Math 255: Spring 2018
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	4	
2	4	
3	4	
4	6	
5	5	
6	6	
7	8	
8	6	
9	7	
GC	5	
TOTAL	50 (or 55)	

Problem 1 : (4 points) Compute $(143, 227)$. You may use any technique you like, but you must justify your answer to receive credit.

$227 = 143 + 84$

$143 = 84 + 59$

$84 = 59 + 25$

$59 = 25 \cdot 2 + 9$

$25 = 9 \cdot 2 + 7$

$9 = 7 + 2$

$7 = 2 \cdot 3 + 1$

$2 = 2 \cdot 1$

By the Euclidean Algorithm

$(143, 227) = 1$

Problem 2 : (4 points) Compute 13^{-1} modulo 15.

$15 = 13 + 2$

$13 = 2 \cdot 6 + 1$

$2 = 2 \cdot 1$

$1 = 13 - 2 \cdot 6$

$= 13 - (15 - 13) \cdot 6$

$= 13 - 6 \cdot 15 + 6 \cdot 13$

$= 7 \cdot 13 - 6 \cdot 15$

Since $7 \cdot 13 - 1 = 6 \cdot 15$,

$13^{-1} \equiv 7 \pmod{15}$

Problem 3 : (4 points) Of the equations below, circle all of the ones that have integer solutions.

You do not need to justify your answer to receive credit, but your justification will be taken into account to award partial credit if necessary.

a) $4x + 6y = 5$

$ax+by=c$ has integer Solutions iff $(a,b) \mid c$

$(4,6)=2 \nmid 5$

b) $2x + 3y = 7$

$(2,3)=1 \mid 7$

c) $7x + 14y = 1$

$(7,14)=7 \nmid 1$

d) $16x + 28y = 4$

$(16,28)=4 \mid 4$

Problem 4 : (6 points) Give all integer solutions to

$$6x + 14y = 6.$$

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

$(6,14) = 2 \mid 6$ so there will be solutions

$14 = 2 \cdot 6 + 2$ so $2 = 14 - 2 \cdot 6$

$6 = 3 \cdot 2$

$x_0 = -2 \quad y_0 = 1$

and $6 = 3 \cdot 14 - 6 \cdot 6$

$x_p = -6 \quad y_p = 3$

The general solution is

$$x = -6 + 7t$$
$$y = 3 - 3t \qquad t \in \mathbb{Z}$$

check: $6(-6+7t) + 14(3-3t)$

$= -36 + 42t + 42 - 42t$

$= 42 - 36 = 6$

Problem 5 : (5 points)

a) (3 points) Let a, b and m be integers, with $m > 1$. Give the definition of the expression

$$a \equiv b \pmod{m}.$$

$a \equiv b \pmod{m}$ iff m divides $a-b$

b) (2 points) Let a and m be integers, with $m > 1$. Show that m divides a if and only if $a \equiv 0 \pmod{m}$.

$a \equiv 0 \pmod{m}$ iff m divides $a-0=a$

Problem 6 : (6 points) It is a theorem that:

Every integer a is congruent $\pmod{m}$ to exactly one of $0, 1, \ldots, m-2, m-1$.

Furthermore, we call this integer the *least residue of* $a \pmod{m}$.
Perform each of the following operations, and **give your answer as the least residue.** For example, the answer to

$$3 \times 4 \pmod{8}$$

should be 4 (and not 12, although those are congruent modulo 8, since 12 is not a least residue modulo 8).

a) $8 + 9 \pmod{12}$

$8+9=17 \equiv 5 \pmod{12}$

b) $-5-7 \pmod{9}$

$-5-7=-12 \equiv 6 \pmod{9}$

c) $8 \times 6 \pmod{11}$

$8 \cdot 6 = 48 \equiv 4 \pmod{11}$

Problem 7 : (8 points)

a) (4 points) Let n be an **odd** number (this means that there is an integer k such that $n = 2k + 1$).
List all of the possible least residues for $n \pmod 8$.

