2

수학 분야

현대 수학 미해결 난계 풀었다

지난 30년 동안 수학계는 순수수학과 응용수학, 두 분야 모두에서 괄목할 만한 발전을 이룩하였다. 순수수학 분야에서는 무엇보다도 먼저 정수론, 더 나아가서는 수학의 모든 분야에서 가장 오래된(360년) 미해결 문제의 하나인 페르마의 마지막 정리가 증명되었다. 또 위상수학분야의 가장 큰 미해결문제인 푸앙카레 예상이 2006년도에 증명되었다. 응용수학 분야에서는 CT 스캔 등 여러 의료 분야에도 수학이 깊숙이 관계되고 있지만, 특히 암호학에서 괄목할 만한 발전을 이루어 요즘 전자상거래, 특히 신용카드를 사용할 때 이용되는 암호기술, 공개키 RSA 방법이 중요하게 쓰이고 있다.

와일즈 교수, '페르마의 마지막 정리' 증명

글 | **김명환** _ 서울대학교 수학과 교수 mhkim@math.snu.ac.kr

1993년 6월 케임브리지대학교의 한 학술회의에 모인 수학자들은 수학사에 길이 남을 사건을 목격하고 있었다. 360여 년 동안 수많은 수학자들의 도전을 물리치고 수학역사상 가장 유명한 미해결문제로 남아 있던 '페르마의 마지막 정리'가 와일즈 교수에 의하여 증명되는 순간이었다. 이 소식은 곧 전세계에 알려졌다. 그 후 와일즈의 증명에 오류가 발견되고 증명이 보완되어 마침내 1995년 5월 세계 최고의 권위를 자랑하는 수학전문학술지 '수학연보'에 장장 130쪽에 달하는 페르마의 마지막 정리의 완전한 증명이 활자화되기까지 전세계 수학계는 놀라움과 감동으로 술렁이며 가히 20세기 최고의 수학적 사건이라고 할 수 있는 페르마의 마지막 정리의 정복여부에 촉각을 곤두세웠다.

페르마, '아리스메티카'에 새로운 의문들 제시

페르마는 프랑스 툴루즈 지방의 의원이자 판사였다. 그는 여가시간에 수학을 공부한 아마추어 수학자였지만, 데카르트와 함께 해석기하학의 개척자로, 파스칼과 함께 확률론의 창시자로, 그리고 특히 정수론 분야에서는 '현대 정수론의 아버지'라 불릴 만큼 위대한 업적을 남긴 17세기 최고의 수학자 중 한 사람으로 여겨지고 있다. 그는 디오판토스가 서기 250년경에 쓴 '아리스메티카'의 라틴어 번역판을 가지고 다니며 시간이 날 때마다 그 책에 소개된 수많은 미해결문제들에 도전하였으며, 그 중 많은 문제를 해결하였고, 또한 새로운 의문들을 제시하였다. 그는 이 모든 것을 그 책의 여백에 기록하거나, 다른 수학자들에게 보낸 편지에 기록하였다. 19세

기 초반에 이르러 오일러, 라그랑주, 가우스 등에 의하여 페르마가 제기한 수많은 새로운 의문들은 하나만 남기고 모두 해결되었다. 마지막으로 남은 것이 바로 '페르마의 마지막 정리'다. 마지막이란 수식어가 붙은 이유는 이 때문인 듯하다. 페르마는 자신이 지니고 있던 '아리스메티카'의 여백에 다음과 같이 기록하고 있다.

"$n \geq 3$인 임의의 양의 정수 n에 대하여, 페르마 방정식 $x^n + y^n = z^n$은 0 아닌 정수 x, y, z를 해로 가질 수 없다. 나는 이러한 사실에 대한 아름다운 증명을 발견하였다. 그러나 책의 여백이 너무 좁아서 나의 증명을 모두 담을 수가 없다."

