Name: _____KEY_____ E-mail ID: _____@virginia.edu

Pledge: _____

_____

_____

Signature: _____

*There are 50 minutes for this exam and 100 points on the test; don't spend too long on any one question!*

*All work must be on these three exam pages.*

*A note on terminology: to differentiate between the two types of induction (mathematical induction and strong induction), they are referred to as weak induction and strong induction, respectively (or weak mathematical induction and strong mathematical induction, respectively).*

Short answer questions (5 points each): these questions only require a sentence or two for full credit.

1. Given a RSA cipher text of 4501, a decryption key of 4669, and $n$ = 10379, how would this message be decrypted? You can leave the answer in formulaic form. Clearly label what your variables represent!

   **Answer:**

   $p = c^d \bmod n$

   $p = 4501^{4669} \bmod 10379$

   Where $p$ is the plaintext message, $c$ is the encrypted message (cipher text), $d$ is the decryption key, and $n$ is from the key generation

2. Find the lowest possible number (greater than 1) that is relatively prime to 210. Note that any number that is relatively prime to 210 will get credit, but the lower the number, the greater the credit.

   **Answer:**

   In increasing order: 11, 13, 17, 19, and successive primes (or products of those primes)

3. Find four numbers congruent to 5 modulo 17.

   **Answer:**

   …, -46, -29, -12, 5, 22, 39, 56, …

   (Rosen, chapter 3 supplementary exercises, question 19)

4. What is $\gcd(63,105)$?

   **Answer:**

   $\gcd(63,105) = 21$

5. What is $\text{lcm}(63,105)$ ?

**Answer:**

$\text{lcm}(63,105) = 315$

6. What is the closed form formula (meaning a non-recursive formula that does not use summations) for the summation $\sum_{k=1}^{n} k$ ?

**Answer:**

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

7. What is the halting problem, and why is it important?

**Answer:**

The halting problem is the quest to write a program that will successfully determine if another program will ever halt. It was the first program to be proven impossible to implement.

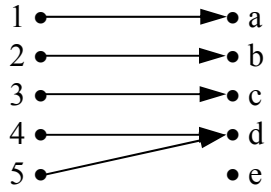
8. What is the difference between weak induction and strong induction?

**Answer:**

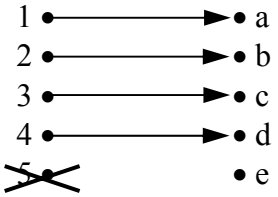
The inductive hypothesis in mathematical induction only assumes $P(k)$ is true, while the inductive hypothesis in strong induction assumes $P(1), P(2), ..., P(k)$ are all true.

9. (20 points) For each of the following parts, draw arrows from the dots on the left to the dots on the right to indicate a function that fulfills the following properties. If necessary, you may cross off elements on either side.

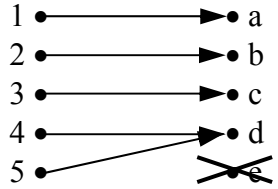
a) A function that is not one-to-one and not onto



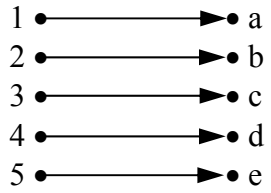

b) A function that is one-to-one but not onto



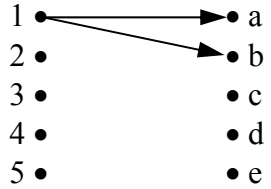

c) A function that is not one-to-one but is onto




d) A function that is both one-to-one and onto




e) An example of a mapping that is not a function



10. (25 points) Consider the recursive definition for $f(n)$ where $f(1)=1$ and $f(n)=f(n-1)+2n-1$ for $n \geq 2$.

a) Write the first 5 terms of $f(n)$.

**Answer:**

$f(1)=1$
$f(2)=f(1)+2*1-1=4$
$f(3)=f(2)+2*4-1=9$
$f(4)=f(3)+2*9-1=16$
$f(5)=f(4)+2*16-1=25$

b) Find an explicit (i.e. non-recursive) formula for $f(n)$.

**Answer:**

$f(n)=n^2$

c) Use weak mathematical induction to prove the result from (b) equals the recursive definition for $f(n)$.

**Answer:**

Base case: $f(1)=1$, as given by the recursive definition

Inductive hypothesis: Assume: $f(k)=k^2=f(k-1)+2k-1$

Inductive step: Show: $f(k+1)=(k+1)^2=f(k+1-1)+2(k+1)-1$

$(k+1)^2=f(k+1-1)+2(k+1)-1$
$k^2+2k+1=f(k)+2(k+1)-1$
$k^2+2k+1=k^2+2k+1$

(Rosen, chapter 3 supplementary exercises, page 295, question 53)

11. (15 points) Give the recursive definitions of the following sequences. Clearly label the parts of your recursive definition.

a) The sequence generated by $a_n = 5$ for $n = 1,2,3,...$

**Answer:**

Basis step: $a_1 = 5$
Recursive step: $a_n = a_{n-1}$
(Rosen, section 3.4, question 7d)

b) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, 32, 0, …

**Answer:**

Basis step: $a_1 = 1, a_2 = 0$
Recursive step: $a_n = 2 * a_{n-2}$
(Rosen, section 3.2, question 9c)

c) 1, 2, 3, 4, 5, 6, 1, 2, 3, 4, 5, 6, 1, 2, 3, 4, 5, 6, 1, 2, 3, 4, 5, 6, 1, … (only one basis step allowed!)

**Answer:**

Basis step: $a_1 = 1$
Recursive step: $a_n = a_{n-1} \bmod 6 + 1$
Note: the question was supposed to have been the repeating sequence 0, 1, 2, 3, 4, 5, which would have had the formula $a_1 = 0, a_n = (a_{n-1} + 1) \bmod 6$. This question was canned during the exam, and everybody got full credit for this one.