creative commons

COMMONS DEED

저작자표시-비영리 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:24011-200000237879

2009년 2월

教育學碩士(數學教育)學位論文

# 페르마의 마지막정리

- On Fermat's Last Theorem -

**朝鮮大學校 教育大學院**

數學教育專攻

**趙 亨 書**

# 페르마의 마지막정리

## - On Fermat's Last Theorem -

2009년 2월

**朝鮮大學校 敎育大學院**

數學敎育專攻

**趙 亨 書**

# 페르마의 마지막정리

- On Fermat's Last Theorem -

指導敎授　朴 順 喆

이 論文을 敎育學碩士(數學敎育)學位 請求論文으로 提出함.

2008년　10월

**朝鮮大學校 敎育大學院**

數學敎育專攻

**趙　亨　書**

**趙亨書의 敎育學 碩士學位 論文을 認准함.**

審査委員長　朝鮮大學校 敎授 _____印

審 査 委 員　朝鮮大學校 敎授 _____印

審 査 委 員　朝鮮大學校 敎授 _____印

2008년　12월

**朝鮮大學校 敎育大學院**

# 목 차

ABSTRACT

제 1장. 논문개요 1

제 2장. 페르마의 마지막 정리의 유래와 연구내용 ..... 2

1. 페르마의 마지막 정리의 유래 ..... 2

2. 페르마의 연구내용 ..... 4

제 3장. 페르마의 마지막정리를 다루는데 필요한 기본정의 ..... 7

1. 약수와 최대공약수 ..... 7

2. 소수 ..... 8

3. 합동 ..... 9

4. Euler의 $\varphi$ 함수 ..... 9

제 4장. 페르마의 마지막정리에 대한 구체적 경우의 증명 ..... 10

1. 지수가 2인 예외적 경우의 피타고라스 방정식 (( $X^2 + Y^2 = Z^2$ )) ..... 10

2. $n = 4$인 경우의 증명 (( $X^4 + Y^4 = Z^4$ )) ..... 13

3. $n = 3$인 경우의 증명 (( $X^3 + Y^3 = Z^3$ )) ..... 15

4. $n = 5$인 경우의 증명 (( $X^5 + Y^5 = Z^5$ )) ..... 24

5. $n = 6$인 경우의 증명 (( $X^6 + Y^6 = Z^6$ )) ..... 30

6. $n = 7$인 경우의 증명 (( $X^7 + Y^7 = Z^7$ )) ..... 31

제 5장. 페르마의 마지막 정리의 증명 도전사 ····· 38

1. Leonhard Euler (1707～1783 : 스위스) ····· 38

2. Marie-Sophie Germain (1776 ～1831 : 프랑스) ····· 38

3. Ernst Eduard Kummer (1810～1893 : 독일) ····· 38

4. Lewis Mordell (1888～1972 : 영국) ····· 39

5. Gerd Faltings (1954～ : 독일) ····· 39

6. Yutaka Taniyama(일본)와 G. Shimura(일본) ····· 40

7. Gerhard Frey(독일)과 K. Ribet(미국) ····· 40

8. Andrew Wiles (영국) ····· 40

제 6장. 결론 ····· 44

참고문헌 ····· 46

# Abstract

## On Fermat's Last Theorem

Hyoung-seo Cho.

Advisor : Prof. Park Soon-cheol Ph.D.
Major in Mathematics Education
Graduate School of Education, Chosun University

Fermat's Last Theorem is that the equation $x^n + y^n = z^n$ has no solution in natural numbers.

Fermat's Last Theorem is one of the most important theories in mathematics history to show that pure mathematics, Topology and Geometry are not the separated fields, but the one theoretical body and they are dependent on each other.

Especially the development Topology such as Taxonomic Theory gave mathematicians a whole mew motivation which they had never expected.

Even though the Fermat's Last Theorem was proved by Andrew Wiles using all the new theories as possible, it couldn't be proved without E. Kummer, L. Mordell of Y. Taniyama's studies.
However, it is true that the foundation of mathematics history has been prove by Andrew Wiles who proves it in 1993.

In this paper, we find out the process of building an mathematical product through the historical trace of Fermat's last theorem's birth and clarification. We also present the classical proof of the theorem in the case of $n=2$, $n=3$, $n=4$, $n=5$, $n=6$, $n=7$.

# 제 1장 논문개요

페르마의 마지막정리(Fermat's Last Theorem)는 수학자뿐만 아니라 일반인에게도 널리 알려진 수학 명제이다.

페르마의 마지막 정리:

"$n$이 2보다 큰 정수이면, 방정식 $X^n + Y^n = Z^n$을 만족하는 0이 아닌 정수 해 $X, Y, Z$은 존재하지 않는다."

페르마 본인은 이 문제를 해결했다고 주장했으나 자세한 풀이 과정은 어디에도 남기지 않았다. 이것은 17세기 전반기(1637년)에 등장한 이후 수많은 전문수학자와 아마추어 수학자의 도전으로 수학의 발전에 큰 기여를 했다. 수학사적 관점에서 보면 페르마의 마지막정리 증명문제는 현대 정수론의 기초를 확립하고, 현대대수학의 핵심개념의 하나인 ideal theory가 개척되었다는데 더 큰 성과라고 할 수 있다([12]).

본 논문에서는 페르마의 마지막 정리의 탄생과 풀이 과정을 역사적으로 추적하여 수학에서 하나의 결과가 만들어지는 과정을 알아본다.

2장에서는 페르마의 마지막 정리의 유래와 연구내용을 살펴본다.

3장에서는 페르마의 정리를 증명하는데 필요한 기본정의와 정리들을 설명한다.

4장에서는 페르마의 마지막 정리를 $n=3$, $n=4$인 경우의 증명을 간략하게 소개하고, $n=5$, $n=6$, $n=7$인 경우의 증명과정을 다룬다.

5장에서는 페르마의 마지막 정리의 증명도전사를 소개한다.

# 제 2장 페르마의 마지막 정리의 유래와 연구내용

## 1. 페르마의 마지막 정리의 유래

페르마는 고대 그리스의 Diophantus가 쓴 <<산학 Arithmetica>> 제 2권을 공부하면서 <피타고라스의 정리> 및 <피타고라스의 삼각수>와 관련된 다양한 문제들을 접하였다.

Diophantus가 이 책에서 제시한 부정방정식에 관한 문제는 통상 단 한 개의 해를 요구했지만, 페르마는 가능성 있는 모든 해를 결정하는 방법을 종종 찾아내기도 했다. 이러한 과정에서 페르마의 마지막 정리가 탄생했다.
"페르마의 마지막 정리"는 산학 제 2권 문제 8의 옆에 남긴 페르마의 기록으로부터 유래한다([1],[5]).

산학 제 2권 문제 8 ;
'주어진 제곱수를 두 개의 제곱수의 합으로 써라.'
(즉, 방정식 $X^2+Y^2=Z^2$을 만족시키는 자연수 $X, Y, Z$를 찾아라.)

산학 제 2권 문제 8의 해 [유클리드의 원론] 공식
$x=2st, \quad y=s^2-t^2, \quad z=s^2+t^2$
은 원래의 방정식에 대한 모든 원시해를 생성한다. 여기에서 $s$와 $t$는 다음 조건을 만족시키는 임의의 자연수이다.
(ⅰ) $s>t$
(ⅱ) $s$와 $t$는 서로 소
(ⅲ) $s, t$ 중 하나만 홀수
더욱이, 방정식에 대한 모든 원시 해는 $s$와 $t$의 적당한 값에 대해 위와 같은 꼴이다([12],[13]).

페르마는 산학 제 2권 문제 8의 옆에 다음에 있는 여백에 다음과 같은 주석을 달아놓았다.
임의의 세제곱수는 다른 두 세제곱수의 합으로 표현될 수 없다. 임의의 네제곱수 역시 다른 두 네제곱수의 합으로 표현될 수 없다. 일반적으로, 3이상의 지수를 가진 정수는 이와 동일한 지수를 가진 다른 두 수의 합으로 표현될 수 없다.

페르마의 마지막 정리를 현대적인 표기법으로 나타내면 다음과 같다.
$2$보다 큰 임의의 큰 자연수 $n$에 대해서 방정식 $x^n+y^n=z^n$은 어떠한 양의 정수근도 갖지 않는다.[1] 즉, $x^n+y^n=z^n$에 있어서 $n>2$ 일 때 정수해 $x, y, z$가 존재하지 않는다. 이 문제를 제외하고 당시 페르마가 제시한 모든 문제는 18세기까지 증명되거나 반증되었기 때문에, 이 정리에 '마지막' 이라는 수식어가 붙게 되었다.

"페르마는 경이적인 방법으로 이 정리를 증명했다. 그러나 책의 여백이 너무 좁아 여기에 옮기지 않겠다".라는 주석을 그 정리 밑에 달아놓았으나 페르마 자신이 이 정리의 증명을 했는지는 알 수 없다.
따라서 페르마의 장남 클레망 사무엘(Clement - Samuel)은 아버지의 뛰어난 업적을 후대에 남겨야 한다는 사명감으로 아버지가 남긴 낙서, 편지, 그리고 Diophantus가 쓴 <<산학 Arithmetica>> 복사본의 여백에 남긴 주석들을 수집, 정리하여 "페르마의 주석이 달린 Diophantus의 Arithmetica" 라는 제목의 책을 1670년에 출판하였다. 이 책에는 42개에 달하는 페르마의 주석이 수록되었다. 이렇게 하여 페르마의 마지막 정리는 전세기의 수학자들의 도전과제로 남게 되었다.

---

1) 디오판토스 시대와 페르마 시대까지도 '0'은 수로 간주되지 않았다. 그래서 변수 중 하나에 자명한 해 0의 대입은 제외된다. 그리고 이 문제는 단지 양의 유리수 해만 고려했다. 유리수 해가 존재하면 공통 분모를 각 해에 곱해서 정수해로 만들 수 있으므로, 자연수 해만을 고려하면 충분하다([13]).

## 2. 페르마의 연구내용

Mersenne 수사 이외의 사람과는 전혀 수학적 토론을 하지 않았던 페르마는 파스칼을 통하여 '확률이론probability theory' 이라는 전혀 새로운 수학 분야를 접하게 된 후 파스칼과 빈번히 교류하며 모호한 확률이론을 정립하고, 여러 개의 정리를 증명함으로써 확률이론의 기초를 탄탄하게 다져놓았다.

페르마와 파스칼은 모든 종류의 확률 게임에 적용할 수 있는 근본적인 확률법칙을 발견하였으며 이들의 결과는 도박사들에게 매우 유용하게 적용되었다. 뿐만 아니라 이 확률법칙은 주식 시세를 예견하거나 핵발전소에서 사고가 터질 확률을 계산하는 등 확률과 관련된 거의 모든 분야에 적용할 수 있다.

페르마가 남긴 수학적 업적은 기하학에 그 당시의 해석학인 급수의 이론과 오늘날 우리가 미적분이라고 일컫는 분야를 도입하였다. 기하학에 관한 것은 주로 미분의 생각을 바탕으로 전개된 내용들이며 곡선의 접선, 곡선에 둘러싸인 면적, 극대 및 극소의 문제 등이 있다.

