The History of The Chinese Remainder Theorem

Law Huong Ing

Department of Mathematics
Faculty of Science and Environmental Studies
Universiti Putra Malaysia
43400 UPM Serdang, Selangor
Malaysia

The History of The Chinese Remainder Theorem

Introduction

The oldest remainder problem in the world was first discovered in a third century Chinese mathematical treatise entitled *Sun Zi Suanjing* 孫子算經(The Mathematical Classic of Sun Zi), of which the author was unknown. Nowadays, the remainder problem in *Sun Zi Suanjing* is popularly known as the Chinese Remainder Theorem, for the reason that it first appeared in a Chinese mathematical treatise.

The Chinese Remainder Theorem is found in Chapter 3, Problem 26 of *Sun Zi Suanjing*:

> *Now there are an unknown number of things. If we count by threes, there is a remainder 2; if we count by fives, there is a remainder 3; if we count by sevens, there is a remainder 2. Find the number of things.*

Besides the problem, the author of *Sun Zi Suanjing* also provided the answer and the methods of solution as follows:

> *Answer: 23.*
>
> *Method: If we count by threes and there is a remainder 2, put down 140. If we count by fives and there is a remainder 3, put down 63. If we count by sevens and there is a remainder 2, put down 30. Add them to obtain 233 and subtract 210 to get the answer. If we count by threes and there is a remainder 1, put down 70. If we count*

by fives and there is a remainder 1, put down 21. If we count by sevens and there is a remainder 1, put down 15. When [a number] exceeds 106, the result is obtained by subtracting 105.

Since antiquity there were many extensive researches which had been done on the Chinese Remainder Theorem, and today this theorem has evolved into a systematic theorem that can easily be found in many elementary mathematical texts. The modern Chinese Remainder Theorem can be stated as:

If the positive integers $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, in other words $\gcd(m_i, m_j) = 1 \ \forall \ i, j$ that $i \neq j$, where gcd denotes the greatest common divisor, let $m = m_1 m_2 \ldots m_k$. If $a_i \equiv 0 \left(\mod \frac{m}{m_i} \right)$ and $a_i \equiv 1 \pmod{m_i}$, $i = 1, 2, \ldots, k$, therefore $N = a_1 r_1 + a_2 r_2 + \ldots + a_k r_k$ is a solution for $N = r_i \pmod{m_i}$, $i = 1, 2, \ldots, k$.

Since its first appearance in *Sun Zi Suanjing*, the Chinese Remainder Theorem continued to attract many ancient mathematicians from other civilizations to discuss and give commentary of it in their respective mathematical treatises. The purpose of this paper is to discuss the development of the interesting Chinese Remainder Theorem in the ancient civilizations, since *Sun Zi Suanjing*.

The Development of the Chinese Remainder Theorem

In modern form, the remainder problem and the solution given in the *Sun Zi Suanjing* can be written as:

Remainder Problem:

$x \equiv 2 (\mathrm{mod}\, 3) \equiv 3 (\mathrm{mod}\, 5) \equiv 2 (\mathrm{mod}\, 7)$,

where x is an unknown that satisfies the requirements given in the remainder problem and needs to be determined.

Moduli-moduli involved:

$m_1 = 3,\ m_2 = 5,\ m_3 = 7$

Formula of solution in the *Sun Zi Suanjing:*

$x = 70b_1 + 21b_2 + 15b_3 - 105n$,

where n = the biggest integer that satisfies $105n < 70b_1 + 21b_2 + 15b_3$

$b_1 = 2, b_2 = 3, b_3 = 2$

b_1, b_2 and b_3 are the remainders of x when x is divided by m_1, m_2 and m_3 respectively.

Solution:

$x = 70(2) + 21(3) + 15(2) - 105(2)$

$x = 23$

Only one solution was given in the *Sun Zi Suanjing*. The author of *Sun Zi Suanjing* did not give further explanation on why the numbers 70, 21 and 15 were chosen nor why a multiple of 105 must be subtracted from the sum of products that was added up. The method of solution in *Sun Zi Suanjing* without further elaboration had raised many queries among researchers who wished to master the method completely.

