2^k-Selmer groups, the Cassels-Tate pairing, and Goldfeld's conjecture

Alexander Smith

28 September 2020

Part I: Ranks

Goldfeld's conjecture

Definition

Given an elliptic curve

$$E : y^2 = x^3 + ax + b$$

defined over $\mathbb{Q}$, and given a nonzero integer d, the quadratic twist E^d is defined to be the curve

$$E^d : y^2 = x^3 + d^2 ax + d^3 b.$$

Conjecture (Goldfeld 1979)

Given any elliptic curve $E/\mathbb{Q}$,

- *50% of the quadratic twists of E have rank zero,*
- *50% of the quadratic twists of E have rank one, and*
- *0% have any higher rank.*

The minimalist conjecture

Goldfeld's conjecture is sometimes called the minimalist conjecture. It predicts that rank is as small "as possible" for 100% of twists.

Question

Why should a positive percentage of twists have positive rank?

Given $E/\mathbb{Q}$, one fundamental invariant of E is its *global root number* $w(E) \in \pm 1$.

- If $w(E) = +1$, $L(s, E)$ has even order of vanishing at $s = 1$.
- If $w(E) = -1$, $L(s, E)$ has odd order of vanishing at $s = 1$.

Conjecture (Birch and Swinnerton-Dyer)

The order of vanishing of $L(s, E)$ *at* $s = 1$ *equals the rank of* E.

The minimalist conjecture

For fixed E, half the quadratic twists E^d of E have $w(E^d) = +1$, and the remainder have $w(E^d) = -1$.

Conjecture (Goldfeld 1979 revisited)

Given any elliptic curve $E/\mathbb{Q}$,

- *100% of the twists with $w(E^d) = +1$ have rank zero,*
- *100% of the twists with $w(E^d) = -1$ have rank one, and*
- *0% have any higher rank.*

The main result for ranks

Conjecture (Goldfeld 1979 revisited)

Given any elliptic curve $E/\mathbb{Q}$,

- *100% of the twists with $w(E^d) = +1$ have rank zero,*
- *100% of the twists with $w(E^d) = -1$ have rank one, and*
- *0% have any higher rank.*

Theorem (S.)

Given an elliptic curve $E/\mathbb{Q}$ whose 4-torsion obeys some technical conditions,

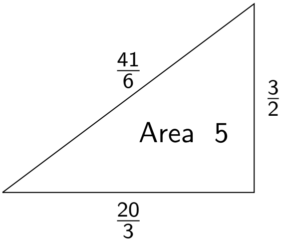
- *100% of the twists with $w(E^d) = +1$ have rank zero,*
- *100% of the twists with $w(E^d) = -1$ have rank* ***at most one****, and*
- *0% have any higher rank.*

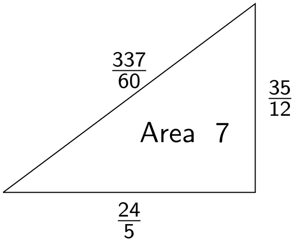
Example: Congruent numbers

Definition

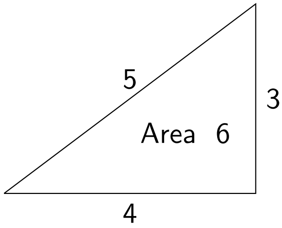
A positive integer d is called a *congruent number* if it is the area of a right triangle with rational side lengths.

Example: Congruent numbers

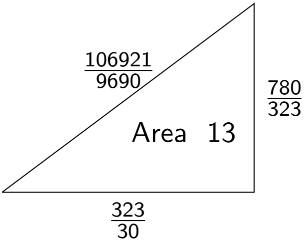




Fibonacci, ∼1200.

