average value of $\operatorname{rk} E(k)$, and in fact nothing to the average value of $p^{\operatorname{rk} E(k)}$. (Proof: Define e_p as the lim sup as $B \to \infty$ of the sum of $p^{\operatorname{rk} E(k)}$ over curves of rank ≥ 2 of height bounded by B divided by the total number of curves of height bounded by B. If q is a larger prime, then $e_p \leq (p^2/q^2)e_q \leq (p^2/q^2)(q+1)$, which tends to 0 as $q \to \infty$, so $e_p = 0$.)

If in addition we assume that the parity of $\operatorname{rk} E(k)$ is equidistributed, we obtain the following well-known conjecture:

Conjecture 1.2. *Fix a global field k. Asymptotically 50% of elliptic curves over k have rank 0, and 50% have rank 1. Moreover, the average rank is 1/2.*

Remark 1.3. D. Goldfeld conjectured that the average rank in a family of quadratic twists of a fixed elliptic curve over $\mathbb{Q}$ was 1/2 [Gol79, Conjecture B]. Other evidence for Conjecture 1.2 was provided by the extensive study by N. Katz and P. Sarnak of a function field analogue [KS99a, KS99b].

Also, as has been observed by Rubin, the distribution in Conjecture 1.1(a) tends, as $p \to \infty$, to the distribution assigning probability 50% to each of 0 and 1. Thus, even without assuming equidistribution of parity, Conjecture 1.1 for any infinite set of primes p would imply not only that 100% of elliptic curves have rank 0 or 1, but also that at least 50% have rank 0, and that the average rank is *at most* 1/2.

Conjecture 1.1(a) for a single p does not duplicate C. Delaunay's prediction for $\dim_{\mathbb{F}_p} Ш(E)[p]$ [Del01, Del07]. Instead the predictions complement each other: we prove that the only distribution on $\operatorname{rk} E(\mathbb{Q})$ compatible with both predictions is the one in Conjecture 1.2, for which $\operatorname{rk} E(\mathbb{Q})$ is 0 or 1, with probability 1/2 each (see Theorem 5.2). A related result, that Conjectures 1.1(a) (for $p = 2$) and 1.2 together imply the $Ш[2]$ predictions for rank 0 and 1, had been observed at the end of [Del07].

If we also use the heuristic that the dimensions of $\dim_{\mathbb{F}_p} \operatorname{Sel}_p E$ for different p are independent except for the constraint that their parities are equal, we are led to the following generalization of Conjecture 1.1:

Conjecture 1.4. *Fix a global field k and let n be a squarefree positive integer. Let $\omega(n)$ be the number of prime factors of n.*

(a) *Fix $d_p \in \mathbb{Z}_{\geq 0}$ for each prime p dividing n. As E varies over all elliptic curves over k,*

$$\operatorname{Prob}\left(\operatorname{Sel}_n E \simeq \prod_{p|n} (\mathbb{Z}/p\mathbb{Z})^{d_p}\right) = 2^{\omega(n)-1} \prod_{p|n} \left(\left(\prod_{j\geq 0}(1+p^{-j})^{-1}\right)\left(\prod_{j=1}^{d_p} \frac{p}{p^j-1}\right)\right)$$

if the d_p all have the same parity, and the probability is 0 otherwise.

(b) *The average of $\#\operatorname{Sel}_n E$ over all E/k is the sum of the divisors of n.*

(c) *For $m \in \mathbb{Z}_{\geq 0}$, the average of $(\#\operatorname{Sel}_n E)^m$ over all E/k is $\prod_{p|n}\prod_{i=1}^{m}(p^i+1)$.*

The factor of $2^{\omega(n)-1}$ arises in (a), because only 2 of the $2^{\omega(n)}$ choices of parities for $p \mid n$ are constant sequences.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Remark 1.5. Based on investigations for $n \leq 5$, Bhargava and Shankar have proposed Conjecture 1.4(b) for *all* positive integers n, at least for $k = \mathbb{Q}$.

Remark 1.6. As was noticed during a discussion with Bhargava and Kane, if we combine Delaunay's heuristics for $Ш[n]$ with Conjecture 1.2 for varying $E/\mathbb{Q}$, we can predict the distribution for the abelian group $\mathrm{Sel}_n E$ for *any* fixed positive integer n. Namely, $E(\mathbb{Q})_{\mathrm{tors}} = 0$ with probability 1, and in that case the term on the left in

$$0 \to \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \to \mathrm{Sel}_n E \to Ш(E)[n] \to 0$$

is free, so the sequence of $\mathbb{Z}/n\mathbb{Z}$-modules splits; thus, given Conjecture 1.2, the distribution of $\mathrm{Sel}_n E$ can be deduced from knowing the distribution of $Ш(E)[n]$ for rank 0 curves and for rank 1 curves.

1.3. **Conjectures for abelian varieties.** In fact, our theorems are proved in a more general context, with $[2]\colon E \to E$ replaced by any self-dual isogeny $\lambda\colon A \to \widehat{A}$ that is of odd degree or that comes from a symmetric line sheaf on an abelian variety A over a global field k. (See Theorem 4.14.) In this setting, we have a surprise: it is not $\mathrm{Sel}_\lambda A$ itself that is the intersection of maximal isotropic subgroups, but its quotient by $Ш^1(k, A[\lambda])$, and the latter group is sometimes nonzero, as we explain in Section 3. Moreover, for certain families, such as the family of all genus 2 curves, there may be "causal" subgroups of $\mathrm{Sel}_\lambda A$, which increase its expected size by a constant factor. Taking these into account suggests the following:

Conjecture 1.7. *Fix a global field k of characteristic not 2, and fix a positive integer g. Let $f \in k[x]$ range over separable polynomials of degree $2g+1$ (with coefficients of height bounded by B, with $B \to \infty$). Let C be the smooth projective model of $y^2 = f(x)$. Construct the Jacobian $A := \mathrm{Jac}\, C$. Then the analogues of Conjectures* 1.1, 1.2, *and* 1.4 *hold for $\mathrm{Sel}_p A$ and $\mathrm{Sel}_n A$, with the same distributions. They hold also with $2g+1$ replaced by $2g+2$* if n is odd.

Conjecture 1.8. *Fix a global field k of characteristic not* 2, *and fix an* even *positive integer g. Let $f \in k[x]$ range over polynomials of degree $2g+2$ (with coefficients of height bounded by B, with $B \to \infty$). Let C be the smooth projective model of $y^2 = f(x)$, and let $A = \mathrm{Jac}\, C$.*

(a) *If X_{Sel_2} is the $\mathbb{Z}_{\geq 0}$-valued random variable predicted by Conjecture* 1.1(a) *to model $\dim_{\mathbb{F}_2} \mathrm{Sel}_2 E$, then the analogous random variable for $\mathrm{Sel}_2 A$ is $X_{\mathrm{Sel}_2} + 1$.*

(b) *The average of $\#\mathrm{Sel}_2 A$ is* 6 *(instead of* 3*).*

(c) *For $m \in \mathbb{Z}_{\geq 0}$, the average of $(\#\mathrm{Sel}_2 A)^m$ is $2^m \prod_{i=1}^{m}(2^i+1)$.*

Example 4.20 will explain the rationale for the +1 in Conjecture 1.8(a) and will explain why we do not venture to make an analogous conjecture for odd g.

Remark 1.9. Although we have formulated conjectures for the family of all curves of a specified type, our model makes sense also for more limited families (e.g., a family of quadratic twists). One should take into account systematic contributions to the Selmer group, however, as was necessary in Conjecture 1.8.

2. Random maximal isotropic subspaces

2.1. **Quadratic modules.** See [Sch85, 1.§6 and 5.§1] for the definitions of this section. Let V and T be abelian groups. Call a function $Q\colon V \to T$ a (T-valued)

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

quadratic form if Q is a quadratic map (i.e., the symmetric pairing $\langle\ ,\ \rangle\colon V\times V\to T$ sending (x,y) to $Q(x+y)-Q(x)-Q(y)$ is bilinear) and $Q(av)=a^2Q(v)$ for every $a\in\mathbb{Z}$ and $v\in V$. Then (V,Q) is called a quadratic module.

Remark 2.1. A quadratic map Q satisfying the identity $Q(-v)=Q(v)$ is a quadratic form. (Taking $x=y=0$ shows that $Q(0)=0$, and then $Q(av+(-v))-Q(av)-Q(-v)=a(Q(0)-Q(v)-Q(-v))$ computes $Q(av)$ for other $a\in\mathbb{Z}$ by induction.)

Lemma 2.2. *Let (V,Q) be a quadratic module. Suppose that $v\in V$ and $\ell\in\mathbb{Z}$ are such that $\ell v=0$. If ℓ is odd, then $\ell Q(v)=0$. If ℓ is even, then $2\ell Q(v)=0$.*

Proof. We have $\ell^2Q(v)=Q(\ell v)=0$, and $2\ell Q(v)=\ell\langle v,v\rangle=\langle\ell v,v\rangle=0$. □

Given a subgroup $W\subseteq V$, let $W^\perp:=\{v\in V:\langle v,w\rangle=0 \text{ for all } w\in W\}$. Call W a maximal isotropic subgroup of (V,Q) if $W^\perp=W$ and $Q|_W=0$. Let $\mathcal{I}_V$ be the set of maximal isotropic subgroups of (V,Q).

Remark 2.3. Say that W is maximal isotropic *for the pairing* $\langle\ ,\ \rangle$ if $W^\perp=W$. If $W=2W$ or $T[2]=0$, then $W^\perp=W$ implies $Q|_W=0$, but in general $Q|_W=0$ is a nonvacuous extra condition.

Call a quadratic module (V,Q) nondegenerate if Q is $\mathbb{R}/\mathbb{Z}$-valued and V is finite (we will relax this condition in Section 2.4) and the homomorphism $V\to V^*:=\mathrm{Hom}(V,\mathbb{R}/\mathbb{Z})$ defined by $v\mapsto(w\mapsto\langle v,w\rangle)$ is an isomorphism. Call (V,Q) weakly metabolic if it is nondegenerate and contains a maximal isotropic subgroup. (Metabolic entails the additional condition that the subgroup be a direct summand.)

Remark 2.4. Suppose that (V,Q) is a nondegenerate quadratic module, and X is an isotropic subgroup of (V,Q). Then

(a) The quotient $X^\perp/X$ is a nondegenerate quadratic module under the quadratic form Q_X induced by Q.
(b) If $W\in\mathcal{I}_V$, then $(W\cap X^\perp)+X\in\mathcal{I}_V$, and $((W\cap X^\perp)+X)/X\in\mathcal{I}_{X^\perp/X}$. Let $\pi^{V,X^\perp/X}(W)$ denote this last subgroup, which is the image of $W\cap X^\perp$ in $X^\perp/X$.

