MODELING THE DISTRIBUTION OF RANKS, SELMER GROUPS, AND SHAFAREVICH–TATE GROUPS OF ELLIPTIC CURVES

MANJUL BHARGAVA, DANIEL M. KANE, HENDRIK W. LENSTRA JR., BJORN POONEN, AND ERIC RAINS

ABSTRACT. Using only linear algebra over $\mathbb{Z}_p$, we define a discrete probability distribution on the set of isomorphism classes of short exact sequences of $\mathbb{Z}_p$-modules with finitely generated Pontryagin duals, and then conjecture that as E varies over elliptic curves over a fixed global field k, the distribution of

$$0 \to E(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty} E \to Ш[p^\infty] \to 0$$

is that one. This single conjecture would explain many of the known theorems and conjectures on ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves. We also prove new theorems on the arithmetic of elliptic curves that partially justify our conjecture.

1. INTRODUCTION

1.1. **Selmer and Shafarevich–Tate groups.** Fix a global field k. Let Ω be the set of nontrivial places of k. Let $\mathscr{E}$ be the set of elliptic curves over k, or more precisely, a set containing one representative of each isomorphism class. Given $E \in \mathscr{E}$ and a positive integer n, the n-Selmer group $\mathrm{Sel}_n E$ is a finite group that is used to bound the rank of the finitely generated abelian group $E(k)$. If n is a product of prime powers p^e, then $\mathrm{Sel}_n E$ is the direct sum of the Sel_{p^e}, so we focus on the latter groups. If p is prime, one may also form the direct limit $\mathrm{Sel}_{p^\infty} E := \varinjlim \mathrm{Sel}_{p^e} E$. This group, together with the p-primary subgroup of the Shafarevich–Tate group $Ш = Ш(E) := \ker\left(\mathrm{H}^1(k, E) \to \prod_{v\in\Omega} \mathrm{H}^1(k_v, E)\right)$, fits into an exact sequence

$$0 \longrightarrow E(k) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0 \qquad (\mathrm{Seq}_E)$$

of $\mathbb{Z}_p$-modules with finitely generated Pontryagin duals (i.e., each $\mathbb{Z}_p$-module in the sequence Seq_E is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^s \oplus F$ for some $s \in \mathbb{Z}_{\geq 0}$ and finite abelian p-group F). Since $E(k) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ is divisible, the sequence splits.

1.2. **Intersection of random maximal isotropic $\mathbb{Z}_p$-modules.** Our goal is to predict the distribution of Seq_E as E varies over $\mathscr{E}$. More precisely, using only linear algebra over $\mathbb{Z}_p$ we will define a discrete probability distribution $\mathscr{Q}$ on the set of isomorphism classes of short exact sequences of $\mathbb{Z}_p$-modules with finitely generated Pontryagin duals, and then conjecture

Date: May 8, 2013.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11E08, 14G25.

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

M.B. was supported by the National Science Foundation grant DMS-1001828. D.K. was supported by a National Science Foundation Graduate Fellowship. B.P. was supported by the Guggenheim Foundation and National Science Foundation grants DMS-0841321 and DMS-1069236.

that for each sequence $\mathscr{S}$, the density of $\{E \in \mathscr{E} : \mathrm{Seq}_E \simeq \mathscr{S}\}$ equals the $\mathscr{Q}$-probability of (the isomorphism class of) $\mathscr{S}$. (To define density of a subset of $\mathscr{E}$ precisely, one orders $\mathscr{E}$ by height as explained in the introductions to [BS10] and [PR12]. The reason for ordering by height is that most other orderings lead to statements that are difficult to corroborate: for instance, the asymptotic behavior of the number of elliptic curves over $\mathbb{Q}$ of conductor up to X is unknown, even when no condition on its Selmer sequence is imposed.)

We now describe the distribution $\mathscr{Q}$. Equip $V := \mathbb{Z}_p^{2n}$ with the standard hyperbolic quadratic form $Q\colon V \to \mathbb{Z}_p$ given by

$$Q(x_1, \dots, x_n, y_1, \dots, y_n) := \sum_{i=1}^{n} x_i y_i. \tag{1}$$

Let $\mathrm{OGr}_V(\mathbb{Z}_p)$ be the set of rank n $\mathbb{Z}_p$-submodules $Z \leq V$ that are direct summands such that $Q|_Z = 0$ (see Section 4). There is a natural probability measure on $\mathrm{OGr}_V(\mathbb{Z}_p)$, defined so that for each $e \geq 0$, the distribution of Z/p^eZ in V/p^eV is uniform among all possibilities (see Section 2). Fix $W := \mathbb{Z}_p^n \times 0 \in \mathrm{OGr}_V(\mathbb{Z}_p)$, and choose a second $Z \in \mathrm{OGr}_V(\mathbb{Z}_p)$ at random. (For what follows, it would be equivalent to choose both W and Z at random, since the orthogonal group of (V, Q) acts transitively on $\mathrm{OGr}_V(\mathbb{Z}_p)$: see Proposition 4.2.) View $Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ and $W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ as $\mathbb{Z}_p$-submodules of $V \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$, where the tensor products are over $\mathbb{Z}_p$. Define

$$\begin{aligned}
R &:= (Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} && \text{“}R\text{ational points”, or “}R\text{ank”} \\
S &:= \left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) && \text{“}S\text{elmer group”} \\
T &:= S/R && \text{“Shafarevich–}T\text{ate group”}
\end{aligned}$$

(The labels on the right hint at what these groups will be modeling. For instance, the $\mathbb{Z}_p$-module $Z \cap W$ is intended to model $E(k) \otimes \mathbb{Z}_p$.) Let $\mathscr{Q}_{2n}$ be the distribution of the isomorphism class of the exact sequence

$$0 \to R \to S \to T \to 0$$

so constructed (here $\mathscr{Q}$ is for “quadratic”). We will prove that $\mathscr{Q}_{2n}$ converges as $n \to \infty$ (see Proposition 5.7). Define $\mathscr{Q}$ as the limit.

Conjecture 1.1. Fix a global field k. For each short exact sequence $\mathscr{S}$ of $\mathbb{Z}_p$-modules, the density of $\{E \in \mathscr{E} : \mathrm{Seq}_E \simeq \mathscr{S}\}$ equals the $\mathscr{Q}$-probability of $\mathscr{S}$.

We will prove that Conjecture 1.1 has the following consequences:

- 50% of elliptic curves over k have rank 0, 50% have rank 1, and 0% have rank 2 or more; cf. [Gol79, Conjecture B] and [KS99a, KS99b].
- $Ш[p^\infty]$ is finite for 100% of elliptic curves over k.
- Conjecture 1.1(a) of [PR12] concerning the distribution of $\mathrm{Sel}_p E$ holds. In fact, our Conjecture 1.1 implies a generalization concerning the distribution of $\mathrm{Sel}_{p^e} E$ for every $e \geq 0$ (see Section 5.5). These consequences are consistent with the partial results that have been proved: see the introduction of [PR12] for discussion.

- C. Delaunay's conjecture in [Del01, Del07, DJ13a] à la Cohen–Lenstra regarding the distribution of $Ш[p^\infty]$ for rank r elliptic curves over $\mathbb{Q}$ holds for $r = 0$ and $r = 1$.[1]

For $r \geq 2$, Conjecture 1.1 cannot say anything about the distribution of $Ш[p^\infty]$ as E varies over the set $\mathscr{E}_r := \{E \in \mathscr{E} : \operatorname{rk} E(k) = r\}$, because the locus of $Z \in \mathrm{OGr}_V(\mathbb{Z}_p)$ where $\operatorname{rk}(Z \cap W) = r$ is of measure 0 (Proposition 5.6). On the other hand, that locus carries another natural probability measure, and if we sample Z with respect to this new measure, the distribution $\mathscr{T}_{2n,r}$ of T tends to a limit $\mathscr{T}_r$ as $n \to \infty$ (see Section 5.4).

Conjecture 1.2. Fix a global field k and $r \in \mathbb{Z}_{\geq 0}$ such that $\mathscr{E}_r$ is infinite. For each finite abelian p-group G, the density of $\{E \in \mathscr{E}_r : Ш[p^\infty] \simeq G\}$ in $\mathscr{E}_r$ equals the $\mathscr{T}_r$-probability of G.

We will prove that Conjecture 1.2 (over $\mathbb{Q}$) implies Delaunay's conjecture for rank r elliptic curves.

Remark 1.3. In fact, Delaunay made predictions for the whole group Ш and not only $Ш[p^\infty]$ for one p at a time. For further discussion of this, see Section 5.6.

Remark 1.4. In fact, one can turn things around, and use Delaunay's conjecture for $Ш[p^\infty]$ together with the conjecture that the rank r is 0 or 1 with 50% probability each to obtain conjectural distributions for $\operatorname{Sel}_{p^\infty} E$ and $\operatorname{Sel}_{p^e} E$ (cf. [DJ13a, §6.2] and [DJ13b, §5]). Specifically, $\operatorname{Sel}_{p^\infty} E \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus Ш[p^\infty]$; if moreover $E(k)_{\mathrm{tors}} = 0$, as holds for 100% of elliptic curves (Lemma 5.8), then $\operatorname{Sel}_{p^\infty} E$ determines $\operatorname{Sel}_{p^e} E$ (Proposition 5.10(c)).

Remark 1.5. Certain restricted families of elliptic curves can exhibit very different Selmer group behavior. The average size of $\operatorname{Sel}_2 E$ can even be infinite in certain families. See [Yu05], [XZ09], [XZ08], and [FX12] for work in this direction.

1.3. **Cokernel of a random alternating matrix.** Moreover, Conjecture 1.2 implies that another natural distribution on finite abelian p-groups yields a model for $Ш[p^\infty]$. We now describe it. For an even integer n, choose an alternating $n \times n$ matrix $A \in M_n(\mathbb{Z}_p)$ (see Section 3.3 for definitions) at random with respect to Haar measure, and let $\mathscr{A}_{n,0}$ be the distribution of $\operatorname{coker} A$.

More generally, for any fixed $r \geq 0$, for n with $n - r \in 2\mathbb{Z}_{\geq 0}$, choose A at random from the set of alternating matrices in $M_n(\mathbb{Z}_p)$ such that $\operatorname{rk} A = n - r$ (with respect to a measure to be described), and let $\mathscr{A}_{n,r}$ be the distribution of $(\operatorname{coker} A)_{\mathrm{tors}}$.

Theorem 1.6. *For each $r \geq 0$,*

(a) *the distributions $\mathscr{A}_{n,r}$ converge to a limit $\mathscr{A}_r$ as $n \to \infty$ through integers with $n - r \in 2\mathbb{Z}_{\geq 0}$, and*

(b) *the distributions $\mathscr{A}_r$ and $\mathscr{T}_r$ coincide.*

1.4. **Cassels–Tate pairing.** The Cassels–Tate pairing on Ш is an alternating bilinear pairing

$$Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$$

[1] For this conjecture, see [Del01, Heuristic Assumption], with the modification that $u/2$ is replaced by u, as suggested by the $u = 1$ case discussed in [Del07, §3.2] (his u is our r); see also [PR12, Section 6] and [DJ13a, Section 6.2]. Strictly speaking, in order to have our model match Delaunay's conjecture, we modify his conjecture to order elliptic curves over $\mathbb{Q}$ by height instead of conductor.

whose kernel on each side is the maximal divisible subgroup of Ш. Taking p-primary parts yields an alternating bilinear pairing

$$Ш[p^\infty] \times Ш[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p.$$

If $Ш[p^\infty]$ is finite, then this pairing is nondegenerate.

Recall that we are modeling $Ш[p^\infty]$ by the random groups T and $(\operatorname{coker} A)_{\mathrm{tors}}$ constructed in Sections 1.2 and 1.3, respectively. As evidence that these models are reasonable, we will construct a canonical nondegenerate alternating pairing on each of T and $(\operatorname{coker} A)_{\mathrm{tors}}$.

1.5. **Arithmetic justification?** The heuristic in [PR12] that $\mathrm{Sel}_p E$ behaves like the intersection of maximal isotropic subspaces in a high-dimensional quadratic space over $\mathbb{F}_p$ was given an arithmetic justification, namely, that $\mathrm{Sel}_p E$ is isomorphic to the intersection of two maximal isotropic subspaces in an infinite-dimensional locally compact quadratic space over $\mathbb{F}_p$.

Question 1.7. Is there an arithmetic justification for the linear algebra processes that produce $\mathscr{Q}$, $\mathscr{T}_r$, and $\mathscr{A}_r$?

For instance, given an elliptic curve E, is $Ш(E)$ isomorphic to $(\operatorname{coker} A)_{\mathrm{tors}}$ for some alternating matrix A over $\mathbb{Z}$ that can be constructed from the arithmetic of E?

Also, can one explain why the maximal isotropic submodules used to define $\mathscr{Q}$ are required to be *direct summands*? Some partial answers and open questions related to this will be discussed in Section 6.

2. The canonical measure on the set of $\mathbb{Z}_p$-points of a scheme

The following is a consequence of work of J. Oesterlé and J.-P. Serre.

Proposition 2.1. *Let X be a finite-type $\mathbb{Z}_p$-scheme. Let $d = \dim X_{\mathbb{Q}_p}$. Equip $X(\mathbb{Z}_p)$ with the p-adic topology.*

(a) *There exists a unique bounded $\mathbb{R}_{\geq 0}$-valued measure $\mu = \mu_X$ on the Borel σ-algebra of $X(\mathbb{Z}_p)$ such that for any open and closed subset S of $X(\mathbb{Z}_p)$, we have*

$$\mu(S) = \lim_{e\to\infty} \frac{\#(\text{image of } S \text{ in } X(\mathbb{Z}/p^e\mathbb{Z}))}{(p^e)^d}.$$

(b) *If Y is a subscheme of X and $\dim Y_{\mathbb{Q}_p} < d$, then $\mu(Y(\mathbb{Z}_p)) = 0$.*

(c) *If S is an open subset of $X(\mathbb{Z}_p)$, and $X_{\mathbb{Q}_p}$ is smooth of dimension d at $s_{\mathbb{Q}_p}$ for some $s \in S$, then $\mu(S) > 0$.*

Proof.

(a) If X is affine, this is a consequence of the discussion surrounding Théorème 2 of [Oes82], which builds on [Ser81, S3], and the Hahn–Kolmogorov extension theorem. In general, let (X_i) be a finite affine open cover of X. Each set $X_i(\mathbb{Z}_p)$ is open *and closed* in $X(\mathbb{Z}_p)$, because $X_i(\mathbb{Z}_p)$ equals the inverse image of $X_i(\mathbb{F}_p)$ under the reduction map $X(\mathbb{Z}_p) \to X(\mathbb{F}_p)$. Since $\mathbb{Z}_p$ is a local ring, the sets $X_i(\mathbb{Z}_p)$ form a cover of $X(\mathbb{Z}_p)$. The measures on $X_i(\mathbb{Z}_p)$ and $X_j(\mathbb{Z}_p)$ are compatible on the intersection, by uniqueness, so they glue to give the required measure on $X(\mathbb{Z}_p)$.

