Chinese Remainder Theorem

漢陽大學校 姜信元 李鶴來

1. Chinese Remainder Theorem

The kind of problem that can be solved by simultaneous congruences has a long history, appearing in the Chinese literature as early as the first century A.D. Sun-Tsu asked: Find a number which leaves the remainders 2, 3, 2 when divided by 3, 5, 7, respectively. (such mathematical puzzles are by no means confined to a single cultural sphere; indeed, the same problem occurs in the *Introductio Arithmetica* of the Greek mathematician Nicomachus, circa 100 A.D.) In honor of their early contributions, the rule for obtaining a solution usually goes by the name of the Chinese Remainder Theorem [1].

**Theorem** (Chinese Remainder Theorem). Let \( n_1, n_2, \ldots, n_r \) be positive integers such that \( \gcd(n_i, n_j) = 1 \) for \( i \neq j \). Then the system of linear congruences

\[
\begin{align*}
x & \equiv a_1 \pmod{n_1}, \\
x & \equiv a_2 \pmod{n_2}, \\
& \vdots \\
x & \equiv a_r \pmod{n_r}
\end{align*}
\]

has a simultaneous solution, which is unique modulo \( n_1 n_2 \cdots n_r \).

**Proof.** We start by forming the product \( n = n_1 n_2 \cdots n_r \). For each \( k = 1, 2, \ldots, r \), let \( N_k = n/n_k = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r \); in other words, \( N_k \) is the product of all integers \( n_i \) with the factor \( n_k \) omitted. By hypothesis, the \( n_i \) are relatively prime in pairs, so that \( \gcd(N_k, n_k) = 1 \). According to the theory of a single linear
congruence, it is therefore possible to solve the congruence \( N_kx \equiv 1 \pmod{n_k} \); call the unique solution \( x_k \). Our aim is to prove that the integer

\[
\bar{x} = a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r
\]
is a simultaneous solution of the given system.

First, it is to be observed that \( N_i \equiv 0 \pmod{n_k} \) for \( i \neq k \), since \( n_k|N_i \) in this case. The result is that

\[
\bar{x} = a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r
\equiv a_kN_kx_k \pmod{n_k}
\]
But the integer \( x_k \) was chosen to satisfy the congruence \( N_kx \equiv 1 \pmod{n_k} \), which forces

\[
\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}.
\]
This shows that a solution to the given system of congruences exists.

As for the uniqueness assertion, suppose that \( x' \) is any other integer which satisfies these congruences. Then

\[
\bar{x} \equiv a_k \equiv x' \pmod{n_k}, \ k = 1, 2, \ldots, r
\]
and so \( n_k | \bar{x} - x' \) for each value of \( k \).

Because \( \gcd(n_i, n_j) = 1 \), \( n_i \cdots n_k | \bar{x} - x' \); hence, \( \bar{x} \equiv x' \pmod{n} \). With this, the Chinese Remainder Theorem is proven.

The problem posed by Sun-Tsu corresponds to the system of three congruences

\[
x \equiv 2 \pmod{3},
\]
\[
x \equiv 3 \pmod{5},
\]
\[
x \equiv 2 \pmod{7}.
\]

In the notation of Theorem 4-8, we have \( n = 3 \cdot 5 \cdot 7 = 105 \) and

\[
N_1 = n/3 = 35,
\]
\[
N_2 = n/5 = 21,
\]
\[
N_3 = n/7 = 15.
\]

Now the linear congruences

\[
35x \equiv 1 \pmod{3},
\]
\[
21x \equiv 1 \pmod{5},
\]
\[
15x \equiv 1 \pmod{7}
\]
are satisfied by \( x_1 = 2 \), \( x_2 = 1 \), \( x_3 = 1 \), respectively. Thus, a solution of the system is given by

\[
\bar{x} = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1
= 233
\]
Modulo 105, we get the unique solution \( \bar{x} = 233 \equiv 23 \pmod{105} \).

We can see the more detailed description of the Chinese problem of remainders in [2].

