MATH 255: ELEMENTARY NUMBER THEORY

JOHN VOIGHT

Course Info

- *Course*: Math 255: Elementary Number Theory
- *Lectures*: Monday, Wednesday, and Friday, 10:40 a.m. – 11:30 a.m.
- *Dates*: 12 January 2009 – 29 April 2009
- *Room*: Votey 254
- *Instructor*: John Voight
- *Office*: 16 Colchester Ave, Room 207C
- *Phone*: (802) 656-2271
- *E-mail*: `jvoight@gmail.com`
- *Instructor's Office Hours*: Mondays and Wednesdays, 11:30 a.m.–1:00 p.m.; or please make an appointment!
- *Course Web Page*: `http://www.cems.uvm.edu/~voight/255/`
- *Instructor's Web Page*: `http://www.cems.uvm.edu/~voight/`

- *Prerequisites*: Math 52 or Math 54 or permission.
- *Required Text*: Kenneth Rosen, *Elementary Number Theory and its Applications*, 5th ed., Addison-Wesley, 2004. The 4th edition is essentially similar and will suffice for anyone on a budget with some effort: section numbers and the homework problems have changed.
- *Grading*: Weekly homework will count for 40% of the grade, two 50-minute midterm exams will count for 20% each, and a final paper will count for 20% in place of the final exam.
- *Final exam*: Not applicable.

Homework

There will be weekly homework assignments which are due on *Wednesdays*. Be sure to show your work and explain how you got your answer. Correct but incomplete answers will only receive partial or no credit. Write in complete sentences! On some problems, you will be allowed to use a computer and on others, you must work the problem out by hand as indicated.

Cooperation on homework is permitted (and encouraged), but if you work together write the solution up on your own. Note that there are solutions to the odd numbered exercises in the back of the text!

Syllabus

According to the "official" catalog description, we will cover:

> divisibility, prime numbers, Diophantine equations, congruence of numbers, and methods of solving congruences.

Although we may deviate from this by adding or skipping topics, the tentative plan for the course is as follows:

- **Part I**
  - **1**, 12 Jan (M): §1.1: Numbers and Sequences
  - **2**, 14 Jan (W): §1.2: Sums and Products, §1.3: Mathematical Induction
  - **3**, 16 Jan (F): §1.5: Divisibility
  - 18 Jan (M): No class, Martin Luther King Day
  - **4**, 21 Jan (W): §3.1: Prime Numbers
  - **5**, 23 Jan (F): §3.2: Distribution of Primes
  - **6**, 26 Jan (M): §3.3: Greatest Common Divisors
  - **7**, 28 Jan (W): §3.4: Euclidean Algorithm
  - **8**, 30 Jan (F): §3.5: Fundamental Theorem of Arithmetic
  - **9**, 2 Feb (M): §3.7: Linear Diophantine Equations
  - **10**, 4 Feb (W): §4.1: Introduction to Congruences
  - **11**, 6 Feb (F): §4.2: Linear Congruences
  - **12**, 9 Feb (M): §4.3: Chinese Remainder Theorem
  - **13**, 11 Feb (W): §5.1: Divisibility Tests, §5.5: Check Digits
  - **14**, 13 Feb (F): Midterm Exam #1 (covers Sections 1.1–4.3)
- **Part II**
  - 16 Feb (M): No class, President's Day
  - **15**, 18 Feb (W): §4.4: Solving Polynomial Congruences
  - **16**, 20 Feb (F): p-adic numbers
  - **17**, 23 Feb (M): §6.1: Wilson's Theorem and Fermat's Little Theorem
  - **18**, 25 Feb (W): §6.3: Euler's Theorem
  - **19**, 27 Feb (F): Group theory
  - **20**, 2 Mar (M): §7.1: Euler Phi-Function
  - **21**, 4 Mar (W): §7.1
  - **22**, 6 Mar (F): §7.2: Sum and Number of Divisors
  - 9-13 Mar (M-F): No class, Spring break
  - **23**, 16 Mar (M): §7.3: Perfect Numbers and Mersenne Primes
  - **24**, 18 Mar (W): §7.4: Möbius Inversion
  - **25**, 20 Mar (F): Odd Perfect Numbers
  - **26**, 23 Mar (M): §8.1: Character Ciphers
  - **27**, 25 Mar (W): §8.4: Public Key Cryptography
  - **28**, 27 Mar (F): Mathematica Lab (Perkins 102)
  - **29**, 27 Mar (F): §8.4
  - **30**, 30 Mar (M): §9.1: Order of an Integer and Primitive Roots
  - **31**, 1 Apr (W): §9.2: Primitive Roots for Primes
  - 3 Apr (F): No class, Lab exchange day
  - **32**, 6 Mar (M): §11.1: Quadratic Residues and Nonresidues
  - **33**, 8 Apr (W): §11.2: The Law of Quadratic Reciprocity
  - **34**, 10 Apr (F): §11.2
  - **35**, 13 Mar (M): §9.3: Existence of Primitive Roots
  - **36**, 15 Apr (W): Review
  - **37**, 17 Apr (F): Midterm Exam #2 (covers Sections 4.4–11.3)
- **Part III**
  - **38**, 20 Mar (M): §13.1: Pythagorean Triples
  - **39**, 22 Apr (W): §13.1
  - **40**, 24 Apr (F): §13.2: Fermat's Last Theorem
  - **41**, 27 Apr (M): TBD
  - **42**, 29 Apr (W): TBD