2.1 Classical full 2-descent

Consider the elliptic curve

\[ E: y^2 = x(x - a)(x - b). \]

We consider the map

\[ \gamma: E(\mathbb{Q}) \to \mathbb{Q}^\times /\mathbb{Q}^\times \times \mathbb{Q}^\times /\mathbb{Q}^\times \]

\[ P \mapsto (x(P) - a, x(P) - b) \text{ if } x(P) \notin \{\infty, a, b\}, \]

\[ (a, 0) \mapsto (a(a - b), a - b), \]

\[ (b, 0) \mapsto (b - a, b(b - a)), \]

\[ \infty \mapsto 1 \]

It is straightforward to check that \( \delta \) is a group homomorphism and that \( \delta(P) = (1, 1) \) if and only if \( P \in 2E(\mathbb{Q}) \). This means that we have

\[ \gamma(E(\mathbb{Q})) \simeq E(\mathbb{Q})/2E(\mathbb{Q}). \]

One part of Mordell’s proof that the rational points on an elliptic curve form a finitely generated group is showing that its image is finite. This is not a hard result to obtain. Note that any potential image \((\delta_1, \delta_2) \in (\mathbb{Q}^\times /\mathbb{Q}^\times)^2\) can be represented with \(\delta_1, \delta_2\) squarefree integers. If \((x, y) \in E(\mathbb{Q})\) is a point with that image, we would have \(z_1, z_2, z_3 \in \mathbb{Q}\) such that

\[ x - a = \delta_1y_1^2, \]

\[ x - b = \delta_2y_2^2, \]

\[ x = \delta_1\delta_2y_3^2 \]

\[ y = \delta_1\delta_2y_1y_2y_3 \]

or, with \(x, y\) eliminated,

\[ C_{\delta_1, \delta_2}: \delta_1\delta_2y_3^2 = \delta_1y_1^2 + a = \delta_2y_2^2 + b. \]

It is straightforward to check that if any prime \(p\) not dividing \(2ab(a - b)\) divides one of the square-free integers \(\delta_1, \delta_2\) then this equation does not have solutions locally at \(p\). So indeed, immediately we see that only finitely many curves \(C_{\delta_1, \delta_2}\) have rational points and thus that the image of \(\gamma(E(\mathbb{Q}))\) is indeed finite.

In general it is difficult to compute the exact image. However, it is possible to determine a necessary condition for \(C_{\delta_1, \delta_2}\) to have points: One should have that \(C_{\delta_1, \delta_2}(\mathbb{Q}_p) \neq \emptyset\) for all \(p\), also for \(\mathbb{Q}_\infty = \mathbb{R}\). Therefore, we know that \(\delta(E(\mathbb{Q}))\) is contained in the finite, computable, Selmer group

\[ \text{Sel}^2(E/\mathbb{Q}) = \{ (\delta_1, \delta_2) \in (\mathbb{Q}^\times /\mathbb{Q}^\times)^2 : C_{\delta_1, \delta_2}(\mathbb{Q}_p) \text{ is nonempty for all primes } p \}. \]

The fundamental ingredient here is the cover

\[ \begin{array}{c}
C_{\delta_1, \delta_2} & \to & E \\
(y_1, y_2, y_3) & \mapsto & (x, y) = (\delta_1, \delta_2y_3^2, \delta_1, \delta_2y_1y_2y_3) 
\end{array} \]

As is straightforward to check, this is an unramified degree 4 cover with

\[ \text{Aut}(C_{\delta_1, \delta_2}/E) = \mathbb{Z}/2 \times \mathbb{Z}/2 \simeq E[2]. \]

2.2 General descent principle

Let \(k\) be a field with separable closure \(k_s\).
We restrict here to the case where \( \pi: D \to C \) is an unramified finite cover with \( \# \text{Aut}_{k_s}(D/C) = \deg(D/C) \), the important part being that the automorphism group acts simply transitively on the fibers.

2.3 Definition: Let \( D_1/C \) and \( D_2/C \) be covers over \( k \). We say that \( D_2/C \) is a twist of \( D_1/C \) if there is an isomorphism \( \phi: D_2 \to D_1 \) over \( k_s \) such that the composition \( D_2 \xrightarrow{\phi} D_1 \to C \) equals the cover \( D_2 \to C \). We say a twist is trivial if there is such an isomorphism over \( k \) already, in which case we say the covers are isomorphic over \( k \). We write \( \text{Twist}(D_1/C) \) for the set of isomorphism classes of twists of \( D_1/C \).

