

Math 55 — Discrete Mathematics — Spring 2003

First Midterm Exam Solutions

Problem 1. (a) Devise an algorithm to find the second-largest element in a list of n integers. Express your solution in pseudo-code.

(b) Give a big- O estimate of the time complexity of your algorithm.

One method is to scan for the position of the maximum element, then scan again for the maximum of the others.

```
procedure second-biggest ( $a_1, \dots, a_n$ : list of integers)
   $m := 1$ 
  for  $i = 2, \dots, n$ 
    if  $a_i > a_m$  then  $m := i$ 
    [at this point  $m$  is the position of the largest element]
  if  $m = 1$  then  $k := 2$  else  $k := 1$ 
  for  $i = 1, \dots, n$ 
    if  $i \neq m$  and  $a_i > a_k$  then  $k := i$ 
    [now  $k$  is the position of the largest element other than  $a_m$ ]
  return  $k$ 
```

Each scan takes $O(n)$ steps, so the total time complexity is $O(n)$.

Another method is to scan once, keeping track at every step of the two largest elements seen so far. This also has time complexity $O(n)$.

Problem 2. Solve the system of congruences

$$\begin{aligned}x &\equiv 7 \pmod{9} \\x &\equiv 3 \pmod{10}.\end{aligned}$$

The basic solutions

$$\begin{aligned}x_1 &\equiv 1 \pmod{9} & \text{and} & & x_2 &\equiv 0 \pmod{9} \\x_1 &\equiv 0 \pmod{10} & & & x_2 &\equiv 1 \pmod{10}\end{aligned}$$

are

$$x_1 \equiv 10 \pmod{90}, \quad x_2 \equiv -9 \pmod{90}.$$

Therefore

$$x \equiv 7x_1 + 3x_2 \equiv 70 - 27 \equiv 43 \pmod{90}.$$

Problem 3. Using $x = 2$ as the base, determine whether the number 41 passes

- (a) Fermat's test;
- (b) Miller's test.

What can you conclude from the results about whether or not 41 is prime (without using any other information)?

For Fermat's test we need to compute $2^{40} \pmod{41}$, while for Miller we need 2^5 , 2^{10} and $2^{20} \pmod{41}$. They are easy to compute by hand:

$$2^5 \equiv 32 \equiv -9$$

$$2^{10} \equiv 81 \equiv -1$$

$$2^{20} \equiv 1$$

$$2^{40} \equiv 1$$

Since $2^{40} \equiv 1 \pmod{41}$, the number 41 passes Fermat's test. Since -1 occurs among 2^5 , 2^{10} , and 2^{20} , it also passes Miller's test. [Technically, you could correctly answer this part of the question without computation: since 41 *is* prime, it must pass both tests.]

Although the test results suggest that 41 may be prime, they don't prove that it is. This information alone is insufficient to decide whether 41 is prime or composite.

Problem 4. If

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

compute \mathbf{A}^2 and \mathbf{A}^3 , and find a formula for \mathbf{A}^n for every positive integer n . You need not prove that your formula is correct.

$$\mathbf{A}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{A}^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}.$$

The formula suggested by the computation is

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

which is in fact correct. I didn't ask you to prove it because the right way to do that is using mathematical induction, which we haven't studied yet.