# A Few CRT Problems and Solutions

P. Reany

June 29, 2023

**Abstract**

The Chinese Remainder Theorem (CRT) states the existence of number in modular arithmetic, that satisfies a collection of modular constraints. Here we will state the theorem and them use the method of undetermined values to solve for this unknown quantity. Three problems will be worked out. This first in great detail. The second is less detail, and the third in a more algebraic method of solution. A little knowledge of modular arithmetic is assumed.

## 1 Introduction

Let $m_1$ and $m_2$ be two relatively prime (coprime) positive integers. [In symbolism, $(m_1, m_2) = 1$.] Let $r_1$ and $r_2$ be any two positive numbers less than $m_1$ and $m_2$ (called 'moduli'), respectively. Then there exists a number $x$ **mod** $m_1 m_2$, such that

$$x \textbf{ mod } m_1 \equiv r_1 \quad \text{and} \quad x \textbf{ mod } m_2 \equiv r_2 \,. \tag{1}$$

So, typically, the constraints are given and then you are asked to find the solution to them that also satisfies

$$x \textbf{ mod } m_1 m_2 \,, \tag{2}$$

which means that the 'best' form of the $x$ is an integer between 0 and $m_1 m_2 - 1$.

There is a version of the CRT for the cases of three or more constraints. Our problems here will always contain three constraint equations.

## 2 Problem 1

Find $x$ such that the following given information must hold.[1]

$$x \equiv 2 \,(\textbf{mod } 3)\,, \tag{3a}$$
$$x \equiv 2 \,(\textbf{mod } 4)\,, \tag{3b}$$
$$x \equiv 1 \,(\textbf{mod } 5)\,. \tag{3c}$$

First, since $(3,4,5) = 1$,[2] we are guaranteed that a solution exists modulo $3 \times 4 \times 5 = 60$. We will solve this problem by the method undetermined values. So, we propose the ansatz solution:

$$x \equiv \overbrace{4 \times 5}^{3} a + \overbrace{3 \times 5}^{4} b + \overbrace{3 \times 4}^{5} c \,, \tag{4}$$

[1] You can find the same problem solved similarly on the YouTube video found at https://www.youtube.com/watch?v=ru7mWZJlRQg.

[2] The numbers are all relatively prime to each other.

where the numbers $a, b, c$ are the values we need to solve for. They'll look more like values in the following form:

$$x \equiv 20a + 15b + 12c \ (\textbf{mod } 60). \tag{5}$$

To use the given information (3a)–(3c), we will need to mod out Eq. (4), one at a time by moduli 3, 4, 5, leaving us with three equations to solve for values $a, b, c$. The reason we chose the multipliers we did is because every time we mod Eq. (4) by one of the moduli, two terms will immediately drop out, leaving us with a much simpler modular equation to solve for.

Let's see how this works in practice. First, we mod out (4) by 3, to get

$$x \equiv 20a \ (\textbf{mod } 3). \tag{6}$$

On comparing this to (3a), we get that

$$2 \equiv 20a \ (\textbf{mod } 3). \tag{7}$$

We can solve this problem by exhaustive search, as $a$ can only take on possible values of $0, 1, 2$. Try $a = 0$: Is

$$2 \equiv 0 \ (\textbf{mod } 3)? \tag{8}$$

Nope. Try $a = 1$: Is

$$2 \equiv 20 \ (\textbf{mod } 3)? \tag{9}$$

This is true because $20 = 6 \times 3 + 2$. So now we know that $a = 1$.

Next, let's mod out (4) by 4, to get

$$x \equiv 15b \ (\textbf{mod } 4). \tag{10}$$

On comparing this to (3b), we get that

$$2 \equiv 15b \ (\textbf{mod } 4). \tag{11}$$

Again, we try exhaustive search, as $b$ can only take on possible values of $0, 1, 2, 3$. Try $b = 0$: Is

$$2 \equiv 0 \ (\textbf{mod } 4)? \tag{12}$$

Nope. Try $b = 1$: Is

$$2 \equiv 15 \ (\textbf{mod } 4)? \tag{13}$$

This is not true because $15 = 3 \times 4 + 3$.
Try $b = 2$: Is

$$2 \equiv 30 \ (\textbf{mod } 4)? \tag{14}$$

This is true because $30 = 7 \times 4 + 2$. So now we know that $b = 2$.

Lastly, let's mod out (4) by 5, to get

$$x \equiv 12c \ (\textbf{mod } 5). \tag{15}$$

On comparing this to (3c), we get that

$$1 \equiv 12c \ (\textbf{mod } 5). \tag{16}$$

Again, we try exhaustive search, as $c$ can only take on possible values of $0, 1, 2, 3, 4$, though this time we will ignore the zero. Try $c = 1$: Is

$$1 \equiv 12 \ (\textbf{mod } 5)? \tag{17}$$

No, because $12 = 2 \times 5 + 2$. Try $c = 2$: Is

$$1 \equiv 24 \ (\textbf{mod } 5)? \tag{18}$$

This is not true because $24 = 4 \times 5 + 4$.
Try $c = 3$: Is

$$1 \equiv 36 \ (\textbf{mod } 5)? \tag{19}$$

This is true because $36 = 7 \times 5 + 1$. Therefore, we know that $c = 3$.

