CECS 528, Exam 1, Spring 2024, Dr. Ebert

Problems

1. Solve each of the following problems. Note: correctly solving these problems counts for passing LO1.

   a. Evaluate $5^{40} \bmod 17$ without the help of a calculator. (10 pts)

   Solution. $5^2 \equiv 8 = 2^3 \bmod 17 \Rightarrow$

   $5^{40} \equiv (5^2)^{20} \equiv (2^3)^{20} \equiv 2^{60} \bmod 17$.

   But $2^4 \equiv -1 \bmod 17$ and so $5^{40} \equiv (-1)^{15} \equiv \boxed{-1} \bmod 17$

   b. In the Strassen-Solovay test, is 8 a witness or accomplice for $n = 15$? Show work in computing both the left and right sides of the mod-15 congruence. (15 pts)

   Solution. $8^{\frac{15-1}{2}} \equiv 8^7 \equiv 2^{21} \bmod 15$.

   Also, $2^4 \equiv 1 \bmod 15$. Thus $2^{21} \equiv 2 \bmod 15$.

   Also, $\left(\frac{8}{15}\right) = \left(\frac{2}{15}\right)^3 = 1$ since $15 \equiv -1 \bmod 8$.

   $\therefore$ $8^7 \not\equiv \left(\frac{8}{15}\right) \bmod 15$ since $2 \not\equiv 1 \bmod 15$. 8 is a witness.

2. Solve each of the following problems. Note: correctly solving these problems counts for passing LO2.

   a. Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 4T(n/2) + n^{\log_3 10} \log^2 n$. (10 pts)

   Solution. By Case 3 of the Master Theorem and the fact that $n^{\log_2 4} = n^2$ and $f(n) = \Omega(n^{2+\delta})$ for some $\delta > 0$, $T(n) = \Theta(n^{\log_3 10} \log^2 n)$.

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

   $$T(n) = 4T(n/2) + n^2,$$

   Then $T(n) = O(n^2 \log n)$. (15 pts)

   Inductive Step. Assume $T(k) \le ck^2 \log k$ for some $c > 0$ and all $k < n$.

Show $T(n) \le cn^2 \log n$.

Solution.

$$T(n) = 4T(n/2) + n^2 \le 4c\left(\frac{n}{2}\right)^2 \log\left(\frac{n}{2}\right) + n^2 =$$

$$cn^2 \log n - cn^2 + n^2 \le cn^2 \log n \iff$$

$$cn^2 \ge n^2 \iff c \ge 1.$$

3. Solve each of the following problems. Note: correctly solving these problems counts for passing LO3.

   a. 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 $P_1 \times 2^n + (P_3 - P_1 - P_2) \times 2^{n/2} + P_2$. Prove that the returned value does in fact equal xy. (15 pts)

      Solution. See solution to Exercise 26 of the Divide and Conquer lecture.

   b. Use Strassen's products $P_1 = a(f-h) = af - ah$, $P_2 = (a+b)h = ah + bh$, $P_3 = (c+d)e = ce + de$, $P_4 = d(g-e) = dg - de$, $P_5 = (a+d)(e+h) = ae + ah + de + dh$, $P_6 = (b-d)(g+h) = bg + bh - dg - dh$, $P_7 = (a-c)(e+f) = ae - ce - cf + af$. to compute the matrix product

$$\begin{array}{cc} a & b \\ & \\ c & d \end{array} \quad \begin{pmatrix} 1 & -3 \\ -4 & 5 \end{pmatrix}\begin{pmatrix} 3 & -1 \\ 2 & 4 \end{pmatrix} \quad \begin{array}{cc} e & f \\ & \\ g & h \end{array}$$

$P_1 = 1(-5) = -5$

$P_2 = (-2)(4) = -8$

$P_3 = (1)(3) = 3$

$P_4 = (5)(-1) = -5$

$P_5 = (6)(7) = 42$

$P_6 = (-8)(6) = -48$

$P_7 = (5)(2) = 10$

Show all work. (10 pts)

Solution.

$r = P_5 + P_6 - P_2 + P_4 = 3$

$s = P_1 + P_2 = -13$

$t = P_3 + P_4 = -2$

$u = -P_7 + P_5 + P_1 - P_3 = 24$

4. Recall that, for integers a, b, and c, $(a, b) \mid c$ iff there exist integer constants x and y for which

$$ax + by = c.$$

Use this fact to prove the following.

a. If the equation

$$ax \equiv b \bmod m$$

has a solution, then $(a, m) \mid b$. (12 pts)

Solution. $ax \equiv b$ mod m $\Rightarrow$ there is a K for which $ax - b = mK$ and

$ax - mK = b$ $\Rightarrow$ b is a linear combination of a and m and so $(a,m) \mid b$.

b. If $(a, m) \mid b$, then the equation

$$ax \equiv b \bmod m$$

has a solution. (13 pts)

Solution. If $(a,m) \mid b$, then $b = ax + my$ for some integers x and y, which implies $m(-y) = ax - b$ $\Rightarrow$ $ax \equiv b$ mod m and so $ax \equiv b$ mod m has a solution.