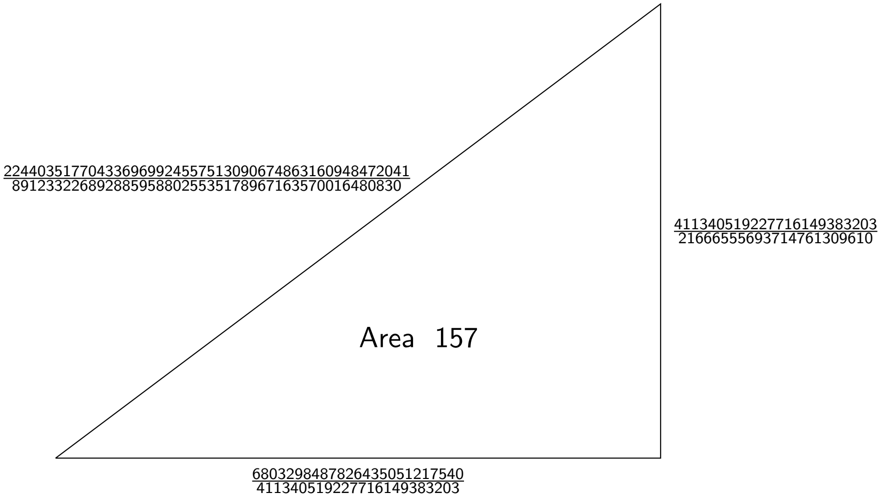


Anon., ∼1000 CE



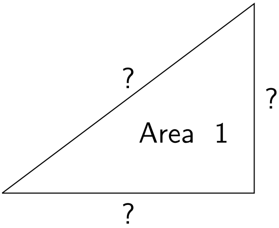
L. Pisanus, ∼1770.

Example: Congruent number



Don Zagier, 1984.

Example: non-congruent numbers



Theorem (Fermat, 1600s)

1 *is not a congruent number.*

Example: Congruent numbers

A positive integer d is a congruent number if and only if the elliptic curve

$$E_{CN}^{d} : y^2 = x^3 - d^2 x$$

has positive rank over $\mathbb{Q}$.

Proposition

Given a positive integer d,

- $w(E_{CN}^{d}) = +1$ *if d equals* $1, 2,$ *or* 3 *mod* 8*, and*
- $w(E_{CN}^{d}) = -1$ *if d equals* $5, 6,$ *or* 7 *mod* 8*.*

Our theorem shows that 0% of d equal to $1, 2,$ or 3 mod 8 are congruent numbers.
It doesn't say anything about d equal to $5, 6$ or 7 mod 8.

Bounds for 0%

Given $\epsilon > 0$ and $N \gg 0$, the number of congruent numbers $d < N$ that equal 1, 2, or 3 mod 8 is predicted to be at most

$$N^{3/4+\epsilon}.$$

In 2017, we bounded this number by

$$\frac{N}{(\log\log\log\log\log N)^{1/3}}.$$

Our current best proven bound is

$$\frac{N}{\exp\left((\log\log\log H)^{1/2}\right)}.$$

Part II:
Selmer Groups

Defining Selmer groups

Definition

Fix a number field F, and take $G_F = \mathrm{Gal}(\overline{F}/F)$. Given a place v of F, take G_v to be the absolute Galois group of the completion of F at v.

Choose a finite G_F-module M. For each place v of F, choose a subgroup $\mathcal{L}_v$ of $H^1(G_v, M)$. We assume $\mathcal{L}_v$ is the set of unramified classes at all but finitely many places.

The Selmer group associated to $(M, (\mathcal{L}_v)_v)$ is then defined by

$$\mathrm{Sel}(M, (\mathcal{L}_v)_v) = \ker\left(H^1(G_F, M) \xrightarrow{\oplus_v \mathrm{res}_{G_v}} \prod_{v \text{ of } F} H^1(G_v, M)/\mathcal{L}_v\right).$$

Example I: Class groups

Given the number field F, take L to be the maximal abelian extension of F that is unramified everywhere. Artin reciprocity gives an isomorphism

$$\mathrm{Gal}(L/F) \cong \mathrm{Cl}\, F.$$

Choose a positive integer n. For every place v of F, take $\mathcal{L}_v$ to be the subset of unramified elements in $H^1(G_v, \mathbb{Z}/n\mathbb{Z})$. Then

$$(\mathrm{Cl}\, F)^*[n] \cong \mathrm{Hom}\left(\mathrm{Gal}(L/F), \mathbb{Z}/n\mathbb{Z}\right) = \mathrm{Sel}\left(\mathbb{Z}/n\mathbb{Z}, (\mathcal{L}_v)_v\right),$$

where the $(\mathrm{Cl}\, F)^*$ denotes the Pontryagin dual $\mathrm{Hom}(\mathrm{Cl}\, F, \mathbb{Q}/\mathbb{Z})$.

