KJHM Vol. 16, No. 1, 2003, 17-24

부정방정식에 대하여

건국대학교 수학교육과 **최상기**

Abstract

The Pythagorean equation $x^2+y^2=z^2$ and Pythagorean triple had appeared in the Babylonian clay tablet made between 1900 and 1600 B. C. Another quadratic equation called Pell equation was implicit in an Archimedes' letter to Eratosthenes, so called 'cattle problem'. Though elliptic equations were contained in Diophantos' *Arithmetica*, a substantial progress for the solution of cubic equations was made by Bachet only in 1621 when he found infinitely many rational solutions of the equation $y^2=x^3-2$. The equation $y^2=x^3+c$ is the simplest of all elliptic equations, even of all Diophantine equations degree greater than 2. It is due to Bachet, Dirichlet, Lebesque and Mordell that the equation is better understood.

0. 서론

정수 계수 방정식의 정수해를 구하는 경우에 그 방정식을 부정방정식(Diophantine equation)이라 한다.

서기 250년경 알렉산드리아에서 활약한 디오판토스(Diophantus)는 **산학**(Arithmetica) 13권을 지술하였는데, 그 중에서 6권의 189개 방정식이 현재 전해지고 있다. 디오판토스의 방정식은 정수 계수(자연수 계수 단항식과 그의 덧셈과 뺄셈) 방정식으로, 디오판토스는 자연수나 양의 유리수만을 해로서 찾고 있다. 당시에는 자연수만이 수로서 인식되었고, 양의 유리수는 자연수의 比로 인식하고 있었다. $\sqrt{2}$는 수가 아니라 작도할 수 있는 크기(magnitude), 즉, 한 변의 길이가 1인 직각이등변삼각형의 빗변의 길이로서 인식하고 있었다[5]. 음수가 없었기 때문에 0보다 작은 해는 찾지 않았는데, 디오판토스는 **산학** V권 문제 2에서 방정식 $4x+20=4$의 해가 없다('absurd')라고 하였다[3, p. 225]. 또한, 방정식의 모든 해를 찾은 것이 아니라 하나의 해만을 찾은 경우가 대부분이다.

디오판토스의 산학에는 이차 부정방정식인 피타고라스 방정식(Pythagorean equation) $x^2+y^2=z^2$의 풀이가 주어져 있다. 그러나 그보다 2000년 전에 만들어진 바빌론인들의 점토판에서 피타고라스 방정식의 풀이를 찾을 수 있다.

또 다른 이차 부정방정식인 펠 방정식(Pell equation), $x^2-dy^2=1$은 아르키메데스(Archimedes of Syracuse, 기원전 287-212)가 에라토스테네스(Eratosthenes of Cyrene, 기원전 230년경)에게 쓴 편지에 나타나 있다('Cattle problem of Archimedes'). 펠 방정식의 풀이는 브라운커(W. Brounker, 1620-1684)의 결과이나, 오일러는 펠(J. Pell, 1611-1685)이 결과로 착각하였고 펠 방정식이라 불리게 되었다. 그러나 인도의 수학자들이 그보다도 600년 이상 빨리 그 풀이를 알고 있었다고 전해진다. 최근에 펠의 방정식의 해를 계산하기 위한 여러 알고리즘과 그의 시간에 대한 효율성을 고려하고 있다[6].

삼차 부정방정식 $y^2=x^3+ax^2+bx+c$를 타원방정식이라 부르는데, 디오판토스의 산학에 그 보기가 소개되고 있으나 실질적인 풀이는 17세기가 되어서야 시작되었다. 방정식 $y^2=x^3+c$는 타원방정식 중에서 가장 간단하며, 더구나 모든 삼차 이상의 부정방정식 중에서 가장 간단한 형태이다. 1621년 바쉐(C. Bache, 1581-1638)는 방정식 $y^2=x^3-2$의 유리수해를 무한히 많이 찾아내었다. 이어서 페르마(P. Fermat, 1601-1665)는 이 방정식의 자연수해는 $x=3,\ y=5$뿐이라고 주장한다. 1738년 오일러(L. Euler, 1707-1783)는 페르마의 주장에 대한 풀이를 내놓았는데 그의 풀이에는 오류가 있었다. 오일러의 틀린 풀이는 이후 150년 가까이 맞는 것으로 받아들여졌으며, 여러 수학자들에 의하여 인용되기도 하였다[7].

