Final Exam

EECS 203

Spring 2016

Name (Print): ____

uniqname (Print): ____

Instructions. You have 120 minutes to complete this exam. You may have two page of notes (8.5x11.5 two-sided) but may not use any other sources of information, including electronic devices, textbooks, or notes. Leave at least one seat between yourself and other students. Please write clearly. If we cannot read your writing, it will not be graded.

Honor Code. This course operates under the rules of the College of Engineering Honor Code. Your signature endorses the pledge below. After you finish your exam, please sign on the line below:

I have neither given nor received aid on this examination, nor have I concealed any violations of the Honor Code.

____

A. Multiple choice (18 points)

In this section, each question will have zero or more correct answers. You are to circle each correct answer and leave uncircled each incorrect answer.

[3 points each, -1 per incorrect circle/non-circle, minimum 0 points per problem]

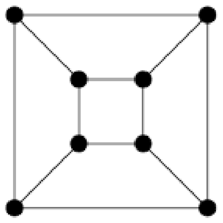
1. Let B(x,y) be the proposition "*y* is the best friend of *x*". Which of the following, if any, expresses the statement: "Everyone has exactly one best friend"?
    - $\forall x \exists y \forall z \left(\left(B(x,y) \wedge B(x,z)\right) \rightarrow (y = z)\right)$
    - $\forall x \exists y \exists z \left(\left((x \neq y) \rightarrow B(x,y)\right) \wedge \left((x \neq z) \rightarrow \neg B(x,z)\right)\right)$
    - $\forall x \exists y \left(B(x,y) \wedge \forall z\left((z \neq y) \rightarrow \neg B(x,z)\right)\right)$
    - $\exists x \forall y \left(B(x,y) \wedge \forall z\left((z \neq y) \rightarrow \neg B(x,z)\right)\right)$
    - $\forall x \exists y \forall z \left((B(x,y) \wedge \left(B(x,z) \rightarrow (y = z)\right)\right)$

2. Which of the following pairs of values (n, k) (if any) make the following statement true: "If 50 chairs are distributed into n piles, there must be a pile with at least k chairs."
    - (100, 3)
    - (3, 15)
    - (7, 8)
    - (51, 2)
    - (15, 3)

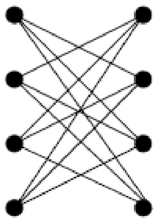
3. Let A and B be two events, with A ⊆ B, and suppose that 0 < P(A) < 1 and 0 < P(B) < 1. Which of the following, if any, must be true?
    - P(A|B) = 1
    - P(B|A) = 1
    - A and B are not independent
    - P(B − A) > 0
    - P(A∩B)>P(A)

4. Circle each of the following (if any) that are *satisfiable*
    - $(\boldsymbol{p} \oplus \boldsymbol{q}) \land (\boldsymbol{p} \land \boldsymbol{q})$
    - $(\boldsymbol{p} \land \boldsymbol{q}) \rightarrow \boldsymbol{T}$
    - $\neg(\boldsymbol{p} \lor \boldsymbol{q}) \land (\boldsymbol{q} \lor \boldsymbol{p})$
    - $\boldsymbol{p} \lor \neg \boldsymbol{p}$
    - $\boldsymbol{p} \oplus \neg \boldsymbol{p}$

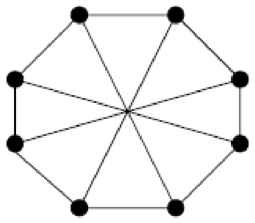
5. Circle each of the following that is a *tautology*
    - $(\boldsymbol{p} \oplus \boldsymbol{q}) \land (\boldsymbol{p} \land \boldsymbol{q})$
    - $(\boldsymbol{p} \land \boldsymbol{q}) \rightarrow \boldsymbol{T}$
    - $\neg(\boldsymbol{p} \lor \boldsymbol{q}) \land (\boldsymbol{q} \lor \boldsymbol{p})$
    - $\boldsymbol{p} \lor \neg \boldsymbol{p}$
    - $\boldsymbol{p} \oplus \neg \boldsymbol{p}$



G_1



G_2



G_3

6. Consider the above graphs. Which of the following statements are true?
    - G_1 and G_3 are bipartite
    - G_1 and G_2 are connected
    - G_1 and G_2 are bipartite
    - G_3 has a Eulerian path
    - G_1 has a Eulerian circuit

B. More multiple choice (14 points)

In this section, each question will have zero or more correct answers. You are to circle each correct answer and leave uncircled each incorrect answer.

[2 points each, -1 per incorrect circle/non-circle, minimum 0 points per problem]

1. Circle each of the following which are a (multiplicative) inverse of 1 modulo 7.

    - 3
    - 1
    - -6
    - -4
    - 10

2. Which of the following are independent of each other (circle zero or more)

    - Roll two dice
      A: The first die is a "1"
      B: The second die is a "1"
    - Flip two coins
      A: The first coin is a head
      B: The two coins are the same
    - Flip three coins.
      A: The first coin is a head
      B: The second and the third are tails
    - Draw two cards from a deck of 52 cards without replacement
      A: The first card is a jack
      B: The second card is an ace

3. Consider an application whose runtime can be expressed as $f(n)=4f(n/3)+4n$. Which of the following (if any) would be true of the runtime?