Example II: Class groups, again

Choose a number field F and a positive integer n. Define

$$\mathrm{Se}_n F = \{\alpha \in F^\times/(F^\times)^n \,:\, (\alpha) \equiv I^n \text{ for some fractional ideal } I\}.$$

The map from α to I gives a well-defined map

$$\mathrm{Se}_n F \twoheadrightarrow \mathrm{Cl}\, F[n]$$

with kernel $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^n$.

The long exact sequence cohomology sequence associated to

$$1 \to \mu_n \to \overline{F}^\times \to \overline{F}^\times \to 1$$

gives a connecting map

$$\delta : F^\times/(F^\times)^n \xrightarrow{\sim} H^1(G_F, \mu_n)$$

that is an isomorphism by Hilbert 90.

Example II: Class groups, again

We defined

$$\mathrm{Se}_n F = \{\alpha \in F^\times/(F^\times)^n \,:\, (\alpha) \equiv I^n \text{ for some fractional ideal } I\}$$

and considered the connecting map

$$\delta : F^\times/(F^\times)^n \xrightarrow{\sim} H^1(G_F, \mu_n)$$

and a surjection $\mathrm{Se}_n F \twoheadrightarrow \mathrm{Cl}\, F[n]$.

Given ϕ in $H^1(G_F, \mu_n)$, we can verify that ϕ is in the image of $\mathrm{Se}_n F$ by checking that it satisfies a certain local condition $\mathcal{L}_v^\perp$ at each place v.

The map δ then gives an isomorphism between $\mathrm{Se}_n F$ and $\mathrm{Sel}(\mu_n,\, (\mathcal{L}_v^\perp)_v)$. We have an exact sequence

$$0 \to \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^n \xrightarrow{\delta} \mathrm{Sel}(\mu_n,\, (\mathcal{L}_v^\perp)_v) \xrightarrow{\pi_{\mathrm{Cl}}} \mathrm{Cl}\, F[n] \to 0.$$

Example III: Selmer groups for abelian varieties

Choose an elliptic curve E over a number field F, and choose a positive integer n. The long exact sequence associated to

$$0 \to E[n] \to E(\overline{F}) \xrightarrow{\cdot n} E(\overline{F}) \to 0$$

gives connecting maps

$$\delta\colon E(F)/nE(F) \hookrightarrow H^1(G_F, E[n]) \quad \text{and}$$
$$\delta_v\colon E(F_v)/nE(F_v) \hookrightarrow H^1(G_v, E[n]).$$

Take $\mathcal{L}_v$ to be the image of δ_v in $H^1(G_v, E[n])$. Given x in $E(F)/nE(F)$, we find that $\delta(x)$ restricts to lie in each $\mathcal{L}_v$. We then have an exact sequence

$$0 \to E(F)/nE(F) \xrightarrow{\delta} \mathrm{Sel}(E[n], (\mathcal{L}_v)_v) \to Ш(E/F)[n] \to 0.$$

Selmer ranks

Given an elliptic curve E/F and a positive integer n, take $r_n(E)$ to be the maximal integer r so there is some embedding

$$(\mathbb{Z}/n\mathbb{Z})^r \hookrightarrow \frac{\mathrm{Sel}(E[n],\, (\mathcal{L}_v)_v)}{\delta\left(E(F)_{\mathrm{tor}}\right)}.$$

Take $r_{2^\infty}(E)$ to be the limit of the sequence $r_2(E), r_4(E), r_8(E) \dots$.

Facts

- We have $r_2(E) \geq r_4(E) \geq \cdots \geq r_{2^\infty}(E) \geq \mathrm{rank}(E) \geq 0$.
- (Conjectured) $r_{2^\infty}(E) = \mathrm{rank}(E)$.
- The integers $r_2(E), r_4(E), \dots, r_{2^\infty}(E)$ all have the same parity.
- If $F = \mathbb{Q}$, the analytic rank of E has the same parity as E

Setup for the main Selmer result

We say an elliptic curve $E/\mathbb{Q}$ obeys the technical conditions if either

- E satisfies $E[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ (full two torsion) and has no rational cyclic 4-isogeny, or
- E satisfies $E[2](\mathbb{Q}) = 0$ (no two torsion).

