Math 109: The final exam.
Instructor: A. Salehi Golsefidy

Name: ....

PID: ....

12/06/2016

1. Write your Name and PID on the front of your exam sheet.
2. No calculators or other electronic devices are allowed during this exam.
3. Show all of your work; no credit will be given for unsupported answers.
4. Read each question carefully to avoid spending your time on something that you are not supposed to (re)prove.
5. Ask me or a TA when you are unsure if you are allowed to use certain fact or not.
6. Good luck!

Question	Points	Bonus Points	Score
1	10	0	
2	5	0	
3	10	0	
4	10	0	
5	10	0	
6	10	0	
7	35	0	
8	0	10	
Total:	90	10	

1. (10 points) Which one of the following propositional forms is not equivalent to $(P \wedge Q) \Rightarrow R$? Justify your answer.

   1. $(P \wedge Q \wedge \neg R) \Rightarrow \perp$, where $\perp$ means contradiction,
   2. $(\neg R) \Rightarrow ((\neg P) \vee (\neg Q))$,
   3. $(P \Rightarrow R) \wedge (Q \Rightarrow R)$,
   4. $(P \Rightarrow R) \vee (Q \Rightarrow R)$.

2. (5 points) Let $a_0 = 0$ and $a_{n+1} := \sqrt{2 + a_n}$. Prove that, for any $n \in \mathbb{Z}^+$, we have $a_n < 2$.

3. (10 points) Write the negation of the following proposition (each part has 5 points):

   (a) $\forall X \subseteq \mathbb{R}, ((\exists m \in \mathbb{R}, \forall y \in X, m \leq y) \Rightarrow (\exists x \in X, \forall y \in X, x \leq y))$.

   (b) $\forall a, n \in \mathbb{Z}^+, (\gcd(a, n) = 1 \Rightarrow (\exists d \in \mathbb{Z}^+, a^d \equiv 1 \pmod{n}))$.

4. Suppose A and B are two non-empty sets. Suppose $f : A \to B$ and $g : B \to A$ are two functions such that $f \circ g = I_B$.

   (a) (6 points) Prove that g is injective.

   (b) (4 points) Is f necessarily injective?

5. (10 points) Prove that, for $a, b, c \in \mathbb{Z}^+$, if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

6. (10 points) Find $x, y \in \mathbb{Z}$ such that $763x + 91y = \gcd(763, 91)$.

7. For each question give a short answer. You are allowed to use all the results proved in the lectures:

   (a) (5 points) Let A be a subset of X. Let $f : P(X) \Rightarrow P(X)$, $f(B) = B \triangle A$, where $P(X)$ is the power set of X. Prove that f is a bijection. (Hint: consider $f \circ f$.)

   (b) (5 points) Prove that, for any integers a, b we have $5|ab$ implies that either $5|a$ or $5|b$.

   (c) (5 points) Let $g : \{0, \cdots, 5\} \to \{0, \cdots, 5\}$ be such that $g(x) \equiv 2x \pmod 6$. Is g bijective?

   (d) (5 points) Give an infinite set which is not enumerable.

(e) (5 points) Find $x \in \mathbb{Z}$ such that $7x \equiv 3 \pmod{76}$.

(f) (5 points) What is the remainder when 120620161395 is divided by 11?

(g) (5 points) What is the remainder when 7^{2018} is divided by 10? (Hint: $7^2 \equiv -1 \pmod{10}$).

8. (Bonus) Suppose p is an odd prime.

   (a) (3 points (bonus)) Prove that for any a in $\{1, 2, \ldots, p-1\}$ there is a unique a' in $\{1, 2, \ldots, p-1\}$ such that $aa' \equiv 1 \pmod{p}$. (We called a' a modular inverse of a modulo p.)

   (b) (2 points (bonus)) Let $f : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$ be a function such that $f(a)$ is a modular inverse of a modulo p. Prove that f is a bijection. (Hint: consider $f \circ f$.)

   (c) (3 points (bonus)) Show that $f(a) = a$ if and only if either $a = 1$ or $a = p - 1$.

(d) (2 points (bonus)) Prove that $(p-1)! \equiv -1 \pmod{p}$. (Hint: Using part (3) any number $a \in \{2, \ldots, p-2\}$ can be paired with $f(a)$.)