(b) We may assume that X is affine and that Y is a closed subscheme of X. Even though $Y(\mathbb{Z}_p)$ might not be open in $X(\mathbb{Z}_p)$, it is an analytic closed subset (see [Oes82, §2]), so

$$\mu(Y(\mathbb{Z}_p)) = \lim_{e\to\infty} \frac{\#Y(\mathbb{Z}/p^e\mathbb{Z})}{(p^e)^d}$$

still holds. According to [Ser81, p. 145, Théorème 8], $\#Y(\mathbb{Z}/p^e\mathbb{Z}) = O((p^e)^{d-1})$ as $e \to \infty$, so the limit is 0.

(c) See the discussion before Théorème 2 of [Oes82]. □

Corollary 2.2. *If X is as in Proposition 2.1, and $X_{\mathbb{Q}_p}$ is smooth of dimension d at $x_{\mathbb{Q}_p}$ for some $x \in X(\mathbb{Z}_p)$, then μ can be normalized to yield a probability measure ν on $X(\mathbb{Z}_p)$.*

From now on, when we speak of choosing an element of $X(\mathbb{Z}_p)$ uniformly at random for X as in Corollary 2.2, we mean choosing it according to the measure ν.

3. Modeling Shafarevich–Tate groups using alternating matrices

3.1. **Notation.** Let R be a principal ideal domain. (We could work with more general rings, but we have no need to.) Let $K = \operatorname{Frac} R$. Given an R-module L, let $L^T := \operatorname{Hom}_R(L, R)$, let $L_K := L \otimes_R K$, and let $L_{\text{tors}} := \{x \in L : rx = 0 \text{ for some nonzero } r \in R\} = \ker(L \to L_K)$. If a free R-module L has been fixed, and N is a submodule of L, define the saturation

$$N^{\text{sat}} := N_K \cap L = \{x \in L : rx \in N \text{ for some nonzero } r \in R\}.$$

Given a homomorphism $A\colon L \to M$, let $A^t\colon M^T \to L^T$ denote the dual homomorphism; this notation is compatible with the notation A^t for the transpose of a matrix. Let $M_n(R)_{\text{alt}}$ be the set of alternating $n \times n$ matrices, i.e., matrices A with zeros on the diagonal satisfying $A^t = -A$. For $S \subseteq M_n(R)$, define $S_{\text{alt}} = S \cap M_n(R)_{\text{alt}}$.

3.2. **Symplectic abelian groups.** Define a symplectic abelian group (called group of type S in [Del01]) to be a finite abelian group G equipped with a nondegenerate alternating pairing $[\ ,\ ]\colon G \times G \to \mathbb{Q}/\mathbb{Z}$. An isomorphism between two symplectic abelian groups is a group isomorphism that respects the pairings. Let $\operatorname{Sp}(G)$ be the group of automorphisms of G respecting $[\ ,\ ]$. One can show that two symplectic abelian groups are isomorphic if and only if their underlying abelian groups are isomorphic. If p is a prime, define a symplectic p-group to be a symplectic abelian group whose order is a power of p; in this case, $[\ ,\ ]$ may be viewed as taking values in $\mathbb{Q}_p/\mathbb{Z}_p$.

3.3. **Pairings on the cokernel of an alternating matrix.** Let L be a free R-module of rank n. Let $\mathcal{A}\colon L \times L \to R$ be an alternating R-bilinear pairing; alternating means that $\mathcal{A}(x, x) = 0$ for all $x \in L$. Let $A\colon L \to L^T$ be the induced R-homomorphism. If we choose a basis for L and use the dual basis for L^T, then A corresponds to a matrix $A \in M_n(R)_{\text{alt}}$; then $\mathcal{A}$ is identified with

$$R^n \times R^n \to R$$
$$x, y \mapsto x^t A y.$$

A change of basis of L is given by a matrix $M \in \mathrm{GL}_n(R)$, which changes A to $M^t A M$; this defines an action of $\mathrm{GL}_n(R)$ on $M_n(R)_{\text{alt}}$.

Let $L^\perp := \{x \in L_K \colon \mathcal{A}(L,x) \subseteq R\}$. Then $\mathcal{A}_K := \mathcal{A} \otimes K$ induces an alternating pairing

$$\frac{L^\perp}{L} \times \frac{L^\perp}{L} \to \frac{K}{R}. \tag{2}$$

3.4. **The pairing in the nonsingular case.** Suppose that A is nonsingular in the sense that $A_K \colon L_K \to (L^\vee)_K$ is an isomorphism (i.e., $\det A \neq 0$). Then $L^\perp = A^{-1}L^T$ and multiplication-by-A induces an isomorphism $L^\perp/L \simeq L^T/AL = \operatorname{coker} A$ of finite torsion R-modules. Substituting (and flipping a sign) rewrites (2) as an alternating pairing

$$\langle\ ,\ \rangle_A \colon \operatorname{coker} A \times \operatorname{coker} A \to \frac{K}{R} \tag{3}$$

induced by

$$\begin{aligned} [\ ,\ ]_A \colon R^n \times R^n &\to \frac{K}{R} \\ x, y &\mapsto x^t A^{-1} y, \end{aligned} \tag{4}$$

where each R^n is L^T. The right kernel of $[\ ,\ ]_A$ is the image $\operatorname{im}(A \colon R^n \to R^n)$ since one has $x^t(A^{-1}y) \in R$ for all $x \in R^n$ if and only if $A^{-1}y \in R^n$. Since the pairing is alternating, the left kernel is the same. Thus the left and right kernels of $\langle\ ,\ \rangle_A$ are 0; i.e., $\langle\ ,\ \rangle_A$ is nondegenerate.

3.5. **The pairing in the singular case.** Suppose that $\det A = 0$. Let $L_0 = \ker A$. The quotient L/L_0 is torsion-free, and hence free, since R is a principal ideal domain. Then $\mathcal{A}$ induces a nonsingular alternating pairing $\mathcal{A}_1$ on L/L_0, corresponding to some A_1. The submodule $(L/L_0)^T$ of L^T is the saturation of $\operatorname{im} A$ in L^T, i.e., $(\operatorname{im} A)^{\mathrm{sat}} = (\operatorname{im} A)_K \cap L^T$. Then $\operatorname{coker}(A_1 \colon L/L_0 \to (L/L_0)^T)$ identifies with $(\operatorname{im} A)^{\mathrm{sat}}/(\operatorname{im} A) \simeq (\operatorname{coker} A)_{\mathrm{tors}}$. Applying Section 3.4 to A_1, we obtain an alternating R-bilinear pairing

$$\langle\ ,\ \rangle_A \colon (\operatorname{coker} A)_{\mathrm{tors}} \times (\operatorname{coker} A)_{\mathrm{tors}} \to \frac{K}{R}$$

whose left and right kernels are 0.

3.6. **Lemmas.** Take $R = \mathbb{Z}_p$. Given $A \in M_n(\mathbb{Z}_p)$, let $\overline{A} := A \bmod p \in M_n(\mathbb{F}_p)$. If $A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}$ and $\det A \neq 0$, then by Section 3.4, $\operatorname{coker} A$ with $\langle\ ,\ \rangle_A$ is a symplectic p-group.

Lemma 3.1. *Suppose that $A, D \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}$, and $\det D \neq 0$. We have $[\ ,\ ]_A = [\ ,\ ]_D$ if and only if $\det A \neq 0$ and $A^{-1} - D^{-1} \in M_n(\mathbb{Z}_p)$.*

Proof. This is immediate from (4). □

Lemma 3.2. *Suppose that $D \in M_n(\mathbb{Z}_p)$ and $\det D \neq 0$. Then*

$$\{A \in M_n(\mathbb{Z}_p) : \det A \neq 0 \text{ and } A^{-1} - D^{-1} \in M_n(\mathbb{Z}_p)\} = \{A \in D + DM_n(\mathbb{Z}_p)D : \operatorname{rk} \overline{A} = \operatorname{rk} \overline{D}\}.$$

Proof. Suppose that $A \in M_n(\mathbb{Z}_p)$ is such that $\det A \neq 0$ and $A^{-1} - D^{-1} = N$ for some $N \in M_n(\mathbb{Z}_p)$. Multiplying by A on the left yields $I - AD^{-1} = AN$, so $AD^{-1} \in M_n(\mathbb{Z}_p)$; similarly $DA^{-1} \in M_n(\mathbb{Z}_p)$, so $AD^{-1} \in \mathrm{GL}_n(\mathbb{Z}_p)$, and in particular $\operatorname{rk} \overline{D} = \operatorname{rk} \overline{A}$. Multiplying instead by D on the left and A on the right yields $D - A = DNA = D(N \cdot AD^{-1})D \in DM_n(\mathbb{Z}_p)D$, so $A \in D + DM_n(\mathbb{Z}_p)D$.

Conversely, suppose that $A = D + DND$ with $N \in M_n(\mathbb{Z}_p)$, and $\operatorname{rk} \overline{A} = \operatorname{rk} \overline{D}$. Then $\overline{A} = \overline{D} + \overline{D}\,\overline{N}\,\overline{D}$, so $\ker \overline{D} \subseteq \ker \overline{A}$, and the rank condition implies $\ker \overline{D} = \ker \overline{A}$. If

$v \in \ker(\overline{I+ND})$, then $v \in \ker \overline{A} = \ker \overline{D}$; so both $\overline{I+ND}$ and $\overline{ND}$ kill v, so $v = 0$. Thus $\overline{I+ND} \in \mathrm{GL}_n(\mathbb{F}_p)$, so $I + ND \in \mathrm{GL}_n(\mathbb{Z}_p)$. Now $D^{-1}A = I + ND$, so its inverse $A^{-1}D$ is in $\mathrm{GL}_n(\mathbb{Z}_p)$ too. Multiplying $A = D + DND$ by A^{-1} on the left and D^{-1} on the right yields $D^{-1} = A^{-1} + A^{-1}DN$, so $A^{-1} - D^{-1} = -(A^{-1}D)N \in M_n(\mathbb{Z}_p)$. □

Corollary 3.3. *Let n be even, let $e_1, \dots, e_{n/2} \in \mathbb{Z}_{\geq 0}$, and let*

$$D = \begin{pmatrix} 0 & \mathrm{diag}(p^{e_1}, \dots, p^{e_{n/2}}) \\ -\mathrm{diag}(p^{e_1}, \dots, p^{e_{n/2}}) & 0 \end{pmatrix} \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}.$$

Let $m = 2\#\{i \in \{1, \dots, n/2\} : e_i = 0\}$. If $A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}$ is chosen at random with respect to Haar measure, then

$$\mathrm{Prob}\left(\det A \neq 0 \text{ and } A^{-1} - D^{-1} \in M_n(\mathbb{Z}_p)\right) = \frac{\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}}{\#M_m(\mathbb{F}_p)_{\mathrm{alt}}} |\det D|_p^{n-1}.$$

Proof. Let $e_{n/2+i} = e_i$ for $i = 1, \dots, n/2$. For $A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}$, the condition $A \in D + DM_n(\mathbb{Z}_p)D$ is equivalent to $a_{ij} \equiv d_{ij} \pmod{p^{e_i}p^{e_j}\mathbb{Z}_p}$ for all $i < j$, so

$$\mathrm{Prob}\left(A \in D + DM_n(\mathbb{Z}_p)D\right) = \prod_{i<j} p^{-e_i}p^{-e_j} = \prod_{i=1}^{n} (p^{-e_i})^{n-1} = |\det D|_p^{n-1}.$$

Let $B \in M_m(\mathbb{Z}_p)_{\mathrm{alt}}$ be the minor formed by the entries a_{ij} such that $e_i = e_j = 0$. The condition $\mathrm{rk}\,\overline{A} = \mathrm{rk}\,\overline{D}$ is equivalent to $\overline{B} \in \mathrm{GL}_m(\mathbb{F}_p)$, which is independent of the congruences above and which holds with probability $\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}/\#M_m(\mathbb{F}_p)_{\mathrm{alt}}$. Multiplying yields the result, by Lemma 3.2. □

Combining Corollary 3.3 with Lemma 3.1 yields

Corollary 3.4. *Retain the notation of Corollary 3.3. Then*

$$\mathrm{Prob}\left([\ ,\ ]_A = [\ ,\ ]_D\right) = \frac{\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}}{\#M_m(\mathbb{F}_p)_{\mathrm{alt}}} |\det D|_p^{n-1}.$$

Corollary 3.5. *Fix* any *alternating pairing $[\ ,\ ]\colon \mathbb{Z}_p^n \times \mathbb{Z}_p^n \to \mathbb{Q}/\mathbb{Z}$ inducing a nondegenerate pairing on a finite quotient G of $\mathbb{Z}_p^n$. Let $m = n - \dim_{\mathbb{F}_p} G[p]$. If $A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}$ is chosen at random, then*

$$\mathrm{Prob}\left([\ ,\ ]_A = [\ ,\ ]\right) = \frac{\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}}{\#M_m(\mathbb{F}_p)_{\mathrm{alt}}} (\#G)^{1-n}. \tag{5}$$

Proof. The structure theorem for symplectic modules over principal ideal domains implies that there exists a change-of-basis matrix $M \in \mathrm{GL}_n(\mathbb{Z}_p)$ and a matrix D as in Corollary 3.3 such that $[\ ,\ ] = [\ ,\ ]_{M^tDM}$. The change of basis reduces the statement to Corollary 3.4. □

The fraction on the right side of (5) can be evaluated:

Lemma 3.6. *For $m \in 2\mathbb{Z}_{\geq 0}$,*

$$\frac{\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}}{\#M_m(\mathbb{F}_p)_{\mathrm{alt}}} = \prod_{i=1}^{m/2} (1 - p^{1-2i}).$$

Proof. There are $p^{m-1}-1$ possibilities for the first column of a matrix in $\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}$, and the number of choices for the rest of the matrix is independent of this first choice, as one sees by performing a change of basis of $\mathbb{F}_p^n$ fixing $(1,0,\dots,0)^t$. If the first column is $(0,1,0,0,\dots,0)^t$, there are p^{m-2} possibilities for the second column (it has the shape $(1,0,*,\cdots,*)$), and then the lower $(m-2)\times(m-2)$ block is an arbitrary element of $\mathrm{GL}_{m-2}(\mathbb{F}_p)_{\mathrm{alt}}$. Thus

$$\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}} = (p^{m-1}-1)p^{m-2}\#\,\mathrm{GL}_{m-2}(\mathbb{F}_p)_{\mathrm{alt}}.$$

Induction on m yields $\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}$, and we divide by $\#M_m(\mathbb{F}_p)_{\mathrm{alt}} = p^{\binom{m}{2}}$. □

The following will be used in Section 5.4.