    - It is Ω (n)
    - It is $\Theta(n^2)$
    - It is $\Theta(n \log n)$
    - It is $O(n^{\log(n)})$

4. Circle zero or more of the following which are *tautologies* where A and B are subsets of $\mathbb{N}$.
    - $(A \cap B) \subset A$
    - $A \subset (A \cup \{-5\})$
    - $A \subseteq (A \cap B)$
    - $A \supset \phi$

5. The equation $3N^3$*log(N)+4N*log(N) is

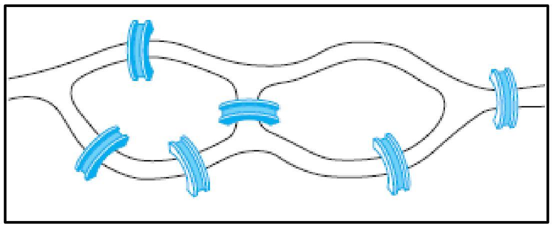
    - $\Theta(N^2\log(N))$
    - $O(N^2)$
    - $\Omega(N^2\log(N))$
    - $\Theta(N^3)$

6. The function on the right has a runtime that can be characterized as having a runtime of

```
j:=1
while(j<N)
  j=j*2
  for (i:= 1 to 5)
    if(A[i]>A[j])
       A[j]=A[j]+1
```

    - $\Theta(N*\log(N))$
    - $\Omega(N*\log(N))$
    - $\Theta(N^2)$
    - $O(N)$

7. Which of the following are true?



    - The shortest path between two vertices in a weighted graph is unique if the weights of edges are distinct.
    - It is possible to cross all of the bridges shown exactly once and finish at the place where you started.
    - It is possible to cross all of the bridges shown exactly once and *not* finish to the place where you started.
    - Dijkstra's algorithm does the same thing as the Floyd-Warshall algorithm, but faster.

C. Functions (6 points)

Each part has one correct answer. ***(-2 for each wrong or blank answer, minimum 0)***

For each of the following mappings indicate what type of function they are (if any). Use the following key:

i. Not a function
ii. A function which is neither onto nor one-to-one
iii. A function which is onto but not one-to-one
iv. A function which is one-to-one but not onto
v. A function which is both onto and one-to-one

1. The mapping *f* from $\mathbb{Z}\ to\ \mathbb{N}$ defined by $f(n) = |2n|$.

   i ii iii iv v

2. The mapping *f* from $\{1, 3\}\ to\ \{2, 4\}$ defined by $f(n) = 2n$.

   i ii iii iv v

3. The mapping *f* from $\mathbb{R}\ to\ \mathbb{R}$ defined by $f(n) = 8 - 2n$.

   i ii iii iv v

4. The mapping *f* from $\mathbb{R}\ to\ \mathbb{Z}$ defined by $f(x) = \lfloor x + 1 \rfloor$

   i ii iii iv v

5. The mapping *f* from $\mathbb{R}^{+} to\ \mathbb{R}^{+}$ defined by $f(x) = x - 1$.

   i ii iii iv v

D. Conditional probability (12 points)

1. Consider the following events when drawing two cards from a standard deck of cards without replacement.
   A. The first card is a Spade
   B. The second card is a Heart
   C. The first card is the Ace of Clubs

   Compute the following values (you can provide an answer that can trivially be input into a calculator): **(7 points -1.5 per wrong or blank answer, minimum 0)**

