1 Weak Mordell-Weil, Selmer groups and 2-descent

In these notes, for an elliptic curve $E$ we define the $n$-Selmer groups and $n$-torsion Tate-Shafarevich groups, prove finiteness of $\text{Sel}_n(E)$ and thus give a proof of Weak Mordell-Weil. We also give an exposition of complete 2–descent starting from a cohomological viewpoint, allowing us to use 2–descent to calculate Selmer groups. Much of this maybe put under the title of Kummer theory of elliptic curves.

1.1 Selmer Groups and III.

Let $E/K$ be an elliptic curve over a number field $K$. We have an effective method of calculating the torsion subgroup of $E$ and so if we could calculate the order (should it be finite) of $E(K)/nE(K)$ we would recover the rank of $E$. For example if $E[2] \subseteq E(K)$ then $\text{rk} E(K) = \log_2 |E(K)/2E(K)| - 2$. If $K$ were instead a local field we would know this quotient is finite as $E(K)$ contains a finite index subgroup isomorphic to $\mathcal{O}_K$ under addition. Consider the “Kummer sequence” (of $E/K$)

$$0 \to E[n] \to E \to 0.$$  \hspace{1cm}  (1)

After taking the elements defined over $K$, the group $E(K)/nE(K)$ appears as a cokernel:

$$0 \to E(K)[n] \to E(K) \xrightarrow{[n]} E(K) \xrightarrow{\kappa} H^1(K, E[n]) \to H^1(K, E)$$

Where we have extended the sequence into cohomology. We can be reasonably explicit about $\kappa$. It is the map which takes $P \mapsto (\sigma \mapsto \sigma(\frac{1}{n}P) - \frac{1}{n}P)$ where $\frac{1}{n}P$ is any element of $E(K)$ s.t. $n\frac{1}{n}P = P$ (this is well defined and the resulting coycle is independent of the choice of $\frac{1}{n}P$). We call $\kappa$ the Kummer map.

We thus have an inclusion $E(K)/nE(K) \hookrightarrow H^1(K, E[n])$. $H^1(K, E[n])$ is a much more uniform object than $E(K)/nE(K)$ (cf. complete 2-descent below). Unfortuanetely this isn’t immediately helpful in showing that $E(K)/nE(K)$ is finite as $H^1(K, E[n])$ is very not finite. Within $H^1(K, E[n])$, $E(K)/nE(K)$ just gets lost. On the other hand $H^1(K, E[n])$ is a very uniform object (see p4). With this in mind we define a different object that depends only on local (easy) information but is still (hopefully) finite.

For all finite places $v$ fix an embedding $G_{K_v} \hookrightarrow G_K$, then restriction of cocyles gives maps $H^1(K, E) \to H^1(K_v, E)$. We get a diagram

$$
\begin{array}{cccccc}
0 & \to & E(K)/nE(K) & \xrightarrow{\kappa} & H^1(K, E[n]) & \to & H^1(K, E) \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \prod_v E(K_v)/nE(K_v) & \xrightarrow{\prod \kappa_v} & \prod_v H^1(K_v, E[n]) & \to & \prod_v H^1(K_v, E) \\
\end{array}
$$

Let $\text{Sel}_n(E) \subseteq H^1(K, E[n])$ denote the subgroup of elements which at all primes $p$ lie in the image of the local Kummer map $\kappa_v$. In other words,

$$\text{Sel}_n(E) := \ker \left( H^1(K, E[n]) \to \prod_v H^1(K_v, E[n])/\kappa_v(E(K_v)/nE(K_v)) \right).$$
We also define the Tate-Shafarevich group to be
\[
\Sha(E/K) = \ker \left( H^1(K, E) \to \prod_v H^1(K_v, E) \right)
\]

Note that \( \Sha_n(E) \) depends on \( n \) whilst \( \Sha(E/K) \) doesn’t. Multiplication by \( n \) on \( E \) translates to multiplication by \( n \) on cohomology so the sequence (1) can be truncated as \( H^1(K, E[n]) \to H^1(K, E)[n] \). Thus there is an exact sequence,
\[
0 \to E(K)/nE(K) \to \Sha_n(E) \to \Sha(E/K)[n] \to 0.
\]

**Theorem 1.1** For all elliptic curves \( E/K \), \( K \) a number field and \( n \in \mathbb{N} \), \( \Sha_n(E/K) \) is finite.

