FALL 2022

MATH 3355-A Number Theory and Applications (Honours)

Instructor:
Dr. Ayse Alaca
AyseAlaca@cunet.carleton.ca

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: Thursday, September 8, 2022.
Last lecture: Thursday, December 8, 2022.

First tutorial class: Monday, September 19, 2022.
Last tutorial class: Friday, December 9, 2022 (follows Monday schedule).

	Day	Time	Room
Lectures	Tuesday and Thursday	1:00--2:30 pm	SA 313
Tutorials	Monday	12:30--1:30 pm	SA 309
My office hour	Thursday	10:00--11:00 am	online via Zoom

Term tests: There will be two 75-minute tests during the regular lecture hours on **October 20 and November 24.** No make up, early, or delayed tests. Any missing test will be counted as zero.

Assignments: There will be two assignments to be submitted online on **October 6 and November 10 by 11:59 pm Ottawa time**. Late assignments will not be accepted. Late/Missing assignments will be counted as zero.

Final examination: This is a three hour exam scheduled by the University and will take place sometime during the examination period **December 10--22**. It is the responsibility of each student to be available at the time of the examination. Please note that the exam date/time cannot be changed by the instructor.

Evaluation: Two tests: 30% (15% each), two assignments: 20% (10% each) and final examination 50% of the final grade.

To pass the course, you must satisfy the following conditions:
(i) Term mark must be at least 30%
(ii) Final exam mark must be at least 30%
(iii) Final overall grade must be at least 50% (50 points out of 100).

Important notes:

- You are responsible for keeping up with information announced in class, posted on the Brightspace course page, 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 emails.
- You are responsible for making sure that your test marks are recorded correctly by visiting **Brightspace.** The deadline to request any corrections to your term marks is **December 9.**
- Students having technical issues with Brightspace should contact the ITS service desk.

MATH 3355-A WEEKLY SCHEDULE, FALL 2022

LECTURE #	DATES	TESTS	TOPICS
1	Sept. 8	~	Integers, Greatest Common Divisor, Least Common Multiple, Euclidean Algorithm
2 & 3	Sept. 13, 15	~	Primes, Fundamental Theorem of Arithmetic
4 & 5	Sept. 20, 22	~	Congruences, Chinese Remainder Theorem, Fermat's Little Theorem
6 & 7	Sept. 27, 29	~	Primitive Roots, Discrete Logarithm, Arithmetic Functions
8 & 9	Oct. 4, 6	**Oct. 6 Assgn 1 due**	Dirichlet Product of Arithmetic Functions, The Mobious Inversion Formula
10 & 11	Oct. 11, 13	~	Quadratic Residues, Gauss' Law of Quadratic Reciprocity
12 & 13	Oct. 18, 20	**Oct. 20 Test 1**	Primes in an Arithmetic Progression, Jacobi and Kronecker Symbols
~	**Oct. 24--28**	~	**FALL BREAK--NO CLASSES**
14 & 15	Nov. 1, 3	~	Public Key Cryptography: The RSA Public Key Cryptosystem, The ElGamal Cryptosystem
16 & 17	Nov. 8, 10	**Nov. 10 Assgn 2 due**	Pseudoprimes, Rabin-Miller Primality Test
18 & 19	Nov. 15, 17	~	Strong Pseudoprimes, Fermat Numbers, Mersenne Numbers
20 & 21	Nov. 22, 24	**Nov. 24 Test 2**	Integer Factorizations: Pollard's p-1 method, Pollard's rho method
22 & 23	Nov. 29, Dec. 1	~	Quadratic Sieve Method, Continued Fractions
24 & 25	Dec. 6, 8	~	Continued Fractions, Diophantine Equations

The above weekly schedule is subject to change depending on the progress of the course.

Policies:

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 here.

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.

COVID-19: 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're 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.

Last Modified: August 30, 2022.