Historia Mathematica Vol. 12, No. 2, 1999, 1-13

페르마의 마지막 정리

광운대학교 수학과 **허 민**

Abstract

Fermat's Last Theorem was proved. In this paper, we survey the historical development of Fermat's Last Theorem and look over the Wolfskehl Prize, Beal's problem, and the *abc* conjecture.

0. 머리말

'페르마의 마지막 정리'가 (공식적으로) 증명되었다. 즉 "2보다 큰 지수 n에 대해 방정식 $x^n+y^n=z^n$은 자연수 해를 갖지 않는다." 17세기 전반기(1637년경)에 등장한 뒤, 수많은 전문 수학자와 아마추어 수학자의 집요한 공격에 저항했으며 '수학에서 가장 유명한 미해결 문제'라는 명예를 얻었던 이 명제는 3세기와 반세기가 더 지난 뒤에야 드디어 완전한 '정리'가 되었다. 그러나 마지막 순간까지도 저항은 계속됐었다. 미국 프린스턴 대학교의 와일스(Andrew Wiles)는 1993년 6월 23일 영국 뉴턴 연구소에서 행한 강연중 이 정리의 증명을 제시했다. 그런데 몇 가지 결함이 발견되었다. 한 가지를 제외한 나머지는 모두 와일스에 의해 즉각 해결되었지만, 마지막 하나의 결함은 쉽게 해결되지 않았다. 와일스도 과거의 수많은 수학자가 거쳤던 길을 또다시 지나가야 하는 불길한 운명에 처한 것으로 보였다. 조바심나고 안타까운 시간을 보낸 와일스는 옛 제자인 케임브리지 대학교의 테일러(Richard Taylor)와의 공동 연구로 1994년 10월 이 결함을 보완했고[16], 페르마의 마지막 정리에 대한 증명을 1995년 5월 논문 [17]을 통해 발표했다.

본 글에서는 먼저 페르마의 마지막 정리의 탄생과 풀이 과정을 역사적으로 더듬어보겠다. 이런 역사는 수학의 결과를 얻는 어려운 과정을 보여준다. 그리고 페르마의 정리가 증명된 뒤 이와 관련된 글에서 찾은 와일스가 받은 볼프스켈 상금, 5만 달러의 상금이 걸린 빌의 문제, 더욱더 중요한 *abc* 추측 등에 대해 간략하게 알아보겠다. 이를 통해 페르마의 마지막 정리의 위치를 알아보고 수학의 발전 방향을 짐작해보고자 한다.

1. 페르마의 마지막 정리의 유래

페르마의 마지막 정리는 의외의 사람으로부터 의외의 상황에서 출현했다. 이를 처음 발견은 페르마(Pierre de Fermat, 1601?-1665)[1]는 전문 수학자가 아닌 법률가였다. 그는 30세 때 툴루즈 지방 의회에서 왕의 고문관 자리를 얻었고, 성실하게 자신의 임무를 수행하면서 여가 시간 대부분을 수학 연구에 이용했다. 그는 생애에 출판한 것이 거의 없었지만, 당대의 많은 지도적인 수학자와 서신 왕래를 빈번히 가졌으며, 이런 방법으로 당대 사람들에게 상당한 영향을 주었다. 페르마는 현대 수론의 창시자로 일반적으로 알려져 있지만(수론에 관한 페르마의 연구 결과 몇 가지는 다음 쪽 상자에 있음), 데카르트와 독립적으로 해석 기하학을 발견했고 극대·극소와 접선을 구하는 방법의 발견으로 뉴턴과 라이프니츠에 의해 결실을 맺은 미분법을 예견했으며 판돈의 분배 문제를 파스칼과 논의하는 가운데 현대적인 확률론을 창시했다. 사실, 페르마가 제시한 수론 결과는 당대의 사람들이 이해할 수 없을 정도로 매우 앞서 있었기 때문에 당시 그는 해석 기하학, 미분법, 확률론의 연구로 더 유명했으며, 17세기의 가장 위대한 프랑스 수학자로 불렸다. 분명히, 그는 아마추어 수학자로 '아마추어의 왕자'라는 별명을 얻었지만, 쿨리지(J.L. Coolidge)의 책 **수학의 위대한 아마추어들**(Great Amateurs in Mathematics)에서 언급되지 않았다. 쿨리지가 말한 대로[14, p. 88], "그는 진정으로 대단히 위대하기 때문에, 전문가로 분류되어야 한다."

페르마가 처음으로 수학을 공부하기 시작할 때 읽은 책 중에는 고대 그리스의 디오판토스가 쓴 책 **산학**(Arithmetica)이 있었다.[2] 디오판토스가 이 책에서 제시한 문제는 통상 단 한 개의 해를 요구했지만, 페르마는 가능성 있는 모든 해를 결정하는 방법을 종종 찾아냈고 일반적인 정리를 찾아내기도 했다. 이런 과정에서 '페르마의 마지막 정리'가 탄생했다. **산학** 제 II권 문제 8은 '주어진 제곱수를 두 개의 제곱수로 나누기'이다. 이 문제를 현대의 기호를 이용해서 다시 쓰면 '임의의 수 z에 대해 관계 $z^2=x^2+y^2$를 만족시키는 두 수 x와 y를 찾기'와 같다.[3] 디오판토스는 여기에서 특별한 경우로 제곱한 합이 16이 되는 분수 두 개를 찾았

1) 페르마의 출생 연도는 불명확하다. 그가 프랑스 툴루즈(Toulouse) 근처의 작은 마을 보몽 드 로마뉴(Beaumont de Lomagne)에서 1601년 8월 17일 태어났다고 주장하는 어느 정도 신빙성 있는 증거가 있다. 그는 1665년 1월 12일 카트레(Castres) 또는 툴루즈에서 죽었는데, 그의 무덤은 원래 툴루즈의 아우구스티누스 교회에 있었다가 나중에 지방 박물관으로 이장되었다. 그의 무덤에는 위의 사망 날짜와 함께 페르마의 사망시 나이가 57세였다고 적혀 있다. 이런 모순된 기록 때문에, 페르마의 생존 기간은 통상 (1601?-1665)와 같이 기록되고 있다. 실제로, 많은 이유 때문에 여러 저자가 기록한 페르마의 출생 연도는 1590에서 1608까지 다양하다[10].