Definition

Given $n \geq j \geq 0$, take $P^{\mathrm{Alt}}(j|n)$ to be the probability that a uniformly selected $n \times n$ alternating matrix with coefficients in $\mathbb{F}_2$ has kernel of rank exactly j.
Take

$$P^{\mathrm{Alt}}(j|\infty) = \frac{1}{2} \lim_{n\to\infty} P^{\mathrm{Alt}}(j|2n+j).$$

The main 2^k-Selmer group result

Theorem (S.)

Suppose $E/\mathbb{Q}$ obeys the technical conditions. Choose $k > 1$, and choose a sequence $r_2 \geq r_4 \geq \cdots \geq r_{2^k} \geq 0$ of integers. Then

$$\lim_{N \to \infty} \frac{\#\{0 < d < N \,:\, r_2(E^d) = r_2, \ldots, r_{2^k}(E^d) = r_{2^k}\}}{N}$$

$$= P^{\text{Alt}}(r_{2^k} | r_{2^{k-1}}) \cdot P^{\text{Alt}}(r_{2^{k-1}} | r_{2^{k-2}}) \cdot \cdots \cdot P^{\text{Alt}}(r_4 | r_2) \cdot P^{\text{Alt}}(r_2 | \infty)$$

The sequence r_2, r_4, $\ldots$, r_{2^k} behaves like a Markov process.

Selmer ranks as a Markov chain

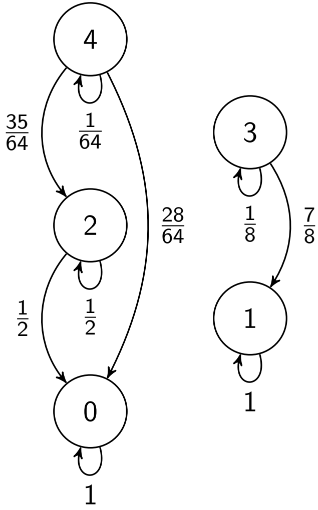


Table: Probability that $r_{2^k}(E^d)$ equals r.

		r 0	1	2	3	4	5
k	1	.21	.42	.28	.08	.01	.00
	2	.35	.49	.15	.01	.00	
	3	.43	.50	.07	.00		
	4	.46	.50	.04			
	5	.48	.50	.02			
	⋮	⋮	⋮	⋮			
	∞	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0

Main consequence

Theorem

Suppose the elliptic curve $E/\mathbb{Q}$ obeys the technical conditions. Then, among the quadratic twists E^d of E,

- *50% have r_{2^∞} equal to zero,*
- *50% have r_{2^∞} equal to one, and*
- *0% have higher r_{2^∞}.*

This additionally holds in the case that

- E satisfies $E[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ (partial two-torsion) and, taking E' to be the associated isogenous curve, $\mathbb{Q}(E'[2]) \neq \mathbb{Q}(E[2])$.

Setup for the main class group result

Given $n \geq j \geq 0$, take $P^{\mathrm{Mat}}(j|n)$ to be the probability that a uniformly selected $n \times n$ matrix with coefficients in $\mathbb{F}_2$ has kernel of rank exactly j.
Take

$$P^{\mathrm{Mat}}(j|\infty) = \lim_{n\to\infty} P^{\mathrm{Mat}}(j|n).$$

Given a number field F and a positive integer n, define the n-class rank $r_n(F)$ to be the maximal integer r so there is some embedding

$$(\mathbb{Z}/n\mathbb{Z})^r \hookrightarrow \mathrm{Cl}\, F.$$

The main 2^k-class group result

Theorem (S.)

Given a sequence of integers $r_4 \geq r_8 \geq \cdots \geq r_{2^k} \geq 0$, we have

$$\lim_{N\to\infty} \frac{\#\{0 < d < N \,:\, r_4\left(\mathbb{Q}(\sqrt{-d})\right) = r_4, \ldots, r_{2^k}(\mathbb{Q}(\sqrt{-d})) = r_{2^k}\}}{N}$$
$$= P^{\mathrm{Mat}}(r_{2^k} | r_{2^{k-1}}) \cdot P^{\mathrm{Mat}}(r_{2^{k-1}} | r_{2^{k-2}}) \cdot \cdots \cdot P^{\mathrm{Mat}}(r_8 | r_4) \cdot P^{\mathrm{Mat}}(r_4 | \infty).$$

For any $C \geq 0$, 100% of imaginary quadratic fields K have $r_2(K) > C$.

