Some Surplus Suspects

A Problem of Remainders

Huaiyu Wu

March 2024

1 Introduction

Imagine yourself as a detective tasked with determining the number of suspects within a heavily secured residence, which is too dangerous to approach directly.

Your team has gathered intelligence indicating that when the suspects exit the property in groups of three, two remain inside; when they depart in groups of five, three are left; and when they leave in groups of seven, two stay behind.

Without compromising your safety, how can you deduce the smallest number of suspects present in the house?

2 Breaking it down

The actual problem is much less complicated (and much less dangerous) than it seems. It embodies the principles of the *Chinese Remainder Theorem* (hereinafter CRT), which we will discuss later on.

By assigning the letter x to represent the smallest possible number of suspects present in the house, we can then express this as:

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases} \tag{1}$$

The information above may appear confusing, so let's break the problem down into smaller pieces.

We are dealing with a system of three modular congruences[1], each congruence being a separate condition that x must satisfy (note that x represents the unknown number that we are trying to find).

- The symbol "$\equiv$" is used to denote congruence of different integers which leave behind the same remainder when divided by another integer.
- The numbers after the "$\equiv$" symbol (2, 3, 2) are the remainders that "x" leaves after being divided by the moduli (3, 5, 7).
- The "mod" (short for modulo) refers to the divisor in the division operation within the context of congruences. It is the number by which we are dividing to find the remainder.

[1] A *modular congruence* is an equation that expresses that two numbers leave the same remainder when divided by a positive integer called the modulus. Formally, we write $a \equiv b \pmod m$ to mean that m divides the difference $a - b$, which is equivalent to saying a and b have the same remainder when divided by m.
In other words, *modular congruences* can be used to categorise integers into groups, where every number in the same group leaves the same remainder after being divided by another integer. For example, 5, 8, 11 and 14 can be allocated to the same group, as all of them leaves a remainder of 2 when divided by 3. Written as

$$5 \equiv 2 \pmod 3$$
$$8 \equiv 2 \pmod 3$$
$$11 \equiv 2 \pmod 3$$
$$14 \equiv 2 \pmod 3$$

- This leads us onto the numbers after "mod" (3, 5, 7), which are the moduli. They are the numbers that "x" is being divided by to find the remainders. In this case, "x" is being divided by 3, 5, and 7 in the respective congruences.

Taking the first modular congruence:

$$x \equiv 2 \pmod{3} \tag{2}$$

as an example, it is simply a mathematical expression for "the number 'x' divided by 3 leaves a remainder of 2".

3 What's next?

Now that we have deciphered the concept, let's return to the question, how could we find the smallest number of suspects present in the house?

Firstly, we can find the product of the moduli (denoted as N), which is calculated as:

$$N = m_1 \times m_2 \times m_3 \tag{3}$$

In our case,

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases} \tag{4}$$

$m_1 = 3$, $m_2 = 5$, and $m_3 = 7$, so:

$$N = 3 \times 5 \times 7 = 105 \tag{5}$$

This product, N, is used to establish a common modulus for which a solution will be the same across all given congruences.

Before going further into solving our problem, let's clarify a few notations:

- m_i - This is one of the divisors from our clues. It represents the group size that leaves the house.
- a_i - This is the remainder or the number of suspects left in the house after the groups leave.
- n_i - This number is a piece of our puzzle that we calculate by dividing a big number (N - the product of all divisors) by each m_i. It helps us spread out the conditions across all clues.
- y_i - This is called the modular multiplicative inverse of n_i for the modulus m_i. It is a special number that when multiplied by n_i, cancels everything out except for a remainder of 1, in the world defined by the modulus m_i.

Then, for each congruence, n_i is defined as:

$$n_i = \frac{N}{m_i} \tag{6}$$

where m_i is one of the moduli and n_i is used to find the modular multiplicative inverse relative to that modulus (y_i), which we use to ensure that each part of the solution interacts correctly with the rest, without causing any conflicts or overlaps.[2]

[2]Imagine you are trying to evenly distribute something—like slices of a pie—among a group of friends, but you need to make sure that everyone gets their fair share according to some specific rules (the moduli). The modular multiplicative inverse helps us to "reverse-engineer" the problem: It's like figuring out how to cut and distribute the pie so that, after everyone has taken their slices according to the rules, the process can be perfectly reversed, and the pie looks as if it was never cut.

