MATH 312: INTRODUCTION TO NUMBER THEORY

UBC, SUMMER TERM 2017: MAY 15 TO JUN 22

1. General Information

Instructor: Nuno Freitas

Office: Mathematics Building, room 209

e-mail: nuno@math.ubc.ca

Lecture room: Leonard S. Klinck (also known as CSCI) building, room 201

Lecture time: Tue Thu Fri 10:00-12:00 and Wed 9:30-10:30

Office hours: Tue 13:00-14:30 and Wed 10:30-12:00, LSK 300B

Website: http://www.math.ubc.ca/~nuno/math312S17.html

Textbook: K. Rosen, Elementary Number Theory, 6th edition.

2. Evaluation

Grading Scheme: Midterm 30% plus final exam 70%.

Homework: A list of suggested problems will be made available weekly. 40% of the midterm and final exam will constitute of listed problems.

Exams: All exams will be closed-book, closed-note, no calculators. You are required to be present at all examinations. Non-attendance will result in a mark of zero being recorded. No make up midterm will be given. If you must miss the midterm and you have a documented medical reason, then you may request to have the weight of the midterm transferred to the final exam.

Date for the midterm **Tuesday the 6th of June**.

The midterm will cover material up to the class of Friday 2nd of June.

3. Description

This is a first course in number theory, aimed at students who have some (but not necessarily much) experience with reading and writing proofs. Specifically, it will be assumed that students are familiar with basic techniques of mathematical proof and reasoning such as induction and proof by contradiction.

Sections of the book that we will (at least partially) be covered.

During the course, it is better to consult the course website for the most up-to-date schedule and references.

- 1.3 Induction
- 1.5. Divisibility
- 2.1. Representations of integers.
- 3.1. Prime numbers
- 3.2. The distribution of primes (only the statement of the Prime Number Theorem)
- 3.3. Greatest common divisors
- 3.4. The Euclidean algorithm
- 3.5. The fundamental theorem of arithmetic
- 3.6. Fermat Factorization only.
- 3.7. Linear Diophantine equations
- 4.1. Introduction to congruences
- 4.2. Linear congruences
- 4.3. The Chinese Remainder Theorem
- 5.1. Divisibility tests
- 5.5. Check digits (ISBN code only)
- 6.1. Wilson's Theorem and Fermat's Little Theorem
- 6.2. Pseudoprimes
- 6.3. Euler's Theorem
- 7.1. The Euler phi-function
- 7.2. The sum and number of divisors
- 7.3. Perfect numbers and Mersenne primes
- 8.1. Character ciphers
- 8.3. Exponentiation ciphers
- 8.4. Public key cryptography
- 9.1. The order of an integer and primitive roots.
- 9.2. Primitive roots for primes.
- 9.3. The existence of primitive roots.
- 9.4. Discrete logarithms and index arithmetic.

Some optional topics:

- 8.6. Cryptographic protocols and applications (digital signatures only)
- 10.2 The ElGamal cryptosystem.
- 13.1 Pythagorean Triples
- 13.2 Fermat's Last Theorem (case n=4 only)