School of Mathematics and Statistics - Carleton University
Modern Computer Algebra, Math 3819, Fall 2022

Instructor: Daniel Panario
Email: daniel@math.carleton.ca
http://www.math.carleton.ca/∼daniel

Day and time of course: Tuesdays and Thursdays 10:05-11:25. Some classes are in person, and some classes are for students to study material and to consult the professor. Material for the students to read will be distributed in advance. The schedule of the classes in person is below.

Room: lectures in person are in Southam Hall 314 (we may move the classes in person to a room in HP); the other classes (not in person) and office hours are in HP 4372.

Office hours: Tuesdays 11:35-12:25 in HP 4372.

Textbook: *Modern Computer Algebra* by Joachim von zur Gathen and Jurgen Gerhard, 3rd edition, Cambridge University Press, 2013. We also use *CryptoSchool* by Joachim von zur Gathen, Springer, 2015.

Prerequisites: MATH 2108 or MATH 3101 or MATH 2100, COMP 1005 or equivalent; or permission of the School.

Course Objective: This course is an introduction to basic algebraic algorithms that are useful for computer algebra systems and their applications. 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 and Newton iteration. Several applications to cryptography are also considered.

Evaluation: There will be two assignments and a midterm test for a total of 50% of the mark. The tentative schedule of assignments and midterm is below. You must pass the term work in order to pass the course. If you have a passing term mark (50% in total from assignments and midterm test) and you

do better in the final exam, then the final exam counts as 100% of the course.

Tutorials: if we have tutorials, there will be on Tuesdays at 17:35-18:25 in B243 Loeb Building. Tutorials should begin on September 20, 2022.

Teaching assistant: TBA.

Midterm test: There will be a midterm test on Thursday November 17, 2022, in class; the midterm test is worth 20% of the final mark.

Assignments: There will be two assignments, each worth 15% of the final mark. The first assignment will be handed-out on Tuesday September 27 and is due on Tuesday October 18. The second assignment will be handed-out on Tuesday November 1 and is due on Tuesday November 22.

Final Examination: There will be a three hour closed-book exam scheduled by the University that will take place sometime during the examination period. The exam is worth 50% of the final mark.

Withdrawal: The last day for withdrawal is November 11, 2022.

Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:

Pregnancy obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Religious obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Academic accommodations for students with disabilities: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, At-

tention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable).

Special Information for Pandemic Measures

It is important to remember that COVID is still present in Ottawa. The situation can change at any time and the risks of new variants and outbreaks are very real. There are a number of actions you can take to lower your risk and the risk you pose to those around you including being vaccinated, wearing a mask, staying home when you are sick, washing your hands and maintaining proper respiratory and cough etiquette.

Feeling sick? Remaining vigilant and not attending work or school when sick or with symptoms is critically important. If you feel ill or exhibit COVID-19 symptoms do not come to class or campus. If you feel ill or exhibit symptoms while on campus or in class, please leave campus immediately. In all situations, you must follow Carleton's symptom reporting protocols.

Masks: Carleton has paused the COVID-19 Mask Policy, but continues to strongly recommend masking when indoors, particularly if physical distancing cannot be maintained. It may become necessary to quickly reinstate the mask requirement if pandemic circumstances were to change.

Vaccines: Further, while proof of vaccination is no longer required as of May 1 to attend campus or in-person activity, it may become necessary for the University to bring back proof of vaccination requirements on short notice if the situation and public health advice changes. Students are strongly encouraged to get a full course of vaccination, including booster doses as soon as they are eligible, and submit their booster dose information in cuScreen as soon as possible. Please note that Carleton cannot guarantee that it will

be able to offer virtual or hybrid learning options for those who are unable to attend the campus.

All members of the Carleton community are required to follow requirements and guidelines regarding health and safety which may change from time to time. For the most recent information about Carleton's COVID-19 response and health and safety requirements please see the University's COVID-19 website and review the Frequently Asked Questions (FAQs). Should you have additional questions after reviewing, please contact covidinfo@carleton.ca.

Tentative lecture schedule in person classes

Class	Date	Topics
1	Sep. 13	Introduction. Addition and multiplication.
2	Sep. 20	Division and Euclidean algorithm.
3	Sep. 27	Extended Euclidean algorithm (EEA). **Assignment #1 handed out**.
4	Oct. 4	Analysis of EEA. Modular arithmetic and RSA.
5	Oct. 11	Modular inverses. Repeated squaring.
6	Oct. 18	Evaluation and interpolation. Secret sharing. **Assignment #1 handed in.**
7	Oct. 20 (Thu)	Chinese remainder theorem and algorithm.
	Oct. 24-28	**Fall break, no classes.**
8	Nov. 1	Karatsuba and Strassen algorithms. **Assignment #2 handed out.**
9	Nov. 8	Discrete Fourier transform (DFT) preparations.
10	Nov. 10 (Thu)	DFT algorithm, example and analysis.
11	Nov. 15	Fast multiplication of polynomials and DFT.
12	Nov. 17 (Thu)	**Midterm test in lecture.**
13	Nov. 22	Fast division with remainder. **Assignment #2 handed in**.
14	Dec. 8 (Thu)	Inversion using Newton iteration. Course review.

Classes not in person are are for students to study material. Unless noticed in advance, the professor will be available in HP 4372 for consultation at the time of those lectures.