MATHEMATICS & NATURE
Mathematics, Physics, Mechanics & Astronomy

· Article ·
Mathematics

Random Vol. 3 Sn: 202301
https://mathnature.github.io

Dongfang Brief General Solutions to Congruence Equations

—Dongfang Concise Expression of Chinese Remainder Theorem

X. D. Dongfang

Orient Research Base of Mathematics and Physics,
Wutong Mountain National Forest Park, Shenzhen, China

Abstract: The Chinese remainder theorem gives the general solution of the strongly constrained linear congruence system of module pairwise coprime, but it can not directly give the minimum natural number solution of the system of congruence equations. Nor does it clarify the necessary and sufficient conditions for the weak constrained linear congruence equations with different modules to have a solution and the formula of weakly constrained general solution. Here, the Chinese remainder theorem is promoted, clarifying the conditional equations for the existence of solutions to weakly constrained systems of linear congruence equations. The new concise formulas are utilized to express the general solutions of strongly constrained congruence systems and weakly constrained congruence systems, thereby improving the theory of system of congruence equations. Then, the concise steps are provided to directly construct the general solutions of linear strongly constrained and weakly constrained system of congruence equations, in order to promote the popularization of congruence equation theory on a wider range. Finally, the question of whether a universal method for solving the rational number solution of the minimum number of digits for an indefinite system of equations exists was brought up.

Keywords: Congruence equations, module pairwise coprime, module pairwise not coprime, Chinese remainder theorem, elementary algebra

MSC(2020) Subject Classification: 11A07, 11R04

Contents

Citation: Dongfang, X. D. Dongfang Brief General Solutions to Congruence Equations. *Mathematics & Nature* **3**, 202301 (2023).

https://orcid.org/0000-0002-3644-5170

1 Introduction

The Chinese remainder theorem[1-3], also known as the Sun Tzu theorem[4-6], is a very ancient principle for solving general solutions to congruence equations. The Chinese remainder theorem provides a general solution for a strongly constrained system of linear congruence equations that satisfy module pairwise coprime. For hundreds of years, the application of linear congruence equations was limited to digital games, and it was not until the rise of computer science that linear congruence equations were applied in computer arithmetic[7] and information science[8-10], which sparked widespread interest in the Chinese remainder theorem.

The focus now is on discussing the most concise formulaic description of the programmatic calculation of the Chinese remainder theorem, the conditions for the existence of solutions and expressions for general solutions to weakly constrained system of linear congruence equations with pairwise differences, as well as the concise steps for constructing solutions to strongly constrained and mutually constrained system of congruence equations, so that congruence equation theory can be popularized on a wider range. Finally, a rational number solution for the minimum number of digits of an indefinite equation system was introduced, while the question of whether there is a general method to obtain a rational number solution for the minimum number of digits of an indefinite equation system of the same kind remains to be solved.

2 Formulaic description of the Chinese remainder theorem

Lemma (Chinese Remainder Theorem) Let both m_i and a_i be integers, where m_i is mutually prime, and the integer $i = 1, 2, \cdots, n$ is a congruence system of equations,

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{2.1}$$

has countless solutions, and the expression for the general solution is

$$x = \left(r + \sum_{i=1}^{n} \frac{a_i t_i}{m_i} \right) \prod_{j=1}^{n} m_j \tag{2.2}$$

Where r is an arbitrary integer and $t_i \, (t_i < m_i)$ is the minimum natural number solution of the double module arithmetic equation

$$\operatorname{mod}\left[t_i \operatorname{mod}\left(m_i^{-1} \prod_{j=1}^{n} m_j, m_i \right), m_i \right] \equiv 1 \tag{2.3}$$

The integer m_i in the congruence equation system (2.1) mentioned above is called the module, the integer a_i is called the remainder, and t_i is called the inverse element in the sense of the module m_i of $m_i^{-1} \, (m_1 m_2 \cdots m_n)$. Using the expression method of scientific computing software, $\operatorname{mod}(N, M)$ is the remainder of integer N divided by integer M, that is, the remainder of integer N to module M. The conditional equation (2.3) is a double congruence equation that determines

the integer t_i that is not greater than the module m_i. First calculate the total modulus product $(m_1 m_2 \cdots m_n)$ of the congruence equation system divided by the quotient of module m_i and the remainder of module m_i, and then solve the congruence equation that the product of this remainder multiplied by the inverse element t_i has a remainder of 1 for module m_i.

The Chinese remainder theorem is the fundamental principle for solving linear congruence equations, but it is not perfect and has two reserved problems. Firstly, the Chinese Remainder Theorem does not clarify the conditions for the existence of solutions to weakly constrained congruence systems with two distinct modules, nor does it provide a general solution formula for the case where there is a solution; Secondly, the Chinese remainder theorem cannot directly represent the minimum natural number solution of a congruence equation system, and the result is a congruence equation with the product of all modules as modules, rather than a simplified form where the constant part is the minimum natural number solution.

Example 1. Find the general solution of the following congruence equation system,

$$\begin{cases} x \equiv 281 \pmod{541} \\ x \equiv 313 \pmod{601} \\ x \equiv 379 \pmod{863} \\ x \equiv 98 \pmod{3571} \end{cases} \tag{2.4}$$

The modulus and remainder of the congruence equation system in the proposition are

$$m_1 = 541,\ m_2 = 601,\ m_3 = 863,\ m_4 = 3571$$
$$a_1 = 281,\ a_2 = 313,\ a_3 = 379,\ a_4 = \sigma$$

Therefore, $\prod_{j=1}^{n} m_j = 1002010754993$. Substitute it into (2.3) to obtain four double congruence equations regarding the inverse element t_i,

$$\begin{aligned} &\mod \left[t_1 \bmod \left(\frac{1002010754993}{541}, 541 \right), 541 \right] \equiv 1 \\ &\mod \left[t_2 \bmod \left(\frac{1002010754993}{601}, 601 \right), 601 \right] \equiv 1 \\ &\mod \left[t_3 \bmod \left(\frac{1002010754993}{863}, 863 \right), 863 \right] \equiv 1 \\ &\mod \left[t_4 \bmod \left(\frac{1002010754993}{3571}, 3571 \right), 3571 \right] \equiv 1 \end{aligned}$$

