MOD p REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES

MATTHEW GREENBERG

The goal of my course/project will be to explore some questions related to mod p representations associated to elliptic curves, i.e., the representation $\bar{\rho}_{E,p}$ of $G_F := \mathrm{Gal}(\bar{F}/F)$ on the p-torsion points in $E(\bar{F})$. (Here, F is a number field.) The lectures will develop the basic number and Galois theoretic properties of these representations. In particular, we will discuss the connection between ramification properties of these representations and reduction types of elliptic curves as well as notions related to conductors and Serre levels.

The motivating problem for the computational projects are the following: Given a representation $\bar{\rho} : G_F \to \mathrm{GL}_2(\mathbb{F}_p)$ with cyclotomic determinant, is there an algorithm to determine whether there is an elliptic curve E such that $\bar{\rho} \cong \bar{\rho}_{E,p}$ and, if so, find one. If such an E exists, we say that $\bar{\rho}$ is *elliptic*. It is known that every mod p representation with cyclotomic determinant with $p \in \{2, 3, 5\}$ is elliptic. That this result is false for $p \geq 7$ was proved by Dieulefait [4] and Calegari [2].

I propose the following computational projets in order to explore these issues:

(1) Let $p \in \{2, 3, 5\}$. For newforms f in the modular forms database whose Hecke fields admit a prime ideal of norm p, find an elliptic curve whose mod p repesentation is isomorphic to that of f.
(2) Let K be a quartic field whose Galois closure L has group $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$. Can we find an elliptic curve E such that the projectivization of $\bar{\rho}_{E,3}$ cuts out L? Try this for as many quartic fields as possible from the tables compiled by Buchmann, Ford and Pohst. (If the candidate elliptic curves lie outside the range of Cremona's tables, methods of Roberts [6] might be useful here.
(3) Let f be a newform in the modular forms database whose Hecke field has a prime ideal of norm 7. Determine if the corresponding mod 7 representation arises from an elliptic curve. If so, find it.
(4) Find a weight two newform f such that for every degree one prime $\mathfrak{p}$ of its Hecke field with $N\mathfrak{p} \geq 7$, the associated mod $\mathfrak{p}$ representation is nonelliptic.

My interest in these questions stem result from work of David Roberts [6] where he finds an elliptic curve realizing a very interesting mod 5 representation of $\mathrm{Gal}(\bar{F}/F)$ that Dembélé, Voight and I [3] originally found in a higher dimensional abelian variety by computing Hilbert modular forms. (Here, F is the unique degree 5 subfield of $\mathbb{Q}(\zeta_{25})$. Roberts' methods are extremely interesting and we could also think about their possible application to the problem of finding equations of elliptic curves over number fields with small conductor.

Date: April 15, 2010.

References

[1] J. Buchmann, D. Ford, M. Pohst, *Enumeration of quartic fields of small discriminant*, Math. Comp. 61 (1993) No. 204, 873-879.

[2] F. Calegari, *Mod p representations on elliptic curves*, Pacific. J. Math. 225 (2006) No. 1, 1-11.

[3] L. Dembélé, M. Greenberg, J. Voight, *Nonsolvable number fields ramified only at* 3 *and* 5, submitted.

[4] L. Dieulefait, *Existence of nonelliptic mod ℓ Galois representations for every $\ell > 5$*, Exp. Math. 13 (2004) No. 3, 327-329.

[5] N. Shepherd-Baron, R. Taylor, *Mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc. 10 (1997) No. 2, 283-298.

[6] D. Roberts, *Polynomials of field discriminant 5^A*, submitted.