

## 4. Homework

Due **Monday 10/4/04** before class

1. 2.2 (page 142)

- (2 points) 10
- (3 points) Which of the functions in exercise 1 a,b,c are
  - a) in  $O(x)$ ?
  - b) in  $\Omega(x)$ ?
  - c) in  $\Theta(x)$ ?

Justify your answers.

- (2 points) 8 a,b (no formal proof needed)
- (3 points) Show that  $f(n) \in O(g(n)) \iff g(n) \in \Omega(f(n))$

2. 2.4 (page 166)

- (2 points) 8 b,c
- (2 points) 10 a,b
- (1 point) 12 e
- (1 point) 16
- (1 point) 38
- (2 points) 42

3. (2 points) Exercise 22c of Section 2.5 (on page 180)

4. (2 points) Find the inverse of 5 modulo 17. (*Hint: Solve the congruence  $x \cdot 5 \equiv 1 \pmod{17}$* )

5. Consider an RSA key set with  $p = 11, q = 29, e = 3$ .

- (a) (2 points) What value of  $d$  should be used in the secret key?
- (b) (2 points) What is the encryption of the message  $x = 100$  ?
- (c) (2 points) What is the decryption of the ciphertext  $y = 100$  ?

For parts (b) and (c) you will need to use a calculator. However, still write down intermediate steps in your computation (to justify your answer; don't just write down the final answer without any justification).