Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/9/20240711

Research and application of Chinese remainder theorem

Qinnan Luo

School of Earth Science and Environmental engineering, Southwest Jiaotong University, Chengdu, 610000, China

2021114842@my.swjtu.edu.cn

Abstract. The Chinese remainder theorem (denoted it as " the theorem" in this article) was originally an important theorem in number theory. It played a vital role in the integer solution of the congruence equation in ancient times. With the continuous development of the algebraic system, the theorem naturally has different forms. This paper will show some research and applications based on the theorem. For example, the theorem in polynomial form, the theorem in the form of group theory, the theorem on unitary rings, the theorem on polynomial ring modules, etc. It is not difficult to know that integers and polynomials are special rings, so this the two forms of the theorem are the theorems that can be covered on the unitary ring. In fact, the theorem in the form of group theory is also covered. This paper will elaborate the first three forms of the theorem and give their specific applications.

Keywords: Chinese Remainder Theorem, Congruence, Polynomial, Matrix.

1. Introduction

The theorem comes from the mathematical classic of Sun Tzu. It gives a solution to congruence equation and has many applications in number theory. Cheng Dawei, a mathematician of the Ming Dynasty, gave a four-word formula for this solution in his 1593 "Comprehensive Collection of Mathematical Methods". After 1800, Western mathematicians Euler and Gauss also came to this theorem. In 1876, Mathiesen pointed out that Gauss's approach was consistent with Sun Tzu's. Later, Chinese remainder theorem has developed into a variety of algebraic systems and has many applications in theory and technology, especially in information technology. This paper will explain its different forms within the scope of Abstract algebra and give specific applications.

The theorem in Number Theory can be proved by Euclidean algorithm or by the principle of the drawer theorem [1]. This article adopts the first method and provides its application in solving integer solutions of congruence equation system and solving higher-order congruence equations. The theorem in number theory can be used in real life, such as timing [2]. It also plays an important role in valuation theory [2].

With the development of polynomial theory, the theorem has also been extended to polynomials. The theorem in polynomial theory can be proved by construction [3]. It can be used to prove the construction of polynomials. The existence of Jordan Chevalley decomposition is a classic application [3]. In addition, it can also be used to prove Lagrange interpolation formula [4]. In fact, the polynomial K [x] on the field K and the Matrix polynomial K [A] on the field K can be seen as the extension ring of K, Therefore,

DOI: 10.54254/2753-8818/9/20240711

indefinite element x can be substituted by either any polynomial in K [x] or any polynomial of matrix A [5]. Therefore, Chinese remainder theorem can also be applied to the problem of matrix existence [6, 7].

With Abel and Galois' research on whether there are radical solutions to the unary Quintic equation, Abstract algebra has become a basic and important branch of algebra. It is not difficult to know that integers, all matrices M (K) on the number field K, and polynomials K [x] on the number field K are special unitary rings. It is natural to think that the theorem can be generalized to a more general form - the Chinese remainder theorem on a unitary ring [8]. This generalization not only includes three special cases, we also provide a solution for finding the square root of the residual class ring. This solution not only has applications in fields such as public key cryptography [9], but also can be used for decomposing additive finite p-groups (Although other methods such as module theory can be used to solve a more general case - the decomposition of finite Abel groups) [10].

It is natural to think that Chinese remainder theorem should be extended to other algebra theories. For example, Chinese remainder theorem on the module of Polynomial ring [11]. And use the Gröbner basis theory and method of module to find the polynomial vector that satisfies the Chinese remainder theorem of module, so as to find the solution of the congruence equation system on the module of Polynomial ring. In 1993, the concept of BCI semigroups was introduced in reference [12], which is a generalization of the concept of rings. In 1998, A further studied this type of algebraic system and introduced the concepts of IS algebra and I-ideals [13, 14]. In [15], it tries to extend the Chinese remainder theorem to IS algebra system and establishes the theorem of IS algebra. As an application, an isomorphism theorem for IS algebra also be given.

2. Theorems

The following five theorems are five forms of Chinese remainder theorems. Theorem 1 and Theorem 2 are the theorem in the form of number theory. Theorem 3 is the theorem in the polynomial form. Theorem 4 is the theorem in the form of group theory, and Theorem 5 is the theorem in the form of ring theory. Lemma 1 and Lemma 2 are used to prove the theorem in the form of ring theory, that is, Theorem 5.

Theorem 1. Suppose $m = m_1 m_2 \ldots m_k$ and $m_1, m_2, \ldots, m_k$ are positive integers that are pairwise and mutually prime. $M_i = \frac{m}{m_i}, 1 \le i \le k$. Then for any positive integer $c_1, c_2, \ldots, c_k$, congruence equation system:

$$\begin{cases} x \equiv c_1 (mod m_1) \\ x \equiv c_2 (mod m_2) \\ \ldots \\ x \equiv c_k (mod m_k) \end{cases} \tag{1}$$

has a solution $x = \sum_{j=1}^{k} a_j M_i M_i'$,where $M_i' (1 \le i \le k)$ satisfy $M_i M_i' \equiv 1 (mod m_i)$.

Proof: Since $(M_i, m_i) = 1$, M_i' and y_i can be found by rolling and dividing and M_i' , y_i, satisfy:

$$M_i M_i' + y_i m_i = 1 \tag{2}$$

Thus $M_i M_i' \equiv 1 (mod m_i)$. This implies:

$$a_i M_i M_i' \equiv a_i (mod m_i), 1 \le i \le k \tag{3}$$

By $m_i M_i = m_j M_j = m$, $(m_i, m_j) = 1, \Rightarrow m_i | M_j, i \ne j$. This implies:

$$\sum_{j=1}^{k} a_j M_i M_i' \equiv a_i M_i M_i' \equiv a_i (mod m_i) \tag{4}$$

And (4) implies:

$$\sum_{j=1}^{k} a_j M_i M_i' \equiv a_i (mod [m_1, m_2, \ldots, m_k]) \equiv a_i (mod m) \tag{5}$$

DOI: 10.54254/2753-8818/9/20240711

$$x \equiv \sum_{j=1}^{k} a_j M_i M_i^{'}(modm) \tag{6}$$

Where formula (6) is the solution.