During the 11th century, Muslim mathematician Ibn Tāhir al-Baghdādī discussed the Chinese Remainder Theorem in his treatise *Al-Takmila fī 'Ilm al-Hisāb*. The moduli that Ibn Tāhir gave were the same as

Sun Zi Suanjing, which were $m_1 = 3$, $m_2 = 5$, $m_3 = 7$. However, his problem was $x \equiv a(\text{mod } 3) \equiv b(\text{mod } 5) \equiv c(\text{mod } 7)$, which was not entirely the same as *Sun Zi Suanjing.* It was clear that Ibn Tāhir had advanced further in his discussion of the remainder problem where arbitrary remainders, *a, b,* and *c* were given in his problem.

It is interesting to note that Ibn Tāhir was the first mathematician in antiquity to give an explanation regarding why the numbers 70, 21 and 15 were related to the moduli 3, 5 and 7 respectively. He explained that for each of the moduli, the related number was obtained by the multiplication of other moduli involved in the problem, given that they are pairwise relatively prime. After that, division was performed on the sum of multiplication repeatedly until the final remainder was 1.

To enable us to understand the explanation regarding how a specific number was chosen to be related to its respective moduli, the steps performed by Ibn Tāhir for his given remainder problem $x \equiv a(\text{mod } 5) \equiv b(\text{mod } 7) \equiv c(\text{mod } 3)$ are given below.

1. For the first modulo m_1, the related number was obtained by the multiplication of the other two moduli involved, $m_2 \times m_3 = 5 \times 7 = 35$.
2. Repeated division was performed on the sum of multiplication of m_2 and m_3 until the final remainder was 1.

   a) $35 = 2(\text{mod } 3)$

   The remainder was 2, the division was continued by adding the product $m_2 \times m_3$ to the remainder.

   b) $2(\text{mod } 3) + 35 = 2(\text{mod } 3) + 2(\text{mod } 3) = 1(\text{mod } 3)$

The division was stopped as the final remainder was 1.

3. Next, the number of remainders (b_1) obtained before the multiplication stopped was counted. In this case, $b_1 = 2$.
4. The number that was related to m_1 was $(m_2 \times m_3) \times b_1 = 35 \times 2 = 70$.

The same procedure was performed to the second and third moduli to find the related number.

For m_2, the related number was $(m_1 \times m_3) \times b_2$.

For m_3, the related number was $(m_1 \times m_2) \times b_3$.

The product $m_1 \times m_2 \times m_3$ was chosen so that the smallest solution that satisfied the given problem could be obtained. The detailed explanation given by Ibn Tāhir had solved the questions in *Sun Zi Suanjing* that had not been answered for several centuries. Ibn Tāhir gave a general solution $x = 21a + 15b + 70c - 105n$, where n = the biggest integer that satisfied $105n < 70a + 21b + 15c$.

The popular Chinese Remainder Theorem found its way to Europe in a famous mathematical treatise by Italian mathematician Leonardo Fibonacci in 1202 entitled *Liber Abaci.* Even though the moduli given were the same, the remainder problem in *Liber Abaci* $x \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 4 \pmod 7$, was slightly different than the one in *Sun Zi Suanjing* in the sense that one of the remainders given was different. However, the method of solution given in *Liber Abaci* was entirely the same as *Sun Zi Suanjing.*

Since *Sun Zi Suanjing,* the Chinese Remainder Theorem was not found again in any Chinese mathematical treatises until the 13th century in the book *Xugu Zhaiqi Suanfa* 續古摘奇算法 (Continuation of Ancient

Mathematical Methods for Elucidating the Strange) in *Yang Hui Suanfa* 楊輝算法 (Yang Hui's Methods of Computation). *Yang Hui Suanfa* was a compilation of three books by Chinese mathematician Yang Hui in 1278.

