Math 255: Spring 2018
Practice 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	12	
2	6	
3	8	
4	8	
5	8	
6	8	
GC	8	
TOTAL	50 (or 55)	

Problem 1 : (12 points) Solve the following equations. For each equation, give **all** distinct solutions (if there are more than one) and be sure to clearly indicate which ring the solutions belong to.

a) $4x \equiv 6 \pmod{18}$

$(4,18) = 2$ and $2 | 6$ ✓

$2x \equiv 3 \pmod{9}$ so $x \equiv 15 \equiv 6 \pmod{9}$

$2^{-1} \equiv 5 \pmod{9}$

$\boxed{x \equiv 6 \pmod{9}}$

b) $3x \equiv 2 \pmod{19}$

$(3,19) = 1$

because $3 \cdot 6 = 18 \equiv -1 \pmod{19}$

$3^{-1} \equiv -6 \equiv 13 \pmod{19}$

$x \equiv 2 \cdot 13 \equiv 26 \equiv 7 \pmod{19}$

$\boxed{x \equiv 7 \pmod{19}}$

c) $9x \equiv 7 \pmod{15}$

$(9,15) = 3$ but $3 \nmid 7$

$\boxed{\text{no solution}}$

Problem 2 : (6 points) Solve the following system of equations. Be sure to give **all** distinct solutions (if there are more than one) and to clearly indicate which ring the solution(s) belong to.

$$6x \equiv 6 \pmod{24}, \quad 3x \equiv 6 \pmod{9}, \quad 9x \equiv 7 \pmod{14}$$

$(6,24)=6$ and $6|6$

$\boxed{x \equiv 1 \pmod 4}$

$(3,9)=3$ and $3|6$

$\boxed{x \equiv 2 \pmod 3}$

$(9,14)=1$

$14 = 9+5$
$9 = 5+4$
$5 = 4+1$

$1 = 5-4$
$= 5-(9-5)$
$= 5-9+5 = 2\cdot 5 - 9$
$= 2(14-9)-9 = 2\cdot 14 - 3\cdot 9$

so $9^{-1} \equiv -3 \equiv 11 \pmod{14}$

$x \equiv -21 \pmod{14}$

$\boxed{x \equiv 7 \pmod{14}}$

$x \equiv 7 \bmod 14$ is equivalent to $x \equiv 7 \bmod 7$, $x \equiv 7 \bmod 2$ or $\boxed{\begin{array}{l} x \equiv 0 \bmod 7 \\ x \equiv 1 \bmod 2 \end{array}}$

$x \equiv 1 \pmod 2$ is implied by $x \equiv 1 \pmod 4$

so we solve $\boxed{x \equiv 1 \pmod 4 \quad x \equiv 2 \pmod 3 \quad x \equiv 0 \pmod 7}$

$M_1 = 3\cdot 7 = 21 \quad x_1 \equiv 21^{-1} \equiv 1^{-1} \equiv 1 \pmod 4$
$M_2 = 4\cdot 7 = 28 \quad x_2 \equiv 28^{-1} \equiv 1^{-1} \equiv 1 \pmod 3$
M_3 & x_3 don't matter since $a_3 = 0$

$x \equiv 1\cdot 21\cdot 1 + 2\cdot 28 \cdot 1 + 0 \pmod{84}$
$\equiv 21 + 56 \pmod{84}$
$\equiv 77 \pmod{84}$

$\boxed{x \equiv 77 \bmod 84}$

Problem 3 : (8 points) If p is a prime, show that for any integer a,

$$a^p + (p-1)!a \equiv 0 \pmod{p}.$$

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$,
So $a^p + (p-1)!a \equiv a^p - a \pmod{p}$

Now first let $(a,p)=1$. Then by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, So $a^p \equiv a \pmod{p}$ and $a^p - a \equiv 0 \pmod{p}$, which completes the proof.

If $(a,p) \neq 1$, then $(a,p)=p$ since the only positive divisors of p are 1 and p. If $(a,p)=p$, then $p \mid a$, and we have shown that this implies that $a \equiv 0 \pmod{p}$. Therefore

$$a^p - a \equiv 0^p - 0 \equiv 0 - 0 \equiv 0 \pmod{p}$$

In any case, $a^p + (p-1)!a \equiv 0 \pmod{p}$.

Problem 4 : (8 points) Find the remainder when 15! is divided by 17.

