Journal of Historia Mathematica Vol. 8. No. 1, (1995), 54 - 60.

Chinese Remainder Theorem

漢陽大學校 姜信元 李鶴來

1. Chinese Remainder Theorem
2. 理藪新編을 通한 考察
3. 結 語

1. Chinese Remainder Theorem

The kind of problem that can be solvd by simultaneous congruences has a long history, appearing in the Chinese literature as early as th first century A. D. Sun-Tsu asked: Find a number which leaves the reminders 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, circe 100 A. D.) In honor of their early contributions, therule for obtaining a solution usually goes by the name of the Chinese Remainder Theorem [1].

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

$$x \equiv a_1 (\bmod\ n_1),$$
$$x \equiv a_2 (\bmod\ n_2),$$
$$\vdots$$
$$x \equiv a_r (\bmod\ n_r)$$

has a simultaneous solution, which is uniqe 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 $k = 1, 2, \cdots, r$, 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 $N_k x \equiv 1 \pmod{n_k}$; 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 theis case. The result is that

$$\begin{aligned}\bar{x} &= a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r \\ &\equiv a_kN_kx_k \pmod{n_k}\end{aligned}$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, 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

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k}, \quad k = 1, 2, \cdots, r$$

and so $n_k | \bar{x} - x'$ for each value of k. Because $\gcd(n_i, n_j) = 1$, $n_1 \cdots n_k | \bar{x} - x'$; 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

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

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

$$\begin{aligned} N_1 &= n/3 = 35, \\ N_2 &= n/5 = 21, \\ N_3 &= n/7 = 15. \end{aligned}$$

Now the linear congruences

$$\begin{aligned} 35x &\equiv 1 \pmod{3}, \\ 21x &\equiv 1 \pmod{5}, \\ 15x &\equiv 1 \pmod{7} \end{aligned}$$

are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectively. Thus, a solution of the system is given by

$$\begin{aligned}\bar{x} &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 233\end{aligned}$$

Modulo 105, we get the unigue 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 centurt A.D., 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 $5 \cdot 7$, $3 \cdot 7$, $3 \cdot 5$ 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 $3 \cdot 5 \cdot 7$ 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 $m = m_1 m_2 m_3 \cdots$, where $m_1, m_2, m_3, \cdots$ are relatively prime in pairs, and if

$$a_i \equiv 0 \pmod{m/m_i},$$

$$a_i \equiv 1 \pmod{m_i} \qquad (i = 1, 23, \cdots)$$

then $x = a_1 r_1 + a_2 r_2 + \cdots$ is a solution of

$$x \equiv r_1 \pmod{m_1},$$

$$x \equiv r_2 \pmod{m_2},$$

$$\cdots.$$

This method is very convenient when one has to treat several problems with fixed $m_1, m_2, m_3, \cdots$, but varying $r_1, r_2, r_3,$ Nicomachus (about 100 A. D.) gave the same problem and solution 23.

Brahmegupta (born, 598 A. D.) gave a rule which becomes clearer when applied to an example: find a number having the reminder 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 simltaneous congruences $x \equiv 2\ (\text{mod}\ 3)$, $x \equiv 3\ (\text{mod}\ 5)$, $x \equiv 2\ (\text{mod}\ 7)$. 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 reminder 1 when divided by 3. 21 is a multiple of 3 and 7 which has remainder 1 whendivided 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. 理藪新編을 通한 考察

頤齋 黃胤錫(1729~1791)은 英祖 5年 己酉에 出生하여 正祖 15年 辛亥에 作故한 實學時代의 學者로 頤齋遺稿 26卷 12冊, 頤齋續稿 14卷 7冊, 理藪新編 23卷 18冊 以外에 多方面에 걸쳐 論著가 많다. 經書, 史集, 心性, 理氣, 聲音, 書藝, 圖書, 醫藥 等을 지나치게 공부하여 健康을 害하고 37歲에 眩氣와 眼疾에 苦生하여 晩年에 가까워서는 거의 失明에 가까웠다한다. 理藪新編은 頤齋 46歲 때에 完成된것으로 英祖 50년(1774, 甲午) 9月의 일이다. 全23卷 18冊으로 되여있어 平生의 硏究와 當時 問題點으로 生覺하였던 것을 整理하고 蒐集한 것이어서 頤齋의 學問의 幅을 짐작케한다. 그러나 그 內容인 즉 中國과 國內의 論著들을 拔萃轉載 한것이 大部分이어서 頤齋의 作으로 誤解해서는 아니된다고 한다. 여기서 數學에 關한 것은 卷21, 22, 23이다. 卷21, 22는 算學入門, 卷23은 算學本源이란 題目이 붙어있고 西溟散人 黃胤錫編輯이라 되여있다.

理藪新編 21卷 24張에 天算頌이라고 있어 다음과 같은 노래(七言絶句詩)부터 시작한다.

