Math 312: Introduction to Number Theory
Summer Term, 2018

Lior Silberman

v1.0 (May 9, 2018)

Course Website	`http://www.math.ubc.ca/~lior/teaching/1011/312_S11/`
Canvas site	`https://canvas.ubc.ca/courses/5511/`
Contact me at	MAT 229B — 604-827-3031 – `lior@math.ubc.ca`
My Website	`http://www.math.ubc.ca/~lior/`
Lectures	TThF 10-12, W 9:30-10:30
Office Hours	Wednesdays 9:30-11, Thursdays 12-13
Textbooks	See below
Prerequisites	(one of MATH 220, MATH 226, CPSC 121) and (9 additional credits of mathematics courses)

Note: You may buy at your option either the 5th or 6th edition of the textbook; you may buy at your option the e-book or paper version.

About the course

This course will cover basic elements of number theory:

- The integers;
- Divisibility, primes, the GCD;
- Congruences;
- Multiplicative functions;
- Cryptology;
- The multiplicative group and primitive roots.

Some applications we may consider:

- Pseudorandom numbers.
- Cryptography: how do you transmit private information across a public channel?
    1. Diffie-Hellman key exchange;
    2. The RSA cryptosystem;
    3. The El-Gamal cryptosystem.

Expectations

What you can expect from me

- Various approaches to the material including lecturing and classroom activities.
- Responses to your questions and concerns: continuously in class and during my office hours, within reasonable time by e-mail outside class.
- Demanding homework and exams.
- Timely and clear explanations of what is correct in your work and what is not, and how you can improve.

What's expected from you

- Be prepared for the course. The course is designed for students familiar with basic techniques of mathematical proof and reasoning, including proof by induction and proof by contradiction.
- Come prepared to each lecture. For every lecture, there will be assigned pre-class reading (see the schedule on the course website), and classes are designed under the assumption that you have read the relevant material in the textbook. Your main goals are to ***work through the examples*** and become ***familiar with the vocabulary and notations*** we will use, as well as think about the ***ideas*** presented.
- Actively participate in the course: do the reading, think about the material, and then ask questions.
- Submit written work that is readable and communicates your ideas. You will be expected to write logically correct and mathematically coherent proofs as part of homework and examinations.
- Ask questions when you don't understand, or want to learn more: most importantly in class but also during office hours. Also, ask your colleagues questions outside of class – both of you will benefit from the discussion!
- Working on the homework and problem sets is *absolutely essential* for learning the material. **It is extremely rare for students who miss problem sets to do well on exams.**

Special tips for a summer course (based on similar advice by Greg Martin)

- The material of the course is cumulative, and the course is really compressed. It's really hard to catch up if you fall behind!
- Remember the 2-1 rule: expect to spend *at least* 2 hours at home for every 1 hour in class – that comes to at least 14 hours per week.
- Except for pre-class reading, most of this time should be spent solving problems! Solve both the assigned homework problems and end-of-section problems from the textbook. Before each class mainly spend time reading the indicated material. After class mainly solve end-of-section exercizes; you should turn to the textbook and your notes mainly when you are stuck on a problem. The same advice applies to preparing for exams.

Official Policies

Writing

- Written work should be presented carefully, in complete English sentences, and with sufficient detail. A "correct sequence of formulas" will at best receive partial credit.
- All assertions require proof unless the problem states otherwise. No matter the operative word ("find", "solve", "establish", "calculate", "determine" ...), you must fully justify your answer.

Assessment

- Missed or late work (problem sets, midterm exams) will not be accepted for credit and will receive the grade of zero. In exceptional circumstances (a proof of the emergency and advance notification if possible will be required) the missed work will not count toward your average of that component of the course.
- There will be regular problem sets, due at the **beginning** of class on the date indicated.
  - The problems will be posted online, on the course website.
  - You are encouraged to work on solving the problems together. However, each of you must write your solutions independently, in your own words. You may (and should) share your ideas but you may not share your written work.
  - It is possible that only certain problems from a problem set will be selected for grading. Complete solutions will be posted in any case.
- There will be regular online problem sets ("WebWork")
  - Access through the course website or Canvas.
- There will be a midterm exam, most probably on Friday morning, May 27th.
  - If you need special accommodations when taking written exams, please contact the Office of Access & Diversity (`access.diversity@ubc.ca`).
  - If the midterm (or final) exam conflicts with a religious observance, please contact me *at least two weeks ahead of time* so we can make appropriate arrangements.
- There will be a final exam.
- Your course grade will be calculated as follows:

Written problem sets: 20%
Online problem sets: 10%
Midterm Exam: 20%
Final Exam: 50%

.