**Proof.** Let \( \Delta \) be the discriminant of \( E \). **Fact:** For any \( p \nmid \Delta \) and \( P \in E(K_p) \), the extension \( L := K_p(\frac{1}{n}P, E[n])/K_p \) is unramified.

**Input:** This comes from the study of the arithmetic of elliptic curves over local fields via formal gpgs etc.

We now translate this into cohomological language. This is the statement that the inertia subgroup \( \text{In}_p \) of an extension unramified at \( p \) is contained in \( G_L \). Thus any element of \( I_p \) fixes \( \frac{1}{n}P \) and so \( \kappa(P) \) sends \( \sigma \mapsto 0 \). Therefore, under inflation-restriction, for any \( p \nmid \Delta \):
\[
\text{res}_p(\Sha_n(E)) \subseteq H^1(K_{\text{unr}}/K_p, E[n]).
\]

Therefore
\[
\Sha_n(E) \subseteq A := \{ t \in H^1(K, E[n]) \mid \text{res}_p(t) \in H^1(K_{\text{unr}}/K_p, E[n]) \forall p \nmid \Delta \} \subseteq H^1(K, E[n]).
\]

For any \( t \in H^1(K, E[n]) \), \( t_v \in \text{inf}(H^1(K_{\text{unr}}/K_p, E[n])) \iff t \) lies in the image under inflation of an extension unramified at \( p \) this is made easy using that as \( E[n] \) is finite any cocycle factors through some finite extension. So \( t \in A \iff t \in \text{inf}(H^1(K_{\Sigma}/K, E[n])) \) where the maximal extension of \( K \) unramified outside \( \Sigma := \{ p \mid p \nmid \Delta \} \cup \{ v \mid \infty \} \).

Now WTS \( H^1(K_{\Sigma}/K, E[n]) \) is finite. Inflation-restriction gives,
\[
0 \to H^1(K(E[n])/K, E[n]) \to H^1(K_{\Sigma}/K, E[n]) \to H^1(K_{\Sigma}/K(E[n]), E[n])
\]

But the first term is finite as \( \text{Gal}(K(E[n])/K), E[n] \) are. So WLOG \( E(K) \supseteq E[n] \). Now \( H^1(K_{\Sigma}/K, E[n]) = \text{Hom}(\text{Gal}(K_{\Sigma}/K), E[n]) \). Now using

**Fact:** \( K_{\Sigma}/K \) has only finitely many galois \( \mathbb{Z}/n\mathbb{Z} \) subextensions.

**Input:** Knowledge of number fields, Dirichlet’s Unit Theorem, finiteness of the class group. Alternatively use Hermite-Minkowski.

as such a homomorphism factors through a galois extension with group isomorphism to a subgroup of \( \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \) we are done. \( \square \)

It is important to understand that other than formal messing there are two major inputs to this theorem. One, from the the properties of elliptic curves over local fields and number fields we get that almost always the local Selmer structure is the unramified structure. Two, from algebraic number theory, Dirichlet’s Unit Theorem finitude of the Class number, we get there are only finitely many extensions unramified outside a finite set of primes.