Sun-Tsu, in a Chinese work Suan-ching (arithmetic), about the first centur AD., gave in the form of an obscure verse a
rule called t'ai-yen (great generalisation) to determine a number having the remainder 2, 3, 2, when divided by 3, 5, 7, respectively. He determined the auxiliary numbers 70, 21, 15, multiples of 5·7, 3·7, 3·5 and having the remainder 1 when divided by 3, 5, 7, respectively. The sum \(2 \cdot 70 + 3 \cdot 2 + 2 \cdot 15 = 233\) is one answer. Casting out a multiple of 3·5·7 we obtain the least answer 23. The rule became known in Europe through an article, "Jottings on the science of Chinese arithmetic," by Alexander Wylie, a part of which was translated into German by K. L. Biernatzki. A faulty rendition by the latter caused M. Cantor to criticize the validity of the rule. The rule was defended by L. Matthiessen, who pointed out its identity with the following statement by C. F. Gauss. If \(m = m_1m_2m_3\ldots\), where \(m_1, m_2, m_3, \ldots\) are relatively prime in pairs, and if
\[
a_i \equiv 0 \left( \mod \frac{m}{m_i} \right),
\]
\[
a_i \equiv 1 \left( \mod m_i \right) \quad (i = 1, 23, \ldots)
\]
then \(x = a_1r_1 + a_2r_2 + \ldots\) is a solution of
\[
x \equiv r_1 \left( \mod m_1 \right),
\]
\[
x \equiv r_2 \left( \mod m_2 \right),
\]
\[
\ldots.
\]
This method is very convenient when one has to treat several problems with fixed \(m_1, m_2, m_3, \ldots\), but varying \(r_1, r_2, r_3,\)

Nicomachus (about 100 A. D.) gave the same problem and solution 23.

Brahmagupta (born, 598 A. D.) gave a rule which becomes clearer when applied to an example: find a number having the remainder 29 when divided by 30 and the remainder 3 when divided by 4. Dividing 30 by 4, we get the residue 2. Dividing 4 by 2, we get the residue zero and quotient 2. Dividing the difference 3 - 29 by the residue 2, we get -13. Multiply the quotient 2 by any assumed multiplier 7 and add the product to -13; we get 1. Then \(1 \cdot 30 + 29 = 59\) is the desired number.

This problem forms the second stage of the solution of the "popular" problem: find a number having the remainders 5, 4, 3, 2 when divided by 6, 5, 4, 3, respectively. The answer is stated correctly to be 59.

Hua Loo Keng had writted the following interesting article in his book [3].

Let us now discuss the ancient method of solutions to this type of problem. The solution to this problem was published as a song in 1593, and it goes as follows:

"Three people walking together, 'tis rare that one be seventy,
Five cherry blossom trees, twenty one branches bearing flowers,
Seven disciples reunite for the half-moon,
Take away (multiple of) one hundred and five and you shall know."
We recall that the problem was to solve the simultaneous congruences \( x \equiv 2 \pmod{3} \), \( x \equiv 3 \pmod{5} \), \( x \equiv 2 \pmod{7} \). The meaning of the song here is as follows: Multiply by 70 the remainder of \( x \) when divided by 3, multiply by 21 the remainder of \( x \) when divided by 5, multiply by 15 (the number of days in half a Chinese (synodic) month) the remainder of \( x \) when divided by 7. Add the three results together, and then subtract a suitable multiple of 105 and you shall have the required smallest solution. For our specific example, we have

\[
2 \times 70 + 3 \times 21 + 2 \times 15 = 233
\]

and on subtracting twice 105 we have the required solution 23.

How do we explain this ancient method of solution, and in particular where do 70, 21, 15 come from? The answer is as follows: 70 is a multiple of 5 and 7 which has remainder 1 when divided by 3. 21 is a multiple of 3 and 7 which has remainder 1 when divided by 5. 15 is a multiple of 3 and 5 which has remainder 1 when divided by 7. It follows that \( 70a + 2b + 15c \) must have remainders \( a \), \( b \) and \( c \) when divided by 3, 5 and 7 respectively.

2. 理叡新編을 通한 考察

頑渙 黃嵐録(1729～1791)은 黄河 5年 己酉에 生하여 正祖 15年 辛亥에 作故한 黃學時代의 学者로 頑渙遺稿 26巻 12冊, 頑渙續稿 14巻 7冊, 理叡新編 23巻 18冊 以外에 多方面에 掌つ 論著가 많다. 聖書, 史集, 心性, 理気, 聲音, 書芸, 園書, 醫術 等을 지나치게 공부하여 健康을 害하고 37歳에 疾病과 疾病에 咳嗽하여 興年에 息を 거세워서는 거의 異萌에 가까웠다 한다. 理叡新編은 頑渙 46歳 때에 完成된 것으로 英祖 50년(1774, 甲午) 9月의 일이다. 余3巻 18冊으로 되어 있어 生平의 研究와 所謂 問題點으로 Advertisement하였던 것을 整理하고 資料한 것이로서 頑渙의 学問의 藍本을 探検해차간다. 그러나 具 之內容은 習慣과 國内の 論著을 追及結論한 것이 大部分이어 서 頑渙의 作用으로 解決해서는 아님이라고 한다. 余이로 數學에 関한 것은 余巻 21, 22, 23이 다. 余巻 21, 22는 算術入門, 余巻 23은 算術本源이 卷 題目이 불어있고 西風 散人 黃嵐録編輯이 라 되어있다.

