Math 255: Spring 2017
Exam 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	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.

The multiplicative order of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the smallest positive integer k such that $a^k \equiv 1 \mod n$

b) What is the order of 3 modulo 7?

$3^1 \equiv 3 \not\equiv 1 \mod 7$

$3^2 \equiv 9 \equiv 2 \not\equiv 1 \mod 7$

$3^3 \equiv 6 \not\equiv 1 \mod 7$

$3^4 \equiv 18 \equiv 4 \not\equiv 1 \mod 7$

$3^5 \equiv 12 \equiv 5 \not\equiv 1 \mod 7$

$3^6 \equiv 15 \equiv 1 \mod 7$

the order of 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$ is 6

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

$\log_3 6 \equiv x \mod 6$ ← exponents exist modulo $\varphi(7) = 6$ since 3 is a primitive root of 7

means

$3^x \equiv 6 \mod 7$

In part b) we see $3^3 \equiv 6 \mod 7$ so

$\log_3 6 \equiv 3 \mod 6$

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

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

We have $4 \equiv 2^2 \bmod 11$ if $x \equiv 2^k \bmod 11$
$3 \equiv 2^8 \bmod 11$ then $x^4 \equiv 2^{4k} \bmod 11$

The equation becomes

$$2^2 \cdot 2^{4k} \equiv 2^8 \bmod 11$$
$$2^{4k+2} \equiv 2^8 \bmod 11$$

Taking $\log_2$ on both sides we get

$4k+2 \equiv 8 \bmod 10$ OR $4k \equiv 6 \bmod 10$
$\nwarrow \varphi(11)=0$

Since $\gcd(4,10)=2$, 4 is not a unit mod 10 but we may divide all the way through by 2:

$2k \equiv 3 \bmod 5 \Rightarrow k \equiv 9 \equiv 4 \bmod 5$ since $2^{-1} \equiv 3 \bmod 5$

If $k \equiv 4 \bmod 5$ then $k \equiv 4$ OR $9 \bmod 10$

So 2 solutions: $x \equiv 2^4 \equiv 5 \bmod 11$
$x \equiv 2^9 \equiv 6 \bmod 11$

Problem 3 : (8 points)

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

Let p be a prime and $\gcd(a,p)=1$.

Then

$$a^{p-1} \equiv 1 \bmod p$$

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

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

Since $\gcd(p,q)=1$, we have

$$p^{q-1} \equiv 1 \bmod q$$
$$q^{p-1} \equiv 1 \bmod p$$

Also since $p-1 \geqslant 1$ and $q-1 \geqslant 1$,

$$p^{q-1} \equiv 0 \bmod p$$
$$q^{p-1} \equiv 0 \bmod q$$

So $p^{q-1} + q^{p-1} \equiv 1+0 \equiv 1 \bmod q$

$p^{q-1} + q^{p-1} \equiv 0+1 \equiv 1 \bmod p$

By the Chinese Remainder Theorem,

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

Problem 4 : (8 points)

a) State Wilson's Theorem.

Let p be a prime, then $(p-1)! \equiv -1 \bmod p$

(OR $(n-1)! \equiv -1 \bmod n$ if and only if n is prime)

b) Let p be an odd prime. Show that

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

$$1^2 3^2 5^2 \ldots (p-2)^2 \equiv 1 \cdot 3 \cdot 5 \ldots (p-2)\, 1 \cdot 3 \cdot 5 \ldots (p-2) \bmod p$$

$$\equiv 1 \cdot 3 \ldots (p-2) (-1)(p-1)(-1)(p-3) \ldots (-1)\, 2 \bmod p$$

Since $a \equiv (-1)(p-a) \bmod p$

$$\equiv \underbrace{1 \cdot 3 \cdot 5 \ldots (p-2)}_{\text{all odd}} \underbrace{(p-1)(p-3) \ldots 2}_{\text{all even}} (-1)^{\frac{p-1}{2}} \bmod p$$

$$\equiv (p-1)!\, (-1)^{\frac{p-1}{2}} \bmod p$$

$$\equiv (-1)(-1)^{\frac{p-1}{2}} \bmod p$$

$$\equiv (-1)^{\frac{p+1}{2}} \bmod p$$

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

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ then

$$\tau(n) = (k_1+1)(k_2+1)\ldots(k_r+1)$$

So if $\tau(n) = 10 = (k_1+1)(k_2+1)\ldots(k_r+1)$

↖ this is some way to factor 10

Note that $k_i \geq 1$ so $k_i + 1 \geq 2$

Factor 10 : $10 = 2 \cdot 5$ OR $10 = 10$

So either $10 = 2 \cdot 5 = (k_1+1)(k_2+1)$

i.e. $k_1 = 1$, $k_2 = 4$

$n = p_1 p_2^4$ (OR $n = p_1^4 p_2$ if you require $p_1 < p_2$)

OR $10 = k_1 + 1$ i.e. $k_1 = 9$

$n = p^9$

So n is of the form $n = p_1 p_2^4$ OR $n = p^9$

$p_1 \neq p_2$

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.

$$\varphi(2^k) = 2^k\left(1-\frac{1}{2}\right) = 2^{k-1} = 2 \cdot \underbrace{2^{k-2}}$$

this is an integer since $k \geq 2$

so $\varphi(2^k)$ is even if $k \geq 2$.

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.

We know that $p | n$, so $n = p^k m$, $k \geq 1$ $\gcd(p, m) = 1$

$\varphi(n) = \varphi(p^k)\varphi(m)$ by multiplicativity

$= (p^k - p^{k-1})\varphi(m)$

$= p^{k-1}(p-1)\varphi(m)$

Since p is odd, $p-1$ is even, say $p-1 = 2l$, $l \in \mathbb{Z}$

$$= 2\underbrace{\left(l p^{k-1} \varphi(m)\right)}$$

some integer since $\varphi(m) \in \mathbb{Z}$

So $\varphi(n)$ is even.

Problem 7 : (10 points)

a) (4 points) Prove that the function

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

is multiplicative.

Let $f(n) = n^3$. f is (totally) multiplicative:

$$f(mn) = (mn)^3 = m^3 n^3 = f(m)f(n)$$

Then by the Big Theorem (Theorem 6.4)

$\sigma_3(n) = \sum_{d|n} f(d) = \sum_{d|n} d^3$ is also multiplicative.

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

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

By the corollary to Fermat's Little Theorem,

$d^3 \equiv d \mod 3$ for <u>all</u> integers d

Then $\sigma_3(n) = \sum_{d|n} d^3 \equiv \sum_{d|n} d = \sigma(n) \mod 3$

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: $1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$.

Since σ_3 is multiplicative we first compute $\sigma_3(p^k)$ for p a prime, $k \geq 1$:

$$\sigma_3(p^k) = \sum_{d \mid p^k} d^3 = \sum_{j=0}^{k} (p^j)^3 = \sum_{j=0}^{k} (p^3)^j$$

This is a geometric sum with $r = p^3$

$$= \frac{(p^3)^{k+1} - 1}{p^3 - 1} = \frac{p^{3k+3} - 1}{p^3 - 1}$$

So now if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, we get

$$\sigma_3(n) = \sigma_3(p_1^{k_1})\, \sigma_3(p_2^{k_2}) \cdots \sigma_3(p_r^{k_r})$$

$$= \frac{p_1^{3k_1+1} - 1}{p_1^3 - 1} \; \frac{p_2^{3k_2+1} - 1}{p_2^3 - 1} \cdots \frac{p_r^{3k_r+1} - 1}{p_r^3 - 1}$$