M325K SPRING 2023

## HW #11 B, Part III Solutions

This solution uses methods of the handout:
"Solving Simple Congruences"

---

The congruence under consideration is

$$7x \equiv 172 \pmod{13}.$$

We need to find a (mod 13) inverse of 7.

The process for doing this is presented well on the next page in the second solution method shown.

On the next page, it is shown that

2 is a (mod 13) inverse of 7.

This is because $2 \times 7 = 14 = (13)(1) + 1$.

So, since 2 is a (mod 13) inverse of 7, we know that

$$2 \times 7 \equiv 1 \pmod{13}.$$

To both sides of this congruence, $7x \equiv 172 \pmod{13}$, we multiply the factor 2,

Thus, $2 \times (7x) \equiv 2(172) \equiv 344 \pmod{13}$, by Theorem 8.4.3.

Also, $2(7x) \equiv (2 \times 7)x \equiv 1 \cdot x \equiv x \pmod{13}$.

$\therefore x \equiv 344 \pmod{13}$, by Transitivity, and this is true about every solution of the congruence.

$344 \equiv 344 \pmod{13}$, so $x = 344$ is one solution.

$344 = (13)(26) + 6$ and $0 \leq 6 < 13$

so, $(344 \bmod 13) = 6$ and $x = 6$ is the least non-negative solution. <u>The Solution Set</u> is $[6] = \{\ldots, -20, -7, 6, 19, 32, \ldots\}$

The Solution to Part III of 11B using the methods shown in class

---

The Congruence to solve is $7x \equiv 172 \pmod{13}$

we need to find a (mod 13) inverse of 7.

$$7\overline{)13}\ \ 1,\quad -7,\quad 6 \qquad\qquad 6\overline{)7}\ \ 1,\quad -6,\quad 1 \qquad \Rightarrow \qquad \begin{aligned} 6 &= (13)(1) - (7)(1) \\ 1 &= (7)(1) - (6)(1) \end{aligned}$$

$$1 = (7)(1) - [(13)(1) - (7)(1)](1)$$
$$1 = (7)(2) - (13)(1)$$
$$1 = (7)(2) + (13)(-1).$$

So, $1 \equiv (7)(2) \pmod{13}$
by Thm 8.4.1.

Thus 2 is a (mod 13) inverse of 7.

It was shown in class that $x_0 = (2)(172)$ is one solution of the congruence; $x_0 = 344$

$2408 - 172 = 2236$

Check: $7 * 344 = 2408$ and $2408 - 172 = 2236 = (13)(172)$

and so, $2408 - 172$

$2408 \equiv 172 \pmod{13}$

so, $2408 \equiv 172 \pmod{13}$. so $x_0 = 344$ is a solution

so $7 * 344 \equiv 172$

$x_1 = (344 \bmod 13) = 6$ is the least non-negative solution.

The Solution set is $[6] = [344]$, the equivalence class of 6 in the Equivalence Relation, $\equiv \pmod{13}$, namely

$[6] = \{\ldots, -20, -7, 6, 19, 32, \ldots, 331, 344, 357, \ldots\}$
$= [344]$.

---