2) 바셰(C. Bachet)는 1621년 그리스어 원문과 함께 라틴어 번역문과 주석을 첨부한 **산학**을 출판했다.

3) 유클리드는 **원론**에서 다음과 같은 공식으로 이 문제의 서로 소인 모든 해를 제시했다.

$$x=2st, \quad y=s^2-t^2, \quad z=s^2+t^2$$

여기에서 s와 t는 다음 조건을 만족시키는 임의의 자연수이며, 이 방정식의 서로 소인 모든 해는 s와 t의 적당한 값에 대해 이와 같은 꼴이다.

(i) $s > t$, (ii) s와 t는 서로 소, (iii) s와 t 중 하나는 홀수이고 다른 하나는 짝수

는데, 그의 해는 $(12/5)^2+(16/5)^2=4^2=16$이었다[4, p. 3]. 그런데 페르마는 이 문제의 옆에 다음과 같은 기록을 남겼다.

> 반면에, 세제곱수를 두 개의 세제곱수의 합으로 또는 네제곱수를 두 개의 네제곱수의 합으로 또는 일반적으로 차수가 2보다 큰 임의의 거듭제곱수를 그와 같은 차수의 두 개의 거듭제곱수로 표현하는 것은 불가능하다. 나는 이 명제에 대한 정말로 놀라운 증명을 발견했지만, 이 여백이 너무 좁아서 증명을 적을 수 없다.

이 문장도 현대적인 표기법으로 나타내면 다음과 같다. 방정식 $x^n+y^n=z^n$은 2보다 큰 임의의 지수 n에 대해 (자연수) 해를 갖지 않는다.[4]

수론에 관한 페르마의 연구

페르마가 얻은 수론의 결과 몇 가지를 나열하면 다음과 같다[14]

(1) **페르마의 작은 정리.** p가 소수이면, p보다 작은 모든 자연수 a에 대해 $a^{p-1}-1$은 p로 나누어 떨어진다.

(2) **두 제곱 정리.** $4n+1$꼴의 모든 소수는 두 제곱수의 합으로 표현되지만, $4n-1$꼴의 모든 소수는 두 제곱수의 합으로 표현될 수 없다.

(3) $4n+1$ 꼴의 소수는 단 하나의 직각 삼각형의 빗변이 될 수 있고, 이런 소수의 제곱은 두 개의 직각 삼각형의 빗변이 될 수 있으며, 이런 소수의 세제곱은 세 개의 직각 삼각형의 빗변이 될 수 있다. 이와 같이 계속된다.
예를 들면, 5의 경우에 다음과 같다.
$5^2=3^2+4^2$, $25^2=15^2+20^2=7^2+24^2$, $125^2=75^2+100^2=35^2+120^2=44^2+117^2$, ...

(4) 모든 수는 삼각수이거나 둘 또는 세 개의 삼각수의 합이다. 또, 모든 수는 제곱수(정사각수)이거나 둘, 셋, 또는 네 개의 제곱수의 합이다. 그리고 모든 수는 오각수이거나 둘, 셋, 넷, 또는 다섯 개의 오각수의 합이다. 이와 같이 계속된다.

---

4) 페르마 시대까지도 0은 수로 간주되지 않았다. 그래서 변수 중 하나에 자명한 해 0의 대입은 제외된다. 그리고 이 문제는 단지 양의 유리수 해만을 고려했다. 유리수 해가 존재하면 공통 분모를 각 해에 곱해서 정수 해로 만들 수 있으므로, 자연수 해만을 고려하면 충분하다.

이렇게 페르마의 마지막 정리가 탄생했다. 관련된 사항은 자연수와 지수에 불과하기 때문에 누구나 이해할 수 있고 쉽게 풀 수 있을 것으로 예상되었다. 그래서 수많은 수학자와 아마추어가 이 문제에 도전했다. 이 문제를 제외하고 당시 페르마가 제시한 모든 문제는 18세기까지 증명되거나 반증되었기 때문에, 이 문제에 '마지막'이라는 수식어가 붙게 되었다.

2. 페르마의 마지막 정리의 풀이 과정 - 페르마에서 쿠머까지

페르마는 1638년과 1659년 사이에 쓴 편지들에서 다음과 같은 문제 두 개를 언급했다[13, p. 17].

(1) 방정식 $x^3+y^3=z^3$과 $x^4+y^4=z^4$이 자연수 해를 갖지 않음을 보여라.
(2) 각 변의 길이가 자연수인 직각 삼각형의 넓이는 완전 제곱수가 될 수 없음을 보여라.

