(Preliminary course outline, subject to change)

MATH 3355-A, FALL 2020

Number Theory and Applications (Honours)

Instructor:
Dr. Ayse Alaca
Herzberg Laboratories Office #4376
Tel: (613) 520 2600 (Ext. 2133)
aalaca@math.carleton.ca
http://www.math.carleton.ca/~aalaca/

Textbook:
There is no required textbook for this course. Here is a list of suggested textbooks.

1. Elementary Number Theory and its Applications, by Kenneth H. Rosen, sixth edition, Addison-Wesley, 2011.
2. Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach, by William Stein, Springer, 2009.
3. A Friendly Introduction to Number Theory, by Joseph H. Silverman, fourth edition, Pearson, 2013.
4. Number Theory with Computer Applications, by Ramanujachary Kumanduri and Cristina Romero, Prentice-Hall, 1998.
5. A Classical Introduction to Modern Number Theory, by Kenneth Ireland and Michael Rosen, second edition, Springer, 1990.

Prerequisite: MATH 2100 with a grade of C- or higher; or (MATH 2108 or MATH 3101 with a grade of B- or higher; and permission of the instructor); or permission of the School.

First Lecture: Wednesday, September 9, 2020.
First tutorial class: Monday, September 21, 2020.
Last lecture and last tutorial: Friday, December 11, 2020.

	Day	Time	Room
Lectures	Monday and Wednesday	8:35--9:55 am	online via BBB
Tutorials	Monday	4:35--5:25 pm	online
My office hour	Wednesday	1:00--2:00 pm	online via BBB

During the tutorial sessions, selected problems will be solved, students' questions will be answered, and the tests will be administered.

Term tests: There will be two 50-minute tests during the regular tutorial hours on **October 19 and November 23.** No make up, early, or delayed tests.

Assignments: There will be two assignments to be submitted online on **October 5 and November 9 by 11:59 pm**. Late assignments will not be accepted.

Final examination: This is a three hour exam scheduled by the University and will take place sometime during the examination period **December 12--23**. It is the responsibility of each student to be available at the time of the examination.

Evaluation: Two tests: 40% (20% each), two assignments: 20% (10% each) and final examination 40%.

Important notes:

- Lectures will be online via BBB on cuLearn during the scheduled class times. Lecture notes will be posted on cuLearn in advance. Students are expected to study the assigned pages of the lecture notes before each class. During the online lecture times, you will have an opportunity to ask your questions. The classes are not a substitute for studying the lecture notes by yourself prior to each class.
- If you are physically in a different time zone, please email me (using your Carleton e-mail account) during the first week of classes with the details of your time zone to discuss suitable accommodation.
- Term tests, assignments and final examination will be run through cuLearn. Details will be posted on cuLearn.
- You are responsible for keeping up with information announced on cuLearn, or sent to your Carleton e-mail account.
- According to Carleton University policy under the Freedom of Information of Privacy Act (FIPPA), please use your Carleton e-mail account for all course related e-mails.
- You are responsible to make sure that your test and assignment marks are recorded correctly by visiting **cuLearn.** The deadline to make any corrections to your term marks is **December 11, 2020**.

Policies:

Class conduct: Students are expected to behave in a professional manner at all times. Disrupting a class is considered to be an Instructional Offence (see University Calendar). If a student exhibits disruptive behavior, they will be reported to the Office of the Dean, Faculty of Science.

Academic integrity: Be sure that you know the academic integrity standards at Carleton, which can be found here.

Religious obligations and/or accommodations for pregnancy: 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, see the Student Guide: Academic Accommodation.

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, Attention 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 scheduled test or exam requiring accommodation (if applicable). For the deadline to request accomodations, and for more details, visit the PMC website.

MATH 3355-A, CLASS OUTLINE for FALL 2020

WEEK	DATES	TESTS	TOPICS
~	Sept. 9	~	Integers, Greatest Common Divisor, Least Common Multiple, Euclidean Algorithm
1	Sept. 14, 16	~	Primes, Fundamental Theorem of Arithmetic
2	Sept. 21, 23	~	Congruences, Chinese Remainder Theorem, Fermat's Little Theorem
3	Sept. 28, 30	~	Primitive Roots, Discrete Logarithm, Arithmetic Functions
4	Oct. 5, 7	**Oct. 5 Assgn 1 due**	Dirichlet Product of Arithmetic Functions, The Mobious Inversion Formula
5	Oct. 14	~	Quadratic Residues, Gauss' Law of Quadratic Reciprocity
6	Oct. 19, 21	**Oct. 19 Test 1**	Primes in an Arithmetic Progression, Jacobi and Kronecker Symbols
~	**Oct. 26--30**	~	**FALL BREAK--NO CLASSES**
7	Nov. 2, 4	~	Public Key Cryptography: The RSA Public Key Cryptosystem, The ElGamal Cryptosystem
8	Nov. 9, 11	**Nov. 9 Assgn 2 due**	Pseudoprimes, Rabin-Miller Primality Test
9	Nov. 16, 18	~	Strong Pseudoprimes, Fermat Numbers, Mersenne Numbers
10	Nov. 23, 25	**Nov. 23 Test 2**	Integer Factorizations: Pollard's p-1 method, Pollard's rho method
11	Nov. 30, Dec. 2	~	Quadratic Sieve Method, Continued Fractions
12	Dec. 7, 9, 11	~	Continued Fractions, Diophantine Equations

The above class outline is subject to change depending on the progress of the course.

Last modified: September 1, 2020.