Let \( \sigma \in \text{Gal}(k_s/k) \). Note that \( \phi^\sigma \circ \phi^{-1} \in \text{Aut}_{k_s}(D_1/C) \) We see that a twist gives rise to a Galois 1-cocycle via

\[
\sigma \quad \mapsto \quad \phi^\sigma \circ \phi^{-1}
\]

In fact, it is straightforward to check that this 1-cocycle has trivial class in \( H^1(\text{Gal}(k_s/k), \text{Aut}(D_1/C)) \) if and only if \( D_1 \to C \) and \( D_2 \to C \) are already isomorphic over \( k \). Conversely, given a cohomology class, one can construct a twist that gives rise to that class:

2.4 Twisting principle:

\[ H^1(k, \text{Aut}(D/C)) \simeq \text{Twist}(D/C) \]

2.5 Lifting rational points: Let \( P \in C(k) \) be a rational point over which \( D \) is unramified. Let \( Q \in D(k_s) \) be a point over \( P \). Since \( \pi \) itself is defined over \( k \), we have

\[ \pi(Q) = \sigma(\pi(Q)) = \sigma P = P, \]

so we see that \( Q \) and \( \sigma Q \) lie in the same fibre of \( \pi \). We assumed that \( \text{Aut}(D/C) \) acts simply transitively on the fibers, so there is a unique \( \psi_{\sigma} \in \text{Aut}(D/C) \) such that \( \psi_{\sigma}(Q) = \sigma Q \). It is straightforward to check that \( \psi_{\sigma \tau} = (\psi_\tau)^\sigma \circ \psi_{\sigma} \), so for any such point \( Q \) we obtain a 1-cocycle. We can check that choosing a different point \( Q \) in the same fibre changes the cocycle by a coboundary, so the cohomology class only depends on the point \( P \). We obtain a map

\[ \gamma: C(k) \to H^1(k, \text{Aut}(D/C)). \]

Interpreting the codomain as \( \text{Twist}(D/C) \), we obtain a map that associates to \( P \in C(k) \) a twist \( D_P \to C \) of \( D \to C \) such that \( P \) has a rational preimage on \( D_P \).

2.6 The Chevalley-Weil Theorem: This states that if \( D \to C \) is an unramified finite cover defined over a number field \( k \) then there is a finite field extension \( L \) of \( k \) such that all rational points of \( C \) have a preimage in \( D(L) \). In the language above, this boils down to the observation that if \( k \) is a local field and if \( \pi: D \to C \) has good reduction, then the image \( \gamma(C(k)) \) lies in the kernel of the restriction map \( H^1(k, \text{Aut}(D/C)) \to H^1(k_u, \text{Aut}(D/C)) \), where \( k_u \subset k_s \) is the maximal unramified extension of \( k \). We call such classes unramified classes.

Let \( k \) now be a number field and let \( S \) be a finite set of places containing all the bad places for \( \pi: D \to C \). If \( v \) is a place of \( k \), then we have the restriction maps \( H^1(k, \text{Aut}(D/C)) \to H^1(k_v, \text{Aut}(D/C)) \) and \( H^1(k_v, \text{Aut}(D/C)) \to H^1(k_{v,u}, \text{Aut}(D/C)) \). Then, by the observation above, \( \gamma(C(k)) \) lies in

\[ H^1(k, \text{Aut}(D/C); S) := \ker \left( H^1(k, \text{Aut}(D/C)) \to \prod_{v \notin S} H^1(k_{v,u}, \text{Aut}(D/C)) \right) \]

In the full 2-descent example that we looked at, we have \( H^1(k, \text{Aut}(D/C)) \simeq (\mathbb{Q}^\times / \mathbb{Q}^\times)^2 \), so the classes unramified outside \( S \) consist of the classes represented by square-free \( S \)-integers. This gives us a finite subset. Indeed, in general \( H^1(k, \text{Aut}(D/C); S) \) is finite.
2.7 Principle of descent: Given an unramified cover $D \rightarrow C$, we can cover $C(k)$ by the rational points $D'(k)$ of a finite number of twists $D'/C$ of $D/C$.

Initially this does not seem to be much of an improvement. However, in special cases it may be that $D'(k)$ is easier to determine.