Theorem 2. Suppose $(m_1, m_2) = 1$ and $m = m_1 m_2, (a_1, m_1)|c_1, (a_2, m_2)|c_2$, the equation $\begin{cases} a_1 x \equiv c_1(modm_1) \\ ax_2 \equiv c_2(modm_2) \end{cases}$ has solution. The solution is $M_1 M_1' q_1 + M_2 M_2' q_2(modm)$ and $q_1 = x_1 \frac{m_1}{d_1} k_1(k_1 = 1, \dots)$, $q_2 = x_2 \frac{m_2}{d_2} k_2(k_2 = 1, \dots)$, $d_1 = (a_1, m_1), d_2 = (a_2, m_2)$. x_1, x_2 are the particular solutions of $ax_1 \equiv c_1(modm_1), ax_2 \equiv c_2(modm_2)$. M_i' satisfies $M_i M_i' \equiv 1(modm_i), i = 1, 2$.

Proof: Since $(a_1, m_1)|c_1$, $(a_2, m_2)|c_2$,$a_1 x \equiv c_1(modm_1)$ and $x \equiv c_2(modm_2)$ have solutions.

The solution of $a_1 x \equiv c_1(modm_1)$ is $q_1 = x_1 \frac{m_1}{d_1} k_1(k_1 = 1, \dots)$. The solution of $ax_2 \equiv c_2(modm_2$ is $q_2 = x_2 \frac{m_2}{d_2} k_2(k_2 = 1, \dots)$.

Hence $\begin{cases} a_1 x \equiv c_1(modm_1) \\ ax_2 \equiv c_2(modm_2) \end{cases}$ and $\begin{cases} x \equiv x_1 + \frac{m_1}{d_1} k_1(modm_1) \\ x \equiv x_2 + \frac{m_2}{d_2} k_2(modm_2) \end{cases}$ have the same number of solutions and solutions $\begin{cases} \mathrm{x} \equiv \mathrm{x}_1 + \frac{\mathrm{m}_1}{\mathrm{d}_1} \mathrm{k}_1(\mathrm{modm}_1) \\ \mathrm{x} \equiv \mathrm{x}_2 + \frac{\mathrm{m}_2}{\mathrm{d}_2} \mathrm{k}_2(\mathrm{modm}_2) \end{cases}$ satisfies Preconditions for the Chinese Remainder Theorem.

Hence the solution is $x = M_1 M_1' q_1 + M_2 M_2' q_2(modm)$. M_i' satisfies $M_i M_i' \equiv 1(modm_i), i = 1,2$. $q_1 = x_1 \frac{m_1}{d_1} k_1(k_1 = 1, \dots)$, $q_2 = x_2 \frac{m_2}{d_2} k_2(k_2 = 1, \dots)$.

Hence the number of the solutions of $\begin{cases} a_1 x \equiv c_1(modm_1) \\ ax_2 \equiv c_2(modm_2) \end{cases}$ is $d = d_1 d_2$ and the solution is $x = M_1 M_1' q_1 + M_2 M_2' q_2(modm)$.

Theorem 3. If $\{f_i(x)|i = 1,2, \dots n\}$ are pairwise coprime polynomials, and $a_1(x), a_2(x), \dots, a_n(x)$ are n polynomials, then there has a polynomial $g(x), q_i(x)$ $(i = 1,2, \dots, n)$ such that $g(x) = f_i(x) q_i(x) + a_i(x)$ for each i [3].

Proof: Firstly, trying to prove there exists polynomials $g_i(x)$ s. t. for arbitrary i.

$$g_i(x) = f_i(x) q_i(x) + 1, f_j(x)|g_i(x)(i \neq j) \tag{7}$$

If this statement can be proved, just let $g(x) = \sum_{i=1}^{n} a_i(x) g_i(x)$ to finish the proof. Now construct $\mathrm{g_i}$ as follows: Since $f_1(x)$ and $f_j(x)(j \neq 1)$ are mutually prime, there exists $u_j(x)$, $v_j(x)$ st.

$$f_1(x) u_j(x) + f_j(x) v_j(x) = 1 \tag{8}$$

Let

$$g_1(x) = f_2(x) v_2(x) \dots f_n(x) v_n(x) = \left(1 - f_1(x) u_2(x)\right) \dots \left(1 - f_1(x) u_n(x)\right) \tag{9}$$

It is trivial that $\mathrm{g_1(x)}$ fulfils requirements. In the same way, $\mathrm{g_i(x)}$ can be constructed.

Theorem 4. Suppose $m = m_1 m_2 \dots m_s$, and $m_1, m_2, \dots, m_s$ are pairwise prime positive integers. Then $Z/mZ = Z/\bar{e_1} \oplus \dots \oplus Z/\bar{e_s} \cong Z/m_1 Z \oplus \dots \oplus Z/m_s Z$. $\bar{x} = b_1 \bar{e_1} + \dots + b_1 \bar{e_s} \mapsto (\overline{b_1}, \dots, \overline{b_s})$ [10].

Proof: Assertion: $Z\bar{e_i} \cong Z/m_i Z$ is a cyclic group of order $\mathrm{m}(i = 1, \dots, s)$. This means the order of $\bar{\mathrm{e}}_\mathrm{i}$ is $\mathrm{m_i}$. The proof of the assertion is as follows: (i) $m_i \bar{e_i} = \overline{m_i e_i} = \overline{m_i q_i u_i} = \overline{m_i u_i} = \bar{0}$. This means when $i \neq j, q_j \bar{e_j} = \bar{0}$. (ii) If $\overline{a e_i} = \bar{0}$, then for arbitrary x, since $x = \sum_{i=1}^{s} b_i \bar{e_i}$.

