CSCI 2824
Midterm Exam 2
Spring 2018

Name: $\underbrace{\hspace{6cm}}_{\text{By writing my name I promise to abide by the Honor Code}}$

Section number: ______________________

Read the following:

- **RIGHT NOW**! Write your name on the top of your exam.
- You are allowed one 8 1/2 × 11in sheet of **handwritten** notes (both sides). No magnifying glasses!
- You may use a calculator provided that it cannot access the internet or store large amounts of data.
- You may **NOT** use a smartphone as a calculator.
- Clearly mark answers to multiple choice questions on the provided answer line.
- Mark only one answer for multiple choice questions. If you think two answers are correct, mark the answer that **best** answers the question. No justification is required for multiple choice questions.
- If you do not know the answer to a question, skip it and come back to it later.
- For free response questions you must clearly justify all conclusions to receive full credit. A correct answer with no supporting work will receive no credit.
- If you need more space for free-response questions, there are blank pages at the end of the exam. If you choose to use the extra pages, make sure to **clearly** indicate which problem you are continuing.
- You have **90 minutes** for this exam.

Page	Points	Score
2	12	
3	12	
4	16	
5	20	
6	20	
7	20	
Total	100	

1. (3 points) Consider the pseudocode for procedure `parity_party(A,B,n)`, given below. The input to the procedure is two matrices A and B, and scalar n. $A[i][j]$ and $B[i][j]$ (the element in row i, column j of matrices A and B, respectively) are all integers. n gives the number of rows and columns of A and B (they are both $n \times n$ square matrices). Give an estimate of the complexity of this procedure, where complexity is measured by the number of **additions and subtractions** needed. Justify your answer.

```
procedure parity_party(A, B, n):
  par_ctr = 0
  for i from 1 to n:
    for j from 1 to n:
        if (A[i][j] + B[i][j]) %2 == 0,
          then par_ctr = par_ctr + 1
        else
          then par_ctr = par_ctr - 1
  return odd_ctr
```

A. `parity_party` is order n

B. `parity_party` is order n^2

C. `parity_party` is order n^3

D. `parity_party` is order n^4

1. **B**

2. (3 points) What is the **smallest** integer p such that $f(n) = 3n^2 + \log(n^2) + n\log(n^4)$ is $\mathcal{O}(n^p)$?

A. $p = 2$

B. $p = 3$

C. $p = 4$

D. $p = 5$

2. **A**

3. (3 points) Select the answer that is a closed form solution to this recurrence relation:

$$a_n = 2a_{n-1} + 3, a_0 = 1$$

A. $a_n = 2^n - 3$

B. $a_n = 2^{n+2} - 3$

C. $a_n = 4n + 1$

D. $a_n = 2n^2 + 2n + 1$

3. **B**

4. (3 points) Suppose b and q are integers, p and m are positive integers, and that $mb + pq \equiv 3 \pmod{m}$. Which of the following necessarily must be true?

A. $pq = 1$

B. $pq \equiv 1 \pmod{m}$

C. $pq \equiv 2 \pmod{m}$

D. $pq \equiv 3 \pmod{m}$

4. **D**

5. (3 points) Which of the following **is not** an inverse of 5 $\pmod{12}$?

   A. -7

   B. 1

   C. 5

   D. 17

5. **B**

6. (3 points) Suppose you're designing an RSA encryption scheme using $p = 13$, $q = 11$, and $n = pq = 143$. Which of the following is **NOT** a valid public key (e, n)?

   A. $(5, 143)$

   B. $(11, 143)$

   C. $(13, 143)$

   D. $(17, 143)$

6. **A**

7. (3 points) What is $5^{12000000000000000000000000002} \textbf{ mod } 13$?

   A. 4

   B. 8

   C. 12

   D. 25

7. **C**

8. (3 points) Suppose you run a surfing camp for 10, 11, and 12 year olds. During practice at the camp the kids use surfboards that are either red, blue, or green. What is the minimum number of kids that must be enrolled at the camp to guarantee that you have at least three kids of the same age with the same color surfboard?

   A. 13

   B. 18

   C. 19

   D. 27

8. **C**

9. (8 points) Use either **Chinese Remainder Theorem** or **Back Substitution** to find all solutions x to the system of congruences:

$$x \equiv 2 \pmod 4$$
$$x \equiv 4 \pmod 7$$

CRT:

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 \pmod m$

$m = 4 \times 7 = 28$

$M_1 = \frac{m}{m_1} = 7$ & $M_2 = \frac{m}{m_2} = 4$

$y_1 =$ inverse of $M_1 \pmod{m_1}$
$7 \pmod 4$

$y_1 = 3$ works! $(7 \cdot 3 = 21 \equiv 1 \pmod 4)$

$y_2 =$ inverse of $M_2 \pmod{m_2}$
$4 \pmod 7$

$y_2 = 2$ works! $(4 \cdot 2 = 8 \equiv 1 \pmod 7)$

$\Rightarrow x \equiv 2 \cdot 7 \cdot 3 + 4 \cdot 4 \cdot 2 \pmod{28}$
$\equiv 42 + 32 \pmod{28}$
$\boxed{x \equiv 18 \pmod{28}}$

Back Sub:

$x \equiv 2 \pmod 4 \rightarrow x = 2 + 4k$ $(k \in \mathbb{Z})$

$\rightarrow 2 + 4k \equiv 4 \pmod 7$

$\rightarrow 4k \equiv 2 \pmod 7$

$\rightarrow$ need inverse of $4 \pmod 7$

$\rightarrow$ 2 works! (see left)

$\rightarrow k \equiv 2 \cdot 2 \pmod 7$

$\rightarrow k = 4 + 7l$ $(l \in \mathbb{Z})$

$\rightarrow x = 2 + 4(4 + 7l)$
$= 18 + 28l$

$\rightarrow \boxed{x \equiv 18 \pmod{28}}$

10. (8 points) Come up with a formula (in terms of n) for the number of **trit-strings** of length n that are **NOT** palindromic. Reminders:

- You must show work to receive credit
- Trit-strings are made up of 0s, 1s and 2s
- A palindrome is the same forwards and backwards. For example: 102201.