Lemma 3.7. *The probability that a random $A \in M_n(\mathbb{F}_p)_{\mathrm{alt}}$ satisfies $\dim\ker A \geq n/2$ tends to 0 as $n \to \infty$.*

Proof. Let $k = \lceil n/2 \rceil$. The number of $A \in M_n(\mathbb{F}_p)_{\mathrm{alt}}$ with $\dim\ker A \geq n/2$ is at most the number of pairs (A, K) with $A \in M_n(\mathbb{F}_p)_{\mathrm{alt}}$ and K a k-dimensional subspace of $\ker A$. The number of K's is $O(p^{k(n-k)})$. For each K, the A's vanishing on K correspond to alternating maps from the $(n-k)$-dimensional space $\mathbb{F}_p^n/K$ to its dual, of which there are $p^{(n-k)(n-k-1)/2}$. Thus the total number of A with $\dim\ker A \geq n/2$ is at most

$$O(p^{k(n-k)}) \cdot p^{(n-k)(n-k-1)/2} = O(p^{(n-k)(n+k-1)/2}).$$

Dividing by $\#M_n(\mathbb{F}_p)_{\mathrm{alt}} = p^{n(n-1)/2}$ yields $O(p^{-k(k-1)/2})$, which tends to 0 as $n \to \infty$. □

Remark 3.8. In fact, Lemma 3.7 remains true if $n/2$ is replaced by any function of n tending to ∞, but the $n/2$ version suffices for our application.

3.7. **The distribution in the nonsingular case.** The following theorem states that the limit $\mathscr{A}_0$ in Theorem 1.6(a) exists and gives an explicit formula for its value:

Theorem 3.9. *For each symplectic p-group G, if A is chosen at random in $M_n(\mathbb{Z}_p)_{\mathrm{alt}}$ with respect to Haar measure for even n, then*

$$\lim_{\substack{n\to\infty \\ n \text{ even}}} \mathrm{Prob}\,(\mathrm{coker}\, A \simeq G) = \frac{\#G}{\#\,\mathrm{Sp}(G)} \prod_{i=1}^{\infty}(1-p^{1-2i}).$$

Moreover, the sum of the right side over all such G equals 1.

Proof. Define

$$\pi_n(G) := \mathrm{Prob}\,(\mathrm{coker}\, A \simeq G), \quad \text{and} \quad \pi(G) := \lim_{\substack{n\to\infty \\ n \text{ even}}} \pi_n(G).$$

Let $m = n - \dim_{\mathbb{F}_p} G[p] \in 2\mathbb{Z}_{\geq 0}$. Given a surjection $f\colon \mathbb{Z}_p^n \to G$, we may pull back the pairing on G to obtain an alternating pairing on $\mathbb{Z}_p^n$. This defines a surjection from $\mathrm{Surj}(\mathbb{Z}_p^n, G)$ to the set of alternating pairings $[\ ,\ ]\colon \mathbb{Z}_p^n \times \mathbb{Z}_p^n \to \mathbb{Q}/\mathbb{Z}$ such that the induced S-group is isomorphic to G. Each fiber is the orbit of a free action of $\mathrm{Sp}(G)$ on $\mathrm{Surj}(\mathbb{Z}_p^n, G)$ (by post-composition), so the number of such $[\ ,\ ]$'s is $\#\,\mathrm{Surj}(\mathbb{Z}_p^n, G)/\#\,\mathrm{Sp}(G)$. By Corollary 3.5, the probability that $[\ ,\ ]_A$ equals any fixed one of these $[\ ,\ ]$ equals

$$\frac{\#\,\mathrm{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}}{\#M_m(\mathbb{F}_p)_{\mathrm{alt}}}(\#G)^{1-n}.$$

Multiplying yields

$$\pi_n(G) = \frac{\#\operatorname{Surj}(\mathbb{Z}_p^n, G)}{\#\operatorname{Sp}(G)} \frac{\#\operatorname{GL}_m(\mathbb{F}_p)_{\mathrm{alt}}}{\#M_m(\mathbb{F}_p)_{\mathrm{alt}}} (\#G)^{1-n}. \tag{6}$$

As $n \to \infty$, we have $m \to \infty$ through even integers, and $\#\operatorname{Surj}(\mathbb{Z}_p^n, G)/(\#G)^n \to 1$ since almost all homomorphisms $\mathbb{Z}_p^n \to G$ are surjective, so by Lemma 3.6, we obtain

$$\pi(G) = \frac{\#G}{\#\operatorname{Sp}(G)} \prod_{i=1}^{\infty} (1 - p^{1-2i}).$$

It remains to prove that $\sum_G \pi(G) = 1$. For fixed n, the event that $\operatorname{coker} A$ is infinite corresponds to the $\mathbb{Z}_p$-points of a hypersurface in the affine space of alternating matrices, so Proposition 2.1(b) shows that it has probability 0; thus $\sum_G \pi_n(G) = 1$. By Fatou's lemma, $\sum_G \pi(G) \leq 1$. In particular,

$$\sum_G \frac{\#G}{\#\operatorname{Sp}(G)} \leq \prod_{i=1}^{\infty} (1 - p^{1-2i})^{-1} < \infty.$$

In (6), we have $\#\operatorname{Surj}(\mathbb{Z}_p^n, G) \leq \#G^n$ and $\#\operatorname{GL}_m(\mathbb{F}_p)_{\mathrm{alt}} \leq \#M_m(\mathbb{F}_p)_{\mathrm{alt}}$, so $\pi_n(G) \leq \#G/\#\operatorname{Sp}(G)$; this lets us apply the dominated convergence theorem to deduce

$$\sum_G \pi(G) = \sum_G \lim \pi_n(G) = \lim \sum_G \pi_n(G) = 1. \qquad \square$$

3.8. **The distribution in the singular case.** Fix $n \geq 0$. The variety $\mathbb{A}^{n(n-1)/2}$ parametrizing alternating $n \times n$ matrices over any field can be stratified according to the rank of the matrix. Namely, given an integer r with $0 \leq r \leq n$ and $n - r$ even, let $V_{n,r}$ be the locally closed subvariety parametrizing alternating $n \times n$ matrices of rank $n - r$. (The hypotheses on r are needed to ensure that $V_{n,r}$ is nonempty.) The existence of symplectic bases shows that $V_{n,r}$ is a homogeneous space for the action of GL_n on $\mathbb{A}^{n(n-1)/2}$.

Lemma 3.10. $\dim V_{n,r} = \binom{n}{2} - \binom{r}{2} =: d$.

Proof. Sending a matrix $A \in M_n(k)$ to $\operatorname{im}(A)$ defines a morphism from $V_{n,r}$ to the Grassmannian of $(n-r)$-planes Π in n-space. The fiber above Π parametrizes nondegenerate alternating maps from $k^n/(\operatorname{im} A)^\perp \simeq \operatorname{im}(A)^T$ to $\operatorname{im}(A)$, so each fiber has dimension $\binom{n-r}{2}$. Thus $\dim V_{n,r} = r(n-r) + \binom{n-r}{2} = \binom{n}{2} - \binom{r}{2}$.

Alternatively, one could compute the dimension of the stabilizer of

$$\begin{pmatrix} & I_{(n-r)/2} & \\ -I_{(n-r)/2} & & \\ & & 0_r \end{pmatrix} \in V_{n,r}$$

by writing an equation in 2×2 block matrices with blocks of size $n - r$ and r. $\square$

We have the locally closed stratification

$$\mathbb{A}^{n(n-1)/2} = \bigcup_r V_{n,r},$$

where r ranges over integers with $0 \leq r \leq n$ and $n - r$ even. The Zariski closure $\overline{V}_{n,r}$ of $V_{n,r}$ in $\mathbb{A}^{n(n-1)/2}$ is the locus $\bigcup_{s \geq r} V_{n,s}$ of alternating matrices of rank *at most* $n - r$: this is

closed since it is cut out by the vanishing of the $(n-r+1)\times(n-r+1)$ minors, and it is in the closure of $V_{n,r}$, as one can see from using standard symplectic matrices. We may extend $\overline{V}_{n,r}$ to a closed subscheme of $\mathbb{A}^{n(n-1)/2}_{\mathbb{Z}_p}$ defined by the same equations.

Let $\mathcal{A}_{n,r} = V_{n,r}(\mathbb{Q}_p) \cap M_n(\mathbb{Z}_p)_{\mathrm{alt}}$, so we have an analogous locally closed stratification of topological spaces

$$M_n(\mathbb{Z}_p)_{\mathrm{alt}} = \bigcup_r \mathcal{A}_{n,r}.$$

The closure $\overline{\mathcal{A}}_{n,r}$ of $\mathcal{A}_{n,r}$ equals $\overline{V}_{n,r}(\mathbb{Z}_p) = \bigcup_{s\geq r} \mathcal{A}_{n,s}$.

Fix r. Proposition 2.1 and Corollary 2.2 applied to $X = \overline{V}_{n,r}$ yields measures μ and ν on $\overline{\mathcal{A}}_{n,r}$. By Proposition 2.1(b), $\mu(\overline{\mathcal{A}}_{n,s}) = 0$ for $s > r$, so the probability measure ν restricts to a probability measure ν on the open subset $\mathcal{A}_{n,r}$. We use μ to denote the μ for different varieties; the meaning will be clear from context.

The following generalization of Theorem 3.9 states that the limit $\mathscr{A}_r$ in Theorem 1.6(a) exists for each $r \in \mathbb{Z}_{\geq 0}$ and gives an explicit formula for its value:

Theorem 3.11. *Fix $r \in \mathbb{Z}_{\geq 0}$, and fix a symplectic p-group G. If $A \in \mathcal{A}_{n,r}$ is chosen at random with respect to ν, then*

$$\lim_{\substack{n\to\infty \\ n-r \text{ even}}} \mathrm{Prob}\left((\mathrm{coker}\, A)_{\mathrm{tors}} \simeq G\right) = \frac{(\#G)^{1-r}}{\#\,\mathrm{Sp}(G)} \prod_{i=r+1}^{\infty} (1-p^{1-2i}).$$

Moreover, the sum of the right side over all such G equals 1.

To prove Theorem 3.11, we need the following two lemmas. Let $|\det|^s \colon M_n(\mathbb{Z}_p) \to \mathbb{R}$ be the function $A \mapsto |\det A|_p^s$.

Lemma 3.12. *For any $s \in \mathbb{R}_{\geq 0}$, we have* $\displaystyle\int_{M_n(\mathbb{Z}_p)_{\mathrm{alt}}} |\det|^s \,\mu = \prod_{i=1}^{n/2} \frac{1-p^{1-2i}}{1-p^{1-2i-2s}}.$

Proof. The proof is an easy induction on n: see [Igu00, p. 164]. □

Lemma 3.13. *Define*

$$\begin{aligned} \beta \colon \mathrm{GL}_n(\mathbb{Z}_p) \times \mathcal{A}_{n-r,0} &\longrightarrow \mathcal{A}_{n,r} \\ (M, A) &\longmapsto M^t \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} M. \end{aligned}$$

Then $\beta_*(\mu \times |\det|^r \mu) = c\mu$ for some $c > 0$ depending on n and r.

Proof. Given $B \in M_n(\mathbb{Z}/p^e\mathbb{Z})$ in the reduction of $\mathcal{A}_{n,r}$, we must count the number of $(M, A) \in \mathrm{GL}_n(\mathbb{Z}/p^e\mathbb{Z}) \times M_{n-r}(\mathbb{Z}/p^e\mathbb{Z})_{\mathrm{alt}}$ such that $M^t \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} M = B$. We may assume that e is large enough that some $(n-r)\times(n-r)$ minor of B has nonzero determinant mod p^e. We may assume also that B itself is of the form $\begin{pmatrix} C & 0 \\ 0 & 0 \end{pmatrix}$; then the set of (M, A) is

$$\left\{ (N^{-1}, N^t B N) : N \in \mathrm{GL}_n(\mathbb{Z}/p^e\mathbb{Z}), N^t B N \text{ has the form } \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

If $N = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$, then the condition on N is equivalent to $P \in \mathrm{GL}_{n-r}(\mathbb{Z}/p^e\mathbb{Z})$, $P^tCQ = 0$, $Q^tCP = 0$, and $Q^tCQ = 0$ (invertibility of P follows from comparing determinants of minors of B to those of N^tBN). Since $C^t = -C$, these conditions are equivalent to $P \in \mathrm{GL}_{n-r}(\mathbb{Z}/p^e\mathbb{Z})$ and $CQ = 0$. The number of possibilities for P is $\#\,\mathrm{GL}_{n-r}(\mathbb{Z}/p^e\mathbb{Z})$, which is independent of B. On the other hand, if we view C as a map from the finite group $(\mathbb{Z}/p^e\mathbb{Z})^{n-r}$ to itself, its kernel has the same size as its cokernel, which is $|\det C|_p^{-1}$, so the number of possibilities for Q is $|\det C|_p^{-r}$. Thus if each pair (M, A) is weighted by $|\det A|_p^r = |\det C|_p^r$, then the weighted count of such pairs is independent of B. □

Proof of Theorem 3.11. Define

$$\mathcal{A}_{n,r}(G) := \{A \in \mathcal{A}_{n,r} : (\operatorname{coker} A)_{\mathrm{tors}} \simeq G\}.$$

As $n \to \infty$ through integers with $n - r$ even,

$$\begin{aligned}
\nu(\mathcal{A}_{n,r}(G)) &= \frac{\int_{\mathcal{A}_{n,r}(G)} \mu}{\int_{\mathcal{A}_{n,r}} \mu} \\
&= \frac{\int_{\mathrm{GL}_n(\mathbb{Z}_p)} \mu \cdot \int_{\mathcal{A}_{n-r,0}(G)} |\det|^r \mu}{\int_{\mathrm{GL}_n(\mathbb{Z}_p)} \mu \cdot \int_{\mathcal{A}_{n-r,0}} |\det|^r \mu} \qquad \text{(by Lemma 3.13)} \\
&= \frac{\#G^{-r} \int_{\mathcal{A}_{n-r,0}(G)} \mu}{\int_{\mathcal{A}_{n-r,0}} |\det|^r \mu} \\
&\to \frac{\#G^{-r} \frac{\#G}{\#\,\mathrm{Sp}(G)} \prod_{i=1}^{\infty}(1 - p^{1-2i})}{\prod_{i=1}^{\infty} \frac{1-p^{1-2i}}{1-p^{1-2i-2r}}} \qquad \text{(by Theorem 3.9 and Lemma 3.12)} \\
&= \frac{\#G^{1-r}}{\#\,\mathrm{Sp}(G)} \prod_{i=r+1}^{\infty}(1 - p^{1-2i}).
\end{aligned}$$

The same argument as in the proof of Theorem 3.9 shows that these numbers sum to 1. □

The remainder of this section proves corollaries to be used in Section 5.6. By $\sum_G$ we mean a sum over (isomorphism classes of) symplectic abelian groups. Similarly, $\sum_{\#G \le n}$ or $\sum_{\#G=n}$ indicates a sum over the subset of such G satisfying the condition. Define

$$w_G := \frac{\#G}{\#\,\mathrm{Sp}(G)}.$$

The sum in Theorem 3.11 being 1 implies that

$$\sum_{k=0}^{\infty} \sum_{\#G=p^{2k}} w_G t^k = \prod_{i=1}^{\infty} (1 - p^{1-2i}t)^{-1},$$

holds for $t = p^{-2r}$, so it holds identically in $\mathbb{Q}[[t]]$. Apply the q-binomial theorem to the right side (take $x = p^{-2}$ and $z = pt$ in the expression Z in [Eul48, §313]) and equate coefficients of t^k to obtain

$$\sum_{\#G=p^{2k}} w_G = p^{-k} \prod_{j=1}^{k} (1 - p^{-2j})^{-1},$$

which is equivalent to [Del01, Corollary 6]. Taking the product over the prime powers in the factorization of a positive integer n, and using

$$\prod_{\text{prime powers } m>1 \text{ dividing } n} (1-m^{-2})^{-1} \le \prod_{m=2}^{\infty} (1-m^{-2})^{-1} = 2$$

yields the following.

