Problem 1

Describe an efficient algorithm that, given a set \( \{x_1, x_2, \ldots, x_n\} \) of points on the real line, determines the smallest set of unit-length closed intervals that contains all of the given points. You may assume that \( x_1 \leq x_2 \leq \ldots \leq x_n \) (i.e., that the points are given to you in sorted order). Briefly argue that your algorithm is correct.

(Hint: Think of which one of the two algorithm design techniques that we have studied is the best to use in this case.)

Problem 2

Define \( \text{lcm}(a_1, a_2, \ldots, a_n) \) to be the least common multiple of the \( n \) integers \( a_1, a_2, \ldots, a_n \), that is, the least nonnegative integer that is a multiple of each \( a_i \). Show how to compute \( \text{lcm}(a_1, a_2, \ldots, a_n) \) using the (two-argument) \( \gcd \) operation as a subroutine.

(Hint: First, write a subroutine \( \text{lcm2}(a_1, a_2) \) that computes the least common multiple of two integers, then use it to write \( \text{lcm}(a_1, a_2, \ldots, a_n) \). The “two-argument” \( \gcd \) operation refers to the plain Euclid’s algorithm that we have studied, the two-argument note there is to prevent you from inventing a \( \gcd(a_1, a_2, \ldots, a_n) \).)

Problem 3

Consider an RSA key set with \( p = 5, q = 11 \), and \( e = 7 \).

a. Why is \( 7 \) a valid choice for \( e \)?

b. What value of \( d \) should be used in the secret key? Write out all the return values in the recursion of \text{EXTENDED-EUCLID} algorithm. (Hint: \( d \) should be greater than 0.)

c. What are the public and secret keys in this system?

d. What is the encryption of message \( M = 8 \)? (Hint: Don’t forget about repeated squaring, and taking mod after each operation. Also don’t forget that you can double-check your answer by decrypting your encrypted message.)