Journal for History of Mathematics
Vol. 28 No. 2 (Apr. 2015), 85–102
http://dx.doi.org/10.14477/jhm.2015.28.2.085

A Historical Overview of Elliptic Curves

타원곡선의 역사 개관

Koh Youngmee 고영미 Ree Sangwook* 이상욱

Elliptic curves are a common theme among various fields of mathematics, such as number theory, algebraic geometry, complex analysis, cryptography, and mathematical physics. In the history of elliptic curves, we can find number theoretic problems on the one hand, and complex function theoretic ones on the other. The elliptic curve theory is a synthesis of those two indeed. As an overview of the history of elliptic curves, we survey the Diophantine equations of 3rd degree and the congruent number problem as some of number theoretic trails of elliptic curves. We discuss elliptic integrals and elliptic functions, from which we get a glimpse of idea where the name 'elliptic curve' came from. We explain how the solution of Diophantine equations of 3rd degree and elliptic functions are related. Finally we outline the BSD conjecture, one of the 7 millennium problems proposed by the Clay Math Institute, as an important problem concerning elliptic curves.

Keywords: Elliptic curves, rational points, congruent numbers, elliptic integral, elliptic function, Weierstrass $\wp$-function, L-function, Birch and Swinnerton-Dyer conjecture(BSD conjecture); 타원곡선, 유리점, 합동수, 타원적분, 타원함수, 바이어슈트라스 $\wp$-함수, L-함수, BSD 추측.

MSC: 01A55, 01A60, 11D45, 11G05, 14H52, 33E05

1 서론

타원곡선은 수학에서 매우 중요한 연구 대상이다. 실제로 페르마의 마지막 정리의 증명에 핵심적인 역할을 하고(1994년) 효율적인 암호체계를 만드는 데도 이용되면서(1985년), 정수론 분야에서 매우 중요한 연구 주제임이 입증되었다. 또한 2000년에 미국의 클레이 수학연구소에서 제시한 백만불의 상금이 걸려있는 일곱 개의 문제 중 하나인 BSD 추측도 타원곡선과 관련된 문제이고 보면 타원곡선이 얼마나 중요한 연구 대상인지 짐작할 만하다. 실제로 타원곡선은 정수론뿐만 아니라, 현대대수학, 대수기하학, 복소해석학 등을 포함한

*Corresponding Author.
Koh Youngmee: Dept. of Math., The Univ. of Suwon E-mail: ymkoh@suwon.ac.kr
Ree Sangwook: Dept. of Math., The Univ. of Suwon E-mail: swree@suwon.ac.kr
Received on Mar. 30, 2015, revised on Apr. 16, 2015, accepted on Apr. 21, 2015.

광범위한 수학적 지식이 요구되는 연구 주제이다.

이 논문은 타원곡선의 정의와 활용을 먼저 간단히 소개하고, 타원곡선의 유래와 관련 역사를 한 눈에 조망함을 목표로 한다. 1901년에 푸앵카레에 의해서 정립된 타원곡선 이론은 정수론 측면의 내용과 복소해석학 측면의 내용을 종합하여 이루어진 것이다. 그래서 타원곡선의 역사를 알기 위해서는 두 줄기의 역사를 살펴보아야 한다. 3세기경 디오판투스로부터 시작되는 이산 수학적 내용으로 구성된 줄기와 17세기경 적분학의 발달과 함께 시작되는 연속 수학적 내용의 줄기가 그것이고, 이들 두 줄기가 서로 어떻게 연관되어져 하나의 이론으로 거듭나게 되었는지를 정리하는 것이 타원곡선의 역사를 이해하는 일이 될 것이다. 그래서 우리는 타원곡선 관련 문제의 시작과 타원곡선의 유래 등을 살펴보고 타원곡선 이론이 생겨나게 되는 배경을 조망함과 더불어 타원곡선과 관련된 중요 문제인 BSD 추측을 소개하는 것으로 논문을 마무리하고자 한다.

2 타원곡선의 소개

2.1 타원곡선이란 무엇인가?

디오판투스로부터 뉴턴에 이르기까지 약 1500년 동안 타원곡선은 특정한 3차방정식으로 정의된 곡선으로 알려졌을 뿐이었다. 타원곡선을 원추곡선의 성질이 조금 일반화된 곡선으로 보았고, 특히 원추곡선에서처럼 간단한 방법으로 타원곡선 위의 유리점을 찾을 수도 있었다.

17세기에 원추곡선인 타원의 길이를 구하는 과정에서 생겨난 타원적분이 다항함수, 유리함수, 삼각함수, 지수함수, 로그함수 등을 아우르는 초등함수로는 계산할 수 없음이 밝혀지면서 원추곡선과 타원곡선의 중요한 차이점이 드러나기 시작하였다. 그것은 타원곡선은 원추곡선과는 다르게 유리함수로 매개변수표현이 되지 않는다는 것이다. 19세기 초에 타원적분 대신 그 역함수인 타원함수를 고려하기 시작하였고, 복소변수가 도입되면서 타원곡선과 원추곡선의 위상적 차이가 분명하게 드러나게 되었다. 타원곡선이란 이름은 그 발생과정에서 우연하게 붙여진 이름이다. 현대에 알려진 타원곡선은 정수론, 기하학, 현대대수학, 해석학, 위상수학이 종합되어 나타난 결과이다 [22].

타원곡선의 정의

타원곡선은 3차방정식이 다루어지는 체의 특성수에 따라 조금은 다르게 표현된다. 여기서는 타원곡선을 소개하기 위한 목적으로 실사영공간 또는 복소사영공간에 정의된 타원곡선을 다루기로 한다.

상수 a, b에 대하여 특이점을 갖지 않는 방정식

$$y^2 = x^3 + ax + b$$

에 의해 정의된 곡선을 「타원곡선(elliptic curve)」이라고 한다. $p(x) = x^3 + ax + b$라 하면 곡선 $f(x, y) = y^2 - p(x) = 0$의 특이점은 $f_x = 0$, $f_y = 0$을 만족시키는 점이다. 이를 다시 쓰면 $p(x) = 0$, $p'(x) = 0$이므로, 특이점이 없다는 말은 다항식 $p(x)$가 중근을 가지지 않음을 뜻한다. 즉, $p(x)$의 판별식이 $\Delta = -16(4a^3 + 27b^2) \neq 0$임을 의미한다.[1] 타원곡선은 기하학적으로는 대수곡선이고, 대수학 측면으로는 아벨군이다. 타원곡선 군에서의 연산은 기하적으로는 교점을 구하기 위한 작도법, 대수적으로는 방정식의 풀이, 해석학적으로는 복소함수를 이용하여 정의하고 설명할 수 있다.

타원곡선은 정수론에서 복소해석학, 그리고 암호론에서 수리물리학에 이르기까지 다양한 분야에서 다루어지는 중요 주제이자 도구이다.

2.2 타원곡선의 활용

타원곡선은 긴 역사를 지녔다. 2–3세기경에 디오판투스에 의해서 처음으로 3차방정식이 연구되었고, 그 후로 타원곡선에 관한 이론이 정수론 분야에서 다루어져오다가, 최근에 이르러 암호학에 응용되기까지에 이르렀다. 1984년에 렌스트라(Lenstra)가 타원곡선을 이용하여 정수를 소인수분해한 것이 암호학에서의 최초의 응용으로 간주된다. 1985년에 밀러(Miller)와 코블리츠(Koblitz)가 타원곡선을 활용한 새로운 암호체계를 제안하였다. 또한, 소수를 판별하거나, 페르마의 마지막 정리의 증명에도 중요한 도구로 활용되는 등, 타원곡선의 응용 범위는 계속해서 늘어나고 있다 [3,7,11].