그러나 페르마가 남긴 기록에서 페르마의 마지막 정리에 대한 증명을 찾아볼 수 없다. 단지, 페르마가 $n=4$인 경우를 증명했음을 암시하는 약간의 증거가 있다. 페르마가 각 변의 길이가 모두 자연수인 직각 삼각형의 넓이는 어떠한 자연수의 제곱도 될 수 없음을 증명한 독창적인 논법(무한 강하법)에서 그 증거를 찾아볼 수 있다. 이 결과로부터, 페르마는 방정식 $x^4+y^4=z^4$이 어떠한 자연수 해도 가질 수 없음을 유도할 수 있었고, 분명히 마지막 정리의 이 경우를 유도하기 위해서 넓이가 제곱수인 삼각형에 관한 이 결과를 그가 증명했다고 추측하는 것이 합리적이다. (이번 절의 자세한 내용은 [7, 제8장]을 참조하라.)

지수 $n=4$인 경우가 증명되었기 때문에, 페르마의 마지막 정리가 모든 소수 지수에 대해 참이면 모든 지수에 대해서도 참임을 즉시 알 수 있다.[5]

페르마의 마지막 정리에 대한 연구 결과는 이 정리가 제시되고 100년 이상이 지난 뒤에야 나타나기 시작했다. 오일러(L. Euler)는 정수 a와 b에 대해 $a+b\sqrt{-3}$ 꼴의 수 체계에서 유일 인수 분해가 성립한다는 사실을 이용해서 1753년 $n=3$인 경우를 증명했고, 1825년 디리클레(P.G.L. Dirichlet)와 르장드르(A.-M. Legendre)는 오일러의 증명을 확장시켜 지수 $n=5$인 경우를 독자적으로 증명했다. 그리고 디리클레는 1832년 $n=7$인 경우를 다루는 방법을 얻는 데 실패했지만 (훨씬 약한 결과인) $n=14$인 경우를 증명하는 데 성공했다. 1839년 드디어 라메(G. Lamé)는 $n=7$인 경우를 증명했는데, 수 7 자체와 매우 밀접하게 관련된 아주 교묘한 방법에 의존해야만 했다. 그리고 라메는 '원분 정수'(cyclotomic integer)의 개념을 도입해서 다른 경우들을 증명하려고 시도했지만 실패했다.

그런데 이렇게 각 지수에 대한 증명은 원래의 정리를 해결할 수 없다. 모든 지수에 적용되는 일반적인 해법이 필요하다. 이런 선상에서 페르마의 마지막 정리에 대한 획기적인 돌

5) 페르마의 방정식이 합성수인 지수 $n=lk$에 대해 자연수 해 $x=a$, $y=b$, $z=c$를 가지면, 즉 $a^{lk}+b^{lk}=c^{lk}$이면 $(a^l)^k+(b^l)^k=(c^l)^k$이므로 지수 k에 대해서도 자연수 해 $x=a^l$, $y=b^l$, $z=c^l$을 가진다.

파구가 독일 수학자 쿠머(E. Kummer)의 연구로부터 나타났다. 1847년 쿠머는 일부 소수들이 분명한 형태의 양식을 나타냄을 알게 되었다. 쿠머는 이 양식을 '정규성'(regularity)이라 불렀는데, 이것이 페르마의 마지막 정리에 대한 오일러 형태의 증명을 지속시킬 수 있도록 만들었다. 쿠머는 새로운 성질인 정규성을 사용해서 페르마의 마지막 정리가 정규 소수인 모든 지수 n에 대해 성립함을 증명할 수 있었다. 100보다 작은 소수 중에서 단지 37, 59, 67만이 정규 소수가 아니다. 그래서 쿠머의 결과는 단번에 36까지의 모든 지수와 37, 59, 67을 제외한 100보다 작은 모든 소수 지수에 대해서 페르마의 마지막 정리를 증명했다.

쿠머가 이런 연구에서 도입한 원분 정수를 일반화시킨 '아이디얼 수'에 대한 결정적인 새로운 개념은 매우 강력하고 광범위한 것으로 판명되었는데, 이것은 '아이디얼'이라는 좀더 일반적인 개념과 수학의 완전한 한 분야인 '아이디얼 이론'을 낳게 했다.

이후의 연구는 쿠머의 방법의 확장으로부터 이루어졌다. 컴퓨터 조사를 통해 4,000,000까지의 대부분의 소수가 정규 소수임이 밝혀졌다. 그리고 4,000,000보다 작은 모든 비정규 소수는 정규성보다는 약간 더 약한 어떤 성질을 만족시키지만, 그 성질도 또한 그런 지수에 대해 페르마의 마지막 정리가 성립하도록 만든다. 그래서 페르마의 마지막 정리는 4,000,000까지의 모든 지수에 대해 참임이 (1992년까지) 밝혀졌다. (페르마의 마지막 정리에 대한 또 다른 접근 방법은 다음 쪽 상자를 보라.)

3. 페르마의 마지막 정리의 풀이 과정 - 프라이에서 와일스까지

최근에 이르러, 페르마의 마지막 정리에 대한 연구는 타원 곡선 이론을 이용한 대수학적 접근 방법과 함께 기하학적, 위상 수학적, 해석학적 접근 방법을 이용하게 되었다. 1983년, 29세의 독일 수학자 팔팅스(G. Faltings)는 2보다 큰 지수 n에 대해 방정식 $x^n+y^n=z^n$은 많아야 '유한' 개의 서로 소인 해를 가짐을 밝혔다. 그는 이 증명으로 1986년 필즈상을 받았다. 그런데 이 결과는 20세기 초에 등장한 '모델의 추측'(Mordell's conjecture)이라는 좀더 일반적인 명제를 팔팅스가 증명함으로써 얻은 특수한 경우이다. 팔팅스는 이런 증명 과정에서 1950년대 이래 발달된 현대적인 대수 기하학의 기법을 이용했다. (이번 절의 개괄적인 내용은 [8, 제6장]을 참조하라.)

