The sequence of quadratic residues modulo a prime $p$ is a sequence of $p - 1$ symbols 1 or $-1$ that encodes the solubility of quadratic congruences modulo $p$ and that behaves in many respects like a random binary sequence of length $p - 1$. In this project we studied a certain “random walk” in the plane formed with this sequence, the “Quadratic Residue Random Walk” (QRRW). The QRRW modulo $p$ is a finite walk in the plane consisting of $p - 1$ steps of unit length and starting at the origin.

A famous result of Gauss predicts the end point of a QRRW, but what happens along the way is rather mysterious and has not been unexplored in the literature. A cursory examination of QRRW graphs shows random-like features such as sudden turns, sharp cusps, and ragged edges, but also some unexpected symmetries, though no obvious patterns.

The goal of this project was to unravel some of these mysteries. We identified six distinct shapes for a QRRW, and we correlated these shapes with congruence classes of $p$ modulo small primes. We developed efficient algorithms and C code to facilitate large scale computations of QRRWs, and we used the campus computing cluster to carry out these computations. We computed a variety of quantities associated with a QRRW, such as the maximal distance to the origin and the amount of time spent in each quadrant. We also created animations showing the evolution of a QRRW.