# Selmer Group Heuristics

Notes by Tony Feng
for a talk by Bjorn Poonen

June 13, 2016

This is on joint work with Eric Rains, Manjul Bhargava, Daniel Kane, Hendrik Lenstra, Jennifer Park, John Voight, and Melanie Matchett Wood.

## 1 Motivation

For $E/\mathbb{Q}$, let $s(E) = \dim_{\mathbb{F}_2} \mathrm{Sel}_2 E - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2]$.

**Theorem 1.1** (Heath-Brown 1994)**.** *For $d \geq 1$, as $E$ varies over quadratic twists of $y^2 = x^3 - x$,*

$$\mathrm{Prob}(s(E) = d) \propto \prod_{j=1}^{d} \frac{2}{2^j - 1}$$

The normalizing constant turns out to be

$$\prod_{j \geq 0} (1 + 2^{-j})^{-1}.$$

I first learned this when Karl Rubin stated this theorem in a seminar talk. I (together with Eric Rains) was motivated by this to think about distributions of "random" $\mathbb{F}_2$ vector spaces.

**Random Linear Algebra.** Let $V = (\mathbb{F}_p)^{2n}$. Let $Q \colon V \to \mathbb{F}_p$ be a quadratic form,

$$(x_1, \ldots, x_n, y_1, \ldots, y_n) \to \sum x_i y_i.$$

The associated bilinear form is

$$\langle v, w \rangle := Q(v + w) - Q(v) - Q(w).$$

*Definition* 1.2. A subspace $Z \subset V$ is *maximal isotropic* if and only if

$$Z^{\perp} = Z \text{ and } Q|_Z = 0.$$

(The second condition is only needed in characteristic 2.)

**Proposition 1.3.** *Choose maximal isotropic subspaces $Z, W \subset V$ at random. Then*

$$\lim_{n\to\infty} \text{Prob}(\dim(Z \cap W) = d) = \prod_{j\geq 0}(1 + p^{-j})^{-1} \cdot \prod_{j=1}^{d} \frac{p}{p^j - 1}$$

This bears an obvious resemblance to Heath-Brown's Theorem. Interesting! Why might this be happening?

## 2 Selmer groups

Let $k$ be a global field, $\mathbb{A}$ the adele ring of $k$, $E$ an elliptic curve over $k$, and $p$ a prime distinct from the characteristic of $k$.

Kummer theory gives

$$\begin{array}{ccc} E(k)/pE(k) & \longrightarrow & H^1(k, E[p]) \\ \downarrow & & \downarrow \beta \\ E(\mathbb{A})/pE(\mathbb{A}) & \xrightarrow[\alpha]{} & H^1(\mathbb{A}, E[p]) \end{array}$$

Here we can $H^1(\mathbb{A}, E[p])$ as notation for a restricted product

$$\prod_v{}' (H^1(k_v, E[p]), H^1_{\text{ét}}(\mathcal{O}_v, \mathcal{E}[p]))$$

Alternatively, it is a theorem that Cesnavisius that this really can be identified with étale cohomology over the adeles.

It is non-trivial but true that $\beta$ is an injection.

*Definition* 2.1. We define the *Selmer group*

$$\text{Sel}_p E := \beta^{-1}(\text{Im } \alpha) \overset{\beta}{\cong} \text{Im}\,(\alpha) \cap \text{Im}\,(\beta).$$

**Theorem 2.2** (P-Rains)**.** *There exists a quadratic form $Q\colon H^1(\mathbb{A}, E[p]) \to \mathbb{Q}/\mathbb{Z}$ for which* Im $\alpha$ *and* Im $\beta$ *are maximal isotropic.*

This shows that the Selmer group is the intersection of two maximal isotropic subspaces in an *infinite-dimensional* vector space, which harmonizes with the random linear algebra.

What is $Q$? In the interest of time, I won't answer this. Let me explain instead the associated bilinear form. Thanks to the Weil pairing

$$E[p] \times E[p] \to \mathbb{G}_m$$

we have an induced pairing

$$\langle \cdot, \cdot \rangle\colon H^1(\mathbb{A}, E[p]) \times H^1(\mathbb{A}, E[p]) \to H^2(A, \mathbb{G}_m).$$

Now $H^2(A, \mathbb{G}_m) = \mathrm{Br}(\mathbb{A})$, which because the Brauer groups of $O_v$ turn out to be trivial is $\cong \bigoplus_v \mathrm{Br}(K_v)$. Then the pairing is the sum of the invariant maps to $\mathbb{Q}/\mathbb{Z}$.

*Example* 2.3. How should $\dim \mathrm{Sel}_p E$ be distributed as $E$ varies in an algebraic family whose generic member has rank 18 over $\mathbb{Q}(t)$? We can adjust the model to guess the answer to such a question.

The 18 rational point generators map to an 18-dimensional subspace of $H^1(\mathbb{A}, E[p])$, containing Im $\alpha$ and Im $\beta$. This suggests the following model.

Let $R \leq V$ be isotropic of dimension 18. Then the answer should be the *conditional* probability

$$\lim_{n\to\infty} \mathrm{Prob}(\dim(Z \cap W) = d \colon Z, W \supset R).$$

The result is that the distribution on $\mathbb{N}$ shifts by +18.

