Richard Cho

Quadratic Residues and Their Application

This project explores quadratic residues, a classical number theory topic, using computational techniques. First I conducted computational experiments to investigate the distribution of quadratic residues modulo primes, looking for patterns or evidence against randomness. The experimental data indicates a non-random distribution of quadratic residues. Certain features of such non-random distributions were then further investigated for application in cryptography, especially semi-prime factorization. Prior research on factoring using quadratic residues searches for quadratic residues that are perfect squares, based on Fermat's Factorization Method. In this project, I developed a novel approach that uses simply the number of quadratic residues to factor semi-primes. Mathematically, I developed and proved the validity of a function that returns the factors of a semi-prime given the semi-prime and the number of quadratic residues of the semi-prime. The function reduces the problem of semi-prime factorization to computing the number of quadratic residues of the semi-prime. Computationally, I developed an approach to make the current method of generating quadratic residues more memory efficient while retaining a near linear speed up from parallelization. (linear time reduction is optimal) The next step will be to run my algorithm in the cloud, in a multi-core environment, to validate the efficiency claim of my multi-threaded approach. Future work will focus on computing the number of quadratic residues quickly and efficiently, especially on multi-core platforms, such as servers or clouds. Also, due to some similarities between my theory and the quadratic sieve factoring method, there may be a way to incorporate my findings into the quadratic sieve factoring algorithm to achieve a much faster run-time for factoring semi-primes. The main outcome of this research will impact the security of the RSA encryption scheme.