Since 17 is prime, by wilson's Theorem

$$16! \equiv -1 \pmod{17}$$

Notice that $16! = 15! \cdot 16$ and $16 \equiv -1 \pmod{17}$,

So

$$15! \equiv 16! \cdot 16^{-1} \pmod{17}$$

$$\equiv (-1)(-1) \pmod{17}$$

$$\equiv 1 \pmod{17}$$

Therefore 15! has remainder 1 when divided by 17

Problem 5 : (8 points) Show that $\sigma(n)$ is odd if and only if n is either a perfect square or twice a perfect square.

Lemma Let $n>1$ have prime-power decomposition $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. Then n is a perfect square if and only if e_i is even for $i=1,2\ldots k$.

proof: Suppose that $n=d^2$ for some $d\in\mathbb{Z}$ (i.e. n is a perfect square). Write $d=q_1^{f_1}q_2^{f_2}\cdots q_\ell^{f_\ell}$ for the prime-power decomposition of d. Then

$$n=(q_1^{f_1}q_2^{f_2}\cdots q_\ell^{f_\ell})^2=q_1^{2f_1}q_2^{2f_2}\cdots q_\ell^{2f_\ell}$$

and this is the prime-power decomposition of n since it is unique. Therefore $k=\ell$, without loss of generality $p_i=q_i$ for each i and $e_i=2f_i$ is indeed even.

Conversely, if each e_i is even, say $e_i=2f_i$ $f_i\in\mathbb{Z}$, then

$$n=p_1^{2f_1}p_2^{2f_2}\cdots p_k^{2f_k}=(p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k})^2 \quad \text{so } n=d^2$$

for $d=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$ and n is a perfect square. $\square$

Now let $n=p_1^{e_1}\cdots p_k^{e_k}$ as usual. Then

$$\sigma(n)=\frac{p_1^{e_1+1}-1}{p_1-1}\,\frac{p_2^{e_2+1}-1}{p_2-1}\cdots\frac{p_k^{e_k+1}-1}{p_k-1}$$

This is odd if and only if $\dfrac{p_i^{e_i+1}-1}{p_i-1}=1+p_i+p_i^2+\cdots+p_i^{e_i}$ is odd for each $i=1,2\ldots k$.

please turn over

If p_i is odd, the sum $1+p_i+p_i^2+\ldots+p_i^{e_i}$, which contains e_i+1 odd terms, is odd if and only if e_i+1 itself is odd (since a sum of an even number of odd terms is even). Therefore the sum is odd if and only if e_i is even.

If $p_i=2$, the sum $1+p_i+p_i^2+\ldots+p_i^{e_i}$ is always odd, so e_i can be even or odd.

Therefore $\sigma(n)$ is odd if and only if e_i is even for each p_i odd (each $p_i \neq 2$). This concludes the proof, because if all e_i's are even then n is a perfect square and if the power of 2 is odd then n is twice a perfect square.

Problem 6 : (8 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 $n = p_1^{e_1} \dots p_k^{e_k}$ is prime-power decomposition of n, then $\omega(n) = k$.

a) Give the definition of a multiplicative function.

Let f have as its domain the positive integers.
Then f is multiplicative if and only if

$(m,n)=1$ implies $f(mn)=f(m)f(n)$

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

Let $m,n \in \mathbb{Z}$, $m,n \geq 1$ be relatively prime.
Then their prime-power factorizations are

$m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ and $n = q_1^{f_1} q_2^{f_2} \dots q_\ell^{f_\ell}$ $(e_i \geq 1, f_i \geq 1)$

and $p_i \neq q_j$ for any i,j (no prime appears in both factorizations!)

Therefore the prime-power factorization of mn is

$mn = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} q_1^{f_1} q_2^{f_2} \dots q_\ell^{f_\ell}$ since all the primes are distinct

So we have $w(m) = k$, $w(n) = \ell$ and $w(mn) = k+\ell$

Then it follows that if $(m,n)=1$,

$f(mn) = 2^{w(mn)} = 2^{k+\ell} = 2^k \cdot 2^\ell = 2^{w(m)} 2^{w(n)} = f(m)f(n)$

Extra problem for graduate credit:

Problem 7 : (8 points) Let p be a prime of the form $p = 1 + 4k$. Show that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}.$$

By Wilson's Theorem $(p-1)! \equiv -1 \pmod{p}$

We have:

$$(p-1)! = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-2)(p-1)$$

$$\equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot -\left(p - \frac{p+1}{2}\right) \cdots -(p-(p-2)) - (p-(p-1)) \pmod{p}$$

$$\equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right) \cdots 2 \cdot 1 \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2$$

Since $p = 1+4k$, $\frac{p-1}{2} = \frac{1+4k-1}{2} = 2k$ is even

so $(-1)^{\frac{p-1}{2}} = 1$. Therefore

$$-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}$$