How to do the Chinese Remainder Theorem

Ernest Michael Nelson

July 25, 2017

1 Introduction

In this article we will be doing a step by step on how to do the Chinese Reminder Theorem. An we will be given a system of three congruences.

2 System of Congruenhces

$$x_1 \equiv (3 \bmod 8)$$
$$x_2 \equiv (1 \bmod 9)$$
$$x_3 \equiv (4 \bmod 11)$$

3 Formulas

The given formula is

$$\bar{x} \equiv a_1 \cdot N_1 \cdot x_1 + a_2 \cdot N_2 \cdot x_2 + a3 \cdot N_3 \cdot x_3 (\bmod n_1 \cdot n_2 \cdot n_3)$$

and we will also need the inverse formula

$$N_1 x_k \equiv a_1 (\bmod n_k)$$

4 Proof:

The very first thing we want to calculate is our modules in the Chinese Remainder Theorem (CRT). An by observation we are also given a_1 from the given system of congruences.

$$\bar{x} \equiv 3 \cdot N_1 \cdot x_1 + 1 \cdot N_2 \cdot x2 + 4 \cdot N_3 \cdot x_3 (\bmod 8 \cdot 9 \cdot 11)$$
$$\bar{x} \equiv 3 \cdot N_1 \cdot x_1 + 1 \cdot N_2 \cdot x_2 + 4 \cdot N_3 \cdot x_3 (\bmod 792)$$

Next we will calculate the N_1,N_2 and N_3 of the (CRT).Fri st we will calculate N_1 and then repeat the process for N_2 and N_3.

$$N_1 = \frac{8 \cdot 9 \cdot 11}{8} = 99$$

$$N_2 = \frac{8 \cdot 9 \cdot 11}{9} = 88$$

$$N_3 = \frac{8 \cdot 9 \cdot 11}{11} = 72$$

Now we input N_1,N_2, and N_3 into the given formula.

$$\bar{x} \equiv 3 \cdot 99 \cdot x_1 + 1 \cdot 88 \cdot x_2 + 4 \cdot 72 \cdot x_3 (\text{mod } 792)$$

Then we simplify the formula.

$$\bar{x} \equiv 297 \cdot x_1 + 88 \cdot x_2 + 288 \cdot x_3 (\text{mod } 792)$$

On the next step we will calculate the x_1,x_2, and x_3 in the (CRT).First we will show how to solve x_1 then x_2 and x_3.

5 Solving for x_1,x_2 and x_3

From the formula section above we plug N_1 into our congruences.

For x_1

$$99x_1 \equiv 1 (\text{mod } 8)$$

Next step we dived 8 into 99 and remainder we put in front of x_1.

$$3x_1 \equiv 1 (\text{mod } 8)$$

Now we add 8 to our congruences.

$$3x_1 \equiv 9 (\text{mod } 8)$$

Final we dived 3 into 9 and get our answer for x_1.

$$x_1 \equiv 3 (\text{mod } 8)$$

Therefore $x_1 = 3$.

For x_2

$$88x_2 \equiv 1 (\text{mod } 9)$$

We repeat the process for x_2 as the same for x_1 so we dived 9 into 88.

$$7x_2 \equiv 1 (\text{mod } 9)$$

Then we add 9 to the congruences.

$$7x_2 \equiv 10 (\text{mod } 9)$$

The next step we subtract 9 on the left hand side.

$$-2x_2 \equiv 10 (\text{mod } 9)$$

To make the congruence correct we make $x_2 = -5$.

$$2(-5) \equiv 10 (\text{mod } 9)$$

Therefor $x_2 = -5$

For x_3

$$72x_3 \equiv 1 (\text{mod } 11)$$

First we dived 72 by 11 and put the remainder in front of x_3.

$$6x_3 \equiv 1 (\text{mod } 11)$$

Now we add 11 to the congruence.

$$6x_3 \equiv 12 (\text{mod } 11)$$

Final we dived 6 on both sides.

$$x_3 \equiv 2 (\text{mod } 11)$$

Therefore $x_3 = 2$

After getting x_1,x_2,and x_3 we input into our (CRT) formula and calculate.

$$\bar{x} \equiv ((297 \cdot 3 + 88 \cdot (-5) + 288 \cdot 2) \text{mod } 792)$$

$$\bar{x} \equiv ((891 + (-440) + 576) \text{mod } 792)$$

$$\bar{x} \equiv 1027 (\text{mod } 792)$$

Lastly we reduce by subtracting 792 from 1027.

$$\bar{x} \equiv 235 (\text{mod } 792)$$

$$(q.e.d)$$

6 Reference:

Bruce M.Burton, Element of Number Theory, page 79

Joseph Cutrona,YouTube.com, Basic example of Chinese Remainder Theorem