Galois Representations with Non-Surjective Traces

Chantal David, Hershy Kisilevsky and Francesco Pappalardi

Abstract. Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $r$ be an integer. According to the Lang-Trotter conjecture, the number of primes $p$ such that $a_p(E) = r$ is either finite, or is asymptotic to $C_{E,r} \sqrt{x}/\log x$ where $C_{E,r}$ is a non-zero constant. A typical example of the former is the case of rational $\ell$-torsion, where $a_p(E) = r$ is impossible if $r \equiv 1 \pmod{\ell}$. We prove in this paper that, when $E$ has a rational $\ell$-isogeny and $\ell \neq 11$, the number of primes $p$ such that $a_p(E) \equiv r \pmod{\ell}$ is finite (for some $r$ modulo $\ell$) if and only if $E$ has rational $\ell$-torsion over the cyclotomic field $\mathbb{Q}(\zeta_\ell)$. The case $\ell = 11$ is special, and is also treated in the paper. We also classify all those occurrences.