18.787: Selmer Groups and Euler Systems

Nir Elber

Fall 2025

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
2-Selmer Groups

1.1 September 4

Here are some administrative notes.

- There are no exams. Half of the grade will be based on problem sets (there will be two or three), all posted before November. The other half will be based on note-taking; currently, one must take notes for at least one lecture.
- There is a Canvas, which contains information about the course.
- There will be office hours from 11AM to 12PM on Tuesday and Thursday in 2-476. There should also be availability by appointment if desired.

There is no class next week, so the next class is September 16th.

1.1.1 Algebraic Rank

We will overview the course today. This course will be interested in Selmer groups and Euler systems. The relationship between these two notions is that Euler systems are a popular way to bound the size of Selmer groups.

To explain these notions, fix an elliptic curve E over a field k. (For us, an elliptic curve is a smooth, proper, connected curve of genus 1 with a distinguished point $\mathcal{O} \in E(k)$.) We will frequently take k to be a global, local, or finite field.

Remark 1.1. If the characteristic of k is not 2 or 3, then E admits an affine model

$$E\colon Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$. The distinguished point is $[0:1:0]$.

We also recall that E is identified with its Jacobian by the isomorphism $E \to \operatorname{Jac} E$ defined by $x \mapsto (x) - (\mathcal{O})$, which gives E a group law.

This group law can be seen to be commutative, so $E(k)$ is an abelian group.

Theorem 1.2 (Mordell–Weil)**.** For any elliptic curve E over a number field k, the abelian group $E(k)$ is finitely generated.

Thus, $E(k)$ can be understood by its torsion subgroup $E(k)_{\text{tors}}$ and its rank $\operatorname{rank} E(k)$. This rank is important enough to be given a name.

Definition 1.3 (algebraic rank)**.** For any elliptic curve E over a number field k. Then the *algebraic rank* $r_{\mathrm{alg}}(E)$ equals $\operatorname{rank} E(k)$.

There is another notion of rank. For this, we recall the definition of the L-function.

Definition 1.4. Fix an elliptic curve E defined over a number field k. Then its *L-function* is defined as

$$L(E,s) \doteq \prod_p \frac{1}{1-a_p p^{-s}+p^{1-2s}},$$

where $a_p \coloneqq (p+1)-\#E(\mathbb{F}_p)$ and $\doteq$ means that this is an equality up to some finite number of factors.

Remark 1.5. If E is defined over $\mathbb{Q}$, it is known that $L(E,s)=L(f,s)$ for some modular Hecke eigenform f with weight 2. Thus, $L(E,s)$ admits a holomorphic continuation to $\mathbb{C}$, and there is a functional equation relating $L(E,s)$ and $L(E,2-s)$.

Once we know $L(E,s)$ admits a continuation, we can make sense of the Birch and Swinnerton-Dyer conjecture.

Definition 1.6 (analytic rank)**.** The *analytic rank* $r_{\mathrm{an}}(E)$ of an elliptic curve E defined over $\mathbb{Q}$ is defined as the order of vanishing of $L(E,s)$ at $s=1$.

Conjecture 1.7 (Birch–Swinnerton-Dyer)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. Then

$$r_{\mathrm{an}}(E)=\operatorname{rank} E(\mathbb{Q}).$$

While this is still a conjecture, there is a lot of evidence nowadays.

Theorem 1.8 (Gross–Zagier–Kolyvagin)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. If $r_{\mathrm{an}}(E)\le 1$, then $r_{\mathrm{an}}=\operatorname{rank} E(\mathbb{Q})$.

1.1.2 The Tate–Shafarevich Group

In fact, Gross–Zagier–Kolyvagin know more: one can prove "finiteness of Ш."

Definition 1.9 (Tate–Shafarevich group)**.** Fix an elliptic curve E defined over a global field k. Then we define the *Tate–Shafarevich group* $Ш(E/k)$ as the kernel

$$Ш(E/k) \coloneqq \ker\left(\mathrm{H}^1(k,E)\to\prod_v \mathrm{H}^1(k_v,E)\right),$$

where the right-hand product is taken over the places v of k.

