Random maximal isotropic subspaces and Selmer groups

Bjorn Poonen
Eric Rains

January 5, 2011

Selmer groups

k: number field

E: elliptic curve over k

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{E(k)}{pE(k)} & \longrightarrow & H^1(k, E[p]) & \longrightarrow & H^1(k, E)[p] & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow{\scriptstyle\beta} & & \big\downarrow & & \\
0 & \longrightarrow & \displaystyle\prod_v \frac{E(k_v)}{pE(k_v)} & \xrightarrow{\alpha} & \displaystyle\prod_v H^1(k_v, E[p]) & \longrightarrow & \displaystyle\prod_v H^1(k_v, E)[p] & \longrightarrow & 0
\end{array}$$

$$\mathrm{Sel}_p\, E := \left\{\xi \in H^1(k, E[p]) : \beta(\xi) \in \mathrm{im}(\alpha)\right\}$$

$$Ш(E) := \ker\left(H^1(k, E) \to \prod_v H^1(k_v, E)\right).$$

$$0 \to \frac{E(k)}{pE(k)} \to \underset{\text{finite, computable}}{\mathrm{Sel}_p\, E} \to Ш(E)[p] \to 0.$$

How do Selmer groups vary in a *family* of elliptic curves?

- Heath-Brown 1994: Define

$$s(E) := \dim_{\mathbb{F}_2} \mathrm{Sel}_2 E - \dim_{\mathbb{F}_2} E(k)[2].$$

  Then as E varies over quadratic twists of $y^2 = x^3 - x$ over $\mathbb{Q}$,

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

  for each $d \geq 0$.

- Swinnerton-Dyer 2008, Kane 2010: Same for quadratic twists of other $E_0/\mathbb{Q}$ with rational 2-torsion and no rational cyclic subgroup of order 4.
- Mazur–Rubin 2010, Klagsbrun 2010: For many E_0/k, construct infinitely many twists E with prescribed $s(E)$.

. . .

How do Selmer groups vary? Average size?

- Yu 2000: For $k = \mathbb{Q}$, for the family of all elliptic curves with rational 2-torsion,

$$\overline{\text{Average}}(\#\,\text{Sel}_2) \text{ is finite.}$$

- de Jong 2002: For $k = \mathbb{F}_q(t)$,

$$\overline{\text{Average}}(\#\,\text{Sel}_3) \leq 4 + O(1/q).$$

He had a heuristic that suggested that the truth was 4, and he predicted the same for number fields.

- Bhargava–Shankar 2010: For $k = \mathbb{Q}$,

$$\text{Average}(\#\,\text{Sel}_2) = 3$$
$$\text{Average}(\#\,\text{Sel}_3) = 4$$

(and results for Sel_4 and Sel_5 are forthcoming!)

Hyperbolic quadratic spaces

Let W be an n-dimensional $\mathbb{F}_p$-vector space. Define

$$V := W \oplus \underbrace{W^*}_{\text{dual}}$$

$$\begin{aligned} Q\colon \quad & V \to \mathbb{F}_p \\ & (w, \phi) \mapsto \phi(w). \end{aligned}$$

This Q is a quadratic map: the function

$$\langle x, y \rangle := Q(x+y) - Q(x) - Q(y)$$

is bilinear.

Definition

Any such (V, Q) is called a hyperbolic quadratic space.

Definition

A subspace $Z \leq V$ is maximal isotropic if $Z^\perp = Z$ and $Q|_Z = 0$.

Random maximal isotropic subspaces

Recall the notation: (V, Q) is hyperbolic, $\dim_{\mathbb{F}_p} V = 2n$.

Proposition

Choose maximal isotropic $Z_1, Z_2 \leq V$ at random. Then

$$\operatorname{Prob}(\dim(Z_1 \cap Z_2) = d) \to c_{d,p} := \prod_{j \geq 0} (1 + p^{-j})^{-1} \prod_{j=1}^{d} \frac{p}{p^j - 1}$$

as $\dim V \to \infty$*.*

When $p = 2$, this is the same distribution on nonnegative integers as in Heath-Brown's theorem!

Is this a coincidence?

Quadratic forms on locally compact abelian groups

Let V be a locally compact abelian group.
Let $Q\colon V \to \mathbb{R}/\mathbb{Z}$ be a continuous map such that

$$\langle x, y\rangle := Q(x+y) - Q(x) - Q(y)$$

is bilinear. Assume that (V, Q) is nondegenerate; i.e.,

$$\begin{aligned} V &\to V^* := \mathrm{Hom}_{\mathrm{conts}}(V, \mathbb{R}/\mathbb{Z}) \\ v &\mapsto \langle v, -\rangle \end{aligned}$$

is an isomorphism.

Definition

(V, Q) is weakly metabolic if and only if it has a compact open maximal isotropic subgroup W.