In mathematical terms, for each modulus m_i, we find n_i to evenly distribute our solution across all conditions. But we need to ensure this distribution does not mess up when applied to each specific condition defined by m_i. The modular multiplicative inverse (let's call it y_i for n_i) ensures that when we multiply n_i by y_i, the effect is neutralised (it's like multiplying by 1), except under the specific conditions we are considering. This "neutralising effect" allows us to construct a solution that fits all the conditions simultaneously, without any interference between them.

To summarise, each congruence

$$x \equiv a_i \pmod{m_i} \tag{7}$$

specifies that a_i is the remainder when an unknown number x is divided by the modulus m_i.

The modular multiplicative inverse of n_i with respect to m_i, denoted by y_i, satisfies

$$n_i \times y_i \equiv 1 \pmod{m_i} \tag{8}$$

To find y_i, first compute n_i as

$$n_i = \frac{N}{m_i} \tag{9}$$

and then to calculate y_i, which is the multiplicative inverse of n_i modulo m_i, we are looking for a number such that:

$$y_i \equiv \frac{1}{n_i} \pmod{m_i} \tag{10}$$

The final solution for x is the sum of the products of the remainders a_i, the n_i, and the y_i, taken modulo N:

$$x \equiv \sum (a_i \times n_i \times y_i) \pmod{N} \ . \tag{11}$$

The complete expression for the solution would be:

$$x \equiv \left(a_1 \times \frac{N}{m_1} \times \left(\frac{N}{m_1} \right)^{-1} + a_2 \times \frac{N}{m_2} \times \left(\frac{N}{m_2} \right)^{-1} + a_3 \times \frac{N}{m_3} \times \left(\frac{N}{m_3} \right)^{-1} \right) \pmod{N} \tag{12}$$

Substituting the values we have found:

$$x \equiv \left(2 \times \frac{105}{3} \times \left(\frac{105}{3}\right)^{-1} + 3 \times \frac{105}{5} \times \left(\frac{105}{5}\right)^{-1} + 2 \times \frac{105}{7} \times \left(\frac{105}{7}\right)^{-1}\right) \pmod{105} \tag{13}$$

Simplifying the expression and calculating the modular inverses, we arrive at the solution:

$$x \equiv (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \pmod{105} \tag{14}$$

$$x \equiv (140 + 63 + 30) \pmod{105} \tag{15}$$

$$x \equiv 233 \pmod{105} \tag{16}$$

When we say $x \equiv 233 \pmod{105}$, we are really saying that x is the remainder of 233 divided by 105; 233 divided by 105 is 2 with a remainder of 23 (because $105 \times 2 = 210$, and $233 - 210 = 23$). This gives us

$$x \equiv 23 \pmod{105} \tag{17}$$

Therefore, the smallest x that satisfies all three congruences is 23 (so the smallest number of suspects present in the house is 23).

4 How did we get here?

4.1 The Historical Example

The aforementioned problem (which, thankfully, has no direct correlation with the number of suspects in a house), is better known as the *Chinese Remainder Theorem*.

This theorem was first proposed by the Chinese mathematician Sunzi in the 5th Century. In his mathematical text, *Sunzi Suanjing*, he presented an arguably less captivating challenge to his readers: to find a number that, when divided by 3, 5, and 7, left remainders of 2, 3, and 2, respectively. This problem was later solved by Qin Jiushao (another mathematician from ancient China) in 1247.

In the west, Carl Friedrich Gauss first discussed congruences in his *Disquisitiones Arithmeticae* (Arithmetical Investigations), notably applying the CRT to a practical problem that involved the synchronisation of different calendrical cycles.

4.2 Progression to the General Theorem

While the specific numbers in Sunzi's problem might seem arbitrary, they exemplify a much broader mathematical principle.

The general form of the CRT asserts that for any set of integers $a_1, a_2, \ldots, a_n$ and pairwise coprime[3] moduli $m_1, m_2, \ldots, m_n$, there exists a unique solution x satisfying:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{18}$$

[3]Two numbers are *coprime* if they have no common factors other than 1. For example, 8 and 15 are coprime because the only positive integer that evenly divides both of them is 1.

The first step is to calculate the product of all the moduli (denoted by N), it is calculated as:

$$N = m_1 \times m_2 \times \ldots \times m_n \tag{19}$$

This product N serves as the modulus for which the solution x to the system of congruences is guaranteed to be unique modulo N.

