GALOIS COHOMOLOGY AND THE GREENBERG–WILES FORMULA: CRM MINICOURSE

ALEXANDER SMITH

Part of the difficulty in recommending the tools in Galois cohomology is that the resources on these tools are somewhat limited. The best source is:

- Milne, *Arithmetic duality theorems*, part I. This has all of the important main results of Tate on Galois cohomology over global and local fields.

The source which develops the theory with no detail skipped is

- Neukirch, Schmidt, Wingberg, *Cohomology of number fields*.

There are many good sources on group cohomology and continuous cochain cohomology. I learned it from the two relevant chapters of Cassels–Fröhlich.

A smattering of other sources I would recommend are:

- Supplementary sheet on Galois cohomology by Ross Paterson and Happy Upal
- The first couple chapters of *Euler Systems* by Karl Rubin.
- The Selmer group, the Shafarevich–Tate group, and the weak Mordell–Weil theorem by Bjorn Poonen.
- My two papers with Adam Morgan, "The Cassels–Tate pairing for finite Galois modules" and "Field change for the Cassels–Tate pairing and applications to class groups", with similar caveats to *Cohomology of number fields*.

1. First half: The tools

Galois modules. Take F to be a field of characteristic 0, and take $\overline{F}$ to be an algebraic closure of F, with $G_F = \mathrm{Gal}(\overline{F}/F)$ the associated absolute Galois group. This is naturally a profinite group, a type of topological group. The map

$$H \subseteq G_F \mapsto \text{Fixed field of } \overline{F} \text{ under } H$$

defines a bijection

$$\{\text{Open subgroups of } G_F\} \xrightarrow{\sim} \{\text{Finite extensions of } F \text{ in } \overline{F}\}.$$

A Galois module M over F will be an abelian group with an action of G_F such that the stabilizer of every $m \in M$ is an open subgroup of G_F. If we think of M as a discrete topological space, this means that the action of G_F on M is required to be *continuous*.

Example 1.1.

E-mail address: asmith@northwestern.edu.
Date: May 4, 2026.

- For every positive integer n, the group $\mathbb{Z}/n\mathbb{Z}$ with the trivial action of G_F.
- The unit group $\overline{F}^\times$ with the standard action of G_F.
- The subgroup of units μ_n of $\overline{F}$. The map taking ϕ to $\phi(1)$ defines an isomorphism
$$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \overline{F}^\times) \xrightarrow{\sim} \mu_n.$$
- More generally, for any module M over F, we can define a *dual module*
$$M^\vee := \text{Hom}(M, \overline{F}^\times).$$
- For any elliptic curve E defined over F, the subgroup $E[n]$ of $E(\overline{F})$ killed under multiplication by n defines a G_F module of size n^2.

  More generally, if $\phi : E \to E'$ is an isogeny of degree d, then the kernel of ϕ in $E(\overline{F})$ is a G_F module of size d that we call $E[\phi]$.

  There is an isogeny $\phi' : E' \to E$ known as the dual isogeny so that $\phi' \circ \phi$ equals multiplication by d. We have a canonical identification
$$E'[\phi'] \cong (E[\phi])^\vee$$
  coming from the Weil pairing.
- If K/F is a finite extension and M is a module over K, then there is an induced module
$$\text{Ind}_{K/F} M := \mathbb{Z}[G_F/G_K] \otimes M.$$
  In this tensor product, a typical basis element looks like $[\sigma] \otimes m$ with σ in G_F. These elements satisfy
$$[\sigma\tau] \otimes m = [\sigma] \otimes \tau m \quad \text{for} \quad \tau \in G_K.$$
  Given $\sigma_0 \in G_F$, the action of G_F is defined by
$$\sigma_0 \left([\sigma] \otimes m\right) = [\sigma_0\sigma] \otimes m.$$

If M is finite, there is an obvious perfect pairing (the *evaluation pairing*)
$$M \otimes M^\vee \to \overline{F}^\times$$
given by $(x, \phi) \mapsto \phi(x)$.

Galois cohomology. Given a closed subgroup G of G_F, and a nonnegative integer i, we may define the i^{th} cohomology functors
$$H^i(G, –) : \text{Category of modules over } F \to \text{Abelian groups}.$$
(The morphisms in the first category are the G_F-equivariant homomorphisms of abelian groups). If $G = G_F$, we also write this map as $H^i(F, –)$.

