Modern Computer Algebra Syllabus

Course Title: MAT Modern Computer Algebra

Course Description: Computer algebra is a recent area of computer science, where mathematical tools and computer software are developed for the exact solutions of equations. The course is designed to expose students to algorithms used for symbolic computation, as well as to concepts from modern algebra which are applied to the development of these algorithms.

Text:

Hours & Credit: 4 hrs lect., 4 Cr

Prerequisite(s): MAT 1475, MAT 2580

Prepared by: Dr. Douglas and Dr. Kahrobaei (To be taught at NYCCT)

Topics:

**Fundamental Algorithm** (Representation and addition of numbers, Representation and addition of polynomials, Multiplication, Division with remainder)

**Euclidean Algorithm** (Euclidean Domains, The Extended Euclidean Algorithm, Cost Analysis for Z and F[X], (non-)uniqueness of gcd)

**Applications of the Euclidean Algorithm** (Modular Arithmetic, Modular inverses via Euclid, Repeated squaring, Modular inverses Fermat, Linear Diophantine equations)

**Modular Algorithms and interpolation** (Change of representation, Evaluation and interpolation, Application: Secret sharing, The Chinese Remainder Algorithm, Modular determinant)

**Fast Multiplication** (Karatsuba's multiplication algorithm, The discrete Fourier Transform and the Fast Fourier Transform)

**Newton iteration** (Division with remainder using Newton iteration, Generalized Taylor expansion and radix conversation, Formal derivatives and Taylor expansion, Solving polynomial equations via Newton iteration)

**Factoring polynomials over finite fields** (Factorization of polynomials, Distinct-degree factorization, Equal degree factorization: Cantor and Zassenhaus’ algorithm, A complete factoring algorithm, Application: root finding, square free factorization)

**Hensel lifting and factoring polynomials** (factoring in Z[x] and Q[x], A factoring algorithm)

**Computational Number Theory**