MATH 312: INTRODUCTION TO NUMBER THEORY

Lectures: MWF 11:00-12:00, 460 LSK
Office hours: MW 9:50-10:50 and by appointment, 300C LSK
Instructor: Laura Peskin
Instructor email: lpeskin@math.ubc.ca
Course webpage: http://www.math.ubc.ca/~lpeskin/ma312.html
Midterm exam dates: Thurs, Oct. 9 and Thurs, Nov. 6, both exams 6:30–7:30pm, 202 Macleod.
Course 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. The course has three parts, each with its own set of goals:

(1) **Divisibility, modular arithmetic, and linear systems of congruences** (weeks 1-6). Topics include the Euclidean Algorithm, Fundamental Theorem of Arithmetic, Chinese Remainder Theorem, and Hensel's Lemma. The ideas will be quite concrete and we will be able to prove almost all statements from the ground up. We'll pay careful attention to proof structure during this part, and students will get plenty of practice at writing their own proofs.

(2) **Quadratic congruences, reciprocity, and primitive roots** (weeks 6-10). Deeper exploration of the multiplicative properties of modular arithmetic, including Fermat's Little Theorem, the quadratic reciprocity law, the Euler $\phi$-function, and existence criteria for primitive roots. This part will be more abstract than the first, introducing theorems which are beautiful in their own right but which also form the seeds of modern algebraic number theory.

(3) **Applications of number theory** (weeks 10-13) After a brief introduction to the analysis of algorithms, we'll apply the ideas of the first two parts to primality testing, fast factorization, and public key cryptography.

A detailed list of topics appears at the end of this document. During the course, however, it's better to consult the course webpage (URL above) for the most up-to-date schedule and references.

**Evaluation**

**Grading scheme:** 20% weekly homeworks (12 assignments, lowest two scores dropped), 30% midterm exams (two exams, weighted equally), 50% final exam.

**Homework info:** Homework assignments are due at 11am on Wednesdays. Assignments will be posted on the course webpage (URL above) one week in advance. Homework problems will ask students to apply theorems from class to carry out calculations, and also to write their own proofs of related facts. Homework assignments are really the most important part of this course: allow yourself plenty of time to solve them carefully, and don’t get behind! Late homework will not be accepted.

**Homework collaboration policy:** Every student must write up their own solutions without looking at any other student’s written work. “Live” collaboration (i.e., discussing problems in person, without sharing written work) is allowed and encouraged. It's also fine to ask the instructor or TA for help, though you will benefit most from this if you’ve already spent some time thinking about the problem by yourself.
Homework grading: Not every assigned problem will be graded; typically two or three problems will be graded in detail, with a small number of points to be given for completing the rest of the assignment. Homework grading schemes will be posted together with solutions. The two lowest homework scores will be dropped.

Exams: All exams will be closed-book, closed-note. Sample exams will be posted in due time. Requests for make-up midterm exams will be considered only with at least three weeks’ notice and with documented academic or medical justification. If you must miss a midterm exam on shorter notice for a documented medical reason, then you may request to have the weight of that exam transferred to the final exam.

Syllabus

This syllabus may change a bit as the course progresses. See the course webpage for the most up-to-date schedule and for more specific references. All section numbers refer to the course textbook.

(1) Divisibility, modular arithmetic, and linear systems of congruences
- The division algorithm (§1.5)
- Prime numbers: infinitude, Sieve of Eratosthenes (§3.1)
- Bezout’s Theorem (§3.3)
- The Euclidean algorithm (§3.4)
- The Fundamental Theorem of Arithmetic (§3.5)
- The extended Euclidean algorithm (§3.4)
- Solvability criteria for linear Diophantine equations (§3.7)
- Congruences: definition and basic properties (§4.1)
- Representations of integers (§2.1)
- Modular exponentiation (§4.1)
- Modular inverses (§4.2)
- Chinese Remainder Theorem (§4.3)
- Hensel’s Lemma (§4.4)
- Solving linear systems of congruences (§4.5)
- Applications of congruences: divisibility tests (§5.1), and if time permits: character ciphers (§8.1), checksums (§5.4)

(2) Quadratic congruences, reciprocity, and primitive roots
- Special congruences modulo primes: Wilson’s Theorem, Fermat’s Little Theorem (§6.1)
- Euler’s criterion and Gauss’s lemma on quadratic residues (§11.1)
- Quadratic reciprocity (§11.2)
- Jacobi symbols (§11.3)
- Euler’s Theorem; Euler $\phi$-function (§6.3, §7.1)
- Multiplicative order and primitive roots (§9.1)
- Primitive roots modulo primes: Lagrange’s Theorem (§9.2)
- Existence criterion for primitive roots (§9.3)
- Discrete logarithm and index arithmetic (§9.4)
Applications of number theory

- Algorithmic efficiency and $O$-notation (§2.2)
- Primality testing using Fermat’s Little Theorem (§6.2)
- Primality testing using orders and primitive roots (§9.5)
- Factorization techniques: Pollard Rho method (§4.6), Pollard $p - 1$ method (§6.1)
- Public key cryptography: textbook RSA (§8.4), improvements, and attacks
- Public key cryptography: Diffie-Hellman key exchange (§8.6)
- Public key cryptography: Hash functions and digital signatures
- (If time permits) Pseudorandom number generation