**Corollary 1.2** (Weak Mordell–Weil) \( E(K)/nE(K) \) is finite.
1.2 Complete 2-descent

How can we actually compute \(E(K)/nE(K)\) or \(\text{Sel}_n(E)\), where \(E\) is an elliptic curve over a field \(K\) of characteristic zero such that \(E[n] \subseteq E(K)\). So assume that \(E\) has form \(y^2 = (x - e_1)(x - e_2)(x - e_3)\). Now, \(H^1(K, E[2]) = \text{Hom}(K, E[2])\) as \(G_K\) acts trivially on \(E[2]\). Enumerate the 2-torsion elements by \(T_i = (e_i, 0)\). We can define a map \(\text{Hom}(K, E[2]) \rightarrow \text{Hom}(K, \mathbb{Z}/2\mathbb{Z}) \times \text{Hom}(K, \mathbb{Z}/2\mathbb{Z}) \times \text{Hom}(K, \mathbb{Z}/2\mathbb{Z})\) by post composition with the quotient \(E[2] \rightarrow E[2]/T_i\). Now, each of these is isomorphic to \(K \times /((K \times)^2\) via a choice of element \(\alpha\) where \(K(\alpha)\) is the kernel of the homomorphism. Let \(\eta\) denote the resulting homomorphism

\[
\eta: H^1(K, E[2]) \rightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.
\]

Then, on projection to any two summands one can check that this becomes an isomorphism. This is basically the observation that as \(E[2] \subseteq E(K), E[2] \cong \mu_2 \times \mu_2\) and so by Kummer theory we get \(H^1(K, E[2]) \cong H^1(K, E[2]^2) \cong (K^\times/(K^\times)^2)^2\).

As constructed \(\eta\) is natural in \(K\), in particular if \(K\) is a number field and \(v\) a place of \(K\) then the following diagram commutes:

\[
\begin{array}{ccc}
\text{Hom}(K, E[2]) & \xrightarrow{\eta} & K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \\
\downarrow & & \downarrow \\
\text{Hom}(K_v, E[2]) & \xrightarrow{\eta_v} & K_v^\times/(K_v^\times)^2 \times K_v^\times/(K_v^\times)^2 \times K_v^\times/(K_v^\times)^2
\end{array}
\]

**Question:** What does \(H^1(K\Sigma^2, E), \text{Sel}_2(E)\) and \(E(K)/2E(K)\) look like under this homomorphism?

Let \(K(\Sigma, 2)\) denote the subgroup of \(K^\times/(K^\times)^2\) of elements which are supported by primes of \(\Sigma\), i.e. have even valuation at all primes not in \(\Sigma\).

**Claim** Let \(K\) be a number field and \(\Sigma\) the places dividing \(n\Delta\) and infinite places. Then, \(\eta(H^1(K\Sigma^2, E[2]))\) is precisely the elements of \(K(\Sigma, 2)^3\) whose product is a square.

**Proof.** WTS image lies in \(K(\Sigma, 2)^3\). By definition the three quadratic extensions \(K(\sqrt{\alpha_i})\) picked out by an element of \(H^1(K^{\Sigma^2}/K, E[2])\) are unramified at \(p \nmid 2\Delta\). This is equivalent to their completions being unramified over \(K_p\) which will be true if and only if we don’t halve the valuation i.e. if \(v_p(\alpha_i)\) is even. Conversely given any unramified biquadratic we can construct such a homomorphism.

Note this proves that \(K(\Sigma, 2)\) is finite.

**Claim** For any field \(K\), given a representative point \(P = (x_0, y_0) \in E(K)/nE(K)\) with \(P \notin E[2]\) then \(\eta_K(P) = (x_0 - e_1, x_0 - e_2, x_0 - e_3)\).

**Sketch Proof** First check that \(K(1/2P) = K(\sqrt{x_0 - e_1}, \sqrt{x_0 - e_2}, \sqrt{x_0 - e_3})\). Then check that if \(\sigma_i\) is the element of \(\text{Gal}(K(1/2P)/K)\) fixing \(K(\sqrt{x_0 - e_1})\), then \(\sigma_i(1/2P) = -1/2P = (e_i, 0)\). Both of these are very concrete explicit calculations (but really are a pain).

