CCSU
DEPARTMENT OF MATHEMATICAL SCIENCES

COLLOQUIUM

Friday, April 26
3:00 – 4:00 PM
Maria Sanford, Room 101

IS N A PRIME NUMBER?
PRIMALITY TESTING ALGORITHMS

SHAWN FALBOWSKI

(MA in Mathematics Thesis Presentation)

CENTRAL CONNECTICUT STATE UNIVERSITY

Abstract: A prime number is a counting number larger than 1 with only two divisors: itself and 1. There are infinitely many prime numbers, therefore for any number, there is always a prime number larger than it. Large prime numbers are used in cybersecurity and cryptography, so, the more large prime numbers we find, the more secure our communications become.

But, how can we use a computer to find large prime numbers? As of right now, the largest known prime number is $2^{82,589,933} - 1$, which has more than 23,000,000 digits. This is a number (much) larger than the estimated number of atoms in the observable universe, so how can the computer deal with such numbers within any reasonable amount of resources (time and memory)?

Algorithms have existed to verify primality since at least the third century BCE, but it was only recently that an algorithm was discovered to be simultaneously fully deterministic and reasonably efficient.

In this presentation we will discuss some of the most efficient methods that use computers to test primality.

For further information:
gotchevi@ccsu.edu 860-832-2839
http://www.math.ccsu.edu/gotchev/colloquium/