유한체상의 타원곡선은 중요한 특징을 갖는다. 정해진 유한체 한 개에 대해서도 다양한 크기의 아벨군이 있고, 군 연산이 효율적이며, 군의 원소들의 표현이 불명확하다는 점 등이 정수의 인수분해, 소수의 판별, 암호 등에 활용되는 중요한 요인이다. 특히, 작은 사이즈의 타원곡선군을 이용하여 다른 암호체계와 같은 수준의 보안성을 가진 암호체계를 만들 수 있고, 많은 경우에 암호화키의 사이즈가 작아지고 작은 밴드폭이 요구되며 빠르게 실행되는 장점이 있다 [24].

진자와 관련된 역학 문제나 끈이론(string theory)에서도 타원함수가 활용되는 등, 물리학에서도 타원곡선의 응용을 발견할 수 있다 [24].

1) $\Delta \neq 0$은 사영공간에서 동차좌표로 나타낸 타원곡선 $Y^2Z = X^3 + aXZ^2 + bZ^3$이 특이점을 갖지 않음을 의미한다.

3 타원곡선의 역사: 정수론

3.1 디오판투스 방정식

디오판투스에 대하여는 정확하게 알려진 것이 없다. 다만 대략 150년에서 350년경에 알렉산드리아에서 살았던 수학자로서 2개 이상의 변수를 포함하는 다항방정식의 유리수해를 구하는 다양한 문제들을 다루어 13권으로 구성된 책《Arithmetica》를 출판하였음이 알려졌을 뿐이다 [18]. 이 책은 알렉산드리아 도서관이 파괴될 때 분실되었으나, 16세기에 6권이 발견되어 페르마를 포함한 유럽 수학자들의 집중 연구 대상이 되었고, 1971년에 추가로 다른 4권이 발견되어, 나머지 3권만 없어진 상태로 남아있다 [12].

디오판투스는 대수적인 기호를 만들어 사용하였고, 6차 부정방정식까지 다루었으며, 그리스 수학의 주류와 다르게 기하적인 맥락이나 함의가 없이 대수방정식 자체만을 다루었다. 그는 방정식의 유리수해를 구하는 데 관심을 두었고, 양의 해를 구하고자 했다 [13,18]. 디오판투스는 눈에 번히 보이는 유리수해를 갖는 부정방정식을 다루었는데 이에 대한 예를 몇 개 살펴보자. 아래에 제시된 문제들은 바슈마코바(Bashmakova)의 논문 [4]에 소개되어 있다.

《Arithmetica》 제2권 8번 문제는 주어진 a^2을 두 개의 제곱수로 나누는 문제이다[2].

$$x^2 + y^2 = a^2, \quad a^2 = 16$$

디오판투스는 이미 알고 있는 유리수해인 $(0,\, 4)$ 외에 다른 해를 구하기 위하여, $y = kx - 4$를 이용하였고 특별히 $k = 2$일 때[3] 해 $x = 16/5$, $y = 12/5$를 구하였다.

위의 문제를 일반화하여 제2권 9번 문제로

$$x^2 + y^2 = N = a^2 + b^2, \quad N = 13$$

과 같은 문제도 다루었다. 이 방정식의 뻔한 유리수해는 $(2,\, 3)$이다. 디오판투스는 $x = t + 2$로 두고 해가 $t = 0, y = 3$이 되게 하여 8번 문제의 형태로 바꾼 다음, $y = kt - 3$으로 두고 $k = 2$일 때 해를 구하였다.

실제로 위의 문제들에서 k가 유리수면 무엇이든 상관없이 유리수해를 구할 수 있다. 디오판투스는 그의 방법으로 무한히 많은 유리수해를 구할 수 있음을 알았다. 더욱이 이 방법은 2차곡선이 k를 매개변수로 하는 유리함수로 매개화됨을 보여준다. 특히, 원 $x^2 + y^2 = 1$을 유리함수 $(\frac{1-k^2}{1+k^2},\, \frac{2k}{1+k^2})$로 매개변수 k를 써서 표현할 수 있고, 이로부터 서로 소인 두 양의 정수 m, n에 대하여 $(n^2 - m^2,\, 2nm,\, n^2 + m^2)$이 원시 피타고라스 세 쌍을 정의해줌은 매우 잘 알려진 사실이다 [20].

디오판투스는 이미 알고 있는 유리수해로부터 다른 해를 구하기 위해서 나름의 방법을 사

2) 이 문제 옆의 여백에 페르마가 그의 마지막 정리를 적어 놓았다는 것은 유명한 사실이다

3) Diophantus는 다음과 같이 설명했다고 한다 [4]. "I form the square from any number of x minus as many units as there are in the side of 16, and let it be $2x - 4$."

용하였다. 8번 문제에서 디오판투스가 고려한 일차식은 점 $(0,\,-4)$를 지나는 직선의 식이다. 실제로 음수를 사용하고 해석기하를 이해하고 있는 우리는 $(0,\,-4)$나 $(0,\,4)$ 중 어떤 점을 이용하더라도 문제가 똑같이 해결될 수 있음을 알고 있다. 그러나 기하적인 해석을 배제하고 디오판투스의 풀이를 이해해보기로 하자. 먼저 주어진 두 개의 미지수를 갖는 부정방정식을 미지수가 한 개인 이차방정식으로 바꾸기 위해 $y = kx \pm c$로 두는 것으로 시작한다. 이 식을 $x^2 + y^2 = 16$에 대입하여 $x = 0$ 외의 다른 한 근을 구하려면 $c^2 = 16$이어야 하므로 $c = 4$이다. 양수만을 다루고 있음을 기억하자. $y = kx + 4$를 이용할 경우, 양수 k로는 디오판투스가 원하는 양의 해를 구할 수 없다. 그러나 4를 뺀 식 $y = kx - 4$를 이용하면 양수 k에 따라 양의 유리해 $(x,\,y)$를 구할 수 있다.

《Arithmetica》의 제4권은 3차 이상의 부정방정식을 다룬다. 제4권 24번 문제[4]는

$$x(a - x) = y^3 - y, \quad a = 6$$

이고 눈에 보이는 해는 $(0,\,1)$이다. 디오판투스는 $y = kx - 1$을 이용하여 해를 구했는데, 이때는 앞의 2차곡선의 경우와는 다르게 k는 임의의 수일 수는 없다. 디오판투스는 $a = 6$일 때 $k = 3$으로 두고 유리수해 $x = 26/27$, $y = 17/9$를 구할 수 있었다.

제4권 18번 문제는

$$x^3 - 3x^2 + 3x + 1 = y^2$$

이고 뻔한 해는 $(0,\,1)$이다. $y = \frac{3}{2}x + 1$을 대입하여 해 $x = 21/4$, $y = 71/8$를 구하였다.

위의 두 문제에서 디오판투스가 풀이에 사용한 1차식은 주어진 곡선의 점 $(0,\,1)$에서의 접선의 식이다. 지금은 접선을 이용하여 접점이 아닌 다른 교점을 구하는 이 방법을 「접선방법」이라고 부른다. 그러나 접선의 기울기를 알기 위하여 미적분학을 알 필요는 없다. 디오판투스는 해석기하학도 미분적분학도 알지 못했다. 1차식을 3차식에 대입하여 나온 x에 관한 다항식에서 $x = 0$이 중근이면 그 1차식이 $x = 0$에서 곡선과 접하므로 3차식에서 일차항 x의 계수가 0이 되도록 k를 정하면 된다. 즉, 디오판투스의 아이디어는 주어진 3차식을 $x^3 = cx^2$의 형태로 바꾸는 것이었다고 추정된다.

디오판투스는 《Arithmetica》의 제4권 26번과 27번에서 먼 훗날 「현 방법」이라고 불리게 된 방법을 사용하였다. 26번 문제는

$$8x^3 + x^2 - 8x - 1 = y^3$$

이고, 그는 $y = 2x - 1$을 대입하여 유리수해 $x = 14/13$, $y = 15/13$을 구하였다.