For $i = 0$, this is given by
$$H^0(G, M) = \{x \in M \ : \ \sigma(x) = x \text{ for all } \sigma \in H\}.$$

For $i = 1$, we have
$$H^1(G, M) = Z^1(G, M)/B^1(G, M),$$

where

$$Z^1(G, M) \subseteq \text{Hom}_{\text{cont}}(G, M)$$

(the *cocycles*) is the set of continuous maps $\phi : G \to M$ that satisfy the *crossed homomorphism condition*

$$\phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma),$$

and where B^1 (the *coboundaries*) is a certain subgroup of Z^1.

$H^2(G, M)$ can be defined as Z^2/B^2, where Z^2 is a subgroup of the continuous maps on $G \times G \to M$ and B^2 is a certain subgroup of that; and so on, with higher powers of G for higher cohomology groups.

Given a short exact sequence

$$0 \to M_1 \to M \to M_2 \to 0$$

in the category of modules over F, we have an associated long exact sequence

$$0 \to H^0(G, M_1) \to H^0(G, M) \to H^0(G, M_2) \to H^1(G, M_1) \to \dots.$$

The maps where the degree increases are known as *connecting maps*.

Example 1.2. For any F, $H^1(F, \overline{F}^\times) = 0$ (Hilbert 90). We have an exact sequence of Galois modules

$$0 \to \mu_n \to \overline{F}^\times \xrightarrow{n} \overline{F}^\times \to 0,$$

so the exact sequence gives

$$H^0(F, \overline{F}^\times) \to H^0(F, \overline{F}^\times) \to H^1(F, \mu_n) \to 0.$$

Or

$$F^\times/(F^\times)^n \cong H^1(G_F, \mu_n).$$

Galois cohomology over local fields. Suppose F_v is a nonarchimedean local field of characteristic 0. Take $G_v = G_{F_v}$ and $I_v \subseteq G_v$ the associated inertia subgroup.

If M is a G_v-module, then the *unramified part* of $H^1(G_v, M)$ is the image of $H^1(G_v/I_v, M^{I_v})$. This is simple to calculate, since G_v/I_v is a procyclic group, topologically generated by a Frobenius element Fr_v. Its size is seen to equal $\#M^{G_v}$.

The quotient $H^1(G_v, M)/H^1_{\text{ur}}(G_v, M)$ can be more complicated, but we have a classic result of Tate to work with this. Corresponding to the bilinear map $M \times M^\vee \to \overline{F_v}^\times$ is a cup product

$$H^1(G_v, M) \otimes H^1(G_v, M^\vee) \to H^2(G_v, \overline{F_v}^\times) = \text{Br}(F_v).$$

This final Brauer group is $\mathbb{Q}/\mathbb{Z}$ for a nonarchimedean local field, and $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and 0 for $\mathbb{R}$ and $\mathbb{C}$, respectively.

Theorem 1.3 (Tate)**.** *This cup product is a perfect pairing.*

If v is nonarchimedean, $|M|$ is indivisible by the residue characteristic of F_v, and $M^{I_v} = M$, then the orthogonal complement of $H^1_{\text{ur}}(G_v, M)$ is $H^1_{\text{ur}}(G_v, M^\vee)$.

The second part of this theorem may be phrased in terms of a short exact sequence

$$0 \to H^1_{\text{ur}}(G_v, M) \to H^1(G_v, M) \to \text{Hom}(H^1_{\text{ur}}(G_v, M^\vee), \mathbb{Q}/\mathbb{Z}) \to 0.$$

Galois cohomology of global fields. We just showed that $H^1(G_v, M)$ is not to be feared. However, if F is a number field (or, with appropriate caveats, a global function field), then $H^1(G_F, M)$ is somewhat scarier.

Example 1.4. If $M = \mathbb{Z}/2\mathbb{Z}$, then $H^1(G_F, M) \cong F^\times/(F^\times)^2$. This is a finite, easily calculable group if F is a local field; if the residue characteristic is not 2, it has cardinality 4. But, for $F = \mathbb{Q}$, this is isomorphic to the set of squarefree integers.

But the local theory gives us some information about what must be happening globally.

