UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

Pure Mathematics 627 Computational Number Theory

(see Course Descriptions: www.ucalgary.ca/pubs/calendar/current/course-desc-main.html)

Syllabus

Topics	**Number of Hours**
Integer Arithmetic: Addition, subtraction, multiplication, division, greatest common divisor, perfect power testing, comutations in (Z/nZ)*.	6
Polynomial Arithmetic: Addition, subtraction, multiplication, division, greatest common divisor	2
Finite Fields: Representation, arithmetic, polynomial factorization, irreducibility testing.	6
Primality Proving: Pseudoprimes and probabilistic primality tests, primality proving of numbers of a special form, Goldwasser-Kilian test, Primality proving in deterministic polynomial time (AKS algorithm).	6
Integer Factorization: p-1 method, Pollard rho method, quadratic sieve.	6
Algorithms in Number Fields: Number fields, ideals and their arithmetic, class groups and regulators.	6
Student Presentations:	7
TOTAL:	**39**

* * * * * * *

2010:08:12 Effective: Fall 2010
RS:jml
Description change: 2011:07:01
WEC