Syllabus for MATH 223 Number Theory
Spring 2009

Instructor Info

Instructor: Ismar Volic
Meeting times: Mondays and Thursdays, every other Wednesday, 9:50—11:00, in SCI 277
Office hours: Tuesdays 1:30—3:30, Thursdays 3—5, and by appointment; in SCI 352
Phone: 781-283-3103
Email: ivolic@wellesley.edu

Textbook, FirstClass Conference, and Webpage

Text:
- *A Friendly Introduction To Number Theory*, by J. Silverman, 3rd edition, Prentice Hall, 2005.
  This is the required textbook.
- *Elementary Number Theory*, by K. Rosen, Addison-Wesley, 2004.
  This is not a required textbook, but it is a good secondary source should you need one. It is on reserve at the Science Library. It has a good chapter on basic cryptography which I will copy and make available to you when we get to that material.

FirstClass Conference: The FirstClass conference for this course is *MATH223-01-S09*. Please add the icon to your desktop and check it often for new items. The conference will contain various important announcements, materials, and information about the course. You can also ask questions, have discussions, or arrange study groups through the conference. I will be checking the messages posted to it regularly.

Webpage: I will also post the materials for this course on my web page at http://palmer.wellesley.edu/~ivolic/classes/MATH223NumberTheorySpring09.html. This page will not contain anything that is not already on our FirstClass conference and is just meant to be a backup source of information in case you cannot access FirstClass for whatever reason.

Prerequisites and Policies

Prerequisites: MATH 116 Calculus II. Some familiarity with proofs is desired but not necessary.

Attendance: It is not required that you come to class, although it is doubtful that you will do well in the course if you miss too many lectures. If you do decide to attend, *please be on time*. If you miss a class, please copy the notes from a classmate. I will not relecture the material in my office hours, but will be happy to clear up any confusion you might still have after you have studied the notes and the textbook.

Special Arrangements: If you need special arrangements for the exams or any other aspect for the course due to religious observances or disabilities, please contact me as soon as possible. If you think you might need special arrangements, you should contact Jim Wice, the Director of Disability Services.

Calculators: Calculators will occasionally be required for some simple computations (such as multiplication of large numbers) but will not be essential for the class. The emphasis in this course will be less on computation and more on understanding the mathematics itself, and reliance on calculators can unfortunately work against this process.

Course Outline and Objectives

Since this course will heavily emphasize mathematical rigor and proofs, we will start with some basics of sets, functions, logic, and other building blocks of proper mathematical arguments (how much of this we do will depend on your background). After seeing examples of some basic proof techniques, we will begin our study of number theory. The goal is to cover the first 25 chapters of the textbook (skipping some of them), before spending a few weeks on cryptography. If there is time left, we will cover other topics from the textbook such as Diophantine approximation and

elliptic curves.

MATH 223 is a "proofs" course, which means that we will spend a lot of time developing rigorous techniques for deriving new mathematical statements from old ones. We will study what constitutes a clear, concise, original, and irrefutable mathematical argument. The more general objective of this course is thus to continue providing you with a deeper understanding and working knowledge of mathematics, while in the process strengthening your analytical skills, increasing your ability to communicate mathematics symbolically and orally, making you comfortable with reading and understanding mathematics on your own, and developing an appreciation for mathematics as one of the greatest intellectual tools that can be applied in a variety of real-life situations.

Assignments, Quizzes, Exams, and Grading

Workload: You should expect to spend 3—4 hours of studying on your own for each hour of lecture.

Homework: Homework sets will be posted on our FirstClass conference every week. You will turn in the solutions the following Friday by 5 pm and you can leave them in an envelope in the box on my door (or you can give them to me in class any time). You will be graded on the content, but also in large part on clarity and presentation, and will be expected to follow the guidelines from the document ***HWguidelines.pdf*** which can be found in the *Homework* subconference. It is very important that you keep up with the assigned work since homework counts for a large portion of your final grade. In addition, exams will be based on the homework problems. Each homework assignment will contain some problems of the sort you have not seen before (i.e. of the sort not done in class or worked out in the textbook). The reason for this is that the best measure of a good grasp of new material is an ability to apply it in new situations, and problems that look unfamiliar at first glance are meant to test this. Feel free to work on the homework assignments together, but write them up individually. Late homework will not be accepted, but you are allowed to turn in any two homework assignments *except the last one* up to one week later than the due date.

Solutions: I will do my best to provide you with the solutions to homework problems, quizzes, and exams. However, please keep in mind that I am under no obligation to do this and may in fact not have the time to do it for all the assignments and review problems. It is your responsibility to solve all the problems and are more than welcome to talk to me in office hours about them.

