한국수학사학회지 제18권 제3호(2005년 8월), 1-24

不定方程式의 歷史

숙명여자대학교 수학과 홍영희
yhhong@sookmyung.ac.kr

중국의 부정방정식은 九章算術에서 시작되어 孫子算經과 張丘建算經에서 취급되었다. 秦九韶가 數書九章에서 大衍總數術을 도입하여 일반적인 연립합동식의 해법을 얻어낼 때까지 부정방정식은 아무런 발전이 없었다. 먼저 秦九韶의 大衍術을 소개하고, 조선에서 부정방정식의 발전 과정을 조사한다. 南秉吉의 算學正義와 秦九韶 數書九章의 大衍術을 비교한다.

주제어 : 부정방정식, 秦九韶, 數書九章, 大衍術, 南秉吉, 算學正義

0. 서론

부정방정식, 즉 미지수의 개수보다 적은 개수의 방정식들로 이루어진 연립 방정식의 역사는 방정식의 역사만큼 오래된 역사를 가지고 있다. 함무라비 시대(1800 - 1600 B.C.)에 이미 부정방정식 $x^2+y^2=z^2$, $u^2+v^2=2w^2$ 등의 해에 대한 기록이 전해지고 있다. 물론 첫 번째 부정방정식은 피타고라스 정리에 의하여 직각삼각형의 세 변을 구하는 문제이고 두 번째 방정식은 사다리꼴의 아래 윗변이 각각 u, v일 때 그 넓이를 이등분하도록 하는 두 변에 평행인 선분의 길이를 w로 하는 문제이다. 두 방정식의 해를 각각 Pythagorean triple, Babylonian triple이라 부르는데, 바빌로니아 사람들은 이미 두 방정식의 관계에서 (x, y, z)이 Pythagorean triple일 때 $u=x-y$, $v=x+y$, $w=z$에 의하여 Babylonian triple (u, v, w)를 구하고 있다([2]). 부정방정식을 Diophantus 방정식이라 부르기도 하는데 이는 2세기에서 3세기에 걸쳐 활동한 것으로 보이는 희랍의 Diophantus의 저서 Arithmetica에서 취급한 2차 이상의 부정방정식의 이론이 획기적인 것으로 현재까지 그 영향을 끼치고 있기 때문이다. Diophantus 이후 Leonardo Pisano(=Fibonacci ca. 1180-1240)가 다시 부정방정식의 문제를 다루기까지 유럽에서는 대수학의 발전이 거의 나타나지 않고 있다([1], [2]).

중국에서 처음 부정방정식이 취급된 것은 九章算術(Jiŭ zhāng suàn shù, [6], [16])의 方程(Fāng chēng)장의 제13문 "五家共井"으로 여섯 개의 미지수와 다섯 개의 1차

방정식으로 이루어진 연립방정식인데, 실제로 方程(Fāng chēng)장에서 취급하고 있는 것으로 보아 그들은 부정방정식으로 이해하기보다는 일반 연립1차방정식과 같이 취급하여 한 개의 해만 구하고 있다([6], [16]). 따라서 실제로 부정방정식이 제대로 취급된 것은 4세기경에 출판된 것으로 추정되는 孫子算經(Sūn zī suàn jing [16], [17]) 의 제 26문 "物不知其數", 즉 연립합동식의 풀이인데 이는 후에 Chinese Remainder Theorem으로 알려지게 된다. 孫子(Sūn Zī)의 연립합동식은 南宋말의 수학자 楊輝(Yáng Huī)의 續古摘奇算法(Xù gǔ zhāi jī suàn fǎ, 1275, [16], [17]) 상권에서 從横圖, 즉 마방진을 다룬 후 翦管術(Jiǎn guǎn shù) 五問으로 다시 나타나는데 첫 번째 문제는 孫子의 문제를 다시 인용하고 같은 종류의 문제를 다섯 개 더 첨가해 놓았지만 그 풀이 방법은 더 발전된 것이 없다.

또 다른 종류의 부정방정식은 5세기경에 출판된 것으로 추정되는 張丘建算經(Zhāng Giū Jiàn suàn jing, [16], [17]) 하권의 마지막 문제 "百鷄問"으로 세 개의 미지수와 두 개의 1차방정식으로 이루어진 연립방정식이다. 위의 孫子의 物不知其數 문제는 연립방정식으로 나타내면 네 개의 미지수와 세 개의 1차방정식으로 이루어진 연립방정식인데 이는 무한히 많은 해를 가지지만 孫子와 楊輝 모두 한 개의 해만 구하고 있는데 반하여 張丘建算經에서는 세 쌍의 자연수 해를 구하고 있다. 이는 중국 산학에서 모든 방정식의 해로 한 개의 양의 해를 구하고 있는데 반하여 매우 특이한 경우로 이런 점에서 百鷄問을 중국에서 최초의 부정방정식으로 보아야 할 것이다. 百鷄問도 楊輝의 續古摘奇算法 하권에 三鷄析直에 다시 나타나는데 첫 번째 문제가 張丘建算經의 百鷄問이고 같은 종류의 문제를 2개 더 첨가해 놓고 이들을 三率分身이라 부르고 있다([16], [17]). 한편 百鷄問은 세 개의 미지수 중에 한 개를 소거하면 가장 간단한 1차 부정방정식 $ax+by=c$ (a, b, c는 정수)로 바뀐다. 이 문제는 인도와 아랍의 여러 학자들에 의하여 취급되었다([2], [4]). 한편 위의 1차 부정방정식 $ax+by=c$는 그 자체로 풀 수도 있지만 $ax \equiv c \mod b$ 또는 $by \equiv c \mod a$와 같이 합동식으로 풀 수도 있다. 따라서 孫子算經과 張丘建算經의 문제는 모두 합동식의 문제로 일원화하여 본 논문에서는 부정방정식의 문제를 합동식의 문제로 정리하기로 한다. 그 이유는 우리의 연구 대상을 중국과 조선의 산학에서 부정방정식의 역사로 제한하기 때문이다.

우리는 지금까지 조선 산학에서 방정식의 역사에 대한 일련의 연구를 진행하였는데 ([19], [20], [21], [22]), 이어서 부정방정식의 역사에 대한 연구는 필연적이다.

본 연구의 목표는 중국과 조선에서 합동식의 역사를 조사하여 부정방정식의 역사를 연구하는 것이다.

孫子算經과 楊輝의 續古摘奇算法에 나와있는 합동식은 매우 제한된 것이다. 즉 각 방정식의 법 (modulus)들이 서로 소인 경우이고, 그 해법도 제대로 기술되어 있지 않

다. 그러나 秦九韶(Qín Jiǔ Shào, 1202? - 1261?)의 저서 數書九章(Shǔ shū jiǔ zhāng, 1247 [4], [7], [16], [17])의 제1권 제2권의 大衍類(Dà yǎn lèi)에 이 문제를 완벽하게 해결하는 방법을 기술하고 있다. 秦九韶의 大衍總數術(Dà yǎn zǒng shǔ shù)은 불행하게도 송, 원시대의 다른 수학자들 뿐 아니라 그 후 명대의 수학자들에게도 전해지지 않고 다만 청대에 와서야 다시 알려지게 된다. 조선 산학도 마찬가지로 그의 해법은 南秉吉(= 南相吉, 1820 - 1869)의 算學正義 (1867, [18])에 와서 조선에 전달되었다. 大衍總數術은 간단히 大衍術(Dà yǎn shù)이라고 한다.

첫째 절에서는 秦九韶의 방법을 가장 일반화된 방법으로 소개하고, 둘째 절에서는 조선 산학에서 부정방정식의 역사를 다루기로 한다.

사료는 가능한 대로 1차 사료를 사용하고 조선 산학은 韓國科學技術史資料大系 數學編 ([18]), 중국 산학은 中國科學技術典籍通彙(Zhōng guó kē xué jì shù diǎn jí tōng huì) 數學卷(Shǔ xué quán, [16])과 中國歷代算學集成(Zhōng guó lì dài suàn xué jí chéng, [17])을 참고하고, 2차 사료로는 [3], [5], [10], [13], [14], [15]를 이용한다.

1. 秦九韶의 大衍總數術

秦九韶의 大衍總數術을 이해하기 위하여 정수론의 理論(이론)을 먼저 소개한다.

두 자연수 a, b에 대하여 다음을 정의하자.