Remark 2.5. If (V,Q) is a nondegenerate quadratic module with $\#V<\infty$, the obstruction to V being weakly metabolic is measured by an abelian group $\mathrm{W}Q\simeq\bigoplus_p\mathrm{W}Q(p)$ called the Witt group of nondegenerate quadratic forms on finite abelian groups [Sch85, 5.§1]. The obstruction for (V,Q) equals the obstruction for $X^\perp/X$ for any isotropic subgroup X of (V,Q) (cf. [Sch85, Lemma 5.1.3]).

2.2. **Counting subspaces.**

Proposition 2.6. *Let (V,Q) be a $2n$-dimensional weakly metabolic quadratic space over $F:=\mathbb{F}_p$, with Q taking values in $\frac{1}{p}\mathbb{Z}/\mathbb{Z}\simeq F$.*

(a) *All fibers of $\pi^{V,X^\perp/X}\colon\mathcal{I}_V\to\mathcal{I}_{X^\perp/X}$ have size $\prod_{i=1}^{\dim X}(p^{n-i}+1)$.*
(b) *We have $\#\mathcal{I}_V=\prod_{j=0}^{n-1}(p^j+1)$.*
(c) *Let W be a fixed maximal isotropic subspace of V. Let X_n be the random variable $\dim(Z\cap W)$, where Z is chosen uniformly at random from $\mathcal{I}_V$. Then X_n is a sum of independent Bernoulli random variables $B_1,\dots,B_n$ where B_i is 1 with probability $1/(p^{i-1}+1)$ and 0 otherwise.*

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

(d) *For $0 \le d \le n$, let $a_{d,n} := \mathrm{Prob}(X_n = d)$, and let $a_d := \lim_{n\to\infty} a_{d,n}$. Then*

$$\sum_{d\ge 0} a_{d,n} z^d = \prod_{i=0}^{n-1} \frac{z+p^i}{1+p^i} = \prod_{i=0}^{n-1} \frac{1+p^{-i}z}{1+p^{-i}},$$

$$\sum_{d\ge 0} a_d z^d = \prod_{i=0}^{\infty} \frac{1+p^{-i}z}{1+p^{-i}}.$$

(e) *For $0 \le d \le n$, we have*

$$a_{d,n} = \prod_{j=0}^{n-1} (1+p^{-j})^{-1} \prod_{j=1}^{d} \frac{p}{p^j-1} \prod_{j=0}^{d-1} (1-p^{j-n}).$$

(f) *For $d \ge 0$, we have*

$$a_d = c \prod_{j=1}^{d} \frac{p}{p^j-1},$$

where

$$c := \prod_{j\ge 0} (1+p^{-j})^{-1} = \frac{1}{2} \prod_{i\ge 0} (1-p^{-(2i+1)}).$$

Proof.

(a) Choose a full flag in X; then $\pi^{V,X^\perp/X}$ factors into $\dim X$ maps of the same type, so we reduce to the case $\dim X = 1$. Write $X = Fv$ with $v \in V$. For $Z \in \mathcal{I}_V$, let $\overline{Z}$ be its image in $\mathcal{I}_{X^\perp/X}$. There is a bijection $\{Z \in \mathcal{I}_V : v \in Z\} \to \mathcal{I}_{X^\perp/X}$ defined by $Z \mapsto \overline{Z} = Z/X$.

Fix $\overline{W} \in \mathcal{I}_{X^\perp/X}$, and let $W \in \mathcal{I}_V$ be such that $\overline{W} = W/X$. We want to show that $\#\{Z \in \mathcal{I}_V : \overline{Z} = \overline{W}\} = p^{n-1} + 1$. This follows once we show that the map

$$\begin{aligned} \{Z \in \mathcal{I}_V : \overline{Z} = \overline{W}\} &\to \{\text{codimension 1 subspaces of } W\} \cup \{W\} \\ Z &\mapsto Z \cap W \end{aligned}$$

is a bijection. If $v \in Z$, then $\overline{Z} = \overline{W}$ implies that $Z = W$. If $v \notin Z$, then $\overline{Z} = \overline{W}$ implies that $Z \cap W$ has codimension 1 in W. Conversely, for a given W_1 of codimension 1 in W, the $Z \in \mathcal{I}_V$ containing W_1 are in bijection with the maximal isotropic subspaces of the weakly metabolic 2-dimensional space $W_1^\perp/W_1$, which is isomorphic to (F^2, xy), so there are two such Z: one of them is W, and the other satisfies $Z \cap W = W_1$ and $\overline{Z} = \overline{W}$. Thus we have the bijection.

(b) Apply (a) to a maximal isotropic X.

(c) If $n > 0$, fix a nonzero v in W, and define $\overline{Z}$ as in the proof of (a). Then

$$\dim(Z \cap W) = \dim(\overline{Z} \cap \overline{W}) + \delta_{v\in Z},$$

where $\delta_{v\in W}$ is 1 if $v \in Z$ and 0 otherwise. The term $\dim(\overline{Z} \cap \overline{W})$ has the distribution X_{n-1}. Conditioned on the value of $\overline{Z}$, the term $\delta_{v\in Z}$ is 1 with probability $1/(p^{n-1}+1)$ and 0 otherwise, since there are $p^{n-1}+1$ subspaces $Z \in \mathcal{I}_V$ with the given $\overline{Z}$, and only one of them (namely, the preimage of $\overline{Z}$ under $V \to V/Fv$) contains v. Thus X_n is the sum of X_{n-1} and the

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

independent Bernoulli random variable B_n, so we are done by induction on n.

(d) The generating function for X_n is the product of the generating functions for $B_1, \dots, B_n$; this gives the first identity. The second follows from the first.

(e) This follows from (d) and Cauchy's q-binomial theorem (which actually goes back to [Rot11] and is related to earlier formulas of Euler). Namely, set $t = 1/p$ in formula (18) of [Cau43], and divide by $\prod_{j=0}^{n-1}(1 + p^{-j})$.

(f) Take the limit of (e) as $n \to \infty$. The alternative formula for c follows from substituting

$$1 + p^{-j} = \frac{1 - p^{-2j}}{1 - p^{-j}}$$

for $j \neq 0$ and cancelling common factors. □

Remark 2.7. There is a variant for finite-dimensional vector spaces V over a finite field F of nonprime order. One can define the notion of weakly metabolic quadratic form $Q\colon V \to F$, and then prove Proposition 2.6 with q in place of p.

If we consider only even-dimensional nondegenerate quadratic spaces over F, then the obstruction analogous to that in Remark 2.5 takes values in a group of order 2. The obstruction is the discriminant in $F^\times/F^{\times 2}$ if $\operatorname{char} F \neq 2$, and the Arf invariant (see [Sch85, 9.§4]) if $\operatorname{char} F = 2$.

Remark 2.8. By Lemma 2.2, a quadratic form on a 2-torsion module will in general take values in the *4-torsion* of the image group. Thus we need an analogue of Proposition 2.6(c) for a $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$-valued quadratic form Q on a $2n$-dimensional $\mathbb{F}_2$-vector space V such that $Q(V) \not\subset \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, or equivalently such that $\langle x, x\rangle = 2Q(x)$ is not identically 0.

The map $x \mapsto \langle x, x\rangle$ is a linear functional $V \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{F}_2$ since

$$\langle x + y, x + y\rangle = \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle = \langle x, x\rangle + \langle y, y\rangle.$$

Hence there exists a nonzero $c \in V$ such that $\langle x, x\rangle = \langle x, c\rangle$ for all $x \in V$. This equation shows that for any maximal isotropic subspace W of V, we have $c \in W^\perp = W$. The map $W \mapsto W/\mathbb{F}_2 c$ defines a bijection between the set of maximal isotropic subspaces of V and the set of maximal isotropic subspaces of $(\mathbb{F}_2 c)^\perp/\mathbb{F}_2 c$, which is a $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued quadratic space. So the random variable $\dim(Z \cap W)$ for V is 1 plus the corresponding random variable for the $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued quadratic space of dimension $\dim V - 2$.

Definition 2.9. Given a prime p, let X_{Sel_p} be a $\mathbb{Z}_{\geq 0}$-valued random variable such that for any $d \in \mathbb{Z}_{\geq 0}$, the probability $\mathrm{Prob}(X_{\mathrm{Sel}_p} = d)$ equals the a_d in Proposition 2.6(d).

In the notation of Proposition 2.6(c), we can also write

$$X_{\mathrm{Sel}_p} = \lim_{n\to\infty} X_n = \sum_{n=1}^{\infty} B_n.$$

Remark 2.10. The distribution of X_{Sel_2} agrees with the distribution of $s(E)$ mentioned at the beginning of Section 1.1.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

2.3. **Some topology.** To interpret a_r as a probability and not only a limit of probabilities, we are led to consider infinite-dimensional quadratic spaces. The naïve dual of such a space V is too large to be isomorphic to V, so we consider spaces with a locally compact topology and use the Pontryagin dual. In order to define a probability measure on the set of maximal isotropic subspaces, we need additional countability constraints. This section proves the equivalence of several such countability constraints.

For a locally compact abelian group G, define the Pontryagin dual $G^* := \mathrm{Hom}_{\mathrm{conts}}(G, \mathbb{R}/\mathbb{Z})$. Recall that a topological space is σ-compact if it is expressible as a union of countably many compact subspaces, first-countable if each point has a countable basis of neighborhoods, second-countable if the topology admits a countable basis, and separable if it has a countable dense subset.

Proposition 2.11. *Let G be a locally compact abelian group. The following are equivalent:*

(a) *G^* is σ-compact.*
(b) *G is first-countable.*
(c) *G is metrizable.*

Moreover, G is second-countable if and only if G and G^* are both σ-compact.

