CALIFORNIA SCIENCE & ENGINEERING FAIR
2018 PROJECT SUMMARY

Name(s)

Alexa A. Wingate

Project Number

38462

Project Title

Fermat vs. Brute Force: The Making of a Better Primality Test

Abstract

Objectives/Goals

RSA encryption is used to protect a person#s privacy on the internet. Part of the encryption process involves quickly distinguishing large prime and composite numbers. The objective of this experiment is to build a much more efficient primality test using probabilistic methods.

Methods/Materials

For this experiment, I programmed my own Probabilistic Fermat primality test using python and also built a simple deterministic brute force algorithm to compare it against. To exploit Fermat#s unique advantages to vary confidence levels, I introduced a #Fermat Witness Limit# parameter to control the number of iterations that the Fermat test performed. With this, I could trade-off precision for speed with the intention of discovering the right balance between the two goals.

To compare the Probabilistic approach (Fermat) vs the deterministic (brute force) approach, my program ran many numbers through both engines while monitoring the time it took for each of the methods to determine a number#s primeness. Then I also added an error-checking component to my python program to see how varying the #Fermat Witness Limit# would add imprecision. I optimized the engine by testing multiple scenarios against the deterministic (brute force) approach. The data was exported to excel to display the relative performance of the two distinct approaches.

Results

The results of this experiment found that as the numbers got larger, the Fermat primality test could decrease the Fermat Witness Limit without sacrificing much imprecision. This would make it find prime numbers the size that would be used in RSA encryption up to 10^100 times faster than the brute force algorithm. However, the Fermat approach was only equally as good compared to the brute force algorithm at verifying composite numbers.

Conclusions/Discussion

The results of this experiment fulfill the objective of the experiment in creating an efficient algorithm for finding primes. The Fermat primality test was found to be much, much faster than the brute force algorithm for finding primes, although it was no better at identifying composites.

Summary Statement

I created an efficient primality test using a probabilistic approach and Fermat's Little Theorem.

Help Received

My former mentor, David Crane, helped me to make the Fermat primality test more efficient by speeding up the time it took to do some of the long calculations.