

Math 255: Spring 2016
Final Exam

NAME: SOLUTIONS

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?

It is the smallest positive integer k with

$$2^k \equiv 1 \pmod{7} :$$

$$2^1 \equiv 2 \not\equiv 1 \pmod{7}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{7}$$

$$2^3 \equiv 8 \equiv 1 \pmod{7}$$

2 has order 3 modulo 7

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

$$\gcd(23, 47) = 1 \text{ so } 23^{-1} \text{ exists}$$

$$47 = 2 \cdot 23 + 1$$

$$\text{so } 1 = 47 - 2 \cdot 23$$

$$-2 \cdot 23 \equiv 1 \pmod{47}$$

$$23^{-1} \equiv -2 \equiv 45 \pmod{47}$$

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

Let $a \in R$, R is a ring.

a is a unit if there is $b \in R$ with

$$ab = 1$$

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

Let's try all the x 's:

$2 \cdot 0 \equiv 0 \pmod{4}$	$x \equiv 0 \pmod{4}$
$2 \cdot 1 \equiv 2 \pmod{4}$	
$2 \cdot 2 \equiv 0 \pmod{4}$	$x \equiv 2 \pmod{4}$
$2 \cdot 3 \equiv 2 \pmod{4}$	

Two solutions, $x \equiv 0, 2 \pmod{4}$

Alternative solution:

$\gcd(2, 4) = 2$ and 2 divides 0, so 2

solutions

(The 2 lifts of $x \equiv 0 \pmod{2}$ which are

$$x \equiv 0 \pmod{4}$$

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

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

Let the positive integer n be written as $n = N^2m$, 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. $n = N^2m$ 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. $n = N^2m$ 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?

Here $N=3$, $m=7$

m is itself prime, its only prime factor is

$$7 = 4 \cdot 1 + 3$$

So no, 63 is not the sum of 2 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.

Euclidean algorithm:

$$66 = 48 + 18$$

$$48 = 2 \cdot 18 + 12$$

$$18 = 12 + 6$$

$$12 = 2 \cdot 6$$

$$\gcd(66, 48) = 6$$

Alternative solution:

$$66 = 2 \cdot 3 \cdot 11$$

$$48 = 2^4 \cdot 3$$

prime factors in common:

$$2 \cdot 3 = 6$$

$$\gcd(48, 66) = 6$$

- 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.

Yes because 6 divides 12.

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.

Step 1: Euclidean algorithm is done already

Step 2: Back solve:

$$\begin{aligned}6 &= 18 - 12 \\ &= 18 - (48 - 2 \cdot 18) = 3 \cdot 18 - 48 \\ &= 3 \cdot (66 - 48) - 48 = 3 \cdot 66 - 4 \cdot 48\end{aligned}$$

$$6 = 3 \cdot 66 - 4 \cdot 48 \quad x_0 = 3 \quad y_0 = -4$$

Step 3: Multiply by 2:

$$12 = 6 \cdot 66 - 8 \cdot 48 \quad x_p = 6 \quad y_p = -8$$

Step 4: Write all solutions

$$x = x_p + \frac{b}{\gcd(a,b)} t = 6 + 8t \quad t \in \mathbb{Z}$$

$$y = y_p - \frac{a}{\gcd(a,b)} t = -8 - 11t$$

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

$$2x \equiv 1 \pmod{5},$$

$$5x \equiv 2 \pmod{7}.$$

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.

This is a Chinese remainder Theorem question, first we get it in the right form

$$2 \cdot 3 \equiv 1 \pmod{5} \quad \text{so} \quad 3 \cdot 2x \equiv 3 \pmod{5}$$

$$5 \cdot 3 \equiv 1 \pmod{7} \quad \text{so} \quad 3 \cdot 5x \equiv 6 \pmod{7}$$

$$\boxed{\begin{array}{l} x \equiv 3 \pmod{5} \\ x \equiv 6 \pmod{7} \end{array}}$$

$$a_1 = 3 \quad N_1 = 7 \quad x_1 = 3$$

$$a_2 = 6 \quad N_2 = 5 \quad x_2 = 3$$

x_1 is such that $N_1 x_1 \equiv 1 \pmod{5}$ or $7x_1 \equiv 1 \pmod{5}$ or $2x_1 \equiv 1 \pmod{5}$
 $x_1 = 3$

x_2 is such that $N_2 x_2 \equiv 1 \pmod{7}$ or $5x_2 \equiv 1 \pmod{7}$, $x_2 = 3$

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 \pmod{35}$$

$$\equiv 3 \cdot 7 \cdot 3 + 6 \cdot 5 \cdot 3 \equiv 63 + 90 \equiv 153 \pmod{35}$$

$$(n=35)$$

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

$$153 \equiv 83 \equiv 13 \pmod{35}$$

13 is the least positive integer solution

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

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

$$30 = 2 \cdot 3 \cdot 5$$

• $x^2 \equiv 21 \pmod{2}$ this is $x^2 \equiv 1 \pmod{2}$

$$x \equiv 1 \pmod{2}$$

• $x^2 \equiv 21 \pmod{3}$ this is $x^2 \equiv 0 \pmod{3}$

$$x \equiv 0 \pmod{3}$$

• $x^2 \equiv 21 \pmod{5}$ this is $x^2 \equiv 1 \pmod{5}$

$$x \equiv 1 \pmod{5}$$

OR

$$x \equiv 4 \pmod{5}$$

We have 2 solutions, we use the Chinese Remainder Theorem to get them mod 30

$x \equiv 1 \pmod{2}$	$a_1 = 1$	$N_1 = 15$	$15x_1 \equiv x_1 \equiv 1 \pmod{2}$	$x_1 = 1$
$x \equiv 0 \pmod{3}$	$a_2 = 0$	$N_2 = 10$	$10x_2 \equiv x_2 \equiv 1 \pmod{3}$	$x_2 = 1$
$x \equiv 1 \pmod{5}$	$a_3 = 1$	$N_3 = 6$	$6x_3 \equiv x_3 \equiv 1 \pmod{5}$	$x_3 = 1$