From (i), $a q_i . \bar{x} = b_1 a(q_i \bar{e_1}) + \dots + b_i q_i (a \bar{e_i}) + \dots + b_s a(q_i \bar{e_s}) = \bar{0}$. This means $m|aq_i$. Since $q_i = \frac{m}{m_i}$, $m_i|a$. This proves the order of $\bar{\mathrm{e}}_\mathrm{i}$ is m_i, $Z\bar{e_i} \cong Z/m_i Z$, $b\bar{e_i} \mapsto \bar{b}$ $(i = 1, \dots, s)$. It is not difficult to complete theorem proving by using assertions.

Lemma 1. Suppose R is a unitary ring, and I and J are ideals that are mutually prime to R, then $\mathrm{IJ + JI = I \cap J}$. In particular when R is unitary$\mathrm{IJ = I \cap J}$ [8].

Proof: It is trivial that:

DOI: 10.54254/2753-8818/9/20240711

$$IJ =< \{ab: a \in I, b \in J\} > \sqsubseteq J \cap I = I \cap J \tag{10}$$

Since $I \cap J$ is closed for addition, $IJ + JI$ is a subset of $I \cap J$.

Since I and J are prime, there exists $i \in I, j \in J$ st. $i + j = 1$. For arbitrary $k \in I \cap J$: $k = 1k = (i + j)k = ik + jk \in IJ + JI$. Hence $I \cap J$ is a subset of $IJ + JI$, $IJ + JI = I \cap J$. When R is a unitary ring $IJ = JI$, hence $IJ + JI = IJ$.

Lemma 2. Suppose R is a commutative monocycle, and $A_1, \ldots, A_n (n > 1)$ are pairwise prime ideals. Then $A_1, \ldots, A_{n-1}$ and $A_n$are mutually prime and $A_1 \ldots A_n = A_1 \cap \ldots \cap A_n$ [8].

Proof: When $n = 2$, just use lemma1 to complete proof.

Suppose $n > 2$, use lemma1, $A_1 \cap A_2 = A_1A_2$ and A_3 are prime. Hence $A_1 \cap A_2 \cap A_3 = A_1A_2 \cap A_3 = (A_1A_2)A_3$. Continue in the same way. Finally, it is not hard to get that $A_1, \ldots, A_{n-1}$ and $A_n$are mutually prime and $A_1 \ldots A_n = A_1 \cap \ldots \cap A_n$ [10].

Theorem 5. Suppose $A_1, A_2, \ldots, A_n$ are the ideals of pairwise coprimes on a monoid R. Then for arbitrary $a_1, \ldots, a_n \in R$,the set $\{x \in R:$ for all $i = 1, \ldots, n, x$ satisfies $x \equiv a_i (\mathrm{mod} A_i)$ is not empty, and is the residual class of module $\bigcap_{i=1}^{n} A_i$.Besides,$R/(A_1 \cap A_2 \ldots \cap A_n) \cong R/A_1 \oplus \ldots \oplus R/A_n$ [8].

Proof: When $n = 1$. It is trivial. Next suppose $n > 1$. For $i = 1,2, \ldots, n$, let $B_i = A_1 \ldots A_{i-1}A_{i+1}A_n$. Use lemma 2 B_i and A_i are prime, hence there exists $x_i \in B_i$ st. $1 - x_i \in A_i$.

When $1 \leq j \leq n$ and $i \neq j$, $x_i \in B_i \sqsubseteq A_j$. Hence for $i, j = 1,2, \ldots, n$, $x_i - \delta_{ij} \in A_j$. Let $x_0 = \sum_{i=1}^{n} a_i x_i$. For $1 \leq j \leq n, x_0 - a_j = \sum_{i=1}^{n} a_i (x_i - \delta_{ij}) \epsilon A_{ij}$. For arbitrary $x \in R$, it is trivial that $x \equiv a_j (\mathrm{mod} A_j)$ $(j = 1,2, \ldots, n)$ if and only if $x \equiv x_0 (\mathrm{mod} A_j)$ also if and only if $x - x_0 \in \bigcap_{i=1}^{n} A_i$. For $x \in R$, define $\sigma(x + \bigcap_{i=1}^{n} A_i) =< x + A_1, \ldots, x + A_n >$. This is a mapping from $R/\bigcap_{i=1}^{n} A_i$ to $R/A_1 \oplus \ldots \oplus R/A_n$.

For arbitrary $a_1, \ldots, a_n \in R$, there exists one unique modulo $\bigcap_{i=1}^{n} A_i$ remainder class $x + \bigcap_{i=1}^{n} A_i$ st. for each $j = 1, \ldots, n$, $x \equiv a_j (\mathrm{mod}(A_j)$ ie. $x + A_j = a_j + A_j$. Hence σ is bijective. For $\bar{x} = x + \bigcap_{i=1}^{n} A_i, \bar{x} = x + \bigcap_{i=1}^{n} A_i \in R/\bigcap_{i=1}^{n} A_i$, because $(x + A_i) + (y + A_i) = (x + y) + A_i$ and $(x + A_i)(y + A_i) = xy + A_i$.

It is not hard to verify $\sigma(x + y) = \sigma(\overline{x + y}) = \sigma(\bar{x}) + \sigma(\bar{y})$,$\sigma(\bar{x}\bar{y}) = \sigma(\overline{xy}) = \sigma(\bar{x})\sigma(\bar{y})$. Hence A is a ring homomorphism. Hence $R/(A_1 \cap A_2 \ldots \cap A_n) \cong R/A_1 \oplus \ldots \oplus R/A_n$.

3. Examples and discussion

The following 12 examples are the application of the theorem in different forms. Among them, Examples 1 to Example4 are the application of Theorem 1 and Theorem2, that is, the application of the theorem in the form of number theory. Examples 5 to Example7 are the application of Theory 3, that is, the application of the theorem in the form of polynomials to polynomials. Examples 8 to 10 are also applications of Theorem3, but in matrix theory. Example11 is the application of the theorem in the form of group theory, that is, the application of Theorem4. Example 12 is the application of the theorem in the form of ring theory, that is, the application of Theorem5. Lemma 3 is used to prove Example 7.