Proof. After peeling off a direct factor $\mathbb{R}^n$ from G, we may assume that G contains a compact open subgroup K, by the Pontryagin–van Kampen structure theorem [vK35, Theorem 2]. Each of (a), (b), (c) holds for G if and only if it holds for K, and for K the three conditions are equivalent to second-countability by [Kak43, Theorem 2 and the bottom of page 366]. To prove the final statement, observe that G is second-countable if and only if K is second-countable and G/K is countable. By the above, K is second-countable if and only G^* is σ-compact; on the other hand, G/K is countable if and only if G is σ-compact. □

Corollary 2.12. *Let G be a locally compact abelian group such that $G \simeq G^*$. Then the following are equivalent:*

(a) *G is σ-compact.*
(b) *G is first-countable.*
(c) *G is metrizable.*
(d) *G is second-countable.*
(e) *G is separable.*

Proof. Proposition 2.11 formally implies the equivalence of (a), (b), (c), and (d). To obtain (d) $\implies$ (e), choose one point from each nonempty set in a countable basis. To prove (e) $\implies$ (a), reduce to the case that G contains a compact open subgroup K; then separability implies that G/K is finite, so G is σ-compact. □

2.4. **Quadratic forms on locally compact abelian groups.**

Definition 2.13. A locally compact quadratic module (V, Q) is a locally compact abelian group V equipped with a continuous quadratic form $Q\colon V \to \mathbb{R}/\mathbb{Z}$. (This notion was introduced in [Wei64, p. 145], where Q was called a "caractère du second degré"; for him, the codomain of Q was the group of complex numbers of absolute value 1, because he was interested in the Fourier transforms of such Q.)

The definitions of maximal isotropic and nondegenerate extend to this setting.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Definition 2.14. Call a nondegenerate locally compact quadratic module (V, Q) weakly metabolic if it contains a *compact open* maximal isotropic subgroup W; we then say also that (V, Q, W) is weakly metabolic.

Remark 2.15. In Definition 2.14, it would perhaps be more natural to require the subgroup W to be only closed, not necessarily compact and open. Here we explain that the two definitions are equivalent when V contains a compact open subgroup, which is not a strong hypothesis, since by the Pontryagin–van Kampen structure theorem, if V is a locally compact abelian group, then $V \simeq \mathbb{R}^n \oplus V'$ as topological groups, where V' contains a compact open subgroup.

If (V, Q) is a nondegenerate locally compact quadratic module containing a compact open subgroup K, then $X := K \cap K^\perp$ is a compact open subgroup that is isotropic for the pairing. Then Q restricts to a continuous *linear* map $X \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and its kernel Y is a compact open subgroup that is isotropic for Q. Next, if W is *any* closed maximal isotropic subgroup of (V, Q), then $(W \cap Y^\perp) + Y$ is a compact open maximal isotropic subgroup of (V, Q) (cf. Remark 2.4(b)).

Remark 2.16. If (V, Q) is a nondegenerate locally compact quadratic module containing a compact open isotropic subgroup X, then the obstruction to (V, Q) containing a maximal isotropic closed subgroup is the same as that for $X^\perp/X$, so the obstruction is measured by an element of $\mathrm{W}Q$ that is independent of X (cf. Remark 2.5).

Example 2.17. If W is a locally compact abelian group, then $V := W \times W^*$ may be equipped with the quadratic form $Q((w, f)) := f(w)$. If W contains a compact open subgroup Y, then its annihilator in W^* is a compact open subgroup Y' of W^*, and $X := Y \times Y'$ is a compact open subgroup of V, so Remark 2.15 shows that (V, Q) is weakly metabolic.

Example 2.18 (cf. [Bra48, Théorème 1])**.** Suppose that (V_i, Q_i, W_i) for $i \in I$ are weakly metabolic. Define the restricted direct product

$$V := \prod_{i \in I}{}' (V_i, W_i) := \left\{ (v_i)_{i \in I} \in \prod_{i \in I} V_i : v_i \in W_i \text{ for all but finitely many } i \right\}.$$

Let $W := \prod_{i \in I} W_i$. As usual, equip V with the topology for which W is open and has the product topology. For $v := (v_i) \in V$, define $Q(v) = \sum_{i \in I} Q_i(v_i)$, which makes sense since $Q_i(v_i) = 0$ for all but finitely many i. Then (V, Q, W) is another weakly metabolic locally compact quadratic module.

Moreover, if I is countable and each V_i is second-countable, then V is second-countable too. (*Proof:* Use Corollary 2.12 to replace second-countable by σ-compact. If each V_i is σ-compact, then each V_i/W_i is countable, so $V/W \simeq \bigoplus_{i \in I} V_i/W_i$ is countable, so V is σ-compact.)

Let (V, Q) be a locally compact quadratic module. Let $\mathcal{I}_V$ be the set of maximal isotropic closed subgroups of (V, Q). Let $\mathcal{X}_V$ be the poset of compact open isotropic subgroups of (V, Q), ordered by (reverse) inclusion.

Theorem 2.19. *Let (V, Q, W) be a second-countable weakly metabolic locally compact quadratic module.*

(a) *The set $\mathcal{X}_V$ is a countable directed poset.*

(b) *The finite sets $\mathcal{I}_{X^\perp/X}$ for $X \in \mathcal{X}_V$ with the maps $\pi^{X_1^\perp/X_1, X_2^\perp/X_2}$ for $X_1 \subseteq X_2$ (cf. Remark* 2.4(b)*) form an inverse system.*

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

(c) *If* $\bigcap_{X \in \mathcal{X}_V} X = 0$, *then the collection of maps* $\pi^{V, X^\perp/X}$ *induces a bijection*

$$\mathcal{I}_V \to \varprojlim_{X \in \mathcal{X}_V} \mathcal{I}_{X^\perp/X}.$$

Equip $\mathcal{I}_V$ *with the inverse limit topology.*

(d) *In the remaining parts of this theorem, assume that* p *is a prime such that* $pV = 0$. *Then there exists a unique probability measure* μ *on the Borel* σ*-algebra of* $\mathcal{I}_V$ *such that for every compact open isotropic subgroup* X *of* (V, Q), *the push-forward* $\pi_*^{V, X^\perp/X}\mu$ *is the uniform probability measure on the finite set* $\mathcal{I}_{X^\perp/X}$.

(e) *The measure* μ *is invariant under the orthogonal group* $\mathrm{Aut}(V, Q)$.

(f) *If* Z *is distributed according to* μ, *then*

$$\mathrm{Prob}(Z \text{ is discrete}) = 1$$

and

$$\mathrm{Prob}(Z \cap W \text{ is finite}) = 1.$$

If moreover $\dim_{\mathbb{F}_p} V$ *is infinite, then the distribution of* $\dim(Z \cap W)$ *is given by* X_{Sel_p} *(see Definition* 2.9*).*

Proof.

(a) The intersection of two compact open isotropic subgroups of V is another one, so $\mathcal{X}_V$ is a directed poset. To prove that $\mathcal{X}_V$ is countable, first consider the bijection

$$\begin{aligned} \{\text{compact open subgroups of } W\} &\to \{\text{finite subgroups of } V/W\} \\ X &\mapsto X^\perp/W. \end{aligned} \tag{1}$$

Since V/W is a countable discrete group, both sets above are countable. The map

$$\begin{aligned} \mathcal{X}_V &\to \{\text{compact open subgroups of } W\} \\ X &\mapsto X \cap W \end{aligned}$$

has finite fibers, since the $X \in \mathcal{X}_V$ containing a given compact open subgroup Y of W are in bijection with the isotropic subgroups of the finite group $Y^\perp/Y$. Thus $\mathcal{X}_V$ is countable.

(b) Given $X_1 \subseteq X_2 \subseteq X_3$ the maps $\pi^{X_i^\perp/X_i, X_j^\perp/X_j}$ for $i < j$ behave as expected under composition.

(c) The same computation proving (b) shows that the map is well-defined. If $X \in \mathcal{X}_V$, then $X^\perp$ is another compact open subgroup of V since it contains X as a finite-index open subgroup. The group $(X^\perp)^* \simeq V/X$ is a discrete $\mathbb{F}_p$-vector space, so it equals the direct limit of its finite-dimensional subspaces. Taking duals shows that $X^\perp$ is the inverse limit of its finite quotients, i.e., of the groups $X^\perp/Y$, where Y ranges over open subgroups of $X^\perp$. Moreover, every open subgroup of $X^\perp$ contains an open subgroup of X (just intersect with X), so it suffices to take the latter.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Now the inverse map $(Z_X) \mapsto Z$ is constructed as follows: given $(Z_X) \in \varprojlim_{X \in \mathcal{X}_V} \mathcal{I}_{X^\perp/X}$, let

$$\widetilde{Z}_X := \varprojlim_{\substack{Y \in \mathcal{X}_V \\ Y \subseteq X}} \left(Z_Y \cap \frac{X^\perp}{Y} \right) \subseteq \varprojlim_{\substack{Y \in \mathcal{X}_V \\ Y \subseteq X}} \frac{X^\perp}{Y} = X^\perp,$$
$$Z := \bigcup_{X \in \mathcal{X}_V} \widetilde{Z}_X.$$

The maps in the inverse system defining $\widetilde{Z}$ are surjections, so the image of $\widetilde{Z}_X$ in $X^\perp/X$ equals Z_X. If $X, X' \in \mathcal{X}_V$ and $X' \subseteq X$, then $\widetilde{Z}_X = \widetilde{Z}_{X'} \cap X^\perp$, so $Z \cap X^\perp = \widetilde{Z}_X$. Since each Z_Y is isotropic in $Y^\perp/Y$, the group $\widetilde{Z}_X$ is isotropic, so Z is isotropic. If $z \in Z^\perp$, then we have $z \in X^\perp$ for some X, and then for any $Y \subseteq X$, the element $z \bmod Y \in Y^\perp/Y$ is perpendicular to $\pi^{V,Y^\perp/Y}(Z) = Z_Y$, but $Z_Y^\perp = Z_Y$, so $z \bmod Y \in Z_Y$, and also $z \bmod Y \in X^\perp/Y$; this holds for all $Y \subseteq X$, so $z \in Z$. Thus $Z^\perp = Z$; i.e., $Z \in \mathcal{I}_V$.

Now we show that the two constructions are inverse to each other. If we start with (Z_X), then the Z produced by the inverse map satisfies $\pi^{V,X^\perp/X}(Z) = Z_X$. Conversely, if we start with Z, and define $Z_X := \pi^{V,X^\perp/X}(Z)$, then the inverse map applied to (Z_X) produces Z' such that $Z \cap X^\perp \subseteq Z'$ for all X, so $Z \subseteq Z'$, but Z and Z' are both maximal isotropic, so $Z = Z'$.

(d) Since V/W is a discrete $\mathbb{F}_p$-vector space of dimension at most $\aleph_0$, we may choose a cofinal increasing sequence of finite-dimensional subspaces of V/W, and this corresponds under (1) to a cofinal decreasing sequence $Y_1, Y_2, \ldots$ of compact open subgroups of W whose intersection is 0. Thus (c) applies. Each map in the inverse system has fibers of constant size, by Proposition 2.6(a) so the uniform measures on these finite sets are compatible. By [Bou04, III.§4.5, Proposition 8(iv)], the inverse limit measure exists.

