MATH 788M: COMPUTATIONAL NUMBER THEORY

COURSE DESCRIPTION:

A more descriptive title for the course might be, "Methods For Doing Arithmetic Quickly." The course will focus on effective algorithms for performing tasks such as multiplication, finding the greatest common divisor of two integers, determining whether a large integer is prime, finding real large primes, factoring integers, and the corresponding problems for polynomials. There will be no requirement to use the computer (though you may want to try out some of the fancy stuff you're learning on a computer). Some tidbits from this course include:

(1) The largest known prime is $2^{859433} - 1$ and contains 258716 digits. We will discuss how the prime was found.

(2) We will discuss how you can communicate privately with someone in the personals even though you have never met or even communicated with the person before. In other words, we will discuss how one can publish, for the whole world to see, a coded message to someone else, and how the other person who might be a complete stranger can be the only one who can understand the message. Sound impossible? It's not.

(3) Methods for factoring large integers, say with about 140 digits, have improved during the last several years. We will discuss what is behind these current methods.

(4) It is not known whether it is possible to factor an integer in polynomial time. We will discuss what this means. On the other hand, it is possible to factor polynomials (i.e., to express a polynomial with integer coefficients as a product of irreducible polynomials with integer coefficients) in polynomial time. We will discuss the proof of this result. The proof is based on an important algorithmic method (called the L^3 algorithm) developed by Lenstra, Lenstra, and Lovász.

(5) Despite (4), Maple (what we use locally for symbolic manipulations) uses an older algorithm, due to Zassenhaus, for factoring polynomials which is not a polynomial time algorithm. Why? Because it's faster. How could that be? Well, it's not really faster, but it's usually faster. We will discuss what this means and what Maple does.