Séminaire de théorie des nombres

Le 15 décembre à 14h

Explicit higher descents on elliptic curves

Exposé de John Cremona

Résumé : Let E/K be an elliptic curve over a number field. Descent on E attempts to get information on both the Mordell-Weil group $E(K)$ and the Shafarevich-Tate group $Ш(E/K)$. For each $n \geq 2$, there is an exact sequence

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

where $\mathrm{Sel}^{(n)}(E/K)$ is the n-Selmer group. Our goal is to compute the n-Selmer group, and represent its elements explicitly as curves $C \subset \mathbb{P}^{n-1}$ (when $n \geq 3$). Having this representation allows searching for points on C (which in turn give points in $E(K)$, since C may be seen as an n-covering of E), and also doing higher descents.

Traditionally, only 2-descent (over $\mathbb{Q}$) has been fully implemented : in this case $C \to \mathbb{P}^1$ is a double cover rather than an embedding, and elements of $\mathrm{Sel}^{(2)}(E/K)$ are represented by curves of the form $Y^2 = g(X)$ where g is a quartic. Our goal has been to be equally explicit for $n > 2$. Our algorithm is fully worked out for all odd prime n, and has been implemented in Magma for $K = \mathbb{Q}$ and $n = 3$.

The talk will be illustrated by numerical examples.

(Joint work with T. A. Fisher (Cambridge), C. O'Neil (MIT), D. Simon (Caen) and M. Stoll (Bremen))