방정식 $y^2=x^3-2$의 자연수해는 $x=3,\ y=5$뿐이라는 페르마의 주장은 1912년 캠브리지 대학의 모델(L. J. Mordell)이 증명한 결과로 나타나며, 모델은 이 공로로 Smith Prize를 수상하고 후에 Sadleirian 석좌교수가 된다.

1. 이차 이하의 부정방정식과 풀이

일변수 방정식의 경우 거듭제곱근에 의한 풀이가 바빌론 시대 이후로 관심의 대상이었는데[3, pp. 60-69], 이 문제는 아벨(N. H. Abel, 1802-1829)과 갈루아(E. Galois, 1811-1832)에 의하여 매듭지어진다. 즉, 아벨은 1824년 계수가 미지수인 일반방정식(general equation)은 5차 이상인 경우 거듭제곱근에 의하여 풀 수 없다는 것을 보였으며, 갈루아는 주어진 방정식이 거듭제곱근에 의하여 풀 수 있다는 것이 그 방정식의 갈루아군이 가해군이라는 사실과 동치임을 보였다(계수체가 유리수체를 포함하는 경우).

따라서 일변수 방정식의 경우에는 디오판토스와 같이 부정방정식의 입장에서 자연수해나 유리수해 만을 구한다는 것이 의미가 없다. 오히려 뉴턴의 방법(Newton's method)으로 근사해를 구하는 것이 실질적인 유용하며 근을 이해하는 데 도움이 된다.

일차 부정방정식 $ax+by=c$가 정수해를 갖기 위한 필요충분조건은 a와 b의 최대공약수가 c의 약수인 경우이다. 이는 $\{ax+by \mid x, y \in \mathbb{Z}\}$가 a와 b의 최대공약수로 생성되는 단항이데알이기 때문이다. 이때, (x_0, y_0)가 이 방정식의 한 정수해이면, 이 방정식의 모든 정수해 (x, y)는 다음과 같다.

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 + \frac{a}{d}t, \quad t \in \mathbb{Z}, \quad d = (a, b)$$

디오판토스는 일차 부정방정식의 경우에도 특정한 자연수해를 찾는데 그치고 있다. 위와 같은 일차 부정방정식의 일반적인 풀이는 인도의 수학자인 브라마굽타(Brahmagupta ; 625 경)가 최초로 발견했다 [3, p231].

이차 부정방정식인 피타고라스 방정식 $x^2+y^2=z^2$은 무한히 많은 자연수해 (x, y, z)를 가지며, 이때 (x, y, z)를 피타고라스의 세 수(Pythagorean triple)라 부른다. 피타고라스 방정식은 동차 방정식(homogeneous)이므로, x, y, z가 서로 소인 경우만 찾으면 되고 자연수해와 유리수해를 구별할 필요가 없다. 피타고라스 방정식은 다음과 같이 푼다.

$$\left(\frac{z}{x}\right)^2 - \left(\frac{y}{x}\right)^2 = 1\text{이므로,} \quad \left(\frac{z}{x}+\frac{y}{x}\right)\left(\frac{z}{x}-\frac{y}{x}\right) = 1\text{이다.}$$

두 자연수 $m > n \geq 1$ 대하여 $\frac{z}{x}+\frac{y}{x} = \frac{m}{n}$, $\frac{z}{x}-\frac{y}{x} = \frac{n}{m}$라 하면, 다음이 성립한다.

$$\frac{z}{x} = \frac{1}{2}\left(\frac{m}{n}+\frac{n}{m}\right) = \frac{m^2+n^2}{2mn}, \quad \frac{y}{x} = \frac{1}{2}\left(\frac{m}{n}-\frac{n}{m}\right) = \frac{m^2-n^2}{2mn}$$