페르마가 도입한 미적분학 때문에 과학자들은 속도와 가속도(시간에 대한 속도의 변화율) 등의 개념을 더욱 확실하게 이해할 수 있었으며 근본적인 물리량들 사이의 상호관계를 더욱 체계적으로 분류할 수 있게 되었다.

수세기 동안 사람들은 미적분학의 창시자가 Isaac Newton이라고 알고 있었으나, Newton이 페르마의 연구를 참조했다는 사실을 아는 사람은 아무도 없다. 그러다 1934년에 "페르마의 접선 계산법을 기초로 하여 미적분학을 개발하였다."는 뉴턴 자신의 친필 원고가 발견되었다. 17세기 이후로 미적분학은 거리와 속도, 그리고 가속도 등의 핵심 개념으로 이루어진 뉴턴의 역학법칙과 중력법칙을 서술하는 데 주로 사용되어 왔기 때문에, 페르마의 업적은 뉴턴이라는 거인의 그림자에 가려져 있었다. 미적분학과 확률이론의 초기 사상을 제공했다는 사실만으로도 페르마는 역사상 가장 위대한 수학자라고 할 수 있지만 페르마

가 위대한 업적을 남긴 분야는 정수론이었다.

정수론에 대한 페르마의 연구 결과 몇 가지를 나열하면 다음과 같다.

**정리 2.2.1 ((페르마의 소정리(Fermat's little theorem))**

$p$는 소수이고 $a \in Z$에 대해 $p \nmid a$면 $a^{p-1} \equiv 1 \pmod{p}$이다.

이 정리는 페르마가 1640년에 드 베지(F. de bessy)에게 보낸 편지에 증명없이 언급되었고, 1736년에 오일러에 의해 최초로 증명되었다. 이 정리는 소수의 성질에 관한 정리인데, 정수론의 발전에 기초가 된 중요한 정리 중의 하나이다. 모든 소수는 두 가지 종류로 분류될 수 있는데, 하나는 $4n+1$로 표현되는 부류이고 다른 하나는 $4n-1$로 표현되는 소수이다(여기서, $n$은 임의의 정수를 나타낸다). 이 분류에 따르면 $13$은 전자의 경우에 속하며($4 \times 3+1$), $19$는 후자의 경우이다($4 \times 5-1$)([1],[3],[9],[12]).

**정리 2.2.2 ((소수의 정리))**

$4n+1$로 표현되는 소수는 항상 두 제곱수의 합으로 표현될 수 있지만, ($13=2^2+3^2$), $4n-1$로 표현되는 소수는 이런 방식으로 표현될 수 없다 ($19=?^2+?^2$)([1],[3],[9],[12])."

이것은 페르마가 남몰래 증명했던 수많은 정리들 중 하나에 불과했다. 당대의 수학 천재였던 오일러는 7년 동안 이 문제와 씨름하던 끝에 1749년에 증명에 성공했다. 페르마가 죽은 지 거의 1세기 만에 그의 증명 중 하나가 천재 오일러에 의해 재현된 것이다.

**정리 2.2.3**

음이 아닌 정수는 네 개 이하의 제곱수의 합으로 나타낼 수 있다 ([1],[3],[9],[12]).

**정리 2.2.4**

피타고라스 삼각형의 면적은 정수의 제곱으로 나타낼 수 없다 ([1],[3],[9],[12]).

**(증명)** 빗면의 길이가 $z$, 이웃변의 길이가 $x, y$인 피타고라스의 삼각형은 $x^2+y^2=z^2$을 만족한다.

이 삼각형의 면적을 $u^2$이라고 가정하면 $u^2=\frac{1}{2}xy$ 즉 $2xy=4u^2$이다.

따라서 $(x+y)^2=x^2+y^2+2xy=x^2+4u^2$

$(x-y)^2=x^2+y^2-2xy=x^2-4u^2$ 이므로

$$\begin{aligned}(x^2-y^2)^2 &= (x+y)^2 \cdot (x-y)^2 \\ &= (z^2+4u^2)\cdot(z^2-4u^2) \\ &= z^4-16u^2 \\ &= z^4-(2u)^4\end{aligned}$$

이다.

이 방정식은 양의 정수해가 존재하지 않으므로 $u$를 구할 수 없다.

그러므로 피타고라스 삼각형의 면적은 정수의 제곱으로 나타낼 수 없다.

**정리 2.2.5**

방정식 $x^2+2=y^2$의 정수해는 단 하나이고, $x^2+4=y^3$의 정수해는 단 두 개다([1],[3],[9],[12]).

첫 번째 방정식의 해는 $x=5,\ y=3$이고, 두 번째 방정식의 해는 $x=2,\ y=2$와 $x=11,\ y=5$인데 페르마는 이외의 해가 존재하지 않다는 것을 증명했지만 그답게 증명을 발표하지 않았기에 위 정리의 증명이 발표된 것은 그가 죽은 지 오랜 세월이 지나서였다([9]).

# 제 3장 페르마의 마지막정리를 다루는데 필요한 기본정의

이 장에서는 페르마의 정리를 다루는데 필요한 정의들을 소개한다([3],[4],[11],[12]).

## 3.1. 약수와 최대공약수

**정의 3.1.1**

두 정수 $a, b$에 대하여 $b=ac$인 정수 $c$가 존재하면 $a$를 $b$의 약수(divisor) 또는 인수(factor)라 하고 $b$를 $a$의 배수(multiple)라고 하며 이것을 $a \mid b$로 나타낸다. 정수 $a$가 $b$의 약수가 아닐 때에는 $a \nmid b$로 나타낸다.

**정의 3.1.2**

두 정수 $a, b$에 대하여 $e \mid a$이고 $e \mid b$인 정수 $e$를 $a$와 $b$의 공약수(common divisor)라고 한다. 또, 다음 세 조건을 만족시키는 정수 $d$를 $a, b$의 최대공약수(greatest common divisor)라 하고, 이것을 $(a, b)$ 또는 GCD $(a, b)$로 나타낸다.

① $d \geq 0$

② $d \mid a$, $d \mid b$, 즉 $d$는 $a$와 $b$의 공약수이다.

③ 정수 $e$에 대하여 $e \mid a$, $e \mid b$이면, $e \mid d$이다. 즉, $a$와 $b$의 공약수는 모두 $d$의 약수이다.

**정의 3.1.3**

두 정수 $a, b$에 대하여 $a \mid c$이고 $b \mid c$인 정수 $c$를 $a$와 $b$의 공배수(common multiple)라고 한다. 또, 다음 세 조건을 만족시키는 정수 $l$을 $a, b$의 최소공배수(Least common multiple)라 하고, 이것을 $[a, b]$ 또는 LCM $\{a, b\}$로 나타낸

다.

① $l \geq 0$

② $a \mid l,\ \ b \mid l$ 즉, $l$은 $a$와 $b$의 공배수이다.

③ 정수 $c$에 대하여 $a \mid c,\ \ b \mid c$이면 $l \mid c$이다. 즉, $a$와 $b$의 공배수는 모두 $l$의 배수이다.

## 3. 2. 소수

**정의 3.2.1**

양의 정수 $p$가 1보다 크고 $p$의 약수는 $1, -1,\ p,\ -p$뿐일 때, $p$를 소수(prime number) 라 한다.

한편, 1보다 큰 정수 $a$가 소수가 아닐 때, 즉 $a = de,\ \ 1 < d < a,\ \ \ 1 < e < a$인 정수 $d, e$가 존재할 때, $a$를 합성수(composite number)라고 한다.

**정의 3.2.2**

양의 정수 $n$이 소수이거나 또한 유한개의 소수의 곱으로 표시될 때, $n$은 소인수분해(prime factorization)된다고 말한다.

또 $n = p_1 \cdot p_2 \cdots p_r,\ \ \ r \geq 1$ ($p_i$는 소수)으로 나타낸 것을 $n$의 소인수분해라 한다.

**정의 3.2.3**

양의 정수 $n(n \geq 2)$의 서로 다른 소인수가 $p_1 \cdot p_2 \cdots p_r$뿐일 때, $n$은 단 한 가지 방법으로 다음과 같이 소인수분해된다.

$n = p_1^{e_1}\ p_2^{e_2}\ \cdots\ p_r^{e_r} \qquad (e_1 \geq 1,\ e_2 \geq 1,\ \cdots\ e_r \geq 1)$

위와 같은 꼴로 나타낸 것을 $n$의 표준분해(standard decomposition)라고 한다.

## 3.3 합동

**정의 3.3.1**

$n$이 1보다 큰 자연수라 할 때, 두 정수 $a, b$라 할 때, 두 정수 $a, b$가 있어서 $a-b$가 $n$의 배수일 때, $a$와 $b$는 법(modulus) $n$에 대하여 합동이라고 하고, 기호로는 $a \equiv b \pmod{n}$이라 표시한다.

## 3.4. Euler의 $\varphi$ 함수

**정의 3.4.1**

정수 집합 위의 합동관계 "$a \equiv b \pmod{n}$"에 대한 동치류를 특히 법 $n$에 관한 잉여류(residue class modulo n)이라 한다. 이 때 $a \in Z$에 의해 결정되는 잉여류를 $\bar{a}$로 나타내면

$\bar{a} = \{ x \in Z \mid x \equiv a \pmod{n} \} = \{ a + kn \mid k \in Z \}$ 이다.

**정의 3.4.2**

법 $n$에 관한 잉여류 $\bar{a} \in \overline{Z_n} = \{ \bar{0}, \bar{1}, \cdots \overline{n-1} \}$에 대하여 $\gcd(a, n) = 1$일 때, $\bar{a}$를 법 $n$에 관한 기약잉여류(reduced residue class)라 한다.

그리고 법 $n$에 관한 기약잉여류 전체의 집합을 $\overline{Z_n^*}$로 나타낸다.

즉, $\{ \bar{a} \in \overline{Z_n} \mid \gcd(a, n) = 1 \}$이다.

**정의 3.4.3**

기약잉여계 전체의 집합을 $Z_n^* = \{ a \in Z_n \mid \gcd(a, n) = 1 \}$이라고 하고, 정수 $0, 1, \cdots, n-1$중에서 $n$과 서로 소인 정수 전체의 개수를 $\varphi(n)$으로 나타내면 $\varphi(n) = |Z_n^*|$이다. 이와 같이 정의된 정수론적 함수 $\varphi$를 오일러의 $\varphi$函數(Euler $\varphi$ - function)이라고 한다.

즉, $\varphi(n)$은 $0, 1, \cdots, n-1$중에서 $n$과 서로 소인 정수들의 개수를 나타낸다. 특히, $p$가 소수일 때, $Z_p^* = \{1, 2, \cdots, p-1\}$이고 $\varphi(m) = p-1$이다 ([3],[4],[11],[12]).

# 제 4장 페르마의 마지막 정리에 대한 구체적 경우의 증명

## 4.1 지수가 2인 예외적 경우의 피타고라스 방정식[2)]

## (( $X^2 + Y^2 = Z^2$ ------① ))

$x^2+y^2=z^2$인 양의 정수 세 개로 이루어진 한 조(triple) $(x, y, z)$는 피타고라스 triple이라고 부른다. (예를 들어, (3, 4, 5)).
만약 $x, y, z$가 $x^2+y^2=z^2$인 0이 아닌 정수들이면, $|x|, |y|, |z|$도 또한 같은 방정식을 만족한다. $x, y$ 둘 다 홀수일 수 없다.
왜냐하면, $x, y$ 둘 다 홀수이면, $z^2 \equiv 1+1 \pmod 4$가 되는데 이것은 불가능하다. 더욱이, 만약 $d = \gcd(x, y, z)$이면, $x/d$, $y/d$, $z/d$ 또한 그 방정식을 만족한다. 그러므로 ①은 원시해 $(x, y, z)$를 결정하는 것으로 충분하다. $x>0$, $y>0$, $z>0$, $x$는 짝수, $\gcd(x, y, z)=1$인 $(x, y, z)$을 원시해라고 부른다. (이 경우에 $y, z$는 홀수이다.)