Corollary 3.14. *For any $n \ge 1$, we have $1/n \le \sum_{\#G=n^2} w_G \le 2/n$.*

Corollary 3.15. *We have $\sum_{\#G\le n} w_G \ge \frac{1}{2}\log n$ and $\sum_{\#G\in[\ell,n]} w_G = O(\log(n/\ell))$.*

4. Orthogonal Grassmannians

4.1. **Grassmannians.** Given $0 \le m \le n$, for each commutative ring A let $\mathrm{Gr}_{m,n}(A)$ be the set of direct summands W of A^n that are locally free of rank m. As is well known, this functor is represented by a smooth projective scheme $\mathrm{Gr}_{m,n}$ of relative dimension $m(n-m)$ over $\mathbb{Z}$, called a Grassmannian.

4.2. **Maximal isotropic direct summands.** Now equip A^{2n} with the hyperbolic quadratic form $Q\colon A^{2n} \to A$ given by

$$Q(x_1,\dots,x_n,y_1,\dots,y_n) := \sum_{i=1}^{n} x_i y_i.$$

The associated bilinear pairing is $\langle a,b\rangle := Q(a+b)-Q(a)-Q(b)$. A direct summand Z is called isotropic if $Q|_Z = 0$ (in general this is stronger than requiring that $\langle\ ,\ \rangle|_{Z\times Z} = 0$). Let $\mathrm{OGr}_n(A)$ be the set of isotropic $Z \in \mathrm{Gr}_{n,2n}(A)$. Such Z will also be called maximal isotropic direct summands of A^{2n}. Let W be the maximal isotropic direct summand $\mathbb{Z}^n \times 0$ of $\mathbb{Z}^{2n}$.

Lemma 4.1. *Let A be a ring. Let $X, X' \in \mathrm{OGr}_n(A)$ be such that $X \oplus X' \to A^{2n}$ is an isomorphism.*

(a) *The restriction of $\langle\ ,\ \rangle$ to $X \times X'$ identifies X' with X^T.*
(b) *Let $\phi\colon X \to X'$ be an A-module homomorphism. Then* $\mathrm{graph}(\phi) \in \mathrm{OGr}_n(A)$ *if and only if ϕ is alternating (with respect to the identification above).*

Proof.

(a) By tensoring with $A/\mathfrak{m}$ for every maximal ideal $\mathfrak{m} \subseteq A$, we reduce to the case in which A is a field. The kernel of $X' \to X^T$ is orthogonal to X, but also to X' since X' is isotropic. By nondegeneracy of $\langle\ ,\ \rangle$ on A^{2n}, this kernel is 0. Since X' and X^T are vector spaces of the same dimension, $X' \to X^T$ is an isomorphism.
(b) For $x \in X$,

$$\langle x, \phi(x)\rangle = Q(x+\phi(x)) - Q(x) - Q(\phi(x)) = Q(x+\phi(x)).$$

By definition, ϕ is alternating if and only if the left side is 0 for all x. Also by definition, $\mathrm{graph}(\phi) \in \mathrm{OGr}_n(A)$ if and only if the right side is 0 for all $x \in X$. □

Proposition 4.2. *Let O_{2n} be the orthogonal group of $(\mathbb{Z}^{2n}, Q)$.*

(a) *Let A be a field, a discrete valuation ring, or a quotient thereof. The action of $\mathrm{O}_{2n}(A)$ on $\mathrm{OGr}_n(A)$ is transitive.*

(b) *Let k be a field. For each $m \in \{0, 1, \dots, n\}$, the action of $\mathrm{O}_{2n}(k)$ on $\{(Y, Z) \in \mathrm{OGr}_n(k)^2 : \dim(Y \cap Z) = m\}$ is transitive.*

Proof.

(a) The hypothesis on A implies that every direct summand of A^{2n} is free. Let $Z \in \mathrm{OGr}_n(A)$. Choose a basis $z_1, \dots, z_n$ of Z. Choose a basis $y_1, \dots, y_n$ for an A-module complement Y of Z in A^{2n}. Since $\langle\ ,\ \rangle$ is nondegenerate, we can change the basis of Y to assume that $\langle y_i, z_j \rangle = \delta_{ij}$. Let $y_i' := y_i - Q(y_i)z_i - \sum_{j>i}\langle y_i, y_j\rangle z_j$. Then the A-linear map sending the standard basis of A^{2n} to $z_1, \dots, z_n, y_1', \dots, y_n'$ is an element of $\mathrm{O}_{2n}(A)$ sending W to Z.

(b) Given (Y, Z) in the set, choose a basis $x_1, \dots, x_m$ for $Y \cap Z$, extend it to bases $x_1, \dots, x_m, z_{m+1}, \dots, z_n$ of Z and $x_1, \dots, x_m, y_{m+1}, \dots, y_n$ of Y, and replace $y_{m+1}, \dots, y_n$ by linear combinations so that $\langle y_i, z_j \rangle = \delta_{ij}$ for $i, j \in [m+1, n]$. Inductively choose $w_i \in k^{2n}$ for $i = 1, \dots, m$ so that w_i is orthogonal to the w_j for $j < i$ and to all the x_j, y_j, z_j except $\langle w_i, x_i \rangle = 1$. Adjust each w_i by a multiple of x_i in order to assume in addition that $Q(w_i) = 0$.

Now, given another pair (Y', Z') in the set, the A-linear map sending the w_i, x_i, y_i, z_i to their counterparts is an element of $\mathrm{O}_{2n}(A)$ sending (Y, Z) to (Y', Z'). □

Lemma 4.3. *Let $\overline{W} \in \mathrm{OGr}_n(\mathbb{F}_p)$ be the mod p reduction of W. Let $Y \le \overline{W}$ be an $\mathbb{F}_p$-subspace. Then the subgroup of $\mathrm{O}_{2n}(\mathbb{Z}_p)$ preserving W and Y acts transitively on $\{X \in \mathrm{OGr}_n(\mathbb{F}_p) : X \cap \overline{W} = Y\}$.*

Proof. For any X, X' in the set, Proposition 4.2(b) yields an element $\bar\alpha \in \mathrm{O}_{2n}(\mathbb{F}_p)$ sending $(\overline{W}, X)$ to $(\overline{W}, X')$. It remains to lift $\bar\alpha \in \mathrm{Stab}_{\mathrm{O}_{2n}(\mathbb{F}_p)}(\overline{W})$ to an element $\alpha \in \mathrm{Stab}_{\mathrm{O}_{2n}(\mathbb{Z}_p)}(W)$, since such an α will preserve also $X \cap \overline{W} = X' \cap \overline{W} = Y$. By Hensel's lemma, the lift exists if the group scheme stabilizer $S \le \mathrm{O}_{2n}$ of W is smooth over $\mathbb{Z}$. In fact, if we define $W' := 0 \times \mathbb{Z}^n \in \mathrm{OGr}_n(\mathbb{Z})$, then there is a short exact sequence of group schemes

$$1 \to B \to S \to \mathrm{GL}_W \to 1$$

where B is the additive group scheme of alternating maps $\beta\colon W' \to W$; namely, $\beta \in B$ maps to the unique $s \in S$ such that $s(w') = w' + \beta(w')$ for all $w' \in W'$, and $S \to \mathrm{GL}_W$ is defined by the action of S on W. Since B and GL_W are smooth, so is S. □

4.3. **Orthogonal Grassmannians.**

Proposition 4.4. *For each $n \ge 0$, the functor OGr_n is represented by a smooth projective scheme of relative dimension $n(n-1)/2$ over $\mathbb{Z}$, called an* orthogonal Grassmannian.

Proof. See [SGA 7_{II}, XII, Proposition 2.8], where OGr_n is denoted Gén(X). The expression for the relative dimension arises in the proof there as the rank of $\bigwedge^2 W$. □

If $V \simeq A^{2n}$ for some ring A, also write OGr_V for the A-scheme $\mathrm{OGr}_{n,A}$.

Proposition 4.5. *Fix $n > 0$.*

(a) *The scheme OGr_n is a disjoint union of two isomorphic schemes $\mathrm{OGr}_n^{\mathrm{even}}$ and $\mathrm{OGr}_n^{\mathrm{odd}}$, distinguished by the property that for $Z \in \mathrm{OGr}_n(k)$ for a field k,*

$$Z \in \mathrm{OGr}_n^{\mathrm{even}}(k) \iff \dim(Z \cap W_k) \text{ is even.} \tag{7}$$

(b) *If k is a field, then $\mathrm{OGr}_{n,k}^{\mathrm{even}}$ and $\mathrm{OGr}_{n,k}^{\mathrm{odd}}$ are geometrically integral.*

(c) *For any field k, two points $Z, Z' \in \mathrm{OGr}_n(k)$ belong to the same component of $\mathrm{OGr}_{n,k}$ if and only if $\dim(Z \cap Z') \equiv n \pmod 2$.*

Proof. See the proof of [SGA 7_{II}, XII, Proposition 2.8], which shows that there is a morphism $e\colon \mathrm{OGr}_n \to \mathrm{Spec}(\mathbb{Z}\times\mathbb{Z})$ with geometrically connected fibers. Define $\mathrm{OGr}_n^{\mathrm{even}}$ and $\mathrm{OGr}_n^{\mathrm{odd}}$ as the preimages of the components of $\mathrm{Spec}(\mathbb{Z}\times\mathbb{Z})$; they can be chosen so that (7) and (c) hold, by [SGA 7_{II}, XII, Proposition 1.12]. Geometrically connected and smooth imply geometrically integral. □

Remark 4.6. For $n=0$, we may define $\mathrm{OGr}_0^{\mathrm{even}} := \mathrm{OGr}_0$ and $\mathrm{OGr}_0^{\mathrm{odd}} := \emptyset$.

Corollary 4.7. *If $Z_1, Z_2, Z_3 \in \mathrm{OGr}_n(k)$ for a field k, then*

$$\dim(Z_1\cap Z_2)+\dim(Z_2\cap Z_3)+\dim(Z_3\cap Z_1)\equiv n \pmod 2.$$

Proof. By Proposition 4.5(c), the parity of $\dim(Z_1\cap Z_2)-n$ measures whether Z_1 and Z_2 belong to the same component. Summing three such integers gives the parity of the number of component switches in hopping from Z_1 to Z_2 to Z_3 and back to Z_1; the latter number is even. □

Lemma 4.8. *Let $q=p^e$ for a prime p and $e\geq 1$. Then*

$$\#\,\mathrm{OGr}_n(\mathbb{Z}/q\mathbb{Z}) = q^{n(n-1)/2}\prod_{i=1}^{n}(1+p^{i-n}).$$

Proof. The case $e=1$ is [PR12, Proposition 2.6(b)]. The $e=1$ case implies the general case since OGr_n is smooth of relative dimension $n(n-1)/2$. □

4.4. **Schubert subschemes.** Suppose that $0\leq r\leq n$. For a field k, let $\mathcal{S}_{n,r}(k)$ be the set of $Z\in \mathrm{OGr}_n^{\mathrm{parity}(r)}(k)$ such that $\dim(Z\cap W_k)\geq r$, or equivalently, the set of $Z\in\mathrm{OGr}_n(k)$ such that $\dim(Z\cap W_k)-r\in 2\mathbb{Z}_{\geq 0}$. For an arbitrary ring R, let $\mathcal{S}_{n,r}(R)$ be the set of $Z\in\mathrm{OGr}_n(R)$ such that $Z_k\in\mathcal{S}_{n,r}(k)$ for every field k that is a quotient of R.

Proposition 4.9. *For $0\leq r\leq n$, the functor $\mathcal{S}_{n,r}$ is represented by a closed subscheme of OGr_n of relative dimension $n(n-1)/2-r(r-1)/2=(n-r)(n+r-1)/2$ over $\mathbb{Z}$.*

Proof. There is a closed subscheme of $\mathrm{Gr}_{n,2n}$ whose k-points parametrize n-dimensional subspaces Z with $\dim(Z\cap W)\geq r$. Its intersection with the closed subscheme $\mathrm{OGr}_n^{\mathrm{parity}(r)}$ is $\mathcal{S}_{n,r}$.