참고로, 위 문제에서 1차식은 곡선의 접선의 식이 아니다. $y = 2x - 1$을 대입함으로써 주어진 식을 $x^2 = cx$의 형태가 되게 한 것이다. 직선과 곡선은 아핀평면 위의 점 $(0,\,-1)$을 공유할 뿐 아니라 사영평면 위의 무한원점 $[1,\,2,\,0]$을 공유한다. 즉 사영평면에서 직선은 곡선

4) "주어진 수를 두 개로 나누어 나뉘어진 두 수의 곱이 어떤 수의 세제곱과 그 수의 차와 같게 하여라(To divide a given number into two numbers such that their product is cube minus its side.)" [3]

위의 두 점을 지나는 현이고, 이 현은 3차곡선과 한 점을 더 공유한다. 이것이 현 방법이다. 접선은 이미 곡선과 한 점을 두 번 중복하여 공유하므로 접선과 곡선은 접점 외의 한 점에서 더 만난다. 이와 같이 복소사영공간에서 직선과 3차곡선이 세 점에서 만난다는 베주의 정리를 이용하여 다른 유리점을 찾는 작도에 의한 방법을 「현-접선 방법」으로 부른다. 디오판투스의 현-접선 방법은 페르마에 의해 자세히 연구되었고, 해석기하학의 도움으로 뉴턴이 디오판투스의 대수적인 풀이 방법을 기하학적으로 해석하고 온전한 이해에 이르게 된다 [22].

위의 24번 문제는 초기역사의 타원곡선 관련 문제로 종종 언급되는 것으로서, 식 $6x - x^2 = y^3 - y$에서 $x - 3 = Y$, $-y = X$로 두면 주어진 식은 타원곡선의 식 $Y^2 = X^3 - X + 9$로 변환된다. 즉, 앞의 식의 유리수해를 구하는 문제는 타원곡선의 유리점을 찾는 문제로 바뀐다.

3.2 합동수 문제

타원곡선의 오랜 역사에서 발견되는 3차방정식과 관련된 문제로 디오판투스의 방정식 외에 합동수 문제가 있다.

합동수

양의 정수 n이 「합동수(congruent number)」라 함은 세 변의 길이가 유리수이고 넓이가 n인 직각삼각형이 존재함을 말한다. 즉, 적당한 유리수 $a, b, c > 0$가 존재해서 $a^2 + b^2 = c^2$, $\frac{ab}{2} = n$을 만족시키면 n이 합동수이다. 이때 세 개의 수 $\frac{b-a}{2}$, $\frac{c}{2}$, $\frac{b+a}{2}$를 각각 제곱하면 이들은 공차가 n인 3항 등차수열을 이룬다. 반대로, 적당한 유리수 r, s, t가 $s^2 = r^2 - n$, $t^2 = r^2 + n$을 만족시키면, $a = t - s, b = t + s, c = 2r$는 넓이가 n인 직각삼각형의 세 변의 길이가 된다. 그러므로, 적당한 x에 대하여 $x^2 - n$, x^2, $x^2 + n$이 각각 유리수의 제곱이라는 것과 세 변을 유리수로 하고 넓이가 n인 직각삼각형이 존재한다는 것은 동치명제이다.

합동수에 대한 위의 두 명제가 동치라는 사실과 합동수를 결정하는 문제는 10세기경 아랍의 al-Khazin에 의해 다루어졌고, 34개의 합동수들의 표가 기록된 문서가 아랍에서 발견되기도 하였다 [18]. 17세기에 이르러 페르마는 합동수에 관한 연구로부터 페르마의 마지막 정리를 제시하게 되었고 [9], 그 정리는 실제로 300년 정도가 흐른 후에야 와일즈에 의해서 증명되었지만, "주어진 양의 정수가 합동수인지 아닌지를 유한번의 단계로 결정하는 알고리즘이 있겠는가?"를 묻는 합동수 문제는 아직까지 해결되지 않고 있다. 그러나 이에 대한 부분적인 답으로 n이 합동수이기 위한 필요조건을 1983년에 터넬(Tunnell)이 제시하였고, BSD 추측이 참임을 가정하면 충분조건도 성립되어 합동수 문제는 완전히 해결된다. 터넬은 자신의 정리의 증명을 위해 합동수 문제를 타원곡선 문제로 바꾸어 접근하였다 [26].

피보나치

13세기경 피보나치는 로마 황제 프레드릭 2세 앞에서 수학 문제로 도전받게 되었는데, 그

문제는 r^2-5와 r^2+5가 모두 유리수의 제곱이 되도록 하는 유리수 r이 무엇인지를 묻는 것이었다. 이 문제는 결국 5가 합동수인지를 묻는 것이었다. 피보나치는 $r=41/12$임을 알아내었다 [8].

합동수란 용어의 유래는 1225년에 출판된 피보나치의 책《Liber Quadratorum(Book of Squares)》에서 발견된다 [10]. 피보나치는 적당한 정수 x에 대하여 $x^2\pm n$이 제곱수일 때 정수 n을「congruum」이라고 불렀다. congruum과 congruence의 어원은 라틴어「congruere (to meet together)」로서 세 개의 제곱수가 공통의 차이를 갖는다는 뜻을 담고 있다. 즉, x^2-n, x^2, x^2+n은 제곱수의 3항 등차수열을 이룬다는 뜻이다.

이제 합동수와 타원곡선의 관련성을 알아보자. 합동수 n에 대하여 r^2-n, r^2, r^2+n은 유리수의 제곱이므로 이들을 곱한 수도 유리수의 제곱 s^2이다. 즉, $(r^2,\, s)$는 타원곡선 $y^2=x^3-n^2x$ 위의 유리점이다. 사실, n이 합동수이기 위한 필요충분조건은 타원곡선 $y^2=x^3-n^2x$ 위에 유리점이 무한히 많이 존재한다는 것이다. 실제로, 이렇게 정의되는 타원곡선 위의 $y\neq 0$인 유리점은 군의 원소로서 무한 위수를 갖는다 [10, 27]. 다시 말해서, n을 넓이로 갖는 유리 직각삼각형이 한 개 있으면 무한히 많이 있다는 뜻이고, 또한 n을 공차로 하는 세 개의 유리 제곱수의 수열이 한 개 있으면 이런 수열이 무한히 많이 있음을 뜻한다.

Arithmetica

16세기에 디오판투스의《Arithmetica》가 유럽에서 재발견되었다. 봄벨리 (Bombelli)가 그의 책《Algebra》(1572)에《Arithmetica》의 문제 143개를 수록하였고, 1575년에 스스로를 자일랜더 (Xylander)라고 불렀던 홀츠만 (Holtzmann)이 그리스어로 된 6권의《Arithmetica》를 라틴어로 번역하였고, 이어서 1621년에 바쉐 (Bachet de Meziriac)가 주석과 문제들을 첨가하여 라틴어로 번역하여 출판하였다. 후일 페르마가 바쉐의 번역서를 읽고 정수론의 발전에 영향을 미치게 된다 [4, 18].

바쉐의 번역서의 부록에는 피보나치의 합동수 문제와 방정식 $y^2=x^3+c$ (c는 정수)에 대하여 $(x,\, y)$가 유리수해이면

$$\left(\frac{x^4-8cx}{4y^2},\, \frac{-x^6-20cx^3+8c^2}{8y^3}\right)$$

도 유리수해라는 내용이 포함되어 있다 [16, 23]. 바쉐의 방정식은 훗날 모델 (Mordell)이 오랜 기간 관심을 가지고 자세히 연구하여, 1920년에 이 방정식이 단지 유한개의 정수해만을 가짐을 보였다 [10]. 유리수해가 무한히 많은지 아닌지는 c의 값에 따라 달라진다. 바쉐의 방정식은 모델의 방정식으로도 불린다.

