Math347, Spring 2018, Homework #12
Due Wednesday, May 2, 2018

7.34 Find all integers that are congruent to 1 mod 7, 3 mod 8, and 5 mod 9. Which solution has the smallest absolute value ?

Solution: This is the Chinese Remainder Problem, i.e. find all integer solutions for the linear congruence systems: $x \equiv 1 \bmod 7$, $x \equiv 3 \bmod 8$, and $x \equiv 5 \bmod 9$. In this case, we have

$$\begin{array}{llllll} a_1 = 1 & n_1 = 7 & N_1 = n_2 n_3 = 72 & \equiv & 2 \bmod 7 & y_1 = 4 \bmod 7 \\ a_2 = 3 & n_2 = 8 & N_2 = n_1 n_3 = 63 & \equiv & 7 \bmod 8 & y_2 = 7 \bmod 8 \\ a_3 = 5 & n_3 = 9 & N_3 = n_1 n_2 = 56 & \equiv & 2 \bmod 9 & y_3 = 5 \bmod 9, \end{array}$$

where y_i are the inverse of $N_i \bmod n_i$. Therefore, we get general integer solutions

$$\begin{aligned} x &= a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3 + n_1 n_2 n_3 k \\ &= 1 \times 72 \times 4 + 3 \times 63 \times 7 + 5 \times 56 \times 5 + (7 \times 8 \times 9)k = 3011 + 504k \end{aligned}$$

for all $k \in \mathbb{Z}$. If we choose $k = -5$, we get the smallest positive integer solution $3011 + 504 \times (-5) = 3011 - 2520 = 491$. If we choose $k = -6$, we get the negative solution -13, which has the smallest absolute value since $|-13| = 13$.

7.41 Let f and g be defined by $f(x) \equiv (x + a) \bmod n$ and $g(x) \equiv ax \bmod n$.

(1) Give a complete description of the functional digraph of f for the case $(n, a) = (8, 3)$ and the case $(n, a) = (11, 7)$.

If we let $(n, a) = (8, 3)$, we consider $f(\overline{x}) = \overline{x} + \overline{3}$ for all $\overline{x} \in \mathbb{Z}_8$. The digraph of f consists of the following cycle

$$\overline{0} \to \overline{3} \to \overline{6} \to \overline{9} = \overline{1} \to \overline{4} \to \overline{7} \to \overline{10} = \overline{2} \to \overline{5} \to \overline{8} = \overline{0}.$$

If we let $(n, a) = (11, 7)$, we consider $f(\overline{x}) = \overline{x} + \overline{7}$ for all $\overline{x} \in \mathbb{Z}_{11}$. The digraph of f consists of the following cycle

$$\overline{0} \to \overline{7} \to \overline{14} = \overline{3} \to \overline{10} \to \overline{17} = \overline{6} \to \overline{13} = \overline{2} \to \overline{9} \to \overline{16} = \overline{5} \to \overline{12} = \overline{1} \to \overline{8} \to \overline{15} = \overline{4} \to \overline{11} = \overline{0}.$$

(2) Draw the functional digraph of g for the case $(n, a) = (19, 4)$. and the case $(n, a) = (19, 3)$.

If we let $\overline{a} = \overline{4}$, the digraph of g on $\mathbb{Z}_{19}$ consists of the trivial cycle $\overline{0} \to \overline{0}$ and the following two cycles

$$\overline{1} \to \overline{4} \to \overline{16} \to \overline{64} = \overline{7} \to \overline{28} = \overline{9} \to \overline{36} = \overline{17} \to \overline{68} = \overline{11} \to \overline{44} = \overline{6} \to \overline{24} = \overline{5} \to \overline{20} = \overline{1}$$

and

$$\overline{2} \to \overline{8} \to \overline{32} = \overline{13} \to \overline{52} = \overline{14} \to \overline{56} = \overline{18} \to \overline{72} = \overline{15} \to \overline{60} = \overline{3} \to \overline{12} \to \overline{48} = \overline{10} \to \overline{40} = \overline{2}$$

