Pure Math 527/627 - Computational Number Theory
Course Outline

Basic Information

Term: Fall 2012
Time: MWF 3-3:50
Location: MS 569
Instructor: David Roe
Email: roed.math@gmail.com
Office: MS 457
Phone: 403-220-3952
Office Hours: TBA
Websites: http://sage.ucalgary.ca
Blackboard: PMAT 627 L01 - (Fall 2012) - Computational Number Theory
Prerequisite: Pure Math 427 or 429

Syllabus

Sage: We will use the mathematics software Sage extensively, since it provides valuable infrastructure as well as reference implementations of many of the algorithms discussed in the course.

Complexity theory: Enough to provide a language for comparing different algorithms

Integer and polynomial arithmetic arithmetic:

- a brief discussion of fast algorithms for multiplication (Karatsuba and FFT) and division;
- the extended Euclidean algorithm for computing GCDs and inverses modulo n;
- effective Chinese remainder theorem;
- computing Jacobi symbols;

Arithmetic modulo n:

- Exponentiation by repeated squaring;
- Multiplicative orders and generators;
- Square roots;
- Algorithms for computing discrete logarithms (baby-step/giant-step, index-calculus);

Primality testing:

- Miller-Rabin test;
- Lucas-Lehmer test;
- Goldwasser-Killian test;
- Atkin-Morain test;

Factoring:

- Pollard $p-1$ algorithm;
- Elliptic curve method;
- Quadratic sieve;
- a brief discussion of the number field sieves;
- factoring polynomials modulo p;

Point counting on elliptic curves:

- Shank-Mestre;
- Schoof;

Number fields:

- Class groups of quadratic fields;
- Hilbert class polynomials;

References

We will be using two texts for this course, with a small amount of material not covered well in either. The first is available free online; the second is available for download from the library.

- V. Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge: Cambridge UP, 2008.
- R. Crandall and C. Pomerance. Prime Numbers: A Computational Perspective. Dordrecht: Springer-Verlag, 2006.

Grading and Schedule

There will be no lecture on Thanksgiving (Oct. 8) or Remembrance Day (Nov. 12). The University policy on grading and related matters is described in sections F.1 and F.2 of the online University Calendar. In determining the overall grade in the course, the following weights will be used.

Homework (40%)

There will be seven assignments during the semester (due on Sep. 21, Oct. 1, Oct. 10, Oct. 26, Nov. 9, Nov. 23, Dec. 7 at the beginning of class), with half of the problems requiring computational experimentation or the implementation of algorithms, and the other half focusing on the theory underlying these algorithms. The assignments will include 50% more problems than necessary for a full homework score: students can skip problems on each assignment to avoid problems they find difficult or they can skip an assignment completely to focus on another course that week. Conversely, doing problems beyond those required for a full score will yield bonus points at one quarter the rate. For example, if there are 150 points total on all the assignments, then getting full credit on all problems will yield a 45% contribution to the final grade, doing 120 points will yield 42%, 80 points will yield 32%.

Midterm (20%)

There will be a midterm exam in class on October 15. Calculators and computers will not be allowed, but you will be allowed one page of hand-written notes.

Final Project (40%)

Students have two options for the format of the final project:

1. A *coding project* consisting of
   (a) The implementation of a number theoretic algorithm or structure;
   (b) A short paper describing the mathematical background for the algorithm and interesting choices made in the implementation;
   (c) A presentation in class describing and demonstrating your code and the underlying mathematics.

2. An *expository project* consisting of

   (a) A longer essay describing an area of computational number theory not covered in the course, or exploring in more detail one of the topics touched upon in the lectures;

   (b) A presentation in class, either providing a broad summary of the mathematics described in the essay or giving a more focused description of one algorithm studied.

In each case an outline of the project will be due on October 31 and worth 5% of the grade, the written portion of the project will account for 85% and the in-class presentation for the final 10%. Students may choose to work on their final project either alone or in groups of two. Note that the quality of students' writing will a factor in the evaluation of the final projects: see `http://www.ucalgary.ca/pubs/calendar/current/e-2.html`.

Final Grade

The various components above will be assigned a percentage score and will be combined with the indicated weights to produce an overall percentage in the course. This percentage will be translated to a letter grade using the following table, though the instructor may choose to lower the percentage required to earn a given latter grade.

A+	98% - 105%
A	94% - 98%
A-	90% - 94%
B+	86% - 90%
B	82% - 86%
B-	78% - 82%
C+	74% - 78%
C	70% - 74%
C-	64% - 70%
D+	58% - 64%
D	52% - 58%
F	0% - 52%

Late and Missed Work

Homework assignments will be automatically submitted on the course's Sage server at the time they are due; late assignments will only be accepted with prior approval of the instructor. Similarly, if extra time is needed for the completion of the final project, students must obtain approval in advance from the instructor.

The regulations of the Faculty of Science pertaining to this matter are found in the Faculty of Science area of the Calendar in section 3.6: `http://www.ucalgary.ca/pubs/calendar/current/sc-3-6.html`. It is the student's responsibility to be familiar with these regulations. See also `http://www.ucalgary.ca/pubs/calendar/current/e-3.html`.

Collaboration and Academic Misconduct

Collaboration on homework assignments is encouraged, but solutions should be written up individually and all collaborators should be listed at the top of the assignment. The use of texts and the source code of open-source math packages is allowed on assignments (unless otherwise stated), but should be cited.

Active collaboration on the final project should be limited to the group of one or two working together. Discussions with other members of the course are permitted, but should be cited if they affect the resulting work.

Academic misconduct (cheating, plagiarism, or any other form) is a very serious offense that will be dealt with rigorously in all cases. A single offense may lead to disciplinary probation, suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under K. Student Misconduct (`http://www.ucalgary.ca/pubs/calendar/current/k.html`) to inform yourself of definitions, processes and penalties.

Other Important Information

Assembly Points

In case of an emergency during class time, the primary assembly point for the Mathematical Sciences building is the Social Science Food Court, and the secondary assembly point is the ICT food court (see `http://www.ucalgary.ca/emergencyplan/system/files/MS.png`).

Academic Accommodation Policy

Students with documentable disabilities are referred to the following links:

Students with disabilities: `http://www.ucalgary.ca/pubs/calendar/current/b-1.html`
Disability Resource Centre: `http://www.ucalgary.ca/drc/`

Safewalk

Campus Security will escort individuals day or night (`http://www.ucalgary.ca/security/safewalk/`). Call 220-5333 for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

Freedom of Information and Privacy

This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). As one consequence, students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. Since homework assignments are submitted electronically, a single name will suffice. For more information see `http://www.ucalgary.ca/secretariat/privacy`.

Student Union Information

Website: `http://www.su.ucalgary.ca/`
Vice President (Academic): 220-3911, `suvpaca@ucalgary.ca`
Science Faculty Rep: 220-3913, `sciencerep@su.ucalgary.ca`
Student Ombuds Office: `http://www.ucalgary.ca/provost/students/ombuds`

Internet and Electronic Communication Device Information

Your cell phone should be turned off in class, and communication with other individuals via laptop computers, Blackberries or other devices is not allowed during class time. If you violate this policy you may be asked to leave the classroom. Repeated abuse may result in a charge of misconduct.