That is,

$$\begin{aligned} &\mod (154 t_1, 541) \equiv 1 \\ &\mod (285 t_2, 601) \equiv 1 \\ &\mod (37 t_3, 863) \equiv 1 \\ &\mod (1787 t_4, 3571) \equiv 1 \end{aligned}$$

The minimum natural number solutions of the four inverse elements are

$$t_1 = 404,\ t_2 = 504,\ t_3 = 70,\ t_4 = 1191$$

Substituting them into (2.2) yields the general solution of the congruence equation system (2.4),

$$\begin{aligned} x &= \left(r + \sum_{i=1}^{4} \frac{a_i t_i}{m_i}\right) \prod_{j=1}^{4} m_j \\ &= \left(\frac{281 \times 404}{541} + \frac{313 \times 504}{601} + \frac{379 \times 70}{863} + \frac{98 \times 1191}{3571} + r\right) \prod_{j=1}^{4} m_j \\ &= 536827387746612 + 1002010754993r \end{aligned} \tag{2.5}$$

The constant part in the above general solution expression is much larger than the total module product $\prod_{j=1}^{n} m_j$, being not the minimum natural number solution. The reduced general solution with the constant part being the minimum natural number solution is the congruence result of (2.5) to the module $\prod_{j=1}^{n} m_j$,

$$x = 751633825357 + 1002010754993k$$

3 Concise solutions to strongly constrained congruence equations

Now let's solve the first reservation problem of the Chinese remainder theorem, which is to provide a simplified general solution for the strongly constrained congruence equations with its module pairwise coprime, so that the constant part of the general solution of the congruence equation system is the minimum natural number solution of the congruence equation system.

Theorem 1 (Dongfang) Assumes that m_i and a_i are both integers, m_i is mutually prime, integer $i = 1, 2, \cdots, n$, integer $n \geqslant 2$, then the congruence equation system

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

has countless solutions, and the expression for the general solution is

$$x = \sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j\right) s_i + a_1 + r \prod_{j=1}^{n} m_j \tag{3.1}$$

Where s_i is the minimum natural number solution of the module arithmetic equation

$$\mod \left[\sum_{i=1}^{l-1} \left(\prod_{j=1}^{i} m_j\right) s_i + a_1 - a_l, m_l\right] \equiv 0 \tag{3.2}$$

where $l = 2, 3, \cdots, n$ and r is any integer.

Proof. Prove this theorem using mathematical induction[11,12]. When $n = 2$, because $(m_1, m_2) = 1$, according to the theory of Diophantine equations, let k_1 be an integer, and the binary quadratic indefinite equation $m_1 s_1 - m_2 k_1 = a_2 - a_1$ with respect to integer s_1 and integer k_1 has a solution, that is, there exists a minimum natural number s_1 that holds the congruence equation

$m_1s_1 + a_1 - a_2 \equiv 0 \pmod{m_2}$, where r is any integer, so

$$\begin{aligned} x - a_1 &= m_1 (rm_2 + s_1) \equiv 0 \pmod{m_1} \\ x - a_2 &= rm_1m_2 + (m_1s_1 + a_1 - a_2) \\ &= m_1s_1 + a_1 - a_2 \equiv 0 \pmod{m_2} \end{aligned}$$

The simplified representations of both are exactly $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$. So, the theorem holds when $n = 2$.

When $n = 3$, the strong constraint condition $(m_1m_2, m_3) = 1$, and it has been proven that $m_1s_1 + a_1 - a_2 \equiv 0 \pmod{m_2}$. Assuming k_2 is an integer, the first-order indefinite equation $m_1m_2s_2 - k_2m_2 = a_3 - a_1 - m_1s_1$ with respect to integer s_2 and integer k_2 has a solution, that is, there exists a minimum natural number s_2 that holds the congruence equation $m_1m_2s_2 + m_1s_1 + a_1 - a_3 \equiv 0 \pmod{m_3}$. Take $x = rm_1m_2m_3 + m_1m_2s_2 + m_1s_1 + a_1$, where r is any integer, so

$$\begin{aligned} x - a_1 &= rm_1m_2m_3 + m_1m_2s_2 + m_1s_1 \equiv 0 \pmod{m_1} \\ x - a_2 &= rm_1m_2m_3 + m_1m_2s_2 + m_1s_1 + a_1 - a_2 \\ &= m_1s_1 + a_1 - a_2 \equiv 0 \pmod{m_2} \\ x - a_3 &= rm_1m_2m_3 + m_1m_2s_2 + m_1s_1 + a_1 - a_3 \\ &= m_1m_2s_2 + m_1s_1 + a_1 - a_3 \equiv 0 \pmod{m_3} \end{aligned}$$

In other words, $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $x \equiv a_3 \pmod{m_3}$. Therefore, the theorem holds when n=3.

Let Theorem 1 hold for any integer $n > 3$, that is, if $m_1, m_2, \cdots, m_n$ are mutually prime, and the congruence equation system $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$,..., $x \equiv a_n \pmod{m_n}$ has countless solutions, the general solution is

$$x = r' \prod_{j=1}^{n} m_j + \sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1$$

Where $\sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 - a_l \equiv 0 \pmod{m_n}$ and r' is any integer. So for integer $n+1$, taking $r' = rm_{n+1} + s_n$, there is

$$\begin{aligned} x &= (rm_{n+1} + s_n) \prod_{j=1}^{n} m_j + \sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 \\ &= rm_{n+1} \prod_{j=1}^{n} m_j + \left[s_k \prod_{j=1}^{n} m_j + \sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j \right) s_i \right] + a_1 \\ &= r \prod_{j=1}^{n+1} m_j + \sum_{i=1}^{n} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 \end{aligned}$$

Because under strong constraint condition $\left(\prod_{j=1}^{n} m_j, m_{n+1} \right) = 1$, let k_n be an integer, and the

indefinite equation

$$\prod_{j=1}^{n} m_j s_n - m_{n+1} k_n = a_{n+1} - a_1 - \sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j \right) s_i$$

for integer s_n and integer k_n must have a solution, i.e

$$\sum_{i=1}^{n} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 - a_{n+1} \equiv 0 \pmod{m_{n+1}}$$

And because $r \prod_{j=1}^{n+1} m_j = r m_{n+1} \prod_{j=1}^{n} m_j \equiv 0 \pmod{m_{n+1}}$, there is

$$r \prod_{j=1}^{n+1} m_j + \sum_{i=1}^{n} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 - a_{n+1} \equiv 0 \pmod{m_{n+1}}$$

or

$$r \prod_{j=1}^{n+1} m_j + \sum_{i=1}^{n} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 \equiv a_{n+1} \pmod{m_{n+1}}$$

Therefore,

$$x - a_{n+1} = r \prod_{j=1}^{n+1} m_j + \sum_{i=1}^{n} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 \equiv 0 \pmod{m_{n+1}}$$

The equivalent formula is $x \equiv a_{n+1} \pmod{m_{n+1}}$, which proves that Theorem 1 also holds for integers n+1.

