Name: ______________________________

Andrew ID: ______________________

Recitation (circle one): **F(10:30)** **G(12:30)** **H(1:30)** **J(3:30)**

Math 127: Final Exam
11 May 2018

Turn off and put away your cell phone.
No notes or books are permitted during this exam.
No calculators or any other devices are permitted during this exam.
Read each question carefully, answer each question completely, and show all of your work.
Write solutions clearly and legibly; credit will not be given for illegible solutions.
If any question is not clear, ask for clarification.

#	Points	Score
1	40	
2	20	
3	20	
4	20	
5	20	
6	18	
7	20	
8	20	
9	18	
10	20	
11	32	
$\boldsymbol{\Sigma}$	248	

1. Define each of the following terms. Be sure to clearly explain any functions, sets, or elements you need for the definition. Example:

   (a) root (as of a polynomial)

   (b) domain (as of a function)

   (c) propositional formula

   (d) power set

   (e) preimage (as with functions)

(f) totient

(g) surjection

(h) random variable

(i) divergent (as in a real-valued sequence)

(j) uncountably infinite

2. Use induction to prove that for all integers $n \geq 2$,

$$\prod_{k=2}^{n} \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

3. Let $f : X \to Y$ be a function. Prove that f is injective if and only if $f(A \cap B) = f(A) \cap f(B)$ for all $A, B \subseteq X$.

4. (a) Define a relation R on the set $\mathcal{P}([2n])$ by ARB if and only if $A \cap [n] = B \cap [n]$. Prove that R is an equivalence relation.

(b) Show that the equivalence classes in $\mathcal{P}([2n])/R$ are in bijection with $\mathcal{P}([n])$.

5. All possible rearrangements of the word “CLASSES” are written on slips of paper, and placed into a hat. You pick one slip of paper out. What is the probability that the rearrangement you see has two S’s in a row, but not 3?

6. Use techniques or theorems from class to determine each of the following. Cite the name/description of the theorem or technique you are using.

   (a) $\gcd(1248, 1044)$

   (b) the remainder of 2^{1000} when divided by 11.

   (c) whether or not 17928 is divisible by 3.

7. Let A, B be events in a probability space $(\Omega, \mathbb{P})$. Prove that the following are equivalent:

   (a) A and B are independent.

   (b) A and B^c are independent.

   (c) A^c and B^c are independent.

8. The Lucas numbers are a sequence defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$.

   Prove that for all $n \geq 1$, $L_n^2 = L_{n+1}L_{n-1} + 5(-1)^n$.

9. Provide a proof for each of the following basic facts about modular arithmetic and divisibility.

   (a) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

   (b) For $a, b, c \in \mathbb{N}$, if $a \perp b$ and $a | bc$, then $a | c$.

   (c) If $au \equiv 1 \pmod{n}$, and $av \equiv 1 \pmod{n}$, then $u \equiv v \pmod{n}$.

10. State each of the following theorems. Be sure to define any variables necessary for the statements.

    (a) Triangle Inequality (in $\mathbb{R}$)

    (b) Bezout's Lemma

    (c) Bayes' Theorem

    (d) DeMorgan's Laws (for sets)

11. Provide a short answer to each of the following questions. You may use pictures to help illustrate your explanations if you wish.

    (a) Explain why $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$ are logically equivalent.

    (b) Let $a, n \in \mathbb{N}$, with $n \geq 1$. When does a have a multiplicative inverse modulo n? Why?

(c) Suppose $f : X \to Y$ is an injective function that is not surjective, but $|X| = |Y|$. Explain when this is possible.

(d) Your friend writes the following "proof" that the sequence (x_n) defined by $x_n = n$ converges:

> Notice that $x_{n+1} = x_n + 1 > x_n$, so the sequence is monotonic. Also, $x_n \geq 0$ for all n, so the sequence is bounded. Therefore, by the Monotone Convergence Theorem, the sequence has a limit.

What's wrong with this proof?

Axioms for a Field: A set X together with elements $0, 1$ and binary operations $+, \cdot$ is a field if the following axioms are met:

F1 $0 \neq 1$

F2 Associativity of addition: For all $x, y, z \in X$, $x + (y + z) = (x + y) + z$.

F3 Additive identity: For all $x \in X$, $x + 0 = x$.

F4 Existence of additive inverses: For all $x \in X$, there exists $y \in X$ such that $x + y = 0$.

F5 Commutativity of addition: For all $x, y \in X$, $x + y = y + x$.

F6 Associativity of multiplication: For all $x, y, z \in X$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

F7 Multiplicative Identity: For all $x \in X$, $x \cdot 1 = x$.

F8 Existence of multiplicative inverses: For all $x \in X$ with $x \neq 0$, there exists $y \in X$ such that $xy = 1$.

F9 Commutativity of multiplication: For all $x, y \in X$, $x \cdot y = y \cdot x$.

F10 Distributivity: For all $x, y, z \in X$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Axioms for an Ordered Field: A field $(X, 0, 1, +, \cdot)$ together with an partial ordering $\leq$ is an ordered field if the following axioms are met:

PO4 For all $x, y \in X$, either $x \leq y$ or $y \leq x$.

OF1 For all $x, y, z \in X$ if $x \leq y$, then $x + z \leq y + z$.

OF2 For all $x, y \in X$, if $0 \leq x$ and $0 \leq y$, then $0 \leq xy$.