Math 255: Spring 2017
Exam 1

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	8	
2	6	
3	6	
4	6	
5	6	
6	6	
7	12	
TOTAL	50	

Problem 1 : (8 points)

a) (4 points) Give the definition of the word "unit," in the context of this class.

Let R be a ring.

An element $u \in R$ is a unit if there is

$v \in R$ with $uv = 1$.

b) (4 points) Compute 7^{-1} modulo 23.

$\gcd(7, 23) = 1$ so 7^{-1} exists modulo 23.

Euclidean algorithm

$23 = 3 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

Back solve

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3(23 - 3 \cdot 7) \\ &= 7 - 3 \cdot 23 + 9 \cdot 7 \\ &= 10 \cdot 7 - 3 \cdot 23 \end{aligned}$$

Since $1 = 10 \cdot 7 - 3 \cdot 23$, $10 \cdot 7 \equiv 1 \mod 23$

Therefore $7^{-1} \equiv 10 \mod 23$

Problem 2 : (6 points) Give all integer solutions to

$$24x + 40y = 16.$$

If there are no solutions, please state "None."

$a=24$
$b=40$
$c=16$

Step 1: Compute $\gcd(24,40)$

Euclidean algorithm

$40 = 1\cdot 24 + 16$

$24 = 1\cdot 16 + 8$

$16 = 2\cdot 8$

$\gcd(24,40) = 8$ $\quad 8 \mid 16$ so there are infinitely many solutions.

Step 2: Solve $24x+40y=8$

Back solve $\quad 8 = 24-16$

$= 24-(40-24)$

$= 24-40+24 = 2\cdot 24 - 40$

So $x_0 = 2 \quad y_0 = -1$

Step 3: Solve $24x+40y=16$

Since $24\cdot 2+40(-1)=8$, we have $2(24\cdot 2+40(-1))=16$

$24\cdot 4+40(-2)=16$

$x_p = 4 \quad y_p = -2$

Step 4: Formula for all integer solutions

$x = x_p + \dfrac{b}{\gcd(a,b)} t = 4+5t$

$t \in \mathbb{Z}$

$y = y_p - \dfrac{a}{\gcd(a,b)} t = -2-3t$

Problem 3 : (6 points) Give all solutions of this equation in the ring $\mathbb{Z}/102\mathbb{Z}$:

$$36x \equiv 8 \pmod{102}.$$

If there are no solutions, please state "None."

$a = 36$
$b = 8$
$n = 102$

gcd $(36, 102)$ using Euclidean algorithm:

$102 = 2 \cdot 36 + 30$
$36 = 1 \cdot 30 + 6$
$30 = 5 \cdot 6$

$\Rightarrow \gcd(102, 36) = 6$

$6 \nmid 8$ so there are no solutions to this congruence.

Problem 4 : (6 points) Show that the fourth power of any integer is either of the form $5k$ or $5k+1$ for $k \in \mathbb{Z}$.

Let $a \in \mathbb{Z}$. Then $a \equiv 0, 1, 2, 3$ or $4 \mod 5$.

If $a \equiv 0 \mod 5$, then $a^4 \equiv 0^4 \equiv 0 \mod 5$

$a \equiv 1 \mod 5$, then $a^4 \equiv 1^4 \equiv 1 \mod 5$

$a \equiv 2 \mod 5$, then $a^4 \equiv 2^4 \equiv 16 \equiv 1 \mod 5$

$a \equiv 3 \mod 5$, then $a^4 \equiv 3^4 \equiv 81 \equiv 1 \mod 5$

$a \equiv 4 \mod 5$, then $a^4 \equiv 4^4 \equiv (-1)^4 \equiv 1 \mod 5$

In any case, a^4 is congruent to either 0 or 1 modulo 5.

If $a^4 \equiv 0 \mod 5$ then $a^4 = 5k$ for some $k \in \mathbb{Z}$

$a^4 \equiv 1 \mod 5$ then $a^4 = 5k+1$ for some $k \in \mathbb{Z}$.

Problem 5 : (6 points) If $r \neq 1$, show that for every $n \geq 0$,

$$a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}.$$

Proof by induction

Base case: $n=0$

Then the left-hand side is a

Right-hand side is $\frac{a(r-1)}{r-1} = a$

$a=a$ so the base case is proved.

