The purpose of this course is to convey a modest competency and substantial willingness to think about discrete mathematical problems that most other people refuse to think about at all.


Model Solutions for Tests on …  
Wed. 27 Jan.       Wed. 10 Feb.       Wed. 3 March  
Thurs. 18 March    Mon. 26 April     Tues. 11 May, 1999

Model Solutions for Final Exam on Fri. 14 May 1999.

Titles of the Notes:
Syllabus: this lists sections of the text “covered” during Spring semester 1999.
Discussion of two problems in the text, p. 20 #26 and p. 34 #14(/).
Euclid’s GCD Algorithm (Extended, with a connection to Continued Fractions)
Fermat’s Little Theorem (with an account of RSA encryption clearer than pp. 146-8)
Enumerating Pairs of Integers (Class Project), and Rational Numbers
Coins and Stamps (General case of text’s problems exhibits a typical long proof.)
Computing $x^n$ (nontrivial example of a program’s correctness proof)
Complexity vs. Cost (about a now common abuse of language)
The Halting Problem (to clarify text pp. 181-2)
Rational Approximations of Irrationals (cf. p. 249 #17 in the text)
Some Inequalities (improves on the text’s; proves Stirling’s approximation for $n!$)
Three Problems about Combinatorial Coefficients (Some illustrate typical long proofs.)
Derangements (Neater treatment than the text’s pp. 365-8)
   Solutions to Easier Problems in H.W. Lenstra’s Notes
Waiting for a Bus (to motivate introducing the concept of Variance)
The Law of Large Numbers (and a statement of the Central Limit Theorem)
The Fragility of Improbability (in the face of small correlations; Marginal Probability)
California Super Lottery
   (Shirley Jackson’s short story The Lottery was posted during the semester but not for so long as to exceed the limitations of Fair Use or infringe the story’s copyright.)

Students are expected to read the notes and to follow their arguments (except perhaps where they involve Advanced Calculus) and to respond to questions like “Can you see why?” in the notes. Students have been told explicitly that they will not be examined on certain material in the notes, specifically Continued Fractions and long proofs, especially of the Inequalities and Stirling’s approximation for $n!$, and of the Demoivre-Laplace theorem.
Topics Covered in the Text’s Chapters 1 to 5

Ch.1: Logic
   truth tables
   functionally complete
   quantifiers

Sets
   Venn diagrams
   Union/Intersection
   Countable vs. Uncountable sets
      Programs are countable; Functions are not, so most are uncomputable.
      Language is countable; Truths are not, so most are unprovable.

Elementary series and their sums
   \[ \sum_{1 \leq i \leq n} i = n(n+1)/2, \text{ etc.} \]
Big-O notation, \( \Omega \), \( \Theta \).

Skip: 1.1 #31-33 (fuzzy logic), 1.5 #47-51 (multisets, fuzzy sets), 1.6 #59,60 (partial functions)

Ch.2: Algorithms - complexity
   prime numbers
   divisibility
   “Division algorithm” relating remainder to quotient, divisor, dividend.
   gcd, lcm
   Modular arithmetic
   Euclidean algorithm for GCD and coefficients in GCD(X, Y) = a·X + b·Y.
   Chinese remainder theorem
   Fermat’s little theorem
   One’s complement and Two’s complement binary encodings

Skip: 2.4 #32-34 (Cantor expansion), 2.5 #38-44 (quadratic res., Legendre sym.), section 2.6

Ch. 3: Rules of inference used in proofs; logical lapses to avoid.
   Halting problem
   Induction
   Recursively defined functions
   Recursive algorithms, some implementable as recurrences

Skip: 3.3 #48-66, section 3.5

Ch. 4: Counting; Sum and Product rules
   Inclusion/Exclusion Principle
   Pigeonhole Principle
   Permutations/Combinations
      Alternative proofs, like p. 295 #43-45, #49
      Two proofs for Vandermonde’s Identity
   Binomial Theorem
Probability, Conditional Probability ≠ Marginal Probability (p. 305 #40)
Independence of events
Bernoulli trials
Random variables
   independence
   expected value
   variance/covariance
Generalized permutations and combinations
   counting with repetition
   “stars and bars”

Skip: Tree diagrams (4.1), Average-case computational complexity (4.5), section 4.7
      Bayes’ formula p. 304 #41-2 though it is important for Artificial Intelligence

Ch.5: Recurrence relations ch. 5.1-5.3
   homogeneous/non-homogeneous
   finding particular solutions
   Divide-and-Conquer recurrences (read over lightly)
Generating functions ch. 5.4 (read over lightly)
   Probability Generating Functions p. 353 #57-60
Inclusion/Exclusion Ch. 5.5 … prove Theorem 1 by Induction
   Application only to Derangements in Ch. 5.6

Skip: ch. 5.1 probs. #48-62