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.

Solution.

$$38 = (15)(2) + 8$$
$$15 = (8)(1) + 7$$
$$8 = (7)(1) + 1$$

So, $8 + 7(-1) = 1 \Rightarrow 8 + (15 + 8(-1))(-1) = 1 \Rightarrow$

$8(2) + 15(-1) = 1 \Rightarrow (38 + 15(-2))(2) + 15(-1) = 1$

$\Rightarrow (38)(2) + 15(-5) = 1 \Rightarrow (15)(-5) \equiv 1 \bmod 38$

$\Rightarrow 15^{-1} \equiv -5 \bmod 38$

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

Solution. $(p-1)(q-1) = (6)(10) = 60$

$$60 = (7)(8) + 4$$
$$7 = (4)(1) + 3$$
$$4 = (3)(1) + 1 \Rightarrow 4 + 3(-1) = 1 \Rightarrow$$

$4 + (7 + 4(-1))(-1) = 1 \Rightarrow 4(2) + 7(-1) = 1$

$\Rightarrow (60 + (7)(-8))(2) + 7(-1) = 1 \Rightarrow$

$60(2) + 7(-17) = 1 \Rightarrow 7^{-1} \equiv d \equiv -17 \bmod 60$

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.

Solution.

By Case 4 of M.T.

$T(n) = \Theta(n^{\log_3 10} \cdot \log^3 n)$

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

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

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

Inductive assumption:

Solution. $T(k) \geq ck^3 \log k$ for all $k < n$.

Show $T(n) \geq cn^3 \log n$.

$T(n) = 8T(n/2) + n^3 \geq 8c\left(\frac{n}{2}\right)^3 \log\left(\frac{n}{2}\right) + n^3 =$

$cn^3(\log n - 1) + n^3 \geq cn^3 \log n \iff$

$cn^3 \leq n^3 \iff c \leq 1$ ✓

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.

Solution.

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

$\frac{5n}{18} - 15 \geq \frac{n}{4} \iff \frac{5n}{18} - \frac{n}{4} \geq 15$

$\frac{10n}{36} - \frac{9n}{36} \geq 15 \iff n \geq (36)(15) = 540.$

3 is replaced by 5 since the pivot M, if $\geq$ median M' from a group of 9, will also be $\geq$ 4 other members of the group, for a total of $4+1=5$. The same holds if $M \leq M'$ for some group.

(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).

Solution. $x = \underbrace{\boxed{1\ 1}}_{x_L}\underbrace{\boxed{0\ 1}}_{x_R}$ $\quad y = \underbrace{\boxed{0\ 1}}_{y_L}\underbrace{\boxed{1\ 0}}_{y_R}$

$P_1 = 3 \quad P_2 = 2 \quad P_3 = (4)(3) = 12$

$xy = P_1 \cdot 2^4 + (P_3 - P_2 - P_1) \cdot 2^2 + P_2 =$

$(3)(16) + (12-3-2)(4) + 2 = 48 + 28 + 2$

$= 78$

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.

Solution. When evaluating the subproblem polynomials A_e and A_o at x^2, for each n^{th} root unity, it is equivalent to evaluating A_e and A_o at the $n/2$ roots of unity, and so the two subproblems are 1/2 the size of original

(b) Compute $\text{DFT}_4(3, -1, 2, -4)$ 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.

Solution.

$\text{DFT}_4(3,-1,2,-4) = (5,1,5,1) + (1,i,-1,-i) \odot (-5,3,-5,3) = \boxed{(0, 1+3i, 10, 1-3i)}$

$\text{DFT}_2(3,2) = (3,3) + (1,-1) \odot (2,2) = \boxed{(5,1)}$

$\text{DFT}_2(-1,-4) = (-1,-1) + (1,-1) \odot (-4,-4) = \boxed{(-5,3)}$

$\text{DFT}_1(3) = 3$ $\text{DFT}_1(2) = 2$

$\text{DFT}_1(-1) = -1$ $\text{DFT}_1(-4) = -4$