Panoramas & Synthèses
36, 2012, p. 51–80

DESCENT ON ELLIPTIC CURVES

by

Michael Stoll

Abstract. — Let E be an elliptic curve over $\mathbb{Q}$ (or, more generally, a number field). Then on the one hand, we have the finitely generated abelian group $E(\mathbb{Q})$, on the other hand, there is the Shafarevich-Tate group $\text{Ш}(\mathbb{Q}, E)$. *Descent* is a general method of getting information on both of these objects – ideally complete information on the Mordell-Weil group $E(\mathbb{Q})$, and usually partial information on $\text{Ш}(\mathbb{Q}, E)$.

What descent does is to compute (for a given $n > 1$) the *n-Selmer group* $\text{Sel}^{(n)}(\mathbb{Q}, E)$; it sits in an exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \text{Sel}^{(n)}(\mathbb{Q}, E) \longrightarrow \text{Ш}(\mathbb{Q}, E)[n] \longrightarrow 0$$

and thus contains combined information on $E(\mathbb{Q})$ and $\text{Ш}(\mathbb{Q}, E)$.

The main problem I want to discuss in this "short course" is how to actually do this explicitly, with some emphasis on obtaining representations of the elements of the Selmer group as explicit covering spaces of E. These explicit representations are useful in two respects – they allow a search for rational points (if successful, this proves that the element is in the image of the left hand map above), and they provide the starting point for performing "higher" descents (*e.g.*, extending a p-descent computation to a p^2-descent computation).

Prerequisites. — Basic knowledge of elliptic curves (*e.g.*, Silverman's book [**10**]), some Galois cohomology and algebraic number theory (*e.g.*, Cassels-Fröhlich [**1**]).

2000 ***Mathematics Subject Classification.*** — 11G05, 14H52.
Key words and phrases. — Elliptic curves, descent, Selmer group.

***Résumé* (Descente sur les courbes elliptiques).** — Soit E une courbe elliptique sur $\mathbb{Q}$ (ou, plus généralement, sur un corps de nombres quelconque). On lui associe, d'une part, le groupe abélien de type fini $E(\mathbb{Q})$, et d'autre part, le groupe de Shafarevich-Tate $Ш(\mathbb{Q}, E)$.

La *descente* est une méthode générale pour obtenir des informations sur ces deux objets – idéalement des informations complètes sur le groupe de Mordell-Weil $E(\mathbb{Q})$, et typiquement des informations partielles sur $Ш(\mathbb{Q}, E)$.

Une descente calcule (pour un $n > 1$ donné) le *n-groupe de Selmer* $\mathrm{Sel}^{(n)}(\mathbb{Q}, E)$, qui se trouve dans une suite exacte

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(n)}(\mathbb{Q}, E) \longrightarrow Ш(\mathbb{Q}, E)[n] \longrightarrow 0$$

et qui contient donc des informations combinées sur $E(\mathbb{Q})$ et sur $Ш(\mathbb{Q}, E)$.

Le sujet principal que de ce mini-cours est de rendre explicite cette descente, et en particulier, de représenter les éléments du groupe de Selmer comme des courbes couvrant E. Ces représentations explicites sont utiles à deux égards : elles permettent de chercher des points rationnels (en cas de succès, l'élément est dans l'image de $E(\mathbb{Q})/nE(\mathbb{Q})$) ; et elles fournissent un point de départ pour effectuer des descentes d'ordre plus élevé (par exemple, une p^2-descente suivant une p-descente).

***Prérequis.* —** Notions sur la théorie des courbes elliptiques (par exemple, Silverman [**10**]), notions de théorie algébrique des nombres et cohomologie galoisienne (par exemple, Cassels-Fröhlich [**1**]).

This chapter contains the notes (with little changes) I wrote for the "short course" with the same title I gave at the Institut Henri Poincaré in the fall of 2004. The purpose of the course was to give an introduction to the topic and at the same time discuss some (then) recent results. Owing to the introductory nature of the text, we give proofs of most theorems, even though some can be found in the literature. Also, in some cases such a proof may be less elegant, but more elementary, than necessary.

The results described in these notes (if not "classical", *i.e.*, to be found in, *e.g.*, Silverman's book [**10**]) were obtained in collaboration with John Cremona, Tom Fisher, Cathy O'Neil, Ed Schaefer and Denis Simon. In some respect, the present text is by now fairly obsolete, since everything that is in it can be found in [**7, 3, 4, 2**]. However, we think that these notes may still be of some use, since they give a good overview over the ideas, without going too much into technical details. If you want to know more about these, you are welcome to consult the papers mentioned above.