페르마

직업 법률가였던 페르마는 디오판투스 이후에 정수론 분야에서 중요한 발전을 일구어낸 아마추어 수학자이다. 그는 바쉐가 번역한《Arithmetica》를 1630년경에 접하게 된 후에 그

내용을 연구하고 확장함으로써 정수론을 수학의 한 분야로 정립하는 데 중요한 역할을 하였다. 페르마는 많은 정리를 만들어냈고, 그 중에 너무도 유명한 정리인『$n > 2$일 때 $x^n + y^n = z^n$은 $xyz \neq 0$인 정수해를 갖지 않는다.』는 마지막 정리가 있다. 이 정리에 대하여 페르마는 $n = 4$인 경우에 대하여만 증명을 하였고, 일반적인 경우에 대한 증명은 1994년에 와일즈와 테일러가 타원곡선을 이용하여 완성하였다. 페르마는 바쉐의 방정식을 연구하여 $y^2 = x^3 - 2$의 정수해는 $(3, \pm 5)$뿐이고, $y^2 = x^3 - 4$의 정수해는 $(2, \pm 2), (5, \pm 11)$뿐이라고 추측하는 등, 특정한 타원곡선의 정수점들을 찾는 데도 관심을 보였다 [16].

합동수를 판별하는 문제는 페르마의 마지막 정리와 깊은 관련을 갖는다. n이 합동수인지를 판별하는 과정에서 n이 제곱수, 즉 $n = k^2$이면 직각삼각형의 각 변의 길이를 k로 나누어 넓이가 1이 되게 만들 수 있다. 따라서 합동수 문제에서는 1과 제곱수가 아닌 수만을 대상으로 한다. 페르마는 1이, 더불어 모든 제곱수가, 합동수가 아님을 페르마 자신이「무한하강법(infinite descent method)」이라고 명명한 방법으로 증명할 수 있었다 [8, 9]. 또한 이로부터 방정식 $x^4 + y^4 = z^4$이 $xyz \neq 0$인 정수해를 갖지 않음을 보일 수 있다.

정리 (Fermat, 1640). 1은 합동수가 아니다. 즉, 제곱수는 합동수가 아니다.

증명. 이 증명은 무한하강법을 사용한다. 제곱수를 넓이로 갖는 원시직각삼각형 (a, b, c)에 대하여 서로소인 두 정수 m, n이 존재해서, $a = n^2 - m^2, b = 2nm, c = n^2 + m^2$으로 나타난다. 삼각형의 넓이 $nm(n+m)(n-m)$은 제곱수이고 여기 포함된 4개의 항은 쌍별로 서로소이므로 $n = x^2, m = y^2, n + m = u^2, n - m = v^2$으로 쓸 수 있다. 여기서 u와 v는 서로소이고 홀수이다. $2y^2 = (u + v)(u - v)$이고 $\gcd(u + v, u - v) = 2$이므로, $u + v$와 $u - v$의 둘 중 하나는 $2r^2$, 다른 하나는 $4s^2$의 형태로 표현된다. 그래서 $x^2 = n = \frac{1}{2}(u^2 + v^2) = r^4 + 4s^2$이다. 이제 $c' = x, a' = r^2, b' = 2s^2$은 넓이가 제곱수 $r^2 s^2$이고 $c' = x < c = x^4 + y^4$으로 처음의 직각삼각형보다 작은 직각삼각형이다. 각 변을 최대공약수로 나누면 처음에 주어진 것보다 작은 원시직각삼각형이 생긴다. 이러한 과정을 무한히 반복할 수 있는데, 이것은 양의 정수 집합에서는 불가능하다. □

따름정리. 방정식 $x^4 - y^4 = z^4$은 $xyz \neq 0$인 정수해를 갖지 않는다.

증명. $x^4 - y^4 = z^2$이 정수해 x, y, z (단, $xyz \neq 0$)를 가지면 (y^2, z, x^2)은 피타고라스 세 쌍이므로, 적당한 정수 p, q에 대하여 $x^2 = p^2 + q^2, y^2 = p^2 - q^2$이다. 그러면

$$\frac{p^2}{q^2} + 1 = \left(\frac{x}{q}\right)^2, \quad \frac{p^2}{q^2} - 1 = \left(\frac{y}{q}\right)^2$$

인데, 이는 1이 합동수임을 뜻한다. 모순이다. □

위의 두 정리를 조금 상세히 들여다보면 1이 합동수가 아니라는 것과 방정식 $x^4 - y^4 = z^2$이 $xyz \neq 0$인 해를 갖지 않는다는 것은 동치임을 금방 알 수 있다. 또한 이 정리로부터 방정식

$x^4+y^4=z^4$이 $xyz\neq 0$인 정수해를 갖지 않음을 쉽게 알 수 있다. 페르마는 Bachet의 번역서 《Arithmetica》의 여백에서 유명한 페르마의 마지막 정리를 언급하고 있지만, 그 외의 그가 기록한 메모나 편지 어떤 곳에서도 마지막 정리에 대한 더 이상의 언급은 발견되지 않는다고 한다 [13].

그런데 $n=4$인 경우의 페르마의 마지막 정리는 타원곡선에 관한 내용을 담고 있다. $x^4+y^4=z^4$에서 식을 z^4로 나누고 $X=\frac{x}{z}$, $Y=\frac{y}{z}$로 두면 $Y^4=1-X^4$은 $XY\neq 0$인 유리수해를 갖지 않는다. 그래서 Y^2을 Y로 바꾼 방정식 $Y^2=1-X^4$의 유리수해는 $(\pm 1,\,0)$, $(0,\,\pm 1)$뿐임을 알 수 있다. $x=\frac{1}{1-X}$, $y=\frac{Y}{(1-X)^2}$로 두면 $Y^2=1-X^4$은 3차 방정식 $y^2=4x^3-6x^2+4x-1$로 변환되고, 여기서 다시 $v=4y$, $u=4x-2$로 두면 타원곡선 $v^2=u^3+4u$로 변환된다. 그리고 이 타원곡선은 유한개의 유리점만을 포함한다.

오일러

1730년대에 오일러는 페르마의 훌륭한 수학적 성과들을 볼 수 있었고, 페르마가 증명하지 않고 남겨둔 대부분의 정리들을 증명함으로써 정수론을 한층 발전시켰다 [7, 16]. 오일러는 합동수 문제에 대하여 상당한 연구를 진행하였는데, 『8로 나눈 나머지가 5, 6, 7이면서 제곱수가 아닌 양의 정수는 합동수임』을 추측하였다. 스페판스는 1975년에 BSD 추측이 참임을 가정하면 오일러의 추측도 참임을 보일 수 있었다 [21].

또한, 오일러는 3차 다항식 $f(x)$에 대하여 $y^2=f(x)$로 정의된 곡선의 유리점들이 매개변수를 이용한 유리함수로 표현되기 위하여 $f(x)$가 중근을 가져야 한다는 사실을 알아내었다. 뿐만 아니라 타원곡선 위의 두 유리점을 지나는 직선을 이용하여 다른 유리점을 얻는 현방법을 적용하기도 하였다 [4]. 오일러는 타원적분에 관한 중요한 정리들을 증명할 수 있었는데 타원적분에 관한 내용은 4절에서 다루기로 한다.

뉴턴

1670년대에 뉴턴은 당시 새로 생겨난 해석기하학의 도움으로 3차 곡선을 상세히 조사하여 디오판투스나 페르마가 디오판투스 방정식의 유리수해를 찾는 방법이 근본적으로 현-접선 작도법임을 기하학적으로 설명할 수 있었고, 1695년에는 3차곡선을 5가지 종류로 완전히 분류하였다. 뉴턴은 모든 3차곡선은 사영적으로 $y^2=x^3+ax^2+bx+c$와 같은 형태임을 설명하였는데, 이것은 근본적으로 모든 원추곡선은 사영적으로 원과 동형이라는 사실과 비교되는 내용이다 [16, 22, 23]. 19세기에 이르러 뉴턴이 분류한 5종류의 3차곡선은 복소사영공간에서 3가지 종류로 분류되고, 그 중의 한 종류인 특이점이 없는 3차곡선이 바로 타원곡선이다. 다른 두 종류의 3차곡선은 특이점을 각각 한 개씩 갖는 곡선으로 유리함수로 매개변수표현을 할 수 있다.