피타고라스 정리에 따른 증명은 중・고등학교 때 기하학적 방법으로 공부했으

2) 피타고라스가 인도에 깔려있는 돌을 보고, "직각삼각형의 직각을 끼는 두 변 위에 그린 정사각형 안에 있는 돌의 개수의 합은 빗변 위에 그린 정사각형 안에 있는 돌의 개수의 합과 같다." 라는 사실을 발견하여 이를 바탕으로 일반적인 직각삼각형까지 확장하여 성립한다는 것을 발견했다는 추측이 있다. 피타고라스 정리의 최초의 일반적인 증명은 피타고라스에 의해 주어 졌다고 한다. 피타고라스 시대 이래로도 피타고라스 정리에 대한 수많은 증명들이 나왔으며 20세기 초까지 밝혀진 증명만도 360여가지가 된다([11]).

므로, 피타고라스의 방정식이 페르마 마지막 정리의 증명에 영향을 준 몇 가지 정리에 대해 살펴보자.

**정의 4.1.1**

부호 $x$의 무게 $w(x)$를 2를 법으로 해서 $w(x) \equiv 0$ 또는 $w(x) = 1$이라고 할 때 0또는 1을 $x$의 패러티(parity: 다른 홀짝 맞춤) 이라고 한다([7]).

**정리 4.1.2**

서로 소인 양의 정수 $a, b$에 대해 (단, $a > b$) $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ 인 triple ( $x, y, z$ )은 식 ①의 원시해이다.
이것은 위의 조건들을 만족하는 짝 $(a, b)$의 집합과 식 ①의 원시해의 집합 사이의 일대일 대응을 준다.

**(증명)** $x, y, z$를 표시한 것 같이 정의되어있다고 하자.

(⇒) $X^2 + Y^2 = Z^2$

$\Rightarrow (2ab)^2 + (a^2 - b^2)^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2$

확실히 $x > 0$, $y > 0$, $z > 0$, $x$는 짝수, $\gcd(x, y, z) = 1$이다.

왜냐하면 만약 $d$가 $x, y, z$을 나누면 $d$는 $2a^2$과 $2b^2$을 나눈다.

따라서 $d = 1$ 또는 $d = 2$이다. ( $\gcd(a, b) = 1$이므로)

그러나, $y$가 홀수이므로 $d \neq 2$이다 ($a, b$는 같은 패러티를 갖지 않는다).

다른 짝은 다른 triple ( $x, y, z$)을 준다.

(⇐) ( $x, y, z$)를 식 ①의 원시해라고 하자.

$\Rightarrow x^2 + y^2 = z^2$, $x$는 짝수, $y, z$는 홀수,

$\gcd(x, y, z) = 1$로부터 $\gcd(x, z) = 1$, $\gcd(z - x, z + x) = 1$ 이다.

$y^2 = (z - x)(z + x)$와 이들의 소인수분해로부터 $z + x = t^2$, $z - x = u^2$ ----**(∗)**

이 된다( 여기서 $t, u$는 $t > u > 0$인 양의 홀수 정수이다).

$a, b$를 $t + u = 2a$, $t - u = 2b$ $(a > b > 0)$인 정수들이라 하자.

$t = a + b$, $u = a - b$ $(a > b > 0)$ 그래서 **(∗)**식을 연립하면,

$x = \dfrac{t^2 - u^2}{2} = \dfrac{(a+b)^2 - (a-b)^2}{2} = 2ab,$

$y^2 = u^2 t^2 = (a-b)^2 (a+b)^2 = (a^2 - b^2)^2 \quad \Rightarrow \; y = a^2 - b^2$

$z^2 = \dfrac{(a+b)^2 + (a-b)^2}{2} = a^2 + b^2$

$\gcd(z - x,\ z + x) = 1$이므로 $\gcd(a,\ b) = 1$이다.

마지막으로, $a + b = t$가 홀수이므로 $a$, $b$ 둘 다 홀수는 아니다.

정리 4.1.2에 의하여, ①의 원시해를 발견하는 것은 어느 홀수인 양의 정수가 두 제곱수의 합이 되는지를 결정하여 각 경우에 모두 그러한 표현으로 쓴다.

**정리 4.1.3**

소수 $p$가 두 제곱수의 합일 필요충분조건은 $p \equiv 2$ 또는 $p \equiv 1 \pmod 4$이다.

**정리 4.1.4**

자연수 $n$이 두 제곱수의 합일 필요충분조건은 $p \equiv 3 \pmod 4$인 꼴의 $n$의 모든 소인수는 $n$의 소인수분해에서 짝수승으로 나타난다.

**(증명)**

($\Leftarrow$) $n = p_1^{k_1} \cdots p_j^{k_j}$ 으로 놓고 만약 $p_j \equiv 3 \pmod 4$이면 $k_j$는 짝수라고 가정하자. 그러면 $n = n_0^2 n_1$이다. ( $n_0 \geq 1$, $n_1 \geq 1$, $n_1$은 4를 법으로 하여 2 또는 1 둘 중의 하나와 합동인 서로 다른 소수의 곱이다)

정리 4.1.3에 의해, $n_1$의 각 인수는 두 제곱수의 합이다 ;

$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2$에 표시된 항등식에 의해, $n_1$과 $n$은 두 제곱수의 합이다. $n = x^2 + y^2$

($\Rightarrow$) $n = x^2 + y^2$ 으로 놓는다. : $x = 0$ 또는 $y = 0$ 이면 이 명제는 자명하다.

따라서, $x$, $y$을 0이 아닌 정수라 하자. 또한 $d = \gcd(x,\ y)$로 놓으면

$d^2 \mid n$, $n = d^2 n'$, $x = d x'$, $y = d y'$ 인 정수 $n', x', y'$ 가 존재한다.
따라서 $\gcd(x', y') = 1$, $n' = x'^2 + y'^2$
만약 $p \mid n'$ 이면 $p$는 $x'$을 못 나눈다.
왜냐하면 만약 $p \mid x'$라면, $p \mid y'$이 되어 $\gcd(x', y') = 1$임에 모순이다.
$k$를 $kx' = y' \pmod p$ 가 되는 것이라고 하면,
$x'^2 + y'^2 \equiv x'^2(1 + k^2) \equiv 0 \pmod p$이고 $p \nmid x'$이므로, $p \mid 1 + k^2$ 이어야 한다. 즉, $k^2 \equiv -1 \pmod p$ 이다([2],[6],[8][12]).

## 4.2. $n = 4$인 경우의 증명 (( $X^4 + Y^4 = Z^4$ ))

페르마가 남긴 기록에서는 페르마의 마지막 정리에 대한 증명은 찾아볼 수 없지만 $n = 4$인 경우를 증명했음을 암시하는 증거가 있다. 각 변의 길이가 모두 자연수인 직각삼각형의 넓이는 어떠한 자연수의 제곱도 될 수 없음을 증명한 독창적인 논법 (무한하강법 : 적당한 수에 대하여 어떤 성질이 사실이면 그보다 작은 수에 대해서도 같은 성질을 가져야 함을 보임으로써 전체 수에 대하여 그 성질이 불가능함을 보이는 것)에서 그 증거를 찾아볼 수가 있다.

**정리 4.2.1**

$X^4 - Y^4 = Z^2$은 모두 0이 아닌 정수들의 해가 없다.

**(증명)** 만약 위의 명제가 거짓이면, $X^4 - Y^4 = Z^2$이 되는 가능한 최소의 $x$를 갖는 양의 정수들의 triple을 ( $x$, $y$, $z$)라 하자.
그러면 $\gcd(x, y) = 1$이다.
왜냐하면 $\gcd(x, y) \neq 1$이면, $\exists\, p \in Z$ s.t. $p \mid x$, $p \mid y$

$$\Rightarrow p^2 \mid z, \quad \begin{cases} x = p x \\ y = p y \\ z = p^2 z \end{cases}$$ 이 되어, 가정에 모순이 생긴다.

따라서, $z^2 = x^4 - y^4 = (x^2+y^2)(x^2-y^2)$이고,

$\gcd(x^2+y^2,\ x^2-y^2) = 1$은 $\gcd(x,\ y) = 1$이기 때문에 쉽게 보일 수 있듯이 1 또는 2이다.

여기서 우리는 두 경우를 구별한다.

**case 1)** $\gcd\ (x^2+y^2,\ \ x^2-y^2) = 1$

$(x^2+y^2)$과 $(x^2-y^2)$의 곱은 제곱수이므로, $x^2+y^2$과 $x^2-y^2$은 제곱수들이다.

$\Rightarrow x^2+y^2 = s^2,\quad x^2-y^2 = t^2$, $\gcd(s,\ t) = 1$인 양의 정수 $s$, $t$가 존재한다.

여기서 $2x^2 = s^2+t^2$, $s$, $t$는 같은 패러티를 갖고, 동시에 짝수일 수밖에 없기 때문에 $s$, $t$는 홀수이다.

$\Rightarrow\ u = \dfrac{s+t}{2}$, $v = \dfrac{s-t}{2}$, $\gcd(u, v) = 1$ 인 양의 정수 $u$, $v$가 존재한다.

$\Rightarrow\ uv = \dfrac{(s^2-t^2)}{4} = \dfrac{y^2}{2}$

$\Rightarrow\ y^2 = 2uv$

$\gcd(u,\ v) = 1$이므로 $\begin{cases} u = 2l^2 \\ v = m^2 \end{cases}$ 또는 $\begin{cases} u = l^2 \\ v = 2m^2 \end{cases}$ 인

양의 정수 $l, m$이 존재한다.

$u$은 짝수이고, $\gcd(u,\ v, x) = 1$,

그리고, $u^2+v^2 = \dfrac{(s+t)^2+(s-t)^2}{4} = \dfrac{s^2+t^2}{2} = x^2$

정리4.1.2로부터, $\begin{cases} 2l^2 = u = 2ab \\ m^2 = v = a^2-b^2 \\ x = a^2+b^2 \end{cases}$

과 같이 되는 $\gcd(a,\ b) = 1$, $0 < b < a$ 인 양의 정수 $a$, $b$가 존재한다.

$\Rightarrow\ l^2 = ab \ \Rightarrow \begin{cases} a = c^2 \\ b = a^2 \end{cases}$

이고, $\gcd(c,\ d) = 1$ 인 양의 정수 $c,\ d$가 존재한다.

$\Rightarrow\ m^2 = c^4 - d^4,\quad 0 < c < a < x$

따라서 양의 정수의 triple $(c,\ d,\ m)$은 원래 방정식의 해이다. 이것은 최소의 $x$의 선택에 모순이다.

**case 2)** $\gcd(x^2+y^2,\ x^2-y^2) = 2$

$x,\ y$는 홀수, $z$는 짝수이다.

