Math 255: Spring 2018
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	12	
4	10	
5	10	
GC	8	
TOTAL	50 (or 58)	

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) $5x \equiv 1 \pmod{13}$

$5^{-1} \equiv -5 \equiv 8 \pmod{13}$

$(5,13)=1$

$13 = 2 \cdot 5 + 3$
$5 = 3 + 2$
$3 = 2 + 1$

$1 = 3 - 2$
$= 3 - (5-3)$
$= 2 \cdot 3 - 5$
$= 2(13 - 2 \cdot 5) - 5$
$= 2 \cdot 13 - 5 \cdot 5$

so $\boxed{x \equiv 8 \pmod{13}}$

b) $10x \equiv 6 \pmod{15}$

$(10,15) = 5$ but $5 \nmid 6$

no solutions

c) $6x \equiv 3 \pmod{15}$

$(6,15) = 3$ and $3 \mid 3$ ✓

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

$2^{-1} \equiv 3 \pmod{5}$ so $\boxed{x \equiv 3 \pmod{5}}$

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.

$$2x \equiv 6 \pmod 8, \quad 2x \equiv 8 \pmod 9, \quad 3x \equiv 3 \pmod{18}$$

$(2,8)=2$ and $2|6$ ✓ $\quad (2,9)=1$ $\quad (3,18)=3$ and $3|3$ ✓

$x \equiv 3 \pmod 4$ $\quad 2^{-1} \equiv 5 \pmod 9$ $\quad x \equiv 1 \pmod 6$

$x \equiv 40 \equiv 4 \pmod 9$

this equation is equivalent to

$x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 3$

$x \equiv 1 \pmod 2$ is implied by $x \equiv 3 \pmod 4$ and $x \equiv 1 \pmod 3$ is implied by $x \equiv 4 \pmod 9$

So we solve $\boxed{x \equiv 3 \pmod 4 \quad x \equiv 4 \pmod 9}$

$M_1 = 9$ $\quad x_1 \equiv 9^{-1} \equiv 1^{-1} \equiv 1 \pmod 4$

$M_2 = 4$ $\quad x_2 \equiv 4^{-1} \equiv -2 \pmod 9$ since $4 \cdot 2 = 8 \equiv -1 \pmod 9$

So $x \equiv 3 \cdot 9 \cdot 1 + 4 \cdot 4 \cdot (-2) \pmod{36}$

$\equiv 27 - 32 \pmod{36}$

$\equiv -5 \equiv 31 \pmod{36}$

$\boxed{x \equiv 31 \pmod{36}}$

Problem 3 : (12 points)

a) State Fermat's Little Theorem (this theorem is also called Fermat's Theorem).

Let $a \in \mathbb{Z}$ and p be a prime. Then if $(a,p)=1$ then

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

b) If $(a, 35) = 1$, show that $(a, 5) = 1$ and $(a, 7) = 1$.

Note that if p is prime, $(a,p)=1$ or p since the only positive divisors of p are 1 and p.

Let $(a,35)=1$ and suppose to the contrary that $(a,5)=5$. Then $5 \mid a$, and since $5 \mid 35$ as well, $(a,35) \geq 5$, contradiction.

Similarly, if $(a,7)=7$, since $7 \mid 35$ this forces $(a,35) \geq 7$, contradiction

c) If $(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.

Consider first $a^{12} \pmod 5$.

Since $(a,5)=1$ by b), $a^4 \equiv 1 \pmod 5$

and therefore $a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \pmod 5$

Now consider $a^{12} \pmod 7$

Since $(a,7)=1$ by b), $a^6 \equiv 1 \pmod 7$

and therefore $a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod 7$

Therefore

$a^{12} \equiv 1 \pmod 5$ and $a^{12} \equiv 1 \pmod 7$

By the Chinese Remainder Theorem, this is equivalent to $a^{12} \equiv 1 \pmod{35}$

Problem 4 : (10 points)

a) State Wilson's Theorem.

Let p be a prime, then

$$(p-1)! \equiv -1 \pmod{p}$$

b) Find the remainder when 2(26!) is divided by 29.
Hint: 29 is a prime.

Since 29 is prime, we have $28! \equiv -1 \pmod{29}$

Notice that $28! = 26! \cdot 27 \cdot 28 \equiv 26!(-2)(-1) \pmod{29}$

So $-1 \equiv 28! \equiv 2 \cdot 26! \pmod{29}$

Therefore the remainder is 28

(a remainder must be positive!)

Problem 5 : (10 points)

a) Show that n is a perfect square (in other words, there is an integer d with $n = d^2$) if and only if in its prime-power factorization, given here by

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k},$$

each e_i is even.

Let $n=d^2$, $d\in\mathbb{Z}$, be a perfect square.
Write $d=q_1^{f_1}q_2^{f_2}\dots q_\ell^{f_\ell}$ for the prime-power factorization of d.

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

Since the prime-power factorization is unique, $k=\ell$ without loss of generality $p_i=q_i$ for each i and $e_i=2f_i$ is even for each i.

Now let each $e_i=2f_i$, $f_i\in\mathbb{Z}$, $f_i\geq 0$ be even

then $n=p_1^{2f_1}p_2^{2f_2}\dots p_k^{2f_k}=(p_1^{f_1}p_2^{f_2}\dots p_k^{f_k})^2$

so $n=d^2$ for $d=p_1^{f_1}p_2^{f_2}\dots p_k^{f_k}\in\mathbb{Z}$ and n is a perfect square.

b) Show that $d(n)$ is odd if and only if n is a perfect square.

As shown in class, if $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then

$$d(n) = (e_1+1)(e_2+1)\dots(e_k+1)$$

Therefore $d(n)$ is odd if and only if each e_i+1 is odd.

This is the case if and only if each e_i is even.

Finally, that is true if and only if n is a perfect square.

Extra problem for graduate credit:

Problem 6 : (8 points)

a) If n is odd, show that $\phi(2n) = \phi(n)$.

If n is odd, $(2, n) = 1$. Since φ is multiplicative,

$$\begin{aligned}\varphi(2n) &= \varphi(2)\varphi(n) \\ &= 2 \cdot \left(1 - \tfrac{1}{2}\right)\varphi(n) \\ &= \varphi(n)\end{aligned}$$

b) If n is even, show that $\phi(2n) = 2\phi(n)$.

Write $n = 2^k m$ with $(2, m) = 1$.

Then

$$\begin{aligned}\varphi(2n) &= \varphi(2^{k+1} m) \\ &= \varphi(2^{k+1})\varphi(m) \\ &= 2^{k+1}\left(1 - \tfrac{1}{p}\right)\varphi(m) \\ &= 2 \cdot 2^k \left(1 - \tfrac{1}{p}\right)\varphi(m) \\ &= 2 \cdot \varphi(2^k)\varphi(m) \\ &= 2\,\varphi(n)\end{aligned}$$