

1086-11-1903

**Andrew V. Sutherland\*** ([drew@math.mit.edu](mailto:drew@math.mit.edu)). *Computing the image of Galois representations attached to elliptic curves.*

Let  $\ell$  be a prime, and let  $E/\mathbb{Q}$  be an elliptic curve. The action of the absolute Galois group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on the  $\ell$ -torsion subgroup  $E[\ell]$  induces a group representation  $\rho_{E,\ell}: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[\ell]) \simeq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ . A conjecture of Serre states that there is an absolute bound  $\ell_{\max}$  such that  $\rho_{\ell,E}$  is surjective for all primes  $\ell > \ell_{\max}$  and all elliptic curves  $E/\mathbb{Q}$  without complex multiplication (CM); it is generally believed that the conjecture holds with  $\ell_{\max} = 37$ . This implies that there is a finite set of groups that arise as the image of a non-surjective representation  $\rho_{\ell,E}$  for an elliptic curve  $E/\mathbb{Q}$  without CM. As a first step toward computing this set, I will describe a highly efficient algorithm for computing  $\rho_{\ell,E}$  (up to isomorphism and usually up to conjugacy) for all primes  $\ell$  up to a given bound  $\ell_{\max}$  and all elliptic curves  $E$  in a given family. I will then present results covering all the elliptic curves without CM listed in Cremona's tables or the Stein-Watkins database. (Received September 24, 2012)