CPSC 499/MATH 499 — Computational Ring Theory

Precluded: Fall 1998 CPSC 499 or Fall 1998 MATH 499.

Overview: This course is intended to be an introduction to the algebra, data structures, and algorithms of abstract algebra, in particular ring theory.

Grading: [1]

Notes	:	10%
Homework	:	10%
Exam 1	:	25%
Exam 2	:	25%
(Final) Exam 3	:	30%

Professor: Dr. David Casperson

Office: Lib 5-444

Telephone: 960-6672

e-mail: casper@unbc.ca

Text: *Modern Computer Algebra* by Joachim von zur Gathen and Jürgen Gerhard

Dates:

First class	:	Tue, Jan 08
Winter break	:	Feb 18–22
Exam 1	:	Thu, Feb 05
Last drop day	:	Wed, Feb 13
Exam 2	:	Thu, Mar 14
Good Friday	:	Fri, Mar 29
Easter Monday	:	Mon, Apr 01
Course evaluations	:	Wed, Apr 03
(Final) Exam 3	:	12–20 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 $\mathbf{Z}[X]$.

[1] subject to revision