Definition 1.5. Suppose F is a number field, and F_v is a completion of F at some place; so F_v is either a p-adic field, or $\mathbb{R}$ or $\mathbb{C}$. We have a diagram

$$\begin{array}{ccc} F & \longrightarrow & F_v \\ \downarrow & & \downarrow \\ \overline{F} & \dashrightarrow & \overline{F_v} \end{array}.$$

There are many ways to choose the final arrow in this diagram; but, once we pick one, we may think of G_v as a subgroup of G_F, since automorphisms of the second column give automorphisms of the first. If we choose a different one, it may lead to a conjugate subgroup of G_v. The preferred strategy for dealing with this is to *ignore the problem* until you need to upload to arXiv.

But, having blessed a particular image of G_v in G_F, we may define a restriction map

$$H^i(F, M) \to H^i(F_v, M)$$

by restricting a cocycle $\phi : G_F \times \cdots \times G_F \to M$ to $\phi : G_v \times \cdots \times G_v \to M$.

Example 1.6. Take E to be an elliptic curve over a number field F. Given an integer $n \geq 2$, we define a subgroup

$$\mathrm{Sel}_n E \subseteq H^1(F, E[n])$$

as the set of ϕ in this cohomology group such that the image ϕ_v in $H^1(F_v, E[n])$ satisfies

$$\phi_v \in \ker\left(H^1(F, E[n]) \to H^1(F, E(\overline{F_v}))\right).$$

This *Selmer group* has two wonderful properties:

- It's finite, and can be calculated unconditionally.
- It contains the image of $E(F)$ under the connecting map

$$E(F) = H^0(F, E(\overline{F})) \to H^1(F, E[n])$$

corresponding to the short exact sequence $0 \to E[n] \to E(\overline{F}) \to E(\overline{F})$.

Selmer groups are essential tools for understanding rational points of elliptic curves, or of abelian varieties more generally.

With only this as motivation, I introduce a category:

Definition 1.7. Given a number field F, take SMod to be the category of tuples $(M, (\mathscr{L}_v)_v)$, where

- M is a finite G_F module, and
- For each place v of F, $\mathscr{L}_v$ is a subgroup of $H^1(G_v, M)$, with all but finitely many chosen to be $H^1_{\text{ur}}(G_v, M)$.

This is the category of decorated Galois modules over F.

The *Selmer group* of this object is defined by

$$\text{Sel}\,(M, (\mathscr{L}_v)_v) = \{\phi \in H^1(F, M) \,:\, \phi_v \in \mathscr{L}_v \text{ for all } v\},$$

where ϕ_v is the image of ϕ in $H^1(F_v, M)$.

A morphism in this category $(M, (\mathscr{L}_v)_v) \to (M', (\mathscr{L}'_v)_v)$ will be a G_F-equivariant map $M \to M'$ that carries $\mathscr{L}_v$ into $\mathscr{L}'_v$ for every v. This is defined so taking the Selmer group is a functor

$$\text{Sel} \,:\, \text{SMod} \to \text{Ab}.$$

This category has a duality $\vee : \text{SMod} \to \text{SMod}^{\text{op}}$:

$$(M, (\mathscr{L}_v)_v)^\vee = (M^\vee, (\mathscr{L}_v^\perp)_v),$$

where $\mathscr{L}_v^\perp \subseteq H^1(F_v, M^\vee)$ is the orthogonal pairing to $\mathscr{L}_v$ under the Tate pairing.

The last twenty years have given plenty of evidence of the importance of the following theorem to arithmetic statistics:

Theorem 1.8 (Greenberg–Wiles formula)**.**

$$\frac{\#\text{Sel}(M, (\mathscr{L}_v)_v)}{\#\text{Sel}(M, (\mathscr{L}_v)_v)^\vee} = \frac{\#H^0(F, M)}{\#H^0(F, M^\vee)} \cdot \prod_v \frac{\#\mathscr{L}_v}{\#M^{G_v}}$$

We sometimes call this expression the *Tamagawa ratio* for a decorated module.

