110A HW2

Warren Kim

Winter 2024

Question 1

Let $n \in \mathbb{Z}$ be positive. Show that n is divisible by 9 if and only if the sum of the digits of n (in base 10) is divisible by 9.

Response

Proof: ($\implies$) Suppose n is divisible by 9. Let $n = n_0 + n_1 10^1 + \cdots + n_k 10^k$ be the string representation of n where n_i is a digit from 0 to 9. Then

$$\begin{aligned} n &\equiv 0 \pmod 9 \\ n_0 + n_1 10^1 + \cdots + n_k 10^k &\equiv 0 \pmod 9 \\ n_0 + n_1 1^1 + \cdots + n_k 1^k &\equiv 0 \pmod 9 && 10 \equiv 1 \pmod 9 \\ n_0 + n_1 + \cdots + n_k &\equiv 0 \pmod 9 \end{aligned}$$

So the sum of the digits of n is divisible by 9.

($\impliedby$) Suppose the sum of the digits of n is divisible by 9. Let $n = n_0 + n_1 10^1 + \cdots + n_k 10^k$ be the string representation of n where n_i is a digit from 0 to 9. Then

$$\begin{aligned} n &\equiv 0 \pmod 9 \\ n_0 + n_1 + \cdots + n_k &\equiv 0 \pmod 9 \\ n_0 + n_1 1^1 + \cdots + n_k 1^k &\equiv 0 \pmod 9 \\ n_0 + n_1 10^1 + \cdots + n_k 10^k &\equiv 0 \pmod 9 && 1 \equiv 10 \pmod 9 \end{aligned}$$

So n is divisible by 9. $\square$

Question 2

Let $[a] \in \mathbb{Z}/n$ be nonzero. Show that precisely one of the follow hold:

1. There exists nonzero $[b] \in \mathbb{Z}/n$ such that $[a][b] = [0]$.
2. There exists $[c] \in \mathbb{Z}/n$ such that $[a][c] = [1]$.

[hint: think about (a, n).]

Response

Proof: Suppose $[a] \in \mathbb{Z}/n$ is nonzero. There are two cases:

Case i: If $(a, n) \neq 1$, then $ax + ny = d$ for some $x, y, d \in \mathbb{Z}$ where $d \neq 1$. We can write $[ab + ny] = [ab] + [ny] = [d]$. But since $[ny] = [n][y] = [0]$, we have $[ab] = [a][b] = [d]$. Recall that $d|n$. Then we can write $d = nm$ for some $m \in \mathbb{Z}$. Then $[a][b] = [nm] = [0]$, so there exists $[b] \in \mathbb{Z}/n$ such that $[a][b] = [0]$.

Case ii: If $(a, n) = 1$, then $ac + ny = 1$ for some $c, y \in \mathbb{Z}$. We can write $[ac + ny] = [ac] + [ny] = [1]$. But since $[ny] = [n][y] = [0]$, we have $[ac] = [a][c] = [1]$, so there exists $[c] \in \mathbb{Z}/n$ such that $[a][c] = [1]$.

$\square$

Question 3

Suppose $[a], [b] \in \mathbb{Z}/n$ such that $[a] \neq [0]$. Suppose $[ax] = [b]$ has no solution. Show that we can find c such that $[ac] = [0]$.

Response

Proof: Suppose $[a], [b] \in \mathbb{Z}/n$ such that $[a] \neq [0]$ and $[ax] = [b]$ has no solutions. Then assume for the sake of contradiction that there does not exist a c such that $[a][c] = [0]$. Then (from **Question 2**, there exists a c such that $[a][c] = [1]$. Then,

$$\begin{aligned}
[a][c] &= [1] && \\
[a][c][b] &= [1][b] && \\
[a][cb] &= [b] && [p][q] = [pq] \\
[a(cb)] &= [b] && [p][q] = [pq]
\end{aligned}$$

Setting $[x] = [cb]$, we can see that there is a solution to the equation $[ax] = [b]$, a contradiction. Therefore, there must exist a b such that $[ab] = [0]$. $\square$

Question 4

Prove the general case of the Chinese remainder theorem:

Theorem 1 (Chinese Remainder Theorem, more general) *Let $m_1, \cdots, m_n \in \mathbb{Z}$ be positive and pairwise relatively prime (i.e., $(m_i, m_j) = 1$ when $i \neq j$). Let $a_1, \cdots, a_n \in \mathbb{Z}$. We can find x such that*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n\,. \end{aligned}$$

Moreover, if y is another solution, then $y \equiv x \mod m_1 m_2 \cdots m_n$

[Hint: the simple version of the Chinese remainder theorem can be useful here.]