廼叡新編 21巻 24巻에 天算遺錄이라고 있어 다음과 같은 노래(七言絕句詩)부터 시작한다.

三朋共暇七旬体
五色橋前訪音疎
赤壁秋生寥月滿
介山春盡落花傷

(註:三朋三也七旬七十也昔++一也秋生七月也月滿十也寥盡寥月三月也 由冬至至此一百五日也).

三人同行七十稀
五老峰頭++餘
七月十五秋夜
冬至寥食百五餘

이 두首의 詩는 前에 있는 Hua Loo Kang (華羅康)教授의 译에 영어로 번역된 詩와

으로 内容은 다르나 3에는 70, 5에는 21, 7에는 15를 遁跡시키고 結果을 105로 나눈다는 暗示을 모두간다. 따라서 이러한 種類의 詩가 이 以外에도 더 存在한다고 探検된다. 数
學問問題的解法: 詩謠, 可以通過中國人的技巧, 例如 Chinese Remainder Theorem, 以及現代的數學方法, 來解決這個問題。在現代的數學中, 這個問題經常被用作示例, 來教授學生數學的技巧。

物不知總數只三三三數之剩立二五五數之剩三
七七數之剩二問本總數幾何

(註, 本出孫孔子文法名曰西管習俗名秦之時然
兵警覆自之術或至一百五數須於題內云知○亦
曰韓信兵觀見宗容鏡焦算法)

答曰三十三

術曰三十剩一七十(註, 剩七百四百五十)五數
剩一七十一(註, 剩三十六)七數剩一七十五
(註, 剩三十七)三位併之二百五數去之(註, 漢之笛一百五)餘三十三為答數(註, 一百五為總法)

歌山解法中計有 70, 21, 15 是的英文
例中有的 35, 2 = 1 (mod 3), 21 = 1
(mod 5), 15 = 1 (mod 7). 以下 25 張
是的謎語的說明是.

今按管之句本原自有精義於此通曉他可類
(三) 以三為主用七相因得三十五法去之
餘二非餘一故須倍三十得七十三去之始餘一
所以三數剩一七十五(五)以五為主用三七相
因得二十一十五去之餘一所以五數剩一七十一
(七) 以七為主用三五相因得三十八去之
餘一所以七數剩一七十五三去之始餘一
所以五數剩一七十一三去之

答曰九十八人銀一十九貫六百酒十四掇肉三
十二斤十兩十銖

草曰三剩二(註, 剩百四百)五數剩三(註, 剩六十
三) 七無剩(註, 不下) 併之得二百三的二百五餘九
十八工二百兩工數為額(註, 以二百兩者即為五
餘所以除) 七除工數為酒三除工數為肉, 以
所得 合同式式 撲之, x = 2 (mod 3),

x = 3 (mod 3), x = 0 (mod 7), 70, 2
+ 21, 1 = 98 (mod 105)

下面是的而 林德之說明是.

今按三數剩二當云剩一五數剩三當云剩二
答當云七人銀一貫四百酒一掇肉二斤五兩鈴草
當云三剩一七五剩二下二十四併之一百九
二減一百五餘七以五除七為銀七除七為酒三
餘為肉.

別術七數剩一八數剩二九數剩三本總數四百
九十八三位相乘四五為總法(七) 以五十
相因七十二七去之餘二故須四倍七十二得二
百八十二幾去之始餘一所以以七數剩一下二百
八十八八減主七九相因六十三去之餘
七故須許七倍

六十三得四百四十一滿去之始餘一所以八
數剩一下百四十一(九)九為主七八相因五十
六滿去之始餘二故須五倍倍六六十得二百八十八
滿去之始餘一所以九數剩一下二百八十八七
九相乘得五百五四所以五去之百五數四去之.

歌山解法中計有 70, 21, 15 是的英文
例中有的 35, 2 = 1 (mod 3), 21 = 1
(mod 5), 15 = 1 (mod 7). 以下 25 張
是的謎語的說明是.

今按管之句本原自有精義於此通曉他可類
(三) 以三為主用七相因得三十五法去之
餘二非餘一故須倍三十得七十三去之始餘一
所以三數剩一七十五(五)以五為主用三七相
因得二十一十五去之餘一所以五數剩一七十一
(七) 以七為主用三五相因得三十八去之
餘一所以七數剩一七十五三去之始餘一
所以五數剩一七十一三去之

答曰九十八人銀一十九貫六百酒十四掇肉三
十二斤十兩十銖

草曰三剩二(註, 剩百四百)五數剩三(註, 剩六十
三) 七無剩(註, 不下) 併之得二百三的二百五餘九
十八工二百兩工數為額(註, 以二百兩者即為五
餘所以除) 七除工數為酒三除工數為肉, 以
所得 合同式式 撲之, x = 2 (mod 3),

x = 3 (mod 3), x = 0 (mod 7), 70, 2
+ 21, 1 = 98 (mod 105)

下面是的而 林德之說明是.

