Department of Mathematics & Statistics
Department of Computer Science & Software Engineering
Concordia University

MAST 332/COMP 367

Techniques in Symbolic Computation

Winter 2024

Instructor: Dr. A. Atoyan, Office: LB 1041.24 (SGW), Phone: 514-848-2424, Ext. 5221
Email: armen.atoyan@concordia.ca

Class Schedule: Mondays & Wednesdays, 11:45-13:00.

Office hours: Wednesdays, 13:30-15:00.

Textbook: *A Concrete Introduction to Higher Algebra*, by L. N. Childs, 3rd Edition.
The hard-copy textbook is available at:
https://www.bkstr.com/concordiastore/home

The e-text (less expensive) can be found online at
https://link.springer.com/book/10.1007/978-1-4419-8702-0

Prerequisites: MAST 234 or COMP 248, MAST 217 or COMP 238.

Software: *MAPLE (version 19 or higher)* is mandatory for this course. The *Maplesoft* is making MAPLE ("Student's edition", quite sufficient for the course) available to students at a special price. Although there will be a brief overview of MAPLE procedures in the beginning of the course, the software **is *not* an object of study** in itself, and is only used as a *tool* for elementary symbolic computations and writing texts. **All the tests, the final examination and the assignments are done using *MAPLE*.**

Course Description: This course is on application-oriented introduction to abstract (groups finite rings and fields) used in the methods of symbolic computation and based on concepts of number theory and modular algebra. The lectures are lab based, and the structure of classes includes lecture time on the theory, alternating with problem-solving tasks done by students individually. Mathematical issues that arise during problem-solving are discussed in class. A background level of a year of undergraduate linear algebra and calculus is implied.

Assignments: Assignments will be given, and should be submitted, online through Moodle as MAPLE files. Assignments are important part of the learning process in this course and contribute 10% to the final grade.

Midterm Test: There will be **one Midterm test** based on the material learned in the previous weeks (1-6) which will contribute up to 30% to your final grade (see the Grading Scheme). It will be held in week 7, on **Monday, March 4, 2024.**

NOTE: It is the Department's policy that tests missed for any reason, **including illness,** cannot be made up. If you missed the midterm because of illness **(to be confirmed by a valid medical note)** the final exam can count for 90% of your final grade, and 10% will be contributed by the assignments.

Final Exam: The Final Examination will be 3 hours long (**closed-book** exam, no notes or electronic material is allowed) written using MAPLE in the lab equipped with computers. Students are responsible for finding out the date and time of the final exam once the schedule is posted by the Examinations Office. Conflicts or problems with the schedule of the final exam must be reported directly to the Examinations Office, ***not*** to the Instructor. **Students are to be available until the end of the final exam period.** Conflicts due to travel plans **will not** be accommodated.

NOTE: There are **no supplemental or alternate exams** for this course.

Grade: The final grade will be based on the higher of (a) and (b) below:
(a) 10% for the assignments, 30% for the class test, 60% for the final exam.
(b) 10% for the assignments, 10% for the class test, 80% for the final exam.

If the grading scheme for this course includes graded assignments, a reasonable and representative subset of each assignment may be graded. Students will not be told in advance which subset of the assigned problems will be marked and should therefore attempt all assigned problems.

CONTENTS

Week	Lectures	Topics
1	**Lecture 1**	• MAPLE Basics (an **Overview**) • Numbers, Equivalence Relations • Division Theorem, GCD & LCM • Primes, Euclid's Algorithm

2	**Lecture 2**	• Bezout's Identity & Extended Euclid's Algorithm
		• Diophantine Equations
		• Prime Factorization
		  o Fundamental Theorem of Arithmetic
		  o Euclid;s Theorem

3	**Lecture 3**	• Congruences: Basic properties
		• Linear Congruences & Bezout's Identity
		• Congruence Classes Z/mZ
		  o Complete Set of Representative, Units
		  o Solutions of linear congruences in Z/mZ