Class ranks as a Markov chain

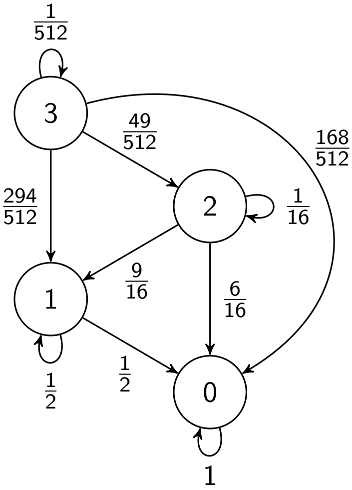


Table: Probability that $r_{2^k}(\mathbb{Q}(\sqrt{-d}))$ equals r

		r				
		0	1	2	3	4
k	2	.29	.58	.13	.01	.00
	3	.63	.36	.01	.00	
	4	.81	.19	.00		
	5	.91	.09			
	6	.95	.05			
	⋮	⋮	⋮			
	∞	1	0	0	0	0

A couple leading questions

- Why do these heuristics involve matrices over $\mathbb{F}_2$? Given an imaginary quadratic field F, is there some important $r_{2^k}(F) \times r_{2^k}(F)$ matrix whose kernel has dimension $r_{2^{k+1}}(F)$?
- Why are the matrices for Selmer ranks of elliptic curves alternating and the matrices for class ranks potentially non-alternating?
- Are there families of number fields where the associated matrices have some sort of forced symmetry?

Part III:
The Cassels-Tate pairing

(Joint with Adam Morgan)

Selmerable modules

Given a number field F, we will define a category SMod_F. Its objects will be tuples $(M, (\mathcal{L}_v)_v)$, where M is a finite G_F module, and where

$$\mathcal{L}_v \subseteq H^1(G_v, M) \quad \text{for each } v,$$

with $\mathcal{L}_v$ equaling the set of unramified classes at v for all but finitely many places v.

A morphism $f\colon (M, (\mathcal{L}_v)_v) \to (M', (\mathcal{L}'_v)_v)$ is any homomorphism $f\colon M \to M'$ satisfying

$$f(\mathcal{L}_v) \subseteq \mathcal{L}'_v \quad \text{for all } v.$$

With this notion of morphism, the notation

$$\mathrm{Sel}(M, (\mathcal{L}_v)_v) = \ker\left(H^1(G_F, M) \xrightarrow{\oplus_v \mathrm{res}_{G_v}} \prod_{v \text{ of } F} H^1(G_v, M)/\mathcal{L}_v\right)$$

defines a functor $\mathrm{Sel}\colon \mathrm{SMod}_F \to \mathrm{Ab}$.

The dual Selmerable module

Given $(M, (\mathcal{L}_v)_v)$ in SMod_F, and given n divisible by the order of n, define

$$M^\vee = \mathrm{Hom}(M, \mu_n).$$

Local Tate duality gives a bilinear pairing

$$H^1(G_v, M) \otimes H^1(G_v, M^\vee) \to \mathbb{Q}/\mathbb{Z}.$$

Taking $\mathcal{L}_v^\perp$ to be the orthogonal complement to $\mathcal{L}_v$ with respect to this pairing, we define

$$(M, (\mathcal{L}_v)_v)^\vee = \left(M^\vee, \left(\mathcal{L}_v^\perp\right)_v\right).$$

This defines a contravariant functor $\vee\colon \mathrm{SMod}_F \to \mathrm{SMod}_F$.

A fun fact

Given $(M, (\mathcal{L}_v)_v)$ in SMod_F, we always have

$$\frac{\#\mathrm{Sel}\, M}{\#\mathrm{Sel}\, M^\vee} = \frac{\# H^0(G_F, M)}{\# H^0(G_F, M^\vee)} \cdot \left(\prod_v \frac{\# H^0(G_v, M) \cdot \# \mathcal{L}_v}{\# H^0(G_v, M^\vee) \cdot \# \mathcal{L}_v^\perp} \right)^{1/2}.$$

This is sometimes called Wiles' formula.

