Chinese Remainder Theorem challenge

October 19, 2024

1 Problem

Given the following set of linear congruences:

$$x \equiv 2 \pmod 5 \tag{1}$$
$$x \equiv 3 \pmod{11} \tag{2}$$
$$x \equiv 5 \pmod{17} \tag{3}$$

Find the integer a such that $x \equiv a \pmod{935}$

2 Solution

1. **Starting with the congruence with the largest modulus** :
We can rewrite the equation as :

$$x = 5 + k \cdot 17$$

for some integer k.

2. **Substitute this expression for x into the congruence with the next largest modulus** :

$$5 + 17 \cdot k \equiv 3 \pmod{11}$$
$$17 \cdot k \equiv -2 \equiv 9 \pmod{11}$$

We know that $17 \equiv 6 \pmod{11}$, so :

$$6 \cdot k \equiv 9 \pmod{11}$$

Next we need to find the inverse of 6 mod 11.

$$6 \cdot 1 \equiv 6 \pmod{11}$$

$$6 \cdot 2 \equiv 12 \equiv 1 \pmod{11}$$

So the inverse of 6 mod 11 is 2.
By multiplying both sides of the equation by 2 we end up getting :

$$2 \cdot 6 \cdot k \equiv 2 \cdot 9 \pmod{11}$$

$$k \equiv 7 \pmod{11}$$

3. **Substitute this expression for k into the expression for x :**

$$x = 5 + 17 \cdot (7 + 11 \cdot j)$$

$$x = 124 + 187 \cdot j$$

For some integer j.

4. **Substitute this expression for x into the final congruence, and solve the congruence for j :**

$$124 + 187 \cdot j \equiv 2 \pmod{5}$$

$$187 \cdot j \equiv -122 \equiv 3 \pmod{5}$$

We also have $187 \equiv 2 \pmod{5}$, so :

$$2 \cdot j \equiv 3 \pmod{5}$$

The inverse of 2 mod 5 is 3 (because $3 \cdot 2 \equiv 1 \pmod{5}$) :

$$3 \cdot 2 \cdot j \equiv 3 \cdot 2 \pmod{5}$$

$$j \equiv 9 \equiv 4 \pmod{5}$$

So we end up with $j = 4 + 5 \cdot l$ for some integer l

3 Result

We can substitute the expression for j into the expression for j :

$$x = 124 + 187 \cdot (4 + 5 \cdot l)$$

$$x = 872 + 935 \cdot l$$

So the final solution is $a = 872$.