MAT 373 Homework 8

Justyce Countryman

March 18, 2024

Problem 1: Solve the linear congruence: $5x \equiv 2 \pmod{26}$

gcd(5, 26) = 1 and 1|2, so we can see there is exactly one solution.

Let's consider the Diophantine equation $5m + 26n = 1$ for which (m, n) represent integer solutions. We can rewrite this as $5m \equiv 1 \pmod{26}$ to represent a linear congruence.

Using the Euclidean algorithm, we can mention:
(26) = (5)5 + (1)
(5) = (1)5 + 0

Which then tells us: 1 = (26) - (5)5

From this, we can refer back to $5m \equiv 1 \pmod{26}$ to say:
$(26) - (5)5 \equiv 1 \pmod{26}$
$-5(5) \equiv 1 \pmod{26}$
$5(-5) \equiv 1 \pmod{26}$

Now we know the multiplicative inverse of 5 (mod 26) = 26 - 5 = 21.

Going back to $5x \equiv 2 \pmod{26}$, we can now say:
$(21)5x \equiv (21)2 \pmod{26}$
$105x \equiv 42 \pmod{26}$

We can notice that $26|104x$ for all integers x and 42 (mod 26) = 16. This information allows us to state that:
$105x - 104x \equiv 16 \pmod{26}$
$x \equiv 16 \pmod{26}$

Problem 2: Solve the linear congruence: $6x \equiv 15 \pmod{21}$

gcd(6, 21) = 3 and 3|15, so we can see there are exactly three solutions.

Firstly, we can divide all components of this linear congruence (including the modulo) by 3, to give us $2x \equiv 5 \pmod{7}$

From this, we can consider that gcd(2, 7) = 1 and 1|5, so this linear congruence has exactly one solution.

Let's consider the Diophantine equation $2m + 7n = 1$ for which (m, n) represent integer solutions. We can rewrite this as $2m \equiv 1 \pmod 7$ to represent a linear congruence.

Using the Euclidean algorithm, we can mention:
(7) = (2)3 + (1)
(2) = (1)2 + 0

Which then tells us: 1 = (7) - (2)3

From this, we can refer back to $2m \equiv 1 \pmod 7$ to say:
$(7) - (2)3 \equiv 1 \pmod 7$
$-(2)3 \equiv 1 \pmod 7$
$2(-3) \equiv 1 \pmod 7$

Now we know the multiplicative inverse of 2 (mod 7) = 7 - 3 = 4.

Going back to $2x \equiv 5 \pmod 7$, we can now say:
$(4)2x \equiv (4)5 \pmod 7$
$8x \equiv 20 \pmod 7$

We can notice that $7|7x$ for all integers x and 20 (mod 7) = 6. This information allows us to state that:
$8x - 7x \equiv 6 \pmod 7$
$x \equiv 6 \pmod 7$

Finally, to present this linear congruence solution in terms of (mod 21) so that we can solve $6x \equiv 15 \pmod{21}$, we just have to consider the following based on our (mod 7) solution:
6 + 7(0) = 6
6 + 7(1) = 13
6 + 7(2) = 20
This allows us to present the final solution: $x \equiv 6, 13, 20 \pmod{21}$

Problem 3: Solve the linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ by solving the system:

$$17x \equiv 3 \pmod 2 \quad 17x \equiv 3 \pmod 3$$

$$17x \equiv 3 \pmod 5 \quad 17x \equiv 3 \pmod 7$$

In order to use the Chinese Remainder Theorem on this linear congruence system, we need to first get all of the linear congruences into the form $x \equiv a_1 \pmod 2$, $x \equiv a_2 \pmod 3$, $x \equiv a_3 \pmod 5$, and $x \equiv a_4 \pmod 7$, for some integers a_1, a_2, a_3, a_4

1: $17x \equiv 3 \pmod 2$:
gcd(17, 2) = 1 and 1|3

$17m + 2n = 1$ for which (m, n) represent integer solutions.
$17m \equiv 1 \pmod 2$

$(17) = (2)8 + (1)$
$(2) = (1)1 + 0$

$1 =$ (17) - (2)8

$(17) - (2)8 \equiv 1 \pmod 2$
$17(1) \equiv 1 \pmod 2$

Multiplicative inverse of 17 (mod 2): (2+1) $\rightarrow$ 4 - 3 = 1

$17x \equiv 3 \pmod 2$
$2|16x$ for all integers x and 3 (mod 2) = 1.
$17x - 16x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 2$

2: $17x \equiv 3 \pmod 3$:
gcd(17, 3) = 1 and $1|3$

$17m + 3n = 1$ for which (m, n) represent integer solutions.
$17m \equiv 1 \pmod 3$

$(17) = (3)5 + (2)$
$(3) = (2)1 + (1)$
$(2) = (1)2 + 0$

$1 =$ (3) - (2)
$1 =$ (3) - ((17) - (3)5)
$1 =$ -1(17) + 6(3)

