University of Toronto Spring 1997

CSC478S/2412S: Computer Algebra

Instructor: Daniel Panario, daniel@cdf (preferable), daniel@cs

Office hours: T 10-11 in SF 2304A, or by appointment.

Lectures: TR 2 in MP 118, and F 2 in LM 157.

Tutor: David Neto, at478net@cdf

Text: K. O. Geddes, S. R. Czapor and G. Labahn, ALGORITHMS FOR COMPUTER ALGEBRA, Kluwer, 1992.

Language: MAPLE, a system for symbolic mathematical computation. Optional for project: C++.

Prerrequisities: mathematical maturity is recommended. Although not required, at least one undergraduate abstract algebra course may be useful. Undergraduate courses in discrete mathematics and in data structures could be helpful.

Marking scheme:

Work	Hand-out Date	Due Date	Value
A1	Jan 14	Jan 28	5%
A2	Jan 28	Feb 14	15%
A3	Feb 14	Mar 7	15%
A4	Mar 7	Mar 28	15%
A5	Mar 21	Apr 11	15%
Proj	Feb 11	Apr 11	35%

Plagiarism: assignments and project have to be your own work. Plagiarism is a serious academic offense.

Web page:

`http://www.eecg.utoronto.ca/~neto/teaching/478/index.html`

Newsgroup: ut.cdf.csc478h

Course goals: This course is an introduction to basic algebraic algorithms that are useful for computer algebra systems. More specifically, operations like multiplication, division, greatest common divisors and factorization are studied over several domains including the ring of integers, finite fields, polynomial rings, and quotient rings. The basic tools considered include modular arithmetic, discrete Fourier transform, Chinese remainder theorem, Newton iteration, and Hensel techniques. Grobner bases and their applications are taken into account. An overview of the structural properties of finite fields covering some applications in detail is considered.

Course outline (some of these topics will be covered):

- Introduction: computer algebra systems; relation with numerical analysis; overview of MAPLE.
- Algebraic structures: groups, rings, integral domains, Euclidean domains, quotient fields, finite fields (each structure introduced when needed).
- Normal forms and data structures: the need for simplification; normal forms for polynomials; data structures for integers, rational numbers and polynomials.
- GCD algorithms: extended Euclidean algorithm and applications; Chinese remainder theorem; modular arithmetic; subresultants; generalization of the Euclidean algorithm for multivariate polynomials.
- Arithmetic: classical methods for multiplication and division of integers and polynomials; Karatsuba and Ofman's algorithm; the fast Fourier transform and fast arithmetic; Newton's iteration; arithmetic on matrices, rational functions and power series.
- Factorization of polynomials: deterministic and probabilistic algorithms over finite fields; Berlekamp's algorithm; Hensel lifting; Lenstra, Lenstra and Lovász' algorithm.

- Grobner basis: term ordering and reduction; Buchberger's algorithm; applications.
- Applications and other topics: primality testing; public key cryptography; solutions of linear equations and systems of sparse linear equations; error-correcting codes; symbolic summation and integration; etc.

Special dates:

Feb 17-21	reading week (no classes)
Mar 7	last day to drop without penalty
Mar 28	Good Friday (University closed)
Apr 11	last lecture