4	**Lecture 4**	• Groups, Rings & Fields
		  o Definitions & Axioms, Properties
		  o Operations in (finite) Rings & Fields
		• Units & Zero-Divisors in Z/mZ

5	**Lecture 5**	• Matrices as (non-commutative) Rings
		• Matrices & Codes: Applications
		  ○ Error Detecting & Correcting Codes: Humming Codes I and II
		  ○ Hill Cryptosystem

6	**Lecture 6**	• Fermat's and Euler's Theorems
		  ○ Order of Elements
		  ○ Euler's Phi function
		• Application of the Theorems: Calculation of large powers modulo m

7	**Lecture 7**	**MIDTERM TEST** (on the material of **Lectures 1-6)**
		• Prime Factorization of Large numbers, and crypto security
		  ○ Trial Division
		  ○ Sieve of Eratosthenes
		• Application: RSA Crypto System

8	**Lecture 8**	• Chinese Remainder Theorem (in Z/mZ)
		  ○ Systems of 2 and 3 congruences
		  ○ The general case of Chinese Remainder systems
		• Applications of the Chinese Remainder Theorem
		  ○ Solving Congruences with composite moduli
		  ○ Reducing a given system to Chinese Remainder form
		  ○ Application of the method to RSA Cryptography

9	**Lecture 9**	• Polynomials Rings R[x]: definition and properties
		• Polynomial Factorization
		  ○ Division Theorem in R[x]
		  ○ The GCD and Extended Euclid's Algorithm for R[x]
		• Irreducible Polynomials, and *Unique Factorization* Theorem in R[x]

10	**Lecture 10**	• Polynomial Congruences modulo a polynomial • Linear Congruences in F[x] • Irreducible Polynomials

11	**Lecture 11**	• Congruence Classes and Algebraic operations in F[x]/m(x)
		  ○ Complete Set of Representatives and Algorithms for its constructions
		  ○ Units and Zero Divisors in F[x]/m(x)
		• Fermat's Theorem, Order of elements, and Primitive Roots in F[x]/m(x)

12	**Lecture 12** **REVIEW**	• Linear Congruences and Chinese Remainder Theorem in F[x] • Application: Lagrange Interpolation of discrete data sets. **Review class**

Academic Integrity and the Academic Code of Conduct
This course is governed by Concordia University's policies on Academic Integrity and the Academic Code of Conduct as set forth in the Undergraduate Calendar and the Graduate Calendar. Students are expected to familiarize themselves with these policies and conduct themselves accordingly. "Concordia University has several resources available to students to better understand and uphold academic integrity. Concordia's website on academic integrity can be found at the following address, which also includes links to each Faculty and the School of Graduate Studies: https://www.concordia.ca/conduct/academic-integrity.html" *[Undergraduate Calendar, Sec 17.10.2]*

Behaviour
All individuals participating in courses are expected to be professional and constructive throughout the course, including in their communications.

Concordia students are subject to the Code of Rights and Responsibilities which applies both when students are physically and virtually engaged in any University activity, including classes, seminars, meetings, etc. Students engaged in University activities must respect this Code when engaging with any members of the Concordia community, including faculty, staff, and students, whether such interactions are verbal or in writing, face to face or online/virtual. Failing to comply with the Code may result in charges and sanctions, as outlined in the Code.

Intellectual Property

Content belonging to instructors shared in online courses, including, but not limited to, online lectures, course notes, and video recordings of classes remain the intellectual property of the faculty member. It may not be distributed, published or broadcast, in whole or in part, without the express permission of the faculty member. Students are also forbidden to use their own means of recording any elements of an online class or lecture without express permission of the instructor. Any unauthorized sharing of course content may constitute a breach of the Academic Code of Conduct and/or the Code of Rights and Responsibilities. As specified in the Policy on Intellectual Property, the University does not claim any ownership of or interest in any student IP. All university members retain copyright over their work.

Extraordinary circumstances

In the event of extraordinary circumstances and pursuant to the Academic Regulations the University may modify the delivery, content, structure, forum, location and/or evaluation scheme. In the event of such extraordinary circumstances, students will be informed of the change.