MATH 115: ELEMENTARY NUMBER THEORY

JOHN VOIGHT

Course Info

- *Course*: Math 115, Elementary Number Theory
- *Lectures*: Monday and Wednesday, 10:10 a.m.–12:00 p.m. and
  Tuesday and Thursday, 10:10 a.m.–11:00 a.m.
- *Dates*: June 21–August 13, 2004
- *Room*: 3 Evans Hall
- *Course Control Number*: 57710
- *Recitation*: Tuesday and Thursday, 11:10 a.m.–12:00 p.m.
  (You must enroll for both lecture and recitation.)
- *Course Control Number*: 57715

- *Instructor*: John Voight
- *Office*: 853 Evans
- *E-mail*: `jvoight@math.berkeley.edu`
- *Instructor's Office Hours*: Tuesday and Thursday, 1:00 - 2:30 p.m., or by appointment!
- *Course Web Page*: `http://www.math.berkeley.edu/~jvoight/115/`
- *Instructor's Web Page*: `http://www.math.berkeley.edu/~jvoight/`

- *Prerequisites*: Math 53 and Math 54
- *Required Text*: Kenneth Rosen, *Elementary Number Theory and its Applications*, 4th ed., 2000.
- *Grading*: Weekly homework will count for 30% of the grade. There will be one 50-minute midterm exam which will count for 25% of the grade and one comprehensive 110-minute final exam which will count for 45% of the grade.

Syllabus

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

> Divisibility, congruences, numerical functions, theory of primes. Topics selected: Diophantine analysis, continued fractions, partitions, quadratic fields, asymptotic distributions, additive problems.

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

(1) *Week* 1:
  - §1.1 (Numbers, sequences, and sums)
  - §1.2 (Mathematical induction)
  - §1.4 (Divisibility)
  - §3.1 (Prime numbers)
  - §3.2 (Greatest common divisor)
(2) *Week* 2:
  - §3.3 (Euclidean algorithm)
  - §3.4 (Fundamental theorem of arithmetic)
  - §4.1 (Congruences)
  - §3.6 (Linear Diophantine equations)
(3) *Week* 3:
  - §4.2 (Linear congruences)
  - §4.3 (Chinese remainder theorem)
  - §4.4 (Solving polynomial congruences)
  - §6.1 (Wilson's theorem, Fermat's little theorem)
  - §6.3 (Euler's theorem)
(4) *Week* 4:
  - §2.1 (Representations of numbers)
  - p-adic numbers
  - A bit of group theory?
  - A selection of topics from §§5.1–5.5
  - §6.2 (Pseudoprimes)
  - **Midterm exam**, Thursday, July **15**, 10:10 a.m.–11:00 a.m., covering material in Weeks 1–3
(5) *Week* 5:
  - §7.1 (Euler's ϕ-function)
  - §7.2 (Sum and number of divisors)
  - §7.3 (Perfect numbers, Mersenne primes)
  - §7.4 (Mobius inversion)
(6) *Week* 6:
  - §9.1 (Order of an integer and primitive roots)
  - §9.2 (Primitive roots for primes)
  - §9.3 (Existence of primitive roots)
  - §9.4 (Index arithmetic, discrete log)
  - §9.5 (Primality tests)
(7) *Week* 7:
  - §8.1 (Character ciphers)
  - §8.4 (RSA)
  - §4.6 (Factorization)
  - §11.1 (Quadratic residues and nonresidues)
  - §11.2 (Quadratic reciprocity)
(8) *Week* 8:
  - §11.3 (Jacobi symbol)
  - §13.1 (Pythagorean triples)
  - Quadratic forms? Elliptic curves? Fermat's last theorem?
  - **Final Exam**: Thursday, August **12**, 10:10 a.m.–12:00 p.m., covering material in Weeks 1–7

Homework

There will be weekly homework assignments which are due on *Mondays*. 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!

Cooperation on homework is permitted (and encouraged), but if you work together write the solution up on your own. We may do some of these problems together (or in groups) in class or recitation. Also note that there are solutions to the odd numbered exercises in the back of the text!

(1) *Homework* #1 (Due June 28):
- §1.1: 4, 5, 8, 9;

  1.1A: A set $S \subset \mathbb{R}$ is *well-ordered* if for every subset $T \subset S$, T has a *least element.*

  (a) Show that the sets
  $$\mathbb{Z}_{<0} = \{-1, -2, -3, \dots\}$$
  and
  $$\{1/n : n \in \mathbb{Z}_{>0}\} = \{1, 1/2, 1/3, 1/4, 1/5, \dots\}$$
  are not well-ordered.

  (b) Show that if $S \subset \mathbb{R}$ is well-ordered, then S cannot contain a decreasing sequence of distinct real numbers.
- §1.4: 6, 7, 8, 17, 18, 36, 46
- §3.1: 6, 7, 10, 11, 16;

  3.1A: Let $p_1 = 2, p_2 = 3, \dots$ be the sequence of increasing primes, so that p_n is the nth prime. Is the number $P_n = p_1 p_2 \cdots p_n + 1$ itself always prime?

  3.1B: For $x \in \mathbb{R}_{>0}$, let $s(x)$ denote the number of positive square integers not exceeding x, namely
  $$s(x) = \#\{n^2 \le x : n \in \mathbb{Z}_{>0}\}$$
  Show that $s(x) \sim \sqrt{x}$.
- §3.2: 5, 6, 8, 9, 16

(2) *Homework* #2 (Due July 6, no class Monday, July 5):
- §3.3: 1(a), 1(d), 3(a), 3(d), 9;

  3.3A: Let $f_0 = 1$, $f_1 = 1$, $f_{i+1} = f_i + f_{i-1}$ (for $i > 0$) be the sequence of Fibonacci numbers. Prove that $f_i < f_{i+2}/2$ for all $i > 0$. *[Hint: Use Theorem 3.11 or prove it directly.]*

  3.3B: Assume that the limit
  $$\alpha = \lim_{i \to \infty} \frac{f_{i+1}}{f_i}$$
  exists. Show that $\alpha = (1 + \sqrt{5})/2$. *[This explains where α comes from in Example 1.24.]*
- §3.4: 2, 4(d), 7, 10, 19–22, 39, 44, 47
- §4.1: 4, 8, 16, 17, 20, 26
- §3.6: 1(a)–(c);

  3.6A: Find all integers $x, y \in \mathbb{Z}$ for which
  $$x^2 = 4y^2 + 9.$$