According to mathematical induction, Theorem 1 holds for any integer n_2. Proof completed.

The Chinese remainder theorem and Theorem 1 respectively provide two forms of expression for the general solution of the modular pairwise coprime congruence equation system, with significant differences between the two expressions.

The conditional equation for constructing a general solution of a congruence equation system using the Chinese remainder theorem is a double congruence equation with respect to several inverse elements t_i, where the number of inverse elements is equal to the number of modules, and the expanded congruence equations are independent of each other. The conditional equation for constructing a general solution of a congruence equation system using Theorem 1 is a single congruence equation with several parameters s_i, where the number of parameters is 1 less than the number of modules. The expanded congruence equations are not completely independent, and the congruence equation with more parameters includes the parameters in the congruence equation with fewer parameters. In fact, they are a set of congruence equations constrained by each parameter s_i.

The complexity of determining the parameter s_i using Theorem 1 is the same as that of determining the inverse element t_i using the Chinese remainder theorem. Indeed, Chinese remainder theorem has a history of nearly 800 years and extensive application experience, making it easier to accept. Unlike the expression of the general solution of the congruence equation system given by the Chinese remainder theorem, Theorem 1 provides the expression of the general solution of the congruence equation system (3.1), where the constant part is the minimum natural number solution of the congruence equation system, and its general solution formula is called the simplified solution of the congruence equation system.

Example 2. Find the general solution of the following congruence equation system,

$$\begin{cases} x \equiv 347 \pmod{449} \\ x \equiv 517 \pmod{571} \\ x \equiv 601 \pmod{643} \\ x \equiv 521 \pmod{659} \\ x \equiv 379 \pmod{739} \end{cases} \tag{3.3}$$

The modulus and remainder of the congruence equation system in the proposition are

$$\begin{aligned} &m_1 = 449,\ m_2 = 571,\ m_3 = 643,\ m_4 = 659,\ m_5 = 739 \\ &a_1 = 347,\ a_2 = 517,\ a_3 = 601,\ a_4 = 521,\ a_5 = 379 \end{aligned} \tag{3.4}$$

From (3.2), take $n = 2,\ 3,\ 4,\ 5$, and obtain the congruence equation system for determining parameters $s_1,\ s_2,\ s_3,\ s_4$,

$$\begin{cases} \mod (m_1 s_1 + a_1 - a_2, m_2) \equiv 0 \\ \mod (m_1 s_1 + m_1 m_2 s_2 + a_1 - a_3, m_3) \equiv 0 \\ \mod (m_1 s_1 + m_1 m_2 s_2 + m_1 m_2 m_3 s_3 + a_1 - a_4, m_4) \equiv 0 \\ \mod [m_1 s_1 + m_1 m_2 s_2 + m_1 m_2 m_3 s_3 + m_1 m_2 m_3 m_4 s_4 + a_1 - a_5, m_n] \equiv 0 \end{cases}$$

Substitute (3.4) into the above equation system to obtain

$$\begin{cases} \mod (449 s_1 - 170, 571) \equiv 0 \\ \mod (449 s_1 + 256379 s_2 - 254, 643) \equiv 0 \\ \mod (449 s_1 + 256379 s_2 + 164851697 s_3 - 174, 659) \equiv 0 \\ \mod [449 s_1 + 256379 s_2 + 164851697 s_3 + 108637268323 s_4 - 32, 739] \equiv 0 \end{cases}$$

Solve the above congruence equations in order, and the minimum natural number solutions for each parameter obtained are

$$s_1 = 476,\ s_2 = 419,\ s_3 = 141,\ s_4 = 82$$

Substitute these parameters and (3.4) into formula (3.1) to obtain the general solution of the congruence equation system (3.3),

$$\begin{aligned} x &= \sum_{i=1}^{n-1} \left(\prod_{j=1}^{i} m_j \right) s_i + a_1 + r \prod_{j=1}^{n} m_j \\ &= m s_1 + m_1 m_2 s_2 + m_1 m_2 m_3 s_3 + m_1 m_2 m_3 m_4 s_4 + r \prod_{j=1}^{5} m_j \\ &= 8931607728635 + 80282941290697 r \end{aligned} \tag{3.5}$$

The constant part in the general solution (3.5) is smaller than the modulus product $\prod_{j=1}^{n} m_j$, so the constant part is the minimum natural number solution. This general solution is the simplified

general solution of the congruence equation system (3.3).

4 Concise solutions to weakly constrained congruence equations

Next, let's solve the second retention problem of the Chinese remainder theorem, which is to provide a simplified general solution for weakly constrained congruence equations with different modules, so that the constant part of the general solution of the weakly constrained congruence equation system is the minimum natural number solution of the congruence equation system.

Theorem 2 (Dongfang) Let the integer $m_1, m_2, \cdots, m_n$ be mutually exclusive, where n_2, denote the minimum common multiple of $m_1, m_2, \cdots, m_n$ as $[m_1, \cdots, m_n]$, If there exists all the smallest integers s_i that satisfy the module arithmetic equation

$$\mod\left(\sum_{i=1}^{l-1}[m_1,\cdots,m_i]\,s_i + a_1 - a_l, m_l\right) \equiv 0 \tag{4.1}$$

where $i = 1, 2, \cdots, l-1$, $l = 2, 3, \cdots, n$, then the congruence equation system

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

has countless solutions, and the expression for the general solution is

$$x = r\,[m_1,\cdots,m_n] + \sum_{i=1}^{n-1}[m_1,\cdots,m_i]\,s_i + a_1 \tag{4.2}$$

Where r is any natural number.