To compute the relative dimension, we work over a field k, and consider the closed subscheme $\mathcal{S}'_{n,r}\subseteq\mathcal{S}_{n,r}\times\mathrm{Gr}_{r,n}$ parametrizing pairs (Z,X) such that $X\subseteq Z\cap W$. Given $X\subseteq W$, the quadratic form Q restricts to a hyperbolic quadratic form on $X^\perp/X$, and the Z's containing X are in bijection with the maximal isotropic subspaces of $X^\perp/X$, via $Z\mapsto Z/X$. Thus the second projection $\mathcal{S}'_{n,r}\to\mathrm{Gr}_{r,n}$ has fibers isomorphic to OGr_{n-r}, so

$$\dim\mathcal{S}'_{n,r}=\dim\mathrm{Gr}_{r,n}+\dim\mathrm{OGr}_{n-r}=r(n-r)+(n-r)(n-r-1)/2=(n-r)(n+r-1)/2.$$

On the other hand, there is an open subscheme $\mathcal{S}^\circ_{n,r}\subseteq\mathcal{S}_{n,r}$ above which $\mathcal{S}'_{n,r}\to\mathcal{S}_{n,r}$ is an isomorphism, namely the subscheme parametrizing Z for which $\dim(Z\cap W)$ *equals* r. If we view $\mathcal{S}^\circ_{n,r}$ as an open subscheme of $\mathcal{S}'_{n,r}$, which maps to $\mathrm{Gr}_{r,n}$, then its fiber above X is the open subscheme of $\mathrm{OGr}_{X^\perp/X}$ consisting of subspaces Y not meeting W/X, and those subspaces are exactly the graphs of alternating maps from an $(n-r)$-dimensional space to its dual, so the fiber is $\mathbb{A}^{(n-r)(n-r-1)/2}$. It follows that $\mathcal{S}^\circ_{n,r}$ has the same dimension as $\mathcal{S}'_{n,r}$. Since $\mathcal{S}_{n,r}$ is sandwiched in between, it too has the same dimension. □

Call $\mathcal{S}_{n,r}$ a Schubert subscheme. It could also have been defined as the closure of the locally closed subscheme $\mathcal{S}^\circ_{n,r} \subseteq \mathrm{OGr}_n$.

5. Modeling Selmer groups using maximal isotropic submodules

5.1. **Properties of the short exact sequence.** Let Z and W be maximal isotropic direct summands of V as in Section 1.2. (For the time being, they do not need to be random; what we say here applies to any choice of Z and W.) From Z and W construct

$$0 \to R \to S \to T \to 0$$

as in Section 1.2.

Proposition 5.1. *The maximal divisible subgroup of S is R.*

Proof. Since the group $R = (Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ is divisible, it suffices to show that every infinitely divisible element a of S is in R. Suppose that $a \in S$ is infinitely divisible. For each $m \geq 1$, write $a = p^m a_m$ for some $a_m \in S$. By definition of S, we have $a_m = (z_m \bmod V) = (w_m \bmod V)$ for some $z_m \in Z \otimes \mathbb{Q}_p$ and $w_m \in W \otimes \mathbb{Q}_p$. Choose n such that $a \in p^{-n}V$; then all the $p^m z_m$ and $p^m w_m$ lie in $p^{-n}V$, which is compact, so there is an infinite subsequence of m such that the $p^m z_m$ converge and the $p^m w_m$ converge. The limits must be equal, since $p^m z_m - p^m w_m \in p^m V$. The common limit in $(Z \cap W) \otimes \mathbb{Q}_p$ represents a. □

Corollary 5.2. *The group T is finite.*

Proof. The maximal divisible subgroup of a $\mathbb{Z}_p$-module with finitely generated Pontryagin dual is of finite index. □

Corollary 5.3. *The exact sequence $0 \to R \to S \to T \to 0$ splits.*

Proof. This follows since R is divisible. □

Proposition 5.4. *If q is a power of p, then $S[q]$ is isomorphic to the intersection $Z/qZ \cap W/qW$ in V/qV.*

Proof. Intersecting

$$S = \left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)$$

with the q-torsion subgroup $\frac{1}{q}V/V$ of $V \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ yields

$$S[q] = \frac{\frac{1}{q}Z}{Z} \cap \frac{\frac{1}{q}W}{W}.$$

The multiplication by q isomorphism $\frac{1}{q}V/V \to V/qV$ sends this to $Z/qZ \cap W/qZ$. □

5.2. **Model for the Cassels–Tate pairing.** Here we define a natural nondegenerate alternating pairing on T. Extend Q to a quadratic form $V \otimes \mathbb{Q}_p \to \mathbb{Q}_p$ and define $\langle\ ,\ \rangle\colon (V \otimes \mathbb{Q}_p) \times (V \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ by $\langle x, y\rangle := Q(x+y) - Q(x) - Q(y)$. Then $\langle\ ,\ \rangle \bmod \mathbb{Z}_p$ identifies $V \otimes \mathbb{Q}_p$ with its Pontryagin dual, and the subgroup

$$Z^\perp := \{v \in V \otimes \mathbb{Q}_p : \langle v, z\rangle \bmod \mathbb{Z}_p = 0 \text{ for all } z \in Z\}$$

equals $Z \otimes \mathbb{Q}_p + V$. Similarly, $W^\perp = W \otimes \mathbb{Q}_p + V$.

Suppose that $x, y \in T$. Lift x to $\widetilde{x} \in \left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)$. Choose $z_x \in Z \otimes \mathbb{Q}_p$ whose image in $V \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ equals $\widetilde{x}$. Define w_x, $\widetilde{y}$, z_y, and w_y analogously.

Proposition 5.5. *The map*

$$\begin{aligned}[\, , \,]\colon T \times T &\to \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \\ x, y &\mapsto Q(z_x - w_y) \bmod \mathbb{Z}_p\end{aligned}$$

is well-defined, and it is a nondegenerate alternating bilinear pairing.

Proof. First,

$$z_x - w_x \in \ker\left(V \otimes \mathbb{Q}_p \to V \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) = V.$$

Since Z and W are isotropic,

$$Q(z_x - w_y) = -\langle z_x, w_y\rangle = -\langle z_x - w_x, w_y\rangle,$$

so changing w_y (by an element of W) changes $Q(z_x - w_y)$ by an element of $\langle V, W\rangle \subseteq \mathbb{Z}_p$, so $Q(z_x - w_y) \bmod \mathbb{Z}_p$ is unchanged. Similarly, changing z_x (by an element of Z) does not change $Q(z_x - w_y) \bmod \mathbb{Z}_p$. If $\widetilde{x} = \widetilde{y}$, then we may choose $w_y = w_x$, so $Q(z_x - w_y) = Q(z_x - w_x) \in Q(V) \subseteq \mathbb{Z}_p$, so $Q(z_x - w_y) \bmod \mathbb{Z}_p = 0$. Thus we have an alternating bilinear pairing on $\left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)$ and it remains to show that the kernel on either side is $(Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ so that it induces a nondegenerate alternating pairing on T.

The following are equivalent for $\widetilde{x} \in \left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)$:

- $Q(z_x - w_y) \bmod \mathbb{Z}_p = 0$ for all $\widetilde{y} \in \left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)$,
- $\langle z_x - w_x, w_y\rangle \in \mathbb{Z}_p$, for all $\widetilde{y} \in \left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)$,
- $\langle z_x - w_x, w\rangle \in \mathbb{Z}_p$, for all $w \in (Z \otimes \mathbb{Q}_p + V) \cap (W \otimes \mathbb{Q}_p + V) = Z^\perp \cap W^\perp$,
- $z_x - w_x \in (Z^\perp \cap W^\perp)^\perp = Z + W$, and
- $\widetilde{x} \in (Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. □

5.3. **Predictions for rank.** Corollary 2.2 defines a probability measure on $\mathrm{OGr}_n(\mathbb{Z}_p)$.

Proposition 5.6. *Fix n. If Z is chosen randomly from $\mathrm{OGr}_n(\mathbb{Z}_p)$, then the $\mathbb{Z}_p$-module $Z \cap W$ is free of rank 0 or 1, with probability 1/2 each.*

Proof. By Proposition 4.9, $\dim \mathcal{S}_{n,r} < \dim \mathrm{OGr}_n$ for $r \geq 2$, so the probability that $\mathrm{rk}(Z \cap W) \geq 2$ is 0 by Proposition 2.1(b). On the other hand, $\mathrm{OGr}_n^{\mathrm{even}}$ and $\mathrm{OGr}_n^{\mathrm{odd}}$ are isomorphic by Proposition 4.5(a), so the parity of $\mathrm{rk}(Z \cap W)$ is equidistributed. □

Conjecture 1.1 implies that the distribution of $E(k) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ matches that of $(Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$, or equivalently that the distribution of $E(k) \otimes \mathbb{Z}_p$ matches that of $Z \cap W$. Thus it implies that 50% of elliptic curves over k have rank 0, and 50% have rank 1.

5.4. **Random models and their compatibility.** One can show that the locus of $Z \in \mathrm{OGr}_n(\mathbb{Z}_p)$ for which the sequence $0 \to R \to S \to T \to 0$ is isomorphic to a given sequence is locally closed in the p-adic topology, and hence measurable. This would show that $\mathscr{Q}_{2n}$ is well-defined. A similar argument using the probability measure on $\mathcal{S}_{n,r}(\mathbb{Z}_p)$ would show that $\mathscr{T}_{2n,r}$ is well-defined. We find it more convenient, however, to prove these measurability claims and to prove that $\lim_{n\to\infty} \mathscr{Q}_{2n}$ and $\lim_{n\to\infty} \mathscr{T}_{2n,r}$ exist by relating them to the distributions $\mathscr{A}_{n,r}$. Recall that we already proved in Section 3.8 that the $\mathscr{A}_{n,r}$ exist and converge to a limit $\mathscr{A}_r$ as $n \to \infty$ through integers with $n - r \in 2\mathbb{Z}_{\geq 0}$.

Before giving the proof that the limit $\lim_{n\to\infty} \mathscr{T}_{2n,r} =: \mathscr{T}_r$ exists and coincides with $\mathscr{A}_r$ (Theorem 1.6(b)), let us explain the idea. There is a simple relationship between alternating matrices A and maximal isotropic direct summands Z: namely, if we view A as a linear map $W \to W^T$, then $Z := \mathrm{graph}(A) \subset W \oplus W^T$ is maximal isotropic. But not every maximal isotropic direct summand $Z \leq W \oplus W^T$ comes from an A. Over a field, the Z's that arise are those that intersect W^T trivially; at the other extreme is W^T itself; a general Z is a hybrid of these two extremes: namely, they arise by writing $W = W_1 \oplus W_2$, forming the corresponding decomposition $W^T = W_1^T \oplus W_2^T$, and taking $Z := W_1^T \oplus \mathrm{graph}(A)$ for some alternating $A\colon W_2 \to W_2^T$. We need to work over $\mathbb{Z}_p$ instead of a field, but we can still represent a general Z in terms of a decomposition as above (note, however, that the Z's that arise directly from an A on the whole of W are those for which the *mod p reductions* of Z and W^T intersect trivially). Moreover, we will show that the uniform distribution of $Z \in \mathcal{S}_{n,r}$ can be obtained by choosing the decompositions of W and W^T at random (with respect to a suitable measure) and then choosing $A\colon W_2 \to W_2^T$ at random from those alternating maps whose kernel has rank r. The distribution $\mathscr{T}_{2n,r}$ is defined in terms of the group T arising from Z. It turns out that $T \simeq (\mathrm{coker}\, A)_{\mathrm{tors}}$, and one shows that with high probability as $n \to \infty$, the size of A is large, so the distribution of $(\mathrm{coker}\, A)_{\mathrm{tors}}$ is well approximated by $\mathscr{A}_r$.

Proof of Theorem 1.6(b). We use the notation $\overline{V} := V/pV$. Fix a maximal isotropic $\mathbb{F}_p$-subspace $\Lambda \leq \overline{V}$ with respect to the $\mathbb{F}_p$-valued quadratic form (Q mod p) such that $\Lambda \cap \overline{W} = 0$ in $\overline{V}$. Define a distribution $\mathscr{G}$ on submodules $Z \leq V$ as follows:

1. Choose a maximal isotropic direct summand $W^T \leq V$ at random conditioned on $\overline{W^T} = \Lambda$. (Then $\langle\ ,\ \rangle|_{W\times W^T}$ is nondegenerate mod p, so it identifies W^T with the $\mathbb{Z}_p$-dual of W, so the name W^T makes sense. Also, $V = W \oplus W^T$.)
2. Choose $m \in \{0, 1, \ldots, n-r\}$ at random so that its distribution matches the distribution of $\dim(\overline{\mathcal{Z}} \cap \Lambda)$ for $\mathcal{Z}$ chosen from $\mathcal{S}_{n,r}(\mathbb{Z}_p)$. The scheme $\mathcal{S}_{n,r}$ is contained in $\mathrm{OGr}_n^{\mathrm{parity}(r)}$, so $\dim(\overline{\mathcal{Z}} \cap \overline{W}) \equiv r \pmod 2$. Corollary 4.7 applied to $(\mathcal{Z}, \overline{W}, \Lambda)$ implies that $m + r \equiv n \pmod 2$.
3. Choose a random $\mathbb{Z}_p$-module decomposition of W as $W_1 \oplus W_2$ such that $\mathrm{rk}\, W_1 = m$. Let $W^T = W_1^T \oplus W_2^T$ be the induced decomposition of W^T; i.e., W_2^T is the annihilator of W_1 with respect to $\langle\ ,\ \rangle|_{W\times W^T}$, and W_1^T is the annihilator of W_2. (Then W_i^T is isomorphic to the $\mathbb{Z}_p$-dual of W_i for $i = 1, 2$.)
4. Choose an alternating $\mathbb{Z}_p$-linear map $A\colon W_2 \to W_2^T$ at random from maps whose kernel has rank r (since $\mathrm{rk}\, W_2 = n - m \equiv r \pmod 2$, the set of such A is nonempty). Let $\mathrm{graph}(A) \leq W_2 \times W_2^T$ be its graph. Let $Z = W_1^T \oplus \mathrm{graph}(A)$.

Since A is alternating, the direct summand $\mathrm{graph}(A)$ of V is isotropic. Since $W_1^T \le W^T$, the direct summand W_1^T is isotropic. Under $\langle\ ,\ \rangle|_{W\times W^T}$, the direct summand W_1^T annihilates W_2^T (since both are contained in W^T) and W_2 (by definition). The previous three sentences show that Z is an isotropic direct summand. Its rank is $\operatorname{rk} W_1^T + \operatorname{rk} W_2 = \operatorname{rk} W_1 + \operatorname{rk} W_2 = n$, so Z is a maximal isotropic direct summand.

Reducing modulo p yields

$$\overline{Z} = \overline{W_1^T} \oplus \mathrm{graph}(\overline{A}),$$

so in $\overline{V}$ we have

$$\overline{Z} \cap \Lambda = \overline{Z} \cap \overline{W^T} = \overline{W_1^T},$$

which is of $\mathbb{F}_p$-dimension m.

Claim: *$\mathscr{G}$ coincides with the uniform distribution on $\mathcal{S}_{n,r}$.* Both distributions assign the uniform measure to the set of maximal isotropic direct summands Z with $\dim(Z \cap W) = r$ having a fixed mod p reduction $\overline{Z}$, so it suffices to show that the distributions of $\overline{Z}$ match. For each m, both distributions for $\overline{Z}$ are uniform over all maximal isotropic subspaces of $\overline{V}$ for which $\dim(\overline{Z} \cap \overline{W}) \ge r$ and $\dim(\overline{Z} \cap \Lambda) = m$, so it suffices to prove that the distribution of the integer $\dim(\overline{Z} \cap \Lambda)$ is the same for both distributions. The latter holds by the choice of m. This proves the claim.