정리4.1.2로부터, $\begin{cases} x^2 = a^2+b^2 \\ y^2 = a^2-b^2 \\ z = 2ab \end{cases}$

이고, $\gcd(a,\ b)=1,\ 0<b<a$인 양의 정수 $a, b$가 존재한다.

그러므로 $x^2y^2 = a^4 - b^4,\quad 0<a<x$ 이다.

이것은 다시 최소의 $x$의 선택에 모순이다([2]).

**정리 4.2.2**

방정식 $X^4+Y^4=Z^4$ 은 0이 아닌 모두 서로 다른 정수해를 갖지 않는다.

**(증명)** 만약 $x,\ y,\ z$가 $X^4+Y^4=Z^4$인 음이 아닌 정수이면, $z^4-y^4=(x^2)^2$인데 이것은 정리 4.2.1에 모순이다.

## 4.3. $n=3$인 경우의 증명 (( $X^3+Y^3=Z^3$ ))

페르마는 $x^3+y^3=z^3$이 되는 0이 아닌 정수 $x, y, z$은 없다는 명제를 보이기 위하여 페르마의 마지막 문제를 제기했다. 오일러는 이 명제의 증명을 발견했다. 오일러는 정수 $a$와 $b$에 대해 $a+b\sqrt{-3}$ 꼴의 수 체계에서 유일인수분해

가 성립함을 이용하여 1753년 $n=3$인 경우를 증명했다.

**정리 4.3.1**

$X^3+Y^3+Z^3=0$은 오직 자명한 해를 갖는다.

**(증명)** $x^3+y^3+z^3=0$인 0이라 하자. 쌍마다 서로 소인 정수 $x, y, z$에 대해 그러면 2는 세제곱수가 아니므로 이들 $x, y, z$ 은 별개의 것들이고 이들 정수 중의 정확히 하나는 짝수이다. (예를 들어 $x$, $y$은 홀수, $z$는 짝수라고 하자).
위의 성질을 갖는 모든 해 중에서, $|z|$가 가능한 가장 작은 해를 선택한다.

여기서, $l^3+m^3+n^3=0$, $n$은 짝수, $|z|>|n|$인 0이 아닌 쌍마다 서로 소인 정수들 $l, m, n$을 만들며 이로부터 모순이 생김을 보이면 충분하다.
$x+y$, $x-y$은 짝수이므로, $2a=x+y$, $2b=x-y$인 정수 $a, b$ 가 존재한다.
따라서 $x=a+b$, $y=a-b$이고, $a, b\neq 0$, $\gcd(a, b)=1$, $a$와 $b$는 다른 패러티(parity)를 갖는다.
그러면 $-z^3=x^3+y^3=(a+b)^3+(a-b)^3=2a(a^2+3b^2)$.
그러나, $a^2+3b^2$은 홀수이고, $z$는 짝수이므로, $8|z^2$, $8 \nmid 2a$이다.
따라서 $b$는 홀수이다.
따라서 $2a$와 $a^2+3b^2$이 서로 소이거나 두 수 모두 3으로 나누어 져야 한다.
$\Rightarrow 3|2a$
만약, $p^k\ (k\geq 1)$이 $2a$와 $a^2+3b^2$을 나누는 소수의 거듭제곱이면, $p\neq 2$이다. 따라서, $p^k|a$, $p^k|3b^2$ 이지만 $p\nmid b$이다.

**case 1)** $\gcd(2a,\ a^2+3b^2)=1$

$3\nmid a$, $-z^3=2a(a^2+3b^2)$와 유일인수분해정리에 의하여 $2a$와 $a^2+3b^2$은 세제곱수들이다.

$$\begin{cases} 2a=r^3 \\ a^2+3b^2=s^3 \end{cases}$$ ( 여기서, $s$는 홀수이고 3의 배수가 아니다 )

여기서, 정당화 되는 사실은

「만약 $s$가 홀수이고 $s^2 = a^2 + 3b^2$, $\gcd(a,\ b) = 1$이면, $s$는 또한 $u, v \in Z$ 에 대해 $a = u(u^2 - 9v^2)$, $b = 3v(u^2 - v^2)$, $s = u^2 + 3v^2$ 형태임이 틀림없다. 그러면 $v$는 홀수이고 $u$는 0이 아닌 짝수이다 ($\because$ $b$ : 홀수).

또 $3 \nmid u$ ($\because 3 \nmid a$), $\gcd(u,\ v) = 1$이다. 그러므로 $2u$, $u + 3v$, $u - 3v$은 쌍마다 서로 소이고, $r^3 = 2a = 2u(u+3v)(u-3v)$로부터, $2u$, $u - 3v$, $u + 3v$는 세 제곱이다.」

$$\begin{cases} 2u = -n^3 \ (n\text{은 짝수}) \\ u - 3v = l^3 \\ u + 3v = m^3 \end{cases}$$

단, $l, m, n \neq 0$($\because 3 \nmid u$), 쌍마다 서로 소

따라서, $l^3 + m^3 + n^3 = 0$이다.

이제 우리는 $|z| > |n|$임을 보이자. 실제로,

$|z|^3 = |2a(a^2 + 3b^2)| = |n^3(u^2 - 9v^2)(a^2 + 3b^2)| \geq 3|n^3| > |n^3| \Rightarrow |z| > |n|$

($\because$ $u^2 - 9v^2 = l^3 m^3 \neq 0$, $b \neq 0$, 3은 홀수이기 때문이다 ).

이것은 $|z|$의 최소성에 모순이다.

**case 2)** $\gcd(2a,\ a^2 + 3b^2) = 3$, $a = 3c$로 쓴다. $c$는 짝수이고, $4 \mid c$, $3 \nmid b$이다. ($\because$ $a, b$가 서로 소이므로)

$-z^3 = 6c(9c^2 + 3b^2) = 18c(3c^2 + b^2)$ ( 여기서 $\gcd(18c,\ 3c + b^2) = 1$ ).

실제로, $c$는 짝수, $b$는 홀수이므로, $3c^2 + b^2$은 홀수이고 $3 \nmid 3c^2 + b^2$, $\gcd(b,\ c) = 1$이다.

유일인수분해정리에 의하여, $18c = r^3$, $3c^2 + b^2 = s^2$ (여기서 $s$는 홀수이고, $3 \mid r$) 이며 앞의 case 1)에 의하여,

$$\begin{cases} s = u^2 + 3v^2 \ (u, v \in Z) \\ b = u(u^2 - 9v^2)\, c = 3v(u^2 - v^2) \end{cases}$$

이다.

그러므로, $n$은 홀수, $v$는 짝수 ( $\because b$가 홀수이므로 ), $v \neq 0$, $\gcd(u, v) = 1$이다.

또한, $2v$, $u+v$, $u-v$는 서로 소이다.

$r^3 = 18c = 54v(u+v)(u-v)$에서 $(\frac{r}{3})^3 = 2v(u+v)(u-v)$, $2v$, $u+v$, $u-v$는 세제곱이다.

$$\begin{cases} 2v = -n^3 \ (n\text{은 짝수}) \\ u+v = l^3 \\ u-v = -m^3 \end{cases} \qquad \text{단, } l, m, n \neq 0,$$

따라서, $l^3 + m^3 + n^3 = 0$이다.

이제 우리는 $|z| > |n|$임을 보인다. 실제로,

$|z|^3 = 18|c|(3c^2 + b^2) = 54|v(u^2 - v^2)(3c^2 + b^2)| = 27|n|^3 |u^2 - v^2|(3c^2 + b^2) > |n|^3$

( $\because$ $u^2 - v^2 = l^3 m^3 \neq 0$, $|3c^2 + b^2| \geq 1$이므로 다시 이것은 $|z|$의 최소성에 모순이다.)

**보조정리 4.3.2**

$m = 3$ 또는 $m = u^2 + 3v^2$ ( $u, v \neq 0$, $\gcd(u, v) = 1$)이라 하자.

만약 $m$이 홀수이고 $m = \prod_{i=1}^{n} p_i^{ei}$ ( 여기서 $p_i$은 소수들이고, $e_i \geq 1$ ) 이면

$p_i = a_i^2 + 3b_i^2$, $u + v\sqrt{-3} = \prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i}$ 가 되는 정수들

$a_i$, $b_i$ $(i = 1, \cdots, n)$가 존재하다.

**정리 4.3.3**

0보다 큰 모든 $m$에 대하여, 방정식 $X^3+Y^3=2^m Z^3$ ----------(②)
은 오직 자명한 정수해만 갖는다 : 즉, 해들은 $xyz=0$인 $(x, y, z)$이고 만약 $m=1$이면 0이 아닌 임의의 $x$에 대한 $(x, x, x)$가 해이다.

**(증명)** $x, y, z$가 0이 아닌 정수들이고,
만약 $m=1$이면 $x, y, z$은 서로 같지 않고 $X^3+Y^3=2^m Z^3$을 만족한다고 가정한다 ; 일반성을 잃지 않고 $\gcd(x, y, z) = \gcd(x, z)=\gcd(y, z)=1$이라고 가정하자.
만약 $m=3m'$ $(m' \geq 0)$이면, $(x, y, 2^{m'}z)$은 $X^3+Y^3=Z^3$의 자명하지 않은 해일 것이다. 이것은 정리 4.3.1에 모순이다. 그러므로 $3 \nmid m$이다.

$m \neq 0$ 이므로 $x, y$는 같은 패러티를 갖는다.
만약 $x, y$가 둘 다 짝수이면, $2s \mid x$, $2s \mid y$ 인 최대정수를 $s$ $(\geq 1)$라 하자.
$x=2sx'$, $y=2sy'$ 로 쓴다. 그래서 $x'$ 또는 $y'$은 홀수이다.

그래서 $x'^3+y'^3=2^{m-3}sz^3$ 이다 ; 그러므로 $(x', y', z)$은 같은 형태의 방정식의 자명하지 않은 해이다 ; 그러면 $x', y'$은 같은 패러티를 갖는다.
따라서 둘 다 홀수이다.
그러므로 $m$을 $m-3s$로 변환하여, ②는 자명하지 않은 해 $(x, y, z)$ $(x, y$은 홀수, $\gcd(x, y, z)=\gcd(x, z)=\gcd(y, z)=1)$를 갖는다고 일반성을 잃지 않고 가정해도 좋다 ; 그러므로 $\gcd(x, y)=1$
같은 논법으로, 또한 $z$는 홀수라고 가정해도 좋다. 그래서 우리는 $\gcd(x+y, x^2-xy+y^2)=1$ 또는 3인 $2^m z^3=x^3+y^3=(x+y)(x^2-xy+y^2)$을 갖는다.

실제로, 만약 $p$가 소수, $e \geq 1$ 이고 $p^e \mid x+y$, $p^e \mid x^2-xy+y^2$ 이면, $x \equiv -y \pmod{p^e}$ 이다.
따라서 $x^2-xy+y^2 \equiv 3x^2 \pmod{p^e}$ 이면 $\Rightarrow$ $\therefore$ $p^e \mid 3x^2$ $\Rightarrow$ $\gcd(x, y)=1$ 이

기 때문에 $p \nmid x$이다. 그러므로 $p^e \mid 3$이다.

즉 $p^e = 3$이다. 또한 $x^2 - xy + y^2 = (x+y)^2 - 3xy$이기 때문에,

$3 \mid x+y \Leftrightarrow 3 \mid x^2 - xy + y^2 \Leftrightarrow 3 \mid z \Leftrightarrow \gcd(x+y,\ x^2 - xy + y^2) = 3$이다.