Response

Proof: We will induct on $n \in \mathbb{N}$.
Base case: At $n = 2$, we have $m_1, m_2 \in \mathbb{Z}$ where $(m_1, m_2) = 1$. Then, we can find $p, q \in \mathbb{Z}$ such that $m_1 p + m_2 q = 1$. Then, because $m_2 q \equiv 0 \pmod{m_2}$, we have $m_1 \equiv 1 \pmod{m_2}$. Similarly, $m_2 \equiv 1 \pmod{m_1}$. Consider $x = (m_2 q)a_1 + (m_1 p)a_2$ for $a_1, a_2 \in \mathbb{Z}$. Then, since $(m_2 q)a_1 \equiv 0 \pmod{m_2}$, we have $x \equiv (m_1 p)a_2 \equiv a_2 \pmod{m_2}$. Similarly, $x \equiv (m_2 q)a_1 \equiv a_1 \pmod{m_1}$. So, $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$. Now suppose y is another solution. Then, we have $y \equiv x \pmod{m}$, which implies that $y - x$ is a multiple of m_1. Similarly, $y - x$ is a multiple of m_2. Then because $(m_1, m_2) = 1$, we have that $y - x$ is a multiple of $m_1 m_2$, so $y \equiv x \pmod{m_1 m_2}$.

Inductive step: At $n = n + 1$, we have $m_1, m_2 \in \mathbb{Z}$ where $(m_1, m_2) = 1$. Then by the inductive hypothesis, we have $x = a_1 + r_1 m_1 = \cdots = a_n + r_n m_n$ where $r_i \in \mathbb{Z}$. Define $M = \prod_{i=1}^{n} m_i$ and consider $x' = x + sM$ for some $s \in \mathbb{Z}$. Then $x' \equiv x + sM \equiv a_i \pmod{m_i}$ since $m_i | M$ for $i = 1, \cdots, n$. Now consider, $x' \equiv x + sM \equiv a_{n+1} \pmod{m_{n+1}}$, so $x' \equiv a_{n+1} \pmod{m_{n+1}}$. Now suppose y is another solution. Then $y \equiv x \pmod{m}$, which implies that $y - x$ is a multiple of m_i for $i = 1, \cdots, n + 1$. Because $(m_i, m_j) = 1$ for $i \neq j$, $i, j = 1, \cdots, n + 1$, we have $y \equiv x \pmod{m_1 m_2 \cdots m_{n+1}}$. $\square$

Question 5

A gang of 17 bandits stole a chest of gold coins. When they tried to divide the coins equally among themselves, there were three left over. This caused a fight in which one bandit was killed. When the remaining bandits tried to divide the coins again, there were ten left over. Another fight started, and five of the bandits were killed. When the survivor divided the coins, there were four left over. Another fight ensued in which four bandits were killed. The survivors then divided the coins equally among themselves, with none left over. What is the smallest possible number of coins in the chest?

Response

From the problem statement, we have the following system of equations:

$$
\begin{aligned}
x &\equiv 3 \pmod{17} \\
x &\equiv 10 \pmod{16} \\
x &\equiv 4 \pmod{11} \\
x &\equiv 0 \pmod{7}
\end{aligned}
$$

By the Chinese Remainder Theorem, we have $y \equiv x \pmod{17 \cdot 16 \cdot 11 \cdot 7} \to y \equiv x \pmod{20944}$. We can rewrite this as $y - x = 20944q$. Solving for x, we get that $x = \sum_{i=1}^{n} a_1 \cdot M_i \cdot M_i^{-1}$ where $M := \prod_{i=1}^{n} m_i = 17 \cdot 16 \cdot 11 \cdot 7 = 20944$, a_i is the remainder of m_i, and $M_i := M/m_i$.

Question 6

Let $d = (m, n)$, where $m, n \in \mathbb{Z}$ are positive. Show that the following system

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

has a solution if and only if $a \equiv b \mod d$.

Response

Proof: ($\implies$) Suppose the following system of equations

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

has an equation. Then $x = a + mp = b + nq$ for some $p, q \in \mathbb{Z}$. Then

$$\begin{aligned} a + mp &= b + nq \\ a - b &= nq - mp \\ a - b &= -(mp + nq) \end{aligned}$$

Since $d| - (mp + nq)$, we have that $d|a - b$, or $a - b = dt$ for some $t \in \mathbb{Z}$. This is equivalent to writing $a \equiv b \pmod d$.
($\impliedby$) Suppose $a \equiv b \pmod d$. We can rewrite this as $a - b = dt$ for some $t \in \mathbb{Z}$. Then

$$\begin{aligned} a - b &= dt \\ &= (mp' + nq')t && (m, n) = d \iff mp' + nq' = d, p', q' \in \mathbb{Z} \\ a - b &= (mp')t + (nq')t \\ a + (-mp')t &= b + (nq')t \\ a + mp &= b + nq && p := -p't, q := q't \end{aligned}$$

Setting $x = a + mp = b + nq$, we have $x - a = mp$ and $x - b = nq$ for some $p, q \in \mathbb{Z}$. Then we have the following system of equations:

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

$\square$