

CPSC/MATH 499/699 — Computational Ring Theory

Precluded: Similar courses taught in Fall 1998 or Winter 2002.

Goal: to present an introduction to the algebra, data structures, and algorithms of abstract algebra, in particular ring theory.

Grading:	Notes	: 10%	Text: <i>Modern Computer Algebra</i> by Joachim von zur Gathen and Jürgen Gerhard
	Homework	: 10%	
	Exam 1	: 25%	
	Exam 2	: 25%	
	(Final) Exam 3	: 30%	
Professor: Dr. David Casperson	Dates:	First class	: Tue, Jan 06
		Exam 1	: Thu, Feb 05
Office: T & L 10-2046		Last drop day	: Fri, Feb 13
		Winter break	: Feb 16–20
Telephone: 960-6672		Exam 2	: Thu, Mar 12
		Course evaluations	: Tue, Mar 31
e-mail: casper@unbc.ca		Good Friday	: Fri, Apr 10
		Easter Monday	: Mon, Apr 13
		(Final) Exam 3	: 14–25 Apr

Syllabus: Topics will be chosen from among the following. I aim to reach modern algorithms for factorizing polynomials over the rationals by the end of the course.

Definition of rings. Examples. The integers. The reals. Fraction fields. Polynomial Rings. Exact division rings. Matrix rings. Formal power series. Modular arithmetic. Prime fields. Quotient rings.

Classification of Rings. Commutative rings. Integral domains. Euclidean domains. Principal Ideal Domains. Unique factorisation domains. Fields. Division rings.

The integers. Addition and subtraction for the integers. The basic multiplication and division algorithms for the integers. Kurasawa's algorithm. Using Newton's method for division.

Euclidean domains and Euclid's algorithm. Arithmetic for the rationals. The Chinese remainder theorem for integers.

Homomorphisms and ideals. The first isomorphism theorem for rings.

Polynomial rings. Lagrange interpolation. Evaluation homomorphisms. Determinants of matrices of univariant polynomials. Fast Fourier transforms and multiplication. Fast Fourier transforms and prime fields.

p -adic number fields. Hensel lifting.

The running time of Berlekamp's algorithm. Factorisation over $\mathbf{Z}[X]$.

Notes

- The precise marking scheme and dates will be finalized in the first two weeks of classes.
- The grading scheme for graduate students will include an extra project to be determined in conjunction with the instructor in the first week of the course.
- Assignments may be tailored to student background and course number.