Restricted direct products of weakly metabolics

Definition (from previous slide)

(V, Q) is weakly metabolic if and only if it has a compact open maximal isotropic subgroup W.

Example (cf. Braconnier 1948)

Suppose that (V_i, Q_i, W_i) is weakly metabolic for $i \in \mathcal{I}$. Construct

$$V := \prod{}'(V_i, W_i)$$
$$W := \prod W_i$$

For $v = (v_i) \in V$, define

$$Q(v) := \sum Q_i(v_i).$$

Then (V, Q, W) is weakly metabolic.

Random maximal isotropic subspaces of an ∞-dim space

Suppose that

- (V, Q, W) is weakly metabolic, $pV = 0$
- V is infinite but second countable (topology has countable basis)

Let $\mathcal{I}_V$ be the set of maximal isotropic closed subgroups of V.

Theorem

- $$\mathcal{I}_V \simeq \varprojlim_X \mathcal{I}_{X^\perp/X},$$

  where X ranges over compact open subgroups of V with $Q|_X = 0$.
- *Define the uniform probability measure on the profinite set $\mathcal{I}_V$.*
- *If $Z \in \mathcal{I}_V$ is chosen at random, then*

  $$\operatorname{Prob}\left(\dim_{\mathbb{F}_p}(Z \cap W) = d\right) = c_{d,p}.$$

  (It turns out that Z is discrete with probability 1.)

Alternative description of the distribution

Define independent Bernoulli random variables $B_0, B_1, \ldots$ where

$$B_i = \begin{cases} 1, & \text{with probability } 1/(p^i + 1) \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$B_0 + B_1 + B_2 + \cdots$$

converges 100% of the time, and has the same distribution as the dimension of the random intersection of maximal isotropic subspaces.

Note: The probability that this sum is odd is $1/2$.

Alternative description of the distribution

Define independent Bernoulli random variables $B_0, B_1, \ldots$ where

$$B_i = \begin{cases} 1, & \text{with probability } 1/(p^i + 1) \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$B_0 + B_1 + B_2 + \cdots$$

converges 100% of the time, and has the same distribution as the dimension of the random intersection of maximal isotropic subspaces.

Note: The probability that this sum is odd is $1/2$.
(This follows since B_0 is odd with probability $1/2$.)

Local fields

Let E be an elliptic curve over a *local* field k_v.
Let $V = H^1(k_v, E[p])$, which is locally compact (and even *finite* if $p \neq \operatorname{char} k_v$).

$$1 \to \mathbb{G}_m \to \underset{\text{Heisenberg}}{\mathcal{H}} \to E[p] \to 1$$

gives rise to a quadratic form

$$q_v \colon H^1(k_v, E[p]) \to H^2(k_v, \mathbb{G}_m) \hookrightarrow \mathbb{R}/\mathbb{Z}$$

whose associated bilinear form is the cup product of the Weil pairing

$$H^1(k_v, E[p]) \times H^1(k_v, E[p]) \xrightarrow{\text{cup}} H^2(k_v, \mathbb{G}_m) \hookrightarrow \mathbb{R}/\mathbb{Z}.$$

Moreover, the subgroup $E(k_v)/pE(k_v)$ is maximal isotropic.

Local fields

Let E be an elliptic curve over a *local* field k_v.
Let $V = H^1(k_v, E[p])$, which is locally compact (and even *finite* if $p \neq \operatorname{char} k_v$).

$$1 \to \mathbb{G}_m \to \underset{\text{Heisenberg}}{\mathcal{H}} \to E[p] \to 1$$

gives rise to a quadratic form

$$q_v \colon H^1(k_v, E[p]) \to H^2(k_v, \mathbb{G}_m) \hookrightarrow \mathbb{R}/\mathbb{Z}$$

whose associated bilinear form is the cup product of the Weil pairing

$$H^1(k_v, E[p]) \times H^1(k_v, E[p]) \xrightarrow{\text{cup}} H^2(k_v, \mathbb{G}_m) \hookrightarrow \mathbb{R}/\mathbb{Z}.$$

Moreover, the subgroup $E(k_v)/pE(k_v)$ is maximal isotropic.

(Proof: Use Tate local duality.)

Global fields

Let E be an elliptic curve over a *global* field k. Suppose $p \neq \operatorname{char} k$.
Let $V = \prod'_v H^1(k_v, E[p])$ w.r.t. the subgroups $E(k_v)/pE(k_v)$.
We get (V, Q, W).

$$\begin{array}{ccc} & & H^1(k, E[p]) \\ & & \downarrow{\scriptstyle \beta} \\ \prod_v \dfrac{E(k_v)}{pE(k_v)} & \xrightarrow{\alpha} & \prod'_v H^1(k_v, E[p]) \end{array}$$

Theorem

(a) $\operatorname{im}(\alpha)$ *and* $\operatorname{im}(\beta)$ *are maximal isotropic.*

(b) β *is injective; i.e.,* $Ш^1(k, E[p]) = 0$.

