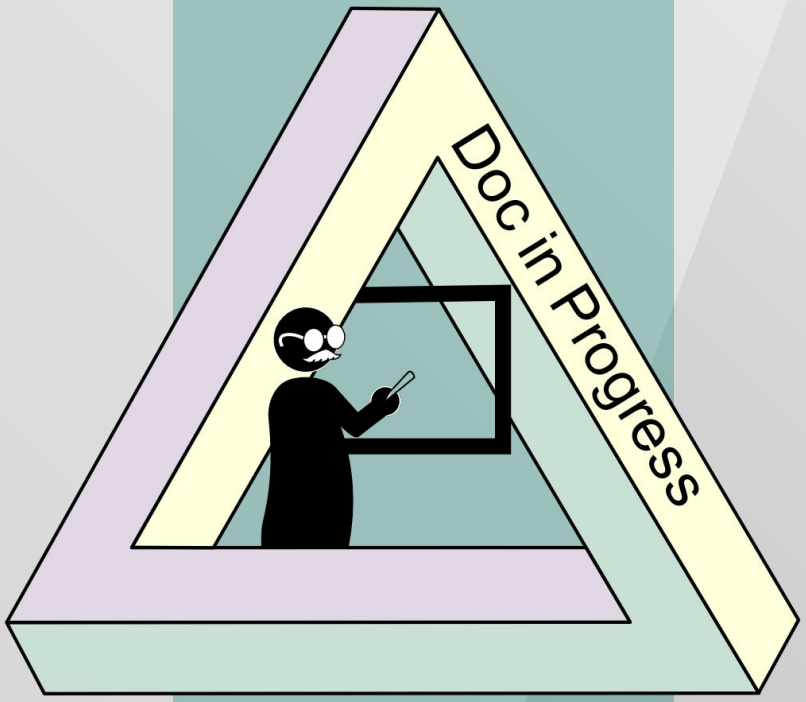
UNIVERSITÀ DI TRENTO
Dipartimento di Matematica



PhD in Mathematics

"Doc in Progress" is pleased to introduce you to

Antigona Pajaziti

University of Luxembourg

PhD in Mathematics

On Congruence classes of orders of reductions of elliptic curves

Let E be an elliptic curve defined over **Q** and $\tilde{E}_p(\mathbf{F}_p)$ 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 $|\tilde{E}_p(\mathbf{F}_p)| \equiv a \pmod m$ holds. We show that the greatest common divisor of the integers $|\tilde{E}_p(\mathbf{F}_p)|$ over all rational primes p cannot exceed 4. We then exhibit elliptic curves over $\mathbf{Q}(t)$ 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 also show that if the torsion of E grows over a quadratic field **K**, then one may explicitly compute $|\tilde{E}_p(\mathbf{F}_p)|$ modulo $|E(\mathbf{K})_{tors}|$. More precisely, we show that there exists an integer $N \geq 2$ such that $|\tilde{E}_p(\mathbf{F}_p)|$ is determined modulo $|E(\mathbf{K})_{tors}|$ according to the arithmetic progression modulo N in which p lies. It follows that given any a modulo $|E(\mathbf{K})_{tors}|$, we can estimate the density of primes p such that the congruence $|\tilde{E}_p(\mathbf{F}_p)| \equiv a \pmod{|E(\mathbf{K})_{tors}|}$ occurs.

Thursday, November 16 – 16:00 CET

The seminar will take place in room "Aula Seminari -1" (Department of Mathematics). If needed, please contact docinprogress.unitn@gmail.com using an institutional e-mail address to ask for a Zoom streaming of the event.

docinprogressunitn.wordpress.com