The process of proving Theorem 2 using mathematical induction is similar to that of Theorem 1, which is omitted here. In the next section, we will use the construction method of the solution of the congruence equation system to prove Theorem 2. The method of proof is also applicable to re proving Theorem 1. Here, we will first deal with two examples of finding the simplified general solution of weakly constrained congruence equations with two distinct modules.

Example 3. Find the general solution of the following congruence equation system,

$$\begin{cases} x \equiv 7 \pmod{30} \\ x \equiv 13 \pmod{28} \\ x \equiv 22 \pmod{75} \\ x \equiv 55 \pmod{63} \end{cases} \tag{4.3}$$

The modulus and remainder of the congruence equation system in the proposition are

$$\begin{aligned} &m_1 = 30,\ m_2 = 28,\ m_3 = 75,\ m_4 = 63 \\ &a_1 = 7,\ a_2 = 13,\ a_3 = 22,\ a_4 = 55, \end{aligned} \tag{4.4}$$

Calculate the minimum common multiple of each group of modules that sequentially increase module

$$\begin{aligned}&[m_1, m_2] = [30, 28] = 420\\ &[m_1, m_2, m_3] = [30, 28, 75] = 2100\\ &[m_1, m_2, m_3, m_4] = [30, 28, 75, 63] = 6300\end{aligned} \tag{4.5}$$

Substitute (4.4) and (4.5) into the three expansion equations of the conditional equation (4.1) of Theorem 2,

$$\begin{aligned}&m_1 s_1 + a_1 - a_2 \equiv 0 \pmod{m_2}\\ &[m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_3 \equiv 0 \pmod{m_3}\\ &[m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_3 \equiv 0 \pmod{m_4}\end{aligned}$$

Obtaining a congruence equation system for parameters s_1, s_2 and s_3,

$$\begin{aligned}&30 s_1 + 7 - 13 \equiv 0 \pmod{28}\\ &[30, 28]\, s_2 + 30 s_1 + 7 - 22 \equiv 0 \pmod{75}\\ &[30, 28, 75]\, s_3 + [30, 28]\, s_2 + 30 s_1 + 7 - 55 \equiv 0 \pmod{63}\end{aligned}$$

Simplify

$$\begin{aligned}&30 s_1 - 6 \equiv 0 \pmod{28}\\ &420 s_2 + 30 s_1 - 15 \equiv 0 \pmod{75}\\ &2100 s_3 + 420 s_2 + 30 s_1 - 42 \equiv 0 \pmod{63}\end{aligned}$$

The minimum natural number solution is

$$s_1 = 3,\ s_2 = 0,\ s_3 = 1 \tag{4.6}$$

Substitute (4.4) and (4.6) into the general solution formula (4.2) of Theorem 2 to obtain the general solution of the congruence equation system (4.3),

$$\begin{aligned}x &= [m_1, m_2, m_3, m_4]\, r + a_1 + m_1 s_1 + [m_1, m_2]\, s_2 + [m_1, m_2, m_3]\, s_3\\ &= [30, 28, 75, 63]\, r + 7 + 30 \times 3 + [30, 28] \times 0 + [30, 28, 75] \times 1\\ &= 6300 r + 2197\end{aligned} \tag{4.7}$$

Because 2197<6300, the constant part 2197 of (4.7) is the minimum natural number solution of the congruence equation system (4.3).

Example 4. Find the minimum universal remainder σ that makes the following congruence equations solvable,

$$\begin{cases} x \equiv 7 \pmod{30}\\ x \equiv 13 \pmod{28}\\ x \equiv 22 \pmod{75}\\ x \equiv \sigma \pmod{63}\end{cases} \tag{4.8}$$

The modulus and remainder of the congruence equation system in the proposition are

$$\begin{aligned} &m_1 = 30,\ m_2 = 28,\ \ m_3 = 75,\ \ \ m_4 = 63 \\ &a_1 = 7,\ a_2 = 13,\ \ a_3 = 22,\ \ \ a_4 = \sigma \end{aligned} \tag{4.9}$$

Calculate the minimum common multiple of each group of modules that sequentially increase module

$$\begin{aligned} &[m_1, m_2] = [30, 28] = 420 \\ &[m_1, m_2, m_3] = [30, 28, 75] = 2100 \\ &[m_1, m_2, m_3, m_4] = [30, 28, 75, 63] = 6300 \end{aligned} \tag{4.10}$$

Substitute (4.9) and (4.10) into the three expansion equations of the conditional equation (4.1) of Theorem 2

$$\begin{aligned} &m_1 s_1 + a_1 - a_2 \equiv 0 \pmod{m_2} \\ &[m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_3 \equiv 0 \pmod{m_3} \\ &[m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_3 \equiv 0 \pmod{m_4} \end{aligned}$$

Obtaining a congruence equation system for parameters s_1, s_2 and s_3,

$$\begin{aligned} &30 s_1 + 7 - 13 \equiv 0 \pmod{28} \\ &[30, 28]\, s_2 + 30 s_1 + 7 - 22 \equiv 0 \pmod{75} \\ &[30, 28, 75]\, s_3 + [30, 28]\, s_2 + 30 s_1 + 7 - \sigma \equiv 0 \pmod{63} \end{aligned}$$

Its simplified form is

$$\begin{aligned} &30 s_1 + 7 - 13 \equiv 0 \pmod{28} \\ &420 s_2 + 30 s_1 + 7 - 22 \equiv 0 \pmod{75} \\ &2100 s_3 + 420 s_2 + 30 s_1 + 7 - \sigma \equiv 0 \pmod{63} \end{aligned}$$

Find the minimum natural number solution from the first two congruence equations

$$s_1 = 3,\ s_2 = 0$$

Substituting into the third congruence equation to obtain the congruence equations for s_3 and σ

$$2100 s_3 + 97 - \sigma \equiv 0 \pmod{63}$$

According to the principle of first order indefinite equations, the minimum natural number solution is,

$$s_3 = 2,\ \sigma = 13$$

So, the minimum residue that makes the congruence equation system (4.8) solvable is $\sigma = 13$. According to the general solution expression (4.2) of Theorem 2, the general solution of the equation system that satisfies the condition is,

$$\begin{aligned} x &= [m_1, m_2, m_3, m_4]\, r + a_1 + m_1 s_1 + [m_1, m_2]\, s_2 + [m_1, m_2, m_3]\, s_3 \\ &= [30, 28, 75, 63]\, r + 7 + [30] \times 3 + 0 + [30, 28, 75] \times 2 \\ &= 6300 r + 4297 \end{aligned}$$

Because 4297<6300, the constant part 4297 of the above result is the minimum natural number solution that satisfies the condition for the congruence equation system (4.8).

