Name:____________________________ **Grade:**______________

Exam 1

CPSC 311 Analysis of Algorithms
Andreas Klappenecker

- This exam contains 7 problems. You have 75 minutes to earn 100 points.
- This exam is closed book.
- You are allow to use a nonprogrammable calculator, although you will not need one.
- Do not spend too much time on a single problem. Read them all through first and attack them in the order that allows you to make the most progress.
- Show your work, as partial credit will be given. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it. Be neat.
- Recall the Aggie code of honor. Cheating will have severe consequences.

The work shown in this exam is my own.

Signature required: ________________________________

All logarithms are with respect to base 2 unless otherwise specified.

NAME: ________________________ **TAMU ID:** __________________

Problem 0 (2 points) Write your name and TAMU ID on each page.

Problem 1 (13 points) Suppose that a and b are $(r+1)n$-bit integers. Splitting a and b into $r+1$ pieces of n bits, it is possible to design a divide-and-conquer algorithm that uses $(2r+1)$ multiplications of n-bit integers and some further operations with execution time $\Theta(n)$. The same algorithm can be recursively applied for the $2r+1$ multiplications.

a) Derive the recurrence equation describing the execution time $T(N)$ of this divide-and-conquer algorithm, where $N = (r+1)n$.

b) Estimate the asymptotic complexity of this algorithm (solve the recurrence equation in a) by the Master theorem, by iteration, or by subsitution).

c) What is the best theoretical upper bound on the asymptotic time complexity of multiplication of two N-bit integers that can be derived from the previous considerations? Circle the correct answer.

i) $O(N)$ ii) $O(N^{1+\varepsilon})$ for some small ε iii) $O(N \log N)$
iv) $O(N^{1+\varepsilon} \log N)$ for some small ε v) none of the above

NAME: ______________________ **TAMU ID:** ________________

Problem 2 (15 points)

a) Prove that $(n+1)^2 \in O(n^2)$ by giving the constants n_0 and c in the definition of the O-notation. Justify your answer.

b) Sort the following functions according to asymptotic growth, starting with the least growing function. Write $f(n) \prec g(n)$ if $f(n) \in O(g(n))$, but $f(n) \notin \Theta(g(n))$. Write $f(n) \approx g(n)$ if $f(n) = \Theta(g(n))$. For example $n \prec n^2 \approx 2n^2$.

The function are given by

$$\begin{array}{cccc} (3/2)^n & (\sqrt{2})^{\log n} & n^2 & (\log n)! \\ n^{\log\log n} & n^3 & \log^2 n & \log(n!) \\ \sqrt{\log n} & n\log n & (\log n)^{\log n} & 2^{\log n} \end{array}$$

The base of the logarithms is 2.

NAME: ______________________ **TAMU ID:** ________________

Problem 3 (20 points) The main parameters of the RSA public key cryptosystem are the modulus $n = pq$, a product of two odd primes p and q, the encoding exponent e, and the decoding exponent d.

a) The three parameters n, e, d have to satisfy certain conditions such that the RSA system allows a faithful decoding of an encoded arbitrary message. Which of the following configurations are valid? If a configuration is not valid, then indicate which condition is violated.
i) $n = 15$, $e = 7$, $d = 11$.

ii) $n = 15$, $e = 5$, $d = 5$.

iii) $n = 15$, $e = 2$, $d = 8$.

b) The modulus is $n = 91$, the encoding exponent is $e = 5$. Determine the decoding exponent with the help of the extended Euclidean algorithm. Show your work.

c) You observe the encrypted message $m^e \equiv 77 \bmod n = 91$. How can you efficiently decode the message, knowing the decoding exponent above. Describe an efficient algorithm.

NAME: ________________________ **TAMU ID:** __________________

Problem 4 (20 points) Give asymptotically tight (big-Θ) bounds for $T(n)$ in each of the following recurrences. Justify your solutions by naming the particular case of the Master theorem, by iterating the recurrence, or by using the substition method; possibly in combination with a change of variables.

a) $T(n) = 5T(n/4) + n \log n$.

b) $T(n) = T(\sqrt{n}) + n$.

c) $T(n) = T(n-2) + 3$.

d) $T(n) = 9T(n/3) + 3n^2$.

e) $T(n) = T(n/2) + 1/\log n$.

NAME: ______________________ **TAMU ID:** __________________

Problem 5 (15 points) Let $A = a_1 a_2 \cdots a_m$ and $B = b_1 b_2 \cdots b_n$ be two sequences of characters. A common supersequence of A and B is a sequence containing both A and B as a subsequence. For instance, if $A = pen$ and $B = hen$, then $hpen$ is a common supersequence. The goal is to determine the length of the smallest common supersequence of A and B.

Let $d(i,j)$ denote the length of a shortest common supersequence of $a_1 \cdots a_i$ and $b_1 \cdots b_j$, where $0 \leq i \leq m$ and $0 \leq j \leq n$.
a) Determine

$$d(i,0) = \qquad\qquad\qquad d(0,j) =$$

b) Complete the recursion formula

$$d(i,j) = \min\left(d(i,j-1) \qquad , d(i-1,j) \qquad , d(i-1,j-1) \qquad\qquad\qquad \right)$$

Hint: How much larger is $d(i,j)$ than $d(i-1,j-1)$? On what does it depend? How much smaller can $d(i-1,j)$ be than $d(i,j)$?
c) Calculate the table of lengths $d(i,j)$ for the sequences $BALD$ and $BEAR$.

D					
L					
A					
B	1				
	0	1			
		B	E	A	R

The upper right corner contains $d(4,4)$, the length of shortest common supersequence containing $BALD$ and $BEAR$ as subsequences.

d) Determine a tight upper bound for the time complexity of an algorithm to calculate the length of the shortest common supersequence of two sequences of length m and n respectively. (Use big-O notation).

NAME: ______________________ **TAMU ID:** ________________

Problem 6 (15 points)
a) Give an asymptotically tight time complexity bound for the fast Fourier transform algorithm (transforming a vector of length $n = 2^k$).

b) Give a bound on for the time complexity of the extended Eucliden algorithm of two numbers with b bits (as derived in the lecture).

c) Calculate $7^{1023} \bmod 11$.

d) Determine a such that $0 \leq a < 77$ and

$$\begin{aligned} a &\equiv 2 \bmod 7, \\ a &\equiv 4 \bmod 11. \end{aligned}$$

e) Let F_n denote the nth Fibonacci number. Recall that $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$. Give a simple description of the sequence $(F_n \bmod 2)_{n \geq 0}$. Hint: Look at small cases.