今按三數剩二當云剩一五數剩三當云剩二
答當云七人銀一貫四百酒一掇肉二斤五兩鈴草
當云三剩一七五剩二下二十四併之一百九
二減一百五餘七以五除七為銀七除七為酒三
餘為肉.

別術七數剩一八數剩二九數剩三本總數四百
九十八三位相乘四五為總法(七) 以五十
相因七十二七去之餘二故須四倍七十二得二
百八十二幾去之始餘一所以以七數剩一下二百
八十八八減主七九相因六十三去之餘
七故須許七倍

六十三得四百四十一滿去之始餘一所以八
數剩一下百四十一(九)九為主七八相因五十
六滿去之始餘二故須五倍倍六六十得二百八十八
滿去之始餘一所以九數剩一下二百八十八七
九相乘得五百五四所以五去之百五數四去之.

歌山解法中計有 70, 21, 15 是的英文
例中有的 35, 2 = 1 (mod 3), 21 = 1
(mod 5), 15 = 1 (mod 7). 以下 25 張
是的謎語的說明是.

今按管之句本原自有精義於此通曉他可類
得一千五百七十三滿二去之始餘一是以十二數剩一下一千五百七十三(十三)十一十二相乘
一百三十二滿七十三去之餘二故七倍相乘數得九
百二十四滿百去之始餘一是以十三數剩一下
九百二十四。

舉其又術而求之問題等通行式而

\[ x \equiv 3 \pmod{11}, \quad x \equiv 2 \pmod{12}, \quad x \equiv 1 \pmod{13}, \quad 156 \cdot 6 \equiv 1 \pmod{11}, \quad 143 \cdot 11 \equiv 1 \pmod{12}, \quad 132 \cdot 7 \equiv 1 \pmod{13}, \quad 156 \cdot 6 \cdot 3 + 143 \cdot 11 \cdot 2 + 132 \cdot 7 \equiv 14 \pmod{1716} \]

又術二數剩一二數剩二七數剩三九數剩四元
總數一百五十七位相乘六百三十之古法(二)
五七七八因三百一十五滿二去之故二數剩
一下三百一十五(五)二七九相因一百二十六滿
五去之餘一故五數剩一下一百二十六(七)二五
九相因九十滿七去之餘六故六倍相因
數得一百四十五去之始餘一是以七數剩一下
五百四十二(九)二五七相因七十滿九去之餘七
故四倍相因數得二百八十滿九去之始餘一是以
九數剩一下二百八十。

舉其又術而求之問題等通行式而

\[ x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{9}, \quad 315 \equiv 1 \pmod{2}, \quad 126 \equiv 1 \pmod{5}, \quad 90 \cdot 6 \equiv 1 \pmod{7}, \quad 70 \cdot 4 \equiv 1 \pmod{9}, \quad 315 + 126 \cdot 2 + 90 \cdot 6 \cdot 3 + 70 \cdot 4 \cdot 4 = 157 \pmod{630} \]

以上內容所述逐一子算經有問題
以外而矣若干問題等以典之例而聞
矣故用問題也故有此例之例亦可
解法在現在的通行式之解法及一致

3. 結論

古代中國的算經十書中有且其中
唐代所存之算經等算經除外有今
前二世紀至五世紀間所存於古算
於中國人之問題及算經解法中

現存孫子算經等算經及
孫子時代的算經及

正多問題有

題及

在

其

古算念

中


ta

T

求

此

版


ta

T

求

此

版


ta

T

求

此

版


ta

T

求

此

版


ta

T

求

此

版


ta

T

求

此

版


ta

T

求

此

版


ta

T

求

此
이 七言律詩로 表現된 問題는 三元一次聯立方程式이다. Greece 사람들의 實用性에 比해 中國人들은 漂泊의이라는 것도 中國人들 이 西洋人들에게 比해 一解 부터 方程式이나 代數學의 分野에 頭角을 나타낸 理由中의 한 가지가 읽는 것 같다.

附記：理數新編의 資料를 甲寅(1974)年에 提供하여주신 前漢陽大學校 文理科大學長 故 心岳 李雲鴻教授의 厚意와 激勵에 感謝하며 又次四次 冥福을 박니다.

참고문헌