5 Proof of solutions to weakly constrained congruence equations

Although mathematical induction is strict in proving propositions, it often conceals the reasoning process from conditions to conclusions, resulting in limited popularization and development of theory. For example, using mathematical induction can effectively prove the formula for the sum of squares or sum of cubes of continuous natural numbers. However, due to the lack of a summation process in the proof process, beginners cannot comprehend the derivation method of formulas for higher power sums of continuous natural numbers. Therefore, the deductive proof method for constructing propositions conclusions should be advocated. The following uses the method of constructing general solutions to prove Theorem 2 for solving weakly constrained linear congruence systems, and the proof process also applies to the proof of Theorem 1.

The proof of Theorem 2. Let the general form of a congruence equation system containing n congruence equations be

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Among them, n modules m_i differ from each other in pairs. In order to construct the general solution of the congruence equation and find the conditions for its existence, the congruence equation system is first written as an algebraic equation system

$$\begin{aligned} x &= m_1 N_1 + a_1 \\ x &= m_2 N_2 + a_2 \\ x &= m_3 N_3 + a_3 \\ &\vdots \\ x &= m_n N_n + a_n \end{aligned} \tag{5.1}$$

(5.2)

Where $i = 1, 2, \cdots, n$, N_i are all arbitrary integers. Use $[m_1, \cdots, m_n]$ to represent the least common multiple of $m_1, m_2, \cdots, m_n$.

i) Eliminating x from the first and second equations of the congruence equation system (4.10), find N_2, and the result is

$$N_2 = \frac{m_1 N_1 + a_1 - a_2}{m_2}$$

Let r_1 be any integer, and s_1 be the smallest positive integer that appears in the conditional formula. Because N_1 and N_2 are both arbitrary integers, one of the necessary and sufficient

conditions for the above equation to satisfy the division relationship $m_2 | (m_1 N_1 + a_1 - a_2)$ is that any integer N_1 satisfies the division equation,

$$N_1 = \frac{[m_1, m_2]}{m_1} r_1 + s_1 \tag{5.3}$$

Substitute into the aforementioned equation and simplify to obtain

$$N_2 = \frac{[m_1, m_2]}{m_2} r_1 + \frac{m_1 s_1 + a_1 - a_2}{m_2}$$

The first item is already an integer. The second term is also an integer, which must satisfy the condition

$$m_2 | (m_1 s_1 + a_1 - a_2)$$

i.e

$$\mod (m_1 s_1 + a_1 - a_2, m_2) \equiv 0 \tag{5.4}$$

Substitute (5.3) into $x = m_1 N_1 + a_1$ of (5.1) to obtain

$$x = [m_1, m_2] r_1 + m_1 s_1 + a_1 \tag{5.5}$$

ii) Substitute the value of x obtained above (5.5) into the third equation of the congruence equation system (4.10), and calculate N_3. The result is

$$N_3 = \frac{[m_1, m_2] r_1 + m_1 s_1 + a_1 - a_3}{m_3}$$

Let r_2 be any integer, and s_2 be the smallest positive integer that appears in the conditional formula. Because N_3 and r_1 are both arbitrary integers, one of the necessary and sufficient conditions for the above equation to satisfy the division relationship

$$m_3 | (r_1 [m_1, m_2] + m_1 s_1 + a_1 - a_3)$$

is that any integer r_1 satisfies the division equation,

$$r_1 = \frac{[m_1, m_2, m_3]}{[m_1, m_2]} r_2 + s_2 \tag{5.6}$$

Substitute into the aforementioned equation and simplify to obtain

$$N_3 = \frac{[m_1, m_2, m_3]}{m_3} r_2 + \frac{[m_1, m_2] s_2 + m_1 s_1 + a_1 - a_3}{m_3} \tag{5.7}$$

The first item is already an integer. The second term is also an integer, which must satisfy the condition

$$m_3 | ([m_1, m_2] s_2 + m_1 s_1 + a_1 - a_3)$$

i.e

$$\mod ([m_1, m_2] s_2 + m_1 s_1 + a_1 - a_3, m_3) \equiv 0 \tag{5.8}$$

Substitute (5.7) into $x = m_3 N_3 + a_3$ of (5.1) to obtain

$$x = [m_1, m_2, m_3] r_2 + [m_1, m_2] s_2 + m_1 s_1 + a_1 \tag{5.9}$$

iii) Substitute the value of x obtained above (5.9) into the third equation of the congruence equation system (4.10), and calculate N_4. The result is

$$N_4 = \frac{[m_1, m_2, m_3]\, r_2}{m_4} + \frac{[m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_4}{m_4}$$

Let r_3 be any integer, and s_3 be the smallest positive integer that appears in the conditional formula. Because N_4 and r_2 are both arbitrary integers, one of the necessary and sufficient conditions for the above equation to satisfy the division relationship

$$m_4 | \left([m_1, m_2, m_3]\, r_2 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_4\right)$$

is that any integer r_2 satisfies the division equation,

$$r_2 = \frac{[m_1, \cdots, m_4]}{[m_1, m_2, m_3]} r_3 + s_3 \tag{5.10}$$

Substitute into the aforementioned equation and simplify to obtain

$$N_4 = \frac{[m_1, \cdots, m_4]}{m_4} r_3 + \frac{[m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_4}{m_4} \tag{5.11}$$

The first item is already an integer. The second term is also an integer, which must satisfy the condition

$$m_4 | \left([m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_4\right)$$

i.e

$$\mod \left([m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_4, m_4\right) \equiv 0 \tag{5.12}$$

