Research Projects

Searching for $E(\mathbb{Q}) \simeq Z_2 \times Z_4 \times \mathbb{Z}^9$. Given a rational number k such that $\sqrt{1-k^2}$ is irrational, the elliptic curve $E:\ y^2 = (1-x^2)\,(1-k^2\,x^2)$ has torsion subgroup $E(\mathbb{Q})_{\rm tors} \simeq Z_2 \times Z_4$. Find a rational k such that this curve has rank larger than 8. (With Goins and Ansaldi.)

***ABC*-Triples in Families.** It is well-known that there are infinitely many $(A:B:C)$ triples with quality $q(A:B:C) \geq 1$. For each $T \in \{Z_2 \times Z_2,\ Z_2 \times Z_4,\ Z_2 \times Z_6,\ Z_2 \times Z_8\}$ show that there are infinitely many $(A:B:C)$-triples such that (1) $q(A:B:C) \geq 1$ and (2) the Frey curve $E:\ y^2 = x\,(x-A)\,(x+B)$ has torsion subgroup $E(\mathbb{Q})_{\rm tors} \simeq T$. (With Goins and Ansaldi.)

Rational Distance Sets on Conic Sections. Leonhard Euler noted that there exists an infinite set of rational points on the unit circle such that the pairwise distance of any two is also rational. Given any conic section, find a necessary and sufficient condition for there to exist a rational distance set of at least five points. (With Goins and Harvey.)

Squares in Arithmetic Progressions. Pierre de Fermat showed that there are no four rational squares in a nontrivial arithmetic sequence. Find those quadratic extensions $\mathbb{Q}(\sqrt{D})$ such that there exists four rational squares in a nontrivial arithmetic sequence by determining those integers D for which the quadratic twist $E^{(D)}:\ y^2 = x^3 + 5\,D\,x^2 + 4\,D^2\,x$ has a nontrivial rational point. (With Goins and Harvey.)

Encoding via ECC. Write code which will take as input a 160-character clear text and return as output a 160-character garbled text by (1) turning the text into a number between 0 and 2^{128} using `Unicode`, (2) manipulate this number using elliptic curve cryptogrphy, and (3) converting the new number back into a 160-character text. (With Goins and Lomelí.)

Decoding via ECC. Write code which will take as input a 160-character garbled text and return as output a 160-character clear text by (1) turning the text into a number between 0 and 2^{128} using `Unicode`, (2) undoing the elliptic curve cryptography by factoring a number, and (3) converting the new number back into a 160-character text. (With Goins and Lomelí.)