**case 1 )** $3 \nmid z$

$\gcd(x+y,\ x^2 - xy + y^2) = 1$ 이고 $x^2 - xy + y^2$ 은 홀수이므로, $z = ab$를 가지고

$$\begin{cases} x+y = 2^m a^3 \\ x^2 - xy + y^2 = b^3 \end{cases}$$

가 되는 홀수인 서로 소인 정수들 $a, b$가 존재한다.

$x+y,\ x-y$은 짝수이기 때문에, $b^3 = (\frac{x+y}{2})^2 + 3(\frac{x-y}{2})^2$ 으로 써도 좋다.

보조정리 4.3.2 로부터,

$\frac{x+y}{2} + \frac{x-y}{2}\sqrt{-3} = (t + w\sqrt{-3})^3$ 과

$$\begin{cases} \frac{(x+y)}{2} = t\,(t^2 - 9w^2), \\ \frac{(x-y)}{2} = 3w(t^2 - w^2), \\ b = t^2 + 3w^2 \end{cases}$$

되는 정수들 $t,\ w$가 존재한다.

만약 $t = 0$ 또는 $t^2 - 9w^2 = 0$이면 $x = -y$이고 $z = 0$이다.

만약 $w = 0$ 또는 $t^2 - w^2 = 0$이면 $x = y = 0$ 또는 $m = 1$인 상태로는 $x = y = z = \pm 1$이다.

이것은 가정에 의해 제외되어지므로, $|t^2 - 9w^2| \neq 1$을 얻는다.

왜냐하면, $|t^2 - 9w^2| = 1$ 이면 $t + 3w = \pm 1$ 인데 계산해 보면 이것은 불가능하므로 $3 \nmid t$를 갖는다 ( $\because$ $3 \mid t$이면 $3 \mid b$ ).

따라서, $3 \mid z$가 되어 가정에 모순이다.

$b$가 홀수이기 때문에, $t+3w$, $t-3w$는 0이 아닌 쌍마다 서로 소인 정수들이다.

$2^{m-1}a^3 = t(t+3w)(t-3w)$ 로부터,

$$\begin{cases} t = 2^{m-1}c^3 \\ t+3w = d^3 \\ t-3w = e^3 \end{cases}$$

이 되는 0이 아닌 정수 $c$, $d$, $e$가 존재한다.

그래서 $a = cde$ 상태를 가진 $c, d, e$은 홀수인 쌍마다 서로 소이다.

따라서 $d^3 + c^3 = 2^m c^3$이므로 $(d, e, c)$는 주어진 방정식의 해이다.

그러나 $2^{m-1}|c^3| = |t| < |t|\,|t^2 - 9w^2| = 2^{m-1}|a^3|$ 이다. 따라서 $|c| < |a|$이다. 더욱이, $2^m|a|^3 = |x+y| \le |x+y|\,|x^2 - xy + y^2| = |x^3 + y^3| = 2^m|z|^3$이다.

따라서, $|c| < |z|$이다.

$3 \nmid c$이기 때문에, 해$(d,\ e,\ c)$를 가지고 이 논법을 되풀이 하면,

모든 $c_i$는 0이 아닌 정수들인 $|z| > |c_1| > |c_2| > \cdots$ 을 가진 해의 수열 $(d_1, e_1, c_1), (d_2, e_1, c_2), \cdots$ 이 만들어진다. 이것은 불가능하다.

**case 2)** $3 \mid z$

$\gcd(x+y,\ x^2 - xy + y^2) = 3$이다. $3^2 \nmid x^2 - xy + y^2 = (x+y)^2 - 3xy$이다 ; 그렇지 않으면 $3 \mid xy$이다. 따라서, $3 \mid x$, $3 \mid y$ 이다. 이것은 모순이다. 그러므로 $3 \nmid b$와 $z = 3ab$를 가지고

$$\begin{cases} x+y = 2^m 3^2 a^3 \\ x^2 - xy + y^2 = 3b^3 \end{cases}$$

이 되는 홀수인 쌍마다 서로 소인 정수들 $a, b$가 존재한다.

$x+y$, $x-y$은 짝수이고 $3 \mid x+y$이기 때문에, $3b^3 = \left(\frac{(x+y)}{2}\right)^3 + 3\left(\frac{(x-y)}{2}\right)^2$

으로 써도 좋다.

그러므로, $b^3 = (\frac{(x-y)}{2})^3 + 3(\frac{(x+y)}{6})^2$ 이다.

보조정리 4.3.2로부터 $\frac{x-y}{2} + \frac{x+y}{6}\sqrt{-3} = (t + w\sqrt{-3})^3$ 이고

$$\begin{cases} \frac{(x-y)}{2} = t(t^2 - 9w^2), \\ \frac{(x+y)}{6} = 3w(t^2 - w^2), \\ b = t^2 + 3w^2 \end{cases}$$

되는 정수들 $t$, $w$가 존재한다.

만약 $t=0$ 또는 $t^2 - 9w^2 = 0$이면, $x = y = 0$ 또는 $m = 1$인 상태에서는 $x = y = z = \pm 1$이다.

만약 $w = 0$ 또는 $t^2 - w^2 = 0$이면, $x = -y$이다. 따라서 $z = 0$이다.

이것은 가정에 의해 제외되어지므로, $|t^2 - w^2| \neq 1$임을 얻는다.

만약 $|t^2 - w^2| = 1$ 이면 $t + w = \pm 1$, $t - w = \pm 1$이 되는데 이것이 불가능함을 쉽게 보일 수 있다.

$b$가 홀수이기 때문에, $t + 3w$, $t - 3w$도 홀수이다 (이상은 $b = t^2 + 3w^2$가 홀수이므로 $t, w$가 다른 패러티를 갖기 때문이다).

따라서 $w$, $t - w$, $t + w$은 0이 아닌 쌍마다 서로 소인 정수들이다.

$2^{m-1}a^3 = \frac{(x+y)}{18} = w(t-w)(t+w)$로부터,

$$\begin{cases} w = 2^{m-1} \\ t + w = d^3 \\ t - w = e^3 \end{cases}$$

이고 $a = cde$인 $c, d, e$는 홀수이고 쌍마다 서로 소가 되는 0이 아닌 정수들 $c, d, e$가 존재한다.

그러므로 $d^3 - e^3 = 2w = 2^m c^3$이다. 그래서 $(d, -e, c)$은 주어진 방정식의 해

이다. 그런데 $2^{m-1}|c|^3 = |w| < |w||t^2-w^2| = \dfrac{|x+y|}{18} = 2^{m-1}|a^3|$.

따라서 $|c| < |a|$이다.

또한, $2^m\ 3^2|a|^3 = |x+y| \le \dfrac{|x+y||x^2-xy+y^2|}{3} = \dfrac{|x^3+y^3|}{3} = \dfrac{2^m|z|}{3}$ 이다.

따라서, $|c| < |a| \le \dfrac{|z|}{3}$ 이다.

3이 $c$를 나누는지 안 나누는지에 따라, 첫 번째 또는 두 번째 경우의 논법을 되풀이 한다.

이것은 $|z| > |c_1| > |c_2| > \cdots$ 인 모든 $c_i$는 0이 아닌 정수인 해의 수열 $(d_1, e_1, c_1)$, $(d_2, e_1, c_2)$, $\cdots$ 을 만든다. 이것은 불가능하다.

이제 우리는 페르마의 3차 방정식이 $Q(\sqrt{-3})$에서 오직 자명한 해만 갖는다는 가우스의 증명을 줄 것이다.

복소수 $a+b\sqrt{-3}$ ( $a, b \in Q$ ) 의 집합은 체(field)를 구성하는데 Eisenstein field라하고 $K = Q(\sqrt{-3})$로 표시한다. 두 수 $a, b$가 같은 패러티의 보통의 정수인 수 $\alpha = \dfrac{(a+b\sqrt{-3})}{2}$ 를 $K$의(대수적) 정수라고 부른다.

오일러의 증명에서 보완해야 할 부분은 $\gcd(p, q) = 1$이고 $p = a^3 - 9ab^2$, $q = 3a^2 - 3b^2$ 이라고 놓을 때 $p^2 + 3q^2$ 이 세제곱이 되는 정수 $a, b$가 존재하는가 하는 점이다. 이 문제의 해결을 위해 오일러가 사용했던 방법은 정수 $a$ 와 $b$ 에 대해 $a+b\sqrt{-3}$ 형태의 수들을 연산에 이용함으로써 수의 연산범위를 확장하는 생각에 기초를 두고 있다.

$p^2 + 3q^2 = (p+q\sqrt{-3})(p-q\sqrt{-3}) = [(a+b\sqrt{-3})(a-b\sqrt{-3})^3] = (a^2+3b^2)^3$ 이 된다.

다른 말로 말하자면 $p^2+3q^2$이 세제곱이 되기 위해서는
$p+q\sqrt{-3}=(a+b\sqrt{-3})^3$임을 보여주는 것만으로 충분하다.
따라서 "$\gcd(p,\ q)=1$이고 $p^2+3q^2$이 세제곱이라고 가정하면
$p+q\sqrt{-3}=(a+b\sqrt{-3})^3$을 만족하는 정수 $a$와 $b$가 존재한다." 라는 정리가 증명되어서 페르마는 $x^3+y^3=z^3$이 되는 $0$이 아닌 정수 $x, y, z$은 없다를 완벽하게 보였다.

## 4.4. $n=5$인 경우의 증명 (( $X^5+Y^5=Z^5$ ))

오일러는 허수 $i$를 증명과정에 도입함으로써 논리의 허점을 성공적으로 보완하였고, 무한하강법을 이용하여 $n=3$인 경우에 페르마의 마지막 정리를 증명하였다. 그러나 $n=5$이상인 경우에는 오일러의 방법도 전혀 효과가 없었다.
$n=5$인 경우는 Dirichlet에 의해 처음 해결됐다.

1828년에 발표된 그의 증명은 모든 가능한 경우를 고려하지 않았다. 그래서 Legendre는 완전히 독립적인 증명을 발표했다. 반면에 Dirichlet는 마지막으로 남아있는 경우를 해결할 수 있었다. 이 두 사람이 사용했던 논리의 배경은 S. Germain이 제안했던 방법이었다.

S. Germain은 $100$보다 작은 모든 소수 $p$에 대하여 페르마의 정리가 참임을 확립했던 새로운 종류의 정리를 증명했다. 그녀의 정리는 특정한 $n$값이 아니고 모든 $n$값에 적용될 수 있는 어떤 일반적인 사실을 밝히고 그 뒤에 정수론 학자들은 그녀의 아이디어를 개개의 소숫값에 대하여 페르마의 마지막 정리를 증명해 나가기 시작했다.

아래의 증명을 위해, $A$를 다음과 같이 정의할 수 있다.
$A$를 $Q(\sqrt{5})$의 정수의 환(the ring of integers)이라 하자.
$A$의 원소는 $\dfrac{a+b\sqrt{5}}{2}$(여기서, $a, b$는 같은 패러티의 정수이다) 형태이다.
$A$는 곱셈 군을 형성한다.

