Name: Solutions

Number Theory for Teachers–Practice Exam 1

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

1	
2	
3	
4	
5	

1. (5 points each)

a. Find the GCD of 654 and 163.

$$\begin{array}{r} 163 \\ \times\ 4 \\ \hline 652 \end{array}$$

$$654 = 163 \cdot 4 + 2$$
$$163 = 2 \cdot 81 + \boxed{1}$$
$$2 = 1 \cdot 2 + 0$$

The GCD of 654 and 163 is 1.

b. Write $\frac{654}{163}$ as a simple continued fraction.

$$\frac{654}{163} = 4 + \frac{2}{163}$$
$$= 4 + \frac{1}{\frac{163}{2}}$$
$$= \boxed{4 + \frac{1}{81 + \frac{1}{2}}}$$

c. Find ***all*** integral solutions to the equation $654x + 163y = 1$.

		4	81	2
0	1	4	325	654
1	0	1	81	163

$163 \cdot 325 - 654 \cdot 81 = 1.$

So one solution is $x = -81$, $y = 325$.

All solutions: $x = -81 + 163k$
$y = 325 - 654k$, where $k \in \mathbb{Z}$.

d. What is the multiplicative inverse of 163 in $\mathbb{Z}_{654}$?

Since $163 \cdot 325 - 654 \cdot 81 = 1$,

$163 \cdot 325 \equiv 1 \mod 654.$

Thus, the multiplicative inverse of 163 is 325 in $\mathbb{Z}_{654}$.

2. Characterize the elements of U_m and justify your characterization. (10 points)

Elements of U_m are the numbers a in $\mathbb{Z}_m$ where $(a, m) = 1$.

For a to be invertible in $\mathbb{Z}_m$, there must be some element x so that $ax \equiv 1 \bmod m$.

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

We can solve $ax + my = 1$ in $\mathbb{Z}$ if $(a, m) = 1$ and we can't solve it if $(a, m) \neq 1$.

Therefore, a is invertible in $\mathbb{Z}_m$ exactly when $(a, m) = 1$.

3. Find the following in $\mathbb{Z}_{17}$. For any expressions with multiple values, be sure to give all possible values. (2 points each)

i. -4

ii. $10 \cdot 4$

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

iv. $\sqrt{-1}$

v. $\sqrt[3]{10}$

i. In $\mathbb{Z}_{17}$, $-4 = 13$.

ii. In $\mathbb{Z}_{17}$, $10 \cdot 4 = 40 \equiv 6$

iii. In $\mathbb{Z}_{17}$, since $18 = 1$, $\frac{1}{3} = 6$.

iv. In $\mathbb{Z}_{17}$, $-1 = 16$, so one square root of -1 is 4.
The other is $-4 = 13$.

v. $\sqrt[3]{10}$: We're looking for x such that $x^3 = 10$.

$0^3 = 0$
$1^3 = 1$
$2^3 = 8$
→ $3^3 = 10$
$4^3 = 16 \cdot 4 = -4 = 13$
$5^3 = 8 \cdot 5 = 6$
$6^3 = 36 \cdot 6 = 2 \cdot 6 = 12$
$7^3 = 49 \cdot 7 = 15 \cdot 7 = (-2) \cdot 7 = -14 = 3$
$8^3 = 64 \cdot 8 = 13 \cdot 8 = (-4) \cdot 8 = 2$
$9^3 = (-8)^3 = -2 = 15$
$10^3 = (-7)^3 = -3 = 14$
$11^3 = (-6)^3 = -12 = 5$
$12^3 = (-5)^3 = -6 = 11$
$13^3 = (-4)^3 = -13 = 4$
$14^3 = (-3)^3 = -10 = 7$
$15^3 = (-2)^3 = -8 = 9$
$16^3 = (-1)^3 = -1 = 15$

So $\sqrt[3]{10} = 3$ in $\mathbb{Z}_{17}$.

4. Using the definition that $a \equiv b \mod m$ means $m \mid a - b$ and any other definitions and axioms from class, prove that if $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$. (10 points)

Given: $a \equiv b \mod m$ and $c \equiv d \mod m$.

By the given definition, this means

$m \mid a-b$ and $m \mid c-d$.

By the definition of divides,

$a-b = mk$ and $c-d = ml$ for some $k, l \in \mathbb{Z}$.

Then, adding these equations together, we get

$$(a-b)+(c-d) = mk + ml$$
$$= m(k+l)$$ by the distributive law.

But also $(a-b)+(c-d) = (a+c)-(b+d)$ using the associative and commutative laws.

So $(a+c)-(b+d) = m(k+l)$.

$k+l$ is in $\mathbb{Z}$ since $k, l \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition.

Thus, by the definition of divides, $m \mid (a+c)-(b+d)$, and by definition,

$a+c \equiv b+d \mod m$.