By applying Theorem1 and Theorem2, it is not hard to obtain solution to some congruence equations. Some examples are as follows.

Example 1. Find the integer solution of the equation $x^3 - 1 \equiv 0(\mathrm{mod}15)$.

Solution: Since $15 = 5 \times 3$ and $(3,5) = 1$, $x^3 - 1 \equiv 0(\mathrm{mod}15)$ and $\begin{cases} x^3 - 1 \equiv 0(\mathrm{mod}5) \\ x^3 - 1 \equiv 0(\mathrm{mod}3) \end{cases}$ have the same solution. If $x^3 - 1 \equiv 0(\mathrm{mod}3)$ has an integer solution, the solution must be obtained in the complete residual system modulo 3, that is, in -1, 0, 1, and put them into equation $x \equiv 1(\mathrm{mod}3)$ to obtain. In the same way, it can be known that the integer solution of $x^3 - 1 \equiv 0(\mathrm{mod}5)$ is obtained in the complete residual system 0, 1, 2, and 3 modulo 5, and put it into the equation to get $x \equiv 1(\mathrm{mod}5)$. So $\begin{cases} x^3 - 1 \equiv 0(\mathrm{mod}5) \\ x^3 - 1 \equiv 0(\mathrm{mod}3) \end{cases}$ and $\begin{cases} x^3 \equiv 1(\mathrm{mod}5) \\ x^3 \equiv 1(\mathrm{mod}3) \end{cases}$ have the same solution.

DOI: 10.54254/2753-8818/9/20240711

Since $\begin{cases} x^3 \equiv 1(\mathrm{mod}5) \\ x^3 \equiv 1(\mathrm{mod}3) \end{cases}$ satisfies the precondition of the theorem, using the application of the theorem, it is not hard to obtain the integer solution of $x^3 - 1 \equiv 0(\mathrm{mod}15)$ is $x \equiv 1(\mathrm{mod}15)$.

Example 2. Solving congruence equations $\begin{cases} x \equiv 2(mod3) \\ x \equiv 3(mod5). \\ x \equiv 2(mod7) \end{cases}$

Solution: $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, and they are pairwise prime. $m = 3 \times 5 \times 7 = 105$. $M_1 = 35$, $M_2 = 21$, $M_3 = 15$. By $M_i M_i' \equiv 1(\mathrm{mod}m_i) \Rightarrow M_1' = -1, M_2' = 1, M_3' = 1$. We have $35 \equiv -1(\mathrm{mod}3) \Longrightarrow 35 \times (-1) \equiv 1(\mathrm{mod}3)$. $21 \equiv 1(\mathrm{mod}5) \Rightarrow 21 \times 1(\mathrm{mod}5)$. $15 \equiv 1(\mathrm{mod}7) \Rightarrow 15 \times 1 \equiv 1(\mathrm{mod}7)$.

$$x \equiv \sum_{j=1}^{k} a_j M_i M_i^{'}(modm) \tag{11}$$

Thus $x = 2 \times 35 \times (-1) + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 23(mod105)$. Formula (11) is the solution.

Example 3. Solving congruence equations $\begin{cases} 2x \equiv 1(mod3) \\ 3x \equiv 2(mod4) \end{cases}$.

Solution: Because $m_1 = 3, m_2 = 4, (2,3)|1, (3,4)|2$, the congruence equations $2x \equiv 1(\mathrm{mod}3$ and $3x \equiv 2(\mathrm{mod}4)$ have solutions, and the number of solutions is $d_1 = (2,3) = 1, d_2 = (3,4) = 1$. From Theorem 2, it can be known that the number of solutions of $\begin{cases} 2x \equiv 1(\mathrm{mod}3) \\ 3x \equiv 2(\mathrm{mod}4) \end{cases}$ is $d = d_1 d_2 = 1$. It is trivial that $2x \equiv 1(\mathrm{mod}3)$ has one particular solution $x \equiv 2(\mathrm{mod}3)$, and $3x \equiv 2(\mathrm{mod}4)$ has one particular solutions $x \equiv 2(\mathrm{mod}4)$.

It is trivial that $M_1 = 4$, $M_2 = 3, q_1 = 2, q_2 = 2$. Let $M_1 M_1' \equiv 1(\mathrm{mod}3)$, $M_2 M_2' \equiv 1(\mathrm{mod}4)$.Then it can be obtained that $M_1' \equiv 1(\mathrm{mod}3), M_2' \equiv 3(\mathrm{mod}4)$. Let $M_1' = 1, M_2' = 3$, from lemma 1, the solution is $x = M_1 M_1' q_1 + M_2 M_2' q_2(\mathrm{mod}m)$. Substitute it into the equation, it is not hard to obtain the solution is $1 \times 4 \times 2 + 3 \times 3 \times 2(\mathrm{mod}12)$ i.e., the solution is $x \equiv 2(\mathrm{mod}12)$.

Next is an application of the theorem in number theory in the valuation theory.

Example 4. For arbitrary n p- valuation $V_{p_1}, V_{p_2}, \ldots, V_{p_n}, a_i \in Q\ (i = 1,2, \ldots, n)$ and arbitrary $\varepsilon > 0, p^{t_1}, p^{t_2}, \ldots, p^{t_m}$.Then there exists b satisfies: (i) $V_\infty(b - a_i) = |b - a_1| < \varepsilon$; (ii) $V_{p_i}(b - a_i) \leq p_i^{-l_i}$ $(i = 1,2, \ldots, n)$.

