Serre's uniformity in the split Cartan case

Pierre Parent

Let E be an elliptic curve over $\mathbf{Q}$, without complex multiplication over $\overline{\mathbf{Q}}$. For p a prime number, consider the representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL(E[p]) \simeq GL_2(\mathbf{F}_p)$ induced by the Galois action on the group of p-torsion points of E. A theorem of Serre, published in 1972, asserts that there exists an integer B_E such that the above representation is surjective for p larger than B_E. Serre then asked the following question: can B_E be chosen independently of E? The classification of maximal subgroups of $GL_2(\mathbf{F}_p)$ shows that this boils down to proving the triviality, for large enough p, of the sets of rational points of four families of modular curves, namely $X_0(p)$, $X_{\mathrm{split}}(p)$, $X_{\mathrm{non-split}}(p)$ and $X_{\mathfrak{A}_4}(p)$ (we say that a point of one of those curves is *trivial* if it is either a cusp, or the underlying isomorphism class of elliptic curves has complex multiplication over $\overline{\mathbf{Q}}$). The (so-called exceptional) case of $X_{\mathfrak{A}_4}(p)$ was ruled out by Serre. The fact that $X_0(p)(\mathbf{Q})$ is made of only cusps for $p > 163$ is a well-known theorem of Mazur. In this talk we will present a proof that $X_{\mathrm{split}}(p)(\mathbf{Q})$ is trivial for large enough p (joint work with Yuri Bilu).