이것이 1630년에 쓴 것으로 알려진 유명한 페르마의 여백기록이다. 후세 수학자들이 그의 주장을 '페르마의 마지막 예상'이라 부르는 대신 '페르마의 마지막 정리'로 부르는 것은 그에 대한 존경의 의미일 것이다.

이후 제르맹, 디리클레, 르장드르, 라메, 코시, 쿠머, 비퍼리히, 판디버, 폴팅스, 미야오카 등 수많은 수학자들이 이 문제에 도전하였으나, 모두 실패하거나 극히 부분적인 결과를 얻는데 그쳤다. 그 중에서도 쿠머는 평생을 바쳐 이 문제를 연구하는 과정에서 대수적 정수론이라는 새로운 분야를 탄생시켰고, 폴팅스는 소위 '모델의 예상'을 증명함으로써 페르마 방정식의 기약정수해가 유한개뿐임을 보이고 이 업적으로 1986년 필즈상을 수상하였다.

와일즈, '시무라 – 다니야마 예상' 증명해 문제 해결

와일즈는 타원곡선을 연구하던 수학자로서, "모든 타원곡선에는 보형형식을 대응시킬 수 있다"는 소위 '시무라 – 다니야마 예상'을 증명함으로써, 360여 년에 걸친 페르마의 마지막 정리의 역사에 종지부를 찍었다. 타원곡선 이론은 수학의 여러 분야에 걸쳐 다양하게 응용되고 있으며, 최근에는 암호이론에의 응용까지 발견되어 각광을 받고 있다.

페르마의 마지막 정리와는 전혀 관련이 없어 보이는 이 예상이 페르마의 마지막 정리와 밀접한 관련이 있을 것으로 생각한 것은 프라이였다. 1980년대초에 그는 페르마 방정식의 정수해를 이용하여 프라이 곡선이라 불리는 타원곡선을 만들고, 프라이 곡선이 존재할 수 없는 가상의 타원곡선임을 보임으로써 페르마의 마지막 정리를 증명할 수 있음을 발표하였다. 그리고 몇 년 후, 리벳은 '시레의 ε–예상'을 증명함으로써 프라이 곡선에는 보형형식을 대응시킬 수 없음을 보였다. 따라서 시무라 – 다니야마 예상을 증명하게 되면 프라이 곡선은 존재할 수 없는 가상의 타원곡선이 되어 페르마의 마지막 정리가 정복되는 상황에 이르렀다. 와일즈는 바로 이 시무라 – 다니야마 예상을 증명한 것이다.

와일즈는 영국 출신의 수학자로서 케임브리지대학교에서 코츠 교수의 지도하에 박사학위를 취득하였으며, 1980년대 중반부터 프린스턴대학교 수학과의 교수로 재직중이다. 10세 때 마을의 도서관에서 우연히 알게 된 페르마의 마지막 정리에 매료된 그는 이 문제를 풀기 위하여 '진이 빠질' 정도로 애를 썼다고 한다. 그 후 와일즈는 페르마의 마지막 정리에서 손을 떼고, 코츠의 지도 아래 타원곡선 이론의 전문가가 된다.

1986년 어느 날 와일즈는 친구의 집에서 차를 마시던 중에 그 친구로부터 리벳이 시레의 ε–예상을 해결하였다는 소식을 접한다. 와일즈는 '전기에 감전된 것 같은 느낌'이었다고 회상하고 있다. 페르마의 마지막 정리가 다시 자신을 찾아온 것으로 받아들인 와일즈는 바로 그날부터 7년 동안 집에서 아무에게도 알리지 않고 혼자서 연구에 몰두하였다. 1993년초, 드디어 그는 증명이 거의 완성되었다는 자신을 가질 수 있었다. 그는 동료인 카츠와 사르낙에게 이 사실을 알리고 케임브리지로 날아갔다. 모교에서 열리는 학술회의에서 발표를 하기 위해서였다. 역사적인 발표가 끝나자 전세계 수학계가 경악하였다. 어느 정도 예상은 하였지만 그 반응은 예상을 훨씬 뛰어 넘는 가히 폭발적인 것이었다.