(e) The construction is functorial with respect to isomorphisms $(V, Q) \to (V', Q')$.

(f) Since $\sum_{r=0}^\infty a_r = 1$, it suffices to prove the last statement, that

$$\mathrm{Prob}(\dim(Z \cap W) = r) = a_r.$$

Let Y_i be as in the proof of (d). Then $\dim(Z \cap W)$ is the limit of the increasing sequence of nonnegative integers $\dim(\pi^{V,Y_i^\perp/Y_i}(Z) \cap \pi^{V,Y_i^\perp/Y_i}(W))$. By Proposition 2.6(c) and its proof, the difference of consecutive integers in this sequence is a sum of independent Bernoulli random variables. Since $\sum_{j \geq 1} \mathrm{Prob}(B_j = 1)$ converges, the Borel-Cantelli lemma implies that

$$\mathrm{Prob}\left(\dim(Z \cap W) \neq \dim(\pi^{V,Y_i^\perp/Y_i}(Z) \cap \pi^{V,Y_i^\perp/Y_i}(W)) \right) \to 0$$

as $i \to \infty$. In particular, $\mathrm{Prob}\left(\dim(Z \cap W) = \infty\right)$ is 0. On the other hand, $\dim Y_i^\perp/Y_i \to \infty$ as $i \to \infty$, so

$$\mathrm{Prob}\left(\dim(Z \cap W) = d\right) = \lim_{n \to \infty} a_{d,n} = a_d = \mathrm{Prob}\left(X_{\mathrm{Sel}_p} = d\right). \qquad \square$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Remark 2.20. There is only one infinite-dimensional second-countable weakly metabolic locally compact quadratic $\mathbb{F}_p$-vector space (V, Q), up to isomorphism. Inside V we are given a compact open maximal isotropic subspace W, and Theorem 2.19(f) implies the existence of a discrete maximal isotropic closed subspace Z with $Z \cap W = 0$. Since V is infinite and second-countable, $\dim_{\mathbb{F}_p} Z = \aleph_0$, so the isomorphism type of Z as locally compact abelian group is determined. The pairing $Z \times W \to \mathbb{R}/\mathbb{Z}$ defined by $(z, w) \mapsto Q(z + w)$ puts Z and W in Pontryagin duality. Now the summing map $Z \times W \to V$ is an isomorphism under which Q corresponds to the standard quadratic form on $Z \times Z^*$ defined in Example 2.17.

Remark 2.21. Suppose that V is as in Theorem 2.19(f) and that $Z \in \mathcal{I}_V$ is chosen at random. The probability that Z contains a given nonzero vector v of V then equals 0, because for any compact open isotropic subgroup $X \leq V$ small enough that $v \in X^\perp - X$, if $\dim X^\perp/X = 2n$, then the probability that $\pi^{V, X^\perp/X}(Z)$ contains the nonzero element $\pi^{V, X^\perp/X}(v)$ is $1/(p^n + 1)$, which tends to 0 as X shrinks. Now, if we fix a *discrete* $Z_0 \in \mathcal{I}_V$ and choose $Z \in \mathcal{I}_V$ at random, then $\dim(Z \cap Z_0) = 0$ with probability 1 by the previous sentence applied to each nonzero vector of the countable set Z_0.

2.5. **Moments.** Given a random variable X, let $\mathbb{E}(X)$ be its expectation. So if $m \in \mathbb{Z}_{\geq 0}$, then $\mathbb{E}(X^m)$ is its m^{th} moment.

Proposition 2.22. *Fix a prime p and fix $m \in \mathbb{Z}_{\geq 0}$. Let X_n be as in Proposition* 2.6(c)*, and let X_{Sel_p} be as in Definition* 2.9*. Then*

(a) *We have*

$$\mathbb{E}\left(\left(p^{X_n}\right)^m\right) = \prod_{i=1}^{m} \frac{p^i + 1}{1 + p^{-(n-i)}},$$

$$\mathbb{E}\left(\left(p^{X_{\mathrm{Sel}_p}}\right)^m\right) = \prod_{i=1}^{m} (p^i + 1).$$

In particular, $\mathbb{E}(p^{X_{\mathrm{Sel}_p}}) = p + 1$.

(b) *We have* $\mathrm{Prob}(X_n \text{ is even}) = 1/2$ *for each* $n > 0$ *and* $\mathrm{Prob}(X_{\mathrm{Sel}_p} \text{ is even}) = 1/2$.

(c) *If we condition on the event that X_{Sel_p} has a prescribed parity, the moments in* (a) *remain the same. The same holds for the m^{th} moment of p^{X_n} if $m < n$.*

Proof.

(a) Substitute $z = p^m$ in Proposition 2.6(d). The products telescope.

(b) Substitute $z = -1$ in Proposition 2.6(d).

(c) Substitute $z = -p^m$ in Proposition 2.6(d).

□

3. Shafarevich-Tate groups of finite group schemes

3.1. **Definitions.** For each field k, choose an algebraic closure $\overline{k}$ and a separable closure $k_s \subseteq \overline{k}$, and let $G_k := \mathrm{Gal}(k_s/k)$. A local field is a nondiscrete locally compact topological field; each such field is a finite extension of one of $\mathbb{R}$, $\mathbb{Q}_p$, or $\mathbb{F}_p((t))$ for some prime p. A global field is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$ for some prime p.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

In the rest of Section 3, k denotes a global field. Let Ω be the set of nontrivial places of k. For $v \in \Omega$, let k_v be the completion of k at v, so k_v is a local field; if v is nonarchimedean, let $\mathcal{O}_v$ be the valuation ring in k_v.

For a sheaf of abelian groups M on the big fppf site of $\operatorname{Spec} k$, define

$$Ш^1(k, M) := \ker\left(\mathrm{H}^1(k, M) \to \prod_{v\in\Omega} \mathrm{H}^1(k_v, M)\right). \tag{2}$$

Remark 3.1. If M is represented by a smooth finite-type group scheme over k, such as the kernel of an isogeny of degree not divisible by $\operatorname{char} k$, then we may interpret the cohomology groups as Galois cohomology groups: $\mathrm{H}^1(k, M) = \mathrm{H}^1(G_k, M(k_s))$ and so on.

Definition 3.2. Let C be a smooth projective curve of genus g over k. Let $A = \operatorname{Jac} C$. The degree $g-1$ component of the Picard scheme of C contains a closed subscheme $\mathcal{T}$ parametrizing line sheaves on C whose square is isomorphic to the canonical sheaf of C. This $\mathcal{T}$ is a torsor under $A[2]$, called the theta characteristic torsor. Let $c_{\mathcal{T}} \in \mathrm{H}^1(k, A[2])$ be its class.

3.2. **Vanishing criteria.** The following criteria for vanishing of $Ш^1(k, M)$ will be especially relevant for Theorem 4.14(b).

Proposition 3.3. *Suppose that M is a finite étale group scheme over k, so we identify M with the finite G_k-module $M(k_s)$.*

(a) *If $M = \mathbb{Z}/n\mathbb{Z}$, then $Ш^1(k, M) = 0$.*
(b) *If M is a direct summand of a direct sum of permutation $\mathbb{Z}/n\mathbb{Z}$-modules arising from finite separable extensions of k, then $Ш^1(k, M) = 0$.*
(c) *Let G be the image of G_k in $\operatorname{Aut} M(k_s)$. Identify $\mathrm{H}^1(G, M)$ with its image under the injection $\mathrm{H}^1(G, M) \hookrightarrow \mathrm{H}^1(k, M)$. Then*

$$Ш^1(k, M) \subseteq \bigcap_{\text{cyclic } H \le G} \ker\left(\mathrm{H}^1(G, M) \to \mathrm{H}^1(H, M)\right).$$

(d) *If p is a prime such that $pM = 0$ and the Sylow p-subgroups of $\operatorname{Aut} M(k_s)$ are cyclic, then $Ш^1(k, M) = 0$.*
(e) *If E is an elliptic curve, and $p \neq \operatorname{char} k$, then $Ш^1(k, E[p]) = 0$.*
(f) *If $\operatorname{char} k \neq 2$, and A is the Jacobian of the smooth projective model of $y^2 = f(x)$, where $f \in k[x]$ is separable of odd degree, then $Ш^1(k, A[2]) = 0$.*

Proof.

(a) See [Mil06, Example I.4.11(i)].
(b) Combine (a) with Shapiro's lemma [AW67, §4, Proposition 2] to obtain the result for a finite permutation module $(\mathbb{Z}/n\mathbb{Z})[G_k/G_L]$ for a finite separable extension L of k. The result for direct summands of direct sums of these follows.
(c) This is a consequence of the Chebotarev density theorem; see [BPS10].
(d) Let G be the image of $G_k \to \operatorname{Aut} M(k_s)$. Then any Sylow p-subgroup P of G is cyclic. But the restriction $\mathrm{H}^1(G, M) \to \mathrm{H}^1(P, M)$ is injective [AW67, §6, Corollary 3], so (c) shows that $Ш^1(k, M) = 0$.
(e) Any Sylow-p-subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ is conjugate to the group of upper triangular unipotent matrices, which is cyclic. Apply (d).
(f) The group $A[2]$ is a direct summand of the permutation $\mathbb{Z}/2\mathbb{Z}$-module on the set of zeros of f. Apply (b). □

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

3.3. **Jacobians of hyperelliptic curves.** See [PR11, Example 3.12(b)] for a 2-dimensional Jacobian A with $Ш^1(\mathbb{Q}, A[2]) \neq 0$. Such examples are rare: a special case of Proposition 3.4 below shows that asymptotically 100% of 2-dimensional Jacobians A over $\mathbb{Q}$ have $Ш^1(\mathbb{Q}, A[2]) = 0$.

Proposition 3.4. *Fix $g \geq 1$ and a prime p. For random $f(x) \in \mathbb{Z}[x]$ of degree $2g+1$ with coefficients in $[-B, B]$, if A is the Jacobian of the smooth projective model C of $y^2 = f(x)$, the probability that $Ш^1(\mathbb{Q}, A[p]) = 0$ tends to 1 as $B \to \infty$. The same holds if $2g+1$ is replaced by $2g+2$ (the general case for a genus g hyperelliptic curve).*

Proof. By Proposition 3.3(e) we may assume $g \geq 2$. We may assume that f is separable.