1980년대 말 페르마의 마지막 정리를 함의하는 여러 가지 추측이 등장했다[4, p. 8]. 이는 페르마의 마지막 정리가 고립된 기이한 명제가 아니라 다른 분야와 밀접하게 관련되어 있음을 보여주었다. 특히, "유리수 체 위의 모든 타원 곡선은 모듈러 곡선이다"라고 주장하는 '시무라-타니야마의 추측'이 있다. 1955년 일본 수학자 타니야마(Y. Taniyama)는 타원 곡선과 모듈러 곡선 사이에 어떤 명확한 관계가 있을 것이라고 추측했다. 타니야마의 추측은 1968년 주어진 타원 곡선과 관계가 있어야 하는 정확한 모듈러 곡선을 결정하는 방법을 밝힌 베유(A. Weil)에 의해 좀더 명확하게 되었으며, 1971년 시무라(G. Shimura)는 베유의 과정이 매우 특별한 방정식족에 대해 적용된다는 사실을 증명했다. 그래서 타니야마의 원래

추측은 시무라-타니야마의 추측으로 불리게 되었다. (좀더 자세한 수학적 내용은 [1], [2], [4]를 참조하라.)

당시 이런 매우 추상적인 추측과 페르마의 마지막 정리 사이에 어떤 관계가 있을 것이라고는 누구도 생각하지 못했다. 그러나 독일 수학자 프라이(G. Frey)는 1985년 이 둘 사이에 매우 밀접한 관계가 있음을 확인했다. 즉, 만약 정수 a, b, c, n이 존재해서 $c^n=a^n+b^n$이 성립하면 이와 관련된 타원 곡선 $y^2=x(x-a^n)(x+b^n)$은 모듈러 곡선이 아닐 것이라고 짐작했다. 그 뒤 1986년 미국 수학자 리벳(K. Ribet)은 페르마의 마지막 정리에 대한 반례의 존재가 모듈러 곡선이 될 수 없는 타원 곡선의 존재를 명확하게 유도하고, 이에 따라 시무라-타니야마의 추측에 모순된다는 사실을 결론적으로 증명했다. 그래서 시무라-타니야마의 추측이 페르마의 마지막 정리를 함의함을 증명했다.

페르마의 마지막 정리에 대한 또 다른 접근 방법

홀수인 소수 p에 대해 방정식 $x^p+y^p=z^p$이 p의 배수가 아니고 서로 소인 자연수만으로 이루어진 해를 갖지 않을 때를 제1의 경우, 적어도 하나가 p의 배수이고 서로 소인 자연수로 이루어진 해를 갖지 않을 때를 제2의 경우라고 한다. 오랜 기간에 걸쳐 매우 중요한 진전을 이루게 만든 것은 제1의 경우이다. (라메와 쿠머의 연구보다 훨씬 앞선) 1820년 프랑스 수학자 제르맹(S. Germain)은 p와 $2p+1$이 모두 소수이면 이런 p에 대해 마지막 정리의 제1의 경우가 성립함을 보였다.

그 뒤 르장드르는 제르맹의 생각을 확장시켜

$$4p+1,\ 8p+1,\ 10p+1,\ 14p+1,\ 16p+1$$

중 하나가 소수인 임의의 소수 p에 대해 제1의 경우를 증명했다. 이것은 100보다 작은 모든 소수 지수 p에 대해 제1의 경우를 밝히는 데 충분하다. 그렇지만 물론 쿠머의 결과가 이것을 대신할 수 있다.

오랜 기간에 걸쳐 얻은 다른 결과에 의해 제1의 경우는 다양한 기준을 만족시키는 모든 소수에 대해 성립한다. 이런 것 중 하나로 1910년 미리마노프(Mirimanoff)가 얻은 기준은 음이 아닌 정수 a와 b에 대해 $2^a3^b\pm1$ 또는 $\pm2^a\pm3^b$ 꼴의 소수 p이다. 1982년까지 레머는 60억 이하의 모든 소수에 대해 제1의 경우가 성립함을 밝혔다.

1985년 미국의 애들만(Adleman)과 프랑스의 푸브리(Fouvry) 및 영국의 히스-브라운(Heath-Brown)은 제르맹 기준을 일반화시켜서 무수히 많은 소수에 대해 마지막 정리의 제1 경우가 성립함을 증명했다.

시무라-타니야마의 추측은 성질이 대단히 많이 알려진 기하학적 대상에 관한 것이었으며, 이 추측을 신뢰할 만한 충분한 근거가 있었다. 또 이를 증명하는 명확한 방법도 몇 가지 있었다. 드디어 수학자들은 마지막 정리에 접근하는 강력한 체제를 갖추게 되었다. 이런 도전을 시작한 사람 중에는 프린스턴 대학교에 근무하고 있는 영국 수학자 와일스도 있었다. 와일스는 그 뒤 7년 동안 시무라-타니야마의 추측을 증명하는 길을 찾으려고 모든 노력을 기울였다. 그는 1991년 모든 타원 곡선이 아니라 특수한 종류의 타원 곡선에 적용된 시무라-타니야마 추측의 특별한 경우를 증명할 수 있다고 확신했고, 2년 뒤인 1993년 드디어 이를 증명하는 데 성공했다.

