CALIFORNIA STATE SCIENCE FAIR
2013 PROJECT SUMMARY

Name(s)

Richard K. Cho

Project Number

S1404

Project Title

A Computational Exploration of Quadratic Residues and Their Applications

Abstract

Objectives/Goals

My objective was to learn how to more quickly compute the number of quadratic residues modulo semiprimes. This was because I proved last year that the number of quadratic residues can be used to factor semiprimes, which is potentially a groundbreaking result since the difficulty of semiprimes being hard to factor is at the backbone of the RSA encryption scheme, which is essential to secure data transmissions across the internet. To this extent a faster factoring algorithm was not created, but gains were made toward a faster algorithm. Evidence was found that the distribution of quadratic residues modulo primes is nonrandom, and patterns were found and proven in the distribution of quadratic residues modulo semiprimes.

Methods/Materials

My objective was to learn how to more quickly compute the number of quadratic residues modulo semiprimes. This was because I proved last year that the number of quadratic residues can be used to factor semiprimes, which is potentially a groundbreaking result since the difficulty of semiprimes being hard to factor is at the backbone of the RSA encryption scheme, which is essential to secure data transmissions across the internet. To this extent a faster factoring algorithm was not created, but gains were made toward a faster algorithm. Evidence was found that the distribution of quadratic residues modulo primes is nonrandom, and patterns were found and proven in the distribution of quadratic residues modulo semiprimes.

Results

During further exploration into the distribution of quadratic residues, many things were discovered. I used the Dieharder test suite in conjunction with my own C++ programs for evaluating the randomness of the distribution of quadratic residues modulo primes. My tests have shown evidence against randomness, although a concrete explanation as to why remains unknown. Symmetry and relation to factors have been found and proven of the distribution of quadratic residues modulo a semprime; previously a relation to just the number of quadratic residues was proven. Furthermore, I implemented a multithreaded version of my program to generate quadratic residues, achieving a 65% time reduction.

Conclusions/Discussion

It is intriguing that my data points to quadratic residues modulo primes to not be random. The question remains, why? An explanation needs to be found. This could reveal very important relations regarding the distribution of quadratic residues, which could in turn be used to factor semiprimes. Also, while I proved relations that could improve the speed of counting the number of quadratic residues modulo semiprimes, it

Summary Statement

The project is on quadratic residues modulo primes and semiprimes and tries to find a quicker method of factoring semiprimes, since this would have a major impact on encryption schemes that rely on semiprimes being hard to factor, like RSA.

Help Received

Dr. Ali Gurel helped me verity the proofs I wrote; Dr. William Wu helped me get started with multithreading