# 3 Variants

Now, what if we were interested in modelling $\mathrm{Sel}_{p^e} E$? The Theorem still holds, but what is a "random maximal isotropic subgroup of $((\mathbb{Z}/4\mathbb{Z})^{2n}, \sum x_i y_i)$? In the $p$-Selmer case automorphisms acted transitively on maximal isotropic subspaces, but in this case the maxial isotropic subgroups can even have different shapes, even as abelian groups. Should $(\mathbb{Z}/4\mathbb{Z})^n \times \{0\}$ and $(2\mathbb{Z}/4\mathbb{Z})^{2n}$ be equally likely?

We were stuck on this for a while, but eventually we realized that the only solution which is consistent with the model for $p$-Selmer groups is to *only consider direct summands* (e.g. assigning probability 0 to $(2\mathbb{Z}/4\mathbb{Z})^{2n}$). Then automorphisms act transitively on such subgroups, and the same model applies.

Consider the sequence

$$0 \to E(k) \otimes \frac{p^{-e}\mathbb{Z}_p}{\mathbb{Z}_p} \to \mathrm{Sel}_{p^e} E \to Ш[p^e] \to 0.$$

Taking the direct limit over $e$, we get

$$0 \to E(k) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \to \mathrm{Sel}_{p^\infty} E \to Ш[p^\infty] \to 0. \tag{1}$$

**Can one model the "distribution" of this whole short exact sequence?**

Let $(V \cong \mathbb{Z}_p^{2n}, Q = \sum x_i y_i)$ be a quadratic space.

*Definition* 3.1. A *Lagrangian submodule* $Z$ is a rank $n$ submodule such that

- $Z$ is a direct summand,
- $Q|_Z = 0$.

Choose a Lagrangian subspace $Z, W \leq V$ at random, and form

$$0 \to \underbrace{(Z \cap W) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}}_{R} \to \underbrace{\left(Z \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cap \left(W \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)}_{S} \to T \to 0$$

We are thinking of $R$ as a model for the rational points, $S$ as a model for the Selmer group, and $T$ as a model for the Tate-Shafarevich group in (1), after letting $n \to \infty$.

**Theorem 3.2** (RST Theorem)**.** *The limit*

$$\lim_{n\to\infty} (\textit{distribution of } 0 \to R \to S \to T \to 0)$$

*exists.*

**Conjecture 3.3.** *The limit equals the distribution of* (1) *as $E$ varies over all elliptic curves over $k$ (ordered by height).*

**Consequences.**

- Conjecture 3.3 implies the "50-50" conjecture that 50% of $E/k$ have rank 0 and 50% have rank 1 (cf. Goldfeld, Katz-Sarnak).
- Conjecture 3.3 implies that the average size of $\#\operatorname{Sel}_n E$ is $\sigma_1(n)$. (As stated, this only holds for $n$ a prime power.) This was proved by Bhargava-Shankar for $n = 2, 3, 4, 5$.
- Conjecture 3.3 implies that $Ш[p^\infty]$ is finite for 100% of $E$. In fact, as $E$ ranges over rank $r$ curves the distribution of $Ш[p^\infty]$ is as conjectured by Delaunay in 2001, 2007 (at least for $r = 0, 1$; there is a variant for higher $r$).

**Model for Ш.** We described a another linear algebra model for Ш. For large $n \equiv r \mod 2$, choose $A \in M_n(\mathbb{Z}_p)$ subject to $A^T = -A$ and $\operatorname{rank}_{\mathbb{Z}_p} \ker A = r$. We view $\operatorname{coker}(\mathbb{Z}_p^n \xrightarrow{A} \mathbb{Z}_p^n)_{\text{tors}}$ as a model for Ш.

**Theorem 3.4** (BKLPR)**.** *Fix $r$. The following distributions coincide:*

1. *The distribution of $T$ in the RST theorem,*
2. *Delaunay's distribution,*
3. $$\lim_{\substack{n\to\infty \\ n\equiv r \mod 2}} \left(\textit{dist. of } \operatorname{coker}(\mathbb{Z}_p^n \xrightarrow{A} \mathbb{Z}_p^n)_{\text{tors}}\right)_{\text{tors}}$$

# 4 Modelling ranks

The theorem suggests that the rank of the elliptic curve is modelled by the rank of $A$. (This idea goes back further, cf. Deninger 2010.)

Clearly this will predicts that 100% of ranks should be as small as possible (0 or 1). We can restrict to matrices of bounded height, and ask how quickly the percentage of higher ranks goes to 0.

To model $E/\mathbb{Q}$ of height $H := \max(|4A^3), |27B^2|)$, choose a random variable $A \in M_n(\mathbb{Z})$ subject to $A^T = -A$ and the entries are bounded in absolute value by $X$, where $n = n(H)$ and $X = X(H)$ are functions of the height such that $n \mod 2$ is random and $X^n = H^{1/12+o(1)}$. (This is calibrated so that the average size of Ш for rank 0 curves is as predicted by standard conjectures.)

**Conjecture 4.1.** *"*$(\operatorname{coker} A)_{\text{tors}}$ *models* Ш*" and "*$\operatorname{rank}_{\mathbb{Z}}(\ker A)$ *models* rank $E(\mathbb{Q})$*".*

**Theorem 4.2** (PPVW)**.** *With probability* 1*,*

$$\{E/\mathbb{Q}\colon\ \operatorname{rank}_{\mathbb{Z}}(\ker A_E) > 21\} \textit{ is finite}.$$

This suggests that

$$\{E/\mathbb{Q}\colon\ \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) > 21\} \text{ is finite.}$$