이제, x, y, z가 서로 소인 경우만 생각하면 되고, 다음을 얻는다.

$$x = 2mn, \quad y = m^2-n^2, \quad z = m^2+n^2$$

위와 같은 피타고라스 방정식의 풀이와 다양한 피타고라스 세수는 기원전 1900년에서 1600년 사이에 고대 바빌론인들이 제작한 점토판에 나타나 있다[3, pp. 70-77, Plimpton 322 of G. A. Plimpton Collection at Columbia University]. 이는 피타고라스보다 1000년 이상 앞서고 있다. 디오판토스는 이 풀이를 이용하여 변의 길이가 자연수인 여러 직각삼각형을 찾아내었다.

또 다른 이차 부정방정식인 $x^2-dy^2=1$은 펠 방정식(Pell equation)이라 불리는데, 자연수 d가 제곱수가 아닌 경우에만 고려하면 된다. 주어진 펠 방정식의 최소 자연수해를 (x_1, y_1) 라 할 때, 모든 자연수해 (x_n, y_n)는 다음과 같다[1, 정리 5.6.5].

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \geq 1$$

x_1과 y_1이 가장 작은 자연수인 경우 (x_1, y_1)을 기본해(fundamental solution)라고 한다.

펠 방정식의 풀이는 브라운커가 페르마의 물음에 대하여 푼 결과이나, 오일러는 펠이 결과로 착각하였고 펠 방정식이라 불리게 되었다. 인도의 수학자들이 브로운커보다도 600년 이상 전에 그 풀이를 알고 있었으며, 브라운커의 풀이는 인도의 수학자들의 오일러의 **대수학**(Algebra)에서 찾을 수 있다([4], [6], [8]).

고대 그리스 수학자들이 위와 같은 펠 방정식의 풀이를 알고 있었다는 증거를 찾을 수 없으나, 아르키메데스가 에라토스테네스에게 쓴 편지에 있는 '소의 문제'(Cattle problem of Archimedes)에서 다음과 같이 펠 방정식이 유도된다.

흰색, 검은색, 얼룩무늬, 갈색의 황소의 수를 각각 W, X, Y, Z이라 하고 같은 색의 암소의 수를 각각 w, x, y, z이라 하면, 편지의 내용 중 황소의 수는 다음의 일차 방정식을 만족시킨다.

$$W = \frac{5}{6}X + Z, \quad X = \frac{9}{20}Y + Z, \quad Y = \frac{13}{42}W + Z$$

편지의 내용에서 암소의 수는 다음 식을 만족시킨다.

$$w = \frac{7}{12}X + x, \quad x = \frac{9}{20}Y + y, \quad y = \frac{11}{30}W + w, \quad z = \frac{13}{42}(W + w)$$

$W + X$는 제곱수이고, $Y + Z$는 삼각수이다.

위의 식으로부터 x와 y 사이의 관계식을 유도하면, 다음의 펠 방정식이 유도된다[3, p. 229].

$$x^2 - 4,729,494y^2 = 1$$

펠 방정식은 대수적 정수환 $\mathbb{Z}[\sqrt{d}]$에서 다음과 같이 인수분해된다.

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}) = 1$$

그리고 펠 방정식의 풀이는 $\mathbb{Z}[\sqrt{d}]$에서 단원(units)을 찾는 정리(Dirichlet's unit theorem)의 일부분으로 볼 수 있다. 즉, $a + b\sqrt{d}$가 $\mathbb{Z}[\sqrt{d}]$에서 단원이라는 것은 $N(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$과 동치이다. 이때, $\mathbb{Z}[\sqrt{d}]$의 단원군은 $\overline{\mathbb{Z}_2} \oplus \mathbb{Z}$이다. 여기서 $\overline{\mathbb{Z}_2} \cong \{\pm 1, \cdot\}$, $\mathbb{Z} \cong \langle (x_1, y_1) \rangle$이다.