First consider the case $p \neq 2$. Generically, the image of $G_{\mathbb{Q}} \to \operatorname{Aut} A[p]$ is as large as possible given the existence of the Weil pairing e_p, i.e., isomorphic to $\mathrm{GSp}_{2g}(\mathbb{F}_p)$. By the Hilbert irreducibility theorem, the same holds for asymptotically 100% of the polynomials f. By Proposition 3.3(c), $Ш^1(\mathbb{Q}, A[p])$ is contained in the subgroup $\mathrm{H}^1(\mathrm{GSp}_{2g}(\mathbb{F}_p), A[p])$ of $\mathrm{H}^1(\mathbb{Q}, A[p])$, and that subgroup is 0 because the central element $-I \in \mathrm{GSp}_{2g}(\mathbb{F}_p)$ has no fixed vector (cf. [Fou64, Lemma 14.4] and [Pol71, Theorem 2.3]).

Now suppose that $p = 2$. In the degree $2g+1$ case, we are done by Proposition 3.3(f). So assume that $\deg f = 2g+2$. Let Δ be the set of zeros of f in $\overline{\mathbb{Q}}$, so $\#\Delta = 2g+2$. For $m \in \mathbb{Z}/2\mathbb{Z}$, let $\mathcal{W}_m$ be the quotient of the sum-m part of the permutation module $\mathbb{F}_2^{\Delta} \simeq \mathbb{F}_2^{2g+2}$ by the diagonal addition action of $\mathbb{F}_2$. Then the $G_{\mathbb{Q}}$-module $A[2]$ may be identified with $\mathcal{W}_0$, and $\mathcal{W}_m$ is a torsor under $\mathcal{W}_0$.

Again by the Hilbert irreducibility theorem, we may assume that the group $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \simeq \mathrm{Gal}(f)$ is as large as possible, i.e., equal to S_{2g+2}. Then $Ш^1(\mathbb{Q}, A[2]) \subseteq \mathrm{H}^1(S_{2g+2}, \mathcal{W}_0) \subset \mathrm{H}^1(\mathbb{Q}, A[2])$. The group $\mathrm{H}^1(S_{2g+2}, \mathcal{W}_0)$ is of order 2, generated by the class $c_{\mathcal{W}_1}$ of $\mathcal{W}_1$ [Pol71, Theorem 5.2]. Computations as in [PS99, §9.2] show that for each prime ℓ, the probability that $f(x)$ factors over $\mathbb{Z}_\ell$ into irreducible polynomials of degree $2g$ and 2 defining unramified and ramified extensions of $\mathbb{Q}_\ell$, respectively, is of order $1/\ell$ (not smaller) as $\ell \to \infty$, and in this case no point in $\mathcal{W}_1$ is $G_{\mathbb{Q}_\ell}$-invariant, so $c_{\mathcal{W}_1}$ has nonzero image in $\mathrm{H}^1(\mathbb{Q}_\ell, A[2])$. Since the conditions at finitely many ℓ are asymptotically independent as $B \to \infty$, and since $\sum 1/\ell$ diverges, there will exist such a prime ℓ for almost all f, and in this case, $c_{\mathcal{W}_1} \notin Ш^1(\mathbb{Q}, A[2])$, so $Ш^1(\mathbb{Q}, A[2]) = 0$. □

Remark 3.5. Proposition 3.4 can easily be extended to an arbitrary global field of characteristic not equal to 2 or p.

Remark 3.6. Let C be the smooth projective model of $y^2 = f(x)$, where $f(x) \in k[x]$ is separable of degree $2g+2$. As torsors under $A[2] \simeq \mathcal{W}_0$, we have $\mathcal{T} \simeq \mathcal{W}_{g-1}$ (cf. [Mum71, p. 191]).

3.4. **Jacobians with generic 2-torsion.** Suppose that C is a curve of genus $g \geq 2$ over a global field k of characteristic not 2 such that the image G of $G_k \to \operatorname{Aut} A[2]$ is as large as possible, i.e., $\mathrm{Sp}_{2g}(\mathbb{F}_2)$. (This forces C to be nonhyperelliptic if $g \geq 3$.) By [Pol71, Theorems 4.1 and 4.8], the group $\mathrm{H}^1(G, A[2]) \subseteq \mathrm{H}^1(G_k, A[2])$ is of order 2, generated by $c_{\mathcal{T}}$. So Proposition 3.3(c) shows that $Ш^1(k, A[2])$ is of order 2 or 1, according to whether the nonzero class $c_{\mathcal{T}}$ lies in $Ш^1(k, A[2])$ or not.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

4. Selmer groups as intersections of two maximal isotropic subgroups

4.1. **Quadratic form arising from the Heisenberg group.** Let A be an abelian variety over a field k. Let $\widehat{A}$ be its dual abelian variety. Let $\lambda\colon A \to \widehat{A}$ be an isogeny equal to its dual. The exact sequence

$$0 \to A[\lambda] \to A \xrightarrow{\lambda} \widehat{A} \to 0$$

gives rise to the "descent sequence"

$$0 \to \frac{\widehat{A}(k)}{\lambda A(k)} \xrightarrow{\delta} \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^1(A)[\lambda] \to 0, \tag{3}$$

where $\mathrm{H}^1(A)[\lambda]$ is the kernel of the homomorphism $\mathrm{H}^1(\lambda)\colon \mathrm{H}^1(A) \to \mathrm{H}^1(\widehat{A})$.

Since λ is self-dual, we obtain an (alternating) Weil pairing

$$e_\lambda\colon A[\lambda] \times A[\lambda] \to \mathbb{G}_m$$

identifying $A[\lambda]$ with its own Cartier dual (cf. [Mum70, p. 143, Theorem 1]). Composing the cup product with $\mathrm{H}^1(e_\lambda)$ gives a symmetric pairing

$$\underset{e_\lambda}{\cup}\colon \mathrm{H}^1(A[\lambda]) \times \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$$

and its values are killed by $\deg\lambda$. It is well known (especially when λ is separable) that the image of the natural map $\widehat{A}(k)/\lambda A(k) \to \mathrm{H}^1(A[\lambda])$ is isotropic with respect to $\underset{e_\lambda}{\cup}$.

In the rest of Section 4, we will assume that we are in one of the following cases:

(I) The self-dual isogeny λ has odd degree.

(II) The self-dual isogeny λ is of the form $\phi_{\mathscr{L}}$ for some symmetric line sheaf $\mathscr{L}$ on A. (Symmetric means $[-1]^*\mathscr{L} \simeq \mathscr{L}$. For the definition of $\phi_{\mathscr{L}}$, see [Mum70, p. 60 and Corollary 5 on p. 131].)

In each of these cases, we will construct a natural quadratic form q whose associated bilinear pairing is $\underset{e_\lambda}{\cup}$. Moreover, in each case, we will show that the image of $\widehat{A}(k)/\lambda A(k) \to \mathrm{H}^1(A[\lambda])$ is isotropic with respect to q.

Remark 4.1. We need Case II in addition to the easier Case I since, for example, we want to study $\mathrm{Sel}_p E$ even when $p = 2$.

Remark 4.2. For any symmetric line sheaf $\mathscr{L}$, the homomorphism $\phi_{\mathscr{L}}$ is self-dual [Pol03, p. 116]. If moreover $\mathscr{L}$ is ample, then $\phi_{\mathscr{L}}$ is an isogeny (see [Mum70, p. 124 and Corollary 5 on p. 131]).

Remark 4.3. If A is an elliptic curve and λ is multiplication-by-n for some positive integer n, then Case II applies. Namely, let P be the origin of A, and let $\mathscr{L}$ be the symmetric line sheaf $\mathscr{O}(nP)$; then $\phi_{\mathscr{L}} = \lambda$.

Remark 4.4. The obstruction to expressing a self-dual isogeny λ as $\phi_{\mathscr{L}}$ is given by an element $c_\lambda \in \mathrm{H}^1(\widehat{A}[2])$. For example, if λ is an odd multiple of the principal polarization on a Jacobian of a curve with no rational theta characteristic, then $c_\lambda \neq 0$. See [PR11, §3] for these facts, and for many criteria for the vanishing of c_λ.

Remark 4.5. If $\lambda = 2\mu$ for some self-dual isogeny $\mu\colon A \to \widehat{A}$, then λ is of the form $\phi_{\mathscr{L}}$, since $c_\lambda = 2c_\mu = 0$. Explicitly, take $\mathscr{L} := (1,\mu)^*\mathscr{P}$, where $\mathscr{P}$ is the Poincaré line sheaf on $A \times \widehat{A}$ (see [Mum70, §20, proof of Theorem 2]).

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

We now return to the construction of the quadratic form.

Case I. $\deg \lambda$ is odd.

Then $q(x) := -\frac{1}{2}\left(x \underset{e_\lambda}{\cup} x\right)$ is a quadratic form whose associated bilinear pairing is $-\underset{e_\lambda}{\cup}$. (The sign here is chosen to make the conclusion of Corollary 4.7 hold for q.) Since the image of $\widehat{A}(k)/\lambda A(k) \to \mathrm{H}^1(A[\lambda])$ is isotropic with respect to $\underset{e_\lambda}{\cup}$, it is isotropic with respect to q too.

Case II. There is a symmetric line sheaf $\mathscr{L}$ on A such that $\lambda = \phi_{\mathscr{L}}$. (This hypothesis remains in force until the end of Section 4.1.)

When λ is separable, Zarhin [Zar74, §2] constructed a quadratic form $q\colon \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ whose associated bilinear pairing was $\underset{e_\lambda}{\cup}$; for elliptic curves, C. O'Neil showed that the image of $\widehat{A}(k)/\lambda A(k) \to \mathrm{H}^1(A[\lambda])$ is isotropic for q (this is implicit in [O'N02, Proposition 2.3]). Because we wish to include the inseparable case, and because we wish to prove isotropy of the quadratic form for abelian varieties of arbitrary dimension, we will give a detailed construction and proof in the general case.

The pairs (x, ϕ) where $x \in A(k)$ and ϕ is an isomorphism from $\mathscr{L}$ to $\tau_x^*\mathscr{L}$ form a (usually nonabelian) group under the operation

$$(x, \phi)(x', \phi') = (x + x', (\tau_{x'}\phi)\phi').$$

The same can be done after base extension, so we get a group functor. Automorphisms of $\mathscr{L}$ induce the identity on this group functor, so it depends only on the class of $\mathscr{L}$ in $\operatorname{Pic} A$.

