BIRS 2012 – Nils Bruin: 2. Explicit Descent

June 12, 2012

2.1 Classical full 2-descent

Consider the elliptic curve

$$E\colon y^2 = x(x-a)(x-b).$$

We consider the map

$$\begin{array}{rccl} \gamma\colon & E(\mathbb{Q}) & \to & \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ & P & \mapsto & (x(P)-a, x(P)-b) \quad \text{if } x(P) \notin \{\infty, a, b\} \\ & (a,0) & \mapsto & (a(a-b), a-b) \\ & (b,0 & \mapsto & (b-a, b(b-a)) \\ & \infty & \mapsto & 1 \end{array}$$

It is straightforward to check that δ 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 $(\delta_1, \delta_2) \in (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$ can be represented with δ_1, δ_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

$$\begin{aligned} x - a &= \delta_1 y_1^2 \\ x - b &= \delta_2 y_2^2 \\ x &= \delta_1 \delta_2 y_3^2 \\ y &= \delta_1 \delta_2 y_1 y_2 y_3 \end{aligned}$$

or, with x, y eliminated,

$$C_{\delta_1,\delta_2}\colon \delta_1\delta_2 y_3^2 = \delta_1 y_1^2 + a = \delta_2 y_2^2 + b$$

It is straightforward to check that if any prime p not dividing $2ab(a-b)$ divides one of the squarefree integers δ_1, δ_2 then this equation does not have solutions locally at p. So indeed, immediately we see that only finitely many curves C_{δ_1,δ_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_{δ_1,δ_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*

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

The fundamental ingredient here is the cover

$$\begin{array}{ccc} C_{\delta_1,\delta_2} & \to & E \\ (y_1, y_2, y_3) & \mapsto & (x,y) = (\delta_1, \delta_2 y_3^2, \delta_1, \delta_2 y_1 y_2 y_3) \end{array}$$

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

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

2.2 : General descent principle

Let k be a field with separable closure k_s.

We restrict here to the case where $\pi\colon D \to C$ is an unramified finite cover with $\#\mathrm{Aut}_{k_s}(D/C) = \deg(D/C)$, 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 $\mathrm{Twist}(D_1/C)$ for the set of isomorphism classes of twists of D_1/C.

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

$$\begin{array}{ccc} \mathrm{Gal}(k_s/k) & \to & \mathrm{Aut}_{k_s}(D_1/C) \\ \sigma & \mapsto & \phi^\sigma \circ \phi^{-1} \end{array}$$

In fact, it is straightforward to check that this 1-cocycle has trivial class in $H^1(\mathrm{Gal}(k_s/k), \mathrm{Aut}(D_1/C))$ 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:

$$H^1(k, \mathrm{Aut}(D/C)) \simeq \mathrm{Twist}(D/C)$$

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 π itself is defined over k, we have

$$\pi({}^\sigma Q) = {}^\sigma(\pi(Q)) = {}^\sigma P = P,$$

so we see that Q and ${}^\sigma Q$ lie in the same fibre of π. We assumed that $\mathrm{Aut}(D/C)$ acts simply transitively on the fibers, so there is a unique $\psi_\sigma \in \mathrm{Aut}(D/C)$ 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

$$\gamma\colon C(k) \;\to\; H^1(k, \mathrm{Aut}(D/C)).$$

Interpreting the codomain as $\mathrm{Twist}(D/C)$, 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 $\pi\colon D \to C$ has good reduction, then the image $\gamma(C(k))$ lies in the kernel of the restriction map $H^1(k, \mathrm{Aut}(D/C)) \to H^1(k_u, \mathrm{Aut}(D/C))$, 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 $\pi\colon D \to C$. If v is a place of k, then we have the restriction maps $H^1(k, \mathrm{Aut}(D/C)) \to H^1(k_v, \mathrm{Aut}(D/C))$ and $H^1(k_v, \mathrm{Aut}(D/C)) \to H^1(k_{v,u}, \mathrm{Aut}(D/C))$. Then, by the observation above, $\gamma(C(k))$ lies in

$$H^1(k, \mathrm{Aut}(D/C); S) := \ker\left(H^1(k, \mathrm{Aut}(D/C)) \to \prod_{v \text{ not in } S} H^1(k_{v,u}, \mathrm{Aut}(D/C))\right)$$

In the full 2-descent example that we looked at, we have $H^1(k, \mathrm{Aut}(D/C)) \simeq (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$, 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 $H^1(k, \mathrm{Aut}(D/C); S)$ is finite.