렌스트라는 주어진 알고리즘이 펠 방정식의 근을 계산하는데 시간이 얼마나 걸리는가 하는 효율성(efficiency)을 고려하고 있으며, 확률적 알고리즘(probabilistic algorithm)과 양자 알고리즘(quantumn algorithm)이 소개되고 있다[6].

2. 삼차 부정방정식과 풀이의 시작

1621년 바쉐는 방정식 $y^2=x^3-2$의 자연수해 $x=3, y=5$로부터 새로운 유리수해를 발견하였는데 그 풀이는 다음과 같다.

주어진 방정식에 $x=3-kY$, $y=5-Y$를 대입하면, 다음과 같다.

$$25-10Y+Y^2=27-27kY+9k^2Y^2-k^3Y^3-2$$

$k=\frac{10}{27}$로 택하면, $Y^2\{k^3Y-(9k^2-1)\}=0$이다. 따라서 $Y=\frac{9k^2-1}{k^3}=\frac{4617}{1000}$이므로 다음을 얻는다.

$$x=3-\frac{10}{27}\cdot\frac{4617}{1000}=\frac{129}{100},\quad y=5-\frac{4617}{1000}=\frac{383}{1000}$$

같은 방법으로 방정식에 $x=\frac{129}{100}-kY$, $y=\frac{383}{1000}-Y$를 대입하면 새로운 유리수해가 나타나며, 따라서 이 방정식의 유리수해는 무수히 많다.

정리 1. (바쉐, 1621년) 방정식 $y^2=x^3-2$은 무수히 많은 유리수해를 가진다.

위와 같은 바쉐의 풀이에 대하여 페르마는 방정식 $y^2=x^3-2$의 자연수해는 $x=3$, $y=5$뿐이라고 주장했는데, 그의 주장은 다음과 같은 **26의 문제**로 불리기도 한다.

문제 2. (**26의 문제**, 페르마) 자연수의 제곱수 하나 건너 자연수의 삼제곱수가 있는 경우는 26을 사이에 두고 있는 $25=5^2$과 $27=3^3$뿐이다.

페르마는 1657년 딕비(Digby)와 프렌니클(B. Frenicle, 1601-1675)에 쓴 편지에서 이 문제의 풀이 방법을 제시하고 있다. 그러나 실제로 페르마는 그의 주장을 정당화할 아무런 증명을 시도하지 않았으며, 그가 자신의 주장이 수학적인 정리가 되지 않도록 교묘하고 사려있게 서술하고 있음이 볼(Ball)이나 히스(T. Heath)와 같은 수학자에 의하여 지적되고 있다.

바쉐 이후 100년 넘게 삼차 부정방정식에 대하여 아무런 결과가 없었다. 1738년 오일러는

방정식, $y^2=x^3+1$의 x가 양수인 유리수해는 $x=2$, $y=3$뿐임을 증명하였다. 이로써 **26의 문제**와 같이 자연수에서 제곱수와 삼제곱수에 대하여 다음의 결과를 얻을 수 있다.

정리 3. (오일러, 1738년) 자연수에서 삼제곱수와 제곱수가 이어져 있는 경우는 $8=2^3$과 $9=3^2$뿐이다.

페르마는 방정식 $x^4+y^4=z^2$의 자연수해가 없다는 것을 보였는데, 이것이 페르마가 그가 주장한 여러 가설에 대하여 증명을 한 유일한 것이라고 전해진다. 무한내림(infinite descent)이라고 불리는 이 증명 방법은 (x, y, z)가 이 방정식의 자연수해인 경우, 다음을 만족하는 새로운 자연수해 (x_1, y_1, z_1)을 발견한다.

$$x=x_1^4-y_1^4,\quad y=2x_1y_1z_1,\quad z=x_1^8+6x_1^4y_1^4+y_1^8$$

이때, $z>(x_1^4+y_1^4)^2=z_1^4$이므로 $\sqrt[4]{z}>z_1$이다. 이와 같이 계속하면, $z_1=1$, $x_1y_1=0$이어서 $y=0$인데, 이는 y가 자연수라는 사실에 모순이다.