$r_{-1}=a$, $r_0=b$라 하고,

$$r_{k-2}=q_k r_{k-1}+r_k \quad (0<r_k<r_{k-1}) \quad (k=1,\ 2,\ \cdots) \qquad \cdots\cdots \quad [A]$$

즉, 귀납적으로 r_{k-2}를 r_{k-1}로 나누어 몫을 q_k, 나머지를 r_k로 정의한 것이다. r_k가 r_{k-1}의 약수가 되는 가장 작은 자연수 k를 n이라 하자.

따라서 위의 [A]의 마지막 식은

$$r_{n-1}=q_{n+1}r_n+r_{n+1} \text{ 이고 } r_{n+1}=0 \text{ 이다.}$$

이 때 r_n은 a, b의 최대공약수이고 이를 $\gcd(a,\ b)=r_n$으로 나타내기로 한다.

또 [A]에서 $r_k=r_{k-2}-q_k r_{k-1}$ $(k=1,\ 2,\ \cdots,\ n)$ $\cdots\cdots$ [B]

를 얻어 r_k는 r_{k-2}, r_{k-1}의 정수 계수를 가지는 일차결합으로 된다. 따라서, 이를

[A]의 $r_n = r_{n-2} - q_n r_{n-1}$에서 시작하여 [B]를 차례로 적용하면 r_n은 $r_{-1} = a$, $r_0 = b$의 일차결합, 즉 정수 s, t가 존재하여

$$\gcd(a, b) = as + bt$$

가 된다. [A]는 Euclidean Algorithm으로 알려져 있다. x가 y의 약수일 때 이를 $x \mid y$로 나타내고, $m \mid x-y$ 일 때, $x \equiv y \bmod m$으로 나타낸다.

이를 이용하여 다음 사실을 얻는다.

정리 1 A. 자연수 a, b, m에 대하여 $\gcd(a, m)$을 d라 하면 다음이 성립한다.

1) 합동식 $ax \equiv b \bmod m$이 해를 가지기 위한 필요충분조건은 $d \mid b$이다. 이 때 m을 법으로 합동이 아닌 해는 꼭 d개 있으며, 한 해를 t라 하면,

$$t,\ t+\frac{m}{d},\ t+\frac{2m}{d}, \cdots,\ t+\frac{(d-1)m}{d}$$

이 구하는 해들이다.

2) 특히 $d=1$, 즉 a, m이 서로 소이면 합동식 $ax \equiv b \bmod m$은 m을 법으로 유일해를 갖는다.

3) a, m이 서로 소이면, $am \mid b$이기 위한 필요충분조건은 $a \mid b$, $m \mid b$이다.

4) m_1, m_2가 서로 소이고 $m = m_1 m_2$일 때,

합동식 $ax \equiv b \bmod m$과 연립합동식 $\begin{cases} ax \equiv b \bmod m_1 \\ ax \equiv b \bmod m_2 \end{cases}$ 는 동치이다.

B. 두 자연수 m_1, m_2와 $\gcd(m_1, m_2) = d$, 두 정수 a_1, a_2에 대하여 다음이 성립한다.

연립합동식 $\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$ 가 해를 가지기 위한 필요충분조건은 $d \mid a_1 - a_2$, 즉 $a_1 \equiv a_2 \bmod d$이다.

孫子算經에 나와 있는 해법을 현대적으로 풀어쓰면 다음과 같다.

정리 2 모든 짝이 서로 소인 자연수 $m_1, m_2, \cdots, m_n$과 정수 a_1, a_2, $\cdots$, a_n에 대하여 다음이 성립한다. 연립합동식

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \quad\vdots \\ x \equiv a_n \bmod m_n \end{cases} \quad \cdots\cdots \quad \text{[C]}$$

는 해를 가진다.

또, $m = m_1 m_2 \cdots m_n$이라 하면 위의 연립합동식은 m을 법으로 유일해를 가진다.

이 정리의 증명에 포함되어 있는 다음 과정이 孫子算經에 나와 있는 해법이다. 이를 간단히 소개하자.

$$M_k = \frac{m}{m_k} \quad (k=1,\ 2,\ \cdots,\ n)$$

이라 놓으면 M_k, m_k는 서로 소이므로 정리 1에 의하여 합동식 $M_k x \equiv 1 \bmod m_k$는 m_k를 법으로 유일해 s_k를 가진다.

$$x = \sum_{k=1}^{n} a_k s_k M_k$$

라 하자. 만일 $k \neq l$이면 $M_l \equiv 0 \bmod m_k$이므로

$$\begin{aligned} x &\equiv a_k s_k M_k \bmod m_k \\ &\equiv a_k \bmod m_k \quad (k=1,\ 2,\ \cdots,\ n) \end{aligned}$$

이다.

정리 1 A. 3)에 의하여 연립합동식의 해는 m을 법으로 유일하다.

마지막으로 위의 x에 대하여 $x = mq + r\ (0 \leq r < m)$이라 하면 $x \equiv r \bmod m$이므로 r은 음이 아닌 최소해가 된다.

이상이 秦九韶 이전의 孫子算經 문제의 해법이다. 따라서 孫子의 문제는 결국 합동식 $ax \equiv 1 \bmod m$ $(\gcd(a,\ m)=1)$의 풀이로 대치된다. 이 문제는 Euclidean algorithm을 써서 $as + mt = 1$을 만족하는 정수 s, t를 구하면 s가 구하는 해이다.

秦九韶는 孫子의 문제에서 조건 "모든 짝이 서로 소인 자연수 m_1, m_2, $\cdots$, m_n"이 성립하지 않는 경우를 孫子의 문제로 치환하는 방법과 위의 $as + mt = 1$을 만족하는 정수 s, t를 구하는데 Euclidean algorithm을 사용하는 방법보다 훨씬 간단한 방법을 만들어 내었다. 이는 13세기에 만들어낸 중국 수학의 또 하나의 위대한 업적이다. 이 두 가지 algorithm을 일반적인 경우로 소개하고자 한다.

앞으로 m_1, m_2, $\cdots$, m_n은 아무 조건 없는 자연수를 뜻하기로 한다.

秦九韶의 大衍總數術은 연립합동식 [C]를 다음 두 과정을 통하여 해결하는 것을 뜻한다.

그는 m_1, m_2, $\cdots$, m_n을 問數(Wèn shǔ)라 부르고, 이들을 모두 자연수인 경우를 元數(Yuán shǔ), 소수 이하 숫자를 가지는 경우를 收數(Shōu shǔ), 분수 형태의 숫자를 通數(Tōng shǔ), 끝자리 숫자가 10^n 형태를 가지는 경우를 復數(Fù shǔ)로 구별하였다.

먼저 問數를 모든 짝이 서로 소가 되면서 원래 연립합동식과 동치가 되는 합동식을 구하는 방법을 다음과 같이 기술하였다. 원수의 경우는 다음과 같다.

"元數者先以兩兩連環求等約奇弗約偶 – 或約得五而彼有十乃約偶而弗約奇 – 或元數俱偶約畢可存一位見偶 或皆約而猶有類數存姑置之俟與其他約徧而後乃與姑置者求等 約之 或諸數皆不可盡類 則以諸元數命曰復數以復數格入之"

한편 復數의 경우 뒷부분에 다음과 같이 이어진다.

"約奇弗約偶復乘偶 或約偶或約奇復乘奇 或彼此可約而猶有類數存者 又相減以求續等以積等 約彼則必復乘此乃得定數"

이는 만일 모든 問數의 공약수가 존재하면 한 問數만 남기고 나머지를 모두 공약수로 나누고 나서 두 수씩 짝을 만들어 공약수가 존재하면 (連環求等) 하나는 남기고 나머지는 그 공약수로 나누는데 다시 공약수가 존재하지 않도록 남기는 부분과 나누는 부분을 선택한다. 또 일단 위의 과정을 통하여 다시 공약수, 즉 續等(Xù děng) 이 나타나는 경우는 한 쪽을 나누고 나머지는 공약수를 곱해주어야 한다. 남병길의 산학정의에 들어 있는 예를 들어 설명하자.

問數는 $343335=3\times5\times47\times487$, $27759=3\times19\times487$, $56400=2^4\times3\times5^2\times47$ 인데 남병길은 모두 일곱 가지 서로 다른 짝을 구하고 있다. 그 중에서 다음을 예로 든다.

