1. True or false? Indicate, why.

(a) (2 point) Sorting belongs to the complexity class P.

(b) (3 points) If a problem belongs to the complexity class NP then it cannot be solved in polynomial time.

(c) (8 points, G only) If a problem belongs to the complexity class NP ∩ coNP then it belongs to P.

2. (8 points) Give a formal definition of NP. “The language L belongs to NP if and only if . . . ” (fill in the dots). No English words allowed. Watch your quantifiers.

3. (3+3 points)

(a) Alice wants to send an encrypted message to Bob using a public-key cryptosystem. Who needs to publish a public key, Alice, or Bob? Why? Describe how the key is used.
(b) John wants to send a digitally signed message to Rachel using a public-key cryptosystem. Who needs to publish a public key, John or Rachel? Why? Describe how the key is used.

4. (6 points) State the (a) public and (b) private information a user of RSA needs to produce.

5. (a) (6 points) Describe Batcher’s Odd-Even Merge in pseudocode.

(b) (6 points) Let \( M(n) \) denote the number of parallel steps (clock beats) required by Batcher’s Odd-Even Merge. Evaluate \( M(n) \) exactly. Assume \( n = 2^k \).

6. (G only, 6 points) Solve the following problem in linear time: INPUT: a digraph. OUTPUT: either a topological sort or an odd cycle.