If \(P = (e_1, 0) \in E[2]\) you can also convince yourself that \(P \mapsto ((e_1 - e_2)(e_1 - e_3), (e_1 - e_2), (e_1 - e_3))\) and similarly for the other points of order 2.

We can now be explicit about whether or tuple \((r_1, r_2, r_3)\) lies in the image of \(\kappa\eta\) (i.e. comes from an element of \(E(K)/2E(K)\)). For a tuple not in the image of \(E[2]\) (this is an easy check),
(r_1, r_2, r_2) \in \text{im } \kappa \eta \iff \text{there are any solutions } (x_0, y_0, z_1, z_2, z_3) \text{ over } K^\times \text{ to the equations (translating being equivalent in } K^\times/(K^\times)^2 \text{ into equations)}

\begin{align*}
y_0^2 &= (x_0 - e_1)(x_0 - e_2)(x_0 - e_3), \quad r_1 z_1^2 = x_0 - e_1, \quad r_2 z_2^2 = x_0 - e_2, \quad r e z_3^2 = x_0 - e_3.
\end{align*}

These simplify to whether or not there exist solutions to

\begin{align*}
r_1 z_1^2 - r_2 z_2^2 &= e_2 - e_1, \quad r_1 z_1^2 - r_2 z_2^2 = e_3 - e_1. \quad (\dagger).
\end{align*}

Now let K be a number field again. Because this description is independent of the field K and we said that the map \( \eta \) was natural under restriction we are able to similarly say that,

\( (r_1, r_2, r_3) \notin \eta \kappa(E[2]) \in \eta \text{Sel}_2(E) \iff (\dagger) \text{ is soluble at all places } v. \)

We record this information in the following diagram:

\[
\begin{array}{ccc}
H^1(K, E[2]) & \sim \leftarrow & \{(a, b, c) \in (K^\times/(K^\times)^2)^3 \mid abc \in (K^\times)^2\} \cup \eta \kappa(E[2]) \\
\cup & \quad & \cup \\
H^1(K^\Sigma/K, E[2]) & \sim \leftarrow & \{(a, b, c) \in K(\Sigma, 2)^3 \mid abc \in (K^\times)^2\} \cup \eta \kappa(E[2]) \\
\cup & \quad & \cup \\
\text{Sel}_2(E) & \sim \leftarrow & \{(a, b, c) \in K(\Sigma, 2)^3 \mid (\dagger) \text{ is everywhere locally soluble}\} \cup \eta \kappa(E[2]) \\
\cup & \quad & \cup \\
E(K)/2E(K) & \sim \leftarrow & \{(a, b, c) \in K(\Sigma, 2)^3 \mid (\dagger) \text{ is soluble over } K\} \cup \eta \kappa(E[2])
\end{array}
\]

So we have converted the problem of calculating the rank into checking if there are any points on a finite list of varieties as opposed to counting the number of such points on a single variety.

**Claim** Given a tuple \((r_1, r_2, r_3) \notin \text{im } \eta \kappa(E[2]), \) at a prime p not in \( \Sigma, \) \( \eta \text{p resp } \text{Sel}_2(E/K) = \eta \text{p resp } H^1(K^\Sigma/K, E[2]). \)

This requires ever so slightly more effort than the proof of Theorem 1.1. Keyphrase to google: at primes not dividing \( n \Delta \) the local Selmer structure is the unramified structure.

This claim has the important consequence that the variety \((\dagger)\) corresponding to \((r_1, r_2, r_3)\) will be automatically soluble at all \( p \notin \Sigma. \) Thus in checking everywhere local solubility we need only check at the finitely many places of \( \Sigma. \) At the infinite places that is easy and checking if a variety has points over a non-archimedean local field is a finite computation via Hensel’s Lemma. Thus

**Theorem 1.3** For \( E/K \) an elliptic curve over a number field with \( E(K) \supseteq E[2], \) \( \text{Sel}_2(E/K) \) is effectively computable.