Example 1.9. Take $M = (\mathbb{Z}/n\mathbb{Z}, (H^1_{\text{ur}}(F_v, \mathbb{Z}/n\mathbb{Z})))$. Then Sel$M$ is identified with the continuous homomorphisms from G_F to $\mathbb{Z}/nZ$ that are unramified at all primes. In other words,

$$\text{Sel}\, M \cong \text{Hom}(\text{Cl}\, F, \mathbb{Z}/n\mathbb{Z}) = \text{Cl}^*\, F[n].$$

Our calculations before show that most of the terms in the product in the Greenberg–Wiles formula. The only terms that don't are the archimedean ones; for these, $\mathscr{L}_v$ is trivial and M^{G_v} has size n. So the Greenberg–Wiles formula takes the form

$$\frac{\#\text{Cl}^*\, F[n]}{\#\text{Sel}\, \mu_n} = \frac{n}{\#H^0(F, \mu_n)} \cdot n^{-r_1 - r_2}.$$

What is Sel μ_n? It's the Selmer group closest to approximating Cl $F[n]$, sometimes called the *Selmer group* of a number field. A little work gives an exact sequence

$$0 \to \mathcal{O}_F^\times / \left(\mathcal{O}_F^\times\right)^n \to \text{Sel}\, \mu_n \to \text{Cl}\, F[n] \to 0$$

This final group has size equal to the dual n torsion, and we're left with

$$\#\mathcal{O}_F^\times / \left(\mathcal{O}_F^\times\right)^n = n^{r_1 + r_2 - 1} \cdot \#H^0(G_F, \mu_n).$$

But you already knew that.

Exercise. *Why did you already know that?*

A sequence

$$0 \to (M_1, (\mathscr{L}_{1v})_v) \xrightarrow{\iota} (M, (\mathscr{L}_v)_v) \xrightarrow{\pi} (M_2, \mathscr{L}_{2v})_v \to 0$$

is *exact* if

- It is exact in the category of G_F modules;
- For all v, $\mathscr{L}_{1v} = \iota^{-1}(\mathscr{L}_v)$ (ι is *strictly monic*; the local conditions on M_1 are as large as possible).
- For all v, $\mathscr{L}_{2v} = \pi(\mathscr{L}_v)$ (π is *strictly epic*; the local conditions on M_2 are as small as possible.)

Given an exact sequence, we get an exact sequence of Selmer groups

$$H^0(F, M_2) \to \text{Sel}\, M_1 \to \text{Sel}\, M \to \text{Sel}\, M_2 \to \text{Hom}(\text{Sel}\, M_1^\vee, \mathbb{Q}/\mathbb{Z})$$

where the first map is the usual connecting map, and the last map comes from the Cassels–Tate pairing; which we will not talk about, but we will use the existence of this exact sequence.

A final result we will use is

Theorem 1.10 (Shapiro's lemma)**.** *For any extension of fields K/F and any G_K module M, there is a natural isomorphism*

$$H^i(K, M) \cong H^i(F, \text{Ind}_{K/F} M).$$

For each place v of K, this extends to a map

$$\prod_{w|v \text{ of } K} H^i(K_w, M) \cong H^i(F_v, \text{Ind}_{K/F} M),$$

For $i = 1$, this map associates the direct product of the unramified local conditions on the left with the unramified local conditions on the right.

As a result, given an extension K/F of number fields, we have a final functor

$$\text{Ind}_{K/F} : \text{SMod}_K \to \text{SMod}_F$$

taking decorated G_K-modules to decorated G_F-modules; and this functor is defined so

$$\text{Sel}_K M = \text{Sel}_F \text{Ind}_{K/F} M$$

for any decorated G_K module M.

Example 1.11. Given a Galois extension of number fields K/F, Shapiro's lemma gives a natural isomorphism of Selmer groups

$$\text{Sel}_K \mathbb{Z}/n\mathbb{Z} \cong \text{Sel}_F \mathbb{Z}/n\mathbb{Z}[\text{Gal}(K/F)],$$

where both modules are decorated with the unramified local conditions.

The Selmer group on the left comes with a natural Galois action; we can conjugate homomorphisms $\phi : G_F \to \mathbb{Z}/n\mathbb{Z}$ by an element in G_F. As an automorphism on

$\mathrm{Sel}_F\, \mathbb{Z}/n\mathbb{Z}[\mathrm{Gal}(K/F)]$, this corresponds functorially to an automorphism of $\mathbb{Z}/n\mathbb{Z}[\mathrm{Gal}(K/F)]$, namely the automorphism defined by

$$[\tau] \otimes m \mapsto [\tau\sigma^{-1}] \otimes m.$$

Exercise 1.12.

