CECS 528, Learning Outcome Assessment 2, Pink, Fall 2023, Dr. Ebert

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

Problems

LO1. Complete the following problems.

(a) Compute the Jacobi symbol $\left(\frac{7}{143}\right)$. Hint: $143 = 13 \times 11$.

(b) Consider the RSA key set $(N = 65 = 5 \cdot 13, e = 11)$. Determine the decryption key d.

LO2. Complete the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 10T(n/3) + n^2$.

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

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

Then $T(n) = \Omega(n \log n)$. Hint: remember to state the inductive assumption.

Solutions

LO1. Complete the following problems.

(a) Compute the Jacobi symbol $\left(\frac{7}{143}\right)$. Hint: $143 = 13 \times 11$.

Solution.

$$= \frac{7}{13} \times \frac{7}{11}$$

$$= \frac{13}{7} \times (-1) \times \frac{11}{7}$$

$$= \left(\frac{6+7}{7}\right)(-1)\left(\frac{7+4}{7}\right)$$

$$= \left(\frac{6}{7}\right)(-1)\left(\frac{4}{7}\right)$$

$$= (-1)\left(\frac{7-1}{7}\right)\left(\cancel{\frac{2}{7} \times \frac{2}{7}}\right) \quad 1$$

$$= (-1)\left(\frac{-1}{7}\right) 1^2$$

$$= (-1)(-1)$$

$$= 1$$

(b) Consider the RSA key set $(N = 65 = 5 \cdot 13, e = 11)$. Determine the decryption key d.

Solution.

$(p-1)(q-1) = 48$

$ed \equiv 1 \bmod 48$

$11d \equiv 1 \bmod 48$

$48 = 11(4) + 4$

$11 = 4(2) + 3$

$4 = 3(1) + 1$

$1 = 4 - 3(1)$

$= 4 - (11 - 4(2))$

$= 4(3) - 11$

$= [48 - 11(4)]3 - 11$

$= 48(3) - 11(13)$

$d = -13 \quad \because d \neq -13 \quad d = -13 + 48$

$= 35$

LO2. Complete the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 10T(n/3) + n^2$.

Solution. $n^{\log_3 a} = n^{\log_3 10}$ $\quad n^{\log_3 10} > n^2$

$\therefore f(n) = O(n^{\log_b a - \epsilon})$

$\epsilon = \log_3 10 - 2$

$\therefore T(n) = \Theta(n^{\log_3 10})$

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

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

Then $T(n) = \Omega(n \log n)$. Hint: remember to state the inductive assumption.

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

$c\left(\frac{2n}{3}\right)\log\frac{2n}{3} + \frac{cn}{3}\log\frac{n}{3} + n \geq cn\log n$

$\frac{2cn}{3}(\log 2n - \log 3) + \frac{cn}{3}(\log n - \log 3) + n \geq cn \log n$

$\frac{2cn}{3}(\log 2 + \log n - \log 3) + \frac{cn}{3}(\log n - \log 3) + n \geq cn\log n$ $\quad 1$

$\frac{2cn}{3} + \frac{2cn\log n}{3} - \frac{2cn\log 3}{3} + \frac{cn\log n}{3} - \frac{cn\log 3}{n} + n \geq cn\log n$

$\frac{2cn}{3} + \frac{3cn\log n}{3} - \frac{3cn\log 3}{3} + n \geq cn\log n$

$\frac{2cn}{3} + cn\log n - cn\log 3 + n \geq cn\log n$

$\frac{2cn}{3} + n \geq cn\log 3$

$\frac{2c}{3} + 1 \geq c\log 3$

$\frac{2c}{3} - c\log 3 \geq -1$

$c\left(\frac{2 - 3\log 3}{3}\right) \geq -1$

$c \geq -\frac{1(3)}{2 - 3(\log 3)}$