Counting Problems in Number Theory
Elliptic and Plane Quartic Curves over Finite Fields

Challenge:

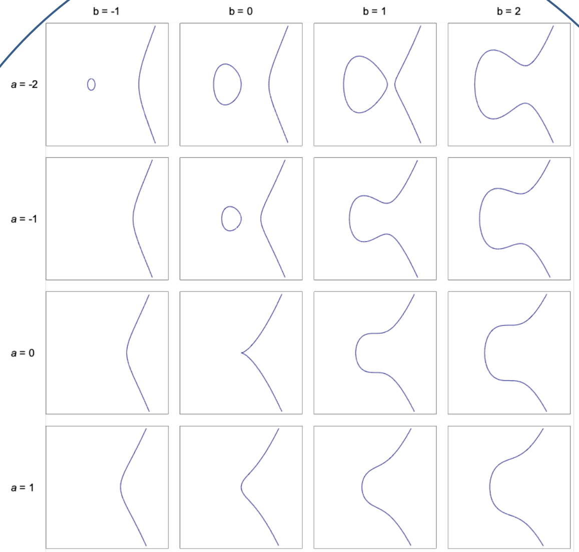
- Many crypto systems work in lattices and groups of rational points of elliptic curves over finite fields. Systems depend on particular choices.
- Want to understand whether choices 'look random'.
- What does a random sublattice of $\mathbb{Z}^n$ 'look like'?
- How are groups of rational points of elliptic curves over finite fields distributed?

Solution:

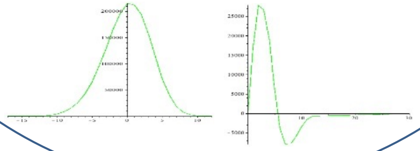
- Techniques from *zeta functions of groups and rings* to study random lattices.
- Techniques from *coding theory* to study rational point count distributions for families of curves.
- Ideas from *random matrix theory over the p-adic integers*.

- Award Number 1802281
- University of California, Irvine
- Contact: nckaplan@math.uci.edu

Elliptic Curves



Point Counts for Quartic Curves



Scientific Impact:

- Understanding distributions of arithmetic objects can highlight what it means for an object to 'look special'.
- Special objects may have algebraic structure that changes the difficulty of cryptographic problems.

Broader Impact and Broader Participation:

- Low technical barriers to entry, opportunities for experimentation and computation. Excellent for students.
- Developed problems for REU program.
- Extensive outreach: REU groups, Math Clubs, Undergraduate Research Symposium, Museum of Mathematics.
- Communication across mathematical cultures

(Number Theory) <-> (Codes and Crypto)