뉴턴의 현-접선 작도법은 궁극적으로 타원곡선 위의 점들을 「더하는」 일반적인 공식을

유도가능하게 하였다.

4 타원곡선의 역사: 복소해석학

4.1 타원적분

베르누이의 렘니스케이트 곡선과 오일러의 합의 공식

적분학의 발달 초기에 수학자들은 다항식의 제곱근을 유리화하는 문제에 부딪히게 된다. 예를 들어 원의 넓이를 구하려면 $\sqrt{1-x^2}$이 포함된 적분을 계산해야 한다. 디오판투스가 원 위의 유리점을 구하는 방법으로 얻은 결과인 $x = \frac{1-t^2}{1+t^2}$을 대입하면 $\sqrt{1-x^2}$은 유리함수로 표현된다. 그러나 중근을 갖지 않는 3차 또는 4차 다항식의 제곱근이 포함된 적분은 유리함수로 표현되지 않는다.

케플러가 제2법칙으로 제시한 타원 궤도를 따라 행성이 움직이는 거리에 대한 설명은 수학자들에게 타원의 호의 길이 문제에 대한 관심을 불러일으켰다. 타원 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$의 호의 길이를 구하기 위한 적분 $\int_0^{\frac{\pi}{2}} \sqrt{a^2\cos^2 t + b^2 \sin^2 t}\, dt$ 에서 $u = \sin t$로 두면 앞의 적분은

$$a\int_0^1 \frac{1-k^2u^2}{\sqrt{(1-u^2)(1-k^2u^2)}}\, du$$

의 형태로 변한다. 이와 같이 중근을 갖지 않는 3차 또는 4차 다항식 $p(x)$와 유리함수 $R(u,\, v)$에 대하여 $\int R(t, \sqrt{p(t)})dt$의 형태로 주어지는 적분을 「타원적분」이라고 부른다.

제이콥 베르누이는 $(x^2+y^2)^2 = x^2 - y^2$으로 표현되는 렘니스케이트 곡선의 길이를 구하는 적분에 포함되는 $\sqrt{1-x^4}$을 유리함수로 바꿀 수 없음을 짐작하였다. 만약 이것이 가능하다면 $a^4 \pm b^4 = c^2$이 $abc \neq 0$인 정수해를 가질 것이고 이는 페르마의 정리에 모순되기 때문이다 [22]. 실제로 1694년에 베르누이가 타원적분은 다항함수, 유리함수, 삼각함수, 지수함수, 로그함수 등의 초등함수를 이용한 계산이 불가능함을 추측하였고, 1833년에 이를 리우빌(Liouville)이 증명하였다 [23]. 베르누이의 렘니스케이트 적분 $\int \frac{dt}{\sqrt{1-t^4}}$로부터 타원적분과 타원함수가 발전된다.

1714년에 이태리 수학자 파그나노(Fagnano)는 $v = 2u\sqrt{1-u^4}/(1+u^4)$이면 식

$$2\int_0^u \frac{dt}{\sqrt{1-t^4}} = \int_0^v \frac{dt}{\sqrt{1-t^4}}$$

이 성립함을 보였는데, 이 사실은 렘니스케이트 적분이 초등함수로 해결되지 않음에도 불구하고 호길이를 구하기 위한 적분의 구간을 나타내는 변수 사이에 대수적인 관계가 있음을 보여주는 것이었다.

1751년에 렘니스케이트 2배 공식을 접하게 된 오일러는

$$\int_0^x \frac{dt}{\sqrt{1-t^4}} + \int_0^y \frac{dt}{\sqrt{1-t^4}} = \int_0^{(x\sqrt{1-y^4}+y\sqrt{1-x^4})/(1+x^2y^2)} \frac{dt}{\sqrt{1-t^4}}$$

로, 이어서 1768년에는 4차다항식 $p(t)=(1-t^2)(1-k^2t^2)$에 대하여 $\int \frac{dt}{\sqrt{p(t)}}$로 주어진 타원적분의 합의 공식으로 일반화하였다. 파그나노의 공식과 오일러의 합의 공식의 증명은 [19] 또는 [25]에서 찾아볼 수 있다.

타원적분 $\int R(t,\sqrt{p(t)})dt$는 위의 오일러 타입 외에도 두 가지 종류가 더 있다. 타원 적분을 세 가지 타입으로 분류하고 각각의 경우에 대한 합의 공식을 제시하여 타원적분을 체계화한 사람은 르장드르였지만, 곧바로 아벨과 쟈코비에 의해 타원함수가 다루어짐으로써 르장드르의 업적은 잊히게 된다 [6,16].

4.2 타원함수

가우스, 아벨, 쟈코비, 아이젠스타인, 바이어슈트라스

1790년대에 가우스는 렘니스케이트 적분의 역함수를 렘니스케이트 사인으로 부르고 이것이 복소수 상에서 두 개의 주기를 갖는 함수임을 밝혔지만, 결과를 발표하지는 않았다. 1820년대에 두 적분 $\int_0^x \frac{dt}{\sqrt{1-t^2}}$와 $\int_0^x \frac{dt}{\sqrt{1-t^4}}$의 유사성에 주목하여 아벨과 자코비는 타원적분의 역함수를 살펴보고 중요 성질들을 밝혀낼 수 있었다. 적분 $\int_0^x \frac{dt}{\sqrt{1-t^2}}$는 x의 함수로 무한히 많은 값을 갖는 다중함수이고, 그 역함수는 사인함수 $x=\sin u$로 주기함수이고 다양한 합의 공식을 만족시킨다. 아벨과 자코비는 각각 「타원함수」로 부르는 일반적인 타원적분의 역함수를 연구하여, 타원함수가 두 개의 주기를 갖는 복소변수함수라는 사실을 보였고, 타원함수에 관한 합의 공식을 유도해내었다 [2,6,15].

자코비는 1835년에 3차방정식의 유리수해를 구하는 디오판투스의 방법과 오일러의 타원적분의 합의 공식간의 관련성을 발견하였다. 예를 들어, 타원적분에 대한 합의 공식

$$m_1\int_0^{x_1}\frac{dt}{\sqrt{p(t)}}+m_2\int_0^{x_2}\frac{dt}{\sqrt{p(t)}}=\int_0^{x_3}\frac{dt}{\sqrt{p(t)}}$$

가 적당한 정수 m_1, m_2와 유리수 $x_1, x_2, y_1=\sqrt{p(x_1)}, y_2=\sqrt{p(x_2)}$에 대하여 성립하면, x_3과 $y_3=\sqrt{p(x_3)}$은 x_1, x_2, y_1, y_2의 유리함수로 표현된다고 기술하였는데, 이것은 합의 공식을 이용하여 타원곡선 $y^2=p(x)$ 위의 유리점들을 무한히 찾을 수 있음을 의미한다. 자코비가 한 일은 근본적으로는 타원곡선 위의 점들의 대수구조를 살펴본 것이지만, 자코비 또는 당시의 어느 수학자도 타원곡선 위의 점들 사이의 연산을 고려하지는 않았다 [4].