2.7 Principle of descent: Given an unramified cover $D \to C$, 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

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

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

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

It is straightforward to see that $D_\delta \to C$ indeed is an unramified double cover. In fact, D_δ is a genus 3 curve. For $\delta \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ we see that D_δ represents different twists. Elementary considerations as before show that D_δ does not have rational points unless $\delta \in \{\pm1, \pm2, \pm3, \pm6\}$, 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

$$(x, y_2) = \{\infty^\pm, (0, \pm1), (\pm1, \pm1)\}$$

We can see which of these points lift to rational points on D_δ or, computationally easier, see which of these x-coordinates give rise to rational points on C. Only the points with $x = \pm1$ do.

We see that the appropriate map γ in this case is

$$\begin{array}{rccl} \gamma\colon & C(k) & \to & \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ & (x,y) & \mapsto & (x^4-x^2+1) \quad \text{(when defined)} \end{array}$$

2.9 Selmer sets:

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

$$\begin{tikzcd} C(k) \arrow[r, "\gamma"] \arrow[d] & H^1(k, \mathrm{Aut}(D \to C)) \arrow[d, "\rho_v"] \\ C(k_v) \arrow[r, "\gamma_v"] & H^1(k, \mathrm{Aut}(D \to C)) \end{tikzcd}$$

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

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

As we saw before, $\mathrm{Sel}(D \to C/k)$ will only contain classes that are unramified outside the primes of bad reduction of $D \to C$ 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 $H^1(k, \mathrm{Aut}(D \to C))$ and of the map γ (and their local versions) and find a way to compute $\gamma_v(C(k_v))$ and use the maps ρ_v.

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

2.10 Galois modules with easily computable cohomology:

Consider the Galois module μ_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 θ 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 dth direct power of M, but with $\mathrm{Gal}(k_s/k)$ 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

$$E \colon y^2 = f(x) = x^3 + a_2 x^2 + a_4 x + a_6.$$

Let $L = k[\theta] = k[x]/f(x)$. Let Δ 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 $\mathrm{Aut}_{k_s}(E \to E) = E[2](k_s)$ 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

$$\begin{array}{rccc} \gamma\colon & E(k) & \to & L^\times / L^{\times 2} \\ & (x, y) & \mapsto & x - \theta \end{array}$$

turns out to be the appropriate map.

2.12 Fake 2-descent on genus 2 curves

Now consider we have a curve

$$C \colon y^2 = f(x) = f_6 (x - \theta_1) \cdots (x - \theta_6),$$

We can construct a degree 16 unramified cover of C in the following way. We write

$$D_\delta\colon \begin{cases} \lambda y_1^2 = \delta_1(x-\theta_1) \\ \quad\vdots \\ \lambda y_6^2 = \delta_6(x-\theta_6) \\ y = \lambda^3 y_1\cdots y_6 \\ f_6 = \delta_1\cdots\delta_6 \end{cases}$$

where we should really think of $\delta_1,\ldots,\delta_6$ and $y_1,\ldots,y_6$ as *conjugates*, in which case $\mathrm{Gal}(k_s/k)$ acts by permutation on them and we see that D_δ is in fact defined over k. So we should really think of δ as taking values in $L=k[\theta]=k[x]/f(x)$. In this case, the isomorphism class of D_δ really only depends on the value of $\delta\in L^\times/L^{\times 2}k^\times$, where the extra $k^\times$ comes from λ. Note, though, that the actual cover $D_\delta\to C$ does depend on the sign of λ.

Indeed, the associated map is

$$\begin{array}{rccc} \gamma\colon & C(k) & \to & L^\times/L^{\times 2}k^\times \\ & (x,y) & \mapsto & x-\theta \end{array}$$

and we define

$$\mathrm{Sel}^2_{\mathrm{fake}}(C/k)=\{\delta\in L^\times/L^{\times 2}k^\times : \rho_v(\delta)\in\gamma_v(C(k_v)) \text{ for all places } v\}$$

We can find that this set is empty even if C has points everywhere locally. That means that for each δ there is a place v such that $D_\delta(k_v)$ is empty. However, since these v may vary per δ and since as soon as $D_\delta(k_v)$ is non-empty then $C(k_v)$ is nonempty 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

Nils Bruin, Bjorn Poonen, Michael Stoll, Generalized explicit descent and its application to curves of genus 3, ArXiv preprint arXiv:1205.4456, 2012.