- Given a procyclic group H with a topological generator σ and a H-module M, show that evaluation at σ defines an automorphism
$$H^1(H, M) \cong M/(\sigma - 1)M.$$
This set of covariants is sometimes written as M_H.
- In this case, assuming M is finite, show that M_H and M^H have the same size by considering the endomorphism $\sigma - 1$ on M.
- In the case $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, give a module M of size 8 where $\#M^H$ and $\#M_H$ are distinct .
- Given a nonarchimedean local field F_v, and given a G_v module M such that $M^{I_v} = M$ and such that $\#M$ is indivisible by the residue characteristic of F_v, give a filtration
$$0 \to M_{G_v} \to H^1(G_v, M) \to M(-1)^{G_v} \to 0,$$
where $M(-1)$ denotes a negative Tate twist.

Exercise 1.13. Suppose F is a number field that contains μ_n. From the isomorphism of G_F modules $\mathbb{Z}/n\mathbb{Z}$ and μ_n, define a homomorphism

$$\mathrm{Cl}^*F[n] \to \mathrm{Cl}\ F[n].$$

How large can the kernel/cokernel of this map be?

Exercise 1.14. Given an exact sequence of H-modules

$$0 \to M_1 \xrightarrow{\iota} M \to M_2 \to 0,$$

the connecting map $\delta : H^0(H, M_2) \to H^1(H, M_1)$ is defined as follows:

- Given $y \in M_2^H$, choose an element $x \in M$ mapping to y.
- The map $\sigma \mapsto (\sigma x - x)$, $\sigma \in H$ takes values in the image of M_1; take $\delta(y)$ to be represented by the map $\sigma \mapsto \iota^{-1}(\sigma x - x)$.

Show that this connecting map is well defined and that the sequence

$$H^0(H, M) \to H^0(H, M_2) \to H^1(H, M_1) \to H^1(H, M)$$

is exact.

Given a field F, use this to give an explicit construction for the isomorphism

$$F^\times/(F^\times)^n \cong H^1(F, \mu_n).$$

Exercise 1.15. Take $K = \mathbb{Q}(\sqrt{d})$ with d not a square. Endow $\mathbb{Z}/2\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ with the unramified local conditions $(\mathscr{L}_v)_v$.

There is a unique exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})] \to \mathbb{Z}/2\mathbb{Z} \to 0$$

in the category of $G_{\mathbb{Q}}$ modules. From this, define an exact sequence of decorated modules

$$0 \to (\mathbb{Z}/2\mathbb{Z}, (\mathscr{L}_{1v})_v) \to (\mathbb{Z}/2\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})], (\mathscr{L}_v)_v) \to (\mathbb{Z}/2\mathbb{Z}, (\mathscr{L}_{2v})_v) \to 0.$$

- What are $\mathscr{L}_{1v}$ and $\mathscr{L}_{2v}$ when v is unramified in $K/\mathbb{Q}$?
- How about when v ramifies?
- Call the first decorated module M_1 and the last module M_2. Show that $M_2 = M_1^\vee$ as a decorated module except at $v = 2$.
- Show $\mathrm{Sel}\, M_2 = 0$ and $\mathrm{Sel}\, M_1^\vee = 0$.
- Taking Δ to be the discriminant of K, show that $\mathrm{Sel}\, M_1$ has dimension $\omega(\Delta)$, the number of primes ramifying in $K/\mathbb{Q}$. From this, show Gauss's result

$$\#\mathrm{Cl}\ K[2] = 2^{\omega(\Delta)-1}.$$

Exercise 1.16.