아이젠스타인은 1847년에 두 개의 주기 $\omega_1, \omega_2\in\mathbb{C}$를 갖는 무한급수로

$$\sum_{m,\,n\in\mathbb{Z}}\frac{1}{(z+m\omega_1+n\omega_2)^2}$$

을 제시하였다 [23]. 현대에는 이 함수처럼 두 개의 주기 $\omega_1, \omega_2\in\mathbb{C}, \omega_1/\omega_2\notin\mathbb{R}$를 갖는 복소수 상에 정의된 meromorphic 함수를 「타원함수」로 정의한다. 즉, 타원함수 g는 $g(z+\omega_1)=g(z+\omega_2)=g(z)$를 만족시킨다. 더 나아가 아이젠스타인은 다음과 같은 형태의

타원함수

$$g(z) = \sum_{m,\, n\in\mathbb{Z}} \frac{1}{(z + m\omega_1 + n\omega_2)^2} - \sum_{m,\, n\in\mathbb{Z},\ (m,\, n)\neq(0,\, 0)} \frac{1}{(m\omega_1 + n\omega_2)^2}$$

은 서로 다른 세 근을 갖는 3차다항식 p에 대하여 식 $(g'(z))^2 = p(g(z))$를 만족시킴을 보였다 [16].

이 결과는 타원함수 $(g(z),\, g'(z))$가 타원곡선 $y^2 = p(x)$의 매개변수표현임을 말해주는 것으로서, 아이젠스타인에 의해서 해석학 분야에서 다루어지는 타원함수와 정수론 분야에서 연구되어 오던 타원곡선 사이에 존재하는 특별한 관련성이 드러나게 되었다는 중요한 의미를 갖는다. 그러나, 타원곡선을 매개변수화하는 데 타원함수를 처음으로 이용했던 사람은 클렙쉬 (Clebsch) 였다 (1864) [23].

1863년에 저명한 해석학자인 바이어슈트라스가 아이젠스타인의 함수와 유사하면서 가장 기본적인 타원함수인 바이어슈트라스 $\wp$-함수

$$\wp(z) = \frac{1}{z^2} + \sum_{(m,\, n)\neq(0,\, 0)} \left(\frac{1}{(z + m\omega_1 + n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right)$$

을 정의하고, 함수 $x = \wp(z)$가 식

$$\wp'(z)^2 = 4\wp^3(z) - g_2\wp(z) - g_3$$

을 만족시킴을 보였다. 여기서,

$$g_2 = 60 \sum_{(m,\, n)\neq(0,\, 0)} \frac{1}{(m\omega_1 + n\omega_2)^4}, \quad g_3 = 140 \sum_{(m,\, n)\neq(0,\, 0)} \frac{1}{(m\omega_1 + n\omega_2)^6}$$

이다 [15, 23–25].

이는 바이어슈트라스 $\wp$-함수가 타원적분

$$z = \int_0^x \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}}$$

의 역함수이고, 타원함수 $(\wp(z),\, \wp'(z))$가 $y^2 = 4x^3 - g_2 x - g_3$으로 정의되는 타원곡선의 매개변수표현임을 의미한다. 즉, 주어진 타원곡선을 $y^2 = 4x^3 - g_2 x - g_3$의 형태가 되도록 적당히 변수변환을 하면 바이어슈트라스 $\wp$-함수를 이용해 매개화할 수 있다. 실제로, 바이어슈트라스 $\wp$-함수는 정수 m, n에 대하여 $z = m\omega_1 + n\omega_2$ 일때만 pole을 갖고 주기가 ω_1, ω_2인 meromorphic 함수이다.

일반적으로, 타원곡선 $y^2 = p(x)$에 대하여 $z = g^{-1}(x) = \int_0^x \frac{dt}{\sqrt{p(t)}}$로 두면, $x = g(z)$는 타원함수이고

$$g'(z) = \frac{dx}{dz} = \frac{1}{\frac{dz}{dx}} = \sqrt{p(x)} = y$$

이므로 $z \mapsto (g(z),\, g'(z))$가 타원곡선 $y^2 = p(x)$의 매개변수표시가 된다.

4.3 타원곡선 이론

푸앵카레

1670년대에 뉴턴이 3차곡선을 자세히 연구하고 분류하였고, 1847년에 자코비가 3차곡선과 타원함수와의 관련성에 주목하였으며, 아이젠스타인이 1864년에 그 관련성을 분명하게 증명하였다. 클렙쉬는 타원함수를 3차곡선의 매개변수표현에 이용하는 아이디어를 제시하였고 바이어스타라쓰가 타원함수의 합의 공식과 디오판투스의 현-접선 방법 간의 관련성을 보였다. 1800년대 후반에 복소해석학이 발전하면서 정수론과 타원함수론 분야에서 다루어지던 타원곡선 관련 내용이 종합적으로 이해되었고, 이전의 연구 결과들을 종합한 것을 토대로 푸앵카레가 1901년에 「On the arithmetic properties of algebraic curves」라는 제목의 논문을 발표하면서 타원곡선 이론이 생겨났다 [16].

푸앵카레는 적분에 대한 성질 대신 곡선의 기하적인 성질을 고려하여 복소사영공간상의 타원곡선과 타원함수의 정의역에 해당하는 평행사변형 위의 점에 대한 합과 곱 등을 살펴보고, 유리수상의 타원곡선이 가환군임을 증명하였다. 또 타원곡선의 모든 유리점들을 생성할 수 있는 최소의 점의 개수를 타원곡선의 「계수(rank)」로 정의하고 계수가 유한할 것으로 추측하였다. 이 추측은 1922년에 모델에 의해서 증명되었다.

타원곡선의 덧셈

복소사영공간에서 타원곡선 $y^2 = x^3 + ax + b$ 위의 두 점 $P = (x_1, y_1)$, $Q = (x_2, y_2)$를 지나는 직선과 타원곡선은 또 다른 점 $R = (x_3, y_3)$에서 만난다. 직선의 기울기를 $r = \frac{y_1 - y_2}{x_1 - x_2}$라 하고, 직선의 식을 3차식에 대입하여 정리하면 세 개의 해가 x_1, x_2, x_3인 방정식을 얻는다. 2차항의 계수를 비교하면 $x_3 = r^2 - x_1 - x_2$와 $y_3 = r(x_3 - x_1) + y_1$을 얻는다. 이제 점들 간의 연산으로서 $P + Q = -R = (x_3, -y_3)$으로 정의한다. 두 점 P, Q가 같은 점이면, 그 점에서의 곡선의 접선을 이용하여 곡선과 접선의 다른 하나의 교점을 구할 수 있다. 이렇게 정의된 덧셈에 관한 항등원을 무한원점 $[0, 1, 0]$으로 하면 덧셈은 교환법칙과 결합법칙을 만족하여 복소수상의 타원곡선 $E(\mathbb{C})$는 덧셈군을 이룬다. 두 점이 유리점이면 다른 한 점도 유리점이므로 타원곡선 위의 유리점들의 집합 $E(\mathbb{Q})$는 $E(\mathbb{C})$의 부분군이다 [20].

타원곡선군, 원환면

두 개의 주기 $\omega_1, \omega_2 \in \mathbb{C}, \omega_1/\omega_2 \notin \mathbb{R}$를 갖는 타원함수 g를 생각해보자. $\langle \omega_1, \omega_2 \rangle$를 ω_1, ω_2에 의해 생성되는 $\mathbb{C}$의 부분군이라고 하면, $\mathbb{C}/\langle \omega_1, \omega_2 \rangle$는 상군(quotient group)이고, 이는 복소평면 $\mathbb{C}$ 위의 두 변을 ω_1, ω_2로 하는 평행사변형으로서 원환면(torus)과 위상동형이다. 그런데, 함수 $z \mapsto (g(z), g'(z))$는 $\mathbb{C}/\langle \omega_1, \omega_2 \rangle$에서 타원곡선으로의 일대일 대응이면서 연속으로 타원곡선도 위상적으로 원환면임을 알 수 있다.