1993년 6월 23일, 와일스는 영국 케임브리지에 있는 뉴턴 연구소에서 열린 학술 회의에서 연속적인 세 번의 강의를 진행하던 중, 페르마의 마지막 정리를 충분히 함의할 수 있는 새롭고 심오한 결과의 증명을 제시했다. 좀더 정확하게 말하면, 와일스는 반안정적 타원 곡선에 대해 시무라-타니야마의 추측이 참임을 증명했다. 몇 년 전 리벳이 밝힌 대로, 이 추측이 모든 반안정적 곡선에 적용될 때 페르마의 마지막 정리는 그 추측의 따름 정리가 된다.

사실, 처음에 와일스는 자신의 증명이 마지막 정리를 내포한다고 확신했고 그래서 그의 6월 발표는 페르마의 오래된 난문에 대한 증명이었다. 그러나 와일스의 증명에서 몇 가지 논리적 비약이 발견되었다. 와일스가 해결할 수 없었던 마지막 한 가지 결함은 1994년 10월 케임브리지 대학교의 테일러와의 공동으로 해결해서 논문 [16]으로 발표했고, 페르마의 마지막 정리의 증명이 포함된 주요한 부분은 논문 [17]로 발표했다. 이렇게 350년 이상의 기나긴 여정이 끝을 맺었다.

4. 볼프스켈 상

페르마의 마지막 정리의 증명을 최초로 찾아내는 사람에게 수여될 몇 가지 큰 상금이 이 문제의 매력을 증폭시켰다. 프랑스 과학원은 1816년 3,000프랑의 상금 및 금메달을 제시했다. 프랑스 과학원은 1850년에도 또다시 상을 제시했는데, 코시(A.-L. Cauchy)의 제의로 이를 철회하고, 쿠머에서 메달을 수여했다.

볼프스켈(Paul Friedrich Wolfskehl, 1856-1906)은 페르마의 마지막 정리를 최초로 완벽하게 증명한 사람에게 줄 상금으로 100,000마르크를 괴팅겐 (왕립) 과학원에 기증했고, 이에 따라 1908년 볼프스켈 상이 제정되었다. (이 상금의 유효 기간은 2007년 9월 13일이었다. 볼프스켈의 생애는 다음 쪽 상자를 보라.) 그리고 상금이 수여될 때까지, 원금에 붙는 이자는 이 학술원의 위원회가 추천하는 용도로 쓰이게 되었다. 이 위원회의 위원장이 된 힐베르트(D. Hilbert)는 2,500마르크의 이자 돈을 푸앵카레(H. Poincaré)를 괴팅겐 대학교에 초청해서 일련의 강의를 듣는 데 사용했다. 그 뒤에도 이런 방법으로 힐베르트는 다른 수학자들을 괴팅겐 대학교에 초청해서 강연을 듣는 데 사용했다.

볼프스켈 상의 수상에 관한 매우 엄격한 제약이 많이 있었지만, 이 상이 제정된 뒤 명예

볼프스켈

볼프스켈은 1856년 6월 30일 독일 다름슈타트(Darmstadt)에서 부유한 유대계 은행가(Joseph Carl Theodor Wolfskehl, 1814-1863)의 둘째 아들로 태어났다. 볼프스켈은 1875년-1880년 라이프니츠, 튀빙겐, 하이델베르크 등의 대학에서 의학을 공부하고 의학 박사 학위 취득했지만, 1880년경부터 나타나기 시작한 다발성 경화증으로 환자를 볼 수 없게 되었다. (다발성 경화증은 뇌, 척추의 도처에 경화 현상이 일어나는 신경증으로, 언어 장애, 하지의 근력 저하, 정신력 황폐, 안구 진탕증 등이 나타난다. 주로 젊은 사람이 걸린다.) 그래서 그는 수학을 공부하기로 결정하고 1880년 본 대학에 입학했다. 1881년 베를린 대학으로 옮겨 1883년까지 다녔는데, 이 때 그는 70대의 쿠머(E.E. Kummer, 1810-1893)의 강의도 들었다. 쿠머의 영향을 받아, 수론, 특히 해석적 수론을 전공했다. 이 때 페르마의 마지막 정리에 대해 알게 되었고, 이와 관련된 쿠머의 논문을 깊이 있게 연구했다. 그 뒤 1887년-1890년 다름슈타트 공과 대학에서 수론을 강의했지만, 다발성 경화증이 더욱 악화되어 완전히 마비되었고 결국 강의를 포기할 수밖에 없었다. 그러나 그 뒤에도 간단한 수학 논문을 몇 편 발표했다. 지속적인 보호가 필요하게 된 그는 1903년 10월 12일 53세의 여성(Susanne Magarethe Marie Frölish)과 결혼했다. 그런데 아내는 악처로 밝혀졌으며, 그의 말년을 산 지옥으로 만들었다. 볼프스켈은 1905년 1월 '페르마의 마지막 증명을 처음으로 증명하는 사람'을 위해 유서의 내용을 바꾸었다. 그는 자신의 재산 중 10만 마르크를 괴팅겐 (왕립) 과학원에 위탁하고 볼프스켈 상의 관리를 부탁했다. 볼프스켈은 1906년 9월 13일에 죽었다[3].

