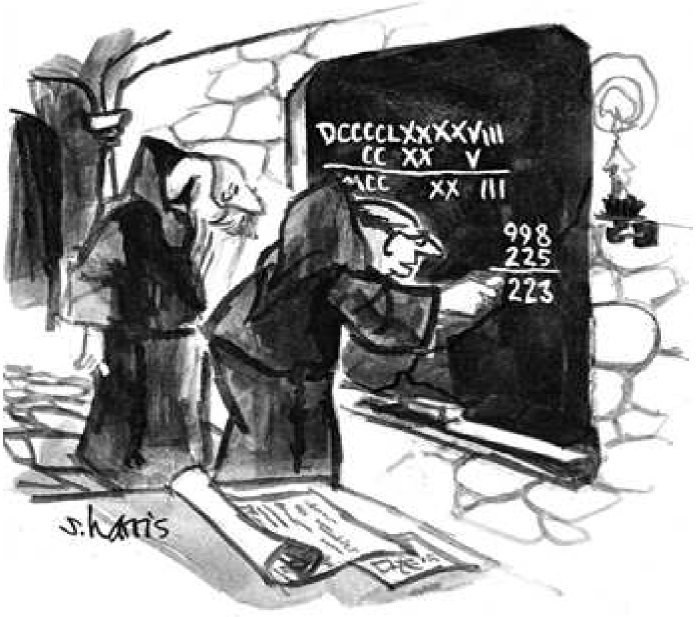
Computer Sciences 812
Arithmetic Algorithms
Spring 2024



"NOW, WITH THE NEW MATH..."

Description.

Number theory deals with the properties of the integers. Ever since the invention of computers, electronic machines have been put to use in answering research questions posed by number theorists. There are also several practical areas within computer science that make essential use of number-theoretic principles. These include computer algebra, cryptography and data security, the design of error-correcting codes, and the production of pseudo-random numbers. Aside from its obvious practical importance, this subject also uses some of the most elegant mathematics known to mankind, and has played a key role in the development of modern complexity theory.

The goal of this course is to introduce you to this area of "applied number theory." We will center attention on algorithms and their complexity analyses. You should think of the material in this course as fundamental knowledge that can be used in any of the areas mentioned in the previous paragraph.

There are many open problems, some very accessible. In the past, 812 students have used these as springboards toward (publishable) research papers.

Time/Place.

We will meet MWF 9:55-10:45, in 1221 CS.

Instructor.

Eric Bach, 4391 CS. E-mail: famous baroque composer at cs.wisc.edu. Office hours MWF 11-12 and by appointment.

Grading.

Grading will be based on occasional problem sets, and a final project (nature to be determined).

Prerequisites.

You should know the basics of abstract algebra, and “big-O” style analysis of algorithms. Math 541 and CS 400 are sufficient for this purpose. Some knowledge of probability theory will be useful for our discussion of randomized algorithms.

Style.

I will try to put the entire course on the board. Make sure you take good notes.

Homework problems will vary in difficulty, from routine problems to challenging exercises requiring creativity. Although I would be delighted if you solve them all, you need not do so to pass the course.

Office hours are a great opportunity for discussing the class material and related topics in an informal setting; please take advantage of them. I would like to see each of you during office hours at least once this semester.

E-mail to students will be sent via DoIT’s class group utility. Please check that your mail is being appropriately forwarded.

The course web page is

http://pages.cs.wisc.edu/∼cs812-1 .