Substitute (5.11) into $x = m_4 N_4 + a_4$ of (5.1) to obtain

$$x = [m_1, \cdots, m_4]\, r_3 + [m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 \tag{5.13}$$

iv) Further introduce any integerr_4, r_5 , $\cdots$, r_{n-2} and the smallest positive integer s_4, s_5, $\cdots$, s_{n-2} that will appear in the conditional formula. Substitute x into the subsequent congruence equations of the congruence equation system, eliminating x. Calculate sequentially and then guess the necessary and sufficient conditions for N_{n-1} to be an integer through induction

$$\mod \left[\begin{pmatrix} [m_1, \cdots, m_{n-2}]\, s_{n-2} + \cdots + [m_1, m_2, m_3]\, s_3 \\ + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 - a_n \end{pmatrix}, m_n \right] \equiv 0 \tag{5.14}$$

as well as the finally calculated the expression for x,

$$x = \left\{ \begin{matrix} [m_1, \cdots, m_{n-1}]\, r_{n-2} + [m_1, \cdots, m_{n-2}]\, s_{n-2} + \cdots \\ + [m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1 \end{matrix} \right\} \tag{5.15}$$

v) Substitute the value of x obtained above (5.15) into the last equation of the congruence equation

system (4.10), and calculate N_n. The result is

$$N_n = \frac{[m_1,\cdots,m_{n-1}]\,r_{n-2}}{m_n} + \frac{1}{m_n}\left\{\begin{array}{l}[m_1,\cdots,m_{n-2}]\,s_{n-2}+\cdots\\ +[m_1,m_2,m_3]\,s_3\\ +[m_1,m_2]\,s_2+m_1s_1+a_1-a_n\end{array}\right\}$$

Let $r_{n-1}=r$ be any integer, and s_{n-1} be the smallest positive integer that appears in the conditional formula. Because N_n and r_{n-1} are both arbitrary integers, one of the necessary and sufficient conditions for the integer equation to satisfy the integer division relationship mentioned above is that any integer r_{n-2} satisfies the integer division equation,

$$r_{n-2} = \frac{[m_1,\cdots,m_n]}{[m_1,\cdots,m_{n-1}]}r + s_{n-1} \tag{5.16}$$

Substitute into the aforementioned equation and simplify to obtain

$$N_n = \frac{[m_1,\cdots,m_n]}{m_n}r + \frac{1}{m_n}\left\{\begin{array}{l}[m_1,\cdots,m_{n-1}]\,s_{n-1}+[m_1,\cdots,m_{n-2}]\,s_{n-2}\\ +\cdots+[m_1,m_2,m_3]\,s_3+[m_1,m_2]\,s_2\\ +m_1s_1+a_1-a_n\end{array}\right\} \tag{5.17}$$

The first term is already an integer, and the necessary and sufficient condition for the second term to be an integer is

$$\mod\left[\left(\begin{array}{l}[m_1,\cdots,m_{n-1}]\,s_{n-1}+[m_1,\cdots,m_{n-2}]\,s_{n-2}+\cdots\\ +[m_1,m_2,m_3]\,s_3+[m_1,m_2]\,s_2+m_1s_1+a_1-a_n\end{array}\right),m_n\right]\equiv 0 \tag{5.18}$$

Substitute (5.17) into $x=m_nN_n+a_n$ of (5.1) to obtain

$$x = [m_1,\cdots,m_n]\,r + \left\{\begin{array}{l}[m_1,\cdots,m_{n-1}]\,s_{n-1}+[m_1,\cdots,m_{n-2}]\,s_{n-2}\\ +\cdots+[m_1,m_2,m_3]\,s_3+[m_1,m_2]\,s_2\\ +m_1s_1+a_1\end{array}\right\} \tag{5.19}$$

Equation (5.18) is exactly Equation (4.1) in Theorem 2, and Equation (5.19) is the general solution expression (4.2) in Theorem 2. So, Theorem 2 holds.

6 Concise formats for the popularization of congruence theorems

Abstracting the problem-solving method into a theorem facilitates memory and simplifies the application process. However, the abstract and strict expression of theorems often does not facilitate the popularization of theories. The construction and expression of general solutions to congruence equations are typical examples. The proof process of Theorem 1 and Theorem 2 is the construction process of the general solution of the congruence equation system, but it is not easy to understand. For a specific congruence equation system, it is very convenient to discard the theorem of constructing a general solution and simplify the construction of the solution for directly obtaining a general solution.

Since the theory of congruence equations has been applied in information science, it should be

widely popularized. This requires a programmatic step that highlights concise logic, and a concise and fluent expression of the mathematical principles and methods for constructing solutions to congruence equations, making it easy to understand. Here are two examples to illustrate the concise process of constructing general solutions for strongly and weakly constrained congruence systems.

Example 5. Find the general solution of the congruence equation system with modulo $m_1,\ m_2,\ m_3,\ m_4$ coprime and remainder are $a_1,\ a_2,\ a_3,\ a_4$.

The standard form of the congruence equation system described by the problem is

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ x \equiv a_4 \pmod{m_4} \end{cases}$$

Write it in the form of an algebraic indefinite system of equations

$$\begin{cases} x = m_1 N_1 + a_1 \\ x = m_2 N_2 + a_2 \\ x = m_3 N_3 + a_3 \\ x = n_4 N_4 + a_4 \end{cases}$$

Among them, $N_1,\ N_2,\ N_3$ and N_4N4 are all arbitrary integers. Let $r_1,\ r_2$ and $r_3 = r$ be any integer, and $s_1,\ s_2$ and s_3 be the smallest positive integers that appear in the conditional formula. Eliminate x from the first and second equations and find the expression for the any integer N_2

$$\begin{aligned} & m_2 N_2 + a_2 = m_1 N_1 + a_1 \\ & \Rightarrow N_2 = \frac{m_1 N_1 + a_1 - a_2}{m_2} \\ & \qquad \langle N_1 = m_2 r_1 + s_1 \uparrow \rangle \\ & \qquad = \frac{m_1 \left(m_2 r_1 + s_1\right) + a_1 - a_2}{m_2} \\ & \qquad = m_1 r_1 + \frac{m_1 s_1 + a_1 - a_2}{m_2} \\ & \langle \bmod \left(m_1 s_1 + a_1 - a_2, m_2\right) \equiv 0 \Rightarrow s_1 =? \downarrow \rangle \\ & \Rightarrow x = m_2 N_2 + a_2 = m_1 m_2 r_1 + m_1 s_1 + a_1 \end{aligned}$$

