

Math 55 — Discrete Mathematics — Spring 2003

Review Problems for 1st Midterm

First midterm exam is Thursday, Feb. 27 in the usual lecture room at the usual time. Try to arrive a few minutes early if possible, to facilitate getting everyone seated and the exams handed out.

In principle, everything from Homeworks 1–5 is fair game for the exam.

The emphasis will be on material from Chapters 2.1–2.7 of your textbook. I expect you to be able to use the concepts from Chapter 1 on logic, sets and functions as needed in context, but I will not pose problems specifically on this material (such as logic puzzles, or asking what rule of inference a deduction is based on).

Basic facts about matrices from Homework 5 are included. However, you may assume that any problem on matrices will be relatively simple, requiring only a knowledge of the basic definitions (matrix addition, multiplication, transpose).

Below is a list of review problems. They are intended to be fairly representative of the subject matter and level of difficulty you can expect from the exam problems. There will be 4 or 5 problems on the exam.

1. Give a big- O estimate of each function, using a simple function no larger than necessary.
 - (a) $f(n) = (n^2 + n \log n)(2^n + n^4)$
 - (b) $f(n) = (n^2 + n \log n)^3$.
2. Consider the following algorithm for counting the number of distinct elements in a list.

```
procedure count ( $a_1, \dots, a_n$ : list of data)
  total  $\Leftarrow$  0
  for  $i = 1, \dots, n$ 
    repeat  $\Leftarrow$  0
    for  $j = 1, \dots, i - 1$ 
      if  $a_j = a_i$ 
        repeat  $\Leftarrow$  1
    if repeat = 0
      total  $\Leftarrow$  total + 1
  return total
```

- (a) Briefly explain why the algorithm works (or why not).
 - (b) Give a big- O estimate of its time complexity.
 - (c) Devise a faster algorithm if you assume that it is possible to sort the list with time complexity $O(n \log n)$.
3. Find the greatest common divisor and least common multiple of 8918 and 1001.
 4. Find the greatest common divisor and least common multiple of $2^3 3^4 5^7 7$ and $2^7 3^5 5^3 11$.
 5. Prove that if n is a product of distinct primes, then 1 is the only perfect square that divides n .
 6. Find the largest divisor of $2^3 3^4 5^7 7^{10}$ that is a perfect square.
 7. Show that if $a \equiv b \pmod{7}$ then $10a + 15 \equiv -4b + 29 \pmod{7}$.
 8. Express $\gcd(84, 119)$ as a linear combination of 84 and 119.

9. (a) Find an inverse of 7 (mod 19).
(b) Solve $7x \equiv 13 \pmod{19}$.

10. Using $x = 8$ as the base, does the number 45 pass
(a) Fermat's test?
(b) Miller's test?

Which of the following can you conclude, based on the results of the above tests:

- 45 is prime
- 45 is composite
- not enough information to be certain?

11. Solve the system of congruences

$$x \equiv 1 \pmod{4}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

12. For the RSA public-key cryptography system with modulus $n = 31 \cdot 41$ and encryption exponent $e = 7$, find the decryption exponent d .

13. Prove that 2821 is a Carmichael number.

14. Find three positive integers m, n, p whose greatest common divisor is 1, but they are not pairwise relatively prime.

15. If

$$\mathbf{A} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

compute \mathbf{A}^2 , and give a rule for finding \mathbf{A}^n for every positive integer n .