Exact sequences in SMod_F

We call a diagram

$$E = \Big[0 \to (M_1, (\mathcal{L}_{1v})_v) \xrightarrow{\iota} (M, (\mathcal{L}_v)_v) \xrightarrow{\pi} (M_2, (\mathcal{L}_{2v})_v) \to 0\Big]$$

in SMod_F *exact* if it gives an exact sequence of G_F-modules and

$$\mathcal{L}_{1v} = \iota^{-1}(\mathcal{L}_v) \quad \text{and} \quad \mathcal{L}_{2v} = \pi(\mathcal{L}_v)$$

for all v.

Given an exact sequence E, the dual diagram

$$E^\vee = \Big[0 \to M_2^\vee \xrightarrow{\pi^\vee} M^\vee \xrightarrow{\iota^\vee} M_1^\vee \to 0\Big]$$

in SMod_F is also exact.

Question

Given an exact sequence

$$E = \left[0 \to M_1 \xrightarrow{\iota} M \xrightarrow{\pi} M_2 \to 0\right]$$

in SMod_F, and given ϕ in $\operatorname{Sel} M_2$, how can we tell if ϕ lifts to an element of $\operatorname{Sel} M$?

The Cassels-Tate pairing

Theorem (Morgan-S.)

Given exact sequences

$$E = \left[0 \to M_1 \xrightarrow{\iota} M \xrightarrow{\pi} M_2 \to 0\right] \quad \textit{and}$$
$$E^\vee = \left[0 \to M_2^\vee \xrightarrow{\pi^\vee} M^\vee \xrightarrow{\iota^\vee} M_1^\vee \to 0\right]$$

in SMod_F*, we have a natural bilinear pairing*

$$\mathrm{CTP}_E \colon \mathrm{Sel}\, M_2 \otimes \mathrm{Sel}\, M_1^\vee \to \mathbb{Q}/\mathbb{Z}$$

with left and right kernels

$$\pi(\mathrm{Sel}\, M) \quad \textit{and} \quad \iota^\vee(\mathrm{Sel}\, M^\vee),$$

respectively.

The Cassels-Tate pairing

From the exact sequence

$$E = \Big[0 \to M_1 \xrightarrow{\iota} M \xrightarrow{\pi} M_2 \to 0 \Big],$$

in SMod_F, we can always derive an exact sequence

$$\operatorname{Sel} M_1 \xrightarrow{\iota} \operatorname{Sel} M \xrightarrow{\pi} \operatorname{Sel} M_2 \xrightarrow{\mathrm{CTP}_E} (\operatorname{Sel} M_1^\vee)^* \xrightarrow{(\iota^\vee)^*} (\operatorname{Sel} M^\vee)^* \xrightarrow{(\pi^\vee)^*} (\operatorname{Sel} M_2^\vee)^*$$

of finite abelian groups.

Symmetry

The Cassels-Tate pairing for

$$E^\vee = \left[0 \to M_2^\vee \xrightarrow{\pi^\vee} M^\vee \xrightarrow{\iota^\vee} M_1^\vee \to 0\right],$$

is a bilinear map

$$\mathrm{CTP}_{E^\vee} \colon \mathrm{Sel}\, M_1^\vee \otimes \mathrm{Sel}\, M_2^{\vee\vee} \to \mathbb{Q}/\mathbb{Z},$$

compared to $\mathrm{CTP}_E \colon \mathrm{Sel}\, M_2 \otimes \mathrm{Sel}\, M_1^\vee \to \mathbb{Q}/\mathbb{Z}$.

Theorem (Morgan-S.)