Substitute the above x into the third equation to find the expression for any integer N_3,

$$\begin{aligned} & m_3 N_3 + a_3 = m_1 m_2 r_1 + m_1 s_1 + a_1 \\ & \Rightarrow N_3 = \frac{m_1 m_2 r_1 + m_1 s_1 + a_1 - a_3}{m_3} \\ & \qquad \langle r_1 = m_3 r_2 + s_2 \uparrow \rangle \\ & \qquad = \frac{m_1 m_2 \left(m_3 r_2 + s_2\right) + m_1 s_1 + a_1 - a_3}{m_3} \end{aligned}$$

$$= m_1m_2r_2 + \frac{m_1m_2s_2 + m_1s_1 + a_1 - a_3}{m_3}$$
$$\langle \mathrm{mod}\,(m_1m_2s_2 + m_1s_1 + a_1 - a_3, m_3) \equiv 0 \Rightarrow s_2 =? \downarrow\rangle$$
$$\Rightarrow x = m_3N_3 + a_3 = m_1m_2m_3r_2 + m_1m_2s_2 + m_1s_1 + a_1$$

Substitute the above x into the forth equation to find the expression for any integer N_4,

$$m_4N_4 + a_4 = m_1m_2m_3r_2 + m_1m_2s_2 + m_1s_1 + a_1$$
$$\Rightarrow N_4 = \frac{m_1m_2m_3r_2 + m_1m_2s_2 + m_1s_1 + a_1 - a_4}{m_4}$$
$$\langle r_2 = m_4r_3 + s_3 \uparrow\rangle$$
$$= \frac{m_1m_2m_3\,(m_4r_3 + s_3) + m_1m_2s_2 + m_1s_1 + a_1 - a_4}{m_4}$$
$$= m_1m_2m_3r_3 + \frac{m_1m_2m_3s_3 + m_1m_2s_2 + m_1s_1 + a_1 - a_4}{m_4}$$
$$\langle \mathrm{mod}\,(m_1m_2m_3s_3 + m_1m_2s_2 + m_1s_1 + a_1 - a_4, m_4) \equiv 0 \Rightarrow s_3 =? \downarrow\rangle$$
$$\Rightarrow x = m_4N_4 + a_4$$
$$= m_1m_2m_3m_4r_3 + m_1m_2m_3s_3 + m_1m_2s_2 + m_1s_1 + a_1$$

The concise process for solving strongly constrained system of linear congruence equations mentioned above is a simplified expression of congruence theorem 1. The congruence theorem 2 for weakly constrained linear congruence systems with different moduli has a similar and concise process. The only difference is that the latter requires the concept of the least common multiple. The concise process of solving system of linear congruence equations will be able to popularize the knowledge of congruence theorem to the greatest extent possible.

Example 6. Find the general solution of a congruence equation system with modules $m_1,\ m_2,\ m_3,\ m_4$ that are different from each other and have remainders $a_1,\ a_2,\ a_3,\ a_4$.

The standard form of the congruence equation system described by the problem is

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ x \equiv a_4 \pmod{m_4} \end{cases}$$

Write it in the form of an algebraic indefinite system of equations

$$\begin{cases} x = m_1N_1 + a_1 \\ x = m_2N_2 + a_2 \\ x = m_3N_3 + a_3 \\ x = n_4N_4 + a_4 \end{cases}$$

Among them, $N_1,\ N_2,\ N_3$ and N_4N4 are all arbitrary integers. Let $r_1,\ r_2$ and $r_3 = r$ be any

integer, and $s_1,\ s_2$ and s_3 be the smallest positive integers that appear in the conditional formula. Eliminate x from the first and second equations and find the expression for the any integer N_2

$$\begin{aligned}
&m_2N_2+a_2=m_1N_1+a_1\\
&\Rightarrow N_2=\frac{m_1N_1+a_1-a_2}{m_2}\\
&\qquad\left\langle N_1=\frac{[m_1,m_2]\,r_1}{m_1}+s_1\uparrow\right\rangle\\
&\qquad=\frac{m_1}{m_2}\left(\frac{[m_1,m_2]\,r_1}{m_1}+s_1\right)+\frac{a_1-a_2}{m_2}\\
&\qquad=\frac{[m_1,m_2]\,r_1+m_1s_1+a_1-a_2}{m_2}\\
&\qquad=\frac{[m_1,m_2]}{m_2}r_1+\frac{m_1s_1+a_1-a_2}{m_2}\\
&\langle\mathrm{mod}\,(m_1s_1+a_1-a_2,m_2)\equiv 0\Rightarrow s_1=?\downarrow\rangle\\
&\Rightarrow x=m_2N_2+a_2=[m_1,m_2]\,r_1+m_1s_1+a_1
\end{aligned}$$

Substitute the above x into the third equation to find the expression for any integer N_3,

$$\begin{aligned}
&m_3N_3+a_3=[m_1,m_2]\,r_1+m_1s_1+a_1\\
&\Rightarrow N_3=\frac{[m_1,m_2]\,r_1+m_1s_1+a_1-a_3}{m_3}\\
&\qquad\left\langle r_1=\frac{[m_1,m_2,m_3]\,r_2}{[m_1,m_2]}+s_2\uparrow\right\rangle\\
&\qquad=\frac{[m_1,m_2]}{m_3}\left(\frac{[m_1,m_2,m_3]\,r_2}{[m_1,m_2]}+s_2\right)+\frac{m_1s_1+a_1-a_3}{m_3}\\
&\qquad=\frac{[m_1,m_2,m_3]\,r_2}{m_3}+\frac{[m_1,m_2]\,s_2+m_1s_1+a_1-a_3}{m_3}\\
&\langle\mathrm{mod}\,([m_1,m_2]\,s_2+m_1s_1+a_1-a_3,m_3)\equiv 0\Rightarrow s_2=?\downarrow\rangle\\
&\Rightarrow x=m_3N_3+a_3=[m_1,m_2,m_3]\,r_2+[m_1,m_2]\,s_2+m_1s_1+a_1
\end{aligned}$$