5. Show how to multiply the complex numbers $a + bi$ and $c + di$ using only three multiplications of real numbers. The algorithm should take a, b, c, and d as input, and produce the real component $ac - bd$ and imaginary component $ad + bc$. Note that the straightforward approach requires four multiplications. We seek a more clever approach. (25 pts)

Solution. The products are ad, bc, and $(a + b)(c - d) = ac - bd + bc - bd$.

6. Given an array a of n positive integers, the maximum window area (MWA) of a is defined as the maximum of

$$(j - i + 1) \min_{i \le k \le j} (a[k]),$$

taken over all combinations i and j for which $0 \le i \le j \le n - 1$. For example if $a = 3, 3, 1, 7, 4, 2, 4, 6, 1$, then $\mathrm{MWA}(a) = 10$ via $i = 3$ and $j = 7$, since the minimum value in this range is $a[5] = 2$, and $(7 - 3 + 1)(2) = 10$. One algorithm for finding MWA(a) is to consider all n^2 possible combinations of i and j and keep track of the combination that produces the maximum window area. But this algorithm has quadratic running time.

a. Describe a divide-and-conquer algorithm that achieves an improved running time. Clearly define the steps of your algorithm. Use any results from the Recurrences lecture to analyze its running time. (15 pts)

Solution. For the base case, if $|a| = 1$, then MWA(a) $= a[0]$. For the recursive case, divide a into two roughly equal halves a_l and a_r and make recursive calls on the algorithm to obtain MWA(a_l) and MWA(a_r). We must also compute the maximum area of any window that overlaps the boundary between a_l and a_r. We assume the last element of a_l is $n/2 - 1$. Initialize two indices $i = n/2 - 1$ and $j = n/2$ to start at the end of a_l and beginning of a_r, respectively. Initialize $h_{\min} = \min(a[n/2 - 1], a[n/2])$ and

$$\mathrm{MWA}_{\mathrm{mid}} = 2h_{\min}.$$

Then while either $i \geq 0$ or $j < n$, either decrement i or increment j depending on which of $a[i]$ or $a[j]$ is larger (breaking ties by decrementing i). If, say, $a[i]$ is the larger, then update $h_{\min}$ as $h_{\min} = \min(h_{\min}, a[i])$, and update $\mathrm{MWA}_{\mathrm{mid}}$ as

$$\mathrm{MWA}_{\mathrm{mid}} = \min(\mathrm{MWA}_{\mathrm{mid}}, (a[j] - a[i] + 1 - \mathrm{offset}_j + \mathrm{offset}_i)h_{\min}),$$

where, e.g. offset_j is 1 if j is out of bounds, and 0 otherwise. Finally, return the minimum of $\mathrm{MWA}_{\mathrm{mid}}$, MWA($a_l$), and MWA($a_r$).
This algorithm satisfies the recurrence

$$T(n) = 2T(n/2) + n$$

since $\mathrm{MWA}_{\mathrm{mid}}$ is computed in $\mathrm{O}(n)$ steps. Thus, by Case 2 of the Master Theorem, $T(n) = \Theta(n \log n)$.

a_l a_r optimal

b. Demonstrate your algorithm on the array $a = [2, 6, 3, 7, 5, 4, 6, 2, 1, 7]$ for the top level of recursion only. For example, if your algorithm makes two recursive calls, then (without working through the algorithm) provide their solutions and show the steps of the combine portion of the algorithm working at the top level. (10 pts)

MWA(a_l) = 3·4 = 12 , MWA(a_r) = 2·4 = 8

6, 3, 7, 5 4, 6

For Computing $\mathrm{MWA}_{\mathrm{mid}}$ we use the following Table

Step	i	j	$\mathrm{MWA}_{\mathrm{mid}}$	$h_{\min}$
0	4	5	8	4
1	3	5	12	4
2	3	6	16	4
3	2	6	16	3
4	1	6	18	3
5	0	6	18	2

The final $\mathrm{MWA}_{\mathrm{mid}}$ is 18 which is the solution to the problem. Window begins at a[1] and ends at a[6]