

Homework 5

CS 3233 – Fall 2003
Tom Bylander, Instructor

assigned October 9, 2003
due October 16, 2003

1. (20 pts.) Do Exercise 3.4.4.
2. (40 pts.) Do Exercise 3.4.12 using mathematical induction. Clearly display the parts of your proof (predicate, basis, induction, assume, show).
3. (20 pts.) In pseudocode, provide a fast recursive algorithm for finding $x^n \bmod m$ whenever n , x , and m are positive integers. Use the fact that:

$$x^n \bmod m = \begin{cases} x \bmod m & \text{if } n = 1 \\ (x^{n/2} \bmod m)^2 \bmod m & \text{if } n \text{ is even} \\ ((x^{n-1} \bmod m) \cdot (x \bmod m)) \bmod m & \text{otherwise} \end{cases}$$

4. (20 pts.) For your algorithm in the previous exercise, write a recurrence relation for the number of mod operations that it performs.