예 1. 차례로 괄호 속의 두수의 약수로 한 수는 나누고 나머지는 그대로 둔 경우

$$\begin{aligned}(343335,27759,56400) &\rightarrow (487,27759,56400) \quad (\gcd(343335,\ 56400)=705)\\ &\rightarrow (487,\ 9253,\ 56400) \quad (\gcd(27759,\ 56400)=3)\\ &\rightarrow (487,\ 19,\ 56400) \quad (\gcd(487,\ 9253)=487)\end{aligned}$$

예 2. 續等이 있어서 한 수는 나누고 나머지는 그 약수를 곱하는 경우

$$\begin{aligned}(343335,27759,56400) &\rightarrow (343335,27759,80) \quad (\gcd(343335,56400)=705)\\ &\rightarrow (235,\ 27759,\ 80) \quad (\gcd(343335,\ 27759)=1461)\\ &\rightarrow (47,\ 27759,\ 400) \quad (\gcd(235,\ 80)=5\text{는 첫 번째 단계에 이미 나타난 약수로 續等임})\end{aligned}$$

예 3. 위의 예 2를 세 수의 최대공약수로 먼저 나누는 경우로, 일곱 가지 예에는 들어 있지 않지만 남병길은 大衍術의 설명 속에 (30, 25, 20)을 예로 이 방법

을 들고 있다.

$$
\begin{aligned}
(343335, 27759, 56400) &\rightarrow (114445, 27759, 18800) \quad (\text{세 수의 최대공약수는 } 3)\\
&\rightarrow (235,\ 27759,\ 18800) \quad (\gcd(114445,\ 27759) = 487)\\
&\rightarrow (235,\ 27759,\ 400) \quad (47\text{은 } 235\text{와 } 18800\text{의 약수})\\
&\rightarrow (47,\ 27759,\ 400) \quad (5\text{는 } 235\text{와 } 400\text{의 약수})
\end{aligned}
$$

위의 세 경우 모두 마지막 결과는 원래 주어진 問數의 약수로 모든 짝이 서로 소인수들이고 이들의 곱은 주어진 問數의 최소공배수이다.

현재 우리가 사용하고 있는 방법으로는 세 수의 소인수분해를 한 후 각 소수의 지수 중 가장 큰 지수만 남기고 나머지는 지워 나가는 방법으로 얻은 수는 모든 짝이 서로 소이며 그 결과의 곱이 세 問數의 최소공배수로 되는 것이다. 즉 위의 예는 모두 이 방법으로 얻을 수 있다. 이 방법은 청의 黃宗憲(Huàng Zōng Xiàn, 1840? - 20세기 初)의 求一術通解(Qiù yī shù tōng jiě, 1874, [16])에 최초로 나타난다. 그는 問數를 泛母(Fàn mǔ)라 하고 소인수 분해한 수들을 차례로 늘어놓고 이를 析母(Xī mǔ)라 하였다.

또 다른 방법은 잘 알려진 최소공배수를 구하는 방법을 통하여 얻는 것이다.

3)	343335	27759	56400
5)	114445	9253	18800
47)	22889	9253	3760
487)	487	9253	80
	1	19	80

에서 최소공배수는 $3 \times 5 \times 47 \times 487 \times 1 \times 19 \times 80$을 얻는데 이들 인수는 5와 80을 제외하고는 모든 짝이 서로 소이다. 따라서 $(5,\ 80) \rightarrow (1,\ 400)$, 또는 $(5,\ 80) \rightarrow (25,\ 16)$으로 치환하면 서로 소이며 그 곱은 같은 수가 된다. 그러나 25를 약수로 가지는 問數는 56400밖에 없으므로 이 분해는 의미가 없다. 따라서, 우리가 구하는 모든 짝이 서로 소이면서 최소공배수는 같으며 원래 주어진 問數의 약수를 구하는 방법으로 위의 인수들에서 5와 80을 1과 400으로 치환한 후 주어진 問數의 약수들을 나누어 곱하면 된다. 예를 들어 다음을 얻는다.

$$(3 \times 47 \times 487,\ 19,\ 400)\ ;\ (3 \times 47,\ 487 \times 19,\ 400)\ ;\ (47 \times 487,\ 19,\ 3 \times 400).$$

秦九韶는 위와 같이 얻어진 수들을 定數(Dìng shǔ), 또는 定(Dìng) 혹은 定母(Dìng mǔ)라 부르고 원래 주어진 연립합동식의 問數, 즉 법을 定母로 치환하여 얻어지는 연립합동식을 푸는 것으로 대치하였다. 이를 위의 예를 통하여 설명하면 다음과 같다.

$$\begin{cases} x \equiv a \bmod 343335 \\ x \equiv b \bmod 27759 \\ x \equiv c \bmod 56400 \end{cases}$$ 이 해를 가지면 정리 1.1 B에 의하여

$a \equiv b \bmod 3\times487 \cdots (i)$; $a \equiv c \bmod 3\times5\times47 \cdots (ii)$; $b \equiv c \bmod 3 \cdots (iii)$

을 얻는다. 구해진 定母를 $(3\times47,\ 19\times487,\ 2^4\times5^2)$이라 하면, 정리 1 A. 4에 의하여 주어진 연립합동식은 다음 연립합동식

$$\begin{cases} x \equiv a \bmod 3\times47 & \cdots(1) \\ x \equiv a \bmod 5 & \cdots(2) \\ x \equiv a \bmod 487 & \cdots(3) \\ x \equiv b \bmod 19\times487 & \cdots(4) \\ x \equiv b \bmod 3 & \cdots(5) \\ x \equiv c \bmod 2^4\times5^2 & \cdots(6) \\ x \equiv c \bmod 3 & \cdots(7) \\ x \equiv c \bmod 47 & \cdots(8) \end{cases}$$ 과 동치이다.

(4)와 (i)에 의하여 (4) $\Rightarrow$ (3), (1)과 (i)에 의하여 (1) $\Rightarrow$ (5), 마찬가지 방법으로 (6) $\Rightarrow$ (2), (1) $\Rightarrow$ (7), (1) $\Rightarrow$ (8) 을 얻는데, 위의 연립방정식의 해는

$$(1)\cap(2)\cap\cdots\cap(8) = (1)\cap(4)\cap(6)$$

즉 연립합동식

$$\begin{cases} x \equiv a \bmod 3\times47 & \cdots(1) \\ x \equiv b \bmod 19\times487 & \cdots(4) \\ x \equiv c \bmod 2^4\times5^2 & \cdots(6) \end{cases}$$

과 동치가 되어 원래 주어진 연립합동식은 定母를 법으로 하는 연립합동식과 동치가 된다. 따라서 연립합동식은 항상 모든 짝이 서로 소인 법을 가지는 연립합동식으로 치환이 가능하여 孫子의 해법을 통하여 해결할 수 있다.

秦九韶가 도입한 $ax \equiv 1 \bmod m$ $(\gcd(a,\ m)=1)$의 해법을 위하여 다음 algorithm을 설명하자.

두 자연수 $a,\ b$에 대하여 위의 [A]에서 도입한

$r_{-1}=a,\ \ r_0=b$

$r_{k-2}=q_kr_{k-1}+r_k \quad (0<r_k<r_{k-1})\ (k=1,\ 2,\ \cdots,\ n)$

$r_{n-1}=q_{n+1}r_n+r_{n+1}$ 이고 $r_{n+1}=0$

(n은 r_k가 r_{k-1}의 약수가 되는 가장 작은 자연수)

이 때, $c_{-1}=1,\ c_0=0,\ c_k=q_kc_{k-1}+c_{k-2} \quad (k=1,\ 2,\ \cdots,\ n)$

$d_{-1}=0,\ d_0=1,\ d_k=q_kd_{k-1}+d_{k-2} \quad (k=1,\ 2,\ \cdots,\ n)$

또 $r_{n-1}=q_{n+1}r_n+r_{n+1}$ 이고 $r_{n+1}=0$ 대신에

$$r_{n-1}=(q_{n+1}-1)r_n+r_n \text{ 으로 놓고}$$

$$c_{n+1}=(q_{n+1}-1)c_n+c_{n-1}, \quad d_{n+1}=(q_{n+1}-1)d_n+d_{n-1}$$

로 정의하자. 앞으로 c_{n+1}, d_{n+1} *이 나타나는 경우는* r_{n+1}*을* r_n, *몫은* $q_{n+1}-1$ *을 뜻하는 것으로 약속한다.* 이 기호를 사용하여 다음 정리를 얻어, a, b의 최대공약수를 a, b에 대한 일차결합으로 나타낼 때, 그 계수를 구할 수 있다.

정리 3 $r_n=(-1)^{n-1}c_na+(-1)^nd_nb=(-1)^nc_{n+1}a+(-1)^{n+1}d_{n+1}b$

증명. 모든 $k=-1, 0, 1, \cdots, n$에 대하여, 다음을 증명하면 된다.

$$r_k=(-1)^{k-1}c_ka+(-1)^kd_kb$$

$k=-1, 0$의 경우는 명백하다.