증명에서 오류가 발견되고, 다시 2년의 연구 끝에 완성된 논문이 발간되었다. 와일즈의 증명은 메이저, 콜리바긴, 루빈, 투넬, 랭글랜즈, 플락, 히다, 테일러, 카츠, 코츠, 이와사와 등의 타원곡선에 관한 최신의 이론들을 총동원하여 이루어진 20세기 최고의 업적이라고 일컬을 만한 걸작이다.

요즈음 같이 너나없이 더 많은 논문을 경쟁적으로 발표하는 분위기를 생각하면 와일즈의 쾌거는 신선한 충격이라 하겠다. 무려 9년 동안, 해결이 불가능해 보이는 문제에 매달려 고독하고 고통스러운 연구를 하는 교수가 있다는 것과 그러한 교수를 지원하는 대학이 있다는 것이 어쩌면 우리와 선진국의 차이가 아닐까? ST

글쓴이는 서울대학교 수학과 졸업 후 오하이오 주립대학에서 석사 · 박사학위를 받았다. 서울대학교 자연과학대학 부학장, 국제수학올림피아드 한국대표단 단장, BK21 서울대학교 수리과학사업단 부단장을 지냈으며, 현재 아시아–태평양 수학 올림피아드 의장을 겸임하고 있다.

페렐만 교수, '푸앙카레 가설' 해결

글 | 조도상 _ 건국대학교 수학교육과 교수 dosjoe@konkuk.ac.kr

2006년 8월 스페인 마드리드에서 개최된 세계수학자대회(ICM 2006) 첫날, 국제수학연맹(IMU) 사무총장인 존 볼 경(Sir John Ball)은 4명의 수학자를 필즈상 수상자로 발표한다. 그 중에는 러시안 수학자 그레고리 페렐만의 이름이 포함되어 있다. 그의 업적은 푸앙카레 가설을 해결한 공로라고 한다. 그러나 그날 대회장에서 그를 본 사람은 아무도 없었다. 존 볼 경은 그가 모든 수학자들의 영예인 필즈메달 수상을 거부했다고 발표하며 아쉬움을 나타냈다. 며칠 후 '뉴요커' 잡지는 '다양체의 운명'이라는 제목과 '전설적인 문제와 누가 풀었는가에 대한 다툼'이라는 부제 아래 푸앙카레 가설과 페렐만과 야우 교수에 관한 이야기를 싣고 있었다. 누가 이 문제를 해결하였는가는 명백해진 상태이고 더 이상의 논란은 없어 보였다. 그렇다면 어떻게 이 어려운 문제가 해결 되었을까?

100년간 못 푼 가설, '단순 연결된 공간은 구다'

20세기초 프랑스 수학자 푸앙카레는 위상수학분야에서 공간에 대한 많은 연구와 업적을 남겼는데 그가 해결하지 못한 문제가 바로 '단순 연결된 공간은 구이다'라는 푸앙카레 가설이다. 단순 연결되어 있음은 그 공간 안에 어떤 원을 그리더라도 그 원을 경계로 하는 모자를 씌울 수 있음을 말하는데, 좀 더 쉽게 이야기하면 그물을 칠 수 있는 공간이라고 할 수 있다. 예를 들어 3차원 공간 안에 평면과 수직인 직선이 있다고 하자. 평면에서 이 직선을 둘러싸는 원을 그린 다음 아무리 이 원을 움직여서 한 점으로 모으려 해도 직선을 지나치지 않고서는 그렇게 할 수 없다. 이러한 개념은 가장 단순한 형태의 공간 유형을 결정하는 척도인데 이러한 성질을 가진 공간은 실제로 구(한 점에서 일정한 거리에 있는 점들의 집합)와 위상적으로 같은 구조를 가지고 있다는 것이다. 2차원 구는 축구공의 껍질과 같고 3차원 구는 3차원 공간에 무한대점 하나를 더한 형태로 이해할 수 있다.