(c) $\operatorname{im}(\alpha) \cap \operatorname{im}(\beta) = \beta(\operatorname{Sel}_p E) \simeq \operatorname{Sel}_p E$.

Global fields: proofs

$$\begin{array}{ccc} & & H^1(k, E[p]) \\ & & \big\downarrow \beta \\ \prod_v \frac{E(k_v)}{pE(k_v)} & \xrightarrow{\alpha} & {\prod_v}' H^1(k_v, E[p]) \end{array}$$

Theorem

(a) $\operatorname{im}(\alpha)$ *and* $\operatorname{im}(\beta)$ *are maximal isotropic.*

(b) β *is injective.*

(c) $\operatorname{im}(\alpha) \cap \operatorname{im}(\beta) = \beta(\operatorname{Sel}_p E) \simeq \operatorname{Sel}_p E$.

Sketch of proof.

(a) $\operatorname{im}(\alpha)$ is the W.
$\operatorname{im}(\beta)$: Use reciprocity of the Brauer group
+ 9-term Poitou–Tate exact sequence.

(b) Chebotarev + Sylow p-subgroup of $GL_2(\mathbb{F}_p)$ is cyclic

(c) Definition of $\operatorname{Sel}_p E$!

Predictions

Because of the theorem, we model $\mathrm{im}(\alpha) \cap \mathrm{im}(\beta)$ as a *random* intersection of maximal isotropic subspaces. This suggests:

- Fix k. Fix $p \neq \operatorname{char} k$. As E varies over all elliptic curves over k, for each $d \geq 0$ we have

$$\mathrm{Prob}\,(\dim \mathrm{Sel}_p\, E = d) \;=\; \prod_{j \geq 0} (1 + p^{-j})^{-1} \prod_{j=1}^{d} \frac{p}{p^j - 1}.$$

- For the same family,

$$\mathrm{Average}(\#\,\mathrm{Sel}_p\, E) = 1 + p$$

- For the same family, for each $m \geq 1$,

$$\mathrm{Average}((\#\,\mathrm{Sel}_p\, E)^m) = (1 + p)(1 + p^2) \cdots (1 + p^m).$$

Generalization

k: global field
A: abelian variety over k
λ: $A \to \widehat{A}$ self-dual isogeny coming from $\mathscr{L} \in \operatorname{Pic} A$

Everything works as before, *except*:

- β need not be injective. So one gets only

$$\frac{\operatorname{Sel}_\lambda A}{\text{Ш}^1(k, A[\lambda])} \simeq \operatorname{im}(\alpha) \cap \operatorname{im}(\beta)$$

  instead of $\operatorname{Sel}_\lambda A$ itself as the intersection.
- There may be "causal" elements of $\operatorname{Sel}_\lambda A$.

Jacobians of genus 2 curves

Example

Suppose char $k \neq 2$. Let X range over genus 2 curves $y^2 = f(x)$ with $\deg f = 6$. Let $A = \operatorname{Jac} X$ and $\lambda = [2]$. Then

- $Ш^1(k, A[2]) = 0$ for 100% of the curves (but not all!)
- But $\{$theta characteristics$\}$ is a torsor under $A[2]$. Its class is in $\operatorname{Sel}_2 A$, and Hilbert irreducibility shows that it is nonzero for 100% of curves.

A refinement of the random model now suggests that $\dim_{\mathbb{F}_2} \operatorname{Sel}_2 A$ is shifted by $+1$, which would imply

$$\operatorname{Average}(\# \operatorname{Sel}_2 A) = 6.$$

Predictions for Sel, Ш, rank

Delaunay, in analogy with the Cohen-Lenstra heuristics, proposed a heuristic for the distribution of $\dim Ш(E)[p]$ as E varies over elliptic curves over $\mathbb{Q}$ of fixed rank r. Assume this.

If we also assume a *prior distribution* on ranks, then we can compute a distribution for $\dim \mathrm{Sel}_p E$.

Question

What prior distributions on ranks lead to the Selmer distribution we predict?

Predictions for Sel, Ш, rank

Delaunay, in analogy with the Cohen-Lenstra heuristics, proposed a heuristic for the distribution of $\dim Ш(E)[p]$ as E varies over elliptic curves over $\mathbb{Q}$ of fixed rank r. Assume this.

If we also assume a *prior distribution* on ranks, then we can compute a distribution for $\dim \operatorname{Sel}_p E$.

Question

What prior distributions on ranks lead to the Selmer distribution we predict?

Theorem

There is only one such rank distribution: namely, the one for which

$$\begin{aligned} \operatorname{rk} E(\mathbb{Q}) = 0 \qquad & \text{with probability 50\% and} \\ \operatorname{rk} E(\mathbb{Q}) = 1 \qquad & \text{with probability 50\%.} \end{aligned}$$