Math 255: Spring 2016
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	3	
2	4	
3	4	
4	3	
5	6	
6	12	
7	8	
8	10	
9	6	
10	8	
11	10	
12	18	
13	12	
TOTAL	100	

Problem 1 : (3 points) What is the order of 2 modulo 7?

Problem 2 : (4 points) What is 23^{-1} modulo 47?

Problem 3 : (4 points) What is the definition of a unit?

Problem 4 : (3 points) How many solutions does the equation $2x \equiv 0 \pmod 4$ have?

Problem 5 : (6 points) Consider the following theorem:

> Let the positive integer n be written as $n = N^2 m$, where m is square-free. Then n can be represented as the sum of two squares if m contains no prime factor of the form $4k + 3$.

a) (2 points) Among the statements below, circle **all** of those that are **hypotheses** of the theorem above.
Remember that a hypothesis is something that can be assumed to be true when proving the theorem.

i. n is a positive integer

ii. $n = N^2 m$ and m is square-free

iii. n can be represented as the sum of two squares

iv. m contains no prime factor of the form $4k + 3$.

b) (2 points) Among the statements below, circle **all** of those that are **conclusions** of the theorem above.
Remember that a conclusion is something that we are trying to show is true, given the hypotheses.

i. n is a positive integer

ii. $n = N^2 m$ and m is square-free

iii. n can be represented as the sum of two squares

iv. m contains no prime factor of the form $4k + 3$.

c) (2 points) Let $n = 63 = 3^2 \cdot 7$. Can n be written as a sum of two squares?

Problem 6 : (12 points)

a) (4 points) Compute $\gcd(66, 48)$. You may use any technique you like, but you must justify your answer.

b) (2 points) Based on your answer above, does the equation $66x + 48y = 12$ have solution(s) in the integers? Please justify with **one** sentence.

c) (6 points) Find all integer solutions of the equation $66x + 48y = 12$. You may use the back of any page if you need more space, but please indicate that you have done so so I can find your work.

Problem 7 : (8 points) Consider the following system of linear congruences:

$$
\begin{aligned}
2x &\equiv 1 \pmod{5}, \\
5x &\equiv 2 \pmod{7}.
\end{aligned}
$$

a) (6 points) Give the solution(s) to this system. Be careful to specify if your answer is an integer or an element of $\mathbb{Z}/n\mathbb{Z}$; in that latter case, say what n is.

b) (2 points) What is the smallest positive integer that is a solution of this system of linear congruences?

Problem 8 : (10 points) Compute the following Legendre symbols:

a) (5 points) $\left(\dfrac{-219}{373}\right)$

Hint: 219 is not a prime, but 373 is.

b) (5 points) $\left(\dfrac{137}{227}\right)$

Hint: Both 137 and 227 are prime.

Problem 9 : (6 points) Find all solutions, if any, to the equation

$$x^2 \equiv 21 \pmod{30}$$

Problem 10 : (8 points) Find all solutions, if any, to the following equations:

a) (4 points) $x^2 \equiv 9 \pmod{16}$

b) (4 points) $x^2 \equiv 21 \pmod{25}$

Problem 11 : (10 points) Note that $108 = 2^2 \cdot 3^3$.

a) (2 points) What is $\phi(108)$, where ϕ is the Euler-ϕ function from class?

b) (6 points) Show that if $\gcd(a, 108) = 1$, then $a^{18} \equiv 1 \pmod{108}$. There is more space for this problem on the following page.

Please continue your work from part b) here. Do not forget to answer part c) below.

c) (2 points) Does 108 have a primitive root? Please justify with **one** sentence.

Problem 12 : (18 points) The Liouville λ-function is defined in the following way:

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{k_1+k_2+\cdots+k_r} & \text{if } n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}. \end{cases}$$

a) (6 points) Prove that λ is multiplicative function.

Recall that we are discussing the function λ given by

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{k_1+k_2+\cdots+k_r} & \text{if } n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}. \end{cases}$$

Now let f be given by

$$f(n) = \sum_{d|n} \lambda(d).$$

b) (4 points) Compute the following values. **To receive credit for this part, you must use the formula above and you must show your work.** In particular, I expect to see as many terms as n has divisors.

i. $f(9)$

ii. $f(10)$

iii. $f(27)$

iv. $f(16)$

c) (2 points) Prove that f is a multiplicative function.

Recall that we are discussing the function λ given by

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{k_1+k_2+\cdots+k_r} & \text{if } n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, \end{cases}$$

and the function f given by

$$f(n) = \sum_{d|n} \lambda(d).$$

d) (6 points) Prove that

$$f(n) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m, \\ 0 & \text{otherwise.} \end{cases}$$

Problem 13 : (8 points)

a) (6 points) Let p be a prime that can be written in the form $p = 2^n + 1$. (For example, $17 = 2^4 + 1$ is such a prime.)
Show that for such a prime p, every quadratic nonresidue of p is a primitive root of p.

b) (2 points) Use the result above to find a primitive root of 17.