면적과 체적 같은 거리개념이 중요한 기하학과는 달리 위상수학에서는 공간의 본질적인 성질을 연구하는 분야로서 연속적으로 변환되는 공간을 구분하지 않는다. 다시 말해 물 컵과 접시는 같은 위상구조를 가진다. 위상적 개념은 공간의 본질적 이해뿐 아니라 매듭이론, 군론, 대수기하, 함수해석, 정수론 등 수학의 모든 분야에 활용되며 20세기 이후의 현대 수학에서의 중요한 자리를 차지하고 있다.

많은 수학자들은 푸앙카레 가설을 해결하고자 했으나 번번이 실패하였다. 그러나 그것은 단순한 실패가 아닌 새로운 방법과 비전을 제시하며 새로운 분야를 만들어 내기도 하였다. 예를 들면 일반화된 푸앙카레 가설의 해결에는 모스 이론과 h-코보디즘, 게이지 이론 등의 방법론들이 개발되어 위상수학뿐만 아니라 기하학과 이론물리에도 응용되어 지금까지 많은 결과와 연구가 진행되고 있다. 1980년대초까지 스메일, 프리드만, 도날드슨 교수 등이 일반화된 푸앙카레 가설에 관한 업적으로 필즈메달을 받을 때까지만 하더라도 3차원 푸앙카레 가설의 해결은 시간문제인 듯이 많은 수학자들이 기대하고 있었다. 그 후로 20년이 넘는 세월을 기다려야 했다.

티안 교수와 함께 페렐만의 업적을 473쪽의 논문으로 정리한 존 모건 교수는 세계수학자대회에서의 푸앙카레 가설 강연 후의 인터뷰에서 "이 문제가 생전에 해결될 수 있으리라는 기대는 하지 못했다"라고 밝히고 있다. 또한 페렐만의 업적이 가능했던 것은 "그가 멀리 볼 수 있었고, 그러기 위해서 그가 거인들의 어깨 위에 서 있었기 때문이다"라고 말했다. 그 거인 중의 한 사람이 리처드 해밀턴인데 그는 대학원생 시절부터 푸앙카레 가설에 관심을 갖고 25년이 넘는 세월 동안 리치 흐름에 대한 기초를 세우고 발전시킨 수학자였다. 물론 페렐만의 업적도 해밀턴의 사전 결과 없이는 가능하지 못했던 일이었다.

해밀턴의 아이디어는 주어진 공간에 줄 수 있는 거리들 중 특별한 성질을 가지는 거리함수를 리치 흐름을 통해 찾아낼 수 있다는 것인데, 이는 우주도 시간이 지나면서 블랙홀 같은 특이점들이 생기더라도 언젠가는 균일한 형태를 갖는 공간으로 수렴할 수 있다는

주장과 일맥상통한다. 문제 해결의 핵심은 이러한 특이점들을 어떻게 제어하고 피할 수 있을까 하는 문제로 귀결된다. 해밀턴은 시가 형태의 치명적인 특이점이 생기지 않는 한 푸앙카레 가설은 증명될 수 있음을 보였다. 그러나 이러한 특이점이 생기는 경우에는 아무런 주장도 할 수 없었다.

부와 명예 초월, 순수한 열정만으로 가설 증명

그러던 중 2002년 11월 페렐만은 웹상에 39쪽짜리 논문을 게재한다. 만약 증명이 틀렸다면 페렐만은 수학계에서 공식적으로 자존심에 큰 상처를 입게 되는 것이 분명한 일이었기 때문에 위험한 일이었다. 그의 논문은 수학계의 많은 관심을 이끌어 내기에 충분했다. 왜냐 하면 논문이 맞으면 푸앙카레 가설뿐 아니라 더 일반적인 3차원 기하학 문제도 해결이 가능했기 때문이다. 그러나 정작 해밀턴과 야우 교수 등 리치 흐름의 전문가들은 그의 논문에 큰 관심을 두지 않았다.

