Math 255: Spring 2017
Exam 2

NAME:

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.

b) What is the order of 3 modulo 7?

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 $\operatorname{ind}_3 6$. This is exactly the same thing and you can just pretend this is what it says above.

Problem 2 : (6 points) It is a fact that 2 is a primitive root of 11. Here is a table of discrete logarithms in base 2 modulo 11:

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	0	1	8	2	4	9	7	3	6	5

Note: In the book, the bottom row of the table would be labeled $\text{ind}_2\, a$ (see #1c)).
Use this table to give all of the solutions of the equation

$$4x^4 \equiv 3 \pmod{11}.$$

Problem 3 : (8 points)

a) State Fermat's Little Theorem (also known as Fermat's Theorem in the book).

b) Show that if p and q are distinct primes,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Problem 4 : (8 points)

a) State Wilson's Theorem.

b) Let p be an odd prime. Show that

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Problem 5 : (4 points) Give the form of all positive integers n satisfying $\tau(n) = 10$.

Problem 6 : (8 points) In this problem we will show that if $n > 2$, $\varphi(n)$ is even.

a) Let $n = 2^k$ with $k \geq 2$. Show that in this case $\varphi(n)$ is even.

b) Now suppose that there is an odd prime p such that p divides n. Show that in this case also, $\varphi(n)$ is even.

Problem 7 : (10 points)

a) (4 points) Prove that the function

$$\sigma_3(n) = \sum_{d|n} d^3$$

is multiplicative.

b) (3 points) Show that for all n,

$$\sigma_3(n) \equiv \sigma(n) \pmod{3}.$$

c) (3 points) Give a closed formula (like the ones we gave for τ, σ and φ in class) for the value of $\sigma_3(n)$.
Hint: $1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$.