I would like to particularly advertise Theorems 2.4 and 2.7. While it has been known for a long time that n-Selmer groups of elliptic curves can be computed in principle, these results give a rather precise statement on what is required if one really wants to perform such a computation. As it turns out, this is usually less demanding when n is a prime number, but even so, it is rarely feasible (with current technology regarding the computational theory of algebraic number fields) to perform the computation when $n \geq 5$.

1. The Selmer Group

In the following, K will be a number field, and E will be an elliptic curve defined over K. E is an algebraic group over K, and so its set of rational points, $E(K)$, forms a group, the so-called Mordell-Weil group. By the Mordell-Weil theorem, it is a finitely generated abelian group, and one of the big questions is how to determine it (in the sense of, say, giving generators as points in $E(K)$ and relations). Descent is the main tool used for that, both in theory and in practice. Doing an n-descent on E means to compute the n-Selmer group $\mathrm{Sel}^{(n)}(K,E)$, which we will introduce in this section.

Note that saying that $E(K)$ is a finitely generated abelian group amounts to asserting the existence of an exact sequence

$$0 \longrightarrow E(K)_{\mathrm{tors}} \longrightarrow E(K) \longrightarrow \mathbb{Z}^r \longrightarrow 0$$

with $r \geq 0$ an integer and $E(K)_{\mathrm{tors}}$ a finite abelian group; it consists of all elements of $E(K)$ of finite order. Less canonical, but sometimes more convenient, we also have

$$E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r .$$

For any concrete curve E, it is fairly straightforward to find $E(K)_{\mathrm{tors}}$, and we will not be concerned with how to do that in these lectures. The hard part is to determine the rank r. This is where descent helps.

1.1. Definition and first properties

We first set some (fairly standard) notation. If v is a place of K, we write K_v for the completion of K at v and K_v^{unr} for the maximal unramified extension of K_v. If v is a finite place, then k_v denotes the residue class field of K_v. If k is any field, $\bar{k}$ denotes an algebraic closure of k.

Let $n > 1$ be an integer. The usual definition of the n-Selmer group makes use of Galois cohomology. We follow the usual convention in writing $H^j(k,M)$ for the Galois cohomology group $H^j(\mathrm{Gal}(k),M)$, where k is a field, $\mathrm{Gal}(k)$ is the absolute Galois group of k, and M is a $\mathrm{Gal}(k)$-module (with continuous action; the group cohomology also is defined in terms of continuous cocycles).

Consider the short exact sequence of $G_K = \mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow E[n](\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{n} E(\bar{K}) \longrightarrow 0$$

(which is usually just written

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0\,).$$

Then we have the long exact sequence of cohomology groups

$$0 \longrightarrow E[n](K) \longrightarrow E(K) \xrightarrow{n} E(K) \xrightarrow{\delta} H^1(K,E[n]) \longrightarrow H^1(K,E) \xrightarrow{n} H^1(K,E)\,.$$

We deduce from it another short exact sequence:

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K,E[n]) \longrightarrow H^1(K,E)[n] \longrightarrow 0$$

It turns out that knowing $E(K)$ is essentially equivalent to knowing its free abelian rank $r = \operatorname{rank} E(K)$. (Once we know r, we can look for points until we have found r independent ones. Then we only need to find the K-rational torsion points and "saturate" the subgroup generated by the independent points. All of this can be done effectively.) Now the idea is to use the above exact sequence to at least get an upper bound on r: r can be read off from the size of the group $E(K)/nE(K)$ on the left, and so any bound on that group will provide us with a bound on r. From the exact sequence, we see that $E(K)/nE(K)$ sits inside $H^1(K, E[n])$; however, this group is infinite, and so it does not give a bound.

But we can use some additional information. We know (trivially) that any K-rational point on E is also a K_v-rational point, for all places v of K. Now it is possible to compute the image of the local map

$$E(K_v)/nE(K_v) \xrightarrow{\delta_v} H^1(K_v, E[n])$$

for any given v explicitly; and for all but a finite explicitly determinable set of places S, the image just consists of the "unramified part" of $H^1(K_v, E[n])$. This means that in some sense, we can compute all the necessary "local" conditions and use this information in bounding the "global" group $E(K)/nE(K)$. Formally, we define the *n-Selmer group* of E, $\mathrm{Sel}^{(n)}(K, E)$, to be the subgroup of $H^1(K, E[n])$ of elements that under all restriction maps res_v are in the image of δ_v in the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & E(K)/nE(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[n]) \arrow[r] \arrow[d, "\prod_v \mathrm{res}_v"] \arrow[dr, "\alpha"] & H^1(K, E)[n] \arrow[r] \arrow[d, "\prod_v \mathrm{res}_v"] & 0 \\
0 \arrow[r] & \prod_v E(K_v)/nE(K_v) \arrow[r, "\prod_v \delta_v"] & \prod_v H^1(K_v, E[n]) \arrow[r] & \prod_v H^1(K_v, E)[n] \arrow[r] & 0
\end{tikzcd}$$

