MATH 405: Assignment 4

Micah Sherry

March 7, 2025

1. Find the smallest positive solution to the system of congruences.

$$x \equiv 4 \bmod 7$$
$$x \equiv 5 \bmod 11$$
$$x \equiv 2 \bmod 16$$
$$x \equiv 1 \bmod 19$$

$$M = 7 \cdot 11 \cdot 16 \cdot 19 = 23408$$
$$M_1 = 11 \cdot 16 \cdot 19 = 3344$$
$$M_2 = 7 \cdot 16 \cdot 19 = 2128$$
$$M_3 = 7 \cdot 11 \cdot 19 = 1463$$
$$M_4 = 7 \cdot 11 \cdot 16 = 1232$$

$$M_1 b_1 \equiv 1 \bmod 7$$
$$5 b_1 \equiv 1 \bmod 7$$
$$1 = 3(5) - 2(7)$$
Therefore $b_1 \equiv 3 \bmod 7$

$$M_3 b_3 \equiv 1 \bmod 16$$
$$7 b_3 \equiv 1 \bmod 16$$
$$1 = 7(7) - 3(16)$$
Therefore $b_3 \equiv 7 \bmod 16$

$$M_2 b_2 \equiv 1 \bmod 11$$
$$5 b_2 \equiv 1 \bmod 11$$
$$1 = -2(5) - (11)$$
Therefore $b_2 \equiv -2 \equiv \bmod 11$

$$M_4 b_4 \equiv 1 \bmod 19$$
$$16 b_4 \equiv 1 \bmod 19$$
$$1 = 6(16) - 5(19)$$
Therefore $b_4 \equiv 6 \bmod 19$

$$x_0 = 4M_1 b_1 + 5M_2 b_2 + 2M_3 b_3 + 1M_4 b_4$$
$$= 4(3344)(3) + 5(2128)(9) + 2(1463)(7) + 1(1232)(6)$$
$$= 163762$$

$$x_k = x_0 + kM \text{(where k is some integer)}$$
$$x_{-6} = 23314 \text{ is the smallest positive value for x.}$$

2. Consider the set $\mathbb{Z}_3[i] = \{a + bi \,|\, a, b \in \mathbb{Z}_3\}$ where $i = \sqrt{-1}$.

(a) find all the elements of $\mathbb{Z}_3[i]$. How many are there?
Notice there are 3 choices for a and 3 for b, so $\mathbb{Z}_3[i]$ has 9 elements.
$0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i$

(b) $1 + 2i \in \mathbb{Z}_3[i]$ has a multiplicative inverse in find it.

$$(1 + 2i)(2 + 2i) =$$
$$= 2 + 4i + 2i + 4i^2$$
$$= 2 - 4$$
$$= -2$$
$$= 1$$

Therefore $(2 + 2i)$ is the multiplicative inverse of (1+2i).

(c) Classify each nonzero element of $\mathbb{Z}_3[i]$ as a unit, a zero divisor or neither.

Number	Inverse	classification
0	NA	Neither
1	1	unit
2	2	unit
i	2i	unit
1+i	2+i	unit
2+i	1+i	unit
2i	i	unit
1 +2i	2i+2	unit
2+2i	1+2i	unit

3. let R be a ring and let S and T be subrings or R. Let $M = S \cap T$. Show that M is a subring of R

Proof. Let S and T be subrings of a Ring R. And Let $M = S \cap T$.
To show M is a subring we need to show that $0, 1 \in M$, M is closed under addition and multiplication, and if $a \in M$ then $-a \in M$

Since S is a subring $0 \in S$. Similarly, T is a subring $0 \in T$. Therefore $0 \in M$.

Since S is a subring $1 \in S$. Similarly, T is a subring $1 \in T$. Therefore $1 \in M$.

Let $a, b \in M$. Since, $a, b \in S$ since S is a subring $a + b \in S$
Similarly, $a, b \in T$ since T is a subring $a + b \in T$
Therefore $a + b \in M$ Thus M is closed under addition.

Let $a, b \in M$. Since, $a, b \in S$ since S is a subring $a \cdot b \in S$
Similarly, $a, b \in T$ since T is a subring $a \cdot b \in T$
Therefore $a \cdot b \in M$ Thus M is closed under multiplication.

Let $a \in M$. Since, $a \in S$ since S is a subring $-a \in S$
Similarly, $a \in T$ since T is a subring $-a \in T$
Therefore if $a \in M$ then $-a \in M$.
Therefore M is a Subring of R $\qquad \square$

4. Let R be a ring (not necessarily commutative).
Let $a, b \in R$, prove that $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Proof. Let R be a ring and let $a, b \in R$. And assuming a^{-1}, b^{-1} exist. Consider:
$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} \qquad \text{(by associativity of R)}$$
$$= a \cdot 1 \cdot a^{-1} \qquad \text{(by definition of multiplicative inverse)}$$
$$= a \cdot a^{-1} \qquad \text{(by definition of multiplicative identity)}$$
$$= 1 \qquad \text{(by definition of multiplicative inverse)}$$

Therefore $(b^{-1} \cdot a^{-1})$ is the multiplicative inverse of $(a \cdot b)$ $\square$

Extra Credit: let R be a ring (not necessarily commutative).
If for any $a, b \in R$, $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ then show that R is commutative.

Proof. Let $a, b \in R$. Assume a^{-1}, b^{-1} exist and $(a \cdot b)^{-1} = (a^{-1} \cdot b^{-1})$. from proof of problem 4 we have $(a \cdot b)^{-1} = (b^{-1} \cdot a^{-1})$. So,

$$
\begin{aligned}
(a^{-1} \cdot b^{-1}) &= (b^{-1} \cdot a^{-1}) & \\
b^{-1} &= a \cdot (b^{-1} \cdot a^{-1}) & \text{(left multiply by a)} \\
1 &= b \cdot a \cdot (b^{-1} \cdot a^{-1}) & \text{(left multiply by b)} \\
a &= b \cdot a \cdot b^{-1} & \text{(right multiply by a)} \\
a \cdot b &= b \cdot a & \text{(right multiply by b)}
\end{aligned}
$$

Therefore since $b \cdot a = a \cdot b$, R is commutative. $\square$