Given

$$\phi \in \mathrm{Sel}\, M_2 \cong \mathrm{Sel}\, M_2^{\vee\vee} \quad \textit{and} \quad \psi \in \mathrm{Sel}\, M_1^\vee,$$

we have

$$\mathrm{CTP}_{E^\vee}(\psi, \phi) = \mathrm{CTP}_E(\phi, \psi).$$

Naturality

Given a commutative diagram

$$\begin{array}{ccccccccccc}
E_a & = & \big[\,0 & \longrightarrow & M_{1a} & \xrightarrow{\iota_a} & M_a & \xrightarrow{\pi_a} & M_{2a} & \longrightarrow & 0\,\big] \\
 & & & & \Big\downarrow{\scriptstyle f_1} & & \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle f_2} & & \\
E_b & = & \big[\,0 & \longrightarrow & M_{1b} & \xrightarrow{\iota_b} & M_b & \xrightarrow{\pi_b} & M_{2b} & \longrightarrow & 0\,\big],
\end{array}$$

in SMod_F with exact rows, and given ϕ in $\mathrm{Sel}\, M_{2a}$ and ψ in $\mathrm{Sel}\, M_{1b}^{\vee}$, we have

$$\mathrm{CTP}_{E_a}\left(\phi,\, f_1^{\vee}(\psi)\right) \,=\, \mathrm{CTP}_{E_b}\left(f_2(\phi), \psi\right).$$

Naturality + Symmetry

Given a commutative diagram

$$\begin{array}{ccccccccc} E & = & \big[\,0 & \longrightarrow & M_1 & \xrightarrow{\iota} & M & \xrightarrow{\pi} & M_2 & \longrightarrow & 0\,\big] \\ & & & & \Big\downarrow{\scriptstyle f_1} & & \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle f_2} & & \\ E^\vee & = & \big[\,0 & \longrightarrow & M_2^\vee & \xrightarrow{\pi^\vee} & M^\vee & \xrightarrow{\iota^\vee} & M_1^\vee & \longrightarrow & 0\,\big], \end{array}$$

and given $\phi, \psi \in \mathrm{Sel}\, M_2$, we have

$$\begin{aligned} \mathrm{CTP}_E(\phi,\, f_2(\psi)) &= \mathrm{CTP}_{E^\vee}(f_2(\psi),\, \phi) \quad \text{by symmetry} \\ &= \mathrm{CTP}_E(\psi,\, f_1^\vee(\phi)) \quad \text{by naturality.} \end{aligned}$$

Cassels-Tate pairing for elliptic curves

Take A/F to be an elliptic curve over a number field, choose a positive integer n, and consider

$$E_n = [0 \to A[n] \to A[n^2] \to A[n] \to 0]$$

in SMod_F. From the Weil pairing, we have an isomorphism

$$f_k \colon A[k] \to A[k]^\vee$$

satisfying $f^\vee = -f$ for each $k \geq 0$.
From Naturality + Symmetry, we have

$$\mathrm{CTP}_{E_n}(\phi,\, f_n(\psi)) = -\mathrm{CTP}_{E_n}(\psi,\, f_n(\phi))$$

for all $\phi, \psi \in \mathrm{Sel}\, A[n]$.
This antisymmetric pairing has kernel $n \cdot \mathrm{Sel}\, A[n^2]$.

The Markov chain

Question

Choose an elliptic curve A randomly with 2-Selmer rank r_2. Why should the probability that it has 4-Selmer rank r_4 equal $P^{\mathrm{Alt}}(r_4|r_2)$?

Our answer is that Cassels-Tate pairing associated to

$$0 \to A[2] \to A[4] \to A[2] \to 0$$

behaves like a random alternating $r_2 \times r_2$ matrix as you move through these elliptic curves.

The Markov chain

Question

Choose an elliptic curve A randomly with 4-Selmer rank r_4. Why should the probability that it has 8-Selmer rank r_8 equal $P^{\mathrm{Alt}}(r_8|r_4)$?

Considering the Cassels-Tate pairing on

$$E_4 \;=\; \big[0 \to A[4] \to A[16] \to A[4] \to 0\big],$$

we find that the definition

$$\langle 2\phi, 2\psi\rangle = 2 \cdot \mathrm{CTP}_{E_4}(\phi, \psi)$$

gives a well-defined alternating pairing

$$\langle\ ,\ \rangle \colon 2 \cdot \mathrm{Sel}\, A[4] \otimes 2 \cdot \mathrm{Sel}\, A[4] \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

with kernel $4 \cdot \mathrm{Sel}\, A[8]$.
Our answer is that $\langle\ ,\ \rangle$ behaves like a random alternating $r_4 \times r_4$ matrix.

