CECS 528, Learning Outcome Assessment 4, Yellow, Fall 2023, 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) Evaluate $2^{2^{2023}}$ mod 3.

Solution. We have

$$2^{2^{2023}} \equiv (2^2)^{2^{2022}} \equiv 4^{2^{2022}} \equiv 1^{2^{2022}} \equiv 1 \bmod 3.$$

(b) Consider the RSA key set $(N = 91 = 7 \cdot 13, e = 11)$. Determine the decryption key d.

Solution. We must determine the multiplicative inverse of 11, mod $(7-1)(13-1) = 72$. Moreover, since

$$72 = 11(6) + 6,$$

$$11 = 6(1) + 5,$$

and

$$6 = 5(1) + 1.$$

Combining these equations, we obtain the linear combination

$$72(2) + 11(-13) = 1$$

and so -13 is the multiplicative inverse of 11, mod 72.

LO2. Solve the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 9T(n/3) + n^{\log_4 16} \log^3 n$. Defend your answer.

Solution. By Case 4 of the Master Theorem, $T(n) = \Theta(n^2 \log^4 n)$.

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

$$T(n) = 4T(n/2) + n \log n$$

then $T(n) = \Omega(n^2)$.

Solution. Inductive assumption: $T(k) \geq Ck^2$ for all $k < n$ and some constant $C > 0$. Then

$$T(n) = 4T(n/2) + n \log n \geq 4C(n/2)^2 + n \log n = Cn^2 + n \log n \geq Cn^2 \Leftrightarrow$$

$$n \log n \geq 0,$$

which is true for any $n \geq 1$. Therefore, for *any* constant $C > 0$, $T(n) \geq Cn^2$, for all $n \geq 1$. Therefore, $T(n) = \Omega(n^2)$.

LO3. Solve each of the following problems.

(a) Recall that the `Find-Statistic` algorithm makes use of the Partitioning algorithm and uses a pivot that is guaranteed to have at least

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

members of array a both to its left and to its right. Rewrite the above inequalities but now assuming the algorithm uses groups of 13 instead of groups of five. Explain your reasoning for each of the numerical changes that you make.

Solution. Replace the 5 with 13 since now the groups have size thirteen. Also, replace the 3 with 7 since every group has at least seven members that are greater than or equal to (respectively, less than or equal to) the chosen pivot (i.e. median of medians). Thus we have

$$7(\lfloor \frac{1}{2} \lceil \frac{n}{13} \rceil \rfloor - 2) \geq 7(\frac{1}{2} \cdot \frac{n}{13} - 3) = \frac{7n}{26} - 21.$$

(b) Demonstrate the partitioning step of Hoare's version of `Quicksort` for the array

$$a = 4, 8, 1, 6, 2, 7, 5, 3, 9, 11, 10$$

where we assume that the pivot equals the median of the first, last, and middle integers of a.

Solution. The pivot equals $M = \text{median}(4, 7, 10) = 7$. After swapping $M = 7$ with 10 and swapping wrong-sided array members, we arrive at $a_{\text{left}} = 4, 3, 1, 6, 2, 5$ and $a_{\text{right}} = 8, 9, 11, 10$.

LO4. Solve each of the following problems.

(a) For n even, state the two properties of the n th roots of unity that allow for a degree-$(n-1)$ polynomial to be recursively evaluated at each of the n th roots of unity in a log-linear number of steps. Hint: you do *not* need to justify your answer. Just state the properties.

Solution. the n th roots of unity come in additive inverse pairs. This is important since the number of distinct squares one obtains when squaring each root is equal to $n/2$. Also, the $n/2$ squares of the n th roots of unity equal exactly the $n/2$ roots of unity, which allows for a recursive algorithm.

(b) Compute $\mathrm{DFT}_4^{-1}(4,-1,0,5)$ using the FFT method. Show the solution to each of the subproblem instances (including the original problem instance) that must be solved.

Solution. $\mathrm{DFT}_1^{-1}(4) = 4$, $\mathrm{DFT}_1^{-1}(-1) = -1$, $\mathrm{DFT}_1^{-1}(0) = 0$, $\mathrm{DFT}_1^{-1}(5) = 5$. Also,

$$\mathrm{DFT}_2^{-1}(4,0) = \frac{1}{2}[(4,4) + (1,-1) \odot (0,0) = (2,2)]$$

and

$$\mathrm{DFT}_2^{-1}(-1,5) = \frac{1}{2}[(-1,-1) + (1,-1) \odot (5,5) = (2,-3)].$$

Finally,

$$\mathrm{DFT}_4^{-1}(4,-1,0,5) = \frac{1}{2}[(2,2,2,2) + (1,-i,-1,i) \odot (2,-3,2,-3)] = (2, 1+3i/2, 0, 1-3i/2).$$