Random maximal isotropic subspaces and Selmer groups

Bjorn Poonen
Eric Rains

January 5, 2011
Selmer groups

\( k \): number field
\( E \): elliptic curve over \( k \)

\[
\begin{array}{cccccccc}
0 & \rightarrow & \frac{E(k)}{pE(k)} & \rightarrow & H^1(k, E[p]) & \rightarrow & H^1(k, E)[p] & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & \prod_v \frac{E(k_v)}{pE(k_v)} & \rightarrow & \prod_v H^1(k_v, E[p]) & \rightarrow & \prod_v H^1(k_v, E)[p] & \rightarrow & 0 \\
\end{array}
\]

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

\[
\text{III}(E) := \ker \left( H^1(k, E) \rightarrow \prod_v H^1(k_v, E) \right).
\]

\[
0 \rightarrow \frac{E(k)}{pE(k)} \rightarrow \text{Sel}_p E \rightarrow \text{III}(E)[p] \rightarrow 0.
\]

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

- **Heath-Brown 1994**: Define

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

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

  \[
  \text{Prob}(s(E) = d) = \prod_{j \geq 0} (1 + 2^{-j})^{-1} \prod_{j=1}^d \frac{2}{2j - 1}
  \]

  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 \( s(E) \).

  \[
  \ldots
  \]
How do Selmer groups vary? Average size?

- **Yu 2000**: For $k = \mathbb{Q}$, for the family of all elliptic curves with rational 2-torsion,
  \[
  \text{Average}(\# \text{Sel}_2) \text{ is finite.}
  \]

- **de Jong 2002**: For $k = \mathbb{F}_q(t)$,
  \[
  \text{Average}(\# \text{Sel}_3) \leq 4 + O(1/q).
  \]

  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

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

$$Q : V \to \mathbb{F}_p$$

$$(w, \phi) \mapsto \phi(w).$$

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 $Q|_Z = 0.$
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

\[
\text{Prob}(\dim(Z_1 \cap Z_2) = d) \rightarrow c_{d, p} := \prod_{j \geq 0} (1 + p^{-j})^{-1} \prod_{j=1}^{d} \frac{p}{p^j - 1}
\]

as \(\dim V \rightarrow \infty\).

When \(p = 2\), this is the same distribution on nonnegative integers as in Heath-Brown’s theorem!

Is this a coincidence?
Let $V$ be a locally compact abelian group.
Let $Q : V \to \mathbb{R}/\mathbb{Z}$ 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.,

$$V \to V^* := \text{Hom}_{\text{conts}}(V, \mathbb{R}/\mathbb{Z})$$

$$v \mapsto \langle v, - \rangle$$

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 \(i \in I\). 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 $\infty$-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

  $\text{Prob} \left( \dim_{\F_p} (Z \cap W) = d \right) = c_{d,p}$.

* (It turns out that $Z$ is discrete with probability 1.)
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 $1/2$. 
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 $p \neq \text{char } k_v$).

$$1 \rightarrow \mathbb{G}_m \rightarrow \mathcal{H} \rightarrow E[p] \rightarrow 1$$

gives rise to a quadratic form

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

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 $p \neq \text{char } k_v$).

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

Heisenberg

gives rise to a quadratic form

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

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

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

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 $p \neq \text{char } k$. Let $V = \prod'_v H^1(k_v, E[p])$ w.r.t. the subgroups $E(k_v)/pE(k_v)$. We get $(V, Q, W)$.

\[
\begin{align*}
H^1(k, E[p]) & \xrightarrow{\beta} \prod_v \frac{E(k_v)}{pE(k_v)} \\
& \xrightarrow{\alpha} \prod'_v H^1(k_v, E[p])
\end{align*}
\]

Theorem

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

(b) $\beta$ is injective; i.e., $\text{III}^1(k, E[p]) = 0$.

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

Global fields: proofs

\[ H^1(k, E[p]) \]
\[ \beta \downarrow \]
\[ \prod_{v} \frac{E(k_v)}{pE(k_v)} \overset{\alpha}{\rightarrow} \prod_{v}' H^1(k_v, E[p]) \]

**Theorem**

(a) \( \text{im}(\alpha) \) and \( \text{im}(\beta) \) are maximal isotropic.

(b) \( \beta \) is injective.

(c) \( \text{im}(\alpha) \cap \text{im}(\beta) = \beta(\text{Sel}_p E) \cong \text{Sel}_p E \).

**Sketch of proof.**

(a) \( \text{im}(\alpha) \) is the \( W \).

\( \text{im}(\beta) \): Use reciprocity of the Brauer group + 9-term Poitou–Tate exact sequence.

(b) Chebotarev + Sylow \( p \)-subgroup of \( \text{GL}_2(\mathbb{F}_p) \) is cyclic

(c) Definition of \( \text{Sel}_p E \)!
Predictions

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

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

\[
\text{Prob}(\dim \text{Sel}_p E = d) = \prod_{j \geq 0} (1 + p^{-j})^{-1} \prod_{j=1}^{d} \frac{p}{p^j - 1}.
\]

- For the same family,

\[
\text{Average}(\# \text{Sel}_p E) = 1 + p
\]

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

\[
\text{Average}((\# \text{Sel}_p E)^m) = (1 + p)(1 + p^2) \cdots (1 + p^m).
\]
Generalization

$k$: global field
$A$: abelian variety over $k$
$\lambda: A \to \hat{A}$ self-dual isogeny coming from $\mathcal{L} \in \text{Pic } A$

Everything works as before, except:

- $\beta$ need not be injective. So one gets only

$$\frac{\text{Sel}_\lambda A}{\mathfrak{M}^1(k, A[\lambda])} \cong \text{im}(\alpha) \cap \text{im}(\beta)$$

instead of $\text{Sel}_\lambda A$ itself as the intersection.

- There may be “causal” elements of $\text{Sel}_\lambda A$. 
Example

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

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

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

\[ \text{Average}(\# \text{Sel}_2 A) = 6. \]
Predictions for Sel, $\text{III}$, rank

Delaunay, in analogy with the Cohen-Lenstra heuristics, proposed a heuristic for the distribution of $\dim \text{III}(E)[p]$ 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 $\dim \text{Sel}_p E$.

**Question**

What prior distributions on ranks lead to the Selmer distribution we predict?
Predictions for Sel, III, rank

Delaunay, in analogy with the Cohen-Lenstra heuristics, proposed a heuristic for the distribution of \( \dim \text{III}(E)[p] \) 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 \( \dim \text{Sel}_p E \).

**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

\[
\begin{align*}
\text{rk} \ E(\mathbb{Q}) &= 0 \quad \text{with probability 50\% and} \\
\text{rk} \ E(\mathbb{Q}) &= 1 \quad \text{with probability 50\%}.
\end{align*}
\]