CECS 528, Learning Outcome Assessment 4, Spring 2024, Dr. Ebert

NO NOTES, BOOKS, ELECTRONIC DEVICES, OR INTERPERSONAL COMMUNICATION ALLOWED. Submit each solution on a separate sheet of paper.

Problem

LO1. Solve the following problems.

(a) Compute the multiplicative inverse of 15 mod 38.

(b) Consider the RSA key set ($N = 77 = 7 \cdot 11, e = 7$). Determine the decryption key d.

LO2. Solve the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 10T(n/3) + n^{\log_3 10} \log^2 n$. Defend your answer.

(b) Use the substitution method to prove that, if $T(n)$ satisfies

$$T(n) = 8T(n/2) + n^3,$$

Then $T(n) = \Omega(n^3 \log n)$.

LO3. Solve each of the following problems.

(a) Recall that the `find_statistic` algorithm makes use of Quicksort's partitioning algorithm and uses a pivot that is guaranteed to have at least

$$3(\lfloor \frac{1}{2} \lceil \frac{n}{5} \rceil \rfloor - 2) \geq 3(\frac{1}{2} \cdot \frac{n}{5} - 3) = \frac{3n}{10} - 9 \geq n/4$$

members of a on both its left and right sides, assuming $n \geq 200$. Rewrite all three inequalities/equalities with updated constants, assuming that the algorithm now uses groups of 9 instead of groups of 5. Give the rationale for how you decided to replace the 3 on the left side of the very first inequality.

(b) Consider the following algorithm called `multiply` for multiplying two n-bit binary numbers x and y. In what follows, we assume n is even. Let x_L and x_R be the leftmost $n/2$ and rightmost $n/2$ bits of x respectively. Define y_L and y_R similarly. Let P_1 be the result of calling `multiply` on inputs x_L and y_L, P_2 be the result of calling `multiply` on inputs x_R and y_R, and P_3 the result of calling `multiply` on inputs $x_L + x_R$ and $y_L + y_R$. Then return the value $P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2$. Apply this algorithm to the numbers $x = 13$ and $y = 6$. Only show the top level of the recursion (i.e. do *not* make a recursion tree).

LO4. Solve each of the following problems.

(a) When performing the alternative algorithm for multiplying two polynomials, evaluating polynomial A at the n th roots of unity is essential for two reasons. Name one of them.

(b) Compute $\mathrm{DFT}_4(3, -1, 2, -4)$ using the FFT method. Show the solution to each of the subproblem instances (including the original problem instance) that must be solved. In other words, provide a recursion tree with the subproblems and provide the solution to each one.