CECS 528, Learning Outcome Assessment 2, Yellow, 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) Evaluate $(3^{30} + 2^{20}) \bmod 5$. Show work.

(b) Consider the RSA key set $(N = 77 = 7 \cdot 11, e = 7)$. 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 $T(n) = 9T(n/3) + n^{2.1}$.

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

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

Then $T(n) = \mathrm{O}(n^2 \log n)$. Hint: remember to state the inductive assumption.

Solutions

LO1. Complete the following problems.

(a) Evaluate $(3^{30} + 2^{20}) \bmod 5$. Show work.
Solution. We have, $3^4 \equiv 1 \bmod 5$, and so

$$3^{30} \equiv (3^4)^7 \cdot 3^2 \equiv 9 \equiv 4 \bmod 5.$$

Also, $2^4 \equiv 1 \bmod 5$ and thus the same is true for $2^{20} = (2^4)^5$. Therefore, $(3^{30} + 2^{20}) \equiv (4+1) \equiv 0 \bmod 5$.

(b) Consider the RSA key set $(N = 77 = 7 \cdot 11, e = 7)$. Determine the decryption key d.
Solution. d is the multiplicative inverse of $e = 7$ modulo $m = (7-1)(11-1) = 60$. Thus, after applying Euclid's algorithm both forward and reverse, we have that $d = 43$.

LO2. Complete the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 9T(n/3) + n^{2.1}$.
Solution.
By Case 3, $T(n) = \Theta(n^{2.1})$.

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

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

Then $T(n) = \mathrm{O}(n^2 \log n)$. Hint: remember to state the inductive assumption.
Solution. Assume, $T(k) \leq Ck^2 \log k$ for all $k < n$ and for some constant $C > 0$. Show, $T(n) \leq Cn^2 \log n$. We have

$$T(n) \leq 4C(\frac{n}{2})^2 \log(\frac{n}{2}) + n^2 = Cn^2(\log n - 1) + n^2 = Cn^2 \log n - Cn^2 + n^2$$

$$\leq Cn^2 \log n \Leftrightarrow Cn^2 \geq n^2 \Leftrightarrow C \geq 1.$$