三朋共暇七旬休
五鳳樓前訪昔儔
赤壁秋生寒月滿
介山春盡落花稠

(註,三朋三也七旬七十也昔廿一也秋生七月也月滿十也春盡寒食三月也 由冬至至此一百五日也).

三人同行七十稀
五老峯頭廿一餘
七月十五初秋夜
冬至寒食百五除

이 두首의 詩는 앞에있는 Hua Loo Kang(華羅康)敎授의 책에 英文으로 번역된 詩와 서로 內容은 다르나 3에는 70, 5에는 21, 7에는 15를 連關시키고 結果를 105로 나눈다는 暗示는 모두같다. 따라서 이러한 種類의 詩가 이 以外에도 더 存在한다고 짐작된다. 數

學問題의 解法을 詩로 나타낸 中國人들의 奇智에 놀라면서도 Chinese Remainder Theorem이 오래되고 사람들의 입에 오르내린 問題임에는 틀림없는 것같다. 같은 張에 실려있는 問題와 解說이 앞에 英文으로 된 例와 똑같은 것으로 Sun-Tsu(孫子)에 依한 問題로 되어있다.

物不知總數只云三三數之剩二五五數之剩三七七數之剩二問本總數幾何
(註,本出孫子○比法名曰筩管術俗名秦王暗點兵猶覆射之術或遇一百五數須於題內云知○亦曰韓信點兵見統宗精揚輝算法)

答曰三十三

術曰三十剩一下七十(註,剩二下百四十)五數剩一下二十一(註,剩三下六十三)七數剩一下十五(註,剩二下三十)三位併之二百三十三滿一百五數去之(註,減兩箇一百五)餘二十三爲答數(註,一百五爲總法)

여기 解法에 있는 70, 21, 15는 앞의 英文의 例에 있는 $35 \cdot 2 \equiv 1 \pmod 3$, $21 \equiv 1 \pmod 5$, $15 \equiv 1 \pmod 7$이다. 다음 25張에는 頤濟의 說明이 있다.

今按筩管之術本原自有精義於比通曉他可類究(三)以三爲主用五七相因得三十五滿三去之餘二非餘一故須倍三十五得七十滿三去之始餘一所以三數剩一下七十(五)以五爲主用三七相因得二十一滿五去之餘一所以五數剩一下二十一(七)以七爲主用三五相因得一十五滿七去之餘一所以七數剩一下一十五右三五七循次相乘得一百五數故本文滿一百五數去之○以上今俗稱爲天算法三五七皆天數故也. 이 解法의 說明이 合同式의 解法과 一致한다.

바로 다음에는 應用問題가 하나 실려있다.

用工不知其數差人支犒每三人支肉一斤剩零五兩八銖(註,乃三數剩二)每五人支錢一貫剩零四百(註,五數剩三)每七人支酒一摋恰攧成摋(註,七數無剩)問總工所支各幾何

答曰九十八人錢一十九貫六百酒十四摋肉三十二斤一十兩十之銖

草曰三剩二(註,下百四十)五剩三(註,下六十三)七無剩(註,不下)併之得二百三減一百五餘九十八工二百乘工數爲錢(註,以二百乘者即以五除所以代除也)七除工數爲酒三除工數爲肉. 이것을 合同式으로 쓰자. $x = 2 \pmod 3$, $x = 3 \pmod 3$, $x = 0 \pmod 7$, $70 \cdot 2. + 21 \cdot 3 \equiv 98 \pmod{105}$

다음에는 바로 頤濟의 說明이 있다.

今按三數剩二當云剩一五數剩三當云剩二答當云七人錢一貫四百酒一摋肉二斤五兩八銖草當云三剩一下七十五剩二下四十二併之一百十二減一百五餘七以五除七爲錢七除七爲酒三除七爲肉.

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五百四爲總法(七)七爲主八九相因七十二滿七去之餘二故須四倍七十二得二百八十八滿七去之始餘一所以七數剩一下二百八十八(八)八爲主七九相因六十三滿八去之餘七故須七倍

六十三得四百四十一滿八去之始餘一所以八數剩一下四百四十一(九)九爲主七八相因五十六滿九去之餘二故須五倍五十六得二百八十滿九去之始餘一所以九數剩一下二百八十○右七八九相乘得五百空四所以滿五百空四數去之.

여기 別術로 되어있는 問題를 合同式으로 나타내면 $x \equiv 1 \pmod 7$, $x \equiv 2 \pmod 8$, $x \equiv 3 \pmod 9$, $72 \cdot 4 \equiv 1 \pmod 7$, $63 \cdot 7 \equiv 1 \pmod 8$, $56 \cdot 5 \equiv 1 \pmod 9$, $72 \cdot 4 + 63 \cdot 7 \cdot 2 + 56 \cdot 5 \cdot 3 = 498 \pmod{504}$이다.