한편, 복소수 z에 대하여 유리함수 $x = p(z), y = q(z)$로 매개변수표현이 되는 원추곡선은

위상적으로 구면이다. 3차곡선 $y^2 = p(x)$에 특이점이 존재하면 특이점의 x좌표는 $p(x)$의 중근에 해당하므로 베주의 정리에 의해 특이점은 한 개뿐이다. 특이점이 있는 3차곡선은, 원의 경우에서처럼, 유리함수로 매개변수 표현을 할 수 있다 [1]. 그래서 원추곡선뿐 아니라 특이점을 갖는 3차곡선은 모두 위상적으로 구면이다. 뉴턴이 분류한 다섯 종류의 3차곡선들 중에 복소사영공간에서 타원곡선으로 분류되는 특이점이 없는 곡선은 모두 원환면이고, 각 원환면은 두 개의 주기에 의해 결정된다.

푸앵카레가 타원곡선의 군의 구조를 발견한 것은 타원함수의 이해로부터 생겼을 것이다. 타원함수 $\Phi(z) = (\wp(z), \wp'(z))$로 매개변수표현이 되는 타원곡선은 가환군이다. $\Phi(z)$는 실제로 평행사변형 $\mathbb{C}/\langle\omega_1, \omega_2\rangle$와 타원곡선군 $E(\mathbb{C})$ 사이의 군동형사상이다. 이 함수를 좀 더 자세히 살펴봄으로써 우리는 앞에서 정의한 타원곡선의 덧셈을 이해할 수 있다.

세 변수 z_1, z_2, z_3가 군 $\mathbb{C}/\langle\omega_1, \omega_2\rangle$에서 $z_1+z_2+z_3 = 0 \pmod{\langle\omega_1, \omega_2\rangle}$을 만족시킨다고 하자. 세 변수에 대응하는 타원곡선 위의 세 점을 $P = (x_1, y_1) = \Phi(z_1)$, $Q = (x_2, y_2) = \Phi(z_2)$, $R = (x_3, y_3) = \Phi(z_3)$이라고 하자. 그러면

$$x_3 = \wp(z_3) = \wp(-z_1 - z_2) = \wp(z_1 + z_2),$$
$$y_3 = \wp'(z_3) = \wp'(-z_1 - z_2) = -\wp'(z_1 + z_2)$$

이므로[5], $-R = -\Phi(z_3) = \Phi(-z_3) = \Phi(z_1+z_2)$이다. 그래서 $P+Q = -R$로 타원곡선의 덧셈을 정의함으로써 $\Phi(z_1) + \Phi(z_2) = \Phi(z_1 + z_2)$가 되게 할 수 있다.

$p(t) = 4t^3 - g_2t - g_3$와 관계식 $z_k = \int_0^{x_k} \frac{dt}{\sqrt{p(t)}}$로부터 타원적분의 합의 공식은 $z_1 + z_2 + z_3 = 0$일 때

$$x_3 = \frac{1}{4}\left(\frac{\sqrt{p(x_1)} - \sqrt{p(x_2)}}{x_1 - x_2}\right)^2 - x_1 - x_2, \text{ 즉,}$$
$$\wp(z_3) = \wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2)$$

로 표현된다.

5 BSD 추측: 밀레니엄 문제

복소사영평면에서 타원곡선의 점들은 무한원점을 항등원으로 하고, 디오판투스의 현-접선 방법을 적용하여 덧셈을 정의하면, 타원곡선은 아벨군이다. 1992년에 모델(Mordell)은 푸앵카레가 추측했던 정리「타원곡선의 유리점들의 아벨군 $E(\mathbb{Q})$가 유한개의 원소에 의해 생성됨」을 증명하였다 [14]. 즉,

$$E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$$

이다. 여기서, r은 음이 아닌 정수이고 T는 유한군이다. r을 타원곡선 $E(\mathbb{Q})$의「계수(rank)」라고 부른다. 계수를 아는 것은 타원곡선에 속한 유리점이 얼마나 많은지를 아는 것과 같다.

5) 바이어슈트라스 $\wp$-함수는 $\wp(-z) = \wp(z)$, $\wp'(-z) = -\wp'(z)$를 만족시킨다.

예를 들어, 1은 합동수가 아니므로 $E:\ y^2 = x^3 - x$에는 오직 $y = 0$인 유리점만이 존재한다. 즉, $E(\mathbb{Q}) = \{(0,\,0), (1,\,0), (-1,\,0), \infty\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$이고 계수는 0이다. $r = 0$은 주어진 타원곡선이 유한개의 유리점만을 포함하고 있음을 뜻한다. 만약 어떤 유리점이 거듭해서 더해도 항등원이 되지 않으면 그 점은 무한히 많은 유리점을 생성하는데, 이 경우에 $r \geq 1$이 된다.

현재까지도 타원곡선 $E(\mathbb{Q})$의 계수를 결정하는 알고리즘은 알려져 있지 않고, 또 어떤 수가 계수로 가능한지도 정확히 알려지지 않았다 [17]. 2006년에 엘키즈(Elkies)가 28을 계수로 갖는 타원곡선을 제시한 결과가 현재 타원곡선의 계수로서 알려진 가장 큰 수이다[6]. 버치(Birch)와 스위너튼 다이어(Swinnerton-Dyer)는 아벨군 $E(\mathbb{Q})$를 군과 완전히 다른 무엇인가와 연관을 짓는데, 이와 관련된 내용이 바로 1965년에 제시된 BSD 추측(Birch and Swinnerton-Dyer conjecture)으로서 $E(\mathbb{Q})$의 크기를 알 수 있는 방법을 설명해준다 [1, 11, 27].

타원곡선 $y^2 = x^3 + ax + b$ (a, b는 정수)[7]에 대하여, 각 소수 p에 대하여 N_p를 방정식 $y^2 = x^3 + ax + b \pmod{p}$의 해의 개수라 하고, $p \nmid \Delta$이면 $a_p = p + 1 - N_p$로 놓고 $p \mid \Delta$이면 $a_p = p - N_p$로 놓아, 타원곡선 E의 L-함수를

$$L(E, s) = \prod_{p \mid \Delta} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p \nmid \Delta} \left(1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}\right)^{-1}$$

으로 정의하면 이것은 복소평면에서 해석함수로 확장가능하다. 그 함수를 $s = 1$에서 s에 대한 테일러급수로 표현하면

$$L(E, s) = c_k(s-1)^k + c_{k+1}(s-1)^{k+1} + \cdots$$

인데 ($k \geq 0, c_k \neq 0$), 이때 k를 타원곡선의 「해석적 계수」라고 한다. 「Birch and Swinnerton-Dyer 추측」은 『타원곡선의 대수적 계수 r과 해석적 계수 k가 같다.』는 것이다. 특히, $L(E, 1) = 0$이면 $k \geq 1$임을 의미하고 이는 타원곡선에 유리점이 무한히 많이 있음을 의미한다.

3세기경 디오판투스로부터 시작된 3차방정식의 유리해를 구하는 문제를 해석기학학의 도움으로 17세기 후반에 3차곡선의 유리점을 구하는 문제로 바꾸어 볼 수 있게 되었다. 뉴턴은 디오판투스의 대수적인 해법을 단순한 작도를 이용하여 유리점을 구하는 기하적인 방법으로 해석하였고, 현재 우리도 디오판투스의 현-접선 방법을 직관적으로 매우 쉽게 이해한다. 디오판투스의 현-접선 방법이 주어진 유리점으로부터 무한히 많은 다른 유리점들이 생성되는 것을 보장하는 듯하지만, 직선과의 교점으로 생기는 유리점이 매번 달라서 결국 타원곡선 위의 유리점이 무한히 많은 것인지, 실제 무한히 많더라도 그 무한의 크기가 얼마나 되는지에 대한 답은 한 동안 알 수 없었다. 푸앵카레가 1901년에 타원곡선의 유리점들의 집합 $E(\mathbb{Q})$

6) `http://web.math.pmf.unizg.hr/ duje/tors/tors.html` 참조.