So, we're almost there. Now we go back to (5) with the values we have collected for $a, b, c$:

$$x \equiv 20(1) + 15(2) + 12(3) \,(\textbf{mod } 60)\,, \tag{20}$$

A little simplification gives

$$x \equiv 86 \,(\textbf{mod } 60)\,, \tag{21}$$

or, in simpler terms,

$$x \equiv 26 \,(\textbf{mod } 60)\,. \tag{22}$$

So this is supposed to be the correct answer, but I'd feel better about it if I checked it against Eqs. (3a)–(3c). So, are those three claims true with $x = 26$? Yes, because,

$$26 = 8 \times 3 + 2\,, \quad \checkmark \tag{23a}$$

$$26 = 6 \times 4 + 2\,, \quad \checkmark \tag{23b}$$

$$26 = 5 \times 5 + 1\,. \quad \checkmark \tag{23c}$$

# 3 Problem 2

Find $x$ such that the following given information (constraints) must hold.

$$x \equiv 4 \,(\textbf{mod } 5)\,, \tag{24a}$$

$$x \equiv 6 \,(\textbf{mod } 8)\,, \tag{24b}$$

$$x \equiv 8 \,(\textbf{mod } 9)\,. \tag{24c}$$

First, since $(5, 8, 9) = 1$,[3] we are guaranteed that a solution exists modulo $5 \times 8 \times 9 = 360$. We will solve this problem by the method undetermined values. So, we propose the ansatz solution:

$$x \equiv \overbrace{72}^{5}\, a + \overbrace{45}^{8}\, b + \overbrace{40}^{9}\, c\,, \tag{25}$$

where the numbers $a, b, c$ are the values we need to solve for. The equation can be expressed in the fuller form:

$$x \equiv 72a + 45b + 40c \,(\textbf{mod } 360)\,. \tag{26}$$

As in the last problem, first, we mod out (25) by 5, to get

$$4 \equiv 72a \,(\textbf{mod } 5)\,. \tag{27}$$

By exhaustive search, we find that $a = 2$ works.

Next, we mod out (25) by 8, to get

$$6 \equiv 45b \,(\textbf{mod } 8)\,. \tag{28}$$

By exhaustive search, we find that $b = 6$ works. Lastly, we mod out (25) by 9, to get

$$8 \equiv 40c \,(\textbf{mod } 9)\,. \tag{29}$$

By exhaustive search, we find that $c = 2$ works.

So, now let's put these values in (26), to get

$$x \equiv 144 + 270 + 80 \,(\textbf{mod } 360)\,, \tag{30}$$

[3] The numbers are all relatively prime to each other.

After reduction, we have that

$$x \equiv 134 \,(\textbf{mod } 360)\,. \tag{31}$$

All we have to do now is to make sure this value satisfies the given constraints.

$$134 \,(\textbf{mod } 5) \equiv 4\,, \quad \checkmark \tag{32}$$

$$134 \,(\textbf{mod } 8) \equiv 6\,, \quad \checkmark \tag{33}$$

$$134 \,(\textbf{mod } 9) \equiv 8\,. \quad \checkmark \tag{34}$$

# 4 Problem 3

Find $x$ such that the following given information (constraints) must hold.

$$x \equiv 2 \,(\textbf{mod } 7)\,, \tag{35a}$$

$$x \equiv 3 \,(\textbf{mod } 11)\,, \tag{35b}$$

$$x \equiv 2 \,(\textbf{mod } 8)\,. \tag{35c}$$

We are looking for a solution relative to the modulus: $7 \times 11 \times 8 = 616$.

$$x \equiv ?? \,(\textbf{mod } 616)\,. \tag{36}$$

But this time, we will try a more algebraic method of solution! According to (35a), there must exist some integer $a$ such that:

$$x = 7a + 2\,. \tag{37}$$

So, now we combine this with (35b):

$$3 \equiv 7a + 2 \,(\textbf{mod } 11)\,. \tag{38}$$

Or,

$$7a \equiv 1 \,(\textbf{mod } 11)\,. \tag{39}$$

We can solve this for $a$ to get

$$a \equiv 8 \,(\textbf{mod } 11)\,. \tag{40}$$

Now let's convert this to an algebraic equation. There exists a $b$ such that

$$a = 11b + 8\,. \tag{41}$$

Next, we substitute this into (37):

$$x = 7(11b + 8) + 2 = 77b + 58\,. \tag{42}$$

To sum up, we've already used two of our given constraints, and this last equation must be consistent with the third constraint (35c). Thus,

$$77b + 58 \equiv 2 \,(\textbf{mod } 8)\,, \tag{43}$$

which simplifies to

$$77b + 56 \equiv 0 \,(\textbf{mod } 8)\,, \tag{44}$$

which further simplifies down to

$$77b \equiv 0 \,(\textbf{mod } 8)\,. \tag{45}$$

But this forces us to insist that

$$b \equiv 0 \,(\textbf{mod } 8)\,, \tag{46}$$

since $(77,8) = 1$. Therefore, there has to exist some integer $c$, such that

$$b = 8c\,. \tag{47}$$

On substituting this last result into (42), we find that

$$x = 77(8c) + 58 = 616c + 58\,. \tag{48}$$

Now that we've used up all the given constraints, all that's left is to take this equation mod 616, and when we do, we get

$$x \equiv\ 58\,(\textbf{mod}\ 616)\,. \tag{49}$$

Lastly, as before, we check it against the given information (constraints).

$$58\,(\textbf{mod}\ 7) \equiv 2\,, \quad \checkmark \tag{50}$$

$$58\,(\textbf{mod}\ 11) \equiv 3\,, \quad \checkmark \tag{51}$$

$$58\,(\textbf{mod}\ 8) \equiv 2\,. \quad \checkmark \tag{52}$$

# 5 Conclusion

Why isn't this 'algebraic' method used more often in math books? I don't know. Maybe it is used more than I think it is.

Anyway, see page 2, Example 3 of

https://www.math.cmu.edu/ mradclif/teaching/127S19/Notes/ChineseRemainderTheorem.pdf

by Mary Radcliffe.