Proposition 4.6 (Mumford)**.**

(a) *This functor is representable by a finite-type group scheme $\mathcal{H}(\mathscr{L})$, called the* Heisenberg group *(or* theta group *or* Mumford group*).*

(b) *It fits in an exact sequence*

$$1 \to \mathbb{G}_m \to \mathcal{H}(\mathscr{L}) \to A[\lambda] \to 1, \tag{4}$$

where the two maps in the middle are given by $t \mapsto (0, \text{multiplication by } t)$ and (x, ϕ) to x. This exhibits $\mathcal{H}(\mathscr{L})$ as a central extension of finite-type group schemes.

(c) *The induced commutator pairing*

$$A[\lambda] \times A[\lambda] \to \mathbb{G}_m$$

is the Weil pairing e_λ.

Proof. See [Mum91, pp. 44–46]. □

Corollary 4.7. *The connecting homomorphism $q\colon \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ induced by* (4) *is a quadratic form whose associated bilinear pairing $\mathrm{H}^1(A[\lambda]) \times \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ sends (x, y) to $-x \underset{e_\lambda}{\cup} y$.*

Proof. Applying [PR11, Proposition 2.9] to (4) shows that q is a quadratic *map* giving rise to the bilinear pairing claimed. By Remark 2.1, it remains to prove the

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

identity $q(-v) = q(v)$. Functoriality of (4) with respect to the automorphism $[-1]$ of A gives a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}(\mathscr{L}) & \longrightarrow & A[\lambda] & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle -1} & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{H}([-1]^*\mathscr{L}) & \longrightarrow & A[\lambda] & \longrightarrow & 1. \end{array}$$

But $[-1]^*\mathscr{L} \simeq \mathscr{L}$, so both rows give rise to q. Functoriality of the connecting homomorphism gives $q(-v) = q(v)$ for any $v \in \mathrm{H}^1(A[\lambda])$. □

Remark 4.8. The proof of the next proposition involves a sheaf of sets on the big fppf site of $\operatorname{Spec} k$, but in the case $\operatorname{char} k \nmid \deg \lambda$, it is sufficient to think of it as a set with a continuous G_k-action.

Proposition 4.9. *Identify $\widehat{A}(k)/\lambda A(k)$ with its image W under δ in* (3)*. Then $q|_W = 0$.*

Proof. Let $\mathscr{P}$ be the Poincaré line sheaf on $A \times \widehat{A}$. For $y \in \widehat{A}(k)$, let $\mathscr{P}_y$ be the line sheaf on A obtained by restricting $\mathscr{P}$ to $A \times \{y\}$. For any $y_1, y_2 \in \widehat{A}(k)$, there is a canonical isomorphism $\iota_{y_1,y_2} \colon \mathscr{P}_{y_1} \otimes \mathscr{P}_{y_2} \to \mathscr{P}_{y_1+y_2}$, satisfying a cocycle condition [Pol03, §10.3].

The group $\mathcal{H}(\mathscr{L})(k)$ acts on the left on the set of triples (x, y, ϕ) where $x \in A(k)$, $y \in \widehat{A}(k)$, and $\phi \colon \mathscr{L} \otimes \mathscr{P}_y \to (\tau_x^*\mathscr{L})$ as follows:

$$(x, \phi)(x', y', \phi') = (x + x', y', (\tau_{x'}\phi)\phi').$$

The same holds after base extension, and we get an fppf-sheaf of sets $\mathcal{G}(\mathscr{L})$ on which $\mathcal{H}(\mathscr{L})$ acts freely. There is a morphism $\mathcal{G}(\mathscr{L}) \to \widehat{A}$ sending (x, y, ϕ) to y, and this identifies $\widehat{A}$ with the quotient sheaf $\mathcal{H}(\mathscr{L})\backslash\mathcal{G}(\mathscr{L})$. There is also a morphism $\mathcal{G}(\mathscr{L}) \to A$ sending (x, y, ϕ) to x, and the action of $\mathcal{H}(\mathscr{L})$ on $\mathcal{G}(\mathscr{L})$ is compatible with the action of its quotient $A[\lambda]$ on A. Thus we have the following compatible diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{H}(\mathscr{L}) & \dashrightarrow & \mathcal{G}(\mathscr{L}) & \longrightarrow & \widehat{A} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A[\lambda] & \longrightarrow & A & \xrightarrow{\lambda} & \widehat{A} & \longrightarrow & 0, \end{array}$$

where the first row indicates only that $\mathcal{H}(\mathscr{L})$ acts freely on $\mathcal{G}(\mathscr{L})$ with quotient being $\widehat{A}$. This is enough to give a commutative square of pointed sets

$$\begin{array}{ccc} \mathrm{H}^0(\widehat{A}) & \longrightarrow & \mathrm{H}^1(\mathcal{H}(\mathscr{L})) \\ \| & & \downarrow \\ \mathrm{H}^0(\widehat{A}) & \longrightarrow & \mathrm{H}^1(A[\lambda]), \end{array}$$

so $\mathrm{H}^0(\widehat{A}) \to \mathrm{H}^1(A[\lambda])$ factors through $\mathrm{H}^1(\mathcal{H}(\mathscr{L}))$. But the sequence $\mathrm{H}^1(\mathcal{H}(\mathscr{L})) \to \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ from (4) is exact, so the composition $\mathrm{H}^0(\widehat{A}) \to \mathrm{H}^1(A[\lambda]) \to \mathrm{H}^2(\mathbb{G}_m)$ is 0. □

Remark 4.10. Proposition 4.9 can be generalized to an abelian scheme over an arbitrary base scheme S. The proof is the same.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

4.2. **Local fields.** Let k_v be a local field. The group $\mathrm{H}^1(k_v, A[\lambda])$ has a topology making it locally compact, the group $\mathrm{H}^2(k_v, \mathbb{G}_m)$ may be identified with a subgroup of $\mathbb{Q}/\mathbb{Z}$ and given the discrete topology, and the quadratic form $q\colon \mathrm{H}^1(k_v, A[\lambda]) \to \mathrm{H}^2(k_v, \mathbb{G}_m)$ is continuous (cf. [Mil06, III.6.5]; the same arguments work even though (4) has a nonabelian group in the middle). The composition

$$\mathrm{H}^1(k_v, A[\lambda]) \xrightarrow{q} \mathrm{H}^2(k_v, \mathbb{G}_m) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

is a quadratic form q_v. By local duality [Mil06, I.2.3, I.2.13(a), III.6.10], q_v is nondegenerate. Moreover, $\mathrm{H}^1(k_v, A[\lambda])$ is finite if $\operatorname{char} k_v \nmid \deg \lambda$ [Mil06, I.2.3, I.2.13(a)], and σ-compact in general [Mil06, III.6.5(a)], so it is second-countable by Corollary 2.12.

Proposition 4.11. *Let k_v be a local field. In* (3) *for k_v, the group*

$$W \simeq \widehat{A}(k_v)/\lambda A(k_v)$$

is a compact open maximal isotropic subgroup of $(\mathrm{H}^1(k_v, A[\lambda]), q_v)$, which is therefore weakly metabolic.

Proof. By Proposition 4.9, q_v restricts to 0 on W, so it suffices to show that $W^\perp = W$. Let $A(k_v)_\bullet$ be $A(k_v)$ modulo its connected component (which is nonzero only if k_v is $\mathbb{R}$ or $\mathbb{C}$). Then W is the image of $\widehat{A}(k_v)_\bullet \to \mathrm{H}^1(k_v, A[\lambda])$, so $W^\perp$ is the kernel of the dual map, which by Tate local duality [Mil06, I.3.4, I.3.7, III.7.8] is $\mathrm{H}^1(k_v, A[\lambda]) \to \mathrm{H}^1(k_v, A)$. This kernel is W, by exactness of (3). □

Suppose that k_v is nonarchimedean. Let $\mathcal{O}_v$ be its valuation ring and let $\mathbb{F}_v$ be its residue field. Suppose that A has good reduction, i.e., that it extends to an abelian scheme (again denoted A) over $\mathcal{O}_v$. Then the fppf-cohomology group $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ is an open subgroup of $\mathrm{H}^1(k_v, A[\lambda])$.

Remark 4.12. If moreover $\operatorname{char} \mathbb{F}_v \nmid \deg \lambda$, then we may understand $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ in concrete terms as the kernel $\mathrm{H}^1(k_v, A[\lambda])_{\mathrm{unr}}$ of the restriction map

$$\mathrm{H}^1(k_v, A[\lambda]) \to \mathrm{H}^1(k_v^{\mathrm{unr}}, A[\lambda])$$

of Galois cohomology groups.

Proposition 4.13. *Suppose that k_v is nonarchimedean. Suppose that A extends to an abelian scheme over $\mathcal{O}_v$. Then the subgroups $W \simeq \widehat{A}(k_v)/\lambda A(k_v)$ and $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ in $\mathrm{H}^1(k_v, A[\lambda])$ are equal. In particular, $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ is a maximal isotropic subgroup.*

Proof. By [Mil80, III.3.11(a)] and [Lan56], respectively, $\mathrm{H}^1(\mathcal{O}_v, A) \simeq \mathrm{H}^1(\mathbb{F}_v, A) = 0$. The valuative criterion for properness [Har77, II.4.7] yields $A(\mathcal{O}_v) = A(k_v)$ and $\widehat{A}(\mathcal{O}_v) = \widehat{A}(k_v)$. So taking cohomology of (3) over $\mathcal{O}_v$ gives the result. □

4.3. **Global fields.** Let k be a global field. For any nonempty subset $\mathcal{S}$ of Ω containing the archimedean places, define the ring of $\mathcal{S}$-integers $\mathcal{O}_\mathcal{S} := \{x \in k : v(x) \geq 0 \text{ for all } v \notin \mathcal{S}\}$.

Let A be an abelian variety over k, Let $\lambda\colon A \to \widehat{A}$ be a self-dual isogeny as in Case I or II of Section 4.1. Choose a nonempty finite $\mathcal{S}$ containing all bad places, by which we mean that $\mathcal{S}$ contains all archimedean places and A extends to an abelian scheme A over $\mathcal{O}_\mathcal{S}$. In Example 2.18 take $I = \Omega$, $V_i = \mathrm{H}^1(k_v, A[\lambda])$, $Q_i = q_v$, and

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$W_i = \widehat{A}(k_v)/\lambda A(k_v)$, which is valid by Proposition 4.11. The resulting restricted direct product

$$V := \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, A[\lambda]), \frac{\widehat{A}(k_v)}{\lambda A(k_v)} \right)$$

equipped with the quadratic form

$$Q\colon \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, A[\lambda]), \frac{\widehat{A}(k_v)}{\lambda A(k_v)} \right) \to \mathbb{Q}/\mathbb{Z}$$
$$(\xi_v)_{v\in\Omega} \mapsto \sum_v q_v(\xi_v)$$

is a second-countable weakly metabolic locally compact quadratic module. Proposition 4.13, which applies for all but finitely many v, shows that

$$V = \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda]) \right).$$

(The subgroup $\mathrm{H}^1(\mathcal{O}_v, A[\lambda])$ is defined and equal to $\widehat{A}(k_v)/\lambda A(k_v)$ only for $v \notin \mathcal{S}$, but that is enough.)