For each modulus m_i, we calculate a corresponding n_i (the factor of N excluding the i-th modulus) which is given by

$$n_i = \frac{N}{m_i} \tag{20}$$

We also need to find the modular multiplicative inverse y_i such that:

$$n_i \times y_i \equiv 1 \pmod{m_i} \tag{21}$$

Once we have all n_i and y_i, the solution x is given by the sum of products of each remainder a_i, its corresponding n_i, and the modular multiplicative inverse y_i:

$$x = \sum_{i=1}^{n} (a_i \times n_i \times y_i) \pmod{N} \tag{22}$$

This solution x will satisfy all the given congruences simultaneously. However, the solution is not unique in an absolute sense but is unique modulo N; that is, if x is a solution, then $x + kN$ is also a solution for any integer k.

To sum up, the CRT allows us to take a system of congruences and find a solution that works for all of them at once.

The theorem ensures that this solution is unique within the range of modulo N, where N is the product of all the moduli in the system.

Application of the general theorem

Drawing on the same curiosity that fascinated Gauss about the remainders of time, let's try another example using the general theorem.

We have three clocks with intervals (clock faces) of 4, 5, and 6 hours (our pairwise coprime moduli), the goal is to find the earliest time after midnight (denoted by x) such that:

- The first clock with a clock face of 4 hours shows 1 hour past (remainder $a_1 = 1$).
- The second clock with a clock face of 5 hours shows 2 hours past (remainder $a_2 = 2$).
- The third clock with a clock face of 6 hours shows 3 hours past (remainder $a_3 = 3$).

To find our time x, we will solve the following system:

$$\begin{cases} x \equiv 1 \pmod 4, \\ x \equiv 2 \pmod 5, \\ x \equiv 3 \pmod 7. \end{cases} \tag{23}$$

1. Find the product of the moduli:

$$N = 4 \times 5 \times 7 = 140 \tag{24}$$

2. Find the partial products (n_1, n_2, and n_3) for each modulus:

$$\begin{cases} n_1 = \frac{N}{4} = 35, \\ n_2 = \frac{N}{5} = 28, \\ n_3 = \frac{N}{7} = 20. \end{cases} \tag{25}$$

3. Find the modular inverses (y_1, y_2, and y_3) needed:

$$\begin{cases} 35y_1 \equiv 1 \pmod 4 \Rightarrow y_1 = 3, \\ 28y_2 \equiv 1 \pmod 5 \Rightarrow y_2 = 2, \\ 20y_3 \equiv 1 \pmod 7 \Rightarrow y_3 = 6. \end{cases} \tag{26}$$

4. Solve for x using the formula from the general theorem:

$$x = \sum_{i=1}^{3} (a_i \times N_i \times y_i) \pmod{N} \tag{27}$$

where a_i are the remainders $1, 2, 3$ for the moduli $4, 5, 7$, respectively.

5. Substituting the values, we get:

$$x = (1 \times 35 \times 3) + (2 \times 28 \times 2) + (3 \times 20 \times 6) \pmod{140} = 17 \tag{28}$$

Calculating this, we find that x is:

$$x = (105) + (112) + (360) \pmod{140} \tag{29}$$

$$x = 577 \pmod{140} \tag{30}$$

Dividing 577 by 140, we find that it goes 4 times with a remainder of 17:

$$577 = 140 \times 4 + 17 \tag{31}$$

Thus, in terms of modular arithmetic, we write:

$$577 \equiv 17 \pmod{140} \tag{32}$$

This leads to the final conclusion that the unique solution x for our system of congruences is:

$$x \equiv 17 \pmod{140} \tag{33}$$

Therefore, the value of x that satisfies all the given congruences is 17.

5 To conclude

You may wonder, what makes the CRT interesting?

Rather than approaching problems in a chronological manner, the CRT allows us to work "backwards" in a problem, by taking known remainders from a set of modular divisions and reconstructing the smallest possible original number that yields those remainders. Unlike traditional problem-solving that progresses from a known starting point to a conclusion, the CRT begins with the end conditions — the remainders — and deduces the starting value.

Beyond working out the smallest number of suspects in a house, the CRT finds extensive application across various domains of our daily lives, ranging from cryptography to computational mathematics.

So, the next time when you come across a lineup of remainders, remember the CRT — your detective in the world of remainders, solving the cases that numbers leave behind.

Isn't that a remainder to remember?

References

[1] Wikipedia contributors. "Chinese remainder theorem." Wikipedia, The Free Encyclopedia.

[2] "Chinese Remainder Theorem." Brilliant.org.