Course Description for Spring 2003

Course Title: Math 788G: The Theory of Irreducible Polynomials II

Instructor: Michael Filaseta

Prerequisites: Graduate Standing (no prior Number Theory course is necessary; background material will be given; see description below)

Meeting Time: To Be Determined

Description: Although this course will be a natural follow-up to Math 788F, being offered in Fall 2002, the intent is for Math 788G to contain material that is sufficiently separate from Math 788F so that new students to the sequence will feel comfortable with the material. One emphasis of Math 788G will be on computational questions (no computer background needed). We will address the issue of what makes one algorithm better than another (the running time of an algorithm) and what are the current best irreducibility and factoring algorithms. We will be interested in computations from both theoretical and practical viewpoints. For example, we will discuss the Lenstra-Lenstra-Lovász algorithm (the L^3-algorithm) which produces a polynomial time algorithm for factoring polynomials. On the other hand, for factoring, this algorithm *typically* runs slower than non-polynomial time algorithms, so we will discuss the non-polynomial algorithms for factoring as well. In addition, we will look at the notion of a "lacunary" or "sparse" polynomial (a polynomial which has a relatively small number of non-zero terms as compared to its degree) and consider irreducibility and factoring algorithms for such polynomials. This will lead us to investigate other related issues. For example, the following will be dealt with in the course:

1. We will show that it is possible to classify the polynomials of the form $x^n \pm x^m \pm 1$ which are irreducible and extend the ideas to polynomials of the form $x^n \pm x^m \pm x^k \pm 1$. Then we will address the issue of extending this further. If non-zero integers $a_d, a_{d-1}, \dots, a_0$ are fixed, we will show that it is possible to classify the positive integers $n_d, n_{d-1}, \dots, n_1$ for which the polynomial $a_d x^{n_d} + a_{d-1} x^{n_{d-1}} + \cdots + a_1 x^{n_1} + a_0$ is irreducible. We will examine these issues from both a theoretical and practical point of view.

2. Schinzel gave the example

$$(5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3)x^n + 12,$$

   which is a polynomial that is reducible for every nonnegative integer n. The constant term 12 in this polynomial is significant. The problem of whether there is a polynomial $f(x) \in \mathbb{Z}[x]$ with nonnegative coefficients such that $f(x)x^n + 1$ is reducible for every nonnegative integer n remains open. We will explain material related to this problem and, in particular, show that a solution to the problem would likely lead to an answer to another long-standing conjecture in Number Theory (for which prize money has been offered).

3. A conjecture of Turán is that there is an absolute constant C such that if $f(x)$ is an arbitrary polynomial in $\mathbb{Z}[x]$, then there is an *irreducible* polynomial $g(x) \in \mathbb{Z}[x]$ for which the sum of the absolute values of the coefficients of $f(x) - g(x)$ is $\leq C$. We will explain a solution to this problem and address the questions of how small C is and how small the degree of $g(x)$ is (as compared to the degree of $f(x)$).