Quizzes: 15-minute quizzes will be given every Thursday at the end of class. They will contain 2-3 problems on the material covered in the most recent homework assignments. Each problem will count as much as a homework problem and your quiz grades will be combined with your homework grades at the end of the course. The goal of the quizzes is to give you an opportunity to practice doing problems under an exam-like time constraint and to get used to the format and style of the kind of questions you will see on the midterms and the final.

Exams: There will be two in-class midterms and a self-scheduled final exam. The midterms will be given on Thursday, March 12, and Thursday, April 23.

Makeup Exams: Please do not ask me for a postponement of an examination. I will not determine if you deserve a postponement, but I will accept your personal judgment based on the policy outlined here.

There are only two contingencies which are acceptable for the postponement of an exam: personal illness or family crisis. If either of these prevents you from taking an exam, you are entitled to take the exam at a later date. However, any illness or crisis which allows you to study for / take another exam or to prepare a paper for another course, but not this class, does not entitle you to a postponement.

If a postponement is taken, the following steps must be followed:

1. Prior to the class period at which the exam is to be given, notify me (x3103 or ivolic@wellesley.edu) or the department administrator Melanie Chamberlin (x3148) that you will not be present at the exam. This notification must be made before the actual class begins.

2. If you are eligible for a postponement, please submit to me a written statement indicating that you are acting in accord with Wellesley's Honor Code and state that the reason for your not being present at the exam is consistent with the criteria I have established. Note that you do not have to specify the reason, just that you fit the criteria. I will assume that anyone who does not notify me before a test that

she will be unable to be present is opting to take a zero for that exam. Unless the circumstances are very unusual, I will ask that you make up the exam within 3 days of the original exam date. The makeup will take place in my office*, will be an oral exam, and will not be curved.*

Extra credit lectures: For every student seminar or a colloquium you attend, you will receive 1/3 extra point on the final exam after the curve. Further, if you give a student seminar, you will receive 3 extra points on your final exam. Schedules for the seminars and colloquia can be found at
http://www.wellesley.edu/Math/activities_lectures.html
http://www.wellesley.edu/Math/activities_seminars.html

Extra credit essay: If you go to http://palmer.wellesley.edu/~ivolic/pages/reading.html, you will find a variety of short stories, essays, etc., available for download and reading. These are all in one way or another mathematically motivated. You may choose one (or more) of the writings and write a 4-5 page essay explaining and elaborating its content and the effect it has had on you (or lack thereof). The essay will be due at the end of the semester. If you are interested, we might even devote some class time to discussion of some of the writings. More details can be found in ***ExtraCreditGuidelines.pdf*** on our conference.

Grading:
20% homework and quizzes
25% each midterm
30% final

Resources

Office hours: Please take advantage of my office hours whenever you can. You do not need an appointment to come in. If you need help with the homework or material from class, if you feel that you are falling behind or that the material is consistently too difficult, or if you simply want to chat about anything, please see me. It is imperative that you talk me as soon as a problem arises so that we can fix it quickly. If you cannot make the office hours, feel free to contact me and we will arrange a time to meet. The best way to reach me is through email, although I cannot guarantee that I will reply to a message sent after 9 pm until the next morning or a message sent during the weekend until the following Monday. When communicating vie email with me or with each other, please follow the suggestions from the ***Netiquette*** handout you received when you entered Wellesley (this can also be found online).

Additional office hours: The grader for our class, Sue He, will be in the helproom every Tuesday (7—9 pm, SCI 362), so feel free to ask her questions during those times as well. She will also hold an additional office hours Wednesday evenings 7—8 pm in SCI 364.

Other materials:

- http://www.cs.sunysb.edu/~algorith/implement/pari/implement.shtml

Pari is a package for computation involving large numbers, and you can download it from this website. We will use it throughout the course, especially during the cryptography portion.

- http://www.math.niu.edu/~rusin/known-math/index/11-XX.html

This website contains a wealth of information on number theory, computation, current research, open problems, reading suggestions, various links, etc.

- *The Code Book*, by Simon Singh, Anchor Books, 2000.

A fun read on the history of cryptography.

Other resources: Variety of assistance is available to you through the Pforzheimer Learning and Teaching Center. Please visit their website at http://www.wellesley.edu/PLTC/. Your academic dean is also a good source of information and advice.

Important Dates

Friday, February 13	Last day to add
Monday, February 16	No classes (Presidents' Day)
Friday, February 27	Last day to drop. Credit/non ends
Thursday, March 12	First in-class midterm
Monday—Friday, March 23—27	No classes (spring break)

Monday, April 20	No classes (Patriot's Day)
Tuesday, April 21	Monday schedule
Thursday, April 23	Second in-class midterm
Wednesday, April 29	No classes (Ruhlman conference)
Wednesday, May 13	Last day of classes
Monday, May 18	Final exams begin
Friday, May 22	Final exams end

For a more complete list of important dates, see http://www.wellesley.edu/Registrar/0809calendar.html.