MATH 381 HW 9 part 1

Christian Jahnel

27 March 2024

1. Find all integer solutions to the following. If there are no integer solutions, explain why.

   (a) $3 + 2x \equiv -2 \pmod 7$

$$\begin{aligned} 3 + 2x &\equiv -2 \pmod 7 \\ 2x &\equiv -5 \pmod 7 \\ 2x + 0 &\equiv -5 + 7 \pmod 7 \\ 2x &\equiv 2 \pmod 7 \\ x &\equiv 1 \pmod 7 \\ x \in \hat{1} &= \{z \in \mathbb{Z} \mid z \bmod 7 = 1\} \\ &= \{\dots, -13, -6, 1, 8, 15, \dots\} \end{aligned}$$

   (b) $2x - 4 \equiv 0 \pmod 6$

$$\begin{aligned} 2x - 4 &\equiv 0 \pmod 6 \\ 2x &\equiv 4 \pmod 6 \\ x &\equiv 2 \pmod 6 \\ x \in \hat{2} &= \{z \in \mathbb{Z} \mid z \bmod 6 = 2\} \\ &= \{\dots, -10, -4, 2, 8, 14, \dots\} \end{aligned}$$

   (c) $x + y \equiv x - y \pmod 5$

$$\begin{aligned} x + y &\equiv x - y \pmod 5 \\ y &\equiv -y \pmod 5 \\ 1 &\equiv -1 \pmod 5 \qquad y \neq 0 \\ 1 &\equiv 4 \pmod 5 \end{aligned}$$

Let $y = 0$.

$$\begin{aligned} x + 0 &\equiv x - 0 \pmod 5 \\ x &\equiv x \pmod 5 \\ x &\in \mathbb{Z} \end{aligned}$$

The equation can be simplified to the equivalent equation that 1 and -1 are equivalent modulo 5. This is a contradiction because 1 and -1 are in their own equivalence classes: $\hat{1}$ and $\hat{4}$, respectively. However, this simplification assume $y \neq 0$. Consequently, in the case where $y = 0$, the equation is satisfied for any $x \in \mathbb{Z}$. Therefore, there are inifinite pairs of solutions: $\{(x, 0) \mid x \in \mathbb{Z}\}$.

2. Prove that for all integers $n \geq 0$, $10^n \equiv 1 \pmod 9$. Then, use that result to show that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Basis step

$$\begin{aligned} 10^0 &\equiv 1 \pmod 9 \\ \iff 1 &\equiv 1 \pmod 9 \\ \therefore P&(0) \end{aligned}$$

Inductive step; assume $P(k)$.

$$\begin{aligned} 10^k &\equiv 1 \pmod 9 \\ 10^k \cdot 10 &\equiv 1 \cdot 1 \pmod 9 \\ 10^{k+1} &\equiv 1 \pmod 9 \\ \therefore P(k) &\to P(k+1) \end{aligned}$$

$\therefore \forall n \in \{z \in \mathbb{Z} \mid z \geq 0\}(10^n \equiv 1 \pmod 9)$ ■

Every positive integer can be written as a sum of its digits weighted by its place value in base-10.

$$k = k_0 + 10k_1 + 100k_2 + \cdots + 10^n k_n = \sum_{i=0}^{n} 10^i k_i$$

$$\begin{aligned} 10^0 \equiv 1 \pmod 9 &\implies 10^0 k_0 \equiv k_0 \mod 9 \\ 10^1 \equiv 1 \pmod 9 &\implies 10^1 k_1 \equiv k_1 \mod 9 \\ 10^2 \equiv 1 \pmod 9 &\implies 10^2 k_2 \equiv k_2 \mod 9 \\ &\vdots \\ 10^n \equiv 1 \pmod 9 &\implies 10^n k_n \equiv k_n \mod 9 \end{aligned}$$

$\therefore \forall 0 \leq i \leq n(10^i k^i \equiv k_i \pmod 9)$

$$\begin{aligned} 9 \mid k \iff 0 &\equiv k \pmod 9 \\ 0 &\equiv \sum_{i=0}^{n} 10^i k_i \pmod 9 \\ 0 &\equiv \sum_{i=0}^{n} k_i \pmod 9 \end{aligned}$$

$\therefore 9 \mid k \iff 9 \mid (k_0 + k_1 + k_2 + \cdots + k_n)$ ■

3. Find gcd(620, 140) and give an integer solution to the equation $620x + 140y = \gcd(620, 140)$.

$$\begin{aligned}
620 &= 4(140) + 60 \iff 60 = 620 - 4(140)\\
140 &= 2(60) + 20 \iff 20 = 140 - 2(60)\\
60 &= 3(20) + 0
\end{aligned}$$

$\therefore \gcd(620, 140) = 20$

$$\begin{aligned}
20 &= 140 - 2(60)\\
&= 140 - 2(620 - 4(140))\\
&= 140 - 2(620) + 8(140)\\
&= 620(-2) + 140(9)
\end{aligned}$$

$\therefore x = -2, y = 9$ is a possible integer solution for the equation.

4. Show that an integer $a \in \mathbb{Z}_n$ has a multiplicative inverse, that is, an element $a^{-1} \in \mathbb{Z}_n$ with $a \cdot_n a^{-1} = 1$, if and only if a and n are relatively prime.

If $a, n \in \mathbb{N}$ are coprime, then there exists some integers s, t such that

$$\begin{aligned}
a \cdot s + n \cdot t &= 1\\
a \cdot s + n \cdot t &\equiv 1 \pmod{n}\\
n \cdot t &\equiv 0 \pmod{n}\\
\implies a \cdot s &\equiv 1 \pmod{n}
\end{aligned}$$

Since $a \in \mathbb{Z}_n$, then there exists an $s \in \mathbb{Z}_n$ such that the above is true, which is the definition of a multiplicative inverse (with respect to n).

Now assume there is a multiplicative inverse such that $a \cdot_n a^{-1} = 1$.

$$\begin{aligned}
a \cdot_n a^{-1} &= 1\\
a \cdot a^{-1} &\equiv 1 \pmod{n}\\
n \cdot t &\equiv 0 \pmod{n} \text{ for all } t \in \mathbb{Z}\\
\implies a \cdot a^{-1} + n \cdot t &\equiv 1 \pmod{n}\\
\implies \exists a \cdot_n a^{-1} &= 1 = \gcd(a, n)
\end{aligned}$$

$\therefore \forall a \in \mathbb{Z}_n \exists a^{-1} \in \mathbb{Z}_n (a \cdot_n a^{-1} = 1 \leftrightarrow \gcd(a, n) = 1) \quad \blacksquare$