M325K SPRING 2024

HW #11 A, PART II SOLUTION

This solution uses methods presented in the handout: "Solving Simple Congruences"

The congruence under consideration is

$$788x \equiv 24 \pmod{1,647}.$$

1. In order to show that 1,415 is a (mod 1,647) inverse of 788, we demonstrate that

$$(1,415)(788) \equiv 1 \pmod{1,647}.$$

Now, $(1,415)\times(788) = 1,115,020$.

So, $\left((1,415)\times(788) - 1\right) = 1,115,019$

and $1,115,019 = (1,647)(677)$,

so, $1,647 \mid 1,115,019$. That is, $1,647 \mid \left((1,415)\times(788) - 1\right)$.

$\therefore$ $(1,415)(788) \equiv 1 \pmod{1647}$.

Another way to prove that $(1,415)(788) \equiv 1 \pmod{1647}$ is to find that $(1415)(788) = (1647)(677) + 1$.

$\therefore$ $(1415)(788) \equiv 1 \pmod{1647}$ by Theorem 8.4.1.

$\therefore$ 1415 is a (mod 1647) inverse of 788.

The solution for the second part of this assignment appears on the next page.

HW #11A, Part II Solution (continued).

2. The congruence under consideration is

$$788x \equiv 24 \pmod{1,647}.$$

In part 1, it was shown that 1,415 is a (mod 1647) inverse of 788.

Multiplying both sides of the congruence by 1,415 (which is a (mod 1647) inverse of 788), we obtain

$(1415)(788x) \equiv (1415)(24) \pmod{1647}$, by Thm. 8.4.3.

Also, $(1415)(788x) \equiv ((1415)(788))x \equiv 1 \cdot x \equiv x \pmod{1647}$

Thus, $x \equiv (1415)(24) \equiv 33,960 \pmod{1647}$.

(So, any integer congruent (mod 1647) to 33,960 is a solution of this congruence.)

$33,960 \equiv 33,960 \pmod{1647}$.

So, $x = 33,960$ is one solution.

$33,960 = (1647)(20) + 1020$ and $0 \leq 1020 < 1647$.

$\therefore 33,960 \equiv 1020 \pmod{1647}$, by Theorem 8.4.1, and $(33,960 \bmod 1647) = 1020$, by definition of the "(K mod 1647)" function.

Thus $(33,960 \bmod 1647) = 1020$ is also a solution.

In fact, $(33,960 \bmod 1647) = 1020$ is the least non-negative solution.

The Solution to Part II of the 11A assignment using the methods shown in class.

Part II of 11A:

The congruence is $788x \equiv 24 \pmod{1,647}$.

Since $\gcd(788, 1647) = 1$,

this is a simple congruence $Bx \equiv D \pmod{n}$ with $\gcd(B, n) = 1$.

1. We verify that 1,415 is a (mod 1,647) inverse of 788.

$(788)(1,415) = (1,647)(677) + 1$,

so, $(788)(1,415) \equiv 1 \pmod{1,647}$.

$\therefore A = 1,415$ is a (mod 1647) inverse of 788.

2. It was shown in class that $x_0 = (1,415)(24)$ is one solution of this congruence.

$x_0 = (1415)(24) = 33,960$

Check: $(788)(33,960) = (1647)(16,248) + 24$,

so, $(788)(33,960) \equiv 24 \pmod{1647}$ by Thm 8.4.1.

So, $x_0 = 33,960$ is a solution of the congruence.

The least non-negative solution of this congruence is $x_1 = (x_0 \bmod 1647) = (33,960 \bmod 1647)$.

$33,960 = (1647)(20) + 1,020$ and $0 \le 1,020 < 1,647$

So $(33,960 \bmod 1,647) = 1,020$.

So, $x_1 = 1,020$ is the least non-negative solution of this congruence.