If we let $\overline{a} = \overline{3}$, the digraph of g consists of the trivial cycle $\overline{0} \to \overline{0}$ and the cycle

$$\begin{aligned} \overline{1} \quad &\to \quad \overline{3} \to \overline{9} \to \overline{27} = \overline{8} \to \overline{24} = \overline{5} \to \overline{15} \to \overline{45} = \overline{7} \to \overline{21} = \overline{2} \to \overline{6} \to \overline{18} \to \overline{54} = \overline{16} \\ &\to \quad \overline{48} = \overline{10} \to \overline{30} = \overline{11} \to \overline{33} = \overline{14} \to \overline{42} = \overline{4} \to \overline{12} \to \overline{36} = \overline{17} \to \overline{51} = \overline{13} \to \overline{39} = \overline{1}. \end{aligned}$$

Additional Problem 1. Suppose $d = \gcd(a, n)$ and $d \,|\, b$. If $\overline{x}$ is a solution for the congruence equation $\overline{ax} = \overline{b}$, show that $\overline{x}$, $\overline{x + \frac{n}{d}}, ..., \overline{x + \frac{(d-1)n}{d}}$ are d-different solutions of $\overline{a} \cdot \overline{x} = \overline{b}$.

Proof: If $d = \gcd(a, n) = 1$, relatively prime, it is known that $\overline{ax} = \overline{b}$ has a unique solution.

Let us suppose that $d = \gcd(a, n) > 1$. Then if $d \,|\, b$, the congruence equation $\overline{ax} = \overline{b}$ has a solution $\overline{x}$. Since $d \,|\, a$, we get $a = \tilde{a}d$ for some positive integer $\tilde{a} = \frac{a}{d}$. For any $1 \leq k \leq d-1$, we have

$$\overline{a}(\overline{x + \frac{kn}{d}}) = \overline{ax} + \overline{\tilde{a}d}\overline{\frac{kn}{d}} = \overline{b} + \overline{kn\tilde{a}} = \overline{b}.$$

So all $\overline{x}, \overline{x + \frac{n}{d}}, ..., \overline{x + \frac{(d-1)n}{d}}$ are solutions of $\overline{ax} = \overline{b}$.

These solutions must all be distinct since if we have $1 \leq i < j \leq d-1$ such that

$$\overline{x + \frac{in}{d}} = \overline{x + \frac{jn}{d}},$$

then we get $\overline{\frac{(j-i)n}{d}} = \overline{0}$, or equivalently, $\frac{(j-i)n}{d} = kn$ for some integer k. This imples that $\frac{(j-i)}{d} = k$ is an integer. But this is impossible since $0 < j - i < d$. So all these solutions must be distincnt.

Additional Problem 2. Let f be the map on $\mathbb{Z}_8$ defined by $f(\overline{x}) = \overline{6x}$.

(1) Find the image $f(\mathbb{Z}_8)$ of f.

Solution: Let us consider the map

$$f : \overline{x} \in \mathbb{Z}_8 \to \overline{6x} \in \mathbb{Z}_8.$$

We get

$$\overline{0} \to \overline{0},\ \overline{1} \to \overline{6},\ \overline{2} \to \overline{12} = \overline{4},\ \overline{3} \to \overline{18} = \overline{2},$$

and

$$\overline{4} \to \overline{24} = \overline{0},\ \overline{5} \to \overline{30} = \overline{6},\ \overline{6} \to \overline{36} = \overline{4},\ \overline{7} \to \overline{42} = \overline{2}.$$

This shows that the image of f on $\mathbb{Z}_8$ is $f(\mathbb{Z}_8) = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$.

(2) Find the inverse image $I_f(\{\overline{1}, \overline{2}, \overline{3}\})$, and the inverse image $I_f(\{\overline{0}, \overline{4}, \overline{5}\})$.

Solution: The inverse image

$$I_f(\{\overline{1}, \overline{2}, \overline{3}\}) = \{\overline{3},\ \overline{7}\}$$

and the inverse image

$$I_f(\{\overline{0}, \overline{4}, \overline{5}\}) = \{\overline{0},\ \overline{2},\ \overline{4},\ \overline{6}\}$$