As usual, define the Selmer group

$$\mathrm{Sel}_\lambda A := \ker \left(\mathrm{H}^1(k, A[\lambda]) \to \prod_{v\in\Omega} \mathrm{H}^1(k_v, A) \right).$$

Below will appear $Ш^1(k, A[\lambda])$, which is a subgroup of $\mathrm{Sel}_\lambda A$, and is not to be confused with the Shafarevich-Tate group $Ш(A) = Ш^1(k, A)$.

Theorem 4.14.

(a) *The images of the homomorphisms*

$$\begin{array}{ccc} & & \mathrm{H}^1(k, A[\lambda]) \\ & & \big\downarrow \\ \displaystyle\prod_{v\in\Omega} \frac{\widehat{A}(k_v)}{\lambda A(k_v)} & \longrightarrow & \displaystyle\prod_{v\in\Omega}{}' (\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda])) \end{array}$$

are maximal isotropic subgroups with respect to Q.

(b) *The vertical map induces an isomorphism from $\mathrm{Sel}_\lambda A/Ш^1(k, A[\lambda])$ to the intersection of these two images. (See Section 3 for information about $Ш^1(k, A[\lambda])$, which is often 0.)*

Proof.

(a) The subgroup $\prod_{v\in\Omega} \widehat{A}(k_v)/\lambda A(k_v)$ (or rather its image W under the horizontal injection) is maximal isotropic by construction.

The vertical homomorphism

$$\mathrm{H}^1(k, A[\lambda]) \to \prod_{v\in\Omega}{}' (\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda]))$$

is well-defined since each element of $\mathrm{H}^1(k, A[\lambda])$ belongs to the subgroup $\mathrm{H}^1(\mathcal{O}_\mathcal{T}, A[\lambda])$ for some finite $\mathcal{T} \subseteq \Omega$ containing $\mathcal{S}$, and $\mathcal{O}_\mathcal{T} \subseteq \mathcal{O}_v$ for all

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$v \notin \mathcal{T}$. Let W be the image. Suppose that $s \in \mathrm{H}^1(k, A[\lambda])$, and let $w \in W$ be its image. The construction of the quadratic form of Corollary 4.7 is functorial with respect to base extension, so $Q(w)$ can be computed by evaluating the global quadratic form

$$q\colon \mathrm{H}^1(k, A[\lambda]) \to \mathrm{H}^2(k, \mathbb{G}_m)$$

on s, and afterwards summing the local invariants. Exactness of

$$0 \to \mathrm{H}^2(k, \mathbb{G}_m) \to \bigoplus_{v\in\Omega} \mathrm{H}^2(k_v, \mathbb{G}_m) \xrightarrow{\sum \mathrm{inv}} \mathbb{Q}/\mathbb{Z} \to 0$$

in the middle (the reciprocity law for the Brauer group: see [GS06, Remark 6.5.6] for references) implies that the sum of the local invariants of our global class is 0. Thus $Q|_W = 0$.

It remains to show that W is its own annihilator. Since e_λ identifies $A[\lambda]$ with its own Cartier dual, the middle three terms of the 9-term Poitou-Tate exact sequence ([Mil06, I.4.10(c)] and [GA09, 4.11]) give the self-dual exact sequence

$$\mathrm{H}^1(k, A[\lambda]) \xrightarrow{\beta_1} \prod_{v\in\Omega}{}'(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda])) \xrightarrow{\gamma_1} \mathrm{H}^1(k, A[\lambda])^*,$$

where $*$ denotes Pontryagin dual. Since $W = \mathrm{im}(\beta_1)$ and the dual of β_1 is γ_1,

$$W^\perp = \ker(\gamma_1) = \mathrm{im}(\beta_1) = W.$$

(b) This follows from the exactness of (3) for $S = \operatorname{Spec} k_v$ for each $v \in \Omega$. □

Remark 4.15. There is a variant of Theorem 4.14 in which the infinite restricted direct product is taken over only a *subset* $\mathcal{S}$ of Ω containing all bad places and all places of residue characteristic dividing $\deg \lambda$. If $\mathcal{S}$ is finite, then the restricted direct product becomes a finite direct product. The same proof as before shows that the images of $\prod_{v\in\mathcal{S}} \widehat{A}(k_v)/\lambda A(k_v)$ and $\mathrm{H}^1(\mathcal{O}_\mathcal{S}, A[\lambda])$ are maximal isotropic. The intersection of the images equals the image of $\mathrm{Sel}_\lambda A$.

Remark 4.16. Suppose that $A = \operatorname{Jac} C$ and λ is multiplication-by-2, with $\mathscr{L}$ as in Remark 4.5. Let $c_\mathcal{T}$ be as in Definition 3.2, and let $c_{\mathcal{T},v}$ be its image in $\mathrm{H}^1(k_v, A[2])$. It follows from [PS99, Corollary 2] that $c_\mathcal{T} \in \mathrm{Sel}_2 A$. By [PR11, Theorem 3.9],

$$x \underset{e_2}{\cup} x = x \underset{e_2}{\cup} c_\mathcal{T} \tag{5}$$

for all $x \in \mathrm{H}^1(k_v, A[2])$. This, with Remark 2.8, implies that q_v takes values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ (instead of just $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$) if and only if $c_{\mathcal{T},v} = 0$. Thus

$$Q \text{ takes values in } \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \iff c_\mathcal{T} \in Ш^1(k, A[2]).$$

For an example with $c_\mathcal{T} \in \mathrm{Sel}_2 A - Ш^1(k, A[2])$, and another example with $0 \neq c_\mathcal{T} \in Ш^1(k, A[2])$, see [PR11, Example 3.12].

Remark 4.17. Suppose that we are considering a family of abelian varieties with a systematic subgroup G of $\mathrm{Sel}_\lambda A$ coming from rational points (e.g., a family of elliptic curves with rational 2-torsion). Let X be the image of G in

$$\prod_{v\in\Omega}{}'(\mathrm{H}^1(k_v, A[\lambda]), \mathrm{H}^1(\mathcal{O}_v, A[\lambda])).$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Then our model for $\mathrm{Sel}_\lambda A$ should be that its image in $X^\perp/X$ is an intersection of random maximal isotropic subgroups. In particular, the size of $\mathrm{Sel}_\lambda A/Ш^1(k, A[\lambda])$ should be distributed as $\#X$ times the size of the random intersection.

Example 4.18. Suppose that $\operatorname{char} k \neq p$ and A is an elliptic curve $E\colon y^2 = f(x)$. The theta divisor Θ on E is the identity point with multiplicity 1. Let $\mathscr{L} = \mathscr{O}(p\Theta)$. Then λ is $E \xrightarrow{p} E$, and $\mathrm{Sel}_\lambda A$ is the p-Selmer group $\mathrm{Sel}_p E$. Moreover, $Ш^1(k, E[p]) = 0$ by Proposition 3.3(e). Thus Theorem 4.14 identifies $\mathrm{Sel}_p E$ as an intersection of two maximal isotropic subspaces in an $\mathbb{F}_p$-vector space. Moreover, the values of the quadratic form on that space are killed by p, even when $p = 2$, since $c_{\mathcal{T}} = 0$ in (5). In particular, $\dim \mathrm{Sel}_p E$ should be expected to be distributed according to X_{Sel_p}, with the adjustment given by Remark 4.17 when necessary for the family at hand. This is evidence for Conjecture 1.1(a). The rest of Conjecture 1.1, concerning moments, is plausible given Proposition 2.22(a).

Example 4.19. The same reasoning applies to the p-Selmer group of the Jacobian of a hyperelliptic curve $y^2 = f(x)$ over a global field of characteristic not 2 in the following cases:

- f is separable of degree $2g + 1$, and p is arbitrary;
- f is separable of degree $2g + 2$, and p is odd.

(Use Propositions 3.3(f) and 3.4, and Remark 3.5.) This suggests Conjecture 1.7.

Example 4.20. Consider $y^2 = f(x)$ over a global field k of characteristic not 2 with $\deg f = 2g + 2$ for *even* $g \geq 2$. Proposition 3.4 and Remark 3.5 show that $Ш^1(k, A[p])$ is 0 with probability 1 for each $p \neq \operatorname{char} k$. But the Hilbert irreducibility theorem shows that $c_{\mathcal{T}} \neq 0$ with probability 1, so Remarks 4.16 and 2.8 suggest that $\dim \mathrm{Sel}_2 A$ now has the distribution $X_{\mathrm{Sel}_2} + 1$. This suggests Conjecture 1.8.

In the analogous situation with g odd, it is less clear what to predict for $\mathrm{Sel}_2 A$: using techniques in [PS99, §9.2] one can show that the probability that $c_{\mathcal{W}_1}$ lies in $\mathrm{Sel}_2 A$ is strictly between 0 and 1, and the existence of this element may invalidate the random model.

5. Relation to heuristics for Ш and rank

The Hilbert irreducibility theorem shows that asymptotically 100% of elliptic curves (ordered by naïve height) have $E(\mathbb{Q})[p] = 0$. (For much stronger results, see [Duk97] and [Jon10].) So for statistical purposes, when letting E run over all elliptic curves, we may ignore contributions of torsion to the p-Selmer group.

In analogy with the Cohen-Lenstra heuristics [CL84], Delaunay has formulated a conjecture describing the distribution of Shafarevich-Tate groups of random elliptic curves over $\mathbb{Q}$. We now recall his conjectures for $\dim_{\mathbb{F}_p} Ш[p]$. For each prime p and $r \in \mathbb{Z}_{\geq 0}$, let $X_{Ш[p],r}$ be a random variable taking values in $2\mathbb{Z}_{\geq 0}$ such that

$$\mathrm{Prob}\left(X_{Ш[p],r} = 2n\right) \;=\; p^{-n(2r+2n-1)} \frac{\prod_{i=n+1}^{\infty}(1 - p^{-(2r+2i-1)})}{\prod_{i=1}^{n}(1 - p^{-2i})}.$$

The following conjecture is as in [Del01, Example F and Heuristic Assumption], with the correction that $u/2$ in the Heuristic Assumption is replaced by u (his u is our r). This correction was suggested explicitly in [Del07, §3.2] for rank 1, and it seems natural to make the correction for higher rank too.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Conjecture 5.1 (Delaunay)**.** *Let $r, n \in \mathbb{Z}_{\geq 0}$. If E ranges over elliptic curves over $\mathbb{Q}$ of rank r, up to isomorphism, ordered by conductor, then the fraction with $\dim_{\mathbb{F}_p} Ш(E)[p] = 2n$ equals* $\operatorname{Prob}\left(X_{Ш[p],r} = 2n\right)$.

