CALIFORNIA STATE SCIENCE FAIR
2012 PROJECT SUMMARY

Name(s)
Richard Cho

Project Number
S1404

Project Title
Exploring Quadratic Residues and Their Potential Applications

Abstract

Objectives/Goals
Objectives:
1) Explore the distribution of quadratic residues and find patterns or explore randomness.
2) Number Theory is quite heavily used in modern-day cryptography. Are there possible applications of quadratic residues?

Methods/Materials
Methods: Use the computer to generate and visualize data. Then, with these leads, proceed mathematically until a suitable explanation is reached, proving some relations. (In the parts of the project emphasizing math.) Also, programs can verify explanations and proofs with cast amounts of empirical data. I used a combination of C++ programs and Mathematica notebooks to generate and process data.

Materials: Computer, Pen/pencil, Paper, Code::Blocks C++ IDE, Mathematica 8 for Students.

Results
This project was a multifaceted one. Several interesting patterns in the distribution of quadratic residues were explored and proven. As for the application into cyprography, a novel way was found for factoring semi-primes, which can revolutionize the current state of cryptography.

Conclusions/Discussion
Through a long exploration through quadratic residues, we learned that some very interesting things. Interesting patterens about the distribution and number of quadratic residues were proven, usually modulo a prime. Mainly C++ programs were deploed to generate quadratic residues, count the number of distinct elements, and count the number of consecutive pairs and triples. Mathematica was used, with its powerful graphical functions, to help us in discovering pattern on the distribuiton of quadratic residues modulo primes.
To end, there was a hint into solving one of the biggest unsolved problems in cryptography, how semi-primes can be factored easily, using the number of quadratic residues. This would be ground breaking, as such a discovery would shatter RSA and would revolutionize the Internet and computer driven world we live in today.

Summary Statement
An investigation into quadratic residues, where interesting patterns were found as well as a competely new way for factoring semi-primes.

Help Received
Dr. Ali Gurel answered some of my mathematical questions about quadratic residues.