Introduction to Number Theory and Cryptography Math3809A, Fall 2011

Instructor: Dr. Steven Wang, 4368HP
Tel: (613) 520 2600 (Ext. 2139)
Email: wang@math.carleton.ca
http://www.math.carleton.ca/∼wang

Lectures: Tuesday, Thursday 11:35am - 12:55pm, Paterson Hall 129

Tutorials: Friday, 10:35am - 11:25pm, TB 219

Office hours: Tuesday 10:30am-11:30am; Thursday 3:00-4:00pm.
Other time is available by appointment.

Textbook: "*Number theory with computer applications*", by R. Kumanduri and C. Romero, Prentice Hall.

Prerequisites: MATH 2108 or MATH 3101 or MATH 2100; knowledge of a computer language.

Evaluation: assignments 20%; midterm exams 20%; final exam 60%.

Midterm Exam: The midterm exam (**Oct. 27**) worths 20 marks.

Assignments: Two assignments (10 marks each). Due days: **Oct. 13 and Nov. 17**.

Final Examination: This is a three hour closed-book exam scheduled by the University and will take place sometime during the examination period (Dec. 8- Dec. 21). Students wishing to see their examination papers must make an appointment within three weeks of the examination. This privilege is for you to learn where you went wrong and is not an opportunity to argue about the marking!

Withdrawal: The last day for withdrawal from the course with a full fee adjustment is Sep. 30, 2011.

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 Student Guide. website: http://www2.carleton.ca/equity/ccms/wp-content/ccms-files/Student-Guide-card-09.pdf

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 Student Guide. website: http://www2.carleton.ca/equity/ccms/wp-content/ccms-files/Student-Guide-card-09.pdf

Students with disabilities requiring academic accommodations: in this course must register with the Paul Menton Centre for Students with Disabilities (PMC) for a formal evaluation of disability-related needs. Documented disabilities could include but are not limited to mobility/physical impairments, specific Learning Disabilities (LD), psychiatric/psychological disabilities, sensory disabilities, Attention Deficit Hyperactivity Disorder (ADHD), and chronic medical conditions. Registered PMC students are required to contact the PMC, 613-520-6608, every term to ensure that I receive your Letter of Accommodation, no later than two weeks before the first assignment is due or the first in-class test/midterm requiring accommodations. If you only require accommodations for your formally scheduled exam(s) in this course, please submit your request for accommodations to PMC by the deadlines published on PMC website. http://www1.carleton.ca/pmc/students/dates-and-deadlines

Note: There are TA opportunities within the School for future terms. Information on how to apply can be found on our School web page. In hiring undergraduate TAs, the priority shall first be given to students who have passed some of the following Honours courses: MATH 1002, 1102, 2000, 2100, STAT 2655, 2559 with grades A- or better.

Math3809 Tentative lecture schedule

Fall 2011

Weeks	Dates	Contents	Remarks
1	Sep. 8		
2	Sep. 12-16	An overview of the course, Divisibility, Primes	Sect. 2.1-2.2
3	Sep. 19-23	Unique factorization Elementary factoring methods	Sect. 2.3-2.4
4	Sep. 26-30	GCD and LCM, Linear Diophantine equations	Sect. 2.5-2.6
5	Oct. 3 - 7	Congruences, inverses mod p Chinese reminder theorem	Sect. 3.1-3.3
6	Oct. 10-14	Fermat's theorem, Euler's Phi function Euler's theorem, Lagrange's theorem	Sect. 4.1-4.4 Assign #1 due (Oct. 13)
7	Oct. 17-21	Classical cryptosystems	Sect. 5.1
8	Oct. 24-28	Public-key cryptography, RSA.	Sect. 5.2-5.3 Midterm (Oct. 27)
9	Oct. 31-Nov. 4	Pseudoprimes and Carmichel numbers Pollard's p-1 and rho factorization methods	Sect. 6.1, 6.3-6.4
10	Nov. 7-10	Order, Discrete logarithm, Lucas-Lehmer test	Sect. 7.1-7.4
11	Nov. 14-18	ElGamal cryptosystem, Signature schemes	Sect. 8.1-8.2 Assign #2 due (Nov. 17)
12	Nov. 21-25	Quadratic residues, Identification schemes	Sect. 9.1, 10.1
13	Nov.28-Dec. 2	Quadratic reciprocity law	Sect. 17.1-17.3
14	Dec. 5	Review	