[6]과 [15]에는 파울 볼프스켈이 페르마의 마지막 정리의 증명에 실패하고 어떤 아름다움 여인으로부터 실연을 당한 뒤 자살을 기도했다는 이야기가 실려 있다. 최종적인 순간에 쿠머의 논문을 읽다가 논리적 비약을 발견하고, 이를 보완하는 과정에서 큰 즐거움을 얻었고 삶의 의욕을 되살렸다고 한다. 그래서 페르마의 마지막 정리는 '한 사람의 생명을 살린 문제'가 되었다. 그런데 바르너(K. Barner)는 [3]에서 이에 이의를 제기했다. 볼프스켈이 자살을 결심했다면, 그것은 오히려 자신의 심각한 병 때문이었을 것이라고 주장했다. 그리고 볼프스켈 상을 제정한 동기는 그의 인생에서 진정으로 유일한 사랑인 수론이 말년에 그에게 큰 위안은 주었다는 사실과 더 큰 관계가 있을 것이라고 썼다.

를 얻고 상금을 타려는 수많은 아마추어 수학자들은 자신의 '증명'을 괴팅겐 과학원으로 보냈다. 이 상이 제정된 첫 해에는 무려 621개의 풀이가 접수되었으며, 최근까지도 매달 평균

네 편씩 답지했다. 현재까지 전체적으로 '5000개 이상'의 풀이가 접수되었다고 한다. 그래서 페르마의 마지막 정리는 '잘못된 풀이가 가장 많은 문제'가 되었다. (이번 절의 내용은 [3]에서 발췌했다.)

와일스는 최종 논문을 1995년 5월 잡지를 통해 발표했지만, 규정에 따라 2년 동안의 심사 기간을 거친 뒤인 1997년 6월 27일 볼프스켈 상을 수상했다. 와일스는 얼마의 상금을 받았을까? 통설에 따르면, 이 상금이 완전히 사라졌다고 한다. 사실, 최근까지도 정확한 금액을 알 수 없었다. 이것은 괴팅겐 과학원이 이를 비밀로 유지했기 때문에 발생했는데, 다른 저자들의 부정확한 주장이 일조를 했다. 이런 부정확한 주장은 벨(E.T. Bell)의 책으로부터 출발했다. 그는 책 **수학을 만든 사람들**(Men of Mathematicians, 1937)에서 제1차 세계 대전 뒤 독일에서 발생한 인플레이션 때문에 볼프스켈 상금이 1페니히도 채 되지 않는다고 썼다. 그 뒤 이 슬픈 이야기는 검증되지 않은 채 많은 저자에 의해 반복되었다. 최근에 몇 명의 저자에 의해 새로운 추측이 등장했었지만, 역시 정확하지는 못했다.

1906년 볼프스켈 상금 100,000(금)마르크는 당시 35.8423킬로그램의 금과 교환할 수 있었다. 그렇지만 제1차 세계 대전 이전의 금을 다른 상품과 비교할 때 오늘날보다 약 5배 이상의 가치가 있다. 그래서 이 상금은 오늘날 약 1,700,000달러의 구매력이 있다. 이 돈은 볼프스켈의 유언에 따라 '안전하게' 비밀로 유지되었다. 1920년대 초 바이마르 공화국에서 심각한 인플레이션이 발생한 뒤, 1924년 라이히스마르크(RM)가 도입되었고 볼프스켈 상금은 20,000RM이 되었다. 이자와 복리에 의해 이 상금의 가치는 1948년 75,000RM로 높아졌다. 이것은 약 5%의 연이율을 반영한다. 1948년 화폐 개혁을 통해 독일 마르크(DM)가 도입되었고, 볼프스켈 상금은 10:1로 축소되어 7,500DM이 되었다. 와일스의 논문이 발표된 뒤인 1995년 9월 드디어 괴팅겐 과학원은 발표된 증명이 정확하다면 '약 70,000DM의 상금이 수여될 것이다'라고 공표했다. 1997년 6월 27일 와일스에게 볼프스켈 상이 수여될 때, 상금은 75,000DM가 되었다. 이것은 약 5%의 연이율 때문에 상금 총액이 지난 49년간 10배로 증가했음을 의미한다[3, p. 1298].

5. 빌의 문제

볼프스켈 상금은 사라졌다. 이제, 수학 연구로 큰돈을 벌 수 있는 길은 없을까? 물론, 작은 상금이 걸린 상이 몇 가지 있다. 그런데 한 은행가가 최근에 5만 달러의 상금이 붙은 문제를 제시했다. (이번 절의 내용은 [9]와 [12]를 요약한 것이다.)

빌(Andrew Beal)은 미국 텍사스 주 달라스에서 가장 큰 지방 은행인 빌 은행(Beal Bank)의 창설자, 소유자, 행장이며, 다섯 자녀의 아버지이다. 그리고 그는 최근에 빌 항공 우주사(Beal Aerospace)를 창설했는데, 이 회사는 지구 궤도에 인공 위성을 쏘아 올릴 차세대 로켓을 설계・제작하고 있다. 빌은 또한 열성적인 아마추어 수학자로서 페르마의 마지막 정리를 오랫동안 고려했었다. 빌은 1993년 여름 페르마의 마지막 정리가 와일스에 의해 증명되

었다는 소식을 듣고, 자신의 독자적인 증명을 찾아보려고 노력하다가 1994년 다음과 같은 문제를 생각해냈다.

> x, y, z, m, n, r은 모두 자연수이고 m, n, $r > 2$라 하자. 만약 $x^m + y^n = z^r$이 성립하면, x, y, z는 공통 인수를 가진다.

달리 표현하면 다음과 같다.

> 2보다 큰 지수 m, n, r에 대해 방정식 $x^m + y^n = z^r$은 서로 소인 자연수 해 x, y, z를 갖지 않는다.

