Exposé court

92 *On congruence classes of orders of reductions of elliptic curves*

Pajaziti, Antigona (University of Luxembourg)

Let E be an elliptic curve defined over $\mathbb{Q}$ and $\widetilde{E}_p(\mathbb{F}_p)$ denote the reduction of E modulo a prime p of good reduction for E. Given an integer $m \geq 2$ and any a modulo m, we consider how often the congruence $|\widetilde{E}_p(\mathbb{F}_p)| \equiv a \mod m$ holds. We then exhibit elliptic curves over $\mathbb{Q}(t)$ with trivial torsion for which the orders of reductions of every smooth fiber modulo primes of positive density at least $1/2$ are divisible by a fixed small integer. We show that the greatest common divisor of the integers $|\widetilde{E}_p(\mathbb{F}_p)|$ over all rational primes p cannot exceed 4. We also show that if the torsion of E grows over a quadratic field K, then one may explicitly compute $|\widetilde{E}_p(\mathbb{F}_p)|$ modulo $|E(K)_{tors}|$. More precisely, we show that there exists an integer $N \geq 2$ such that $|\widetilde{E}_p(\mathbb{F}_p)|$ is determined modulo $|E(K)_{tors}|$ according to the arithmetic progression modulo N in which p lies. It follows that given any a modulo $|E(K)_{tors}|$, we can estimate the density of primes p such that the congruence $|\widetilde{E}_p(\mathbb{F}_p)| \equiv a \mod |E(K)_{tors}|$ occurs. This is joint work with Assoc. Prof. Mohammad Sadek.