2.8 Example: We will determine the rational points on the genus 2 curve

$$C: 2y^2 = x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1).$$

The first thing to try, of course, is to determine the rational points on the curve $2y^2 = u^3 + 1$ and recognise for which points we have $u = x^2$. However, this curve has infinitely many rational points, so this approach does not help much. Instead, we proceed essentially as before and consider the curve

$$D_\delta: \begin{cases} x^2 + 1 = 2\delta y_1^2 \\ x^4 - x^2 + 1 = \delta y_2^2 \\ y = \delta y_1 y_1 \end{cases}$$

It is straightforward to see that $D_\delta \rightarrow C$ indeed is an unramified double cover. In fact, $D_\delta$ is a genus 3 curve. For $\delta \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ we see that $D_\delta$ represents different twists. Elementary considerations as before show that $D_\delta$ does not have rational points unless $\delta \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$, and considerations at $\mathbb{R}$ show that $\delta > 0$. Locally at 3 we can quickly rule out $\delta = 3, 6$ and local considerations at 2 give that $\delta = 1$.

Note, however, that $D_1$ covers the curve $y_2^2 = x^4 - x^2 + 1$. This is also a genus 1 curve. It is isomorphic to the elliptic curve given by the equation $v^2 = x^3 - x^2 - 4x + 4$, which has 8 rational points (with group structure $\mathbb{Z}/2 \times \mathbb{Z}/4$). We find the rational points

$$(x, y_2) = \{\infty_\pm, (0, \pm 1), (\pm 1, \pm 1)\}$$

We can see which of these points lift to rational points on $D_\delta$ or, computationally easier, see which of these $x$-coordinates give rise to rational points on $C$. Only the points with $x = \pm 1$ do.

We see that the appropriate map $\gamma$ in this case is

$$\gamma: \begin{array}{c} C(k) \rightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ (x, y) \mapsto (x^4 - x^2 + 1) \end{array}$$

(when defined)

2.9 Selmer sets:

Let $k$ be a global field and let $\pi: D \rightarrow C$ be an unramified cover with $\text{Aut}_{k_s}(D/C)$ acting transitively on the fibers. For any place $v$ of $k$ we have the restriction map $\rho_v : \text{Gal}(k_s/k) \rightarrow \text{Gal}(k_{v,s}/k_v)$. We get a commutative diagram

$$\begin{array}{c} C(k) \xrightarrow{\gamma} H^1(k, \text{Aut}(D \rightarrow C)) \\ \downarrow \text{id} \quad \downarrow \rho_v \\ C(k_v) \xrightarrow{\gamma_v} H^1(k, \text{Aut}(D \rightarrow C)) \end{array}$$

Hence, we can describe all twists $d$ that have points everywhere locally via

$$\text{Sel}(D \rightarrow C/k) = \{\delta \in H^1(k, \text{Aut}(D \rightarrow C)) : \rho_v(\delta) \in \gamma_v(C(k_v)) \text{ for all places } v\}$$

As we saw before, $\text{Sel}(D \rightarrow C/k)$ will only contain classes that are unramified outside the primes of bad reduction of $D \rightarrow C$ or primes dividing the degree of $D/C$.

There are two approaches to computing Selmer sets:

- Generate the candidate twists of $D$ and check them for local solvability everywhere
Find a computationally efficient representation of $H^1(k, \text{Aut}(D \to C))$ and of the map $\gamma$ (and their local versions) and find a way to compute $\gamma_v(C(k_v))$ and use the maps $\rho_v$.

The main observation here is that $\gamma_v$ is a locally constant map, so if you can split $C(k_v)$ up into finitely many sufficiently small neighbourhoods in which $\gamma_v$ is constant, you can find the image by evaluating $\gamma_v$ at representatives of each of those neighbourhoods.

2.10 Galois modules with easily computable cohomology:

Consider the Galois module $\mu_n$, i.e., the $n$-th roots of unity. The short exact sequence related to multiplication-by-$n$:

$$1 \to \mu_n(k_s) \to \mathbb{G}_m(k_s) \xrightarrow{n} \mathbb{G}_m(k_s) \to 1$$

yields

$$\cdots \to k^\times \xrightarrow{n} k^\times \to H^1(k, \mu_n) \to H^1(k, \mathbb{G}_m) \to \cdots$$

and from Hilbert ’90 we get that $H^1(k, \mathbb{G}_m)$ is trivial and hence that

$$H^1(k, \mu_n) \simeq k^\times / k^{\times n}$$

We can extend this result a bit. Let $f(x)$ be a separable polynomial over $k$ of degree $d$, let $\Delta = \{\theta_1, \ldots, \theta_d\}$ be the roots of $f(x)$ in $k_s$ and let $L = k[x]/(f(x))$, and write $\theta$ for the image of $x$ in $L$ (i.e., a root of $f(x)$ in $L$).

