Name: SOLUTIONS

Number Theory for Teachers–Midterm 1

For full credit, all work must be shown and clearly presented. No calculators.

1	
2	
3	
4	

1. (5 points each)

a. Find the GCD of 761 and 252.

$$\begin{array}{l} 761 \\ 756 \end{array}$$

$$\begin{aligned} 761 &= 252 \cdot 3 + 5 \\ 252 &= 5 \cdot 50 + 2 \\ 5 &= 2 \cdot 2 + \boxed{1} \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

The GCD of 761 and 252 is 1.

b. Write $\frac{761}{252}$ as a simple continued fraction.

$$\frac{761}{252} = 3 + \cfrac{1}{50 + \cfrac{1}{2 + \cfrac{1}{2}}}$$

(Numbers from the Euclidean algorithm).

c. Find ***two distinct*** integral solutions to the equation $761x + 252y = 3$.

		3	50	2	2	
0	1	3	151	305	761	
1	0	1	50	101	252	

$761 \cdot 101 - 252 \cdot 305 = 1$

So $761 \cdot 303 - 252 \cdot 915 = 3$

One solution: $\boxed{x = 303,\ y = -915.}$

To find a second solution, add 761 to -915 and subtract 252 from 303

Second solution: $\boxed{x = 51,\ y = -154}$

d. What is the multiplicative inverse of 252 in $\mathbb{Z}_{761}$?

In $\mathbb{Z}_{761}$, we have $-252 \cdot 305 = 1$,

So the multiplicative inverse of 252 is -305, or 356.

2. Find the following in $\mathbb{Z}_{13}$. For any expressions with multiple values, be sure to give all possible values. (2 points each)

   i. -3

   ii. $10 \cdot 5$

   iii. $\frac{1}{3}$

   iv. $\sqrt{-1}$

   v. $\sqrt[4]{3}$

i. $-3 \equiv 13-3 = 10$ in $\mathbb{Z}_{13}$

ii. $10 \cdot 5 = 50 \equiv -2$ (since $52 = 13 \cdot 4$)

$\equiv 11$ mod 13.

iii Want $3x \equiv 1$ mod 13

Guess and check gives $x = 9$ ($3 \cdot 9 = 27 \equiv 1$ mod 13).

So $\frac{1}{3} = 9$ in $\mathbb{Z}_{13}$.

iv $\sqrt{-1}$: Check

$$\begin{aligned} 0^2 &= 0 \\ 1^2 = 12^2 &= 1 \\ 2^2 = 11^2 &= 4 \\ 3^2 = 10^2 &= 9 \\ 4^2 = 9^2 &= 3 \\ 5^2 = 8^2 &= 12 \leftarrow 12 \equiv -1 \text{ in } \mathbb{Z}_{13}. \\ 6^2 = 7^2 &= 10 \end{aligned}$$

So the square roots of -1 are 5 and 8.

v. $\sqrt[4]{3}$ Want $(x^2)^2 = 3$.

$4^2 = 9^2 = 3$. and $2^2 = 11^2 = 4$ and $3^2 = 10^2 = 9$.

So $\sqrt[4]{3}$ are 2, 11, 3 and 10.

3. For which a in $\mathbb{Z}$ can you find $\frac{1}{a}$ in $\mathbb{Z}_m$? Explain. (10 points)

We can find $\frac{1}{a}$ in $\mathbb{Z}_m$ when $(a, m) = 1$.

If $\frac{1}{a} \in \mathbb{Z}_m$, then we can solve $ax \equiv 1 \mod m$

But this is equivalent to solving $ax + my = 1$ over the integers.

We can solve $ax + my = 1$ exactly when a and m are relatively prime. (That is, if $(a, m) = 1$, we can find integers x and y such that $ax + my = 1$ and if $(a, m) \neq 1$, we can't find x and y integers such that $ax + my = 1$). Therefore, we can solve $ax \equiv 1 \mod m$ exactly when $(a, m) = 1$, and we can find $\frac{1}{a}$ in $\mathbb{Z}_m$ if $(a, m) = 1$ and we can't find $\frac{1}{a}$ in $\mathbb{Z}_m$ if $(a, m) \neq 1$.

4. Using the definitions and axioms from class, prove that if $a \mid b$ and $a \mid c$, then $a \mid (bx+cy)$. (10 points)

Given: $a|b$ and $a|c$.

By the definition of divides, this means

$b = ak$ and $c = al$ for some integers k, l.

Then $bx = (ak)x$ and $cy = (al)y$

So
$$\begin{aligned} bx + cy &= (ak)x + (al)y \\ &= a(kx) + a(ly) \quad \text{(associativity)} \\ &= a(kx + ly) \quad \text{(distributivity)}. \end{aligned}$$

Since k, x, l, y are integers, $kx + ly$ is an integer ($\mathbb{Z}$ is closed under $+$ and $\cdot$).

Thus, by the definition of divides, $a | bx + cy$.