Substitute the above x into the forth equation to find the expression for any integer N_4,

$$\begin{aligned}
&m_4N_4+a_4=[m_1,m_2,m_3]\,r_2+[m_1,m_2]\,s_2+m_1s_1+a_1\\
&\Rightarrow N_4=\frac{[m_1,m_2,m_3]\,r_2+[m_1,m_2]\,s_2+m_1s_1+a_1-a_4}{m_4}\\
&\qquad\left\langle r_2=\frac{[m_1,\cdots,m_4]}{[m_1,m_2,m_3]}r_3+s_3\uparrow\right\rangle\\
&\qquad=\frac{[m_1,m_2,m_3]}{m_4}\left(\frac{[m_1,\cdots,m_4]}{[m_1,m_2,m_3]}r_3+s_3\right)+\frac{[m_1,m_2]\,s_2+m_1s_1+a_1-a_4}{m_4}\\
&\qquad=\frac{[m_1,\cdots,m_4]}{m_4}r_3+\frac{[m_1,m_2,m_3]\,s_3+[m_1,m_2]\,s_2+m_1s_1+a_1-a_4}{m_4}\\
&\langle\mathrm{mod}\,([m_1,m_2,m_3]\,s_3+[m_1,m_2]\,s_2+m_1s_1+a_1-a_4,m_4)\equiv 0\Rightarrow s_3=?\downarrow\rangle\\
&\Rightarrow x=m_4N_4+a_4
\end{aligned}$$

$$= [m_1, \cdots, m_4]\, r_3 + [m_1, m_2, m_3]\, s_3 + [m_1, m_2]\, s_2 + m_1 s_1 + a_1$$

7 The new application of indefinite equations in physics

A system of linear congruence equations is a system of equations composed of linear indefinite equations. To solve linear indefinite equations, the properties of congruence equations can be used to transform indefinite equations into congruence equations for solution.

Attempting to find a universal solution method for a class of linear indeterminate equations[13], in order to obtain the optimized rational number solution with the minimum number of digits for macroscopic quantum theory system of indeterminate equations, this raises our attention to the Chinese remainder theorem for solving system of linear congruence equations and provides a simplified general solution for system of congruence equations. One of the indefinite equations in macroscopic quantum theory[14] is as follows:

$$\begin{aligned}
\frac{x_1 + 2x_2 + 2^2x_3 + 2^3x_4 + 2^4x_5}{2\,(x_6 + 2x_7 + 2^2x_8 + 2^3x_9 + 2^4)} &= \frac{1034}{1625} \\
\frac{x_1 + 3x_2 + 3^2x_3 + 3^3x_4 + 3^4x_5}{3\,(x_6 + 3x_7 + 3^2x_8 + 3^3x_9 + 3^4)} &= \frac{1975}{4522} \\
\frac{x_1 + 4x_2 + 4^2x_3 + 4^3x_4 + 4^4x_5}{4\,(x_6 + 4x_7 + 4^2x_8 + 4^3x_9 + 4^4)} &= \frac{323}{966} \\
\frac{x_1 + 5x_2 + 5^2x_3 + 5^3x_4 + 5^4x_5}{5\,(x_6 + 5x_7 + 5^2x_8 + 5^3x_9 + 5^4)} &= \frac{26887}{99000} \\
\frac{x_1 + 6x_2 + 6^2x_3 + 6^3x_4 + 6^4x_5}{6\,(x_6 + 6x_7 + 6^2x_8 + 6^3x_9 + 6^4)} &= \frac{2676}{11687}
\end{aligned} \tag{7.1}$$

There is a group of minimum digit rational number solutions for this system of indefinite equations is,

$$\begin{aligned}
x_1 &= \frac{63}{16}, \quad x_2 = \frac{447}{32}, \quad x_3 = \frac{69}{4}, \\
x_4 &= \frac{69}{8}, \quad x_5 = \frac{3}{2}, \quad x_6 = \frac{105}{32}, \\
x_7 &= \frac{389}{32}, \quad x_8 = \frac{227}{16}, \quad x_9 = \frac{13}{2}
\end{aligned} \tag{7.2}$$

However, currently there is no universal method for obtaining the rational solution of the minimum number of digits, nor has it been proven that the rational solution of the minimum number of digits for the above indefinite system of equations is unique. The rational solution of the minimum number of digits has looser conditions than the integer solution, but lacks much theoretical experience.

When analyzing observational data of quantum phenomena[15], fitting a certain quantization law through the optimal rational number solution of an indefinite equation system is similar to the construction of a reduced general solution of a congruence equation system. The results can unexpectedly solve certain problems in physics, which should be a new starting point[16] for the

practical application of elementary number theory[7].

Acknowledgements *The authors wish to thank the polymath Andy Baker(University of Glasgow) for testing the validity of the theorems and to Dr. Dean Rubine(Former Faculty at Carnegie Mellon School Of Computer Science) for providing many revision suggestions .*

Conflict of interest The authors declare that they have no conflict of interest.

References

[1] H. Cohen, A course in computational algebraic number theory, Springer Science & Business Media, 2013.
[2] A. Kondracki, The chinese remainder theorem. Formalized Mathematics 6 (1997) 573-577.
[3] D. Pei, A. Salomaa, C. Ding, Chinese remainder theorem: applications in computing, coding, cryptography, World Scientific, 1996.
[4] J. Qin, Mathematical Treatise in Nine Chapters (in Chinese), Commercial Press, 1937.
[5] L. Hua, An introduction to the theory of numbers (in Chinese), Beijing: Science Press, 1957.
[6] J. Chen, Elementary Number Theory (in Chinese) [M], Beijing: Science Press, 1978.
[7] K.H. Rosen, Elementary number theory, Pearson Education London, 2011.
[8] J.H. Lac, Chinese remainder theorem and its applications. (2008).
[9] Grossschadl J. The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip. Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference. IEEE, 2001.
[10] K.K.A. Al-qader, Chinese Remainder Theorem and It's Applications. (2014).
[11] G.H. Hardy and E. M. Wright . An Introduction to the Theory of Numbers [M] Oxford University Press , 1979 .
[12] M. B . Nathanson . Elementary Methods in Number Theory [M] Springer - verlag , 2008 .
[13] C.C. Paige, M.A. Saunders, Solution of sparse indefinite systems of linear equations. SIAM journal on numerical analysis 12 (1975) 617-629.
[14] Dongfang, X. D. Dongfang Com Quantum Equations of LIGO Signal. *Mathematics & Nature* **1**, 202106 (2021).
[15] B.P. Abbott, R. Abbott, T. Abbott, M. Abernathy, F. Acernese, K. Ackley, C. Adams, T. Adams, P. Addesso, R. Adhikari, Observation of gravitational waves from a binary black hole merger. Physical review letters 116 (2016) 061102.
[16] Dongfang, X. D. The Morbid Equation of Quantum Numbers. *Mathematics & Nature* **1**, 202102 (2021).