Let $n = 2k+1$. Let's see what n can be as k ranges over all of the possibilities mod 8

k	$n = 2k+1 \pmod 8$
0	$n \equiv 1 \pmod 8$
1	$n \equiv 3 \pmod 8$
2	$n \equiv 5 \pmod 8$
3	$n \equiv 7 \pmod 8$
4	$n \equiv 9 \equiv 1 \pmod 8$
5	$n \equiv 11 \equiv 3 \pmod 8$
6	$n \equiv 13 \equiv 5 \pmod 8$
7	$n \equiv 15 \equiv 7 \pmod 8$

n can be $1, 3, 5, 7 \pmod 8$

b) (4 points) If n is odd, list all of the possible least residues for $n^2 \pmod 8$.

n	$n^2 \pmod 8$
1	$n^2 \equiv 1 \pmod 8$
3	$n^2 \equiv 9 \equiv 1 \pmod 8$
5	$n^2 \equiv 25 \equiv 1 \pmod 8$
7	$n^2 \equiv 49 \equiv 1 \pmod 8$

n^2 can only be $1 \pmod 8$

Problem 8 : (6 points) Use induction on n to show that

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

for each integer $n \geq 1$.

Base case: $n=1$ $\quad \sum_{i=1}^{1} i^3 = 1$

$$\left(\frac{1 \cdot 2}{2}\right)^2 = 1$$

✓

Now assume that for some $k \geq 1$,

$$\sum_{i=1}^{k} i^3 = \left(\frac{k(k+1)}{2}\right)^2$$

Then

$$\sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3$$

$$= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$$

$$= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4}$$

$$= \frac{(k+1)^2(k^2+4k+4)}{4} = \frac{(k+1)^2(k+2)^2}{4}$$

$$= \left(\frac{(k+1)(k+2)}{2}\right)^2$$

So the claim follows by induction

Problem 9 : (7 points)

a) (3 points) Give the definition of *prime*.

Def ①: $p \in \mathbb{Z}$, $p > 1$ is a prime if its only positive divisors are 1 and itself

Def ② $p \in \mathbb{Z}$, $p > 1$ is a prime if $p | ab$ implies $p | a$ or $p | b$.

b) (4 points) How many primes are there that have the last digit 5? Justify your answer.

Suppose that p is a prime and its last digit is 5. This means that there is $k \in \mathbb{Z}$ with

$$p = 5 + 10k$$

Then $p = 5(1+2k)$ and 5 divides p.

Since the only positive divisors of p are 1 and itself, $p = 5$ and there is only one prime with last digit 5.

Extra problem for graduate credit:

Problem 10 : (5 points) In this question, you will show that:

If $(a, b) = 1$, then $(a + b, a - b) = 1$ or 2.

a) (2 points) Show that $(a + b, a - b) \leq (2a, 2b)$.

Let $d = (a+b, a-b)$. Then there are $s, t \in \mathbb{Z}$ with

$a+b = ds$ and $a-b = dt$. Therefore

$2a = (a+b) + (a-b) = ds + dt = \underbrace{d(s+t)}_{s+t \in \mathbb{Z}}$ so $d \mid 2a$

and

$2b = (a+b) - (a-b) = ds - dt = \underbrace{d(s-t)}_{s-t \in \mathbb{Z}}$ so $d \mid 2b$

Therefore d is a common divisor of $2a$ and $2b$ and by definition $d \leq (2a, 2b)$.

b) (2 points) Show that if $(a, b) = 1$, then $(2a, 2b) = 2$.

First, since $2 \mid 2a$ and $2 \mid 2b$, certainly $2 \leq (2a, 2b)$.

Now let $c \mid 2a$ and $c \mid 2b$.

If c is odd, then $(2, c) = 1$ so $c \mid a$ and $c \mid b$

So $c \leq (a, b) = 1$

If c is even, say $c = 2r$, then since $c \mid 2a$ and $c \mid 2b$ there are $s, t \in \mathbb{Z}$ with $2a = cs = 2rs$ or $a = rs$ and $2b = ct = 2rt$ or $b = rt$ and

$r \leq (a, b) = 1$ so $c = 2r \leq 2$.

Since all common divisors of $2a$ and $2b$ are ≤ 2, $(2a, 2b) = 2$

c) (1 point) Assuming parts a) and b) (even if you did not prove them), conclude that if $(a, b) = 1$, then $(a+b, a-b) = 1$ or 2.

We have that

$$1 \leq (a+b, a-b) \overset{\text{part a)}}{\leq} (2a, 2b) \overset{\text{part b)}}{=} 2$$

since it is a gcd

So $(a+b, a-b)$ is an integer between 1 and 2 and so must be 1 or 2.