Proof: Suppose m is the lowest common denominator of $a_1, \ldots, a_n$. Let $P_l^{Si} = V_{p_i}(m), r_i = l_i + s_i (i = 1, \ldots, n)$, $r = \max\{1, r_1, \ldots, r_n\}$. Using the theorem, it is not hard to find a c which satisfy: $c \equiv ma_1(\mathrm{mod}p_1^r), c_2 \equiv ma_2(\mathrm{mod}p_2^r), \ldots, c_n \equiv ma_n(\mathrm{mod}p_n^r)$ i.e., $V_{p_i}(c - ma_i) \leq p_i^{-r}, V_{p_i}(\frac{c}{m} - a_i) \leq p_i^{-l_i}$.

Suppose $q = (p_1 \ldots p_n)^r$. Take the appropriate $u, v \in Z$st. $\left|\frac{c}{m} \frac{1+uq}{1+vq} - a\right| < \epsilon$. Then let $b = \left|\frac{c}{m} \frac{1+uq}{1+vq} - a\right|$, b satisfies the condition (i).

By the property of p-distance $D_p : \max\{(D_p(a,b), D_p(b,c)\} \geq D_p(a,c), V_{p_i}(b - a_i) = V_{p_i}\left(\left(b - \frac{c}{m}\right) + \left(\frac{c}{m} - a_i\right)\right) \leq \max\left\{V_{p_i}\left(b - \frac{c}{m}\right\} = V_{p_i}\left(\frac{c}{m} - a_i\right)\right\} = V_{p_i}\left(\frac{c}{m} - a_i\right) \leq p_i^{-l_i} (i = 1, \ldots, n)$.

The valuation theory is an important section of the field theory and an important tool for studying several important branches of modern mathematics, such as Algebraic number theory and commutative number theory. The above Example 1-3 is actually proof of the independence of valuation.

In daily life, what we need to notice is often not certain integers but rather the remainder obtained by dividing these numbers by a fixed number. For example, suppose it is 9 o'clock in the morning, what time was it two hours ago? We will immediately receive the correct answer at 7am; so what time is it after thirteen hours? The formula is $9 + 13 - 12 = 10$, which means 10 pm; What time will the watch pointer point to after 28 hours? The formula is $(9 + 28) - (3 \times 12) = 1$point.

DOI: 10.54254/2753-8818/9/20240711

The way to solve this problem is: if the current time is the time after B hours, just calculate $A + B = C\ (\mathrm{mod}12)$ The remainder C is the watch hours [2]. Using the Chinese remainder theorem in polynomial form, it is not hard to Lagrange interpolation formula.

Example 5. For function $f(x) = \sum_{i=1}^{n} a_i(x)M_i(x) = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{x-b_i}{b_j-b_i} (i \neq j)$, where $M_i(x) = \frac{(x-b_1)\ldots(x-b_{i-1})(x-b_{i+1})\ldots(x-b_n)}{(b_i-b_1)\ldots(b_i-b_{i-1})(b_i-b_{i+1})\ldots(b_i-b_{n)}}$ $(i = 1,2,\ldots,n)$ are n pairwise prime polynomials, b_i $(i = 1,2,\ldots,n)$ are unequal constants, a_i $i = (1,2,\ldots,n)$ are arbitrary constants [4].

Solution: According to the existence and uniqueness theorem of interpolating polynomials, just need to find polynomial $M_i(x)$ $i = 1 \ldots n)$ st: $M_i(x) \equiv 1(\mathrm{mod}x - b_i), M_i(x) \equiv 0(\mathrm{mod}x - b_j(i \neq j)$. $M_i(x) = \frac{(x-b_1)\ldots(x-b_{i-1})(x-b_{i+1})\ldots(x-b_n)}{(b_i-b_1)\ldots(b_i-b_{i-1})(b_i-b_{i+1})\ldots(b_i-b_{n)}}$ $(i = 1,2,\ldots,n)$ fulfils requirements.

Hence $f(x) = \sum_{i=1}^{n} a_i(x)M_i(x) = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{x-b_i}{b_j-b_i} (i \neq j)$ is what the Example5 asks for. It is not difficult to obtain another proof of the sum of squares formula by using Example5. Suppose the sum be the cubic polynomial f(n) of n, where n represents the number of terms, so $f(0) = 0, f(1) = 1, f(2) = 1, f(3) = 5$. Use interpolation formula $f(n) = 0 \times M_1(n) + 0 \times M_2(n) + 1 \times M_3(n) + 5 \times M_4(n) = \frac{(n-0)(n-1)(n-3)}{(2-0)(2-0)(2-3)} + 5 \times \frac{(n-0)(n-1)(n-2)}{(3-0)(3-1)(3-2)} = \frac{n(n-1)(2n-1)}{6}$. Hence $\sum_{i=1}^{n-1} i^2 = \frac{n(n-1)(2n-1)}{6}$ [4].

The next example is the direct application of the Chinese remainder theorem in polynomial form.

Example 6. f(x) is a polynomial with integer coefficients, for each positive integer m, write $N_m = |\{x \in Z|f(x) \equiv 0(\mathrm{mod}m)$. Prove when $m_1, \ldots, m_s$ are mutually prime, $N_{m_1 \ldots m_s} = N_{m_1} \ldots N_{m_s}$ [7].

Solution: Only need to prove when $s = 2$.Note $m = m_1 m_2$. $S = \{0 \leq x < m|f(x) \equiv 0(\mathrm{mod}m)\}$ and $S_i = \{0 \leq x < m_i|f(x) \equiv 0\ (\mathrm{mod}m_i)\}$ $i = 1.,2$.

The following proves that there is a natural one-to-one correspondence between S and $S_1 \times S_2$.Take any $x \in S$, that is $0 \leq x < m$ and $m|f(x)$.Note $x = q_i m_i + x_i$ where $0 \leq x_i < m_i$. q_i is integer.$m_i|x - x_i$.Notice that $x - x_i|f(x) - f(x_i)$, then $m_i|f(x_i)$, ie. $x_i \in S_i$.Hence $(x_1, x_2) \in (S_1 \times S_2)$.