又術十一數餘三十二數餘二十三數餘一本總數一十四三位相乘一千七百一十六爲總法(十一)十二十三相乘一百五十六滿十一去之餘二故六倍相乘數得九百三十六滿十一去之始餘一是以十一數剩一下九百三十六(十二)十一十三上乘一百四十三滿十二去之餘十一故十一倍相乘數

得一千五百七十三滿十二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十三去之餘二故七倍相乘數得九百二十四滿十三去之始餘一是以十三數剩一下九百二十四.

여기 又術로 되여있는 問題를 合同式으로 나타내면 $x \equiv 3 \pmod{11}$, $x \equiv 2 \pmod{12}$, $x \equiv 1 \pmod{13}$, $156 \cdot 6 \equiv 1 \pmod{11}$, $143 \cdot 11 \equiv 1 \pmod{12}$, $132 \cdot 7 \equiv 1 \pmod{13}$, $156 \cdot 6 \cdot 3 + 143 \cdot 11 \cdot 2 + 132 \cdot 7 \equiv 14 \pmod{1716}$이다.

又術二數餘一五數餘二七數餘三九數餘四元總數一百五十七四位相乘六百三十爲總法(二)五七九相因三百一十五滿二去之餘一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

數得五百四十滿七去之始餘一是以七數剩一下五百四十(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.

여기 又術로 되여있는 問題를 合同式으로 나타내자. $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{9}$, $315 \equiv 1 \pmod{2}$, $126 \equiv 1 \pmod{5}$, $90 \cdot 6 \equiv 1 \pmod{7}$, $70 \cdot 4 \equiv 1 \pmod{9}$, $315 + 126 \cdot 2 + 90 \cdot 6 \cdot 3 + 70 \cdot 4 \cdot 4 \equiv 157 \pmod{630}$.

以上의 內容으로보아 孫子算經에 있는 問題以外에 여러가지 問題들이 널리 알려져 있었고 應用問題도 있다는 것을 알 수 있으며, 解法이 現在의 合同式의 解法과 一致한다.

3. 結　語

古代中國에 算經十書가 있었고 그 中에서 唐代에 만들어진 緝古算經을 除外하면 모두 前二世紀부터 五, 六世紀에 걸처서 만들어졌다고 한다. 그 中의 하나가 孫子算經이고 孫子의 年代는 紀元一世紀로 推定하고 있다. 剩餘에 關한 中國人의 問題가 孫子算經에 실려있어 現存 孫子에 依하여 提起된 問題로 알려져있지만 問題의 註에 있는 바와 같이 이 問題가 箭管術, 覆射之術 또는 秦王暗點兵韓信點兵 等의 이름으로 當時 널리 퍼져서 利用된 것으로 보아 孫子以前의 古代 때 부터 알려져있던 것 같다. 마치 Euclid가 原本을 만들어 現存 Euclid의 이름으로 불리워지는 定理가 Eucid 以前에 만들어진 定理라고 推定하고 있는 것과 같다. [4]에는 이 問題에 對하여 다음과 같은 註가 있다. More rarely known as the Formosa Theorem. Formosa는 現存 自由中國이 있는 Taiwan의 古稱이다. 따라서 Taiwan이나 福建省 附近의 海上貿易商들은 그 들대로 이 문제를 알고 있었던 것 같다. 古代에서 부터 數學의 모든 分野에서 西洋人들이 앞서있다고 보이는 데, 오직 이 問題에 對해서만 中國人의 問題라고 불리워지는 것은 奇異한 感이 든다. 그러나 理數新編을 여기 저기 읽어보면 中國人들이 方程式이나 代數學的 問題에 있어서는 原理와 解法을 完全히 理解하여 日常의 卑近한 生活方法에 까지 活用하고, 나아가서는 이것을 風流로 美化하고 있음에 놀라지 않을 수 없다. 例를 들어

一百饅頭一百僧
大僧三箇更無爭
小僧三人分一個
幾是大僧幾小僧

이 七言絶句로 表現된 問題는 二元一次聯立方程式이다. 또,

婦人洗碗在河邊
試問家中客幾人
答道不知人數目
六十五碗自分明
二人共餐一碗飯
三人共吃一碗羹
四人共肉無餘數
請問布算無差爭

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 浪漫的이라는 것도 中國人들이 西洋人들에 比해 일찍 부터 方程式이나 代數學的 分野에 頭角을 나타낸 理由中의 한 가지가 된는 것 같다.

附記 : 理藪新編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 李崇寧敎授의 厚意와 激勵에 感謝하며 다시한번 冥福을 빕니다.

참고문헌

1. D. M. Burton, Elementary Number Theory, Allyn and Bacon Inc., 1980.
2. L. Dickson, History of the Theory of Numbers, Vol. Ⅰ, Ⅱ, Ⅲ, Carnegie Instituts of Washington, Washington, D. C., 1920 (Reprinted Chelsea Pub. Co., New York, 1952).
3. Hua Loo Keng, Introduction to Number Theory, Springer-Verlag Berlin Heiderberg, 1982.
4. H. M. Stark, An Introduction to Number Theory, MIT Press, 1978.