$k>0$이라 하고 모든 $l<k$에 대하여 성립한다고 가정하자.

$$\begin{aligned} r_k &= r_{k-2}-q_kr_{k-1} \\ &=(-1)^{k-3}c_{k-2}a+(-1)^{k-2}d_{k-2}b-q_k((-1)^{k-2}c_{k-1}a+(-1)^{k-1}d_{k-1}b) \\ &=(-1)^{k-3}(c_{k-2}+c_{k-1}q_k)a+(-1)^{k-2}(d_{k-2}+q_kd_{k-1})b \\ &=(-1)^{k-1}c_ka+(-1)^kd_kb \end{aligned}$$

를 얻어 귀납법에 의하여 증명이 된다. 또 남은 등식도

$r_n=r_{n-1}-(q_{n+1}-1)r_n$에 위와 같은 방법으로 증명하면 된다.

위의 두 번째 등식은 다음에 의하여도 증명이 된다.

정리 4 모든 $k=-1, 0, 1, \cdots, n$에 대하여 다음이 성립한다.

$$r_{k+1}c_k+r_kc_{k+1}=b, \quad r_{k+1}d_k+r_kd_{k+1}=a.$$

귀납법을 사용하면 곧 증명되므로 생략한다. 다만 $k=n$인 경우는 다음과 같이 증명된다.

$c_{n+1}'=q_{n+1}c_n+c_{n-1}$, $d_{n+1}'=q_{n+1}d_n+d_{n-1}$이라 하면 귀납법의 방법으로 $r_nc_{n+1}'=b$, $r_nd_{n+1}'=a$ ($r_{n+1}=0$이기 때문이다)를 얻고,

$$c_{n+1}=(q_{n+1}-1)c_n+c_{n-1}=c_{n+1}'-c_n,$$

$$d_{n+1}=d_{n+1}'-d_n$$

에서, $a = r_n(d_n + d_{n+1})$, $b = r_n(c_n + c_{n+1})$ …… [D]
를 얻는다(이 경우, $r_{n+1} = r_n$임을 유의하자).

한편, $(-1)^n c_{n+1}a + (-1)^{n+1}d_{n+1}b$

$$= (-1)^n (c_{n+1}' - c_n)a + (-1)^{n+1}(d_{n+1}' - d_n)b$$

$$= (-1)^{n-1} c_n a + (-1)^n d_n b + (-1)^n r_n d_{n+1}' c_{n+1}' + (-1)^{n+1} r_n c_{n+1}' d_{n+1}'$$

$$= r_n$$

특히 $r_n = 1$, 즉 a, b가 서로 소인 경우는

$$1 = (-1)^{n-1} c_n a + (-1)^n d_n b$$

$$= (-1)^n c_{n+1} a + (-1)^{n+1} d_{n+1} b \quad \cdots\cdots \quad [E]$$

이고, [D]에서

$a = d_n + d_{n+1}$, $b = c_n + c_{n+1}$ …… [D′]이 된다.

또 이 경우에 $\frac{a}{b}$의 연분수 표현은 $[q_1, q_2, \cdots, q_{n-1}, q_n, q_{n+1}]$인데 이 사실을 이용한 것으로 추정되는 何承天(Hé Chéng Tiān, 370? - 447?)과 祖冲之(Zǔ Chōng Zhī, 430? - 501?)의 결과에 대하여 [4]를 참조한다.

예 4. gcd(6188, 4709)를 6188, 4709의 일차결합으로 표시하자.
위의 과정을 다음 표에 의하여 계산하자.

k	q_k	r_k	c_k	d_k
-1		6188	1	0
0		4709	1	0
1	1	1479	1	1
2	3	272	3	4
3	5	119	16	21
4	2	34	35	46
5	3	17	121	159
6	2	0		

에서 $\gcd(6188, 4709) = 17 = 121 \times 6188 + (-159) \times 4709$
를 얻는다. 또 위의 여섯 번째 단계를 다음과 같이 변형하면

6	1	17	156	205

에서, $17=(-156)\times 6188+205\times 4709$를 얻는다.

다시 秦九韶의 해법으로 돌아가자.

지금부터 짝이 서로 소인 定母를 m_1, m_2, …, m_n으로 나타내자.

孫子의 해법에서와 같이 $m=m_1m_2\cdots m_n$을 구하여 이를 衍母(Yǎn mǔ)라 하고,

$M_k=\frac{m}{m_k}$ $(k=1, 2, \cdots, n)$를 衍數(Yǎn shǔ)라 부르고, 각 k에 대하여 衍數 M_k를 定母 m_k로 나누어 $M_k=m_ks_k+b_k$ $(0<b_k<m_k)$일 때 나머지 b_k를 奇(Jī) 또는 奇數(Jī shǔ)라 부른다.

$M_k \equiv b_k \bmod m_k$이므로 $M_kx \equiv 1 \bmod m_k$와 $b_kx \equiv 1 \bmod m_k$는 동치이고, b_k와 m_k는 여전히 서로 소이다. 따라서 그는 $bx \equiv 1 \bmod a$를 푸는데 위의 [E]와 [D′]을 이용하여

$$x \equiv d_n \bmod a \text{ 혹은 } x \equiv d_{n+1} \bmod a$$

를 구한다. 실제로 사용하는 것은 d_n, d_{n+1}이므로 그는 c_k를 구하지 않고 d_k를 구하는 과정, 즉 $d_0=1$, $d_k=q_kd_{k-1}+d_{k-2}$ $(k=1, 2, \cdots, n)$를 사용하여 d_n을 구하는 것을 大衍求一術(Dà yǎn qiù yī shù)이라 하였다. $d_0=1$을 天元一(Tiān yuàn yī)이라 하고,

$d_1=q_1$, $d_k=q_kd_{k-1}+d_{k-2}$ $(k=2, \cdots, n)$를 계산하고 있다.

그 과정을 인용하면 다음과 같다.

"大衍求一術云置奇右上 定居右下 立天元一於左上 先以右上除右下 所得商數與左上一相生入 左下 然後乃以右行上下以少除多遞互除之 所得商數隨即遞互累乘歸左行上下須使右上末後奇 一而止乃驗左上 所得以爲乘率 或奇數已見單一者便爲乘率"

秦九韶는 양의 해를 구하여야 하므로 위의 [E]에서, n이 짝수이면 d_n이 양의 해이지만, n이 홀수인 경우에는 d_{n+1}이 양의 해로 되는데 이 경우를 구별하지 않고 다만 문제의 풀이에서, [D′]을 $d_{n+1}=a-d_n$으로 구하였다. 이 사실도 언급되어 있는 것은 아니고 답을 보고 추정하였다([4]). 그러나 남병길의 算學正義에는 우리가 위에서 설명한대로 d_{n+1}을 구하고 있다([18]).

위의 인용에서와 같이 $b_kx \equiv 1 \bmod m_k$의 해 t_k를 乘率(Chéng lǜ)이라 하고 M_kt_k를 泛用(Fàn yòng)이라 하고, 泛用에 a_k를 곱한 것을 總數(Zǒng shǔ), 또는

간단히 總(Zǒng)이라 하고, 이들의 합 $\sum_{k=1}^{n} M_k t_k a_k$을 衍母 m으로 나누어 그 나머지가 연립합동식 [C]의 구하는 최소해인 것은 전술한 孫子 해법과 마찬가지다.

이상에서 秦九韶는 완벽하게 연립합동식 [C]를 해결하고 있는데, 그는 Euclidean Algorithm을 알고 있는 것도 아니고 최대공약수가 1인 경우이기는 하지만 두 수의 최대공약수를 그 두 수의 일차결합으로 표현하는 algorithm도 Euclid의 방법보다 훨씬 간편하고, 서로 소가 아닌 법을 가지는 경우에 대한 풀이는 서양에서는 19세기말에야 해결된 것과 ([4]) 비교하면 서양의 해법보다 600년 먼저 이 문제를 완벽하게 해결하고 있다. 서로 소인 경우도 Euler(1707 - 1783)가 해결한 방법보다 500년은 앞서 있다.