In turn, Take any $(y_1, y_2) \in S_1 \times S_2$ ie. $m_1|f(y_1)$, $m_2|f(y_2)$.Use the Chinese remainder theorem, there exists a unique integer y. $0 \leq y < m_1 m_2 = m$ and satisfies $\begin{cases} y \equiv y_1(\mathrm{mod}m_1) \\ y \equiv y_2(\mathrm{mod}m_2) \end{cases}$.Since $m_i|y - y_i$, and $y - y_i|f(y) - f(y_i)$.Hence $m_i|f(y)$, $m_1 m_2|f(y)$, ie. $m|f(y)$, $y \in S$.This proves $N_{m_1 m_2} = |S| = |S_1 \times S_2| = N_{m_1} N_{m_2}$.

Lemma 3. Suppose $f(x)g(x) + h(x)k(x) = 1$, $u(x) = \sum_{j=0}^{n-1} \binom{m+n-1}{j} f(x)^m (f(x)g(x))^{n-1-j} (h(x)k(x))^j$. $v(x) = \sum_{j=n}^{m+n-1} \binom{m+n-1}{j} h(x)^n (f(x)g(x)^{m+n-1-j} (h(x)k(x))^{j-n}$. Then, $u(x)g(x)^m + v(x)h(x)^n = 1$, specially, $(g^m(x), k(x)^n) = 1$ [16].

Proof: Using the Binomial Expansion Theorem: $1 = (f(x)g(x) + h(x)k(x))^{m+n-1} = \sum_{j=0}^{m+n-1} \binom{m+n-1}{j} (f(x)g(x))^{m+n-1-j} (h(x)k(x))^j = \sum_{j=0}^{n-1} \binom{m+n-1}{j} (f(x)g(x)^{m+n-1-j} (k(x)h(x))^j + \sum_{j=n}^{m+n-1} \binom{m+n-1}{j} (f(x)g(x))^{m+n-1-j} (h(x)k(x))^{j-n} = g(x)^m u(x) + h(x)^n v(x)$.

Example 7. Let $f(x)$ be a polynomial of degree $2n - 1$ over the field K, and $(x-1)^n|f(x) + 1, (x+1)^n|f(x) - 1$. Find f(x) [16].

Solution: The original proposition is equivalent to finding the solution of the following congruence equations under modulo $(x^2 - 1)^n$ $\begin{cases} f(x) \equiv -1(\mathrm{mod}(x^2-1)^n) \\ f(x) \equiv 1(\mathrm{mod}(x^2+1)^n) \end{cases}$.

Since $(x-1)^n$ and $(x+1)^n$ are mutually prime, according to the theorem of polynomials, the congruence equations have a unique solution in the sense of modulo $(x^2 - 1)^n$.

Since $(x-1)^n$ and $(x+1)^n$ are prime, then there exists a polynomial $u(x), v(x) \in F(x)$ of degree less than n, such that $u(x)(x-1)^n + v(x)(x+1)^n = 1$.

DOI: 10.54254/2753-8818/9/20240711

Notice that $-\frac{1}{2}(x-1)+\frac{1}{2}(x+1)=1$, according to lemma3. Suppose $u(x)=(-1)^n 2^{1-2n}\sum_{j=0}^{n-1}\binom{2n-1}{j}(1-x)^{n-j-1}(x+1)^j$. $v(x)=2^{1-2n}\sum_{j=n}^{2n-1}\binom{2n-1}{j}(1-x)^{2n-1-j}(x+1)^{j-n}$ .Then $u(x)(x-1)^n+v(x)(x+1)^n=1$. Let $f(x)=u(x)(x-1)^n-v(x)(x+1)^n$. Then $(x-1)^n|f(x)+1$, $(x+1)^n|f(x)-1$ and the degree of $f(x)$ is $2n-1$. Hence $f(x)=2^{1-2n}\sum_{j=0}^{n-1}\binom{2n-1}{j}(1-x)^{2n-1-j}(x+1)^j-2^{1-2n}\sum_{j=n}^{2n-1}\binom{2n-1}{j}(1-x)^{2n-1-j}(x+1)^j$, $f(x)$ is the polynomial that meets the requirement.

There are other methods for this problem, such as Taylor expansion and integral solution. But the theorem in polynomial form is more general and can go deep into the essence of the problem. First, the existence and uniqueness of the solution can be clarified by using the Chinese remainder theorem in polynomial form, and specific solutions can be given by using the theorem. Other combinatorial identities can also be obtained by using similar ideas.

As mentioned in the introduction, the theorem in polynomial form can be used to construct polynomials to prove some propositions about matrix. Next, using the theorem in polynomial form to prove the existence of Jordan-Chevalley decomposition. Jordan-Chevalley decomposition is very important in the study of Algebraic group, and has many applications in lie algebra.

Example 8. If A is an n-th order complex matrix, then A can be decomposed into$B+C$, where B and C are suitable for the following conditions: (i) B is a diagonalizable matrix. (ii) C is a nilpotent matrix. (iii)$BC=CB$. (iv) B, C can be represented as a polynomial of A [3].

Proof: Firstly, prove the conclusion on the Jordan standard form J of A. Suppose the different eigenvalues of A are $\lambda_i(i=1,\dots,k)$ and $J=\mathrm{diag}\{J_1,\dots,J_k\}$. Among them is the block corresponding to the root subspace belonging to the eigenvalues, and its order is set to m_i. obviously for each i, $J_i=M_i+N_i$ where $M_i=\lambda_i$ is a diagonal matrix, N_i is nilpotent and $M_iN_i=N_iM_i$.Let $M=\mathrm{diag}\{M_1,\dots,M_k\}$, $N=\mathrm{diag}\{N_1,\dots,N_k\}$.Then $J=M+N$, $MN=NM$, M is a diagonal matrix and N is a nilpotent matrix.