Equivalently, $\mathrm{Sel}^{(n)}(K, E)$ is the kernel of the map α. The image of $\mathrm{Sel}^{(n)}(K, E)$ in $H^1(K, E)[n]$ is the kernel of the rightmost vertical map in the diagram. More generally, one defines the *Shafarevich-Tate group* of E, $Ш(K, E)$ to be

$$Ш(K, E) = \ker\Big(H^1(K, E) \longrightarrow \prod_v H^1(K_v, E)\Big)\,.$$

Then we get another short exact sequence:

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} \mathrm{Sel}^{(n)}(K, E) \longrightarrow Ш(K, E)[n] \longrightarrow 0\,.$$

This time, one can (and we will) prove that the middle group is finite. And at least in principle, it is computable. In this way, we can compute the product $(\#E(K)/nE(K))(\#Ш(K, E)[n])$, and in particular, we obtain a bound on the rank r. The obstruction against this bound being sharp lies in $Ш(K, E)$, which is therefore also an interesting object. Of course, its size (conjectured, but not generally proved to be finite) also shows up in the famous Birch and Swinnerton-Dyer conjecture, and there are other reasons to study $Ш(K, E)$ for its own sake.

We need some more notions and notation. The *unramified part* of $H^1(K_v, E[n])$ is the kernel of the restriction map $H^1(K_v, E[n]) \longrightarrow H^1(K_v^{\mathrm{unr}}, E[n])$. For any finite set of places S of K containing the infinite places, we define $H^1(K, E[n]; S)$ to be the subgroup of $H^1(K, E[n])$ of elements that map into the unramified part of $H^1(K_v, E[n])$ for all places $v \notin S$.

The finiteness of the Selmer group then follows from the two observations that $\mathrm{Sel}^{(n)}(K, E) \subset H^1(K, E[n]; S)$ for a suitable finite set S, and that $H^1(K, E[n]; S)$ is finite for all finite sets S of places of K.

The latter is a standard fact; in the end it reduces to the two basic finiteness results of algebraic number theory: finiteness of the class group and finite generation of the unit group.

Theorem 1.1. — *If S is a finite set of places of K containing the infinite places, then $H^1(K, E[n]; S)$ is finite.*

Proof. — This is a standard result, see for example [**9**, II.6.2] for a more general version. We give a proof tailored to the situation at hand, since it also gives some insight into the computational issues.

There is a finite extension $L = K(E[n])$ of K (the n-division field of E) such that $E[n]$ becomes a trivial L-Galois module. We have the inflation-restriction exact sequence

$$0 \longrightarrow H^1(L/K, E[n](L)) \longrightarrow H^1(K, E[n]) \longrightarrow H^1(L, E[n])\,,$$

and the group on the left is finite. Taking into account the ramification conditions, we see that $H^1(K, E[n]; S)$ maps into $H^1(L, E[n]; S_L)$ with finite kernel, where S_L is the set of places of L above some place of K in S. Therefore it suffices to show that $H^1(L, E[n]; S_L)$ is finite. Now

$$H^1(L, E[n]) = H^1(L, (\mathbb{Z}/n\mathbb{Z})^2) = \mathrm{Hom}(G_L, (\mathbb{Z}/n\mathbb{Z})^2)\,,$$

and the ramification condition means that the fixed field of the kernel of a homomorphism coming from $H^1(L, E[n]; S_L)$ is unramified outside S_L. On the other hand, this fixed field is an abelian extension of exponent dividing n; it is therefore contained in the maximal abelian extension M of exponent n that is unramified outside S_L.

By Kummer theory (L contains the nth roots of unity because of the n-Weil pairing), $M = L(\sqrt[n]{U})$ for some subgroup $U \subset L^\times/(L^\times)^n$. Enlarging S_L by including the primes dividing n, the ramification condition translates into

$$U = L(S_L, n) = \{\alpha \in L^\times : n \mid v(\alpha) \text{ for all } v \notin S_L\}/(L^\times)^n$$

(the "n-Selmer group of $\mathcal{O}_{L,S_L}$"). Applying the Snake Lemma to the diagram below then provides us with the exact sequence

$$0 \longrightarrow \mathcal{O}_{L,S_L}^\times/(\mathcal{O}_{L,S_L}^\times)^n \longrightarrow L(S_L, n) \longrightarrow \mathrm{Cl}_{S_L}(L)[n] \longrightarrow 0\,.$$

Since the S_L-unit group $\mathcal{O}_{L,S_L}^\times$ is finitely generated and the S_L-class group $\mathrm{Cl}_{S_L}(L)$ is finite, $U = L(S_L, n)$ is finite, and hence so is the extension M. We see that