For Z sampled from $\mathscr{G}$, the definition of Z yields

$$\left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) = \mathrm{graph}\left(A \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \simeq \ker\left(A \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right),$$

whose Pontryagin dual is $\operatorname{coker} A$. The quotient T of the left side by its maximal divisible subgroup $(Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ is dual to the finite group $(\operatorname{coker} A)_{\mathrm{tors}}$, hence isomorphic to $(\operatorname{coker} A)_{\mathrm{tors}}$. Thus the distribution $\mathscr{T}_{2n,r}$ of T is a weighted average over m of the distribution $\mathscr{A}_{n-m,u}$ of $(\operatorname{coker} A)_{\mathrm{tors}}$ for $A \in \mathcal{A}_{n-m,u}$; this proves in particular that $\mathscr{T}_{2n,r}$ is well-defined.

We next show that as $n \to \infty$, the probability that m is small, say less than $n/2$, tends to 1. In fact, we show that this holds even after conditioning on the intersection $\overline{\mathcal{Z}} \cap \overline{W}$; i.e., we will prove that

$$\inf_Y \mathrm{Prob}\left(m < n/2 \mid \overline{\mathcal{Z}} \cap \overline{W} = Y\right) \to 1$$

as $n \to \infty$, where Y ranges over the possibilities for $\overline{\mathcal{Z}} \cap \overline{W}$. Fix Y. Let $y := \dim Y$. Since $m + y \le \dim \overline{\mathcal{Z}} = n$, the probability is 1 if $y > n/2$, so assume that $y \le n/2$. The subgroup of $\mathrm{O}_{2n}(\mathbb{Z}_p)$ preserving W and Y acts transitively on the maximal isotropic subspaces $\overline{\mathcal{Z}}$ of $\mathbb{F}_p^{2n}$ satisfying $\overline{\mathcal{Z}} \cap \overline{W} = Y$, by Lemma 4.3, so the distribution of $\overline{\mathcal{Z}}$ is uniform among such subspaces. Thus $\overline{\mathcal{Z}}/Y$ is a uniformly random maximal isotropic subspace of $Y^\perp/Y$ intersecting $\overline{W}/Y$ trivially. In $Y^\perp/Y$, the image of $\Lambda \cap Y^\perp$ is a maximal isotropic complement C of $\overline{W}/Y$, so $\overline{\mathcal{Z}}/Y$ is the graph of a uniformly random alternating map $B\colon C \to \overline{W}/Y$ (see Lemma 4.1(b)). Then $m = \dim\ker B$. By Lemma 3.7, $m < (n-y)/2$ with high probability, so $m < n/2$ with high probability.

So the size $n - m$ of the matrix A is large with high probability, and we have already seen that $n - m \equiv r \pmod 2$. Thus the weighted average converges as $n \to \infty$ to $\mathscr{A}_r$. In other words, $\mathscr{T}_r$ exists and coincides with $\mathscr{A}_r$. □

Proposition 5.7. *The distribution $\mathscr{Q} = \lim_{n\to\infty} \mathscr{Q}_{2n}$ exists.*

Proof. Define a new distribution $\mathscr{Q}'_{2n}$ on short exact sequences as follows. Choose $r \in \{0,1\}$ uniformly at random, and let $R = (\mathbb{Q}_p/\mathbb{Z}_p)^r$. Choose T with respect to the distribution $\mathscr{T}_{2n,r}$. Form the exact sequence

$$0 \longrightarrow R \longrightarrow R \oplus T \longrightarrow T \to 0.$$

By Proposition 5.6 and Corollary 5.3, the distribution $\mathscr{Q}_{2n}$ coincides with $\mathscr{Q}'_{2n}$; in particular, it is well-defined.

For each r, the distribution $\mathscr{T}_{2n,r}$ tends to a limit as $n \to \infty$, so the same is true of $\mathscr{Q}'_{2n} = \mathscr{Q}_{2n}$. □

5.5. **Predictions for** Sel_{p^e}**.**

Lemma 5.8. *Fix a global field k. Asymptotically 100% of elliptic curves over k satisfy $E(k)_{\mathrm{tors}} = 0$.*

Proof. For each global field k and prime p, the theory of modular curves and Igusa curves shows that the generic elliptic curve (over $k(a_1, a_2, a_3, a_4, a_6)$) has no nonzero rational p-torsion point. By the Hilbert irreducibility theorem, the same holds for asymptotically 100% of elliptic curves over k. The size of the torsion subgroup is bounded by a constant depending only on k [Lev68, Maz77, KM95, Mer96], so we need consider only finitely many p. Thus 100% of $E \in \mathscr{E}$ satisfy $E(k)_{\mathrm{tors}} = 0$. □

Remark 5.9. One could also prove Lemma 5.8 without using [Mer96]: the torsion subgroup can also be controlled by using reduction modulo primes.

Proposition 5.10. *Suppose that E is an elliptic curve over a global field k with $E(k)_{\mathrm{tors}} = 0$. Let m and n be positive integers such that* $\mathrm{char}\, k \nmid m, n$ *and $m|n$. Then*

(a) *The inclusion $E[m] \to E[n]$ induces an isomorphism $\mathrm{H}^1(k, E[m]) \to \mathrm{H}^1(k, E[n])[m]$.*
(b) *This isomorphism identifies $\mathrm{Sel}_m E$ with $(\mathrm{Sel}_n E)[m]$.*
(c) *If p is a prime number and $e \in \mathbb{Z}_{\geq 0}$, then $\mathrm{Sel}_{p^e} E \simeq (\mathrm{Sel}_{p^\infty} E)[p^e]$.*

Proof.

(a) Taking cohomology of $0 \to E[m] \to E[n] \xrightarrow{m} E[n/m] \to 0$ yields a homomorphism α fitting into the exact sequence

$$0 \to \mathrm{H}^1(k, E[m]) \to \mathrm{H}^1(k, E[n]) \xrightarrow{\alpha} \mathrm{H}^1(k, E[n/m]).$$

Replacing m by n/m shows that $E[n/m] \hookrightarrow E[n]$ induces an injection $\mathrm{H}^1(k, E[n/m]) \to \mathrm{H}^1(k, E[n])$. The composition $E[n] \xrightarrow{m} E[n/m] \hookrightarrow E[n]$ induces a composition $\mathrm{H}^1(k, E[n]) \xrightarrow{\alpha} \mathrm{H}^1(k, E[n/m]) \hookrightarrow \mathrm{H}^1(k, E[n])$ that equals multiplication by m, so $\mathrm{H}^1(k, E[m]) \simeq \ker \alpha \simeq \mathrm{H}^1(k, E[n])[m]$.

(b) An element of $\mathrm{H}^1(k, E[m])$ lies in the subgroup $\mathrm{Sel}_m E$ if and only if its image in $\mathrm{H}^1(k, E[n])$ lies in $\mathrm{Sel}_n E$, since the condition for either is that it map to 0 in $\mathrm{H}^1(k_v, E)$ for every v.

(c) Apply (b) to $p^e | p^n$ and take the direct limit as $n \to \infty$. □

Let $q = p^e$ for some prime p and $e \geq 0$. Because of Propositions 5.4 and 5.10(c), Conjecture 1.1 implies that the distribution of $\mathrm{Sel}_q E$ is the limit as $n \to \infty$ of the distribution of $Z \cap W$ for random $Z, W \in \mathrm{OGr}_n(\mathbb{Z}/q\mathbb{Z})$. Taking $q = p$, we recover [PR12, Conjecture 1.1(a)].

Theorem 5.11. *Fix $m \in \mathbb{Z}_{\geq 0}$. If $Z, W \in \mathrm{OGr}_n(\mathbb{Z}/q\mathbb{Z})$ are chosen at random, then the expected number of injective homomorphisms $(\mathbb{Z}/q\mathbb{Z})^m \to Z \cap W$ tends to $q^{m(m+1)/2}$ as $n \to \infty$.*

Proof. For each n, we may fix W. The desired number is the number of injective homomorphisms $h\colon (\mathbb{Z}/q\mathbb{Z})^m \to W$ times the probability that a random $Z \in \mathrm{OGr}_n(\mathbb{Z}/q\mathbb{Z})$ contains $\mathrm{im}(h)$. The number of h's is $(\#W)^m \prod_{i=0}^{m-1}(1-q^{i-n})$. The Z's containing $\mathrm{im}(h)$ correspond to the maximal isotropic direct summands of $\mathrm{im}(h)^\perp/\mathrm{im}(h)$, a hyperbolic quadratic $\mathbb{Z}/q\mathbb{Z}$-module of rank $2n-2m$, so their number is $\#\,\mathrm{OGr}_{n-m}(\mathbb{Z}/q\mathbb{Z})$. Using Lemma 4.8, we compute

$$(\#W)^m \prod_{i=0}^{m-1}(1-p^{i-n})\frac{\#\,\mathrm{OGr}_{n-m}(\mathbb{Z}/q\mathbb{Z})}{\#\,\mathrm{OGr}_n(\mathbb{Z}/q\mathbb{Z})} = q^{m(m+1)/2}\prod_{i=0}^{m-1}(1-p^{i-n})\prod_{i=n-m}^{n-1}(1+p^{-i}),$$

which tends to $q^{m(m+1)/2}$ as $n \to \infty$. □

Combining Conjecture 1.1 and Theorem 5.11 yields the prediction that the expected number of injective homomorphisms $(\mathbb{Z}/q\mathbb{Z})^m \to \mathrm{Sel}_q E$ as E varies over $\mathscr{E}$ is $q^{m(m+1)/2}$.

Remark 5.12. Suppose that q is a prime p. By [PR12, Proposition 2.22(a)], the m^{th} moment of $\#(Z \cap W)$ equals $\prod_{i=1}^{m}(p^i+1)$. Theorem 5.11 lets us compute this moment in another way, as the expected number of homomorphisms $(\mathbb{Z}/p\mathbb{Z})^m \to G$, injective or not, by summing over the possibilities for the kernel.

One could also compute the moments for non-prime q, but the answers appear to be complicated. See [DJ13a] for an analogous calculation of the conjectural moments of $\#Ш[p^e]$.

Remark 5.13. For $q = 2$ and $m = 1$, the result of Theorem 5.11 can be related to the Tamagawa number $\tau(\mathrm{PGL}_2) = 2$. (See [BS10] and [Poo12].) Is there a Tamagawa number explanation for all q and m?

5.6. **Considering all p-primary parts at once.** Let $\mathrm{Sel}\, E := \varinjlim_n \mathrm{Sel}_n E$ be the direct limit over all $n \in \mathbb{Z}_{>0}$, ordered by divisibility, so $\mathrm{Sel}\, E \simeq \bigoplus_p \mathrm{Sel}_{p^\infty} E$. It fits in an exact sequence

$$0 \longrightarrow E(k) \otimes \frac{\mathbb{Q}}{\mathbb{Z}} \longrightarrow \mathrm{Sel}\, E \longrightarrow Ш \longrightarrow 0$$

of discrete $\widehat{\mathbb{Z}}$-modules (i.e., torsion abelian groups). The p-primary parts of this sequence should not be completely independent, because if Ш is finite, then the $\mathbb{Z}_p$-corank of the p-primary part $\mathrm{Sel}_{p^\infty} E$ of $\mathrm{Sel}\, E$ is independent of p.

Therefore we condition on the rank r, in which case we need only focus on the model for Ш. Here is our model: independently for each prime p, choose a finite symplectic abelian p-group T_p with respect to $\mathscr{T}_r$ (or equivalently $\mathscr{A}_r$, by Theorem 1.6(b)), and define $T := \bigoplus_p T_p$.

Theorem 5.14. *If $r \geq 1$, then the group T above is finite with probability 1, and has the distribution of* [Del01, Heuristic Assumption]*, with the correction that $r/2$ is replaced by r.*

Proof. By Theorem 3.11 for $G = 0$,

$$\mathrm{Prob}(T_p \neq 0) = 1 - \prod_{i=r+1}^{\infty}(1-p^{1-2i}) = O(p^{-1-2r}).$$

If $r \geq 1$, then $\sum_p \mathrm{Prob}(T_p \neq 0)$ converges, so the Borel–Cantelli lemma implies that $T_p = 0$ for all but finitely p with probability 1, so T is finite with probability 1. The probability that T is isomorphic to a given symplectic abelian group G is the (convergent) product over p of the probability that $T_p \simeq G[p^\infty]$. Since the formula in [Del01, Heuristic Assumption] is multiplicative on p-primary parts, the result follows. □

For the rest of this section, assume that $r = 0$. Then $\sum_p \mathrm{Prob}(T_p \neq 0)$ diverges, and the probability that T is isomorphic to any particular finite abelian group is 0, so we do not obtain a discrete probability distribution on finite abelian groups. This situation is similar to that for class groups of imaginary quadratic fields: the density of such fields having a specified class group is 0.

Following [Del01], however, we can measure the probability of certain infinite sets of isomorphism classes of symplectic abelian groups, or more generally, compute the average of certain functions f defined on such isomorphism classes. Let $\mathscr{E}_{0,<X}$ be the set of $E \in \mathscr{E}_0$ of height less than X. Let $\sum_{\#G \leq n}$ have the same meaning as at the end of Section 3.8. For $k = \mathbb{Q}$, Delaunay [Del01, Heuristic Assumption], inspired by the Cohen–Lenstra heuristics for class groups of imaginary quadratic fields [CL84], proposed the heuristic

$$\lim_{X \to \infty} \frac{\sum_{E \in \mathscr{E}_{0,<X}} f(Ш(E))}{\sum_{E \in \mathscr{E}_{0,<X}} 1} \stackrel{?}{=} \lim_{n \to \infty} \frac{\sum_{\#G \leq n} f(G) w_G}{\sum_{\#G \leq n} w_G}. \tag{8}$$

Some hypotheses on f are necessary since one can construct wildly oscillating functions f for which even the "easy" limit on the right side of (8) fails to exist. Fix a set of primes P such that $\sum_{p \in P} 1/p < \infty$. Given G, write $G = H_G \times H'_G$ where $\#H_G$ is divisible only by primes in P, and $\#H'_G$ is divisible only by primes not in P. We use $\sum_H$ (resp. $\sum_{H'}$) to denote a sum restricted to symplectic abelian groups of order divisible only by primes in P (resp., not in P), and we may restrict the sum further by limiting the size of H or H'. Then $\sum_{p \in P} \mathrm{Prob}(T_p \neq 0) \leq \sum_{p \in P} O(1/p) < \infty$, so the Borel–Cantelli lemma implies that the random group $\bigoplus_{p \in P} T_p$ is given by a discrete probability distribution on the set of isomorphism classes of (finite) symplectic abelian groups H of order divisible only by primes in P; in fact, Theorem 3.9 implies that $\mathrm{Prob}\left(\bigoplus_{p \in P} T_p \simeq H\right) = c_P w_H$, where c_P is a normalizing constant defined as the convergent product $\prod_{p \in P} \prod_{i=1}^{\infty} (1 - p^{1-2i})$; in particular, $\sum_H w_H < \infty$. By an L^1 function on the set of such H, we mean a real-valued function f such that $\sum_H |f(H)| w_H < \infty$; in particular, bounded functions are L^1. Given such an L^1 function f, we define

$$\int f := \frac{\sum_H f(H) w_H}{\sum_H w_H}$$

and extend f to all symplectic abelian groups G by defining $f(G) := f(H_G)$.