다음해 4월 페렐만은 프린스턴, MIT, 뉴욕 주립대학(스토니 부룩), 컬럼비아 등 미국 유수의 대학을 돌며 자신의 논문을 전문가들에게 설명했다. 그리고 그는 고향인 성 페테르부르크로 돌아갔다. 그해 7월 페렐만은 2편의 논문을 다시 인터넷에 올렸다. 그 후 많은 수학자들의 고통스러운 확인 작업이 시작되었다. 논문의 중요성뿐만 아니라 푸앙카레 가설의 해결에는 클레이 재단이 내놓은 100만 달러라는 상금이 걸려 있었다. 그 다음해 2004년 9월 프린스턴에서 열린 2주간의 페렐만의 증명에 관한 학회를 마친 뒤 강 티안 교수는 페렐만에게 "모든 증명을 이해했다. 모두 맞았다"라는 이메일을 보냈다.

페렐만은 오페라 공연장을 즐겨 찾는다고 한다. 그에 따르면 맨 뒷자리에서 서서 들으면 배우들의 의상이나 연기는 잘 볼 수 없으나 소리만큼은 어느 자리보다 더 잘 들을 수 있다고 말한다. 그는 그렇게 멀리서 수학계와 세상을 바라보고 듣고 있다. 현재 페렐만은 성 페테르부르크의 작은 임대 주택에서 어머니와 함께 살고 있다. 미국 유수대학의 영년직 교수 제의도, 필즈상 수상도 거부한 채 조용한 삶을 살고 있다. 어떤 사람들은 그가 필즈상 수상을 거부한 일에 오만하다는 말들을 하고 있지만, 그는 단지 순수한 마음으로 문제를 해결하려고 노력하였다. 그러나 그것이 맞고 틀리고, 상을 받고 안 받고는 그의 관심의 대상이 아니었다.

위대한 업적은 그런 순수한 마음과 정열로 가능했던 것이었다. 그가 살고 싶어 한 이상적인 세상을 지금 우리가 살고 있는 지구에서 찾기는 힘들어도 어딘가에서 숨 쉬고 있을 순수한 마음과 아름다운 열정이 존재하고 있음을 믿어본다. ST

글쓴이는 서울대학교 수학과 졸업 후 동대학원에서 석사학위를, 컬럼비아대학교에서 박사학위를 받았다. 이화여자대학교 연구전임강사, 포항공과대학교 방문강사, 고등과학원 조교수를 지냈다.

암호기술 획기적 발전 이끈 '공개키 암호'

글 | 임종인 _ 고려대학교 정보경영공학전문대학원장 jilim@korea.ac.kr

암호는 군대나 국가와 같은 특정한 분야에서 이용되는 특수기술로 사용되었으나 현대사회의 발전과 함께 차세대 사회경제의 기반 기술로 변화되었다. 디지털 정보사회가 고도화되고 전자상거래가 활성화됨에 따라, 암호기술은 인터넷을 기반으로 한 사회경제적 활동의 안전성과 신뢰성, 사용자 프라이버시 보호 등을 위한 핵심기술로 인식되고 있다. 세계 제2차 대전 때 수학적 논리가 암호 해독에 매우 유용하다는 것이 알려지면서, 이후 암호 알고리즘의 설계와 분석 연구에 수학이 깊이 관여하게 되었다.

현대 암호 시스템은 간단히 대칭키 암호 알고리즘과 공개키 암호 알고리즘으로 구성된다. 간단히 말해서, 대칭키 암호 알고리즘은 암호화 및 복호화시 동일한 키가 사용되는 반면, 공개키 암호 알고리즘은 암호용 키와 복호용 키가 서로 다르다는 차이점이 있다. 대칭키 암호 알고리즘은 고속 연산이 가능하며, 평문이 암호화되어도 길이가 늘어나지 않는다는 장점 때문에 대용량 데이터의 암호화나 실시간 암호 통신에 주로 사용된다. 그러나 대칭키 암호 알고리즘은 데이터의 송신자와 수신자가 동일한 키를 갖고 있어야 동작할 수 있기 때문에 키를 안전하게 전달해야 하는 문제점을 안고 있다.