그러나 원과 명에서 授時曆(Shòu shì lì)을 사용하면서 上元積年([15])의 계산이 필요 없게 되어 합동식에 대한 필요성이 없게 되고, 또 朱世傑(Zhū Shì Jié), 李冶(Lǐ Yě)의 업적들과 함께 秦九韶의 업적이 완전히 잊혀지고 19세기에 張敦仁(Zhāng Dūn Rén, 1754 - 1834)의 求一算術(Qiú yī suàn shù, 1803, [16]), 駱騰鳳(Luò Téng Fèng, 1770 - 1841)의 藝游錄(Yì yóu lù, 1815, [16]), 宋景昌의 數書九章札記(Shǔ shū jiǔ zhāng zhá jì, 1842, [17]), 時日醇(Shí Rì Chún, 1807 - 1880)의 求一術指(Qiù yī shù zhǐ, 1873), 黃宗憲의 求一術通解 등을 통하여 다시 秦九韶의 업적이 세상에 알려질 때까지 그의 大衍術은 잊혀졌다([11]).

2. 조선시대의 부정방정식

중국의 수학과 마찬가지로 조선의 수학에서도 秦九韶의 數書九章은 朱世傑의 四元玉鑑 (Sì yuán yù jiàn, 1302)과 함께 연구가 전혀 이루어지지 않다가 남병길과 李尙爀 (1810 - ?)에 의하여 연구가 됨으로 그들의 업적을 이해하게 된다. 실제로 數書九章에 대한 연구는 남병길이 1858년에 출판한 測量圖解 ([18])에 數書九章의 測望類 (제7권, 제8권)에서 여덟 문제와 軍旅類 (제15권)에서 한 문제를 인용하고, 각 문제마다 주석을 달고, 또 圖解, 즉 도형을 통하여 문제를 해결하고 있다.

앞에서도 언급한대로 大衍術은 數書九章의 제1권, 제2권에 들어 있고, 또 大衍이라는 단어는 易經(Yì jīng)의 繫辭上傳 제9장에 나오는데 이는 蓍數를 헤아려 卦를 얻는 방법인데 이 때 점대를 세어나가 나머지만 택하여 괘를 정한다(자세한 내용은 [8], [24]를 참조). 즉 합동식을 가지고 점괘를 만들고 있다. 數書九章의 제1문 蓍卦發微가 바로 이 문제를 다루고 있고, 또 제2문 古曆會積과 제3권 天時類의 제3문 治曆演紀는 모두 천문학의 문제를 大衍術을 이용하여 해결하는 문제들이다. 따라서 동양에서 역경이 차지하는 위치와 천문학의 문제를 생각하면 數書九章을 읽을 기회가 있었다면

반드시 이에 대한 연구를 하였을 것으로 보인다. 특히 남병길은 산학자이지만 그는 천문학자로 더 알려져 있는 사람이다. 그러나 이 문제를 測量圖解보다 9년 늦게 그의 저서 算學正義 (1867)의 하권 제일 마지막에 소개한 것은 이해하기가 힘들다. 算學正義는 이상혁과 공저로 보아야 한다([19])

한편 秦九韶의 數書九章은 大衍術과 함께 增乘開放法(Zēng chéng kāi fàng fǎ)을 통하여 다항방정식의 근사해를 구하는 것을 완벽하게 나타내었다. 증승개방법을 통하여 나타나는 다항식을 차례로 천원술을 이용하여, 이를 제5권 田域類의 尖田求積의 正負開三乘方圖에 잘 나타내었다. 이 역시 조선에 전달되지 않고 이에 미치지 못하는 楊輝의 楊輝算法 (Yàng Huī suàn fǎ, 1274, 1275, [16], [17])과 朱世傑의 算學啓蒙 (Suàn xué qǐ mèng, 1299, [16], [17]) 등만 연구가 된 것도 조선에서 방정식의 해법의 발전에 큰 장애가 된 것이다. 이상혁은 그의 저서 翼算 (1868, [12], [18])의 상편에 그가 秦九韶의 數書九章을 연구한 것을 기술하였다.

조선 산학자들이 취급한 부정방정식에 대하여 알아보자. 먼저 秦九韶 이전의 孫子 해법을 취급한 역사를 알아보자.

현존하는 최초의 조선 산서는 慶善徵 (1616 - ?)의 默思集算法 ([18])인데 地卷의 引剩求總門 三問이 부정방정식으로 이는 모두 口訣을 먼저 들고 문제 풀이를 설명하고 있다. 실제로 孫子의 문제는 중국에서 수학 문제라기보다는 신비스러운 놀이로 이해되고 그 이름도 여러 가지가 있다. 예를 들어 송의 周密(Zhōu Mì)은 그의 저서 志雅堂雜鈔(Zhì yǎ tàng zá chāo, 1290)의 陰陽算術절에서 孫子의 해법을 鬼谷算 또는 隔牆算이라 부르고 구결을 만들었다. 楊輝는 위의 翦管術을 秦王暗點兵, 程大位 (Chéng Dà Wèi, 1533 - 1606)는 그의 算法纂要(Suàn fǎ zuān yào, 1592, [17])에서 韓信點兵이라 부르는데 이는 모두 진왕이나 한신이 병사의 수를 3줄, 5줄, 7줄로 세워서 그 나머지만 가지고 알아내었다는 전설에서 붙여진 이름들이다. 구결은 다르지만 算法纂要에서 먼저 구결을 들고 이에 따라 문제를 해결하는 것은 경선징과 마찬가지이다. 默思集算法에서 $ax \equiv 1 \bmod m$의 답을 구하는 방법을 전혀 언급하지 않은 것은 算學正義를 제외한 다른 모든 산서에서와 같다. 단지 구결에 따라 얻어진 수가 孫子의 해법에 적합하다는 설명만 들고 있다. 그의 문제의 법들은 모두 (3, 5, 7), (5, 7, 9), (7, 9, 11)인데 다른 산서와 마찬가지로 모든 짝이 서로 소이다.

洪正夏 (1684 - ?)는 그의 저서 九一集 ([17]), 卷之三의 物不知總門 十三問의 처음 여섯 문제에서 孫子의 해법을 다루고 있다. 그는 秦九韶의 衍母를 滿法이라 부르고, 그 방법에 대한 언급은 없지만 $ax \equiv 1 \bmod m$의 해를 구하는 것을 求一之法이라 하였는데 秦九韶의 大衍求一術과는 상관없게 구한 것으로 보인다. 왜냐하면 제4문에서 구하는 합동식은

$63x \equiv 1 \bmod 5$, 즉 $3x \equiv 1 \bmod 5$인데

이 경우 大衍求一術에 의하면 해가 2인데 그는 해로 7을 택하고 있다. 어떻게 7을 얻었는지는 알 수 없다. 차례대로 곱하여 나갔다면 2를 지나치기가 어려웠기 때문이다. 그의 여섯 개의 문제중 세 개의 방정식으로 이루어진 것이 세 문제로 그 법은 (3, 5, 7), (5, 7, 9), (7, 9, 11)이고 나머지 세 문제는 두 개의 방정식으로 이루어진 것으로 그 법은 (7, 8), (15, 16), (105, 106)인데 보통은 孫子 문제가 세 개의 방정식으로 이루어진 것을 주로 취급하는데 그는 두 개의 방정식으로 이루어진 문제를 취급하고, 또 법들이 모두 $(k, k+1)$형태가 되어 $(k+1)x \equiv 1 \bmod k$, 즉 $x \equiv 1 \bmod k$는 구일지법을 사용할 것도 없이 그 해는 1이고, 나머지 합동식 $kx \equiv 1 \bmod k+1$의 해는 k자신이 되는데, 그는 등식 $k \times k-(k+1)(k-1)=1$을 이용한 것으로 추정된다. 그 나머지는 孫子의 해법과 다른 것이 하나도 없다.

물부지총문 13문중에 위의 여섯 개의 문제를 제외한 나머지는 모두 定方程式으로 이들을 함께 포함시킨 것으로 보아 洪正夏는 不正方程式에 대한 완전한 개념을 이해하지 못한 것으로 보인다. 그러나 秦九韶를 소개한 남병길을 제외하고는 조선 산학서에서 孫子의 해법을 가장 잘 이해하고 있는 학자가 洪正夏이다.

黃胤錫(1729 - 1791)은 그의 저서 理藪新編(1774)의 외편에 들어 있는 算學入門([18])의 天算頌에서 默思集算法과 같이 먼저 구결을 들고 이를 통하여 법이 (3, 5, 7)인 경우의 孫子의 해법을 설명하려고 하고 있는데 그는 이를

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$$ 에 적용하여 해 1을 구하고 있다.

