Math347, Spring 2018, Homework #11 Solution
Due Wednesday, April 25, 2018

Page 151, 7.5. What is the congruence class of 10^n modulo 11 ? Use this to determine the remainder when 654321 is divided by 11.
Solution: We note that $10 = -1 + 11$. So $\overline{10} = \overline{(-1)}$ and thus

$$\overline{10^n} = \overline{10}^n = \overline{(-1)}^n = \overline{(-1)^n}.$$

Note that $654321 = 6 \times 10^5 + 5 \times 10^4 + 4 \times 10^3 + 3 \times 10^2 + 2 \times 10^1 + 1$. Then the corresponding equivalence class mod 11 is

$$\begin{aligned} \overline{654321} &= \overline{6 \times 10^5} + \overline{5 \times 10^4} + \overline{4 \times 10^3} + \overline{3 \times 10^2} + \overline{2 \times 10^1} + \overline{1} \\ &= \overline{-6} + \overline{5} + \overline{-4} + \overline{3} + \overline{-2} + \overline{1} = \overline{-3} = \overline{8} \end{aligned}$$

The remainder of 654321 divided by 11 is 8.

Page 151, 7.6. Determine the last digit in the base 8 expansion of 9^{1000}, 10^{1000}, and 11^{1000}.
Solution: Consider the congruence classes of mod 8.

Since $9 = 8 + 1$, we get $\overline{9} = \overline{1}$ and thus

$$\overline{9^{1000}} = \overline{1}^{1000} = \overline{1}.$$

The last digit of 9^{1000} in the base 8 is 1.

Since $10 = 8 + 2$, we get $\overline{10} = \overline{2}$. Then

$$\overline{10^{1000}} = \overline{2}^{1000} = \overline{2}^3\overline{2}^{997} = \overline{0}.$$

The last digit of 10^{1000} in the base 8 is 0.

Since $11 = 8 + 3$, we get $\overline{10} = \overline{3}$. Then

$$\overline{11^{1000}} = \overline{3}^{1000} = \overline{9}^{500} = \overline{1}.$$

The last digit of 11^{1000} in the base 8 is 1.

Page 151, 7.9. Use Fermat's Little Theorem to find a number between 0 and 12 that is congruent to 2^{100} mod 13.
Solution: By Fermat's little theorem, $2^{12} \equiv 1 \mod 13$ and thus $2^{96} = (2^{12})^8 \equiv 1 \mod 13$.
So $2^{100} = 2^{96} \cdot 2^4 = 16 \cdot 2^{96} \equiv 16 \equiv 3 \mod 13$. The remainder (of 2^{100} mod 13) we want to find is 3.

We can also solve this problem without using Fermat's Little theorem by considering

$$2^{100} \equiv (2^4)^{25} \equiv (16)^{25} \equiv 3^{25} \equiv 3 \cdot (27)^8 \equiv 3 \cdot 1 \equiv 3 \text{ mod } 13.$$

Additional Problem 1. Let $f_{\overline{a}}$ be the map on $\mathbb{Z}_{13}$ defined by $f_{\overline{a}}(\overline{x}) = \overline{a} \cdot \overline{x}$.

(1) Find the digraph of the map $f_{\overline{a}}$ on $\mathbb{Z}_{13}$ for $\overline{a} = \overline{3}, \overline{4}$, and $\overline{7}$ respectively.

Solution: The digraph of $f_{\overline{3}}$ on $\mathbb{Z}_{13}$ is given by $\overline{0} \to \overline{0}$, and

$$\overline{1} \to \overline{3} \to \overline{9} \to \overline{27} = \overline{1},$$
$$\overline{2} \to \overline{6} \to \overline{18} = \overline{5} \to \overline{15} = \overline{2},$$
$$\overline{4} \to \overline{12} \to \overline{36} = \overline{10} \to \overline{30} = \overline{4},$$
$$\overline{7} \to \overline{21} = \overline{8} \to \overline{24} = \overline{11} \to \overline{33} = \overline{7}.$$

The digraph of $f_{\overline{4}}$ on $\mathbb{Z}_{13}$ is given by $\overline{0} \to \overline{0}$, and

$$\overline{1} \to \overline{4} \to \overline{16} = \overline{3} \to \overline{12} \to \overline{48} = \overline{9} \to \overline{36} = \overline{10} \to \overline{40} = \overline{1},$$
$$\overline{2} \to \overline{8} \to \overline{32} = \overline{6} \to \overline{24} = \overline{11} \to \overline{44} = \overline{5} \to \overline{20} = \overline{7} \to \overline{28} = \overline{2}.$$