In contrast with Delaunay's heuristic (8), our heuristic predicts that the left hand side of (8) should equal $\int f$. We now prove that Delaunay's prediction agrees with ours.

Theorem 5.15. *Let P be a set of primes such that $\sum_{p \in P} 1/p < \infty$. Let f be an L^1 function on the set of (isomorphism classes of) symplectic abelian groups H of order divisible only by primes in P. Extend f to all symplectic abelian groups G by defining $f(G) := f(H_G)$. Then*

$$\lim_{n \to \infty} \frac{\sum_{\#G \leq n} f(G) w_G}{\sum_{\#G \leq n} w_G} = \int f. \tag{9}$$

Proof of Theorem 5.15. We may add a constant to f in order to assume that $\int f = 0$; in other words, $\sum_H f(H) w_H = 0$. For any $M \in \mathbb{R}$, define $S_M := \sum_{\#H \le M} f(H) w_H$; thus the S_M are bounded and $\lim_{M\to\infty} S_M = 0$. Suppose that $\epsilon > 0$ is given; fix m such that $M > m$ implies $|S_M| < \epsilon$. Then

$$\begin{aligned}
\left| \sum_{\#G \le n} f(G) w_G \right| &= \left| \sum_{\#H' \le n} \sum_{\#H \le \frac{n}{\#H'}} f(H) w_H w_{H'} \right| \qquad \text{(we write each } G \text{ as } H \times H') \\
&\le \sum_{\#H' \le n} w_{H'} \left| S_{n/\#H'} \right| \\
&\le \sum_{\#H' < n/m} w_{H'} \epsilon + \sum_{\#H' \in [n/m, n]} w_{H'} O(1) \\
&\le \left(\frac{1}{2} \log n \right) \epsilon + O(\log m) \qquad \text{(by Corollary 3.15)}
\end{aligned}$$

and

$$\sum_{\#G \le n} w_G \ge \frac{1}{2} \log n \qquad \text{(by Corollary 3.15).}$$

Thus the lim sup of the absolute value of the ratio in (9) is bounded by ϵ. This holds for every ϵ, so the limit is 0, matching $\int f$. □

6. Arithmetic justification

In this section, we prove results on the arithmetic of elliptic curves that partially explain why $\mathrm{Sel}_{p^e} E$ should behave like an intersection of maximal isotropic direct summands.

6.1. **Shafarevich–Tate groups of finite group schemes.** For any G_k-module or finite k-group scheme M, define

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

(If M is not étale, then the cohomology should be interpreted as fppf cohomology.)

Proposition 6.1. *Let E be an elliptic curve over a global field k. Let $e \in \mathbb{Z}_{\ge 0}$. If $\operatorname{char} k \neq p$, suppose that the image G of $G_k \to \operatorname{Aut} E[p^e] \simeq \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ contains $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$. If $\operatorname{char} k = p$, suppose that the image G of $G_k \to \operatorname{Aut} E[p^e](k^{\mathrm{sep}})$ is cyclic. Then $Ш^1(k, E[p^e]) = 0$.*

Remark 6.2. For each k, the hypothesis of Proposition 6.1 holds for 100% of elliptic curves over k, as we now explain. If $\operatorname{char} k \neq p$, then the result follows from the Hilbert irreducibility theorem. If $\operatorname{char} k = p$ and either $p > 2$ or $e \le 2$, then $E[p^e](k^{\mathrm{sep}})$ is cyclic of order p^f for some $f \le e$, and its automorphism group is $(\mathbb{Z}/p^f\mathbb{Z})^\times$, which is cyclic; thus the hypothesis holds for *all* elliptic curves over k. Finally, if $\operatorname{char} k = 2$, then an explicit calculation with Weierstrass equations shows that $E[2](k^{\mathrm{sep}}) = 0$ for 100% of E, and in that case, $E[2^e](k^{\mathrm{sep}}) = 0$ follows.

Before proving Proposition 6.1, we introduce some more definitions and prove a few basic facts. For any finite group G and G-module M, define

$$\mathrm{H}^1_{\mathrm{cyc}}(G,M) := \bigcap_{\text{cyclic } H \leq G} \ker\left(\mathrm{H}^1(G,M) \to \mathrm{H}^1(H,M)\right),$$

which, like $\mathrm{H}^1(G,M)$, is contravariant in G and covariant in M. For any Galois extension L/k and $\mathrm{Gal}(L/k)$-module M, define

$$Ш^1(L/k,M) := \ker\left(\mathrm{H}^1(\mathrm{Gal}(L/k),M) \to \prod_{v\in\Omega} \mathrm{H}^1(\mathrm{Gal}(L_w/k_v),M)\right),$$

where $\mathrm{Gal}(L_w/k_v)$ is a decomposition group associated to a chosen place w of L above v; since the conjugation action $\mathrm{Gal}(L/k)$ on itself induces the identity on $\mathrm{H}^1(\mathrm{Gal}(L/k),M)$, it does not matter which w is chosen, and we could alternatively take the kernel of the map to the product over *all* w instead of using only one above each v.

Lemma 6.3 (cf. [BPS12, Proposition 8.3])**.**

(a) *If a finite group G acts trivially on an abelian group M, then $\mathrm{H}^1_{\mathrm{cyc}}(G,M) = 0$.*
(b) *If L/k is a finite Galois extension with Galois group G, and M is a G-module, then $Ш^1(L/k,M) \subseteq \mathrm{H}^1_{\mathrm{cyc}}(G,M)$.*
(c) *If L/k is a Galois extension with Galois group G, and G acts trivially on an abelian group M, then $Ш^1(L/k,M) = 0$.*
(d) *If L/k is a finite Galois extension, and M is a $\mathrm{Gal}(L/k)$-module, and L'/k is a larger Galois extension (so $\mathrm{Gal}(L'/L)$ acts trivially on M), then inflation induces an isomorphism $Ш^1(L/k,M) \xrightarrow{\sim} Ш^1(L'/k,M)$.*
(e) *If L'/k is a Galois extension, and M is a finite $\mathrm{Gal}(L'/k)$-module, and G is the image of $\mathrm{Gal}(L'/k) \to \mathrm{Aut}\, M$, then $Ш^1(L'/k,M)$ is isomorphic to a subgroup of $\mathrm{H}^1_{\mathrm{cyc}}(G,M)$.*

Proof.

(a) A homomorphism $G \to M$ that restricts to 0 on each cyclic subgroup of G is 0.
(b) By the Chebotarev density theorem, each cyclic subgroup of G arises as a decomposition subgroup.
(c) If L/k is finite, this follows from (a) and (b). The general case follows by taking a direct limit.
(d) From the inflation-restriction sequence

$$0 \to \mathrm{H}^1(\mathrm{Gal}(L/k),M) \to \mathrm{H}^1(\mathrm{Gal}(L'/k),M) \to \mathrm{H}^1(\mathrm{Gal}(L'/L),M)$$

mapping to its local analogues, we obtain an exact sequence

$$0 \to Ш^1(L/k,M) \to Ш^1(L'/k,M) \to Ш^1(L'/L,M).$$

The last term is 0 by (c).
(e) The quotient G of $\mathrm{Gal}(L'/k)$ is $\mathrm{Gal}(L/k)$ for a finite Galois extension L/k. Apply (d) and then (b). □

Proof of Proposition 6.1 for $\mathrm{char}\, k \neq p$. The case $e = 1$ is [PR12, Proposition 3.3(e)], so assume $e \geq 2$. Let $S_e := \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$. Let $M := E[p^e] \simeq (\mathbb{Z}/p^e\mathbb{Z})^2$. By Lemma 6.3(e), $Ш^1(k,M)$ is isomorphic to a subgroup of $\mathrm{H}^1_{\mathrm{cyc}}(G,M)$. The invariant subgroup M^{S_e} is 0,

so the inflation-restriction sequence for $S_e \leq G$ shows that $\mathrm{H}^1_{\mathrm{cyc}}(G, M) \to \mathrm{H}^1_{\mathrm{cyc}}(S_e, M)$ is injective. It remains to show that $\mathrm{H}^1_{\mathrm{cyc}}(S_e, M) = 0$.

The inflation-restriction sequence associated to the central subgroup $\{\pm 1\} \leq S_e$ is

$$0 \longrightarrow \mathrm{H}^1(S_e/\{\pm 1\}, M[2]) \xrightarrow{\inf} \mathrm{H}^1(S_e, M) \longrightarrow \mathrm{H}^1(\{\pm 1\}, M)^{S_e}. \tag{10}$$

If p is odd, $M[2] = 0$ and $\mathrm{H}^1(\{\pm 1\}, M) = 0$ (killed by both 2 and p), so $\mathrm{H}^1(S_e, M) = 0$.

So assume that $p = 2$. Then $\mathrm{H}^1(\{\pm 1\}, M) \simeq (\mathbb{Z}/2\mathbb{Z})^2$, on which S_e acts through S_1 in the standard way, so $\mathrm{H}^1(\{\pm 1\}, M)^{S_e} = 0$, so the map inf in (10) is an isomorphism. The map inf factors as

$$\mathrm{H}^1(S_e/\{\pm 1\}, M[2]) \longrightarrow \mathrm{H}^1(S_e, M[2]) \longrightarrow \mathrm{H}^1(S_e, M),$$

so the second map is surjective. It is also injective, since $\mathrm{H}^0(S_e, 2M) = 0$. Thus $\mathrm{H}^1(S_e, M[2]) \simeq \mathrm{H}^1(S_e, M)$.

Define a filtration $\{1\} \leq \Gamma_{e-1} \leq \cdots \leq \Gamma_2 \leq \Gamma_1 \leq S_e$ by $\Gamma_m := \ker(S_e \to S_m)$. We prove by induction on e that the inclusion $\Gamma_1^2[\Gamma_1, \Gamma_1] \leq \Gamma_2$ is an equality. We check the cases $e = 2$ and $e = 3$ by hand. For $e \geq 4$, every element of Γ_{e-1} is represented by $1 + 2^{e-1}A$ for some trace-0 integer matrix A, and is the square of $1 + 2^{e-2}A \in \Gamma_{e-2} \leq \Gamma_1$; now apply the inductive hypothesis to $S_{e-1} = S_e/\Gamma_{e-1}$.

The previous paragraph shows that Γ_2 is contained in the kernel of every homomorphism $\Gamma_1 \to \mathbb{Z}/2\mathbb{Z}$. Thus the restriction map $\mathrm{H}^1(\Gamma_1, M[2]) \to \mathrm{H}^1(\Gamma_2, M[2])$ is 0 (the actions are trivial). Consider the maps α and β in the inflation-restriction sequence

$$0 \longrightarrow \mathrm{H}^1(S_2, M[2]) \xrightarrow{\alpha} \mathrm{H}^1(S_e, M[2]) \xrightarrow{\beta} \mathrm{H}^1(\Gamma_2, M[2]).$$

Since β factors through the previous restriction map, $\beta = 0$, and α is an isomorphism. Let $U_e \leq S_e$ be the subgroup of unipotent upper triangular matrices. The horizontal maps in the bottom row of the commutative diagram

$$\begin{array}{ccccc}
\mathrm{H}^1(S_2, M[2]) & \xrightarrow{\sim} & \mathrm{H}^1(S_e, M[2]) & \xrightarrow{\sim} & \mathrm{H}^1(S_e, M) \\
\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\
\mathrm{H}^1(U_2, M[2]) & \xhookrightarrow{\inf} & \mathrm{H}^1(U_e, M[2]) & \longrightarrow & \mathrm{H}^1(U_e, M)
\end{array}$$

are injective (for the second map, observe that $M^{U_e} \xrightarrow{2} (2M)^{U_e}$ is surjective). Direct calculation shows that the left vertical map is injective too (in fact, it is an isomorphism between groups of order 2). So the right vertical map is injective. In particular, $\mathrm{H}^1_{\mathrm{cyc}}(S_e, M) = 0$. □

The following two lemmas will be used in the proof of the $\mathrm{char}\, k = p$ case of Proposition 6.1.

Lemma 6.4. *Let k be a field of characteristic p. Let E be an elliptic curve over k.*

(a) *If E is ordinary, then for any $e \in \mathbb{Z}_{\geq 0}$ there is an exact sequence*

$$0 \to M^\vee \to E[p^e] \to M \to 0 \tag{11}$$

involving a finite étale group scheme M of order p^e and its Cartier dual $M^\vee$.

(b) *If E is supersingular, then $E[p^e]$ is an iterated extension of copies of α_p.*

Proof. Let $F\colon E \to E'$ be the p^e-Frobenius morphism, and let $V\colon E' \to E$ be its dual. Then F is surjective and $VF = p^e$, so there is an exact sequence

$$0 \to \ker F \to E[p^e] \to \ker V \to 0.$$

Moreover, $\ker F$ is the Cartier dual of $\ker V$, by [Mum70, III.15, Theorem 1] (the proof there works over any field).

(a) If E is ordinary, then $\ker V$ is a finite étale group scheme of order $\deg V = p^e$.
(b) Suppose that E is supersingular. The group scheme $E[p^e]$ is an iterated extension of copies of $E[p]$, so we may reduce to the case $e = 1$. If $e = 1$, then $\ker F$ and $\ker V$ are isomorphic to α_p: over an algebraically closed field, this is well known [Oor66, II.15.5], and it follows over any field of characteristic p since the twists of α_p are classified by $\mathrm{H}^1(k, \mathbf{Aut}\,\alpha_p) = \mathrm{H}^1(k, \mathbb{G}_m) = 0$. □

Lemma 6.5. *Let k be a global field of characteristic p. Let M be a finite commutative group scheme over k that is an iterated extension of copies of μ_p and α_p. If $v \in \Omega$, then $\mathrm{H}^1(k, M) \to \mathrm{H}^1(k_v, M)$ is injective. In particular, $Ш^1(k, M) = 0$.*

Proof. When $M = \mu_p$, Hilbert's theorem 90 implies that $\mathrm{H}^1(k, M) \to \mathrm{H}^1(k_v, M)$ is $k^\times/k^{\times p} \to k_v^\times/k_v^{\times p}$. Similarly, when $M = \alpha_p$, it is the homomorphism of additive groups $k/k^p \to k_v/k_v^p$. Both homomorphisms are injective, by [PV10, Lemma 3.1].