이는 저자가 연립합동식을 제대로 이해하지 못하고 있음을 단적으로 나타내고 있는 것이다. 왜냐하면 당연히 나머지가 모두 1이므로 그해는 바로 1이 되기 때문이다. 그리고 나서 楊輝의 續古摘奇算法 翦管術 五問에 들어 있는 孫子의 문제와 다섯 문제를 차례로 인용하고 제2문의 경우 나머지를 바꾸어 한 문제를 더 만들어 설명하고 있다. 大衍求一術에 해당되는 방법은 물론 찾을 수 없고 다만 $ax \equiv 1 \bmod m$에서 $a \equiv a' \bmod m$ $(0 \leq a' < a)$을 생각하여 $a' \neq 1$이므로 a의 배수를 생각하여야 한다고 하였다. 물론 秦九韶의 奇數를 생각하고 있는 것으로 보이지 않는다. 秦九韶는 합동 관계가 덧셈과 곱셈에 관하여 닫혀 있는 관계로 보고 있는 것으로 보이지만, 그 나머지 산학자들은 이 사실을 간과하고 있다. 그는 衍母를 總法이라 부르고, 秦九韶의 泛用만 구하고 나머지는 제2문과 같이 하는 것으로 생략하고 있다.

위의 鷄管術의 제2문은 裵相說(1759 - 1788?)도 그의 저서 書計瑣錄(1807, [18]) 下卷의 差分의 제3문으로 인용하고 있다. 이 문제의 특이한 점은 나머지를 구해야 하는데 다음에 남병길의 문제와 유사하므로 그 때 자세한 내용을 설명하기로 한다.

洪正夏의 九一集을 재정리한 작자 미상, 출판 연대 미상의 東算抄([18])의 卷之一에도 物不知總門이 들어 있는데 이 중에 다섯 개의 합동식 문제가 들어 있다. 九一集의 문제를 네 개 인용하고 한 문제만 법이 (15, 19)로 홍정하가 다루지 않은 형태이다. 위에서 언급한 최소의 해를 구하지 않은 것도 그대로 인용하고 있다.

남병길은 算學正義의 서문에서 언급하였듯이 그는 많은 산서를 구할 수 있었는데([19]), 그 중에 數書九章과 宋景昌의 數書九章札記도 포함되어 이를 연구하여 算學正義에 그 결과를 下編의 大衍에 기술하고 있다. 우선 그는 大衍術의 동기부터 언급하고 있다.

大衍術卽古曆演紀之法 而九章之所未及 天元之所未馭 故爲算家之逸格也

그리고 나서 大衍術을 설명한다.

其法 以各數先求總等 留一遍約 又連環求等一約一不約 又求續等約彼乘此
然後命爲定母 以之連乘爲衍母 維乘各爲衍數 去其定母餘一者 仍爲用數
餘二以上者以其所餘命爲奇數 用求乘率 各乘衍數爲用數 因其所剩得總併之
滿衍母去之 盖衍母卽各數皆可度盡之數 而衍數則它數度盡 而本數餘一
然後可以爲用 故必求餘一之用數 而定母有等數 則衍母必增幾倍 且無以求餘一之用數
故輾轉求等約之 又約其於無等也

이는 앞에서 언급한 數書九章의 모든 짝이 서로 소인 定母를 구하는 것을 기술한 것보다 명백하고, 또 그는 모든 단락에서 예를 들어 실제로 일어 나는 algorithm을 설명하고 있다.

定母를 구하는 방법을 가장 잘 설명하고 있는 것은 전술한 張敦仁의 求一算術, 黃宗憲의 求一術通解 등인데 이들에 대한 언급이 없고 또 그들과 남병길의 기술한 방법이 전혀 다르다. 또 秦九韶와 달리 모든 問數의 최대공약수를 먼저 처리하고 나서 매 짝을 소거해 나가는 것도 남병길과 이상혁이 秦九韶의 방법을 완전히 이해하고 있다는 증거이다.

일반적으로 문제 풀이 방법을 나타내는 "術"에 대하여 매우 민감한 산서들에 비하여 남병길이 大衍求一術이라는 단어를 언급하지 않은 것은 이례적이고, 다만 乘率을 구하는 방법을 孫子의 문제에 들어 있는 定母가 3, 5, 7인 경우 衍數 35, 21, 15,

奇數는 2, 1, 1를 얻어 첫 번째 경우에 大衍求一術을 적용하였다. 또 定母와 奇數의 짝이 (67, 27)인 경우에 대한 乘率을 계산한 후 다음 문장을 첨가하였다.

蓋所求者即奇數遞加滿定母去之餘一之數 故以遞加次數與餘一相加亦得乘率

즉 그는 乘率이 위의 식 [E]를 만족하는 수를 구하는 것으로 이해하고 있다. 즉 奇數, 定母, 乘率을 각각 a, m, s라 하면 as를 m으로 나누어 나머지가 1, 즉 $as=mt+1$이 되는 것을 뜻한다. "滿定母去之"라는 것은 as를 定母 m으로 뺄 수 있을 만큼 빼라는 뜻이다. 따라서 大衍求一術에서 t에 해당되는 부분을 계산하고 있지 않았지만 남병길은 그 구조를 알고 있는 것을 나타낸다. 따라서 두 번째 문장은 m의 배수를 차례로 더해나가면서 1을 더한 것이 a의 배수가 되는 경우, 즉 $as=mt+1$을 만족하는 s로 乘率을 계산할 수 있음을 나타낸 것으로 보인다. 전통적인 孫子 해법에 나타나는 방법을 설명하고 있는 것으로 보인다. 숫자가 적은 경우는 좋은 방법일 수 있지만 역시 大衍求一術이 완벽한 방법이다. 이 방법의 예로 定母, 奇數가 각각 8, 5인 경우를 들어 놓았는데 저자가 착각을 하고 있다. 이 경우에 大衍求一術을 사용하면 다음과 같다.

如定母爲八 奇數爲五 則以奇數四次遞加與本奇數共爲奇數之五倍二十五
以定母三次遞減餘爲一 故以遞加次數加餘一得五則爲乘率 而定母遞減次數之三
即前法之歸數也

k	q_k	r_k	c_k	d_k
−1		8	1	0
0		5	0	1
1	1	3	1	1
2	1	2	1	2
3	1	1	2	3
4	1	1	3	5

에서 $5\times5=8\times3+1$인데 이 때 몫 3은 c_4인데 남병길은 d_3으로 착각하고 있다. 이는 우연히 일치한 것일 뿐이다. 위의 세 경우 모두 홀수 번째에서 r_k가 1이 되는데, 짝수 번째에서 일어나는 경우는 다음에 인용할 예에 들어 있다. 남병길은 다만 두 개의 예만 취급하는데, 예를 들기 전에 定母를 반드시 모든 짝이 서로 소가 되도록 구해야 하는 이유를 問數가 4, 6인 경우를 들어서 설명하고 있다. 그 두 수의 최소공배수, 즉 衍母가 12인데, 이를 그대로 곱하면 24가 되므로 문제가 생길 수 있고, 또

그것보다 衍數를 각각 6, 4로 택하면 奇數는 2, 4가 되어 합동식

$$2x \equiv 1 \mod 4,\quad 4x \equiv 1 \mod 6$$

이 모두 해가 없음을 2의 배수가 4로 나누어 나머지가 1이 될 수 없고, 마찬가지로 4의 배수가 6으로 나누어 나머지가 1이 될 수 없다는 것으로 설명하고 있다. 일차합동식의 해가 존재하지 않는 경우를 언급한 것은 매우 의미있는 일이다.

첫 번째 예는 위에서 언급한 楊輝의 翦管術 제 2문과 유사한 문제이지만 서로 소가 아닌 법이 들어 있는 것이 다르다. 이를 인용하면 다음과 같다.

今興造功訖犒賞匠手 每二十人酒一石則剩一斗五升 每十六人肉五斤則剩二斤三兩 每十五人醬一斗則醬少八升 問人數幾何 答曰五十七人

20명에 술 1섬, 즉 100되이므로 1인당 5되씩 나누어 준 것이고, 남는 술이 1말 5되, 즉 15되이므로 세 사람의 몫이 남는다. 따라서 일한 사람의 수로 보면 20명씩 세면 17명 이 남는 것과 같다. 한 근은 16냥이므로 고기는 1인당 5냥이 돌아가는데 남은 고기가 35냥이므로 7인분이 남았다. 따라서 16명씩 세면 9명이 남는 것과 같다. 마찬가지로 醬의 조건에서 15명씩 세면 12명이 남게 된다. 따라서 구하는 합동식은 다음과 같다.

$$\begin{cases} x \equiv 17 \mod 20 \\ x \equiv 9 \mod 16 \\ x \equiv 12 \mod 15 \end{cases} \quad \cdots\cdots \quad \text{(i)}$$

(20, 16, 15) → (5, 16, 3)에서 定母 5, 16, 3, 衍母 240, 衍數 48, 15, 80,
또 奇數 3, 15, 2를 구하여 (i)과 동치인 연립합동식

$$\begin{cases} x \equiv 17 \mod 5 \\ x \equiv 9 \mod 16 \\ x \equiv 12 \mod 3 \end{cases} \quad \cdots\cdots$$

(ii)를 풀어야 한다. 이를 위하여

$$\begin{cases} 3x \equiv 1 \mod 5 \\ 15x \equiv 1 \mod 16 \\ 2x \equiv 1 \mod 3 \end{cases} \quad \cdots\cdots$$

(iii)에, 大衍求一術을 적용하는데 처음 두 경우만 인용한다.