The digraph of $f_{\overline{7}}$ on $\mathbb{Z}_{13}$ is given by $\overline{0} \to \overline{0}$, and

$$\begin{aligned} \overline{1} \quad &\to \quad \overline{7} \to \overline{49} = \overline{10} \to \overline{70} = \overline{5} \to \overline{35} = \overline{9} \to 63 = \overline{11} \to \overline{77} = \overline{12} \\ &\to \quad \overline{84} = \overline{6} \to \overline{42} = \overline{3} \to \overline{21} = \overline{8} \to \overline{56} = \overline{4} \to \overline{28} = \overline{2} \to \overline{14} = \overline{1}. \end{aligned}$$

(2) Find the order and the inverse of $\overline{3}, \overline{4}$, and $\overline{7}$ in $\mathbb{Z}_{13}$..

Solution: It is easy to see from the digraphs of $f_{\overline{3}}, f_{\overline{4}}, f_{\overline{7}}$ that

The the order of $\overline{3}$ in $\mathbb{Z}_{13}$ is $k = 3$, and the inverse of $\overline{3}$ in $\mathbb{Z}_{13}$ is $\overline{9}$ since $\overline{3} \cdot \overline{9} = \overline{27} = \overline{1}$.

The order of $\overline{4}$ in $\mathbb{Z}_{13}$ is $k = 6$, and the inverse of $\overline{4}$ in $\mathbb{Z}_{13}$ is $\overline{10}$

The order of $\overline{7}$ is $k = 12$, and the inverse of $\overline{7}$ in $\mathbb{Z}_{13}$ is 2 since $\overline{2} \cdot \overline{7} = \overline{14} = \overline{1}$.

Additional Problem 2. Let a, b, and n be positive integers. Show that the congruence equation $\overline{a} \cdot \overline{x} = \overline{b}$ has a solution if and only if $\gcd(a, n) \mid b$.

Proof: Let x be an integer. According to the definition, $\overline{a} \cdot \overline{x} = \overline{b}$ if $ax \equiv b \bmod n$. This is equivalent to say that $ax = b + kn$ or equivalently $ax + (-k)n = b$ for some integer $k \in \mathbb{Z}$. It is known from Chapter 6 that the Diophantine equation $ax + (-k)n = b$ has an integer solution if and only if $d = \gcd(a, n) \mid b$. Therefore, we can conclude that $\overline{a} \cdot \overline{x} = \overline{b}$ has a solution in $\mathbb{Z}_n$ if and only if $\gcd(a, n) \mid b$.

Additional Problem 3. Let $n = 12$ and $a = 8$, and consider Z_{12}.

(1) Find all $\overline{b}$ in Z_{12} such that the congruence equation $\overline{8} \cdot \overline{x} = \overline{b}$ has a solution,
(2) Find all solutions for each $\overline{b}$ found in (1).

Solution: (1) Since $\gcd(8, 12) = 4$, $\overline{ax} = \overline{b}$ has a solution in $\mathbb{Z}_{12}$ if and only if $4|b$. Therefore, for $\overline{b} = \overline{0}, \overline{4}, \overline{8}$, the congruent equations $\overline{8} \cdot \overline{x} = \overline{b}$ has solutions.

(2) For each $\overline{b}$ in part (1), we should have $\gcd(8, 12) = 4$ solutions.
For $\overline{b} = \overline{0}$, $\overline{8} \cdot \overline{x} = \overline{0}$ has solutions $\overline{0}, \overline{3}, \overline{6}, \overline{9}$ in $\mathbb{Z}_{12}$.
For $\overline{b} = \overline{4}$, $\overline{8} \cdot \overline{x} = \overline{4}$ has solutions $\overline{2}, \overline{5}, \overline{8}, \overline{11}$ in $\mathbb{Z}_{12}$.
For $\overline{b} = \overline{8}$, $\overline{8} \cdot \overline{x} = \overline{8}$ has solutions $\overline{1}, \overline{4}, \overline{7}, \overline{10}$ in $\mathbb{Z}_{12}$.