Math 255: Spring 2017
Final Exam

NAME:

Time: **2 hours and 45 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	4	
2	4	
3	10	
4	12	
5	9	
6	6	
7	12	
8	10	
9	8	
10	10	
11	5	
12	10	
TOTAL	100	

Problem 1 : (4 points) Please compute 7^{-1} modulo 23.

Problem 2 : (4 points) Prove that if a is odd, then

$$a^2 \equiv 1 \pmod 8.$$

Hint: What are the possibilities for $a \pmod 8$?

Problem 3 : (10 points)

a) (4 points) If $\gcd(a, n) = 1$, please give the definition of the (multiplicative) order of a modulo n.

b) (3 points) What is the order of 3 modulo 7?

c) (3 points) 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 $\mathrm{ind}_3\, 6$. This is exactly the same thing and you can just pretend this is what it says above.

Problem 4 : (12 points) For each of the following statements, state if it is true or false. **Justify each of your answers.** There will be partial credit for this question.

a) Let φ be the Euler-φ function from class. Then $\varphi(16) = \varphi(2)\varphi(8)$.

b) The system of linear congruences

$$\begin{aligned} x &\equiv 2 \pmod{12} \\ x &\equiv 6 \pmod{15} \end{aligned}$$

has a unique solution modulo $n = 12 \cdot 15 = 180$.

c) The equation

$$2x \equiv 4 \pmod{6}$$

has the unique solution $x \equiv 2 \pmod{6}$.

d) If $x \equiv 0 \pmod{2}$, then $x \equiv 2 \pmod{4}$.

Problem 5 : (9 points)

a) (4 points) Compute $\gcd(36, 102)$. You may use any technique you like, but you must justify your answer.

b) (5 points) Please give all integer solutions to the linear equation

$$36x + 102y = 12.$$

Problem 6 : (6 points) Consider the following system of simultaneous linear congruences:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ 2x &\equiv 1 \pmod 3 \\ 2x &\equiv 1 \pmod 5 \end{aligned}$$

a) (1 point) There is an integer n such that there is exactly one solution to this set of congruences in $\mathbb{Z}/n\mathbb{Z}$. What is the value of n?

b) (5 points) Solve this system of congruences.

Problem 8 : (10 points) Give all solutions to the following quadratic congruences.

a) $x^2 \equiv 7 \pmod{27}$

b) $x^2 \equiv 25 \pmod{40}$

Problem 9 : (8 points)

a) Give all of the lifts of

$$x \equiv 2 \pmod 5$$

to values in $\mathbb{Z}/10\mathbb{Z}$. In other words, if $x \equiv 2 \pmod 5$, what can x be modulo 10?

b) Show that any integer of the form $10k + 7$ is of the form $5j + 2$, but not conversely.

Problem 10 : (10 points) Let $\omega(1) = 0$ and, for $n > 1$ let $\omega(n)$ denote the number of distinct prime divisors of n. In other words, if $n = p_1^{k_1} \dots p_r^{k_r}$ is the factorization of n into distinct prime powers, $\omega(n) = r$.

a) Prove that $f(n) = 2^{\omega(n)}$ is multiplicative.

b) Prove that $\sum_{d|n} 2^{\omega(d)}$ is multiplicative.

Problem 11 : (5 points) Prove that $\varphi(n^2) = n\varphi(n)$.

Problem 12 : (10 points)

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

b) Let $p \equiv 3 \pmod 4$ be a prime. Let a be an integer such that $\gcd(a, p) = 1$ and assume that the equation

$$x^2 \equiv a \pmod p$$

has a solution. Show that

$$x \equiv a^{(p+1)/4} \pmod p$$

is a solution to this equation.