Since $(J_i-\lambda_i)^{m_i}=0$, so it fits polynomial $(\lambda-\lambda_i)^{m_i}$. And $\lambda_i(i=1,\dots,k)$ are different from each other, so the polynomials $(\lambda-\lambda_1)^{m_1}$, …, $(\lambda-\lambda_k)^{m_k}$are mutually prime. By the theorem there has a polynomial $f(\lambda)$ that satisfies the condition:$f(\lambda)=h(\lambda)(\lambda-\lambda_i)^{m_i}+\lambda_i(i=1,\dots,k)$.

Substitute J_i into the equation, it is not hard to obtain $f(J_i)=h_i(J_i)(J_i-\lambda_iI)^{m_i}+\lambda_iI=\lambda_iI=M_i$.

Hence $f(J)=\mathrm{diag}\{f(J_1),\dots,f((J_k)\}=\mathrm{diag}\{M_1,\dots,M_k\}=M$.Since $J-M=J-g(J)$, N is also a polynomial in J.

Now consider the general situation. Suppose $P^{-1}AP=J$, $A=P(M+N)P^{-1}$. Let $B=PMP^{-1}$, $C=PNP^{-1}$. Then B is a diagonalizable matrix, and C is a nilpotent matrix, and$f(A)=f(PJP^{-1})=Pf(J)P^{-1}=PMP^{-1}=B$. It is not hard to prove $BC=CB$, $C=A-f(A)$.

In fact, the Jordan-Chevalley decomposition is also unique, as it is not the focus of this paper and omits the proof of existence.

The following two examples are also the application of the theorem in the form of polynomials to matrices. It is not difficult to see that the theorem plays a vital role in the construction.

Example 9. A, B are 2 block diagonal matrices, and $A=\mathrm{diag}\{A_1,A_2,\dots,A_n\}$, $B=\mathrm{diag}\{B_1,B_2,\dots,B_n\}$, where A_i and B_i are matrices of the same order. Let A_i be suitable for the polynomial $g_i(x)$ $i=(1,2,\dots,n)$and g be mutually prime. Prove that for each i, there exists a polynomial $f_i(x)$ such that $B_i=f_i(A_i)$, then there must exist a polynomial $f(x)$ of degree not exceeding $n-1$ which satisfies $B=f(A)$ [6].

Proof: Since $g_i(x)$ is mutually prime, it can be seen from the theorem that there is a polynomial $h(x)$ that satisfies $h(x)=g_i(x)q_i(x)+f_i(x)$.

Substituting A_i into the above formula, it can be gotten $h(A_i)=f_i(A_i)=B_i$ .Hence $h(A)=\mathrm{diag}\{h(A_1),\dots,h(A_k)\}=\mathrm{diag}\{B_1,\dots,B_k\}=B$ .Let the characteristic polynomial of A be $g(x)$,do division with remainder$h(x)=q(x)g(x)+f(x)$.Substitute $x=A$ into the above formula.By Cayley-Hamilton formula $B=h(A)=f(A)$.

Example 10. The Adjugate matrix of A can be expressed as a polynomial of A [7].

DOI: 10.54254/2753-8818/9/20240711

Proof: $\begin{pmatrix} A_{11} & \cdots & A_{n1} \\ \vdots & \ddots & \vdots \\ A_{1n} & \cdots & A_{nn} \end{pmatrix}$ When $r(A) \leq n-2$, $A^* = O$.When $r(A) = n$, $A^* = |A|A^{-1}$ where A^{-1} is a polynomial of A. Therefore, it is only necessary to prove that the conclusion holds when $r(A) = n-1$. When $r(A) = n-1$, 0 is the eigenvalue of A, at this time there is an invertible matrix P, such that $P^{-1}AP = \text{diag}\{J, B\}$. Where $J = \begin{pmatrix} 0 & 1 \cdots & 0 \\ \vdots & \ddots & 1 \\ 0 & \cdots & 0 \end{pmatrix}$, $1 \leq r \leq n$. B is reversible, and thus the adjoint matrix of is obtained:$(P^{-1}AP)^* = \text{diag}\{J, B\}^* = D = \text{diag}\{(-1)^{1+r}|B|J^{r-1}, O\}$.

According to the theorem, there has a polynomial $f(\lambda)$ that $\begin{cases} f(\lambda) \equiv (-1)^{1+r}|B|\lambda^{r-1}(\text{mod}\lambda^r) \\ f(\lambda) \equiv 0(\text{mod}|\lambda I - B|) \end{cases}$.

Hence $(P^{-1}AP)^* = \text{diag}\{J, B\}^* = D = \text{diag}\{(-1)^{1+r}|B|J^{r-1}, O\} = \text{diag}\{f(J), f(B)\} = f(\text{diag}\{J, B\})$ $= f(P^{-1}AP)$. Hence, $P^*A^*(P^{-1})^* = P^*A^*(P^*)^{-1} = P^{-1}f(A)P$. $A^* = (P^*)^{-1}P^{-1}f(A)PP^* = (PP^*)^{-1}f(A)(PP^*) = f(A)$. The adjugate matrix of A can be expressed as a polynomial of A.

Example 11. Congruence equations are clearer from the view of Chinese remainder theorem in group theory. For instance, considering the congruence equation mentioned before $\begin{cases} x \equiv 2(\text{mod}3) \\ x \equiv 3(\text{mod}5) \\ x \equiv 2(\text{mod}7) \end{cases}$,this problem corresponds to the decomposition $Z/105Z = \overline{70Z} \oplus \overline{21Z} \oplus \overline{15Z} \cong Z/3Z \oplus Z/5Z \oplus Z/7Z$,$\overline{23} = 2 \times \overline{70} + 3 \times \overline{21} + 2 \times \overline{15} \mapsto (\bar{2}, \bar{3}, \bar{2}) = (\overline{23}, \overline{23}, \overline{23})$ [10].

As mentioned in the introduction, the theorem in the form of group theory can be used to classify groups. But this classification is not thorough. So, it will not be described in detail here. For details, please refer to [10].