$\frac{a+b\sqrt{5}}{2}$가 단원이기 위한 필요충분조건은 이것의 노름(norm)

$(\frac{a+b\sqrt{5}}{2})(\frac{a-b\sqrt{5}}{2}) = \frac{a^2-5b^2}{4}$이 $\pm 1$인 경우이다(즉, $a^2-5b^2=\pm 4$).

$A$의 단원들은 정확히 $\pm(\frac{1+\sqrt{5}}{2})^e$ ($e$는 임의의 정수) 형태임을 보일 수 있다. 증명에 요구되는 중요한 사실은 $A$의 모든 원소가 소원의 멱의 곱으로 유일하게 (단원을 무시하고)쓰여 진다는 것이다.

**정리 4.4.1**

(1) $a$, $b$를 $\gcd(a, b)=1$, $a \not\equiv b \pmod 2$, $5 \nmid a$, $5 \mid b$인 0이 아닌 정수들이라 하자.

만약 $a^2-5b^2$가 $A$의 어떤 원소의 5제곱이면,

$$\begin{cases} a = c\,(c^4+50c^2d^2+125d^4), \\ b = 5d\,(c^4+10c^2d^2+5d^4), \end{cases}$$ 이고

$\gcd(c, d)=1$, $c \not\equiv d \pmod 2$, $5 \nmid c$가 되는 0이 아닌 정수들 $c$, $d$가 존재한다.

(2) $a$, $b$를 $\gcd(a, b)=1$, $a$, $b$는 둘 다 홀수, $5 \nmid a$, $5 \mid b$가 되는 정수들이라 하자.

만약 $\frac{a^2-5b^2}{4}$ 가 $A$의 어떤 원소의 5제곱이면,

$$\begin{cases} a = \dfrac{c\,(c^4+50c^2d^2+125d^4)}{16}, \\ b = \dfrac{5d\,(c^4+10c^2d^2+5d^4)}{16}, \end{cases}$$

이고 $\gcd(c, d)=1$, $c, d$는 모두 홀수, $5 \nmid c$가 되는 0이 아닌 정수들 $c$, $d$가 존재한다.

**정리 4.4.2**

$X^5+Y^5+Z^5=0$은 모두 0이 아닌 정수들의 해를 갖지 않는다.

**(증명)** $x^5+y^5+z^5=0$이 되는 0이 아닌 정수들 $x, y, z$라 존재한다고 가정한다. 우리는 $\gcd(x, y, z)=1$이라고 가정해도 좋다. 또한 $x, y, z$은 쌍마다 서로소라고 가정해도 좋다.

**case 1)** $5 \nmid xyz$

$x, y, z$은 5를 법으로 하여 $\pm 1$또는 $\pm 2$와 합동이다.

$x^5 \equiv x \pmod 5$, $y^5 \equiv y \pmod 5$, $z^5 \equiv z \pmod 5$ 이기 때문에,

$x+y+z \equiv x^5+y^5+z^5 = 0 \pmod 5$.

만약 $x, y, z$는 5를 법으로 하여 쌍마다 비합동이면, $x+y+z \not\equiv 0$ 이다.

왜냐하면, 예를 들어 $x \equiv y \pmod 5$이면 $-z \equiv x+y \equiv 2x \pmod 5$이다.

$\Rightarrow$ $x^5 \equiv y^5 \pmod{5^2}$, $-z^5 = 2^5x^5 \pmod{5^2}$.

$-z^5 = x^5+y^5 \equiv 2x^5 \pmod{5^2}$.

그러므로 $2^5x^5 = 2x^5 \pmod{5^2}$, $2^5 = 2 \pmod{5^2}$. 이것은 모순이다.

따라서 $0 \not\equiv x+y+z \equiv x^5+y^5+z^5 = 0 \pmod 5$.

**case 2)** $5 \mid z$ (예를 들어) 그러면 $5 \nmid xy$이다.

$\gcd(x, y)=1$이기 때문에, $x$와 $y$는 둘 다 홀수이든지 또는 다른 패러티를 갖든지 둘 중의 하나이다.

① $x$와 $y$는 둘 다 홀수인 경우

가정에 의해 $2 \mid z$, $5 \mid z$ 이다.

$z=2^m5^nz'$ ($m \geq 1$, $n \geq 1$, $z'$은 2 또는 5의 배수가 아니다)로 쓴다.

$z$를 $z'$로 치환하여, $-2^{5m}5^{5n}z^5 = x^5+y^5$가 되는 0이 아닌 쌍마다 서로 소인 정수 $x, y, z$가 존재한다고 해도 된다 (여기서 $x, y, z$은 홀수이고 5의 배수

가 아니다)로 쓴다.

$x+y=2p,\quad x-y=2q$ ($p$, $q$은 0이 아닌 정수들)로 놓는다.

그래서 $x=p+q,\quad y=p-q$ ( $\gcd(p,\ q)=1$, $p, q$은 모두가 홀수는 아니다).

$-2^{5m}5^{5n}z^5=(p+q)^5+(p-q)^5=2p(p^4+10p^2q^2+5q^4)$.

$5 \mid p$ 또는 $5 \mid p^4+10p^2q^2+5q^4$ 이기 때문에, $5 \mid p$이다. $p=5r$로 쓴다.

$5 \nmid q$이고 $\gcd(r,\ q)=1$ ($q$, $r$은 다른 패러티를 갖는다)이다.

그러므로 $-2^{5m}5^{5n}z^5=2\cdot 5^2 r(q^4+50q^2r^2+125r^4)$

$t=q^4+50q^2r^2+125r^4=(q^2+25r^2)^2-5(10r^2)^2$로 놓는다.

$u=q^2+25r^2,\quad v=10r^2$로 놓는다.

따라서 $u, v$은 0이 아니고, $u$는 홀수, $10 \mid v$, $\gcd(u,\ v)=1$.

그러면 $t$는 홀수, $5 \nmid t$, $\gcd(t,\ r)=1$이고 $5n>2$이기 때문에 $5 \mid r$ 이다.

$\gcd(2\cdot 5^2 r,\ t)=1$이므로 $2\cdot 5^2 r$과 $t$는 정수의 5제곱들이다.

그러나 $t=u^2-5v^2$ ($u \not\equiv v \pmod 2$), $\gcd(u,\ v)=1$, $5 \nmid u$, $5 \mid v$ ).

정리 4.4.1에 의해

$$\begin{cases} a=c(c^4+50c^2d^2+125d^4), \\ b=5d(c^4+10c^2d^2+5d^4), \end{cases}$$

이고 $\gcd(c,\ d)=1$, $c \not\equiv d \pmod 2$, $5 \nmid c$가 되는 0이 아닌 정수들 $c, d$가 존재한다. 이것으로부터 $5 \mid d$이다. $5 \mid r$이기 때문에, $5^3 \mid v$이다.

또한 $v=10r^2$이므로 $d>0$이다.

$2\cdot 5^3$을 마지막 관계식에 곱하면,

$(2\cdot 5^2 r)^2=2\cdot 5^3\cdot 10r^2=2\cdot 5^4 d(c^4+10c^2d^2+5d^4)$이고

$2\cdot 5^2 r$은 5제곱이기 때문에 $2\cdot 5^2\cdot r$은 5제곱이다.

그러나 $(c^4+10c^2d^2+5d^4)$은 홀수이고 $5 \nmid c$, $\gcd(c,\ d)=1$, 이기 때문에

$\gcd(2\cdot 5^4 d^4,\ c^4+10c^2d^2+5d^4)=1$이다.

따라서 $2\cdot 5^4 d$와 $c^4+10c^2d^2+5d^4=(c^2+5d^2)^2-5(2d^2)^2$은 5제곱들이다.

여기서 $c^2+5d^2$ 과 $2d^2$은 홀수가 아니고,

$\gcd(c^2+5d^2,\ 2d^2)=1, 5 \nmid c^2+5d^2,\quad 5 \mid 2d^2$이고 정리 4.4.1.에 의해서,

$$\begin{cases} c^2+5d^2 = c'(c'^4+50c'^2d'^2+125d'^4), \\ 2d^2 = 5d'(c'^4+10c'^2d'^2+5d'^4), \end{cases}$$ 이고

$\gcd(c',\ d')=1,\ c' \not\equiv d' \pmod 2,\ 5 \nmid c'$가 되는 0이 아닌 정수들 $c',\ d'$가 존재한다.

이것으로부터 $5^2 \mid d^2$이므로, $5 \mid d'$이고 $d'>0$이다.

$2 \cdot 5^8$을 마지막 관계식에 곱하여

$2^2\,5^8\,d^2\,(2 \cdot 5^4 d)^2 = 2 \cdot 5^9 d'(c'^4+10c'^2d'^2+5d'^4)$이다.

이 수는 5제곱이다.

$\gcd(2 \cdot 5^9 d',\quad c'^4+10c'^2d'^2+5d'^4)=1$이므로,

$2 \cdot 5^9 d'$와 $c'^4+10c'^2d'^2+5d'^4$은 5제곱들이다.

이것은 $2 \cdot 5^4 d$와 $c^4+10c^2d^2+5d^4$도 또한 5제곱임은 이전의 주장과 비슷하다. 더욱이, $25d'^5 \le 5d'(c'^4+10c'^2d'^2+5d'^4)=2d^2$ 이기 때문에,

$0 < d' \le \sqrt[5]{\dfrac{(2d^2)}{25}} < d$ 이고, 이 절차가 계속 된다면, $0<d''<1$인 정수 $d''$에 도달할 것이다. 이것은 불가능하다. 따라서 남아있는 것은 $x$와 $y$가 다른 패러티를 갖는 경우를 생각하는 것이다.

② $x$와 $y$가 남은 패러티를 갖는 경우

여기서 계산에 대한 상세한 몇 가지는 생략한다.

$x+y=p,\quad x-y=q$라 놓으면 $p,\ q$는 홀수,

$\gcd(p,\ q)=1,\quad 2x=p+q,\quad 2y=p-q$ 이다.

그러면 $-2^5\,5^{5n}z^5 = 2p\,(p^4+10p^2q^2+5q^4)$이다.

$5 \mid p$이므로 $p=5r$로 쓰고, $5 \nmid q$ , $\gcd(q,\ r)=1,\quad q, r$은 둘 다 홀수,

$-2^5 \cdot 5^{5n}z^5 = 2 \cdot 5^2 \cdot r \cdot t$

$(t=q^4+50q^2r^2+125r^4=u^2-5v^2,\quad u=q^2+25r^2,\quad v=10r^2)$이다.

그러면 $u, v$는 0이 아닌 짝수이고, $u = 2 \pmod 4$, $5 \nmid t$, $\gcd(r, t) = 1$.
$5n > 2$이므로 $5 \mid r$.
$u = 2u'$, $v = 2v'$, $u', v'$은 홀수, $\gcd(u', v') = 1$, $5 \nmid u'$, $5 \nmid v'$.
만약 $t' = \frac{t}{4} = u'^2 - 5v'^2$ 이면 $t' \equiv 0 \pmod 4$이고 $\gcd(5^2 r, \frac{t'}{4}) = 1$인
$-5^{5n} z^5 = \frac{5^2 r t'}{4}$. 그래서 $5^2 r$, $\frac{t'}{4} = \frac{(u'^2 - 5v'^2)}{4}$은 5제곱들이다.