Remark 1.10. Roughly speaking, $\mathrm{H}^1(k,E)$ classifies torsors of E, which amount to curves C with Jacobian isomorphic to E. Being in the kernel means that C is isomorphic to E over each local field k_v, which amounts to $C(k_v)$ being nonempty. Thus, we see that $Ш(E/k)$ being nontrivial amounts to the existence of certain genus-1 curves admitting points locally but not globally.

It may seem strange to have points locally but not globally, but such things do happen.

Example 1.11. The projective cubic curve $C\colon 3X^3+4Y^3+5Z^3=0$ has points over every local completion over $\mathbb{Q}$, but C turns out to not admit rational points. Note that it is not so easy to actually prove that C does not admit rational points. Also, this example is not so pathological: C is a torsor for the elliptic curve $E\colon X^3+Y^3+60Z^3=0$, so it provides a nontrivial element of $Ш(E/\mathbb{Q})$.

Remark 1.12. It turns out that $[C]$ has order 3. Professor Zhang explained that this can be seen because C has an effective divisor of degree 3.

However, these bizarre things should not happen so frequently.

Conjecture 1.13. Fix an elliptic curve E over a global field k. Then $Ш(E/k)$ is finite.

Remark 1.14. When trying to prove this conjecture, one frequently just wants to know $Ш(E/k)[p^\infty]$ is finite for all primes p. (Of course, one also wants to know that $Ш(E/k)$ vanishes for primes p large enough.) It is often possible to verify that $Ш(E/k)[p^\infty]$ is finite for a given prime p, but it is difficult to actually show that $Ш(E/k)$ is then finite! One does not even know if the dimensions $\dim_{\mathbb{F}_p} Ш(E/k)[p]$ are bounded.

Let's now add to our previous theorem.

Theorem 1.15 (Gross–Zagier–Kolyvagin)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. If $r_{\mathrm{an}}(E)\le 1$, then $r_{\mathrm{an}}=\operatorname{rank}E(\mathbb{Q})$ and $\#Ш(E/\mathbb{Q})<\infty$.

This theorem is more or less the only way one can know that $Ш(E/k)$ is finite. In particular, we do not have a single example of an elliptic curve E with analytic rank at least 2 and $Ш(E/k)$ known to be finite.[1]

Remark 1.16. Professor Zhang does not know the answer to the following question: for each prime p, does there exist an elliptic curve E with $Ш(E/\mathbb{Q})[p]\neq 0$?

1.1.3 Selmer Groups

Even though r_{alg} and $Ш$ appear to be difficult invariants, one can combine them into the Selmer group, and then they seem to be controlled.

For the moment, it is enough to know that these Selmer groups $\mathrm{Sel}_m(E)$ are indexed by integers $m\in\mathbb{Z}$ and sit in a short exact sequence

$$0\to E(k)/mE(k)\to \mathrm{Sel}_m(E/k)\to Ш(E)[m]\to 0.$$

For example, it follows that

$$\dim_{\mathbb{F}_p}\mathrm{Sel}_p(E/k)=r_{\mathrm{alg}}(E)+\dim_{\mathbb{F}_p}\#Ш(E)[p]+\dim_{\mathbb{F}_p}E[p].$$

This last term is easy to compute, so we may ignore it; for example, it is known to vanish when $k=\mathbb{Q}$ and p is large. Anyway, the point is that the Selmer group has managed to combine information about the algebraic rank and $Ш$.

But now we have a miracle: Selmer groups are rather computable. In particular, $\mathrm{Sel}_2(E)$ is pretty well-understood, using quadratic twists. Working concretely, an elliptic curve $E\colon Y^2=f(X,Z)$ admits a quadratic twist $E^{(d)}\colon dY^2=f(X,Z)$; this is called a quadratic twist because E and $E^{(d)}$ become isomorphic after base-changing from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{d})$. It now turns out that

$$\mathrm{Sel}_m(E)\subseteq \mathrm{H}^1(\mathbb{Q},E[m]),$$

[1] Gross–Zagier have also proven that there exist elliptic curves with analytic rank larger than 1.

cut out by some local conditions; the point is that this right-hand group can frequently be computed by hand. For example, if $m = 2$, then $E[2]$ is found as from the roots of $f(X, 1)$. Notably, $E[2]$ won't change when taking quadratic twists, but the Selmer group may get smaller.

