NAME | STUDENT NUMBER

TOTAL MARKS: 50
TOTAL TIME: 50 minutes

Problem 1: **[10 pts]** Use the definition of "$f(x)$ is $O(g(x))$" to prove the following statements.

a) $2x^2 + 3x - 1$ is $O(x^2)$.

SOLUTION:
We are looking for witnesses C and k satisfying

$$2x^2 + 3x - 1 \le Cx^2, \ \forall x \ge k$$

Clearly $2x^2 \le 2x^2$ for $x \ge 1$. Also, $3x - 1 \le 3x \le x^2$ for $x \ge 3$. Adding the last two inequalities, it follows that

$$2x^2 + 3x - 1 \le 3x^2, \ \forall x \ge 3.$$

b) $2x^2$ is NOT $O(x)$.

SOLUTION:
Assume, by contradiction, that $2x^2$ is $O(x)$. Then, there exist constants C and k satisfying:

$$\begin{aligned} & 2x^2 \le Cx, \ \forall x \ge k. \\ \rightarrow \ & 2x \le C, \ \forall x \ge \max\{k, 0\} \\ \rightarrow \ & x \le \frac{C}{2}, \ \forall x \ge \max\{k, 0\}, \end{aligned}$$

a contradiction.

Problem 2: **[8 pts]** Given below is a table of big-O estimates for some basic functions, where ϵ, a, b are constant values. Using this table and the sum and product rules, find a simple function $g(n)$ of smallest order satisfying the statement "$f(n)$ is $O(g(n))$" for the following functions.

$\log n$ is $O(n^\epsilon)$ if $\epsilon > 0$	n^a is $O(n^b)$ if $a \le b$	n is $O(a^n)$ if $a > 1$
a^n is $O(n^n)$ for any $a > 1$	$n!$ is $O(n^n)$	

a) $f(n) = n \log n + 3n^2 + 2n$.

SOLUTION:
$g(n) = n^2$.

b) $f(n) = (n^3 + 2n^2 \log n)(1 + \log n) + 12n^2(n + \log n)$

SOLUTION:
$g(n) = n^3 \log n$ or $g(n) = n^{3+\epsilon}$, for $\epsilon > 0$.

c) $f(n) = n + 2^n + n!$.

SOLUTION:
$g(n) = n^n$

d) $f(n) = n \log(n^2 + 2n + 1)$.

SOLUTION:
$g(n) = n \log n$ or $g(n) = n^{1+\epsilon}$.

Problem 3: **[8 pts]** Are the following statements true or false? Use the definition to explain your answer.

a) $17 \equiv 3 \pmod 5$.

SOLUTION:
False, because 5 does not divide $17 - 3 = 14$

b) $99 \mod 5 = 4$.

SOLUTION:
True, because by integer division $99 = 5 \cdot 19 + 4$.

c) $-12 \equiv 0 \pmod 6$.

SOLUTION:
True because $6|(-12 - 0)$.

d) $27 \mod 13 = 14$.

SOLUTION:
False, because the remainder of the division to 13 must be less than 13.

Problem 4: **[6 pts]** Use Fermat's Little Theorem to compute $7^{4803} \mod 13$. Show your work. (*Recall Fermat's Little Theorem: if p is prime, then $a^{p-1} \equiv 1 \pmod p$ for all $1 \le a \le p - 1$*)

SOLUTION:
Since 13 is prime, using Fermat's Little Theorem we get $7^{12} \equiv 1 \pmod{13}$. Since $4803 = 4800 + 3 = 12 \cdot 400 + 3$, it follows that $7^{4803} \equiv 7^{12 \cdot 400 + 3} \equiv 7^3 \pmod{13}$. Since $7^2 \equiv 49 \equiv 10 \pmod{13}$, it follows that $7^3 \equiv 7^2 \cdot 7 \equiv 10 \cdot 7 \equiv 5 \pmod{13}$.

Problem 5: **[12 pts]** RSA decryption: let $p = 13$, $q = 7$ be two prime numbers. Let $N = pq = 91$ and $(p - 1)(q - 1) = 72$. Suppose that you receive a message encrypted using exponent $e = 35$ whose encrypted value is $y = 77$.

a) Verify that $e = 35$ has an inverse modulo $(p-1)(q-1) = 72$.

SOLUTION:
Observe that $35 = 5 \cdot 7$ and $72 = 2^3 \cdot 3^2$, therefore $\gcd(35, 72) = 1$ and 35 has an inverse modulo 72. The second approach is to use the Euclidean algorithm to find $\gcd(35, 72)$. See below.

b) Let d be the inverse of e modulo $(p-1)(q-1)$. Use the Euclidean Algorithm to compute d.

SOLUTION:
We use the Euclidean algorithm to compute $\gcd(72, 35)$.

$$\begin{aligned} 72 &= 35 \cdot 2 + 2, \\ 35 &= 2 \cdot 17 + 1. \end{aligned}$$

Let $M = 72$ and $r_2 = 2$. Using these symbols, we have

$$\begin{aligned} M &= 2e + r_2, \\ e &= 17r_2 + 1. \\ \to 1 &= e - 17r_2 = \\ &= e - 17(M - 2e) = 35e - 17M. \end{aligned}$$

The inverse of e modulo M is 35. Check: $35^2 = 1225 = 72 \cdot 17 + 1$.

c) Let d be the inverse of 35 modulo 72 which you computed in subproblem 5b. Decode message $y = 77$ by computing y^d modulo 91.

SOLUTION:
$35 = 32 + 2 + 1$

$$\begin{aligned} 77^2 &\equiv 5929 \equiv 14 \pmod{91} \\ 77^4 &\equiv 14^2 \equiv 196 \equiv 14 \pmod{91} \\ \ldots 77^{32} &\equiv 77^{16} \equiv 77^8 \equiv 77^4 \equiv 14 \pmod{91}. \\ \to 77^{35} &\equiv 77^{32} \cdot 77^2 \cdot 77 \equiv 14 \cdot 14 \cdot 77 \equiv 14 \cdot 77 \equiv 1078 \equiv 77 \pmod{91}. \end{aligned}$$

Therefore, the decoded message is also 77.

Problem 6: **[6 pts]** Let

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 2 \\ 2 & 1 \\ 3 & 5 \\ 4 & 1 \end{bmatrix}$$

a) Compute A^2.

SOLUTION:

$$A^2 = \begin{bmatrix} 1 & 3 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 2 & 4 & 2 & 2 \\ 1 & 2 & 1 & 1 \end{bmatrix}$$

b) Compute $A \cdot B$.

SOLUTION:

$$A \cdot B = \begin{bmatrix} 7 & 4 \\ 2 & 1 \\ 10 & 9 \\ 5 & 6 \end{bmatrix}$$

c) Compute the 2-nd Boolean power of A.

SOLUTION:

$$A^{[2]} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

d) Let I_4 be the 4×4 identity matrix. Compute $A + I_4$.

SOLUTION:

$$A + I_4 = \begin{bmatrix} 2 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

e) Compute $A \vee I_4$.

SOLUTION:

$$A \vee I_4 = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

f) Compute $A \wedge I_4$.

SOLUTION:

$$A \wedge I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

FINAL SCORE (out of 50)