The remainder problem in *Xugu Zhaiqi Suanfa* was exactly the same as the original remainder problem in the *Sun Zi Suanjing* and the same single solution was given for the problem. In *Xugu Zhaiqi Suanfa,* Yang Hui clearly stated that he had taken the remainder problem from *Sun Zi Suanjing*. However, in addition to the original remainder problem in *Sun Zi Suanjing,* Yang Hui had also given another four remainder problems, as follow:

1. $x \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 0 \pmod 7$, Solution: $x = 98$
2. $x \equiv 1 \pmod 7 \equiv 2 \pmod 8 \equiv 3 \pmod 9$, Solution: $x = 498$
3. $x \equiv 3 \pmod{11} \equiv 2 \pmod{12} \equiv 1 \pmod{13}$, Solution: $x = 14$
4. $x \equiv 1 \pmod 2 \equiv 2 \pmod 5 \equiv 3 \pmod 7 \equiv 4 \pmod 9$, Solution: $x = 157$

Fibonacci was the first European to pave the way for the discussion of the Chinese Remainder Theorem in his treatise. Later, in the 14th and 15th century Isaac Argyros and Frater Frederius discussed the remainder problem in their treatises *Eisagog`e Arithm`etik`e* and Munich Manuscript respectively. Both of them gave the problem $x \equiv a \pmod 3 \equiv b \pmod 5 \equiv c \pmod 7$, which was the same as the remainder problem given by the Muslim mathematician Ibn Tāhir in *Al-Takmila fī 'Ilm al-Hisāb* in 11th century.

Since both of them gave a remainder problem with arbitrary remainders, the solution given for the problem was general: $x = 21a + 15b + 70c - 105n$, n = integer. Frater Frederius was the only mathematician after

Ibn Tāhir who offered explanation regarding the specific number that was related to its respective moduli, an unsolved mystery since *Sunzi Suanjing.*

It was not surprising that the discussion of the remainder problem in the treatises of Argyros and Frederius was similar to that of Ibn Tāhir. In general, many European mathematical treatises in antiquity were greatly influenced by the works of the Muslim mathematicians. Fibonacci was the pioneer of the European mathematicians who had done research extensively on Muslim mathematical works such as *Tarā'if al-Hisāb* by Abu Kamil. He later incorporated many of the problems into his great treatise like *Liber Abaci.* From his treatises, the works of the Muslim mathematicians were spread to Europe, including the Chinese Remainder Theorem that was originated from China.

Conclusion

The chronological development of the Chinese Remainder Theorem in the ancient mathematical treatises is summarized as follow:

Mathematicians	Century	Title of Treatise	Civilization
Sun Zi	3	*Sun Zi Suanjing*	China
Ibn Tāhir	11	*Al-Takmila fī 'Ilm al-Hisāb*	Arab
Leonardo Fibonacci	13	*Liber Abaci*	Europe
Yang Hui	13	Buku *Xugu Zhaiqi Suanfa* dalam *Yang Hui Suanfa*	China
Isaac Argyros	14	*Eisagog`e Arithm`etik`e*	Europe
Frater Frederius	15	Munich Manuscript	Europe

In conclusion, the famous Chinese Remainder Theorem managed to raise much interest from the mathematicians in antiquity to give commentary of it in their respective treatises due to the unelaborated explanation given in *Sun Zi Suanjing*. Muslim mathematician Ibn Tāhir should be given credit for cracking the unresolved mystery posed in *Sun Zi Suanjing* since 3th century. Through the Muslim mathematicians, the Chinese Remainder Theorem spread into the works of the European mathematicians.

References

A. S. Saidan. 1978. The Arithmetic of Al-Uqlīdisī. The Story of Hindu-Arabic Arithmetic as told in *Kitāb al-Fusūl fī al-Hisāb al-Hindī* by Abū al-Hasan Ahmad ibn Ibrāhīm al-Uqlīdisī written in Damacus in the year 341 (A. D. 952/3). Holland: D. Reidel Publishing Company.

Lam Lay Yong. 1977. *A Critical Study of the Yang Hui Suan Fa.* Singapore: Singapore University Press.

Lam Lay Yong dan Ang Tian Se. 1992. *Tracing the Conception of Arithmetic and Algebra in Ancient China Fleeting Footsteps.* Singapore: World Scientific Publishing.

Libbrecht, U. 1973. *Chinese Mathematics in the Thirteenth Century. The Shu-shu chiu-chang of Ch'in Chiu-shao.* Massachusetts: The Massachusetts Insittute of Technology.

Yang Hui 楊輝 . 1278 A. D. *Yang Hui Suanfa* 楊輝算法 in Kodama, Akihito 兒玉明人, 1966, *Jūgo seiki no Chōsen kan: dō-katsuji-han sūgaku*, pp. 53-97. Tokyo: Kodama Akihito