Optimizing the Search for Mersenne Primes

Cato, Carson

Mersenne Primes are prime numbers of the form 2^p-1 where p is prime. These numbers have been studied for over 2,000 years and continue to mesmerize mathematicians today with a number of unsolved problems. It was the goal of this project to incorporate number theory and higher mathematics into a program to find Mersenne Primes. The Lucas-Lehmer test is the only primality test designed specifically for Mersenne Numbers. However, it is time consuming; so, this project worked to incorporate quick fails which would limit its use. The quick fail of this project involved the existing theorem that only prime numbers of the form 2kp+1 can possibly divide the Mersenne Number, 2^p-1. By incorporating this property, the program performed fewer operations and consequently consumed less time when testing for the primality of a Mersenne Number. The time and the number of operations required to divide each Mersenne Number, 2^p-1, for 2=p=50,000 by every prime less than 50,000,000 using both the brute force method and the 2kp+1 method were recorded. The brute force times increased linearly to over two minutes while the 2kp+1 times remained constant at around 0.4 seconds. The number of operations required for brute force increased to a constant 3,001,134 while the operations required for 2kp+1 quickly decreased to under 1,000 and less than 100 for larger p.

Awards Won:
National Security Agency Research Directorate : Honorable Mention in Mathematics