정리 4.4.1에 의해서,

$$\begin{cases} u' = \dfrac{c(c^4 + 50c^2d^2 + 125d^4)}{16}, \\ v' = \dfrac{5d(c^4 + 10c^2d^2 + 5d^4)}{16}, \end{cases}$$

이고 $\gcd(c, d) = 1$, $c, d$는 모두 홀수, $5 \nmid c$가 되는 0이 아닌 정수들 $c, d$가 존재한다.

또한 $5 \mid r$이기 때문에 $5^2 \mid v'$, $5 \mid d$, $d > 0$이다.
$5^3$을 마지막 관계식에 곱하면,
$(5^2 r)^2 = 5^3 v' = \frac{5^4 d}{4} \left[ \left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4 \right]$ 이 성립한다
( 여기서, $\left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4 \equiv 0 \pmod 4$ ).
우변에 있는 두 인수는 서로 소이고 $(5^2 r)^2$은 5제곱이기 때문에,
$s^4 d$와 $\frac{1}{4} \left[ \left(\frac{(c^2 + 5d^2)}{2}\right)^2 - 5(d^2)^2 \right]$는 5제곱들이다.

정리 4.4.1에 의해서, $\begin{cases} \dfrac{c^2+5d^2}{2} = \dfrac{c'(c'^4+50c'^2d'^2+125d'^4)}{16}, \\ d^2 = \dfrac{5d'(c'^4+10c'^2d'^2+5d'^4)}{16}, \end{cases}$

이고 $\gcd(c',\ d')=1$, $c'$와 $d'$는 모두 홀수, $5 \nmid c'$가 되는 0이 아닌 정수들 $c'$, $d'$가 존재한다.

이것으로부터 $5 \mid d'$이고 $d' > 0$이다.

$5^8$을 마지막 방정식에 곱하면

$5^8 d^2 = \dfrac{5^9 d'(c'^4+10c'^2d'^2+5d'^4)}{16} = \dfrac{5^9 d'}{16}\left[\left(\dfrac{c'^2+5d'^2}{2}\right)^2 - 5(d'^2)^2\right]$이다.

다시 $5^9 d'$와 $\dfrac{1}{4}\left[\left(\dfrac{c'^2+5d'^2}{2}\right)^2 - 5(d'^2)^2\right]$은 5제곱들이다.

①의 경우와 똑같이 하여, $0 < d'' < d$ 에 이른다. ( $\because$ $25d'^2 \le 16d^2$ )

이 과정을 계속적으로 진행하면 모순이 생긴다.

위의 정리를 확장하면 다음과 같은 정리가 나온다.

**정리 4.4.3.**

방정식 $X^5 + Y^5 + Z^5 = 0$ 은 $Q(\sqrt{5})$의 정수의 해는 자명한 해 뿐이다 ([2]).

## 4.5. $n=6$인 경우의 증명 (( $X^6 + Y^6 = Z^6$ ))

$n=6$인 경우는 Breusch(1960년)에 의해 증명되었다.

**정리 4.5.1**

$x^2+y^2=u^2+v^2$이고 $xy=2uv$가 되는 양의 정수 $x, y, u, v$가 존재하지 않는다.

**정리 4.5.2**

$x^6+y^6=z^6$이 되는 양의 정수들 $x, y, z$가 존재하지 않는다.

**(증명)** 존재한다고 가정하여, $x, y, z$는 $x^6+y^6=z^6$이 되는 쌍마다 서로 소인 양의 정수들의 해라고 하자. 그러면 $3 \nmid x$, $3 \nmid y$일 수 없다. 따라서 $3 \nmid x$이라고 가정해도 된다.

$x^6=z^6-y^6=(z+y)(z-y)(z^2+zy+y^2)(z^2-zy+y^2)$

위 식에서 각 인수 $z^2+zy+y^2$, $z^2-zy+y^2$은 홀수이고, 우변의 다른 세 인수와 서로 소이다.( $\because$ $3 \nmid x$ )

그러므로 유일인수분해정리에 의해

$$\begin{cases} z^2+zy+y^2=b^2 \\ z^2-zy+y^2=c, \quad b>c>0 \end{cases}$$

이 되는 $b, c$가 존재한다.

이들 관계식을 더하고 빼면, $2(z^2+y^2)=b^6+c^6$, $2zy=b^6-c^6$을 갖는다.

그러나 $b, c$는 홀수이다.

따라서, $b^3+c^3=2m$, $b^3-c^3=2n$ $(m>0, \ n>0)$.

제곱하여 더하면, $b^6+c^6=2(m^2+n^2)$이고, 제곱하여 곱하면, $b^6-c^6=4mn$을 얻는다. 그러므로 $z^2+y^2=m^2+n^2$, $zy=2mn$이다.

정리 4.5.1에 의하여 이것은 불가능하다([2]).

## 4.6. $n=7$인 경우의 증명 (( $X^7+Y^7=Z^7$ ))

1839년에 Lame는 지수 7에 대한 페르마의 정리를 증명했다.

그러나 는 Lame는 7자체와 매우 밀접하게 관련된 아주 교묘한 방법에 의존해야

만 했다. 그리고 Lame는 '원분 정수'의 개념을 도입해서 다른 경우들을 증명하려고 시도했지만 실패했다.

Lebesgue는 1840년에 더 간단한 증명을 했다. Genocchi는 Legendre가 이미 발견했던 생각 (1830)을 이용하여 1874년과 1876년에 한층 더 간단한 증명을 생각해냈다.

**정리 4.6.1**

(1) 만약 $x, y, z$가 유리수 계수를 갖는 3차방정식의 근이면, $x^7+y^7+z^7=0$의 $x, y, z$은 $xyz=0$이든지 또는 (적당한 순서에 의해) 1의 3제곱들 (즉, $1$, $\zeta=\frac{1-\sqrt{3}}{2}$, $\eta=\frac{-1+\sqrt{-3}}{2}$ )에 비례하든지 둘 중의 하나가 성립한다.

(2) 방정식 $x^7+y^7+z^7=0$은 오직 자명한 정수해만을 갖는다.

**(증명)** $x, y, z$가 $f(x)=X^3-pX^2+qX-r$, $p, q, r \in Q$ 의 근이라고 가정하면 $p=x+y+z$, $q=xy+yz+xz$, $r=xyz$

**case 1)** $p=0$

우리는 다음과 같은 항등식을 이용해본다 :

$(X+Y)^7-X^7-Y^7=7XY(X+Y)(X^2+XY+Y^2)^2$ 만약 $x+y+z=0$이고 $x^7+y^7+z^7=0$이면, $7xy(x+y)(x^2+xy+y^2)^2=0$ 이다.

그러므로 $x=0$ 또는 $y=0$이든지, $x+y+z=0$에서 $z=-(x+y)=0$이든지, 또는 $xyz\neq 0$, $x^2+yx+y^2=0$ 이든지 셋 중의 하나가 성립하게 된다.

앞의 두 경우이면 성립하기 때문에, 세 번째가 성립하는 경우를 조사해보자.

$(\frac{y}{x})^2+\frac{y}{x}+1=0$이다. 따라서 $\frac{y}{x}(\neq 1)$은 1의 세제곱근이다.

$y=x\zeta$ ( 또는 $y=x\eta$ )이다. $z=-(x+y)=-x(1+\zeta)=x\eta$ ( 또는 $x\zeta$ )이다. 따라서, $x, y, z$는 $1, \zeta, \eta$ 또는 $1, \eta, \zeta$ 에 비례한다.

case 2) $p \neq 0$. $k > 1$에 대하여 $s_k$는 $f(X) = 0$의 근의 $k$제곱의 합 $x^k + y^k + z^k$이라 놓는다.

뉴턴의 공식[3]에 의해,

$s_1 = p$,
$s_2 = s_1 p - 2q$,
$s_3 = s_2 p - s_1 q + 3r$,
$s_4 = s_3 p - s_2 q + s_1 r$,
$s_5 = s_4 p - s_3 q + s_2 r$,
$s_6 = s_5 p - s_4 q + s_3 r$,
$s_7 = s_6 p - s_5 q + s_4 r$,

대입하면 다음을 얻는다 :

$x^7 + y^7 + z^7 = p^7 - 7p^5 q + 7p^4 r + 14p^3 q^2 - 21p^2 qr - 7pq^3 + 7pr^2 + 7q^2 r = 0$

$m = pq - r \in Q$ 라 놓으면,

$x^7 + y^7 + z^7 = p^7 - 7(pq - r)(p^4 - p^2 q + q^2) + 7(pq - r)^2 p = p^7 - 7m(p^4 - p^2 q + q^2) + 7m^2 p = 0$

$\frac{q}{p^2} = Q$, $\frac{m}{p^3} = M$이라 놓으면,

$p^7 - 7p^3 M(p^4 - p^4 Q - p^4 Q^2) + 7p^2 M^2 = 0$

따라서 $M^2 - M(1 - Q + Q^2) + \frac{1}{7} = 0$

$M$은 유리수이므로, 판별식 $(\frac{(1 - Q + Q^2)}{2})^2 + \frac{1}{7} = 0$은 0이 아닌 유리수의 제곱이다.

---

3) $s_v = \sum X_i^{\,v}$ 라 하면,
$s_1 = \sigma_1$
$s_2 = \sigma_1^{\,2} - 2\sigma_2$
$s_3 = \sigma_1^{\,3} - 3\sigma_1\sigma_2 + 3\sigma_3$
$s_4 = \sigma_1^{\,4} - 4\sigma_1^{\,2}\sigma_2 + 2\sigma_2^{\,2} + 4\sigma_1\sigma_3 - 4\sigma_4$인 기본대칭식과 $s_v$와의 사이에는 다음의 관계가 있다.
$s_v - \sigma_1 s_{v-1} + \sigma_2 s_{v-2} - \cdots + (-1)^{v-1}\sigma_{v-1} s_1 + (-1)^v v s_v = 0$ $(v = 1, 2, \cdots n)$,
$s_u - \sigma_1 s_{u-1} + \cdots + (-1)^n \sigma_n s_{u-n} = 0$ $(u = n+1,\ n+2,\ \cdots)$([7]).

$2Q-1=\frac{s}{t}$ (여기서, $s$, $t$ 는 서로 소인 정수들로 $t>0$ ) 라 놓는다.

그러면 $Q=\frac{(t+s)}{2t}$. $64\,t^4\,[\,(\frac{(3t^2+s^2)}{8t^2})^2-\frac{1}{7}\,]=s^4+6t^2s^2-\frac{t^4}{7}=u^2$

($u$는 0이 아닌 유리수)이다.

$7u^2$은 정수이기 때문에, $u$는 정수이고, $7\mid t$.

따라서, $7\nmid s$ (왜냐하면 $s,t$는 서로 소인 정수들이기 때문이다.)

$t=7^e v$, $e\geq 1$, $7\nmid v$라고 하자.

그러면 $s^4+6\cdot 7^{2e}v^2s^2-7^{4e-1}v^4=u^2$ -------- (6-1)

위의 (6-1)로 부터, $(s^2+3\cdot 7^{2e}v^2)^2-u^2=64\cdot 7^{4e-1}v^4$ --------- (6-2)

이므로 $(s^2+3\cdot 7^{2e}v^2+u)\,(s^2+3\cdot 7^{2e}v^2-u)=64\cdot 7^{4e-1}v^4$-------- (6-3)

여기에서 우리는 $\gcd(s^2+3\cdot 7^{2e}v^2+u,\ s^2+3\cdot 7^{2e}v^2-u)$는 2의 거듭제곱임을 보이자. $p\,(\neq 2)$를 $p\mid s^2+3\cdot 7^{2e}v^2+u$, $p\mid s^2+3\cdot 7^{2e}v^2-u$가 되는 소수라고 하자.