7) $y^2 = x^3 + ax + b$의 계수 a, b가 유리수이면 간단한 사영변환으로 계수를 정수로 바꿀 수 있다.

가 아벨군임을 보이고, 이어서 모델이 1922년에 아벨군 $E(\mathbb{Q})$가 유한개의 원소로 생성됨을 증명한 후에야 $E(\mathbb{Q})$를 개략적으로 파악할 수 있게 되었다.

그러나 특정 타원곡선에 대한 $E(\mathbb{Q})$를 알기엔 여전히 부족하다. 생성원이 구체적으로 몇 개이고 생성원이 무엇인지를 아는 것이 $E(\mathbb{Q})$를 정확히 아는 것이고, 디오판투스의 3차방정식을 푸는 일일 것이다. 유한 위수를 갖는 원소들만으로 이루어진 $E(\mathbb{Q})$의 부분군(torsion subgroup)은 15종류로 마주르(Mazur)에 의해 완벽하게 분류되었고(1978) [20], $E(\mathbb{Q})$의 계수를 알 수 있는 방법으로 제시된 명제가 바로 BSD 추측이다. 타원곡선의 계수들의 평균이 0.89보다 작고, 더 나아가 계수가 0인 곡선, 다시 말해서 유한개의 유리점만으로 이루어진 $E(\mathbb{Q})$가 전체의 $1/5$ 이상임이 바르가바(Bhargava)[8]에 의해 밝혀졌다 [5].

6 결론

우리는 위에서 타원곡선의 역사를 개괄적으로 살펴보았다. 타원곡선은 고대 그리스 시대로부터 시작되는 매우 긴 역사를 가지고 있다. 타원곡선은 특히 한편으로 방정식의 유리수해를 구하거나 합동수를 판단하는 정수론 문제뿐만 아니라, 타원의 호길이를 구하는 적분문제로부터 시작되는 복소해석학 분야의 역사도 가지고 있음을 보았다. 서로 상관없어 보이는 두 줄기를 따른 수학 내용이었지만, 자코비와 바이어슈트라스에 의해서 그 관련성이 조금씩 드러나기 시작하였고 결국 푸앵카레에 의해서 20세기 초에 타원곡선이론이라는 하나의 수학 이론으로 자리매김하게 되었음을 보았다. 양 줄기를 따른 타원곡선의 역사를 하나로 연결해주는 열쇠는 근본적으로 오일러, 아벨, 자코비 등이 유도한 타원적분의 합의 공식에 감추어져 있었다. 합의 공식은 타원함수의 중요하고 특징적인 성질로 타원곡선의 군의 구조를 암시한 것으로 푸앵카레에 의해 밝혀졌다.

리만은 복소사영평면에서 대수곡선을 종수(genus)에 따라 분류하였다. 앞에서 타원곡선은 원환면으로 종수가 1임을 보았다. 일반적으로 초타원곡선 $y^2 = p(x)$에서 서로 다른 n개의 근을 갖는 다항식 $p(x)$의 차수 n이 곡선의 종수를 결정하는데, 종수 g는 $\frac{n-1}{2}$을 넘지 않은 최대 정수와 같다. 종수가 0인 곡선은 유리점을 포함하지 않거나 무한히 많이 포함한다. 종수가 2 이상인 곡선은 유한개의 유리점을 포함할 뿐이다. BSD 추측은 종수가 1인 곡선의 유리점의 개수에 관한 내용을 담고 있는 것으로, 간단한 정수론 문제가 타원곡선의 군의 구조가 밝혀진 후 현대대수학과 복소해석학 등이 복잡하게 개입된 해석정수론 문제로 발전되어 생긴 것이다.

19세기에 타원함수에 대한 상세한 연구가 진행되면서 복소해석학, 기하학 등이 함께 발달되었다. 타원곡선은 수학의 여러 분야를 아우르며 발전을 이끌어낸 중요 문제로 그 가치가 매우 크다고 여겨진다. 특히, 유한체 상에 정의된 타원곡선군은 암호학에 중요하게 응용되는

8) 바르가바는 타원곡선과 BSD 추측에 관해 얻은 결과들로 2014년에 필즈상을 수상하였다.

등의 점이 그 연구가치를 한층 더 크게 한다.

References

1. A. Ash, R. Gross, *Elliptic Tales*, Princeton University Press, 2014.
2. M. Barnes, *Abel on Elliptic Integrals: A Translation*. http://www.maa.org/publications/periodicals/convergence/abel_on_elliptic_integrals_a_translation
3. M. Barsagade, S. Meshram, Overview of history of elliptic curves and its use in cryptography, *Int. Jour. of Scientific & Engineering Research*, 5(4) (2014), 467–470.
4. I. Bashmakova, Arithmetic of algebraic curves from Diophantus to Poincaré, *Historia Mathematica* 8 (1981), 393–416.
5. M. Bhargava, A. Shankar, The average size of the 5-Selmar group of elliptic curves is 6, and the average rank is less than 1, 2013. http://arxiv.org/pdf/1312.7859.pdf
6. U. Bottazzini, J. Gray, *Hidden Harmony- Geometric Fantasies: The Rise of Complex Function Theory*, Springer, 2013.
7. E. Brown, Three Fermat trails to elliptic curves, *The College Math. Jour.*, 31(3) (2000), MAA, 162–172.
8. V. Chandrasekar, The congruent number problem, *Resonance*(Aug. 1998), 33–45.
9. J. Coates, Congruent number problem, *Pure and Applied Mathematics Quarterly* 1(1) (2005), 14–27.
10. K. Conrad, The congruent number problem. http://www.math.uconn.edu/~kconrad
11. K. Devlin, *The Millenium Problems*, Basic Books, 2002.
12. G. Harder, D. Zagier, *The conjecture of Birch and Swinnerton-Dyer*. people.mpim-bonn.mpg.de/zagier/files/tex/BSDwHarder/fulltext.pdf
13. P. Hewitt, A brief history of elliptic curves, 2005. http://livetoad.org/Courses/Documents/132d/Notes/history_of_elliptic_curves.pdf
14. L. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Cambridge Philos. Soc.* 21 (1922), 179–192.
15. J. Nekovar, *Elliptic functions and elliptic curves* (lecture note). http://webusers.imj-prg.fr/~jan.nekovar/co/ln/el/el1.pdf
16. A. Rice, E. Brown, Why ellipses are not elliptic curves, *Math. Mag.* 85 (2012), 163–176
17. K. Rubin, A. Silverberg, Ranks of elliptic curves, *Bulletin of the AMS* 39(4) (2002), 455–474.
18. N. Schappacher, *Diophantus of Alexandria: a Text and its History*, 2005. http://www-irma.u-strasbg.fr/~schappa/NSch/Publications-files/Dioph.pdf
19. C. L. Siegel, Elliptic Functions and Uniformization Theory, *Topics in Complex Function Theory*, Volume I, Wiley-Interscience, 1988.
20. J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, UTM, Springer, 1992.
21. N. Stephens, Congruence properties of congruent numbers, *Bull. London Math. Soc.* 7 (1975), 182–184.
22. J. Stillwell, The evolution of elliptic curves, *Amer. Math. Monthly* 102(9) (1995), 831–837.
23. J. Stillwell, *Mathematics and Its History*, 3rd ed., Springer, 2010.

24. A. Sutherland, *Elliptic curves*, 2013. http://oct.mit.edu/courses/mathematics/\18-783-elliptic-curves-spring-2013/lecture-notes
25. V. Tkachev, *Elliptic functions: Introduction course* (lecture note). http://www.math.kth.se/~tkachev
26. J. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, *Inventiones Math.* 72 (1883), 323–334.
27. A. Wiles, The Birch and Swiinerton-Dyer conjecture, In James Carlson, Arthur Jaffe, Andrew Wiles, *The Millenium Prize Problems*, AMS, 2006, 31–44.