Math 255: Spring 2016
Midterm 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	4	
2	5	
3	5	
4	8	
5	8	
6	8	
7	12	
TOTAL	50	

Problem 1 : (4 points) What is the order of 4 modulo 17?

$\varphi(17)=16$ so the order of 4 divides 16

$4^2=16\equiv -1 \mod 17$

$4^4\equiv(-1)^2\equiv 1 \mod 17$

4 has order 4 modulo 17.

Problem 2 : (5 points) What is 22^{-1} modulo 47?

Euclidean algorithm:

$47=2\cdot 22+3$ $\quad$ $3=47-2\cdot 22$

$22=7\cdot 3+1$ $\quad\rightarrow$ $1=22-7\cdot 3$

$1=22-7(47-2\cdot 22)$

$=22-7\cdot 47+14\cdot 22$

$=15\cdot 22-7\cdot 47$

So $22^{-1}\equiv 15 \mod 47$

Problem 3 : (5 points) It is a fact that 2 is a primitive root of 5. Here is a table of discrete logarithms in base 2 modulo 5:

a	1	2	3	4
$\log_2 a$	0	1	3	2

Note: In the book, the author talks about the "index of a relative to 2 modulo 5," and uses the symbol $\text{ind}_2\, a$. This is exactly the same thing and you can just pretend this is what it says above.

Use this table to solve the equation

$$3x^{15} \equiv 4 \pmod{5}.$$

Let $x = 2^k$ for $k = 0, 1, 2, 3$.

$$3(2^k)^{15} \equiv 4 \mod 5$$
$$2^3 \cdot 2^{15k} \equiv 2^2 \mod 5$$
$$2^{15k+3} \equiv 2^2 \mod 5$$

Taking $\log_2$:

$$15k+3 \equiv 2 \mod 4$$
$$-k+3 \equiv 2 \mod 4$$
$$-k \equiv -1 \mod 4$$
$$k \equiv 1 \mod 4$$

so $x \equiv 2 \mod 5$

Problem 4 : (8 points) Consider the following system of linear congruences:

$$2x \equiv 1 \pmod{3},$$
$$3x \equiv 2 \pmod{7}.$$

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.

Since $2 \cdot 2 \equiv 1 \bmod 3$, $2X \equiv 1 \bmod 3 \Rightarrow X \equiv 2 \bmod 3$

To find $3^{-1} \bmod 7$, do Eucl. alg: $7 = 2 \cdot 3 + 1$

So $1 = 7 - 2 \cdot 3$

and $3^{-1} \equiv -2 \equiv 5 \bmod 7$

$3X \equiv 2 \bmod 7 \Rightarrow X \equiv 10 \equiv 3 \bmod 7$

So $a_1 = 2$, $N_1 = 7$, solve $N_1 X_1 \equiv 1 \bmod 3$
$7X_1 \equiv 1 \bmod 3$
$X_1 \equiv 1 \bmod 3$
$X_1 = 1$

$a_2 = 3$, $N_2 = 3$, solve $N_2 X_2 \equiv 1 \bmod 7$
$3X_2 \equiv 1 \bmod 7$
$X_2 \equiv 5 \bmod 7$ by above
$X_2 = 5$.

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

$X = 17$ is the smallest positive integer.

So
$X \equiv 2 \cdot 7 \cdot 1 + 3 \cdot 3 \cdot 5 \bmod 21$
$\equiv 14 + 45 \bmod 21$
$\equiv 59 \bmod 21$
$\equiv 17 \bmod 21$

Problem 5 : (8 points) Note that $72 = 2^3 \cdot 3^2$.

a) (2 points) What is $\phi(72)$, where ϕ is the Euler-ϕ function we know and love?

$$\varphi(72) = 72 \cdot (1-\tfrac{1}{2})(1-\tfrac{1}{3}) = 72 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} = \tfrac{72}{3} = 24$$

b) (2 points) Show that if $\gcd(a, 8) = 1$, then $a^2 \equiv 1 \pmod 8$.

If $\gcd(a,8)=1$, then $a = 2n+1$ (a is odd)

Then $a^2 = (2n+1)^2 = 4n^2+4n+1$

$= 4n(n+1)+1$

Now $n(n+1)$ is even, since n or $n+1$ is even.