곧이어 오일러는 **26의 문제**의 문제를 유일인수분해를 이용하여 풀었는데, 아래와 같다. 방정식 $y^2+2=x^3$에서 다음을 얻는다.

$$(y-\sqrt{-2})(y+\sqrt{-2})=x^3$$

그리고 $y-\sqrt{-2}$과 $y+\sqrt{-2}$가 서로 소이므로 유일인수분해에 의하여 다음이 성립한다.

$$y-\sqrt{-2}=(a-b\sqrt{-2})^3,\quad y+\sqrt{-2}=(a+b\sqrt{-2})^3$$

위의 식을 풀면, $a=\pm1$, $b=1$, $x=3$, $y=\pm5$를 얻는다.

그러나 1837년이 되어서야 가우스에 의하여 $\mathbb{Z}[\sqrt{-1}]$ 의 유일인수분해성이 밝혀졌으며, 1848년 완첼(Wantzel)에 의하여 $\mathbb{Z}[\sqrt{-2}]$의 유일인수분해성이 밝혀지게 된다. 더구나 $y-\sqrt{-2}$와 $y+\sqrt{-2}$는 일반적으로 서로 소가 아니다. $2-\sqrt{-2}$과 $2+\sqrt{-2}$는 $\sqrt{-2}$를 최대공약수로 갖는다. 이와 같은 오일러의 풀이의 잘못은 이 후 150년 가까이 맞는 것으로 받아졌으며, 여러 논문에 인용되기도 하였다.

1869년 르베그(V. A. Lesbeque)는 새로운 아이디어와 방법으로 삼차 부정방정식의 풀이를 시도하였으며, 방정식 $y^2=x^3+7$의 자연수해가 없다는 것을 다음과 같이 보였다.

y^2은 $4n+1$ 또는 $4n+2$ 꼴이므로, x는 짝수가 아니다. 그러므로 x는 $4n+1$ 또는 $4n+3$ 꼴이다. x가 $4n+3$ 꼴이라고 하면 x^3+7는 $4n+2$ 꼴이며, y^2은 $4n+2$ 꼴이 될

수 없으므로 이는 모순이다.

이제, x가 $4n+1$ 꼴이라고 하자. 이때, 다음이 성립한다.

$$y^2+1=x^3+8=(x+2)(x^2-2x+4)$$

그러므로 $x+2$는 $4n+3$ 꼴이다. 그러나 가우스 정수환 $Z[i]$에서 $y^2+1=(y+i)(y-i)$로 인수분해되고 $4n+3$ 꼴의 자연수 소수는 $Z[i]$에서도 소원이므로, y^2+1은 $4n+3$ 꼴의 약수를 가지지 못한다. 따라서 방정식 $y^2=x^3+7$의 자연수 해가 없다.

정리 4. (르베그, 1869년) 방정식 $y^2=x^3+7$의 자연수해는 없다

가우스나 완첼 등에 의하여 대수적 정수환의 유일인수분해성이 밝혀지고, 또한 유일인수분해 정역이 아닌 대수적 정수환에 대한 계산이 고려됨에 따라서 방정식 $y^2=x^3-2$에 대한 오일러의 풀이의 잘못이 인식이 되기 시작하였다. 방정식 $y^2=x^3-2$의 자연수해가 $x=3$, $y=5$뿐이라는 것은 1912년 모델에 의하여 밝혀졌다.

정리 5. (모델 1912년) 방정식 $y^2=x^3-2$의 자연수해는 $x=3$, $y=5$뿐이다.