$$x \equiv 15 + 0 + 6 \equiv 21 \pmod{30}$$

$x \equiv 1 \pmod{2}$
 $x \equiv 0 \pmod{3}$
 $x \equiv 4 \pmod{5}$

only difference is $a_3 = 4$
 everything else is the same

$$x \equiv 15 + 0 + 24 \equiv 39 \equiv 9 \pmod{30}$$

2 solutions:

$$x \equiv 9 \pmod{30}$$

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

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

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

Because 16 is a power of $p=2$ (even), we solve $x^2 \equiv 9 \equiv 1 \pmod{4}$ and lift directly to a solution mod 16 (we skip mod 8)

A solution to $x^2 \equiv 1 \pmod{4}$ is $x \equiv 1 \pmod{4}$. Therefore we lift $x_0 = 1$ to $x_1 = 1 + 4y_0$ such that $x_1^2 \equiv 9 \pmod{16}$.

$$x_1^2 = (1 + 4y_0)^2 = 1 + 8y_0 + 16y_0^2 \equiv 1 + 8y_0 \pmod{16}$$

So we solve $9 \equiv 1 + 8y_0 \pmod{16}$

$$8 \equiv 8y_0 \pmod{16}$$

$$\gcd(8, 16) = 8: 1 \equiv y_0 \pmod{2}$$

$$\text{So } x_1 = 1 + 4 = 5$$

This equation has four solutions:

$$x \equiv 5 \pmod{16}$$

$$x \equiv -5 \equiv 11 \pmod{16}$$

$$x \equiv 5 + 8 \equiv 13 \pmod{16}$$

$$x \equiv -13 \equiv 3 \pmod{16}$$

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

First we solve

$$x^2 \equiv 21 \equiv 1 \pmod{5}$$

This has solution

$$x \equiv 1 \pmod{5}$$

We lift $x_0 = 1$ to $x_1 = 1 + 5y_0$

where $x_1^2 \equiv 21 \pmod{25}$

$$x_1^2 = (1 + 5y_0)^2 = 1 + 10y_0 + 25y_0^2 \equiv 1 + 10y_0 \pmod{25}$$

So we solve $21 \equiv 1 + 10y_0 \pmod{25}$

$$20 \equiv 10y_0 \pmod{25}$$

$$\gcd(10, 25) = 5: 4 \equiv 2y_0 \pmod{5}$$

$$y_0 \equiv 2 \pmod{5} \quad 10$$

Alternate solution to part a):
By inspection $x \equiv 3 \pmod{16}$ is a solution
the other 3 are

$$x \equiv -3 \equiv 13 \pmod{16}$$

$$x \equiv 3 + 8 \equiv 11 \pmod{16}$$

$$x \equiv -11 \equiv 5 \pmod{16}$$

$$\text{So } x_1 = 1 + 5 \cdot 2 = 11$$

This equation has two solutions:

$$x \equiv 11 \pmod{25}$$

$$x \equiv -11 \equiv 14 \pmod{25}$$

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?

$$\begin{aligned}\phi(108) &= 108 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \\ &= 108 \cdot \frac{1}{2} \cdot \frac{2}{3} \\ &= 36\end{aligned}$$

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.

If $\gcd(a, 108) = 1$, then $\gcd(a, 4) = 1$. Since $\phi(4) = 2$, Euler's Theorem says that $a^2 \equiv 1 \pmod{4}$. Raising both sides to the 9^{th} power, $a^{18} \equiv 1 \pmod{4}$.

Similarly, $\gcd(a, 27) = 1$ as well. Since $\phi(27) = 27 - 9 = 18$, Euler's Theorem says that $a^{18} \equiv 1 \pmod{27}$

Now $\gcd(4, 27) = 1$, so by the Chinese Remainder Theorem we conclude that

$$a^{18} \equiv 1 \pmod{108}.$$

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.

No. Every element in $(\mathbb{Z}/108\mathbb{Z})^\times$ has order at most 18 by part b) and a primitive root would have order 36.

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

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

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

Let $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$
 $n = q_1^{l_1} q_2^{l_2} \dots q_s^{l_s}$ be 2 integers with

$\gcd(m, n) = 1$. Then

$$mn = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} q_1^{l_1} q_2^{l_2} \dots q_s^{l_s}$$

and all of these primes are distinct.

Then

$$\begin{aligned} \lambda(mn) &= (-1)^{k_1+k_2+\dots+k_r+l_1+l_2+\dots+l_s} \\ &= (-1)^{k_1+k_2+\dots+k_r} (-1)^{l_1+l_2+\dots+l_s} \\ &= \lambda(m) \lambda(n) \end{aligned}$$

Remark: λ is actually totally multiplicative but the argument is more annoying since we must allow for m and n to share prime factors.