디피와 헬만, 공개키 암호 알고리즘 개념 소개

1976년에 스탠퍼드대학의 교수인 마틴 헬만과 그의 제자 화이트필드 디피는 논문 '현대 암호학의 새로운 방향'에서 간단한 수학적 아이디어를 이용하여 이 문제를 해결할 수 있음을 보였는데, 이른바 '디피-헬만 키 교환'이라는 것으로 송신자와 수신자가 정보의 노출 없이 같은 키를 생성하게 하는 방법이다. 제3자가 그들의 키를 알기 위해서는 이산대수를 계산해야 하는 어려움을 극복해야 하는데, 이것은 효율적인 해법이 알려지지 않은 수학적 난제로 분류되어 있다. 디피와 헬만은 그 논문에서 공개키 암호 알고리즘의 개념을 소개하여 암호 기술 분야에 큰 획을 그었다. 공개키 암호는 고속연산이 불가능한 대신, 대칭키 암호를 보완하여 키 전달문제를 해결할 수 있을 뿐만 아니라 전자서명이 가능하다. 특히, 공개키 암호의 전자서명 기능으로 인하여 암호 시스템의 용도는 광범위하게 확대되었다. 오늘날 원격 로그인 프로토콜, 다자간 제어 시스템, 전자 투표, 전자 화폐, 전자 대금 결제, DB의 분산 운용 등에 있어서 그 필요성은 절대적이며, 소프트웨어 외에도 칩 등으로 구현되어 널리 사용되고 있다.

공개키 암호의 특징은 암호화에 사용되는 키(공개키)는 공개되며, 복호화에 사용되는 키(개인키)는 사용자가 비밀로 관리한다는 것이다. 사용자 외의 어떤 사람도 공개키나 암호문으로부터 개인키에 대한 정보를 얻을 수 없어야 한다. 대부분의 공개키 암호는 어떠한 수학적 난제를 이용하여 개인키에 대한 안전성을 확보한다. 즉, 어떤 수학적 난제를 풀어야만 개인키에 대한 정보를 얻을 수 있도록 알고리즘이 설계되어 있는 것이다. 가장 많이 사용되는 공개키 암호 알고리즘은 1977년에 론 리베스트, 아디 샤미르, 레오나르드 아델만에 의해 개발된 RSA 알고리즘으로서, 두 개의 큰 소수(약 512비트)의 곱으로 이루어진 합성수의 인수분해가 어렵다는 점을 이용한다. RSA의 세팅 및 연산 과정은 정수론에 대한 기초적인 지식을 가진 사람이면 누구나 이해할 수 있을 정도로 간단하지만, 공개키와 암호문으로부터 평문이나 개인키의 정보를 얻기 위한 길은 매우 험난하다. 1024비트 사이즈의 임의의 정수를 인수분해할 수 있는 방법을 찾는다면 RSA를 깰 수 있으나, 정수의 인수분해 문제는 이산대수 문제와 함께 암호학에서 가장 유명한 수학적 난제다.

RSA 외에도 이산대수 문제의 어려움을 이용한 엘가멜, 타원곡선군에서의 이산대수 문제를 이용하는 ECC 알고리즘이 대표적인 공개키 암호 알고리즘으로서 많은 환경에서 응용되고 있다. 오늘날 공개키 암호를 비롯한 암호 기술의 전반적인 발전에는 대수학, 정수론, 확률론과 같은 다양한 수학 이론이 뒷받침되었으며, 수학을 이용한 암호 연구는 앞으로도 지속되어 많은 연구 결과를 산출할 것으로 기대된다. ST

글쓴이는 고려대학교 수학과 졸업 후 동대학원에서 석사 · 박사학위를 받았다. 현재 고려대 정보보호기술 연구센터장, 한국정보보호학회 부회장, 국회 과학기술정보통신위원회 정책자문위원, 정보통신부 정보보호 자문위원 등을 겸임하고 있다.