Given a Galois module $M$, we write $M^\Delta := M\theta_1 \oplus \cdots \oplus M\theta_d$, which is the $d$th direct power of $M$, but with $\text{Gal}(k_s/k)$ also acting by permutation on the $d$ components. You can check that $H^0(k, \mathbb{G}_m^\Delta) = L^\times$. This operation has nice functorial properties, so

$$H^1(k, \mu_n^\Delta) \simeq L^\times / L^{\times n}$$

2.11 2 descent on elliptic curves in general

Let

$$E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6.$$  

Let $L = k[\theta] = k[x]/f(x)$. Let $\Delta$ be the Galois-set of roots of $f(x)$ in $k_s$. We have

$$0 \to E[2] \to \mu_2^\Delta \to \mu_2 \to 1.$$  

We take $D \to C$ to be $[2] : E \to E$, so that $\text{Aut}_{k_s}(E \to E) = E[2](k_s)$ and we get the exact sequence

$$H^1(k, E[2]) \to L^\times / L^{\times 2} \xrightarrow{N_{L/k}} k^\times / k^{\times 2},$$

where the first arrow turns out to be injective. Indeed, the map

$$\gamma : E(k) \to L^\times / L^{\times 2} \quad (x, y) \mapsto x - \theta$$

turns out to be the appropriate map.

2.12 Fake 2-descent on genus 2 curves

Now consider we have a curve

$$C : y^2 = f(x) = f_6(x - \theta_1) \cdots (x - \theta_6),$$
We can construct a degree 16 unramified cover of $C$ in the following way. We write
\[
D_\delta : \begin{cases} 
\lambda y_1^2 = \delta_1(x - \theta_1) \\
\vdots \\
\lambda y_6^2 = \delta_6(x - \theta_6) \\
y = \lambda^3 y_1 \cdots y_6 \\
f_6 = \delta_1 \cdots \delta_6
\end{cases}
\]
where we should really think of $\delta_1, \ldots, \delta_6$ and $y_1, \ldots, y_6$ as conjugates, in which case $\text{Gal}(k_\delta/k)$ acts by permutation on them and we see that $D_\delta$ is in fact defined over $k$. So we should really think of $\delta$ as taking values in $L = k[\theta] = k[x]/f(x)$. In this case, the isomorphism class of $D_\delta$ really only depends on the value of $\delta \in L^x/L^{x^2}k^x$, where the extra $k^x$ comes from $\lambda$. Note, though, that the actual cover $D_\delta \to C$ does depend on the sign of $\lambda$.

Indeed, the associated map is
\[
\gamma : C(k) \to L^x/L^{x^2}k^x \\
(x, y) \mapsto x - \theta
\]
and we define
\[
\text{Sel}_2(C/k) = \{ \delta \in L^x/L^{x^2}k^x : \rho_v(\delta) \in \gamma_v(C(k_v)) \text{ for all places } v \}
\]
We can find that this set is empty even if $C$ has points everywhere locally. That means that for each $\delta$ there is a place $v$ such that $D_\delta(k_v)$ is empty. However, since these $v$ may vary per $\delta$ and since as soon as $D_\delta(k_v)$ is non-empty then $C(k_v)$ is non-empty as well, it can easily happen that $C$ does have points everywhere locally.

**2.13 Some numerical data:** If one tries this with $f(x)$ having coefficients randomly chosen from $\{-100, \ldots, 100\}$ then about 15% of the curves seem to have a local obstruction somewhere, about 65% has empty fake 2-Selmer set (this includes the previous 15%) and about 20% has a small rational point. That leaves about 15% of the curves that likely do not have rational points but still have non-empty 2-Selmer set.

**2.14 : Literature references**

An algorithm to compute fake 2-Selmer sets is described in

Nils Bruin, Michael Stoll, Two-cover descent on hyperelliptic Curves, Math. Comp. 78 (2009), 2347-2370. See also Electronic Resources. (or see ArXiv preprint arXiv:0803.2052, 2008)

A modern perspective on how to get setups suitable for doing this kind of descent computation in more complicated cases, see