Arithmetic Progressions on Elliptic Curves

Alejandra Alvarado
under the supervision of Dr. Andrew Bremner

Abstract: Consider an elliptic curve of the form $y^2 = x^3 + ax + b$. Under the supervision of Dr. Andrew Bremner, we investigated arithmetic progressions in the $x$-coordinates of points of finite order. In particular, we looked at the curve $y^2 = x^3 - x$ over the field of rational numbers. We proved that for any rational point $P$ on the curve, there exist infinitely many other points $Q$ on the curve such that $P - Q$ is a point of finite order. We used techniques from algebraic geometry, number theory, and elliptic curve theory to prove our results. Our findings have implications for cryptographic applications and the study of Diophantine equations.