Indian Journal of Advanced Mathematics (IJAM)
ISSN: 2582-8932 (Online), Volume-6 Issue-1, April 2026

Analyzing the Chinese Remainder Theorem to Find Solutions Efficiently

Aditi S. Phadke

Abstract: ***In this paper, we explain the logic for simultaneously solving linear congruences using the Chinese Remainder Theorem and apply it to develop an easy method for finding the solution.***

Mathematics Subject Classification [2020]: Primary 11A41

Keywords: Simultaneous Linear Congruences, Chinese Remainder Theorem

I. INTRODUCTION

The Chinese remainder theorem is one of the most important theorems in elementary number theory. The theorem deals with solving linear congruences simultaneously under certain conditions. The theorem was first discovered in the 3rd century in a Chinese mathematical treatise entitled Sun Zi Suanjing. The problem studied was to find a simultaneous solution to the three congruences: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. In 5th-century India, Aryabhata's mathematics addressed instances of the Chinese Remainder Theorem. (See [1], [2])

The Chinese explained how to obtain a solution, but they did not explain why it works.

The problem generated continued interest, and during the 11th century, a mathematician, Ibn Tahir-al Baghdadi, discussed the Chinese Remainder Theorem in his treatise AI Takmilafi 'lim ai-Hisab. He was the first person to not only give a solution to the problem but also give a method to solve the congruences: $x \equiv a \pmod 3$, $x \equiv b \pmod 5$, $x \equiv c \pmod 7$. The problem was further studied in China by Yang Hui in the 13th century. It was studied in Europe by Leonardo Fibonacci in the 13th century, Isaac Argyros in the 14th century and Frater Frederius in the 15th century. (See [1])

The algorithm for finding a solution to simultaneous linear congruences is a standard problem taught in an elementary number theory course. But after teaching this topic for several years to high school students preparing for the Mathematical Olympiad Competitions as well as undergraduate students, it has been noted that when students first study the algorithm to solve the problem, it appears very complicated and magical. Students cannot independently uncover the algorithm's beauty.

Manuscript received on 23 March 2026 | First Revised Manuscript received on 30 March 2026 | Second Revised Manuscript received on 07 April 2026 | Manuscript Accepted on 15 April 2026 | Manuscript published on 30 April 2026.

*Correspondence Author(s)

Dr. Aditi Sunil Phadke*, Associate Professor, Department of Mathematics, Modern Education Society's, Nowrosjee Wadia College, Pune (Maharashtra), India. Email ID: phadkeaditi@gmail.com, ORCID ID: 0000-0003-2546-3944

II. UNDERSTANDING AND ANALYSING THE CHINESE REMAINDER THEOREM

In this section, we understand the logic and develop an efficient method to solve simultaneous linear congruences using the Chinese Remainder Theorem.

Let us now look at the formal statement of the theorem. (See [3])

Theorem: Given a system of congruences: $x \equiv a_1 \pmod{n_1}$; $x \equiv a_2 \pmod{n_2}$;…; $x \equiv a_k \pmod{n_k}$ where $n_1, n_2, \ldots, n_k$ are pairwise coprime, then there exists a unique solution modulo $N = n_1 * n_2 * \ldots * n_k$

Note that the pairwise coprime condition of $n_1, n_2, \ldots, n_k$ is a sufficient condition but not necessary. For example, $x \equiv 2 \mod 4$ and $x \equiv 0 \mod 2$ have infinitely many solutions, and a unique solution modulo 4. Note that 4 is the LCM of 2 and 4.

We now discuss a method to solve the problem naturally. We consider the problem of finding a simultaneous solution to three congruences:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 7$.

Note that $\gcd(3,5) = \gcd(5,7) = \gcd(3,7) = 1$.

Let us denote the expected simultaneous solution by S.

Now, this S is expected to leave a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 5 when divided by 7.

Since divisibility by 3, 5, and 7 is involved, let us try to find a solution modulo the product of these three integers.

Also, S has to behave differently modulo 3, 5, 7. So we can assume that S is of a certain form. Thus

S ≡ __ __ __ __+__ __ __ __ +__ __ __ __mod 3*5*7.

Let us call the places to be filled first place, second place, and third place, separated by two + signs.

Now, modulo 3, S ≡ 2 mod 3, but nothing should remain in the second and third places. To do this, we put 3 in the second and third places and 2 in the first.

So, the form of the solution will be

S ≡ 2 __ __ __+__ __ __ 3 +__ __ __ 3 mod 3*5*7. Note here that in this case,

S ≡ 2 mod 3.

Similarly, S ≡ 3 mod 5, but nothing should remain in the first and third places. To do this, we put 5 in the first and third places and 3 in the second.

Lastly, we desire S ≡ 5 mod 7, but nothing should remain in the first and second places. So, we put 7 in first and second place, and 5 in third.

So, the form of the solution will be

S ≡ 2 [7* 5] __+3[7* 3] +5 [5* 3] __mod 3*5*7.

Note here that if we now consider S mod 3, we have 7*5 extra. So, we will multiply it by x_1 such that

$35x_1 \equiv 1 \bmod 3$. Such x_1 exists from the coprimality condition in the statement of the theorem. Similarly, we find x_2 such that $21x_2 \equiv 1 \bmod 5$ and x_3 such that $15x_3 \equiv 1 \bmod 7$. Here $x_1=2$, $x_2=1$ and $x_3=1$. Thus

$S \equiv 2\ [7^*\ 5]\ ^*2+3[7^*\ 3]\ ^*1+5\ [5^*\ 3]\ ^*1 \bmod 3^*5^*7$.

Thus $S \equiv 140+63+75 \bmod 105$

Thus $S \equiv 68 \bmod 105$. One can easily check that 68 satisfies all three congruences.

III. CONCLUSION

Over more than 15 years, I have used this method while teaching the Chinese Remainder Theorem, and students have been able to comprehend the logic behind it and find the correct solution easily.

DECLARATION STATEMENT

Some of the cited references are older and are noted explicitly as [1], [2] and [3]. However, these works remain significant for the current study, as they are pioneering in their fields.

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and without external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed solely by the author.

REFERENCES

1. https://sgmathsociety.org/volume-30-2003/, works remain significant, see the declaration
2. Sury, B. Multivariable Chinese remainder theorem. Reson 20, 206–216 (2015). DOI: https://doi.org/10.1007/s12045-015-0171-x, works remain significant, see the declaration
3. Childs, L.N. (1995). The Chinese Remainder Theorem. In: A Concrete Introduction to Higher Algebra. Undergraduate Texts in Mathematics. Springer, New York, NY.
   DOI: https://doi.org/10.1007/978-1-4419-8702-0_12, works remain significant, see the declaration

AUTHOR'S PROFILE

Dr. Aditi Sunil Phadke is an Associate Professor in the Department of Mathematics at Nowrosjee Wadia College, Pune, where she has been serving since 2011. She completed her M.Sc. in Mathematics from IIT Bombay in 1998 and obtained her PhD from Savitribai Phule Pune University in 2006, receiving the Gold Medal for the Best PhD thesis. Thesis in Mathematics that year. She has been actively involved for many years in training and mentoring students for national and international Mathematical Olympiads. She has taught at the International Mathematical Olympiad Training Camp organised by HBCSE in Navi Mumbai. She has served in leadership roles for the Indian team at international competitions and has also contributed to research publications, conferences, academic workshops, and university textbooks.