3. 결론

부정방정식은 수와 식에 대한 연구로서 디오판토스의 산학에서 본격적으로 시작되었다. 그러나 그에 대한 생각과 풀이는 기원전 1900년경에 만들어진 바빌론의 점토판에 이미 나타나 있다. 그러나 차수가 삼차 이상인 경우 부정방정식에 대한 실질적인 연구는 1621년 바쉐에 의하여 시작되었으며, 오일러와 모델 등을 거치는 동안 각각 100년이 넘는 공백이 있었다. 모델은 1922년 '3차 곡선 위의 유리수 격자점에 관한 기본 정리'를 밝혔는데, 1980년대 폴팅(G. Faltings)에 의한 모델 가설 및 테이트 가설의 해결, 1994년 와일즈(A. Wiles)에 의한 타니야마 가설의 해결과 함께 타원방정식과 같은 부정방정식의 풀이와 이해에 획기적인 도구를 제공하고 있다. 이와 같은 부정방정식의 연구는 '정수론'이라고 불리는 수학의 정통적인 분야이다.

페르마가 '26의 문제'를 주장하며 아무런 증명을 제시하지 않은 것이나, 그 문제에 대한 오일러의 잘못된 증명이 150년 가까이 맞는 것으로 받아들여진 것에 대한 반성이 필요하다. 페르마는 왜 아무런 근거 없이 그와 같은 주장을 하였는가? 수학자들의 증명은 완벽한가 또는 완벽해야만 하는가?

모델에 의하여 해결된 '26의 문제'나 정리 3에 나타난 오일러의 결과에서 부정방정식 $y^2 = x^3 - k$가 제곱수와 삼제곱수의 놀이를 나타내는 것을 인식할 수 있다. 수의 놀이는 인도의 전설적인 수학자 라마누잔(S. Ramanujan, 1887-1920)에게서 엿볼 수 있는데, 영국의 수학자 리틀우드(J. Littlewood, 1885-1977)는 "라마누잔에게 자연수 하나 하나가 친한 친구 같았다"며 다음과 같이 증언하고 있다. 아픈 라마누잔을 하디(G. Hardy, 1877-1947)가 問病 갔는데, 그 때 하디가 탄 택시의 번호가 1729였다. 그를 본 라마누잔은 '아니(No)'라고 놀라며, 1729는 두 가지 다른 방법의 두 제곱수의 합으로 나타날 수 있는 수 중 가장 작은 수라고 하였다. 즉, $1729 = 1^3 + 12^3 = 9^3 + 10^3$ 이다[3, pp. 640-641].

초등학교 수학 2-나의 110쪽에는 50원짜리와 100원짜리 동전으로 500원을 만드는 놀이를 하고 있다. 이는 일차 부정방정식 $50x + 100y = 500$으로 나타낼 수 있다. 아르키메데스가 에라토스테네스에게 쓴 편지에 있는 '소의 문제' 역시 아르키메데스의 말대로 알렉산드라아인들 자신이 해결해야 할 문제이자 놀이인 것이다.

인류사회학자 호이징하(J. Huizinga)는 인간을 '생각하는 인간'으로 호모 사피엔스 사피엔스(Homo Sapiens Sapiens)보다는 '놀이하는 인간'으로 '호모 루덴스(Homo Ludens, Man the Player)'라고 불렀다[2]. 부정방정식은 우리들의 일상의 놀이에서 찾을 수 있으며, 또한 數의 놀이에서도 나타난다. 호이징하가 말하는 놀이의 요소를 부정방정식과 數에서 찾을 수 있다.

참고 문헌

1. 김응태 · 박승안, **정수론** 제3판, 경문사, 1992.
2. 호이징하/김윤수 옮김, **호모 루덴스**, 까치, 1993.
3. Burton, D. M., *Burton's History of Mathematics* 3rd ed. WCB, 1995.
4. Euler, L., *Elements of Algebra*, English translation, Springer, 1984.
5. Hartshorne, R., "Teaching Geometry according to Euclid", *Notices of AMS* Vol, 47, No. 4(2000), 460-465.
6. Lenstra Jr. H. W., "Solving the Pell Equation", *Notices of AMS* Vol. 49, No. 2(2002), 182-192.
7. Mordell, L. J., *A Chapter in the Theory of Numbers*, Cambridge University Press, 1947.
8. Weil, A., *Number Theory, an Approach through History*, Birkhauser, 1984.