Say $n(n+1) = 2\ell$

$a^2 = 4 \cdot 2\ell + 1 = 8\ell + 1 \equiv 1 \mod 8$

Alternatively, if $\gcd(a,8)=1$, $a \equiv 1,3,5,7 \mod 8$

the square of each is $\equiv 1 \mod 8$

c) (4 points) Show that if $\gcd(a, 72) = 1$, then $a^6 \equiv 1 \pmod{72}$.

Hint: $\lambda(72) = \text{lcm}(2, \phi(9)) = 6$, where λ is the universal exponent function which we discussed in Homework 9.

If $\gcd(a,72)=1$, then $\gcd(a,8)=1$,
so $a^2 \equiv 1 \bmod 8$ and cubing both sides, $a^6 \equiv 1 \bmod 8$

If $\gcd(a,72)=1$, then $\gcd(a,9)=1$.
Since $\varphi(9) = 9-3=6$, by Euler's theorem
$a^6 \equiv 1 \bmod 9$.

Because $\gcd(8,9)=1$, we can apply the Chinese Remainder Theorem to conclude that $a^6 \equiv 1 \bmod 72$.

Problem 6 : (8 points)

a) (4 points) Let a be an odd integer that is divisible by 5. Show that the last digit of a is 5.

Proof #1:

$a \equiv 1 \mod 2$

$a \equiv 0 \mod 5$

$a_1 = 1,\ N_1 = 5,\ N_1 x_1 \equiv 1 \mod 2$

$\Rightarrow x_1 \equiv 1 \mod 2$

$a_2 = 0$ so N_2, x_2 don't matter

$x \equiv 5 \mod 10$

Proof #2: A multiple of 5 is of the form $a = 5n$ but if a is odd, n is odd,

So $a = 5(2m+1)$

$a = 10m + 5 \equiv 5 \mod 10$

b) (4 points) Let b be a power of 5 (i.e. $b = 5^n$ for some $n > 0$). Show that the last digit of b is 5.

Proof #1: A power of 5 is an odd multiple of 5 so by a) the last digit of b is 5.

Proof #2: Induction on n: Base case $5^1 = 5 \equiv 5 \mod 10$

Assume $5^{k-1} \equiv 5 \mod 10$

then $5^k = 5 \cdot 5^{k-1} \equiv 5 \cdot 5 \equiv 25 \equiv 5 \mod 10$

Problem 7 : (12 points) Throughout this problem, let $f\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ be given by the rule

$$f(n) = \sum_{d|n} \phi(d),$$

where ϕ is the Euler-ϕ again. If anything in this previous paragraph doesn't make sense, please ask for help.

a) (4 points) Using the definition given above, compute the values $f(n)$ below. **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. $f(9) = \varphi(1) + \varphi(3) + \varphi(9) = 1 + (3-1) + (9-3) = 9$

ii. $f(10) = \varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 10 \cdot \frac{1}{2} \cdot \frac{4}{5}$
$= 6 + 4 = 10$

iii. $f(27) = \varphi(1) + \varphi(3) + \varphi(9) + \varphi(27) = 1 + (3-1) + (9-3) + (27-9)$
$= 27$

iv. $f(16)$

$= \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) + \varphi(16) = 1 + (2-1) + (4-2) + (8-4) + (16-8) = 16$

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

Since φ is multiplicative and $f(n) = \sum_{d|n} \varphi(d)$ by a theorem proved in class f is also multiplicative.

Recall that in this problem, we define

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

c) (4 points) Prove that for all $n > 0$, $f(n) = n$.

Since f is multiplicative, if $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$
$f(n) = f(p_1^{k_1}) \ldots f(p_r^{k_r})$

It suffices thus to show that for any prime p, $k > 0$, $f(p^k) = p^k$. It will then follow that $f(n) = n$.

$$f(p^k) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^{k-1}) + \varphi(p^k)$$
$$= 1 + (p-1) + (p^2 - p) + \ldots + (p^{k-1} - p^{k-2}) + (p^k - p^{k-1})$$
$$= p^k$$

(the sum collapses)

d) (2 points) Use Möbius inversion to write $\phi(n)$ in terms of f.

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$