In the field of public key Cryptography and other fields, it is often necessary to find the square root of an element a in the modular m residue class ring Z_m, where $m = pq$. p, q is a different prime odd number. This can be found by using the Chinese remainder theorem in ring theory.

Example 12. In Z_{91}, find the square root of $\bar{1}$ [9].

Solution: $Z_{91} = Z/(91)$.Since $91 = 7 \times 13$ and 7 and 13 are prime.$(91) = (7)(13) = (7) \cap (13)$.

Hence $Z/(91) \cong Z/(7) \oplus Z/(13)$. Where the isomorphic mapping is$\varphi: a + (91) \mapsto (a + (7), a + (13))$. Hence $(a + (91))^2 = 1 + (91) \Leftrightarrow \big(a + (7).a + (13)\big)^2 = (1 + (7),\ 1 + (13)) \Leftrightarrow \big(a + (7)\big)^2 = 1 + (7)$ and $(a + 13)^2 = 1 + (13)$.

Since $Z/(7), Z/(13)$ are fields, and in the unary polynomial ring F[x] on any field F, the n-degree polynomial f(x) has at most n roots on F, so $x^2 - 1$ has at least 2 roots in $Z/(7)$ and $Z/(13)$. Obviously, $1 + (7), -1 + (7)$ are two different square roots of $1 + (7)$; $1 + (13)$ and $-1 + (13)$ are two different square roots of $1 + (13)$. Hence $(a + 91)^2 = 1 + (91) \Leftrightarrow a + (7) = \mp 1 + (7)$and $a + (13) = \mp 1 + (13) \Leftrightarrow \begin{cases} a \equiv 1(\text{mod}7) \\ a \equiv 1(\text{mod}13) \end{cases}$. Or $\begin{cases} a \equiv 1(\text{mod}7) \\ a \equiv -1(\text{mod}13) \end{cases}$, Or $\begin{cases} a \equiv -1(\text{mod}7) \\ a \equiv 1(\text{mod}13) \end{cases}$, Or $\begin{cases} a \equiv 1(\text{mod}7) \\ a \equiv -1(\text{mod}13) \end{cases}$.

First solve the following two congruence equations:$\begin{cases} x \equiv 1(\text{mod}7) \\ x \equiv 0(\text{mod}13) \end{cases} \Longrightarrow x = e_1 = 78 + 91k, k \in Z$;

$\begin{cases} x \equiv 0(\text{mod}7) \\ x \equiv 1(\text{mod}13) \end{cases} \Longrightarrow x = e_2 = 14 + 91k, k \in Z$.According to the theorem, it can be concluded that the solution of $\begin{cases} a \equiv 1(\text{mod}7) \\ a \equiv 1(\text{mod}13) \end{cases}$ is $a = 1 \times 78 + 1 \times 14 + 91k = 1 + 91l, l \in Z$.

Similarly, it can be concluded that the solutions of the remaining three congruence equations are: $a = 1 \times 78 + (-1) \times 14 + 91k = 64 + 91k, k \in Z$; $a = (-1) \times 78 + 1 \times 14 + 91k = 27 + 91l, l \in Z$; $a = (-1) \times 78 + (-1) \times 14 + 91k = -1 + 91l, l \in Z$ .Hence in Z_{91} , the square roots of $\bar{1}$ are $\bar{1}, \overline{64}, \overline{27}, \overline{-1}$.

DOI: 10.54254/2753-8818/9/20240711

4. Conclusion

From the full text, it can be known that the Chinese remainder theorem has various forms, including number theory, polynomial theory, group theory and ring theory. Its different forms solve many problems in different fields, including proving mathematical propositions, engineering applications, and computer applications. It can be seen from this that the theorem is important in algebra because the content of this paper is in the abstract scope, and the theorem in other forms is not discussed. With the continuous development of the current algebraic system, it is natural to extend the theorem to more algebraic systems.

References

[1] Deng LY 2019 Another proof of the Chinese remainder theorem. Science and Technology Vision, (09), 174.
[2] Wang HJ and Wang MX 2005 Chinese Remainder Theorem and Its Application. Journal of Tonghua Normal University, (06), 12-13.
[3] Yao M S, WU Q S and XIE Q H 2014 Advanced Algebra. Third edition. Shanghai: Fudan University press.
[4] Liu M M and Shang JJ 2009 Chinese Remainder Theorem and Its Application. Wisdom, (24), 212-213.
[5] Qiu WS 2010 Advanced Algebra Study Guide Volume 2. Beijing: Tsinghua University Press.
[6] Xie Q H and Yao M S 2022 Advanced Algebra. Shanghai: Fudan University press.
[7] Liu HG and Zhao J 2022 The Chinese Remainder Theorem in the mathematical core courses. Journal of Hubei University (Natural Science Edition), 44(01), 31-45.
[8] Shun Z W 2022 Modern Algebra. Nanjing: Nanjing University Press.
[9] Qiu W S 2015 Fundamentals of Abstract Algebra. Beijing: Higher Education Press.
[10] Zhang X K 2022 Abstract Algebra. Beijing: Tsinghua University Press.
[11] Liu J W, Wu T and Li D M 2022 Chinese Remainder Theorem for Multivariate Polynomial Rings. Chinese Science: Mathematics, 52(09), 989-996.
[12] Jun Y B, Hong S M and Roh E H 1993 BCI semigroups. Honam Math J, 15, 59-64.
[13] Jun Y B, Xin X L and Roh E H 1998 A class of algebras related BCI algebras and semigroups. Soochow J Math, 24(4), 309-312.
[14] Jun Y B, Roh E H and Xin X L 1998 I ideas generated by a set in IS algebras. Bull Korean Math Soc, 35, 615-624.
[15] Xin X L 2001 Chinese remainder theorem for IS-algebras. Journal of Northwest University (Natural Science Edition), 473-475+478.
[16] Liu H G, Xu X Z and Liao J 2022 Analysis of a polynomial problem. University Mathematics, 38(01), 83-89.