Math 255: Spring 2017
Exam 2

NAME: SOLUTIONS

Time: **50 minutes**

For each problem, you **must** write down all of your work carefully and legibly to receive full credit. For each question, you **must** use theorems and/or mathematical reasoning to support your answer, as appropriate.

Failure to follow these instructions will constitute a breach of the UVM Code of Academic Integrity:

- You may not use a calculator or any notes or book during the exam.
- You may not access your cell phone during the exam for any reason; if you think that you will want to check the time please wear a watch.
- The work you present must be your own.
- Finally, you will more generally be bound by the UVM Code of Academic Integrity, which stipulates among other things that you may not communicate with anyone other than the instructor during the exam, or look at anyone else's solutions.

I understand and accept these instructions.

Signature: ______________________________

Problem	Value	Score
1	6	
2	6	
3	8	
4	8	
5	4	
6	8	
7	10	
TOTAL	50	

Problem 1 : (6 points)

a) If $\gcd(a, n) = 1$, give the definition of the (multiplicative) order of a modulo n.

The multiplicative order of $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ is the smallest positive integer k such that $a^k \equiv 1 \bmod n$

b) What is the order of 3 modulo 7?

$3^1 \equiv 3 \not\equiv 1 \bmod 7$

$3^2 \equiv 9 \equiv 2 \not\equiv 1 \bmod 7$

$3^3 \equiv 6 \not\equiv 1 \bmod 7$

$3^4 \equiv 18 \equiv 4 \not\equiv 1 \bmod 7$

$3^5 \equiv 12 \equiv 5 \not\equiv 1 \bmod 7$

$3^6 \equiv 15 \equiv 1 \bmod 7$

the order of 3 in $(\mathbb{Z}/7\mathbb{Z})^{\times}$ is 6

c) What is $\log_3 6$ in $(\mathbb{Z}/7\mathbb{Z})^{\times}$?
Note: In the book, the author talks about the "index of 6 relative to 3 modulo 7," and uses the symbol $\text{ind}_3\, 6$. This is exactly the same thing and you can just pretend this is what it says above.

$\log_3 6 \equiv x \bmod 6$ ← exponents exist modulo $\varphi(7)=6$ since 3 is a primitive root of 7

means

$3^x \equiv 6 \bmod 7$

In part b) we see $3^3 \equiv 6 \bmod 7$ so

$\log_3 6 \equiv 3 \bmod 6$