$-1(17) + 6(3) \equiv 1 \pmod 3$
$17(-1) \equiv 1 \pmod 3$

Multiplicative inverse of 17 (mod 3): 3 - 1 = 2

$(2)17x \equiv 3(2) \pmod 3$
$34x \equiv 6 \pmod 3$
$3|33x$ for all integers x and 6 (mod 3) = 0.
$34x - 33x \equiv 0 \pmod 3$

$x \equiv 0 \pmod 3$

3: $17x \equiv 3 \pmod 5$:
gcd(17, 5) = 1 and 1|3

$17m + 5n = 1$ for which (m, n) represent integer solutions.
$17m \equiv 1 \pmod 5$

(17) = (5)3 + (2)
(5) = (2)2 + (1)
(2) = (1)2 + 0

1 = (5) - 2(2)
1 = (5) - 2((17) - 3(5))
1 = 17(-2) + 5(7)

$17(-2) + 5(7) \equiv 1 \pmod 5$
$17(-2) \equiv 1 \pmod 5$

Multiplicative inverse of 17 (mod 5): 5 - 2 = 3

$(3)17x \equiv 3(3) \pmod 5$
$51x \equiv 9 \pmod 5$
$5|50x$ for all integers x and 9 (mod 5) = 4.
$51x - 50x \equiv 4 \pmod 5$

$x \equiv 4 \pmod 5$

4: $17x \equiv 3 \pmod 7$:
gcd(17, 7) = 1 and 1|3

$17m + 7n = 1$ for which (m, n) represent integer solutions.
$17m \equiv 1 \pmod 7$

(17) = (7)2 + (3)
(7) = (3)2 + (1)
(3) = (1)3 + 0

1 = (7) - (3)2
1 = (7) - 2((17) - (7)2)
1 = 17(-2) + 7(5)

$17(-2) + 7(5) \equiv 1 \pmod 7$
$17(-2) \equiv 1 \pmod 7$

Multiplicative inverse of 17 (mod 7): 7 - 2 = 5

$(5)17x \equiv 3(5) \pmod 7$

$85x \equiv 15 \pmod 7$
$7|84x$ for all integers x and $15 \pmod 7 = 1$.
$85x - 84x \equiv 1 \pmod 7$

$$x \equiv 1 \pmod 7$$

Now with this simplified linear congruence system, the Chinese Remainder Theorem allows us to work out the following:

$$b_1(3 \cdot 5 \cdot 7) \equiv 1 \pmod 2 \quad b_2(2 \cdot 5 \cdot 7) \equiv 1 \pmod 3$$

$$b_3(2 \cdot 3 \cdot 7) \equiv 1 \pmod 5 \quad b_4(2 \cdot 3 \cdot 5) \equiv 1 \pmod 7$$

for some integers b_1, b_2, b_3, b_4.

$b_1(3 \cdot 5 \cdot 7) \equiv 1 \pmod 2$
$105b_1 \equiv 1 \pmod 2$
$105b_1 - 104b_1 \equiv 1 \pmod 2$

$$b_1 \equiv 1 \pmod 2$$

$b_2(2 \cdot 5 \cdot 7) \equiv 1 \pmod 3$
$70b_2 \equiv 1 \pmod 3$
$70b_2 - 69b_2 \equiv 1 \pmod 3$

$$b_2 \equiv 1 \pmod 3$$

$b_3(2 \cdot 3 \cdot 7) \equiv 1 \pmod 5$
$42b_3 \equiv 1 \pmod 5$
$42b_3 - 40b_3 \equiv 1 \pmod 5$
$2b_3 \equiv 1 \pmod 5$

$\frac{5+1}{2} = 3$, so this tells us:

$$b_3 \equiv 3 \pmod 5$$

$b_4(2 \cdot 3 \cdot 5) \equiv 1 \pmod 7$
$30b_4 \equiv 1 \pmod 7$
$30b_4 - 28b_4 \equiv 1 \pmod 7$
$2b_4 \equiv 1 \pmod 7$

$\frac{7+1}{2} = 4$, so this tells us:

$$b_4 \equiv 4 \pmod 7$$

Lastly, let's provide four integers x_1, x_2, x_3, x_4 so that they satisfy the first, second, third, and fourth linear congruence in the system respectively:
Let $x_1 = 1$ because $2|1 - 1$ and $1 \equiv 1 \pmod 2$.
Let $x_2 = 0$ because $3|0 - 0$ and $0 \equiv 0 \pmod 3$.
Let $x_3 = 4$ because $5|4 - 4$ and $4 \equiv 4 \pmod 5$.
Let $x_4 = 1$ because $7|1 - 1$ and $1 \equiv 1 \pmod 7$.