이것이 '빌의 문제'이다. 이것은 페르마의 문제에서 세 개의 지수가 서로 다를 수 있는 약간 더 일반적인 형태로, 페르마의 마지막 정리는 빌의 문제에서 $m=n=r$인 특수한 경우이다. 빌의 문제는 여러 가지 면에서 페르마의 마지막 정리와 유사하다. 페르마의 마지막 정리와 같이, 서술하기도 쉽고 자연수로 해를 구해야 하는 간단한 방정식 이외에 더 이상의 복잡한 내용은 없다. 그러나 이 문제가 쉽게 풀릴 것으로 보이지는 않는다. 어쩌면 이 문제도 쉽게 제시할 수 있지만 답을 얻기가 몹시 어려운 수론 문제의 또 다른 예가 될 수도 있다. 빌은 많은 전문 수학자에게 문의했는데, 그들은 이 문제가 모든 면에서 페르마의 마지막 정리만큼 어려울 수 있다고 빌에게 알려주었다.6)

빌은 이 문제의 증명에 대한 상금으로 5만 달러를 제시했다. 이 상을 관리할 위원회는 세 명의 저명한 수학자 페퍼만(C. Fefferman), 그레이엄(R. Graham), 몰딘(R.D. Mauldin, 위원장)으로 구성되어 있다. 이 문제를 해결하면, 증명 또는 반례를 다음 주소로 보내면 된다.

> The Beal Conjecture and Prize
> c/o Professor R. Daniel Mauldin
> Department of Mathematics
> Box 305118
> University of North Texas
> Denton, Texas 76203
> U.S.A.

또, 팩스 미국 940-565-4805와 전자 우편 mauldin@dynamics.math.unt.edu를 이용해서 보낼 수도 있다. 인터넷에서 빌 문제에 관한 정보는 http://www.math.unt.edu/~mauldin/beal.html에서 찾아볼 수 있다.

6) 1995년 다몬(H. Darmon)과 그랜빌(A. Granville)은 [5]에서 빌의 문제가 많아야 유한 개의 해를 가진다는 사실을 증명했다.

6. 디오판토스 해석학과 '*abc* 추측'

페르마의 마지막 정리에 등장하는 방정식은 특수한 디오판토스 방정식이며, 타니야마-시무라의 추측은 타원 곡선 이론과 디오판토스 해석학을 연결하는 고리이다. 그러므로 이 정리의 증명 방법과 결과는 디오판토스 해석학에 큰 진전을 일으킬 것으로 보인다. 역사적으로, 디오판토스 문제는 개별적으로 서술되고 풀렸다. 수세기 동안, 수학자들은 특별한 종류의 방정식에 대한 특수한 과정을 고안했을 뿐이다. 힐베르트(D. Hilbert)가 1900년 국제 수학자 대회에서 제시한 23개의 문제 중 열째 문제는 디오판토스 방정식의 해의 존재를 판정하는 알고리즘을 고안하는 것이었지만, 1970년 마티야세비치(Y. Matijasevich)는 그런 알고리즘이 존재하지 않는다는 사실을 증명했다[7]. 즉 디오판토스 문제를 푸는 어떠한 과정을 고안하더라도 해를 결정할 수 없는 방정식이 언제나 존재한다. 다시 말하면, 결코 해를 찾을 수 없지만 해가 존재하지 않음을 증명할 수 없는 방정식이 존재한다. (이번 절의 내용은 [11]을 참조했다.)

이미 지적한 대로, 디오판토스 해석학에서는 각 문제를 개별적으로 해결했으며, 문제들을 연결하는 통합된 이론이 없었다. 그런데 이제, 이런 이론이 가까이 존재하는 것으로 보인다. 열쇠는 '*abc* 추측'이라 불리는 문제인데, 이것은 1980년대 중반 프랑스의 에스테를(J. Oesterle)과 영국의 매서(D.W. Masser)가 공식화시켰다. *abc* 추측은 누구나 이해할 수 있을 정도로 간단하며, 한 가지 정의만이 필요하다. 자연수 n의 서로 다른 소인수를 한 개씩 모두 선택해서 곱한 결과를 n의 '제곱 인수가 없는 부분'(square free part)이라 하고, sqp(n)로 나타낸다. 예를 들면, sqp(15)=15, sqp(16)=2, sqp(17)=17, sqp(18)=6, $\mathrm{sqp}(2^3\times 5^2\times 7)=2\times 5\times 7=70$이다. *abc* 추측은 다음과 같다.

> 서로 소인 자연수 a, b와 이것의 합 c에 대해, n이 1보다 큰 임의의 수이면 $[\mathrm{sqp}(abc)^n]/c$은 양의 최소값을 가진다.7)

만약 *abc* 추측이 참으로 밝혀지면, 무수히 많은 디오판토스 문제를 표현하는 새로운 방법을 제공하고 단 한 개의 수학적 명제로 만들어 이를 해결할 것이다. 이런 문제에는 세 개의 변수를 가진 대부분의 고전적인 방정식이 포함된다. 특히, *abc* 추측은 페르마의 마지막 정리를 함의하며[11], 빌의 문제도 (충분히 큰 지수에 대해) 함의한다[12]. *abc* 추측이 풀리면 오랫동안 해결되지 않았던 대단히 많은 문제가 풀릴 것이다. 이런 문제 중 일부는 이론적인 관심 이외에도 디오판토스 해석학을 이용하는 암호의 제작 등과 같은 많은 응용도 가능하다. *abc* 추측은 디오판토스 해석학에서 가장 중요한 미해결 문제이다.