- Take $K = \mathbb{Q}(\sqrt{d})$. Give an automorphism between $\mathrm{Hom}(\mathrm{Cl}\ K[3], \mathbb{Q}/\mathbb{Z})$ (what I call $\mathrm{Cl}^* K[3]$) and $\mathrm{Sel}\, (\mathbb{Z}/3\mathbb{Z})^{\chi_d}$, where $(\mathbb{Z}/3\mathbb{Z})^{\chi_d}$ is a copy of $\mathbb{Z}/3\mathbb{Z}$ with $G_{\mathbb{Q}}$ action given by
$$\sigma x = \frac{\sigma(\sqrt{d})}{\sqrt{d}} x,$$
and where this module has been endowed with the unramified local conditions at all places.
- Show that the module $((\mathbb{Z}/3\mathbb{Z})^{\chi_d})^\vee$ and $(\mathbb{Z}/3\mathbb{Z})^{\chi_{-3d}}$ are isomorphic as modules. How do their local conditions differ?
- Prove the *Scholz reflection principle*:
$$\left|\dim \mathrm{Cl}\ \mathbb{Q}(\sqrt{d})[3] \ - \ \dim \mathrm{Cl}\ \mathbb{Q}(\sqrt{-3d})[3]\right| \leq 1.$$

2. Second half: Applying the tools

Definition 2.1. If E is an elliptic curve over a number field F, and $\phi : E \to E'$ is an isogeny, then $E[\phi]$ is most naturally endowed with the local conditions

$$\mathscr{L}_v = \ker\left(H^1(F_v, E[\phi]) \to H^1(F_v, E)\right).$$

The ϕ-Selmer group of E is the Selmer group of this object.

The dual Galois module to $E[\phi]$ is $E'[\phi']$, where ϕ' is the dual isogeny, and the decorations for this object are defined in the natural way in E'. In the case that $\phi = [n]$, these decorated modules are isomorphic (a result of Tate). In other cases, they are not, and Greenberg–Wiles can give us information.

Example 2.2. Take $E : y^2 = x^3 + ax^2 + bx$ to be an elliptic curve over $\mathbb{Q}$. This has a rational 2-torsion point, at $(0, 0)$. We take $\phi : E \to E_0$ to be the isogeny with kernel generated by this point, and ϕ_0 to be the dual isogeny.

Given squarefree d, we have a twist

$$E^d : dy^2 = x^3 + ax^2 + bx.$$

This still has a rational point at $(0,0)$, and we denote the respective isogeny also by ϕ, this time as a map from E^d to E_0^d.

In this case, $E^d[\phi]$ and $E_0^d[\phi_0]$ are always isomorphic as modules to $\mathbb{F}_2$, but they can have complicated local conditions.

For instance, take $p|d$ to be an odd prime of good reduction for E. The local conditions $\mathscr{L}_p$ for $E^d[\phi]$ are the kernel of the map

$$H^1(\mathbb{Q}_p, E^d[\phi]) \to H^1(\mathbb{Q}_p, E^d[2^\infty])$$

From the long exact sequence associated to

$$0 \to E^d[\phi] \to E^d[2^\infty] \to E_0^d[2^\infty] \to 0$$

this kernel is identified with the cokernel of the final map of

$$0 \to \mathbb{F}_2 \to \left(E^d[2^\infty]\right)^{G_p} \to \left(E_0^d[2^\infty]\right)^{G_p}.$$

Everything to this point works at all places besides 2. But now, we take advantage of the fact that I_p acts trivially on $E[2^\infty]$ and the fact that we are twisting by a character ramified at p to say that

$$E^d[2^\infty]^{G_p} = E^d[2]^{G_p} \cong E[2]^{G_p} \quad \text{and} \quad E_0^d[2^\infty]^{G_p} = E_0^d[2]^{G_p} \cong E_0[2]^{G_p}.$$

Then

$$\#\mathscr{L}_p = 2 \cdot \frac{\#H^0(G_p, E_0[2])}{\#H^0(G_p, E[2])}.$$

And Greenberg–Wiles gives

Proposition 2.3. *If $\phi : E \to E_0$ is fixed and d is allowed to vary,*

$$\frac{\#\text{Sel}_\phi E^d}{\#\text{Sel}_{\phi_0} E_0^d} \approx \prod_{p|d} \frac{\#H^0(\mathbb{Q}_p, E_0[2])}{\#H^0(\mathbb{Q}_p, E[2])}.$$

Take $K/\mathbb{Q}$ to be the minimal extension so $E[2]$ is trivial over G_K. Since E has a rational 2-isogeny, K is either a quadratic field or equal to $\mathbb{Q}$. Define K_0 similarly. Then the above ratio of Selmer sizes is approximately

$$2^r \quad \text{where} \quad r = \#\{p|d \,:\, K_0/\mathbb{Q} \text{ splits at } p\} - \#\{p|d \,:\, K/\mathbb{Q} \text{ splits at } p\}.$$

The most common case is that K and K_0 are distinct quadratic extension.