Here is the sort of thing we are recently (!) able to prove, using 2-Selmer groups.

Theorem 1.17 (Zywina)**.** Let K/F be a quadratic extension of number fields. Then there is an elliptic curve E over F such that

$$r_{\mathrm{alg}}(E/K) = r_{\mathrm{alg}}(E/F) = 1.$$

Remark 1.18. Zywina's argument follows an idea of Koymans–Pagano. The idea is to compute the 2-Selmer groups by hand to upper-bound the rank, and then one can do some tricks to lower-bound the rank.

If we have time, we may also get to the following result about distribution of ranks.

Theorem 1.19 (Smith)**.** Fix an elliptic curve E over $\mathbb{Q}$. As d varies, $\mathrm{Sel}_{2^\infty}\left(E^{(d)}/\mathbb{Q}\right)$ has rank 0 half of the time and 1 half of the time.

Let's see what we can say for higher dimensions, so throughout X is smooth proper variety over $\mathbb{Q}$. It turns out that a Selmer group can be defined for any Galois representation, so the following conjecture makes sense.

Conjecture 1.20 (Bloch–Kato)**.** Let X be a smooth proper variety over $\mathbb{Q}$. Then for any integer i, we have

$$\mathrm{Sel}_{p^\infty}\left(\mathrm{H}^{2i-1}_{\text{ét}}(X_{\overline{\mathbb{Q}}}; \mathbb{Q}_\ell)(i)\right) = \mathrm{ord}_{s=0}\, L\left(\mathrm{H}^{2i-1}_{\text{ét}}(X_{\overline{\mathbb{Q}}}; \mathbb{Q}_\ell)(i), s\right).$$

There is some evidence for this conjecture in higher dimensions, but they largely arise from Shimura varieties. Most of what is known is for when the order of vanishing is zero.

Let's end class by actually defining a Selmer group.

Definition 1.21 (group cohomology)**.** Fix a group G. The *group cohomology groups* $\mathrm{H}^\bullet(G; -)$ are the right-derived functors for the invariants functor $(\cdot)^G \colon \mathrm{Mod}_{\mathbb{Z}[G]} \to \mathrm{Ab}$. When G is profinite, we define the group cohomology as the limit. When G is an absolute Galois group of a field k, we may write $\mathrm{H}^\bullet(k; -)$ for the group cohomology.

To define the Selmer groups, we recall the short exact sequence

$$0 \to E[m] \to E \xrightarrow{m} E \to 0$$

of group schemes (and also over $\overline{k}$-points). Taking Galois cohomology produces a long exact sequence

$$E(k) \xrightarrow{m} E(k) \to \mathrm{H}^1(k; E[m]) \to \mathrm{H}^1(k; E) \xrightarrow{m} \mathrm{H}^1(k; E),$$

so there is a short exact sequence

$$0 \to E(k)/mE(k) \to \mathrm{H}^1(k; E[m]) \to \mathrm{H}^1(k; E)[m] \to 0.$$

If k is global, there is also a short exact sequence at each completion for each finite place v.

Definition 1.22 (Selmer group)**.** We define the m-Selmer group is defined as the fiber product in the following diagram.

$$\begin{array}{ccc} \mathrm{Sel}_m(E/k) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}; E[m]) \\ \downarrow & \lrcorner & \downarrow \\ \prod_v E(\mathbb{Q}_v)/mE(\mathbb{Q}_v) & \longrightarrow & \prod_v \mathrm{H}^1(\mathbb{Q}_v; E[m]) \end{array}$$

BIBLIOGRAPHY

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

List of Definitions