MATH 312: INTRODUCTION TO NUMBER THEORY

UBC, WINTER 2016 TERM 1: SEP 06 TO DEC 02

1. General Information

Instructor: Nuno Freitas

Office: Mathematics Building, room 209

e-mail: nuno@math.ubc.ca

Lecture room: Leonard S. Klinck building, room 460

Lecture time: Mon Wed Fri: 11:00 AM to 12:00 PM

Office hours: Mon Wed 12:30-14:00, room 300B LSK building

Website: http://www.math.ubc.ca/~nuno/math312W16.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. The final exam will correspond to the remaining 60% of the final grade.

Homework: A list of suggested problems from the textbook will be made available weekly. 20% of each 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.

Midterm: All the midterms will take place during class. Probable dates are: 1st midterm on **30th of Sep**, 2nd midterm **28th of Oct** and 3rd midterm **18th 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.

- 1.5 Divisibility;
- 3.1. Prime numbers;
- 3.2. The distribution of primes;
- 3.3. Greatest common divisors;
- 3.4. The Euclidean algorithm;
- 3.5. The fundamental theorem of arithmetic;
- 3.6. Fermat Factorization;
- 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
- 8.6. Cryptographic protocols and applications (digital signatures only)
- 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.