Proposition 2.4. *In this case,*

$$\frac{\#\text{Sel}_\phi E^d}{\#\text{Sel}_{\phi_0} E_0^d} = \begin{cases} \gg 1 & \textit{for } 50\% \textit{ of } d \\ \ll 1 & \textit{for } 50\% \textit{ of } d \\ \approx 1 & \textit{for } 0\% \textit{ of } d. \end{cases}$$

From the short exact sequence

$$0 \to E[\phi] \to E[2] \to E_0[\phi_0] \to 0,$$

a portion of the long exact sequence gives

$$E_0^d[\phi_0] \to \text{Sel}_\phi E^d \to \text{Sel}_2 E^d \to \text{Sel}_{\phi_0} E_0^d.$$

So the ϕ-Selmer groups being large in this case means that the 2-Selmer groups are also large. Specifically, for any positive integer r, more than 50% of the twists of E have 2-Selmer rank larger than r.

This should be compared with:

Theorem 2.5 (Kane 2012, S. '26)**.** *Suppose $E/\mathbb{Q}$ either*

- *Has no rational 2 torsion, or*
- *Has full rational 2-torsion; and, given any degree 2 isogeny $\phi : E \to E_0$, $E_0[2]$ does not have full rational 2-torsion.*

Then the statistic

$$\dim \text{Sel}^2 E^d - \dim H^0(G_\mathbb{Q}, E[2])$$

has the Poonen–Rains distribution as d varies; it behaves like the kernel of a large random alternating matrix over $\mathbb{F}_2$.

A moral of the partial two torsion case is that 2-isogenies get in the way of the 2-Selmer group behaving nicely. So it makes sense that the first case here gives a nice distribution. Why the second?

Theorem 2.6 (Kane–Klagsbrun '17, S. '25)**.** *Take $\phi : E \to E_0$, $\phi_0 : E_0 \to E$ as above. Fix an integer k, and take $\mathscr{D}_k(H)$ to be the set of squarefree integers d of magnitude at most H so that $\frac{\#\text{Sel}_\phi E^d}{\#\text{Sel}_{\phi_0} E_0^d} = 2^k$.*

Assuming this set is nonempty, for any integer r,

$$\lim_{H\to\infty} \frac{\#\{d \in \mathscr{D}_k(H) \,:\, \dim \text{Sel}_\phi E^d - \delta_0 = r\}}{\#\mathscr{D}_k(H)}$$
$$= \lim_{N\to\infty} (\textit{Prob. a random } N \times (N+k) \textit{ matrix over } \mathbb{F}_2 \textit{ has kernel of rank } r)\,.$$

Here, $\delta_0 = 0, 1$ is a correction term to account for an image of $H^0(\mathbb{Q}, E_0[2])$.

This is recognizable as a Cohen–Lenstra-like distribution. For Cohen–Lenstra heuristics, the disparity between the number of rows and columns is usually a term of the form $r_1 + r_2 - 1$ or something similar, to account for archimedean places. This adjustment can also be determined using the Greenberg–Wiles formula.

We return to Kane's result. Given a 2-isogeny $\phi : E \to E_0$ from a curve with full rational 2 torsion to one without, we see that the Tamagawa ratio is usually of the form 2^k with k very negative. In this, a random $N \times (N+k)$ matrix almost always has rank exactly $N+k$, and kernel of dimension 0. So $\text{Sel}_\phi E^d$ is almost always trivial in this case, for each of the three isogenies. From the point of view of the statistics, the isogenies may as well not even be there.

Example 2.7. The curve

$$E : y^2 = x(x-1)(x+1)$$

has full rational 2-torsion and satisfies Kane's condition, whereas

$$E' : y^2 = x(x-1)(x-4)$$

has full rational 2-torsion but doesn't. This latter curve has a 2-isogeny whose Tamagawa ratios are usually ≈ 1.

This affects the Selmer groups. We have

$$\text{Average size of } \mathrm{Sel}_2 E^d = 12,$$

in line with the Poonen–Rains heuristics; but

$$\text{Average size of } \mathrm{Sel}_2 (E')^d > 12.$$