Diophantine approximation and rational points on modular curves

Yuri Bilu, Pierre Parent (Sakura workshop, Bordeaux, January 25-29, 2010)

November 15, 2009

Let E be an elliptic curve over a number field K, without potential complex multiplication. For p a prime number, let $\rho_{E,p}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ be the mod p representation defined by the Galois action on the p-torsion of E. A well-known theorem of Serre asserts that there is an integer c_E such that ρ_p is surjective when p is larger than c_E. It is natural to wonder if there is a uniform version of this theorem, i.e. a statement where c_E would be replaced by a bound not depending on E (but only on K, or perhaps even its degree).

Making the list of relevant maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ allows to reformulate this question in terms of non-existence of rational points (except trivial ones, which are cusps or CM points) on the modular curves associated with those subgroups. It happens that those subgroups are of four types: exceptional ones, Borel, normalizer of split Cartan, normalizer of non-split Cartan. Points on curves associated with exceptional groups are not very hard to exclude, but for an arbitrary base field K, the rational points of the other curves are far form being understood. Over $\mathbb{Q}$, however, the Borel case (curves $X_0(p)$) had been ruled out by Mazur in the late 1970s, and the normalizer of split Cartan case (curves $X_{\mathrm{split}}(p)$) was treated in a recent joint work of the speakers. This last work will be the motivation of this series of talks.

The proof uses three main ingredients. The first one is an integrality result (Mazur et al.) for the rational points of $X_{\mathrm{split}}(p)$, which is algebro-geometric. The second one is effective upper bounds for isogenies in terms of heights provided by Masser, Wüstholz and Pellarin: this is transcendence theory. The third ingredient is the use of upper bounds for the height of integral points on modular curves, which was achieved by the speakers via Diophantine approximation.

The programs of the talks should be as follows:

(i) **Modular curves, their Jacobians and arithmetics** (Pierre Parent)
We will define our main objects and present a proof of some integrality properties for rational points.

(ii) **Effective Diophantine analysis** (Yuri Bilu).
This will be a very basic introduction into effective Diophantine analysis on curves (the methods of Runge and Baker). This lecture will be absolutely independent of the first one.

(iii) **Effective Diophantine analysis on modular curves** (Yuri Bilu)
Here we will give a more detailed account of effective Diophantine analysis in the special case of modular curves; these curves are especially well suited for applying Baker's and Runge's methods.

(iv) **Rational points on $X_{\mathrm{split}}(p)$** (Pierre Parent)
If time permits, we will sketch a description of the proof of the bounds for isogenies by Masser and Wüstholz. We will then complete the proof of the triviality, for large enough p, of $X_{\mathrm{split}}(p)(\mathbb{Q})$, and perhaps present related results.