Induction step:

Assume that $a+ar+\ldots+ar^k = \frac{a(r^{k+1}-1)}{r-1}$

Then

$$a+ar+\ldots+ar^k+ar^{k+1} = (a+ar+\ldots+ar^k)+ar^{k+1}$$

$$= \frac{a(r^{k+1}-1)}{r-1} + ar^{k+1}\frac{(r-1)}{r-1}$$

$$= \frac{ar^{k+1}-a+ar^{k+2}-ar^{k+1}}{r-1}$$

$$= \frac{ar^{k+2}-a}{r-1} = \frac{a(r^{k+2}-1)}{r-1}$$

The induction step is proved, and the formula is true $\forall n \geq 0$.

Problem 6 : (6 points) Show that a divides b if and only if ac divides bc for all $c \neq 0$.

($\Rightarrow$) Assume that a divides b

Then by definition there is $k \in \mathbb{Z}$ with $b = ak$

Now let $c \in \mathbb{Z}$, $c \neq 0$.

$$b = ak \Rightarrow bc = akc = (ac)k$$

By definition, $ac \mid bc$

($\Leftarrow$) Assume that $ac \mid bc \quad \forall c \neq 0$

Let $c=1$. Then $a \mid b$.

Problem 7 : (12 points)

a) (4 points) Give all solutions of this equation in the ring $\mathbb{Z}/4\mathbb{Z}$:

$$2x \equiv 2 \pmod 4$$

$a=2$
$b=2$
$n=4$

$\gcd(2,4)=2$ and $2|2$, so there are 2 solutions.

Divide through by 2: $2x \equiv 2 \bmod 4$
$\rightsquigarrow x \equiv 1 \bmod 2$

Lift to $\mathbb{Z}/4\mathbb{Z}$: $x = 1+2t$, $t=0,1$

then $x \equiv 1 \bmod 4$ or $x \equiv 3 \bmod 4$

b) (6 points) Consider now the following set of simultaneous congruences:

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 2x &\equiv 2 \pmod 4 \\ 2x &\equiv 1 \pmod 5 \end{aligned}$$

Note that the middle congruence is the one you solved in part a).

There is an integer n such that there are exactly two solutions to this set of congruences in $\mathbb{Z}/n\mathbb{Z}$. Give this value of n and the two solutions.
Hint: Do the Chinese Remainder Theorem with each of the solutions for part a).

We first write these in the form $x \equiv a_i \bmod n_i$

$2x \equiv 1 \bmod 3$: Since $2^{-1} \equiv 2 \bmod 3$,

$2x \equiv 1 \bmod 3 \Rightarrow x \equiv 2 \bmod 3$

This problem is continued on the next page.

For your convenience, the set of congruences is

$$2x \equiv 1 \pmod 3$$
$$2x \equiv 2 \pmod 4$$
$$2x \equiv 1 \pmod 5$$

$2x \equiv 1 \mod 5$: Since $2^{-1} \equiv 3 \mod 5$,

$2x \equiv 1 \mod 5 \Rightarrow x \equiv 3 \mod 5$.

Then the two sets of congruences are

$x \equiv 2 \mod 3$ $x \equiv 2 \mod 3$ $a_1 = 2$ $n_1 = 3$ $N_1 = 20$

$x \equiv 1 \mod 4$ OR $x \equiv 3 \mod 4$ $a_2 = 1$ OR 3 $n_2 = 4$ $N_2 = 15$

$x \equiv 3 \mod 5$ $x \equiv 3 \mod 5$ $a_3 = 3$ $n_3 = 5$ $N_3 = 12$

x_1 is such that $20x_1 \equiv 1 \mod 3$ OR $2x_1 \equiv 1 \mod 3$. $x_1 = 2$ is a solution.

x_2 is such that $15x_2 \equiv 1 \mod 4$ OR $3x_2 \equiv 1 \mod 4$. $x_2 = 3$ is a solution

x_3 is such that $12x_3 \equiv 1 \mod 5$ OR $2x_3 \equiv 1 \mod 5$, $x_3 = 3$ is a solution.

Then $x \equiv 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \equiv 80 + 45 + 108 \equiv 53 \mod 60$

OR $x \equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \equiv 80 + 135 + 108 \equiv 23 \mod 60$

c) (2 points) What is the smallest positive integer that is a solution of this set of congruences? $\boxed{n = 60}$

$x = 23$