We can in fact descend by cyclic isogeny for any prime \( p. \) Thus if III is finite then we can find a prime such that III[p] = 0 adjacent elements of \( E[p] \) perform descent where rk \( \text{Sel}_p = \text{rk } E \) and galois descend back to find the rank of \( E. \) Thus if III is known to be finite we have an algorithm for calculating the rank of \( E. \) This has worked in practice for all elliptic curves.

### 1.3 Examples of 2-descent

**1.3.1 An example with \( \Delta \nmid 2 \times 5 \times 5, \) \( \text{rk } E = 1. \)

Let \( E: y^2 = (x + 15)(x - 5)(x - 10) \) be an elliptic curve over \( \mathbb{Q}. \)
• By checking that differences of roots we observe that $\Delta$ is supported at 2, 5 (note the equation is minimal apart from maybe at 2). Therefore, $K(\Sigma, 2) = (-1, 2, 5)$ has order $2^3$ and the subset of $K(\Sigma, 2)^3$ of elements whose product is a square has order $2^6$.

• The image of $E[2]$ is spanned by the images of $(5, 0), (10, 0)$ which are $(5, -1, -5), (1, 5, 5)$ respectively. There is also an “obvious” point $(1, 24)$ whose image is $(1, -1, -1)$ so must be of infinite order. So we have found a $2^3$ dimensional subspace of $K(\Sigma, 2)^3$ contained in the image of $E(K)/2E(K), \text{Sel}_2(E)$. Call this $A$.

• We claim that this is precisely the image of $\text{Sel}_2(E)$. To prove this we need to show that any other elements correspond (as in Section 1.2) to varieties which are not everywhere locally soluble. Consider a tuple $(a, b, ab)$. In general the signs of these elements could be,

$$(+, +, +) \quad (+, -, -) \quad (-, +, -) \quad (-, -, +)$$

all occurring equally often. The corresponding variety (assuming we’re not in the image of $E[2]$) is given by

$$az^2_1 - bz^2_2 = 5$$
$$az^2_1 - abz^2_3 = 1$$

where have removed any squares of coefficients as we may whilst preserving solubility. Now if $a > 0$, (2) only has solutions over $\mathbb{R}$ when $b > 0$, and when similarly $ab > 0$ using (3) (note $E[2]$ does not land pts with $a < 0$. This discounts half of all possible elements of the image so $\text{rk}_2 \text{Sel}_2(E) \leq 5$.

• Denote the remaining elements by $B$. To prove that $\text{rk}_2 \text{Sel}_2(E) = 3$ we must prove that a choice of three coset reps of $B/A$.

• $(2, 1, 2)$: We ask if there are any solutions in $(\mathbb{Q}_5^\times)^3$ to $2z_1^2 - z_2^2 = 5, 2z_1^2 - 2z_3^2 = 1$. By moving denominators to the RHS this is equivalent to solving,

$$2z_1^2 - z_2^2 = 5w^2,$$
$$2z_1^2 - 2z_3^2 = v^2$$

in $(\mathbb{Z}_5 \setminus \{0\})^5$. Suppose that $(z_1, ..., v)$ is a solution. Then looking at the first equation modulo 5 we get that the only solutions to $2z_1^2 - z_2^2 \equiv 0 \pmod{5}$ are when $5 \mid z_1, z_2$. So let $z_1 = 5z_1', z_2 = 5z_2'$ with $z_i' \in \mathbb{Z}_5 \setminus \{0\}$. Then these satisfy

$$10z_1'^2 - 5z_2'^2 = w^2.$$

So $5 \mid w$ and similarly if $w = 5w'$ then

$$2z_1'^2 - z_2'^2 = 5w'^2.$$

But this is our original equation so we may iterate and $5 \mid z_1$ “infinently” \footnote{This is a contradiction and so $(2, 1, 2) \notin \text{im Sel}_2(E)$.}.