If the "rank" r itself is a random variable R, viewed as a prior distribution, then the distribution of $\dim \operatorname{Sel}_p E$ should be given by $R + X_{Ш[p],R}$. On the other hand, Theorem 4.14 suggests that $\dim \operatorname{Sel}_p E$ should be distributed according to X_{Sel_p}. Let $R_{\text{conjectured}}$ be the random variable taking values 0 and 1 with probability $1/2$ each.

Theorem 5.2. *For each prime p, the unique $\mathbb{Z}_{\geq 0}$-valued random variable R such that X_{Sel_p} and $R + X_{Ш[p],R}$ have the same distribution is $R_{\text{conjectured}}$.*

Proof. First we show that $R_{\text{conjectured}}$ has the claimed property. This follows from the following identities for $n \in \mathbb{Z}_{\geq 0}$:

$$\begin{aligned}
\operatorname{Prob}\left(X_{\operatorname{Sel}_p} = 2n\right) &= c \prod_{j=1}^{2n} \frac{p}{p^j - 1} \\
&= \frac{1}{2} \prod_{i \geq 0} (1 - p^{-(2i+1)}) \cdot p^{-n(2n-1)} \prod_{j=1}^{2n} (1 - p^{-j})^{-1} \\
&= \frac{1}{2} p^{-n(2n-1)} \prod_{i \geq n+1} (1 - p^{-(2i-1)}) \prod_{i=1}^{n} (1 - p^{-2i})^{-1} \\
&= \frac{1}{2} \operatorname{Prob}\left(X_{Ш[p],0} = 2n\right), \\
\operatorname{Prob}\left(X_{\operatorname{Sel}_p} = 2n+1\right) &= c \prod_{j=1}^{2n+1} \frac{p}{p^j - 1} \\
&= \frac{1}{2} \prod_{i \geq 0} (1 - p^{-(2i+1)}) \cdot p^{-n(2n+1)} \prod_{j=1}^{2n+1} (1 - p^{-j})^{-1} \\
&= \frac{1}{2} p^{-n(2n+1)} \prod_{i \geq n+1} (1 - p^{-(2i+1)}) \prod_{i=1}^{n} (1 - p^{-2i})^{-1} \\
&= \frac{1}{2} \operatorname{Prob}\left(X_{Ш[p],1} = 2n\right).
\end{aligned}$$

Next we show that any random variable R with the property has the same distribution as $R_{\text{conjectured}}$. For $r \in \mathbb{Z}_{\geq 0}$, define a function $f_r \colon \mathbb{Z}_{\geq 0} \to \mathbb{R}$ by $f_r(s) := \operatorname{Prob}(X_{Ш[p],r} = s - r)$. The assumption on R implies that

$$\sum_{r=0}^{\infty} \operatorname{Prob}(R = r) f_r(s) = \sum_{r=0}^{\infty} \operatorname{Prob}\left(R_{\text{conjectured}} = r\right) f_r(s).$$

Thus to prove that R and $R_{\text{conjectured}}$ have the same distribution, it will suffice to prove that the functions f_r are linearly independent in the sense that for any sequence of real numbers $(\alpha_r)_{r \geq 0}$ with $\sum_{r \geq 0} |\alpha_r| < \infty$, the equality $\sum_{r=0}^{\infty} \alpha_r f_r = 0$ implies that $\alpha_r = 0$ for all $r \in \mathbb{Z}_{\geq 0}$. In fact, $\alpha_r = 0$ by induction on r, since $f_r(s) = 0$ for all $s > r$, and $f(r, r) > 0$. □

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Acknowledgements

The authors thank Christophe Delaunay, Benedict Gross, Robert Guralnick, Karl Rubin, and the referee for comments.

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115. MR0219512 (36:2593) ↑257

[BS10a] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, June 9, 2010. Preprint, arXiv:1006.1002. ↑246

[BS10b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, July 1, 2010. Preprint, arXiv:1007.0052. ↑246

[Bou04] Nicolas Bourbaki, *Integration. I. Chapters 1–6*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2004. Translated from the 1959, 1965 and 1967 French originals by Sterling K. Berberian. MR2018901 (2004i:28001) ↑255

[Bra48] Jean Braconnier, *Sur les groupes topologiques localement compacts*, J. Math. Pures Appl. (9) **27** (1948), 1–85 (French). MR0025473 (10:11c) ↑253

[BPS10] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus* 3, July 24, 2010. Preprint. ↑257

[Cau43] A. Cauchy, *Mémoire sur les fonctions dont plusieurs valeurs sont liées entre elles par une équation linéaire, et sur diverses transformations de produits composés d'un nombre indéfini de facteurs*, C. R. Acad. Sci. Paris **17** (1843), 523–531 (French). Reprinted in *Oeuvres*, Ser. 1, Vol. 8, Gauthier-Villars, Paris, 1893, 42–50. ↑251

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082 (85j:11144) ↑265

[dJ02] A. J. de Jong, *Counting elliptic surfaces over finite fields*, Mosc. Math. J. **2** (2002), no. 2, 281–311. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. MR1944508 (2003m:11080) ↑246

[Del01] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670 (2003a:11065) ↑247, 265

[Del07] ———, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340. MR2322355 (2008i:11089) ↑247, 265

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818, DOI 10.1016/S0764-4442(97)80118-8 (English, with English and French summaries). MR1485897 (99b:11059) ↑265

[Fou64] David A. Foulser, *The flag-transitive collineation groups of the finite Desarguesian affine planes*, Canad. J. Math. **16** (1964), 443–472. MR0166272 (29:3549) ↑258

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR2266528 (2007k:16033) ↑264

[Gol79] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118. MR564926 (81i:12014) ↑247

[GA09] Cristian D. González-Avilés, *Arithmetic duality theorems for* 1*-motives over function fields*, J. Reine Angew. Math. **632** (2009), 203–231, DOI 10.1515/CRELLE.2009.055. MR2544149 (2010i:11169) ↑264

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York, 1977. MR0463157 (57:3116) ↑262

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

[HB93] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195, DOI 10.1007/BF01231285. MR1193603 (93j:11038) ↑245

[HB94] ———, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, DOI 10.1007/BF01231536. With an appendix by P. Monsky. MR1292115 (95h:11064) ↑245, 246

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570, DOI 10.1090/S0002-9947-09-04804-1. MR2563740 ↑265

[Kak43] Shizuo Kakutani, *On cardinal numbers related with a compact Abelian group*, Proc. Imp. Acad. Tokyo **19** (1943), 366–372. MR0015124 (7,375a) ↑252

[Kan11] Daniel M. Kane, *On the ranks of the* 2*-Selmer groups of twists of a given elliptic curve*, March 9, 2011. Preprint, arXiv:1009.1365. ↑245, 246

[KS99a] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR2000b:11070 ↑247

[KS99b] ———, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) **36** (1999), no. 1, 1–26, DOI 10.1090/S0273-0979-99-00766-1. MR1640151 (2000f:11114) ↑247

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR0086367 (19,174a) ↑262

[MR10] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575. MR2660452 ↑246

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 (81j:14002) ↑262

[Mil06] ———, *Arithmetic duality theorems*, Second edition, BookSurge, LLC, Charleston, SC, 2006. MR2261462 (2007e:14029) ↑257, 262, 264

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970. MR0282985 (44:219) ↑259

[Mum71] ———, *Theta characteristics of an algebraic curve*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 181–192. MR0292836 (45:1918) ↑258

[Mum91] ———, *Tata lectures on theta. III*, Progress in Mathematics, vol. 97, Birkhäuser Boston Inc., Boston, MA, 1991. With the collaboration of Madhav Nori and Peter Norman. MR1116553 (93d:14065) ↑260

[O'N02] Catherine O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), no. 2, 329–339, DOI 10.1016/S0022-314X(01)92770-2. Erratum in *J. Number Theory* **109** (2004), no. 2, 390. MR1924106 (2003f:11079); MR2106488 (2005g:11096) ↑260

[Pol03] Alexander Polishchuk, *Abelian varieties, theta functions and the Fourier transform*, Cambridge Tracts in Mathematics, vol. 153, Cambridge University Press, Cambridge, 2003. MR1987784 (2004m:14094) ↑259, 261

[Pol71] Harriet Pollatsek, *First cohomology groups of some linear groups over fields of characteristic two*, Illinois J. Math. **15** (1971), 393–417. MR0280596 (43:6316) ↑258

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, April 10, 2011. Preprint. ↑258, 259, 260, 264

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR1740984 (2000m:11048) ↑258, 264, 265

[Rot11] H. A. Rothe, *Systematisches Lehrbuch der Arithmetik*, Barth, Leipzig, 1811. ↑251

[Sch85] Winfried Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 270, Springer-Verlag, Berlin, 1985. MR770063 (86k:11022) ↑248, 249, 251

[SD08] Peter Swinnerton-Dyer, *The effect of twisting on the* 2*-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526, DOI 10.1017/S0305004108001588. MR2464773 (2010d:11059) ↑245, 246

[vK35] E. R. van Kampen, *Locally bicompact abelian groups and their character groups*, Ann. of Math. (2) **36** (1935), no. 2, 448–463, DOI 10.2307/1968582. MR1503234 ↑252

[Wei64] André Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211 (French). MR0165033 (29:2324) ↑245, 252

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

[Yu05] Gang Yu, *Average size of* 2*-Selmer groups of elliptic curves. II*, Acta Arith. **117** (2005), no. 1, 1–33, DOI 10.4064/aa117-1-1. MR2110501 (2006b:11054) ↑246

[Yu06] ———, *Average size of* 2*-Selmer groups of elliptic curves. I*, Trans. Amer. Math. Soc. **358** (2006), no. 4, 1563–1584 (electronic), DOI 10.1090/S0002-9947-05-03806-7. MR2186986 (2006j:11080) ↑246

[Zar74] Ju. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419 (Russian). MR0354612 (50:7090) ↑246, 260

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139-4307

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

E-mail address: rains@caltech.edu

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use