立天元一於左 以奇數三除定母五商得一爲歸數 又以定餘二除奇數三商得一 以乘歸數一加於天元一 得二 而奇餘爲一 故以二爲乘率也

즉, 다음 표에서 c_k 열을 제거한 것을 설명하고 있다. 이 경우에 $k=2$에서 $r_k=1$을 얻고, 또 2는 짝수이므로 전술한대로 $d_2=2$가 乘率이 된다.

k	q_k	r_k	c_k	d_k
-1		5	1	0
0		3	0	1
1	1	2	1	1
2	1	1	1	2
3	2	0		

한편 두 번째 합동식에 大衍求一術을 적용한 것을 인용하면 다음과 같다.

立天元一於左 以奇數十五除定母十六商得一爲歸數 又以定餘一除奇數十五商得十四 以乘歸數一加於天元一 得十五 而奇餘爲一 故以十五爲乘率也

즉, 다음 표에서 c_k 열을 제거한 것을 설명하고 있다. 이 경우에 전술한대로 위의 방법대로 하면 $k=1$에서 $r_k=1$을 얻고, 따라서 위의 방법대로 하면 $q_2=14$, $r_2=0$이 되어야 하지만, $k=1$은 홀수이므로 $15=1\times14+1$의 과정을 한번 더 하여 아래 표를 얻은 것이다.

k	q_k	r_k	c_k	d_k
-1		16	1	0
0		15	0	1
1	1	1	1	1
2	14	1	14	15

세 번째 경우도 두 번째 경우와 같지만 이들을 설명하는데, 저자는 그 이유를 들지 않고 있다. 그 乘率은 2이다.

남병길은 秦九韶의 泛用을 用數라 하였는데, 편의상 그대로 泛用을 사용하기로 한다.

따라서 泛用 $48\times 2=96$, $15\times 15=225$, $80\times 2=160$을 얻어, 이들에 각각 17, 9, 12를 곱하여 總數를 구하여 더하면 5577을 얻는다. 衍母는 240이므로, $5577=240\times 23+57$, 즉 $5577 \equiv 57 \mod 240$에서 최소해 57을 얻는다. 이 경우도

"倂三總得五千五百七十七爲實 以衍母二百四十累減之得人數"

에서 "累減"이라는 단어를 사용하는데 나눗셈을 하여 나머지를 계산하는 것을 계속하여 240을 빼 나가는 것으로 기술하고 있는데 이는 九章算術에서 시작된 것인데 이를 버리지 못하고 있다. 또 $48 \equiv 3 \mod 5$는 사용하고 있지만 (ii)에서

$$17 \equiv 2 \mod 5,\ 12 \equiv 0 \mod 3$$

을 사용하면, (ii)는 다음 연립합동식과 동치이다.

$$\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 9 \mod 16 \\ x \equiv 0 \mod 3 \end{cases} \quad \cdots\cdots \quad \text{(ii')}$$

이를 푸는데는 위에서 구한 泛用에 각각 2, 9, 0을 곱하면 되므로, 세 번째 乘率은 구할 필요가 없고, 또 계산도 훨씬 간략하게 된다. 나머지가 0인 경우 풀이가 간단해지는 것은 바로 다음 예에 나타난다. 奇數를 구할 때 사용한 합동식은 定母로 세어나갈 때 定母의 배수는 나머지와 상관없는 것으로 생각한 것이지, 합동 관계가 동치관계이면서 덧셈과 곱셈에 관하여 닫혀 있는 congruence로 본 것은 아닌 것으로 추정된다.

다음 예제는 남병길이 宋景昌의 數書九章札記에서 인용한 것이다. 실제로 秦九韶는 이런 종류의 문제를 大衍類의 두 번째 문제 古曆會積에서 다루는데 이 문제는 해가 존재하지 않는 경우로 저자가 잘못 풀고 있는 것을 宋景昌이 數書九章札記에 지적하고 있다([17]). 천문학의 문제로 인용하면 다음과 같다.

今天正朔爲甲戌日九百四十分日之四百一十 冬至爲丁酉日四分日之三 用四分曆法
歲實三百六十五日四分日之一 朔實二十九日九百四十分日之四百九十九 紀法六十
求之問一會積年月日 及曆過年月日 未至年月日各幾何
答曰 一會積年一千五百二十 積月一萬八千八百 積日五十五萬五千一百八十
曆過年一千一百一十五 月一萬三千七百九十 又二十三日九百四十分日之二百九十五
日四十萬七千二百五十三 九百四十分日之七百五
未至年四百五 月五千零九 又六日九百四十分日之二百四
日十四萬七千九百二十六 九百四十分日之二百三十五

이 문제에서 古曆(Gŭ lì)은 漢대에 사용되었던 오래된 역법인데 이를 四分曆法(Sì fēn lì fă)이라 부르기도 하고 위의 문제에서 설명하였듯이 일 년을 $365\frac{1}{4}$ 일로, 음력으로 한 달을 $29\frac{499}{940}$ 일로 측정한 것이다. 秦九韶의 당시에도 이미 古曆이 정확하지 않으므로 開禧曆法(Kāi xĭ lì fă)을 사용하는데 이 역법에 관한 문제도 그의 數書九章 제3권 天時類의 治曆推閏부터 나타난다. 이 경우는 일 년을 $365\frac{79}{325}$, 음력 한 달은 $29\frac{8967}{16900}$ 일이다. 紀法은 干支, 즉 60일이 한 주기이다.

會積年月日은 위의 세 주기가 다시 함께 돌아오는 햇 수, 달 수, 날 수를 뜻한다. 따라서 최소공배수를 구하는 문제이다. 이 문제는 問數가 분수 형태, 즉 通數인 경우이다. 이 경우 모두 통분하여 $365\frac{1}{4}=\frac{343335}{940}$, $29\frac{499}{940}=\frac{27759}{940}$, $60=\frac{56400}{940}$ 을 얻어 그 분자들을 각각 氣分, 朔分, 紀分이라 하고, 이 세수를 問數로 택하고 定母 487, 19, 56400 을 구하였다.

한가지 언급할 것은 秦求韶와 宋景昌은 모두 통분할 때 분모를 940 으로 하지 않고 $4\times940=3760$으로 하여 계산을 훨씬 복잡하게 만들었다. 남병길은 "歲實分母四可以度盡朔實分母九百四十"이므로 통분한 분모를 940으로 택한다고 하였다. 따라서 問數의 최소공배수, 즉 衍母 $487\times19\times56400=521869200$를 얻어낸다.

따라서 會積年은

$$\frac{\frac{521869200}{940}}{\frac{343335}{940}}=1520$$

이 된다. 마찬가지로 회적월은

$$\frac{521869200}{27759}=18800$$

회적일은 $\frac{521869200}{56400}\times60=555180$을 얻어내었다.

한편 과년과 미지년을 구하기 위하여 동지인 丁酉日四分日之三은 甲子에서부터

$$33\frac{3}{4}=\frac{31725}{940}$$

일이고, 朔인 甲戌日九百四十分日之四百一十부터는

$$33\frac{705}{940}-10\frac{410}{940}=23\frac{295}{940}=\frac{21915}{940}$$

일이다. 따라서 주어진 조건에서 연립합동식

$$\begin{cases} x \equiv 0 \mod 343335 \\ x \equiv 21915 \mod 27759 \\ x \equiv 31725 \mod 56400 \end{cases}$$

에서 위에 얻어 놓은 定母 487, 19, 56400, 衍母 521869200, 衍數 1071600, 27466800, 9253을 얻어, 奇數를 구하면 200, 1, 9253을 얻는다. 그런데 앞의 예에서 설명하였듯이 첫 번째 합동식에 대한 乘率은 구할 필요가 없고 두 번째 합동식에 대한 것은 奇數가 1이므로 泛用은 衍數 27466800과 같고, 마지막 합동식에 대하여 $9253x \equiv 1 \mod 56400$을 풀어 乘率 3517을 얻는다.

