MATH 312: INTRODUCTION TO NUMBER THEORY

UBC, WINTER 2017 TERM 1: SEP 05 TO DEC 01

1. General Information

Instructor: Nuno Freitas

Office: Mathematics Building, room 209

e-mail: nuno@math.ubc.ca

Lecture room: Chemistry building, room D300

Lecture time: Mon Wed Fri: 11:00-12:00

Office hours: Mon 12:30-14:00, Fri 9:00-10:30, room 300C LSK building

Website: http://www.math.ubc.ca/~nuno/math312W17.html

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

2. Evaluation

Grading Scheme: There will be 3 midterms from which the least score will be automatically discarded. The two top scores in the midterms will count for 20% + 20% = 40% of the final grade. Grading homework will count for 10% of the grade. The final exam will correspond to the remaining 50% of the final grade. **Attention:** Independently of your term average, you need to obtain at least 40% on the final exam to pass the course.

Homework: A list of suggested problems will be made available regularly; students will be asked to solve some of them for grading.

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.

Midterms: All the midterms will take place during class. Probable dates are: 1st midterm on **29th of Sep**, 2nd midterm **27th of Oct** and 3rd midterm **17th of Nov**.

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 will (at least partially) be covered.

During term, 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
- 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.

Depending on time availability we will also cover some of the following topics:

- 5.5. Check digits (ISBN code only)
- 8.6. Cryptographic protocols and applications (digital signatures only)
- 10.2 The ElGamal cryptosystem.
- 11.1 Quadratic residues and nonresidues
- 11.2 The Law of Quadratic reciprocity

- 11.1 The Jacobi Symbol
- 13.1 Pythagorean Triples
- 13.2 Fermat's Last Theorem (case n=4 only)