From this, we can say:
$x \equiv (105 \cdot 1 \cdot 1) + (70 \cdot 1 \cdot 0) + (42 \cdot 3 \cdot 4) + (30 \cdot 4 \cdot 1) \pmod{2 \cdot 3 \cdot 5 \cdot 7}$
$x \equiv 105 + 504 + 120 \pmod{210}$
$x \equiv 729 \pmod{210}$

729 - 210(3) = 99, so the final answer is:

$x \equiv 99 \pmod{210}$

Problem 4: When eggs in a basket are removed 2, 3, 4, 5, 6 at a time there remain, respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

This problem can be represented by the following linear congruence system:

$$x \equiv 0 \pmod 7 \quad x \equiv 1 \equiv -1 \pmod 2$$

$$x \equiv 2 \equiv -1 \pmod 3 \quad x \equiv 3 \equiv -1 \pmod 4$$

$$x \equiv 4 \equiv -1 \pmod 5 \quad x \equiv 5 \equiv -1 \pmod 6$$

From this information, we can use this linear congruence:

$$x \equiv -1 \pmod{lcm(2, 3, 4, 5, 6)}$$

Simplifying and manipulating the linear congruence gives us:

$$x \equiv -1 \pmod{60}$$

$$x \equiv -1 \equiv 59 \pmod{60}$$

This linear congruence tells us that the minimum number of eggs x is denoted by $x = 60k + 59$ for some non-negative integer k since we cannot have a negative number of eggs. Let's start at the base case and work our way up until we find an x that satisfies $x \equiv 0 \pmod 7$, thus fully satisfying the linear congruence system.

$k = 0 \implies x = 60(0) + 59 = 59$, but $59 \not\equiv 0 \pmod 7$ since $7 \nmid 59 - 0$, so this is not the answer.

$k = 1 \implies x = 60(1) + 59 = 119$, and $119 \equiv 0 \pmod 7$ because $7|119 - 0$, so this tells us that the smallest number of eggs that could have been contained in the basket is 119.

Problem 5: A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

This problem can be represented by the following linear congruence system:

$$x \equiv 3 \pmod{17}$$

$$x \equiv 10 \pmod{16}$$

$$x \equiv 0 \pmod{15}$$

Since we know $gcd(17, 16) = gcd(17, 15) = gcd(16, 15) = 1$ and the created linear congruence system is of the form $x \equiv a_1 \pmod{17}$, $x \equiv a_2 \pmod{16}$, $x \equiv a_3 \pmod{15}$ for some integers a_1, a_2, a_3, we can immediately apply the Chinese Remainder Theorem, which tells us to find the following:

$$b_1(16 \cdot 15) \equiv 1 \pmod{17} \;\; b_2(17 \cdot 15) \equiv 1 \pmod{16} \;\; b_3(16 \cdot 17) \equiv 1 \pmod{15}$$

for some integers, b_1, b_2, b_3.

$b_1(16 \cdot 15) \equiv 1 \pmod{17}$
$240b_1 \equiv 1 \pmod{17}$
$240b_1 - 238b_1 \equiv 1 \pmod{17}$
$2b_1 \equiv 1 \pmod{17}$

$\frac{17+1}{2} = 9$, so this tells us:

$$b_1 \equiv 9 \pmod{17}$$

$b_2(17 \cdot 15) \equiv 1 \pmod{16}$
$255b_2 \equiv 1 \pmod{16}$
$255b_2 - 256b_2 \equiv 1 \pmod{16}$
$-b_2 \equiv 1 \pmod{16}$

$$b_2 \equiv -1 \pmod{16}$$

$b_3(16 \cdot 17) \equiv 1 \pmod{15}$
$272b_3 \equiv 1 \pmod{15}$

$272b_3 - 270b_3 \equiv 1 \pmod{15}$
$2b_3 \equiv 1 \pmod{15}$

$\frac{15+1}{2} = 8$, so this tells us:

$$b_3 \equiv 8 \pmod{15}$$

Now, let's provide three integers x_1, x_2, x_3 so that they satisfy the first, second, and third linear congruence in the system respectively:
Let $x_1 = 3$ because $17|3 - 3$ and $3 \equiv 3 \pmod{17}$.
Let $x_2 = -6$ because $16|-6-10$ and $-6 \equiv 10 \pmod{16}$.
Let $x_3 = 0$ because $15|0 - 0$ and $0 \equiv 0 \pmod{15}$.

With this information, we can then write:
$x \equiv (240 \cdot 9 \cdot 3) + (255 \cdot -1 \cdot -6) + (272 \cdot 8 \cdot 0) \pmod{15 \cdot 16 \cdot 17}$
$x \equiv 6480 + 1530 \pmod{4080}$
$x \equiv 8010 \pmod{4080}$

8010 - 4080(1) = 3930, so we now get the linear congruence:

$$x \equiv 3930 \pmod{4080}$$

We can now see that 3930 is the least number of coins that could have been stolen.