NOTE: other answers exist!

Even n: $\underbrace{102}201$

$\frac{n}{2}$ choices to make, & 3 options for each

$\rightarrow \boxed{f(n) = 3^{n/2} \text{ if } n \text{ even}}$

Odd n: $\underbrace{102}01$

$\frac{n+1}{2}$ choices to make, 3 options for each

$\rightarrow \boxed{f(n) = 3^{\frac{n+1}{2}} \text{ if } n \text{ odd}}$

11. (20 points) Let $x > 0$ be some fixed real number.

Use induction to prove that $(1+x)^n > 1 + nx$ for all $n \geq 2$. Be sure to mention whether you are using strong or weak induction.

Solution: Base case: $n = 2$

strong induction

$(1+x)^2 = 1 + 2x + x^2 > 1 + 2x$ since $x > 0$

IH: assume for all $2 \leq k \leq n$ $(1+x)^k > 1 + kx$

will show: for $k = n+1$: $(1+x)^{n+1} > 1 + (n+1)x$

$\cdot\ (1+x)^{n+1} = (1+x)^n (1+x) \overset{IH}{>} (1+nx)(1+x)$

$= 1 + x + nx + nx^2 = 1 + (n+1)x + nx^2 >$

$1 + (n+1)x$

$\blacksquare$

12. (20 points) After a very successful surfing season, the Interstellar Surfing Association (ISA) is putting on surfing demonstrations. There are 8 demonstrations total, which are split up between the two champion surfers (Alex and Tony, of course). Neither surfer can perform 4 demonstrations in a row, but either of them can perform more (or less) than 4 demonstrations total.

For example, one possible arrangement is for Alex to do 2 demonstrations, then Tony do 3, then Alex do 3.

Determine how many possible ways are there for the ISA to organize those 8 demonstrations. You do **not** need to simplify your answer.

Solution: The problem is equivalent to asking how many length 8 binary strings are there with no 4 consecutive 1's or 0's.

[Let Alex performing = 0 Tony Performing = 1
Then arrangements of surfing demonstrations = binary strings]

$\underbrace{\text{\# of length 8 binary strings with no 4 consecutive 1's or 0's}}_{A}$ = $\underbrace{\text{\# of length 8 bin. strings}}_{B}$ − $\underbrace{\text{\# of length 8 bin strings with 4 consecutive 1's or 4 cons. 0's}}_{C}$

$|A| = |B| - |C|$

- $|A| = 2^8$
- $|C|$: We calculate # strings with 4 consecutive 0's # strings with 4 consecutive 1's is same.

5 positions that 0000 can start:

1) $0000XXXX \Rightarrow 2^4$
2) $10000XXX \Rightarrow 2^3$
3) $X10000XX \Rightarrow 2^3$
4) $XX10000X \Rightarrow 2^3$
5) $XXX10000 \Rightarrow 2^3$

- Total $= 2^4 + 4 \cdot 2^3 = 16 + 4 \cdot 8 = 16+32 = 48$
- same for 1's = 48
- Two strings with 4 cons. 0's & 1's

00001111
11110000 } need to subtract

$|C| = 2 \cdot 48 - 2 = 94$

$\boxed{|A| = 2^8 - 94 = 256 - 94 = 162}$

13. (20 points) Consider the function $f(n) = 3n^2 + \log(n^3) - n$.

(a) Find a tight big-$\mathcal{O}$ bound for $f(n)$. Be sure to specify your values of C and k in the definition of big-$\mathcal{O}$.

(b) Find a tight big-Ω bound for $f(n)$. Be sure to specify your values of C and k in the definition of big-Ω.

(c) Can you state that $f(n)$ is $\Theta(h(n))$ for some function $h(n)$? If so, state $h(n)$ and briefly justify your reasoning.

Solution:

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

$3\log n \leq 3n$ for all $n > 1$

$\leq 3n^2$

& $-n < 0$ for all $n > 0$

$\Rightarrow f(n) \leq 3n^2 + 3n^2 + 0 = 6n^2$ for $\underline{n > 1}$

$\Rightarrow$ $\boxed{f \text{ is } O(n^2) \text{ w/ } C = 6 \text{ \& } k = 1}$

b.) $n \leq n^2$ for $n > 1$

$\Rightarrow \underline{-n \geq -n^2}$

$\Rightarrow f(n) \geq 3n^2 + 3\log n - n^2$

$\geq 3n^2 - n^2 = 2n^2$ for $\underline{n > 1}$

$\Rightarrow$ $\boxed{f \text{ is } \Omega(n^2) \text{ w/ } C = 2 \text{ \& } k = 1}$

c.) Yes - $\boxed{f \text{ is } \Theta(n^2)}$ b/c it is both $\underline{\underline{O(n^2) \text{ \& } \Omega(n^2)}}$