Math 4713: Number Theory

Professor: Paul Fili
E-mail: paul.fili@okstate.edu (e-mail me with questions at any time)
Lecture: MWF 12:30-1:20 in MS 509
Office: 532 Mathematical Sciences Building
Office Hours: Wed. 1:30-3:20 pm, Thurs 1:30-2:20 pm, and by appointment.
Website: We will primarily use the Online Classroom (D2L) at https://online.okstate.edu/.
Prerequisite: Math 3613.
Textbook: Elementary Number Theory: Primes, Congruences, and Secrets: A Computation Approach, by William Stein.

About this course: This course will cover modern number theory, beginning with a basic overview of primes and the fundamental theorem of arithmetic, modular arithmetic, the Chinese remainder theorem, discrete logarithms, continued fractions, and elliptic curves. We will largely follow the presentation in Stein's book, occasionally delving deeper in the lectures and the homework into some topics of particular interest. We will often be motivated by problems in cryptography, and in particular we will discuss the basics of public key cryptography.

Number theory used to be considered perhaps the “purest” area of mathematics, a subject studied purely for its own sake. The famous English number theorist G.H. Hardy said of his own work, “I have never done anything 'useful'. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.” While number theory certainly retains its pure attraction, this contention (which arguably wasn't entirely true about Hardy's own work anyway) certainly can no longer really be made about number theory today, as ideas from number theory (including many unproven conjectures and speculation) have come to play a huge role in the information age. For example, in this course we will see the basics of public key cryptography, which has enabled “secure” communication over the internet and the rise of e-commerce, and as we discuss elliptic curves we will see how these schemes can be adopted in this new setting to form what is often called “elliptic curve cryptography.” To see the importance of these ideas to our world today, one need only look at (say) an article from the technology site Ars Technica:

http://arstechnica.com/security/2013/08/crytpo-experts-issue-a-call-to-arms-to-avert-the-cryptopocalypse/

One can only imagine what will happen in the future with the advent of quantum computers, and post-quantum cryptography is itself a very active field already. This course will give students a thorough grounding in the basics of number theory and allow you to explore these issues further.

As part of this emphasis on these computational applications, we will also make use from time to time of the open-source computational software package Sage, which is available for free download from www.sagemath.org or can be run remotely on the server www.sagenb.org. You are encouraged to familiarize yourself as early as possible with the use of Sage.

Homework: There will be weekly homework in this course. ***You should expect the homework to take a significant amount of time each week.*** As some of the questions assigned might be rather difficult, I expect each of you to e-mail me, come to my office hours, and talk with each other in order to complete the homework. You are allowed (and encouraged) to collaborate on homework so long as you do not copy each other's work (i.e., you can discuss the ideas and work together to find a solution, but you must write your own solutions without looking at other students' write-ups). *Direct copying of other students' work is an academic integrity violation may result in an an F! grade for the course, so be* *sure to write up your own solutions.*

Students are encouraged to use LaTeX to typeset their homework. **A 5% bonus will be given on each typeset homework.** Templates will be provided to ease learning of LaTeX, and you can easily find answers to many basic LaTeX questions on the web. For more information on typesetting software, visit the LaTeX project at http://www.latex-project.org. You will need to download and install first a "distribution" and then download a typesetting front-end which will use that distribution. Common choices for a front-end include Texmaker (cross-platform), Kile (Linux – my personal favorite), and LyX (Mac and Linux, Windows under cygwin). LyX in particular is a WYSIWYG editor so it might be easier for first time users.

Exams: There will be two midterm exams. The first will be an hour-long in class; the second may be again in class or may be a take-home exam depending on the material covered at that point in the semester. (Perhaps I will take a vote to see what students would prefer.)

Grading: The grading for this course will be as follows:

Two midterm exams	15% each (x 2 = 30%)
Final exam	20%
Homework, quizzes, any other misc. classwork	50%

Graduate credit: You may take this course for graduate credit. You will be required to do an extra project on a topic related to this course if you do so.

Attendance: *Attendance is required for this course.* I will sometimes discuss material that is not included in the textbook. If you will be unable to attend lecture for any reason, you must contact me privately to discuss your situation. Repeated absences from lecture without excuse will receive 2% off their final grade for each of those recorded absences (thus, for example, a student with 6 recorded absences without excuse would receive 12% off their final grade).

Policy on missed work: Students will be offered reasonable accommodation in the event of a missed major assessment activity for a valid and documented reason. You will be required to notify me and provide me documentation of this reason as soon as is possible.

Syllabus Attachment: Please read the OSU syllabus attachment on the web, linked at http://academicaffairs.okstate.edu/current-students. This has a lot of important information, including instructions about disability accommodations. Please contact me privately during the first week of the course if you need accommodations as the result of a disability.