따라서 泛用은 $3517 \times 9253 = 32542801$을 얻는다.

總數의 합을 구하면

$27466800 \times 21915 + 32542801 \times 31725 = 1634355283725$ 이고, 또

$$1634355283725 \equiv 382818525 \mod 521869200$$

이므로, 구하는 積日數는 382818525이다. 따라서 과년, 과월은 앞에서와 같이 적일수를 氣分, 朔分으로 나누고, 과일은 紀分으로 나누어 60을 곱하여 구한다. 또 회적년, 회적월, 회적일에서 위에 구한 과년, 과월, 과일을 빼면 미지년, 미지월, 미지일을 얻는다.

위의 합동식 $9253x \equiv 1 \mod 56400$을 孫子의 해법, 즉 9253의 배수를 56400으로 나누어 나머지가 1이 되는 것을 찾으려면 2배부터 시작하여 3517배까지 계산해야 된다는 것을 생각하면 거의 불가능에 가깝다. 이를 大衍求一術을 사용하면 네 번째 단계에서 3517을 얻을 수 있다. 秦九韶의 해법과 孫子의 해법을 극명하게 대비하기 위하여 남병길은 秦九韶와 마찬가지로 이와 같이 큰 숫자가 포함된 합동식의 문제를 예로 택한 것으로 보인다.

算學正義에 나타나는 大衍은 저자 미상의 籌學續解 (1892, [24]) 3권에 다시 나타난다.

籌學續解는 算學正義를 거의 그대로 인용한 책으로 大衍도 위의 예제까지 그대로 인용하고, 다만 두 번째 예제에 대하여 그 풀이 과정을 매우 자세히 정리하였다.

그밖에 [18]에 들어 있지 않은 조선시대의 산서로 부정방정식을 다룬 책으로 남병길의 저서로 보이는 六一抄 ([9], 남병길의 호가 六一齊임)와 저자와 출판 연대 미상의 東國算書 ([23])에 孫子 해법에 대한 口訣이 들어 있는 것을 찾을 수 있었다. 두 책 모두 定母가 3, 5, 7인 경우의 구결이 들어 있고, 六一抄에는 흔히 접할 수 없는 定母가 3, 4, 5인 경우에 六旬除法訣이 다음과 같이 주어져 있다.

三而有立四十仕 四日于粔半九旬 五柳春光六六宮 六甲歸來是本身

즉, 定母 3,4,5에 대한 泛用이 각각 40,45,36이고 衍母는 60임을 나타내고 있다.

3. 결론

해가 존재하면 무한히 많은 해를 가지는 특성을 가진 부정방정식은 張丘建算經의 문제에서만 두 개 이상의 해를 찾아내었고, 이 문제를 합동식으로 취급하지는 않았고, 또 연립합동식의 경우에도 한 개의 해만 찾는 것으로 취급하여 중국과 조선에서는 부정방정식과 정방정식을 거의 구별하지 않고 있다.

孫子의 해법도 口訣을 통하여 그 명맥을 이어 오다가 秦九韶에 의하여 완전히 해결할 수 있게 되었는데, 명대의 趙琦美(Zhào Qí Měi)가 數書九章에 대한 跋을 萬曆(Wàn lì) 45년, 즉 1617년에 쓴 것을 제외하고는 19세기초에 다시 나타날 때까지 불행하게도 그의 위대한 업적은 완전히 잊혀졌다.

조선에서도 중국과 마찬가지로 孫子 문제의 口訣 정도의 것만 다루다가 19세기 중엽에 남병길과 이상혁에 의하여 秦九韶의 數書九章이 연구되면서 그의 大衍術이 조선에 소개되었다. 그러나 20세기에 들어오면서 서양 수학이 들어오게 되어 동양 산학의 결과는 다시 잊혀지고 大衍術은 서양 수학에 의하여 해결되는 것으로 오해가 되고, 실제로 大衍求一術은 서양 방법보다 훨씬 우수한데도 불구하고 현재에도 이를 사용하지 않고 있다. 이와 같은 일은 반드시 교정되어야 한다.

조선의 中人 산학자들이 일찍 數書九章과 같은 훌륭한 저서를 접할 수 있었다고 가정을 하면 산학이 훨씬 발전하였을 것이다. 19세기 중엽 쇄국정책과 함께 나라가 쇠락해지는 시기에 數書九章과 四元玉鑑이 들어와 더 발전을 못하였고, 중국에는 조선보다 일찍 그들을 발견하여 송, 원대의 수학과 서양 수학을 접목시키면서 큰 발전을 이룬 것과 비교가 된다.

참고 문헌

1. I. G. Bashmakova, *Diophantus and Diophantine Equations*, MAA, 1997
2. I. G. Bashmakova and G. S. Smirnova, *The Beginnings and Evolution of Algebra*, MAA, 2000
3. Y. Li and S. Du, *Chinese Mathematics*, A concise history, tr. J. N. Crossely

and A. W.-C. Lun, Clarendon Press, 1987

4. U. Libbrecht, *Chinese Mathematics in the Thirteenth Century*, The Shu-shu chiu-chang of Ch'in Chiu-shao, The MIT Press, 1973
5. J-C. Martzloff, *A History of Chinese Mathematics*, Springer-Verlag, 1997
6. K. Shen, J. N. Crossley and A. W.-C. Lun, *The Nine Chapters on the Mathematical Art*, Oxford Univ. Press, 1999
7. 郭書春, 秦九韶 <<數書九章>> 序注釋, 湖州師范學院學報, 26(2004), 35-44
8. 南東園, 주역해의, 전3권, 나남출판, 2001
9. 南秉吉, 六一抄, 연세대학교 도서관 소장
10. 吳文俊 主編, 中國數學史大系, 第一卷 - 第八卷, 北京師範大學出版社, 1998
11. 王翼勳, 淸代學者對"大衍總數術"的探討, 明淸數學史論文集, 317-333, 1990
12. 李相赫, 翼算, 홍성사 역, 한국수학사학회, preprint
13. 李儼, 中算史論叢 (一), 中華學藝社出版, 商務印書館發行, 1933
14. 李迪, 中國數學通史, 宋元卷, 江蘇敎育出版社, 1999
15. 錢寶琮 主編, 中國數學史, 科學出版社, 1964
16. 中國科學技術典籍通彙 數學卷 全五卷, 河南敎育出版社, 1993
17. 中國歷代算學集大成, 上, 中, 下, 山東人民出版社, 1994
18. 韓國科學技術史資料大系, 數學編, 1卷 - 10卷, 驪江出版社, 1985
19. 홍성사, 홍영희, 朝鮮 算學者 李尙赫의 方程式論, 한국수학사학회지 17(2004), No. 1, 1-14
20. 홍영희, 初期 群論의 歷史, 한국수학사학회지 13 (2000), No. 2, 33-40
21. 홍영희, 다항식의 대수적 표현, 한국수학사학회지 16 (2003), No. 4, 15-32
22. 홍영희, 조선시대의 방정식론, 한국수학사학회지 17(2004), No. 4, 1-16
23. 저자 미상, 東國算書, 연세대학교 도서관 소장
24. 저자 미상, 籌學續解, 1897, 연세대학교 도서관 소장

History of Indeterminate Equations

Department of Mathematics, Sookmyung Women's University **Young Hee Hong**

Although indeterminate equations were dealt in Jiǔ zhāng suàn shù and then in Sūn zī suàn jing and Zhāng Giū Jiàn suàn jing in China, they did not get any substantial development until Qín Jiǔ Shào introduced dà yǎn shù in his great book Shǔ shū jiǔ zhāng which solves general systems of linear congruences. We first investigate his dà yǎn shù and then study the history of indeterminate equations in Chosun Dynasty. Further, we compare Qín's dà yǎn shù with that in San Hak Jung Eui written by Chosun mathematician Nam Byung Gil.

Key words : indeterminate equations, *Qín Jiǔ Shào*(秦九韶), *Shǔ shū jiǔ zhāng*(數書九章), *Dà yǎn shù*(大衍術), *Nam Byung Gil*(南秉吉), *San Hak Jung Eui*(算學正義)

2000 Mathematics Subject Classification - 01A13, 01A25, 11A07, 11D04, 11D09

논문 접수 : 2005년 4월 7일, 심사 완료 : 2005년 5월