Math 302 Introduction to Proofs via Number Theory Spring 2009

Instructor Amites Sarkar

Text Elementary Number Theory (6^{th} ed.)
David M. Burton

Syllabus Chapters 1–5, 7 and 10.

Overview

Number theory, the "queen of mathematics", has a long and rich history. In this course we will encounter some fundamental ideas of **Euclid** (who lived around 2300 years ago), as well more recent contributions from great mathematicians such as **Fermat**, **Euler** and **Gauss**. Fascinating work in number theory is still being done today, since there are many important unsolved problems. These include the **twin prime conjecture** (are there infinitely many pairs of primes which differ by exactly 2), **Goldbach's conjecture** (is every even number greater than 2 the sum of two primes) and the **Riemann hypothesis** (which is a bit harder to explain). Number theory also provides the mathematical basis for modern **cryptography**, some of which we shall study in this course.

This course has another purpose: to introduce you to mathematical proof. A **proof** is really just an argument which convinces somebody *very skeptical* of some fact, or **theorem**. The argument should establish the truth of the theorem beyond **all doubt** (reasonable or unreasonable).

Relation to overall program goals

Among other things, this course will (i) enhance your problem-solving skills; (ii) help you recognize that a problem can have different useful representations (graphical, numerical, or symbolic); (iii) increase your appreciation of the role of mathematics in the sciences and the real world.

Exams

Midterm 1 Friday 24 April
Midterm 2 Friday 22 May
Final Tuesday 9 June 8–10 am

Grading

The midterms are each worth 25%, and the final is worth 50%. If you feel too ill to take an exam, don't take it, but bring a doctor's certificate to me when you feel better and I will make arrangements.

Office hours

My office hours are 11–12 on Mondays, Tuesdays, Thursdays and Fridays, in 216 Bond Hall. My phone number is 650 7569 and my e-mail is amites.sarkar@wwu.edu

Course objectives

The successful student will demonstrate:

1. Understanding of the principles of mathematical induction and the ability to use them.

2. Knowledge of Pascal's rule and the binomial theorem.

3. Knowledge of the proof of the division algorithm and its application, the concepts of greatest common divisor and the euclidean algorithm, including the solution of linear diophantine equations in two variables.

4. Knowledge of the proof of the fundamental theorem of arithmetic, its application, and basic facts about prime numbers, including Euclid's theorem.

5. Competence in congruence arithmetic. This includes its use in divisibility tests, the Chinese remainder theorem, and the solution of systems of linear congruences.

6. Knowledge of Fermat's and Wilson's theorems (and proofs of both).

7. Computations involving Euler's phi-function and knowledge of Euler's generalization of Fermat's theorem (and its proof).

8. Understanding the application of the above topics to cryptography, including the ability to encode and decode simple messages using the RSA public key cryptography system.

9. Clarity and precision of thought and expression.