• $(1, 2, 2)$: An identical argument applied to the first equation suffices.
• (2, 2, 1): This time we claim that the corresponding equations
\[
2z_1^2 - 2z_2^2 = 5w^2, \\
2z_1^2 - z_3^2 = v^2
\]

have no non-zero solutions over \( \mathbb{Z}_2 \). Again suppose we have a solution. Then modulo 8 the squares are 0, 1, 4 and so the equation \( 2\bar{z}_1 - \bar{z}_2 \equiv \bar{v}^2 \pmod{8} \) only has solutions if \( 2 \mid z_1, z_3, w \) but then after replacing and cancelling we will get an identical equation and again \( 2 \mid z_1 \) infinitely. 

Therefore the |\( E(\mathbb{Q})/2E(\mathbb{Q}) \)| = |\( \text{Sel}_2(E) \)| = 8 and \( \text{rk}_2 E = 1 \).

### 1.3.2 An example with \( \text{III}(E/K)[2] \neq 0 \).

Let \( E : y^2 = (x - 22)(x + 10)(x + 12) \). Warning: this example is sketched and not pretty! For a pretty example of finding an elliptic curve with \( \text{III}(E)[2] \neq 0 \) see Tom Fisher’s Part III notes (last lecture). This does require non-complete descent though.

i) In this example \( \Delta \) is supported at 2, 17. Recall we can check this by checking which primes divide the differences of the roots.

ii) Therefore the image of \( \text{Sel}_2(E/\mathbb{Q}) \) lies in a subgroup of order \( 2^6 \).

iii) Again looking over \( \mathbb{R} \) cuts this to a \( 2^5 \) dimensional subspace.

iv) Now, we can similarly check that \( (2, 17, 34) \) (I hope this is right certainly it has a 17 factor in the middle) is not soluble over \( \mathbb{Q}_2 \) by looking mod 8. Thus \( 2 \geq \text{rk}_2 \text{Sel}_2(E/\mathbb{Q}) \leq 4 \).

v) The variety given by \( (2, 1, 2) \) is everywhere locally soluble. Recall we need only check this over \( \mathbb{R} \) (easy) and over \( \mathbb{Q}_2, \mathbb{Q}_{17} \). For these use a multivariable form of Hensel's lemma. This should be something along the lines of saying if you find points over sufficiently high reductions mod \( p \) that the Jacobian of \( f_1, f_2 \) (wrt \( z_1, z_2, z_3, w, v \)) has rank 2 then points lift.

vi) Therefore \( 3 \geq \text{rk}_2 \text{Sel}_2(E/\mathbb{Q}) \leq 4 \). But what about the rank? In particular does the everywhere locally soluble variety corresponding to \( (2, 1, 2) \) have a global point? To check this perform a 2-descent over \( K : = \mathbb{Q}(\sqrt{2}) \). Over \( K \) the descent goes as in the previous example and we can check that \( \text{rk} E(K) = 0 \) simply by proving tuples are not everywhere locally soluble. Therefore \( \text{rk} E(\mathbb{Q}) = 0 \) and in particular \( \text{III}(E/\mathbb{Q})[2] \neq 0 \). We have also produced a variety which is everywhere locally but not globally soluble.

vii) It remains to decide on the exact rank of \( \text{Sel}_2(E/\mathbb{Q}) \). For this we can repeat set v) for all other coset reps. Otherwise, if you want to take a shortcut, it is known that \( \text{FACT: Assuming that III is finite, |III[n]| is a square. So assuming finiteness, as we know it to be non trivial by vi) |III(E/K)[2]| = 4 \) and \( \text{rk}_2 \text{Sel}_2(E/\mathbb{Q}) = 4 \).

Exercise: Can you find a neat proof that \( (2, 1, 2) \) is not globally soluble? Maybe possible using Legendre Symbols.