MATH 312: Introduction to Number Theory

Instructor: Shamil Asgarli

Summer 2021, Term 2: July 5-August 20, 2021

E-mail: sasgarli@math.ubc.edu
Office Hours: Wed 11am-12pm, Thu 4pm-5pm

Class Hours: Tue/Thu/Fri 10am-12pm
Class Hours: Wed 10am-11am

Canvas Page

All the course information, course announcements and course materials will be posted on the Canvas page. Students are also recommended to contact me using the Canvas inbox.

Course Description

The course is a gentle introduction to number theory. The subject is one of the oldest branches of mathematics with a history of more than 2300 years. We will learn about prime numbers, factorization, congruences, primitive roots, and applications of these concepts to cryptography. For example, we will prove that there are infinitely many primes, a result Euclid discovered more than two millennia ago! We will also learn how to find integer solutions to the equation $ax + by = c$, and see how this fits into the framework of Euclid's algorithm. There will be mathematical proofs in this course from the beginning to the end. You will have plenty of opportunity to practice writing proofs, which is an integral part of your learning experience in this course.

Textbook

The required textbook for the course is **Elementary Number Theory** by Kenneth Rosen. Since homework will be assigned from the textbook, it is important for the students to have the **6th edition** of the textbook. In addition to consulting the textbook, the students will also have access to the course notes.

Schedule of Topics

The following list shows the topics that we will cover in this course week by week. The reference in the parentheses indicates the relevant chapters in the textbook by Kenneth Rosen (6th edition).

1. Week 1 topics
   (a) Principle of Mathematical Induction (1.3)
   (b) Divisibility (1.5)
   (c) Primes and their properties (3.1-3.3)
   (d) Euclidean Algorithm (3.4)
   (e) Fundamental Theorem of Arithmetic (3.5)
   (f) Integer solutions to $ax + by = c$ (3.7)
2. Week 2 topics
   (a) Fundamental Theorem of Arithmetic (continued) (3.5)
   (b) Congruences (4.1)
   (c) Linear congruences (4.2)
   (d) Representation of integers in different bases (2.1)
   (e) Chinese Remainder Theorem (4.3)
3. Week 3 topics
   (a) Chinese Remainder Theorem (continued) (4.3)
   (b) Divisibility tests (5.1)
   (c) Application of congruences to error-correcting codes (5.5)
   (d) Wilson's theorem and Fermat's Little Theorem (6.1)
   (e) Pollard's factorization method (4.6)
4. Week 4 topics
   (a) Primality Testing and pseudoprimes (6.2)
   (b) Euler's theorem (6.3)
   (c) The Euler Phi-function (7.1)
   (d) Sum of divisors function (7.2)
   (e) Perfect numbers (7.3)
5. Week 5 topics
   (a) Introduction to cryptography (8.1)
   (b) Exponential ciphers (8.3)
   (c) The RSA cryptosystem (8.4)
   (d) Digital signatures (8.6)
6. Week 6 topics
   (a) Order of an integer (9.1)
   (b) Primitive roots (9.2-9.3)
   (c) Discrete Logarithms (9.4)
   (d) ElGamal Cryptosystem (10.2)

Course Structure

Lectures

Participation in class (through Zoom) is a basic expectation from students. While no formal attendance will be taken, you are strongly encouraged to attend every lecture. If students do not attend class, they are fully expected to watch the recordings on their own. Unless otherwise noted, everything discussed during the live sessions constitute testable material, even if it does not explicitly show up in the assignments.

Homework and Exams

There will be 3 homework assignments, and 3 in-class tests with dates that will be released on Canvas page. The tests will be held on Fridays of Week 2, 4, and 6. There will also be a 2.5 hour final exam for the course. For each test, there will be two sittings of the exam, one for students in North America (10:00 am PST) and for one students outside of North America (7:30 pm PST).

Important information about the exams

The three tests and the final exam will be invigilated via Zoom and it is absolutely necessary for every student to have a webcam. If a student does not have a webcam in their computer, they will not be able to complete the course.

Grading Scheme

Your final grade will be calculated according to one of the two schemes below (whichever gives the higher grade):

Grading Scheme I:

- **10%** of your grade will be determined by homework (the best 2 homework sets count).
- **60%** of your grade will be determined by in-class tests (20% for each test, all tests count)
- **30%** of your grade will be determined by the final exam.

Grading Scheme II:

- **10%** of your grade will be determined by homework (the best 2 homework sets count).
- **40%** of your grade will be determined by in-class tests (the best 2 tests count).
- **50%** of your grade will be determined by the final exam.

Given the changing circumstances around the world (COVID-19), the instructor reserves the right to change the grading scheme and the nature of the assessments at any point during the semester.

UBC's policies and resources to support student success

UBC provides resources to support student learning and to maintain healthy lifestyles but recognizes that sometimes crises arise and so there are additional resources to access including those for survivors of sexual violence. UBC values respect for the person and ideas of all members of the academic community. Harassment and discrimination are not tolerated nor is suppression of academic freedom. UBC provides appropriate accommodation for students with disabilities and for religious and cultural observances. Details of the policies and how to access support are available below:

https://senate.ubc.ca/policies-resources-support-student-success

UBC's policies for academic honesty

Academic honesty is essential to the continued functioning of the University of British Columbia as an institution of higher learning and research. All UBC students are expected to behave as honest and responsible members of an academic community. Breach of those expectations or failure to follow the appropriate policies, principles, rules, and guidelines of the University with respect to academic honesty may result in disciplinary action. It is the student's obligation to inform himself or herself of the applicable standards for academic honesty. Students must be aware that standards at the University of British Columbia may be different from those in secondary schools or at other institutions. If a student is in any doubt as to the standard of academic honesty in a particular course or assignment, then the student must consult with the instructor as soon as possible, and in no case should a student submit an assignment if the student is not clear on the relevant standard of academic honesty.