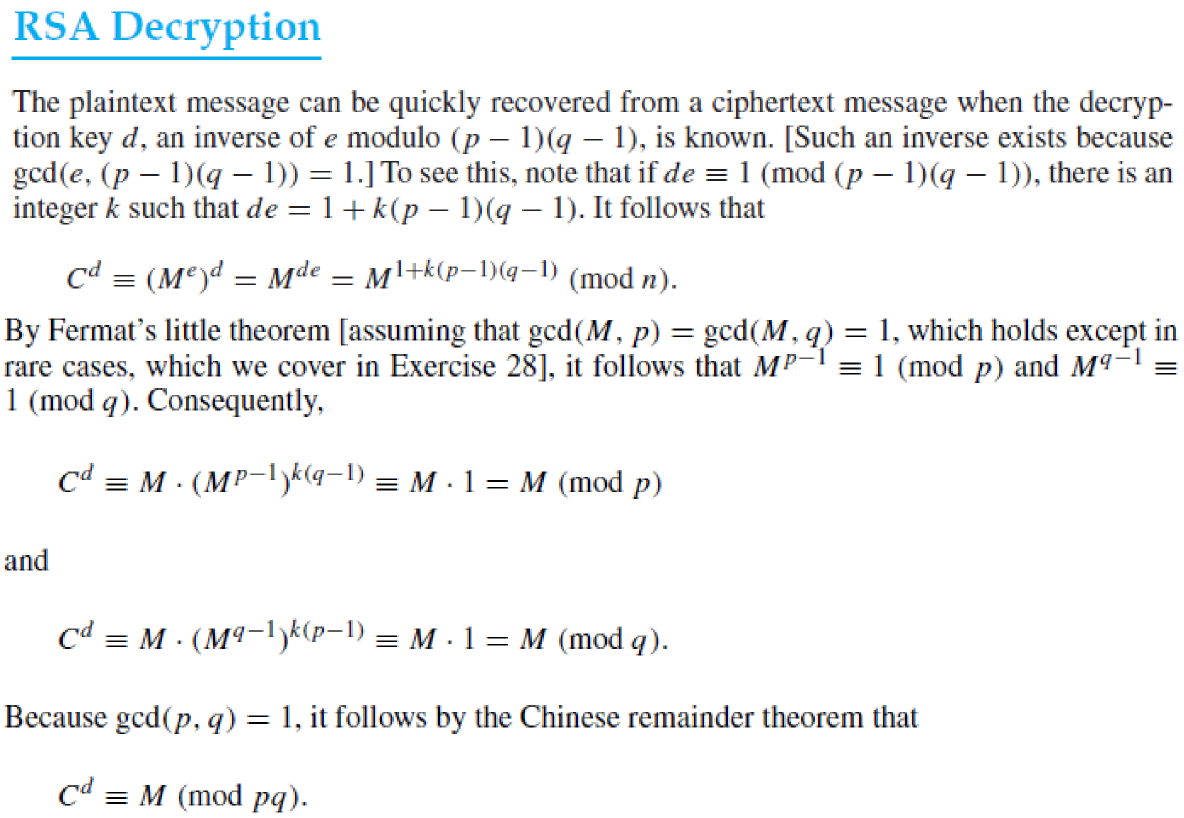
   $P(B)$: ____________________ $P(A \cap B)$: ____________________

   $P(C|A)$: ____________________ $P(A \cup C)$: ____________________

   $P(A|B)$:____________________ $P(B|A)$: _____________________

2. A diagnostic test has a probability 0.98 of giving a positive result when applied to a person suffering from a certain cancer, and a 0.05 probability of giving a false positive when testing someone without that cancer. Say that 1 person in 20,000 suffers from this cancer. What is the probability that someone will be misclassified by the test? Your answer should be in a form we could easily enter it into a calculator. **(5 points)**

E. Public key encryption (8 points)



RSA Decryption

The plaintext message can be quickly recovered from a ciphertext message when the decryption key d, an inverse of e modulo $(p-1)(q-1)$, is known. [Such an inverse exists because $\gcd(e,(p-1)(q-1)) = 1$.] To see this, note that if $de \equiv 1 \pmod{(p-1)(q-1)}$, there is an integer k such that $de = 1 + k(p-1)(q-1)$. It follows that

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}.$$

By Fermat's little theorem [assuming that $\gcd(M, p) = \gcd(M, q) = 1$, which holds except in rare cases, which we cover in Exercise 28], it follows that $M^{p-1} \equiv 1 \pmod{p}$ and $M^{q-1} \equiv 1 \pmod{q}$. Consequently,

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \pmod{p}$$

and

$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \pmod{q}.$$

Because $\gcd(p, q) = 1$, it follows by the Chinese remainder theorem that

$$C^d \equiv M \pmod{pq}.$$

a. Let n=22, and e=3. What is the decryption key, "d"? Briefly explain/justify your answer. **[5]**

b. In your own words, explain why it is that one can find the decryption key in part a, but in general having only "n" and "e" won't let you easily find the decryption key for "real-world" instances of RSA. **[3]**

F. Finding recurrence relations (10 points)

Suppose you are writing a quiz with n questions each with 5 options, a,b,c,d,e.

a. Say you choose not to have any two questions in a row have the same answer. Write a recurrence relation to count how many possible sets of answers you could have on a quiz with n questions. Provide sufficient base cases. **[4]**

b. Later you decide this is too restrictive and choose instead to just require that you never have 3 of the same answer in a row. Write a new recurrence relation and provide base case(s) for this new restriction. **[6]**

G. Graphs (10 points)

Let G be a simple graph with *n* vertices.

a. What is the *maximum* number of edges G can have? **[2]**

b. If G is connected, what is the *minimum* number of edges G can have? **[2]**

c. Show that if the minimum degree of any vertex of G is greater than or equal to $\frac{n-1}{2}$, then G must be connected. [**6]**

H. Solving a recurrence relation (8 points)

Find a closed-form solution to the following recurrence relation:

$$a_n = 2a_{n-1} + 8a_{n-2};\ a_0 = 1, a_1 = 7$$

I. Induction (9 points)

Let $x \in \mathbb{R}$ and $x - 1 \neq 0$. Show, using mathematical induction, that for all integers $n \geq 0$,

$$\sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}$$

J. Last problem (5 points)

20 hockey players have scored a total of 155 points this season. Show that at least two of them must have scored the same number of points.