Class groups

Take F to be a number field and choose $n > 1$. Previously, we gave an isomorphism

$$(\mathrm{Cl}\, F)^*[n] \cong \mathrm{Sel}(\mathbb{Z}/n\mathbb{Z}, (\mathcal{L}_v)_v)$$

and an exact sequence

$$0 \to \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^n \xrightarrow{\delta} \mathrm{Sel}(\mu_n, (\mathcal{L}_v^\perp)_v) \xrightarrow{\pi_{\mathrm{Cl}}} \mathrm{Cl}\, F[n] \to 0.$$

The natural pairing

$$(\mathrm{Cl}\, F)^*[n] \otimes \mathrm{Cl}\, F[n] \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z},$$

has kernels $n \cdot (\mathrm{Cl}\, F)^*[n^2]$ and $n \cdot \mathrm{Cl}\, F[n^2]$, and can be identified via π_{Cl} with the Cassels-Tate pairing

$$\mathrm{Sel}\, \mathbb{Z}/n\mathbb{Z} \otimes \mathrm{Sel}\, \mu_n \longrightarrow \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

associated with the sequence

$$0 \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n^2\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0.$$

Symmetry?

If F contains μ_n, we can embed $\mathrm{Sel}\,\mathbb{Z}/n\mathbb{Z}$ in $\mathrm{Sel}\,\mu_n$ via an isomorphism $\mathbb{Z}/n\mathbb{Z}$ to μ_n, but there's no reason a priori to expect the corresponding Cassels-Tate pairing

$$\mathrm{Sel}\,\mathbb{Z}/n\mathbb{Z} \otimes \mathrm{Sel}\,\mathbb{Z}/n\mathbb{Z} \longrightarrow \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

to have any kind of symmetry.
In the elliptic curve case, an isomorphism $A[n^2] \xrightarrow{\sim} A[n^2]^\vee$ led to the symmetry. So it was not surprising to find

Theorem (Morgan-S., Lipnowski-Sawin-Tsimerman '20)

If F contains μ_{n^2}, the above pairing is a symmetric pairing.

Imaginary quadratic fields

Because the imaginary quadratic fields almost never have extra roots of unity, we expect the Cassels-Tate pairing that gives the 4-class rank from the 2-class rank to just be a random $r_2 \times r_2$ matrix in $\mathbb{F}_2$, etc.

Part IV: Why 2?

2-torsion

Given an elliptic curve $A/\mathbb{Q}$ and a squarefree integer $d > 1$, there is a geometric isomorphism

$$\beta_d \colon A^d \to A$$

given by scaling both coordinates.
This is not a G_F-equivariant map. Otherwise, twisting wouldn't be very interesting.
However, it is equivariant on two torsion. In particular, we can consider $\operatorname{Sel} A^d[2]$ as a subgroup of $H^1(G_F, A[2])$.
The question for 2-Selmer groups then becomes "How does the portion of $H^1(G_F, A[2])$ cut out by a random set of local conditions behave?", which is easier.

8-torsion?

Given squarefree integers d_1, d_2, d_3, we can express the G_F-module

$$A^{d_1 d_2 d_3}[8]$$

as a subquotient of

$$A[8] \oplus A^{d_1}[8] \oplus A^{d_2}[8] \oplus A^{d_3}[8] \oplus A^{d_1 d_2}[8] \oplus A^{d_2 d_3}[8] \oplus A^{d_1 d_3}[8].$$

E.g. the module $A^{30}[8]$ can be found as a subquotient of

$$A[8] \oplus A^{2}[8] \oplus A^{3}[8] \oplus A^{5}[8] \oplus A^{6}[8] \oplus A^{10}[8] \oplus A^{15}[8].$$

And $A^{210}[16]$ can be found as a similar subquotient, etc.

The plan

From this trick, once we have the 2^k-Selmer groups of a somewhat sparse portion of the twists with $d < N$, we can figure out the 2^k-Selmer groups at all the other twists.

We need to show that, no matter how the 2^k-Selmer groups of this sparse set of twists behave, the Cassels-Tate pairings that give 2^{k+1}-Selmer ranks are forced to be uniformly distributed among all alternating possibilities.

This is possible, but requires a fiddly blend of algebra, combinatorics, and analysis.

Some bad news

$A[3]$ is not a subquotient of

$$\bigoplus_{d \neq \square} A^d[3].$$

Thank you!