---

7) 다음과 같이 표현할 수도 있다[11]. "각 $\varepsilon > 0$에 대해 상수 $\mu > 1$가 존재해서 a와 b가 서로 소이고 $a+b=c$이면 $\max(|a|,|b|,|c|)\le\mu[\mathrm{sqp}(abc)]^{1+\varepsilon}$이 성립한다."

7. 맺음말

페르마의 마지막 정리는 증명되었다. 그런데 이 정리는 고대의 삼대 작도 불능 문제와 같이 부정적인 결과이다. 해가 존재하지 않는 방정식이 어디에 쓸모가 있겠는가? 사실, 페르마의 마지막 정리를 증명하려는 시도는 이 정리 하나만을 위한 연구가 아니었으며, 훨씬 더 큰 목표를 향한 연구 과정의 일부에 지나지 않았다. 페르마의 마지막 정리의 증명은 더 중요한 문제를 해결하기 위한 과정에서 얻은 부산물에 불과하다.

실제로, 페르마의 마지막 정리에 대한 획기적인 돌파구를 연 쿠머는 페르마의 마지막 정리가 아니라 이른바 '상호 정리'(reciprocity theorem)를 증명하려고 시도했었다. 고차 상호 법칙을 증명하려는 쿠머의 시도로부터 원분 정수와 아이디얼 수가 등장했는데, 이런 개념은 페르마의 마지막 정리와 흥미로운 관계를 갖고 있을 뿐만 아니라 유체(class field) 이론과 추상 대수학의 발달에도 중요한 공헌을 했다[4, p. 6]. 그리고 와일스의 연구도 오래 전부터 수학자에게 큰 과제를 제시한 디오판토스 방정식의 풀이와 관련이 있으며, 타원 곡선과 모듈러 형식(modular form) 및 갈루아 표현(Galois representation) 이론을 창조하고 이들 사이의 관계를 연구한 많은 수학자의 도움으로 이루어졌다. 와일스가 증명한 결정적인 명제인 시무라-타니야마의 추측은 근본적으로 다른 내용이었으며, 페르마의 마지막 정리는 우연한 부산물이었다. 이 결과는 그 자체로 페르마의 마지막 정리만큼 아름답고, 사실 훨씬 더 중요하다.

페르마의 마지막 정리의 증명은 끝이 아니라 또 다른 시작이다. 증명을 얻기 위해 사용된 방법은 페르마의 마지막 정리 자체보다 훨씬 더 중요하다. 와일스가 얻은 결과와 이를 뒷받침해 준 다른 많은 수학자의 연구는 분명히 수학의 많은 분야에 엄청난 영향을 줄 것이다. 페르마의 마지막 정리를 증명한 뒤 와일스는 말했다[15]. "사람들은 내가 그들의 문제를 빼앗아 가 버렸다고 말했다. 그리고 다른 문제를 제시해 줄 수 있는지를 물었다. 울적한 감정이 남아있다. 우리는 오랫동안 우리 곁에 있었으며 많은 사람을 수학으로 유혹했던 것을 잃었다. 아마도, 이것은 수학 문제의 운명일 것이다. 우리는 우리의 관심을 사로잡을 새로운 문제를 찾아야 한다."

참고 문헌

1. 박화신, "Fermat Last Theorem은 풀렸는가?" **대한수학회 뉴스레터**, 제36호(1993년 10월), 1-3.
2. 한상근, "페르마 문제에 관한 이야기," **대한수학회 뉴스레터**, 제43호(1995년 7월), 16-19.
3. Barner, Klaus, "Paul Wolfskehl and Wolfskehl Prize," *Notices of the AMS*, Vol. 44, No. 10(Nov. 1997), 1294-1303.

4. Cox, David A., "Introduction to Fermat's Last Theorem," *Amer. Math. Monthly*, Vol. 101, No. 1 (Jan. 1994), 3-14.
5. Darmon, Henri & Granville, Andrew, "On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$," *Bull. London Math. Soc.* 27 (1995), 513-543.
6. Davis, P.J. & Chin, W.G., *3.1416 and all that*, Birkhäuser, Boston, 1984.
7. Devlin, Keith/허민 옮김, **수학: 새로운 황금 시대**, 경문사, 서울, 1995.
8. Devlin, Keith/허민·오혜영 옮김, **수학: 양식의 과학**, 경문사, 서울, 1996.
9. Devlin, Keith, "Move Over Fermat, Now Its Time for Beal's Problem," *Math Horizons*, Feb. 1998, 8-10.
10. Eves, Howard W., *Mathematical Circles Adieu*, Prindle, Weber & Schmidt, Inc., Boston, 1977.
11. Goldfeld, Dorian, "Beyond the Last Theorem," *Math Horizons*, Sept. 1996, 26-34.
12. Mauldin, R. Daniel, "A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem," *Notices of AMS*, Vol. 44, No. 11 (Dec. 1997), 1436-1437.
13. Osserman, R. ed., *Fermat's Last Theorem*(A Supplement to the Video), Mathematical Sciences Research Institute, Berkeley, CA, 1995.
14. Reid, Constance/허민 옮김, **영부터 무한대까지**, 경문사, 서울, 1997.
15. Singh, Simon, "How math can save your life," *Math Horizons*, Feb. 1998, 5-7.
16. Taylor, Richard & Andrew Wiles, "Ring-theoretic properties of certain Hecke algebras," *Annals of Mathematics*, Vol. 141 (1995), 553-572.
17. Wiles, Andrew, "Modular elliptic curves and Fermat's Last Theorem," *Annals of Mathematics*, Vol. 141 (1995), 443-551.