If $0 \to M' \to M \to M'' \to 0$ is an extension of group schemes as in the statement, and the result holds for M' and M'', then it holds for M too (this uses injectivity of $\mathrm{H}^1(k_v, M') \to \mathrm{H}^1(k_v, M)$, which follows since $\mathrm{H}^0(k_v, M'') = 0$). So the general case follows by induction on $\#M$. □

Proof of Proposition 6.1 for $\operatorname{char} k = p$.

Case 1: E is supersingular. Combine Lemmas 6.4(b) and 6.5.

Case 2: E is ordinary. Let M be as in Lemma 6.4(a). Let $N = E[p^e](k^{\mathrm{sep}})$, which injects into $M(k^{\mathrm{sep}})$ under the map induced by (11). Let L be the splitting field of M. Thus L is a Galois extension of k and the image of $\mathrm{Gal}(L/k) \to \operatorname{Aut} N$ is G. We now break into subcases.

Case 2a: $L = k$. Then (11) has the form

$$0 \to \mu_{p^e} \to E[p^e] \to \mathbb{Z}/p^e\mathbb{Z} \to 0.$$

By Lemma 6.3(c), $Ш^1(k, \mathbb{Z}/p^e\mathbb{Z}) = 0$, so any $\xi \in Ш^1(k, E[p^e])$ must come from an element $\eta \in \mathrm{H}^1(k, \mu_{p^e})$. Pick any $v \in \Omega$. The middle vertical map in the commutative diagram

$$\begin{array}{ccccc} \mathbb{Z}/p^e\mathbb{Z} & \longrightarrow & \mathrm{H}^1(k, \mu_{p^e}) & \longrightarrow & \mathrm{H}^1(k, E[p^e]) \\ \| & & \downarrow & & \downarrow \\ \mathbb{Z}/p^e\mathbb{Z} & \longrightarrow & \mathrm{H}^1(k_v, \mu_{p^e}) & \longrightarrow & \mathrm{H}^1(k_v, E[p^e]) \end{array}$$

is injective by Lemma 6.5, and a diagram chase shows that η comes from an element of $\mathbb{Z}/p^e\mathbb{Z}$. Thus $\xi = 0$.

Case 2b: L is general. By definition of L, we have $E[p^e](L) = N$. For any place w of L, every element of L_w that is algebraic over L is actually separable over L [PV10, Lemma 3.1], so $E[p^e](L_w) = N$ too. By Case 2a, $Ш^1(L, E[p^e]) = 0$. Because of the (fppf) inflation-restriction sequence

$$0 \to \mathrm{H}^1(\mathrm{Gal}(L/k), N) \to \mathrm{H}^1(k, E[p^e]) \to \mathrm{H}^1(L, E[p^e]),$$

which maps to its analogue for each extension L_w/k_v of local fields, we have $Ш^1(k, E[p^e]) \simeq Ш^1(\mathrm{Gal}(L/k), N)$. By Lemma 6.3(e), the latter is isomorphic to a subgroup of $\mathrm{H}^1_{\mathrm{cyc}}(G, N)$, which is trivial since G is cyclic by assumption. □

Remark 6.6. In Proposition 6.1, when $p = 2$ and $e = 3$, the hypothesis that the image of $G_k \to \mathrm{Aut}\, E[p^e](k^{\mathrm{sep}})$ is cyclic can fail. The last line of the proof above cannot be immediately extended to the case in which the image is non-cyclic, because one can check that $\mathrm{H}^1_{\mathrm{cyc}}((\mathbb{Z}/8\mathbb{Z})^\times, \mathbb{Z}/8\mathbb{Z}) \neq 0$ for the standard nontrivial action. The *conclusion* of Proposition 6.1 might still hold, however.

6.2. **Intersection of maximal isotropic subgroups.** For nonarchimedean v, let $\mathcal{O}_v$ be the valuation ring in k_v. Let $\mathbf{A} = \prod'_{v\in\Omega}(k_v, \mathcal{O}_v)$ be the adele ring of k. Suppose that E, k, and p^e satisfy the hypothesis of Proposition 6.1, so that $Ш^1(k, E[p^e]) = 0$. Then [PR12, Theorem 4.14] applied with $\lambda\colon A \to \widetilde{A}$ being $[p^e]\colon E \to E$ shows that $\mathrm{Sel}_{p^e} E$ is isomorphic to the intersection of two maximal isotropic subgroups of

$$\mathrm{H}^1(\mathbf{A}, E[p^e]) := \prod_{v\in\Omega}{}'(\mathrm{H}^1(k_v, E[p^e]), \mathrm{H}^1(\mathcal{O}_v, E[p^e])) \simeq \prod_{v\in\Omega}{}' \left(\mathrm{H}^1(k_v, E[p^e]), \frac{E(k_v)}{p^e E(k_v)}\right),$$

namely the images of $E(\mathbf{A})/p^eE(\mathbf{A}) = \prod_v E(k_v)/p^eE(k_v)$ and $\mathrm{H}^1(k, E[p^e])$.

6.3. **Direct summands.** It is natural to ask whether these images are direct summands, given that we *modeled* $\mathrm{Sel}_{p^e} E$ by an intersection of direct summands. Corollary 6.8 below shows that at least the first of these images is a direct summand.

Proposition 6.7. *Let E be an abelian variety over an arbitrary field k. Let $n \in \mathbb{Z}_{>0}$. Then the image of the coboundary map $E(k)/nE(k) \xrightarrow{\delta} \mathrm{H}^1(k, E[n])$ is a direct summand of $\mathrm{H}^1(k, E[n])$.*

Proof. (We thank Bart de Smit and Christopher Skinner for ideas used in this proof.) For each $m|n$, the commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1(k, E[m]) & \twoheadrightarrow & \mathrm{H}^1(k, E)[m] \\ \downarrow & & \downarrow \\ \mathrm{H}^1(k, E[n]) & \xrightarrow{\alpha} & \mathrm{H}^1(k, E)[n] \end{array}$$

shows that any order m element of $\mathrm{H}^1(k, E)[n]$ lifts to an order m element of $\mathrm{H}^1(k, E[n])$ under the surjection α in the diagram. Any $\mathbb{Z}/n\mathbb{Z}$-module is a direct sum of cyclic groups [Prü23, §17], [Bae35, pp. 274–275]; applying this to $\mathrm{H}^1(k, E)[n]$ and using the previous sentence shows that α is split. Finally, $\ker(\alpha) = \mathrm{im}(\delta)$. □

Corollary 6.8. *Let E be an abelian variety over a global field k. Let $n \in \mathbb{Z}_{>0}$. Then the image of $E(\mathbf{A})/nE(\mathbf{A}) \xrightarrow{\delta} \mathrm{H}^1(\mathbf{A}, E[n])$ is a direct summand of $\mathrm{H}^1(\mathbf{A}, E[n])$.*

Proof. Proposition 6.7 yields a complement C_v of $E(k_v)/nE(k_v)$ in $\mathrm{H}^1(k_v, E[n])$. Then $\bigoplus_{v\in\Omega} C_v$ is a complement of $E(\mathbf{A})/nE(\mathbf{A})$ in $\mathrm{H}^1(\mathbf{A}, E[n])$. □

Question 6.9. Is the image of $\mathrm{H}^1(k, E[n]) \to \mathrm{H}^1(\mathbf{A}, E[n])$ a direct summand?

Lemma 6.10. *If* $\operatorname{char} k \nmid n$ *and the action of* G_k *on* $E[n]$ *is trivial, then the answer to Question 6.9 is yes.*

Proof. We have $E[n] \simeq \mu_n \times \mu_n$, so we must show that the image of $k^\times/k^{\times n} \to \mathbf{A}^\times/\mathbf{A}^{\times n}$ is a direct summand. By Lemma 6.11 below, it is enough to show that $k^\times/k^{\times m} \to \mathbf{A}^\times/\mathbf{A}^{\times m}$ is injective for each $m|n$. This "local-global principle for m^{th} powers" is a well known consequence of the Chebotarev density theorem. □

Lemma 6.11. *Let* $n \in \mathbb{Z}_{>0}$. *Let* $\delta\colon A \to B$ *be a homomorphism of* $\mathbb{Z}/n\mathbb{Z}$*-modules such that the induced morphism* $A/mA \to B/mB$ *is injective for every* $m|n$. *Then* $\delta(A)$ *is a direct summand of* B.

Proof. (We thank Bart de Smit for this proof.) Taking $m = n$ shows that δ is injective, so it fits into a short exact sequence

$$0 \to A \xrightarrow{\delta} B \to C \to 0$$

of $\mathbb{Z}/n\mathbb{Z}$-modules. Write C as a direct sum of cyclic groups C_i. For each m, the hypothesis together with the snake lemma shows that $B[m] \to C[m]$ is surjective. Thus we can construct a splitting of the surjection $B \to C$, by lifting a generator of each C_i to an element of B of the same order. □

6.4. **Freeness of the ambient group.** On the arithmetic side, the $\mathbb{Z}/p^e\mathbb{Z}$-module $\mathrm{H}^1(\mathbf{A}, E[p^e])$ carrying a quadratic form is not always free. But we have modeled it by the free module $(\mathbb{Z}/p^e\mathbb{Z})^{2n}$ with $(Q \bmod p^e)$.

Question 6.12. Can we develop a more sophisticated model in which we start with a compatible system consisting of a quadratic form on a non-free $\mathbb{Z}/p^e\mathbb{Z}$-module for each e?

Acknowledgements

We thank Kęstutis Česnavičius, Bart de Smit, Christophe Delaunay, and Christopher Skinner for comments. This research was begun during the "Arithmetic Statistics" semester at the Mathematical Sciences Research Institute, and continued during the "Cohen-Lenstra heuristics for class groups" workshop at the American Institute of Mathematics, the 2012 Canadian Number Theory Association meeting at the University of Lethbridge, and the Centre Interfacultaire Bernoulli semester on "Rational points and algebraic cycles".

References

[Bae35] Reinhold Baer, *Der Kern, ein charakteristische Untergruppe*, Compositio Math. **1** (1935), 254–283. ↑6.3

[BS10] 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`, to appear in *Annals of Math.* ↑1.2, 5.13

[BPS12] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus* 3, May 18, 2012. Preprint, `arXiv:1205.4456v1`. ↑6.3

[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) ↑5.6

[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) ↑1.2, 1, 3.2, 3.8, 5.14, 5.6

[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) ↑1.2, 1

[DJ13a] Christophe Delaunay and Frédéric Jouhet, *p^ℓ-torsion points in finite abelian groups and combinatorial identities*, March 31, 2013. Preprint, `arXiv:1208.6397v2`. ↑1.2, 1.4, 1, 5.12

[DJ13b] ———, *The Cohen–Lenstra heuristics, moments and p^j-ranks of some groups*, March 31, 2013. Preprint, `arXiv:1303.7337v1`. ↑1.4

[Eul48] Leonhard Euler, *Introductio in analysin infinitorum. Tomus primus*, Marcum-Michaelum Bousquet & Socios, Lausanne, 1748; English transl., *Introduction to analysis of the infinite. Book I*, Springer-Verlag, New York, 1988. Translated from the Latin and with an introduction by John D. Blanton. MR961255 (89g:01067). ↑3.8

[FX12] Keqin Feng and Maosheng Xiong, *On Selmer groups and Tate-Shafarevich groups for elliptic curves $y^2 = x^3 - n^3$*, Mathematika **58** (2012), no. 2, 236–274, DOI 10.1112/S0025579312000046. MR2965971 ↑1.5

[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) ↑1.2

[Igu00] Jun-ichi Igusa, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, American Mathematical Society, Providence, RI, 2000. MR1743467 (2001j:11112) ↑3.8

[KM95] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Astérisque **228** (1995), 3, 81–100. With an appendix by A. Granville; Columbia University Number Theory Seminar (New York, 1992). MR1330929 (96c:11058) ↑5.5

[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 ↑1.2

[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) ↑1.2

[Lev68] Martin Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462. MR0230723 (37 #6283) ↑5.5

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287 (80c:14015) ↑5.5

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449 (French). MR1369424 (96i:11057) ↑5.5, 5.9

[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) ↑6.1

[Oes82] Joseph Oesterlé, *Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$*, Invent. Math. **66** (1982), no. 2, 325–341, DOI 10.1007/BF01389398 (French). MR656627 (83j:12014) ↑a, b, c

[Oor66] F. Oort, *Commutative group schemes*, Lecture Notes in Mathematics, vol. 15, Springer-Verlag, Berlin, 1966. MR0213365 (35 #4229) ↑b

[Poo12] Bjorn Poonen, *Average rank of elliptic curves*, 2012. Preprint. ↑5.13

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483 ↑1.2, 1.2, 1, 1.5, 4.3, 5.5, 5.12, 6.1, 6.2

[PV10] Bjorn Poonen and José Felipe Voloch, *The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields*, Ann. of Math. (2) **171** (2010), no. 1, 511–532, DOI 10.4007/annals.2010.171.511. MR2630046 (2011j:14048) ↑6.1

[Prü23] Heinz Prüfer, *Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen*, Math. Z. **17** (1923), no. 1, 35–61, DOI 10.1007/BF01504333 (German). MR1544601 ↑6.3

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401 (French). MR644559 (83k:12011) ↑a, b

[SGA 7_{II}] *Groupes de monodromie en géométrie algébrique. II*, Lecture Notes in Mathematics, Vol. 340, Springer-Verlag, Berlin, 1973 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II); Dirigé par P. Deligne et N. Katz. MR0354657 (50 #7135) ↑4.3, 4.3

[XZ08] Maosheng Xiong and Alexandru Zaharescu, *Distribution of Selmer groups of quadratic twists of a family of elliptic curves*, Adv. Math. **219** (2008), no. 2, 523–553, DOI 10.1016/j.aim.2008.05.005. MR2435648 (2009e:11113) ↑1.5

[XZ09] ———, *Selmer groups and Tate-Shafarevich groups for the congruent number problem*, Comment. Math. Helv. **84** (2009), no. 1, 21–56, DOI 10.4171/CMH/151. MR2466074 (2010c:11068) ↑1.5

[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) ↑1.5

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA
E-mail address: bhargava@math.princeton.edu

Department of Mathematics, Stanford University, Stanford, CA 94305, USA
E-mail address: dankane@math.stanford.edu
URL: http://math.stanford.edu/~dankane/

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
E-mail address: hwl@math.leidenuniv.nl
URL: http://www.math.leidenuniv.nl/~hwl/

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: poonen@math.mit.edu
URL: http://math.mit.edu/~poonen/

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125
E-mail address: rains@caltech.edu