만약 $p=7$이면, $e\geq 1$이기 때문에, $7=p\mid s$ 이지만, 위의 $7\nmid s$에 모순이다.

만약 $p\neq 7$이면, (6-3)에 의해서, $p\mid 64\cdot 7^{4e-1}v^4$, $p\mid v$이고, $7\nmid v$에 모순이다.

그러므로 (6-3)에 있는 좌변의 gcd는 2의 거듭제곱이다.

① $v$는 홀수인 경우

(6-3)으로부터, $\begin{cases} s^2+3\cdot 7^{2e}v^2\pm u=7^{4e-1}A\,a^4, \\ s^2+3\cdot 7^{2e}v^2\mp u=B\,b^4, \end{cases}$ --------- (6-4)

(여기서 $a,b$는 서로 소인 정수이고 $ab=v$($a,b$는 홀수), $A,B$는 짝수, $AB=64$).

위의 (6-4)로부터, $2s^2+6\cdot 7^{2e}v^2=7^{4e-1}A\,a^4+Bb^4$ -------- (6-5)

만약 $x$가 홀수라면, $x^2 \equiv 1 \pmod 8$임을 주목하면,

$$s^2 \equiv -3 \cdot 7^{2e} a^2 b^2 + 7^{4e-1} \cdot \frac{A}{2} a^4 + \frac{B}{2} b^4 \equiv -3 - \frac{A}{2} + \frac{B}{2} \pmod 8.$$

여기에서 $A, B$에 대한 여러 가능성을 생각해 보자.

$A = 32, \quad B = 2 \rightarrow s^2 \equiv -2 \pmod 8$, 불가능,
$A = 16, \quad B = 4 \rightarrow s^2 \equiv -1 \pmod 8$, 불가능,
$A = 8, \quad B = 8 \rightarrow s^2 \equiv -3 \pmod 8$, 불가능,
$A = 4, \quad B = 16 \rightarrow s^2 \equiv 3 \pmod 8$, 불가능,
$A = 2, \quad B = 32 \rightarrow s^2 \equiv 4 \pmod 8$,

마지막 경우에, (6-5)는 $s^2 + 3 \cdot 7^{2e} v^2 = 7^{4e-1} a^4 + 16 b^4$이 된다. 64를 양변에 곱하면, $64 s^2 + 6 \cdot 7^{2e} \cdot 32 a^2 b^2 - 64 \cdot 16 b^4 = 7^{4e-1} \cdot 64 a^4$이고
$64 s^2 - (32 b^2 - 3 \cdot 7^{2e} a^2)^2 = 7^{4e-1} \cdot 64 a^4 - 7^{4e} \cdot 3^2 a^4 = 7^{4e-1} \cdot a^4$이다.
그러므로 $(8s + 32 b^2 - 3 \cdot 7^{2e} a^2) = (8s - 32 b^2 + 3 \cdot 7^{2e} a^2) = 7^{4e-1} a^4$ ------ (6-6)
우리는 $\gcd(8s + 32 b^2 - 3 \cdot 7^{2e} a^2,\ 8s - 32 b^2 + 3 \cdot 7^{2e} a^2) = 1$임을 주장한다.
$a$가 홀수이므로, 위의 수들은 다 홀수이다.
만약 $p$가 이 두 수의 gcd이면, $p \mid 16s$, $p \mid s$이고, $p \mid 32 b^2 - 3 \cdot 7^{2e} a^2$, $p \mid 7^{4e-1} a^4$ ((6-6)에 의해)이다.

만약 $p = 7$이면, $p = 7 \mid s$이지만, $7 \nmid s$에 모순이다.
만약 $p \neq 7$이면, $p \mid a$, $p \mid b$인데, $a, b$가 서로 소인 것에 모순이다.
이것은 최대공약수가 1임을 증명한다.

따라서 $\begin{cases} 8s \pm 32 b^2 \mp 3 \cdot 7^{2e} a^2 = c^4 \\ 8s \pm 32 b^2 \pm 3 \cdot 7^{2e} a^2 = 7^{4e-1} d^4 \end{cases}$ -------- (6-7)

여기서 $c, d$는 서로 소인 정수이고 $cd = a$ ($c, d$는 홀수)이다.
(6-7)로부터 $\mp 3 \equiv c^4 \pmod 8$이 유도되는데 이것은 불가능하다.

그러므로 ①의 경우가 불가능하다.

② $v$는 짝수인 경우

$t=7^e v$가 짝수이므로 $s$는 홀수이고, (6-2)에 의해 $u$또한 홀수이다.

이 경우, 우리는 (6-2)를 $(s^2+3\cdot 7^{2e}v^2)^2-u^2=4\cdot 7^{4e-1}\cdot(2v)^4$으로 쓴다.

그리고 (6-3)의 두 인자는 짝수임을 알 수 있고, $e\geq 2$에 대하여 $2^e$이 최대공약수이면, $2^e \mid s^2+u$, $2^e \mid s^2-u$이다. $s^2+u=l\,2^e$, $s^2-u=m\,2^e$이 되는 정수들 $l$, $m$이 존재한다.

$-u+l\,2^e=m\,2^e+u$, $2u=(l-m)\,2^e$, $u=(l-m)2^{e-1}$. $u$는 짝수이다. 이것은 $u$가 홀수라는 사실에 모순이다.

그러므로 두 인자의 gcd는 2임을 알 수 있다.

$$\begin{cases} s^2+3\cdot 7^{2e}v^2 \pm u=2\cdot 7^{4e-1}A^4, \\ s^2+3\cdot 7^{2e}v^2 \mp u=2\cdot B^4, \end{cases}$$

여기서 $A, B$는 서로 소인 정수이고, $AB=2v$이다.

그리고 $A$또는 $B$ 중의 하나는 짝수이다.

$$s^2=-3\cdot 7^{2e}v^2+7^{4e-1}A^4+B^4=-\frac{3}{4}\cdot 7^{2e}A^2B^2+7^{4e-1}\cdot A^4+B^4 \quad \text{-----}$$

(6-9) 이고 만약 $B$가 짝수이면, $A$는 홀수이고 $s^2\equiv -3v^2-1 \pmod 8$이다.

그러므로 $s^2\equiv -1 \pmod 4$인데 이것은 불가능하다.

만약 $A$가 짝수이면, $B$는 홀수이다. (6-4)로부터 $A=2A_1$로 놓는다.

$s^2=-3\cdot 7^{2e}A_1^2B^2+7^{4e-1}\cdot 2^4\cdot A_1^4+B^4$ 이므로

$1\equiv s^2\equiv -3A_1^2+1 \pmod 8 \Leftrightarrow 3A_1^2\equiv 0 \pmod 8$, $4 \mid A_1$이고,

$A_1=4A_2$로 놓으면 $A=8A_2$이다.

(6-9)는 $s^2=-3\cdot 16\cdot 7^{2e}\cdot A_2^2B^2+7^{4e-1}\cdot 8^4\cdot A_2^4+B^4$과 같이 쓰여진다.

따라서 $s^2-(B^2+3\cdot 8\cdot 7^{2e}\cdot A_2{}^2)^2=7^{4e-1}\cdot 8^4\cdot A_2^4-3^2\cdot 8^2\cdot 7^{4e}\cdot A_2^4$

$=7^{4e-1}\cdot 8^2 A_2^4$ -------- (6-10)

으로부터 아래와 같이 (6-11)을 준다.

$(s^2-B^2+3\cdot 8\cdot 7^{2e}\cdot A_2{}^2)\ (s+B^2-3\cdot 8\cdot 7^{2e}\cdot A_2^2)=7^{4e-1}\cdot 4\cdot (2A_2)^2$

-------- (6-11)

(6-11)의 두 약수는 짝수이고, 앞에서 한 방법대로 이들의 최대공약수는 2임을 보일 수 있다.

그러므로 $\begin{cases} s\mp B^2\pm 3\cdot 8\cdot 7^{2e}\cdot A_2{}^2=2c_2^4, \\ s\pm B^2\mp 3\cdot 8\cdot 7^{2e}\cdot A_2{}^2=7^{4e-1}\cdot 2d_2^4 \end{cases}$

이다. ---------- (6-12)

(여기서 $c_2$, $d_2$는 $c_2 d_2=2A_2$가 되는 서로 소인 정수이다.)

(6-12)로부터, $\mp B^2\pm 3\cdot 8\cdot 7^{2e}\cdot A_2{}^2=c_2{}^4-7^{4e-1}\cdot d_2{}^4$이다.

그러므로 $\pm B^2=\pm 6\cdot 7^{2e}\cdot c_2{}^2 d_2{}^2-c_2{}^4+7^{4e-1}\cdot d_2{}^4$. -------- (6-13)

7을 법으로 하는 임의의 0이 아닌 제곱은 1, 2 또는 4이기 때문에, $B^2+c_2{}^4\not\equiv 0\pmod 7$이다. 따라서 (6-13)에서 우리는 음의 부호(-)를 가져야한다.

$B^2=c_2{}^4+6\cdot 7^{2e}\cdot c_2{}^2 d_2{}^2-7^{4e-1}\cdot d_2{}^4$ --------(6-14)

이 방정식은 (6-1)과 같은 형태이고, $v=\dfrac{AB}{2}=4A_2B\geq 2c_2 d_2>\mathrm{d}_2$이다.

그래서 우리는 무한하강법에 의해 이런 방법을 계속하면, 우리는 ② 또한 불가능함을 보인다.

그러므로 case 2) 는 불가능 하고 이것으로 (1)을 증명한다.

(2) 만약 $x, y, z$가 $x^7+y^7+z^7=0$을 만족하면,

우리는 다항식 $f(X)=X^3-pX^2+qX-r$을 생각해보자.

이 다항식은 $x, y, z$를 근으로 갖는다.
(1)에 의해, $x, y, z$는 $1, \zeta, \eta$에 비례할 수 없으므로, $xyz = 0$이다([2]).

# 5장. 페르마의 마지막 정리의 증명도전사

## 1. Leonhard Euler (1707～1783 : 스위스)

무한히 많은 종류에 적용되는 법칙을 증명하기 위해서 어느 하나의 방정식에 정수해가 없음을 먼저 증명한 뒤 논리의 적용 범위를 늘려가는 그럴듯한 방법을 찾으면 페르마의 마지막 정리가 임의의 정수 $n$에 대하여 안전하게 증명되리라고 생각했다. 이미 페르마는 무한하강법으로 $n=4$인 경우를 증명해 놓았다.
그러나 오일러는 허수 $i$를 증명과정에 도입함으로써 논리의 허점을 성공적으로 보완하였고 무한하강법을 이용하여 $n=3$인 경우에 한하여 페르마의 마지막 정리를 증명했다. 이는 수학사적으로 볼 때 단단한 진보였으나 $n=5$이상인 경우에는 오일러의 방법도 전혀 효과가 없었다. $n=3, 4$일 때 성공적으로 증명된 결과를 토대로 무한하강법을 적용하려는 오일러의 시도는 결국 실패로 끝나고 말았다.

## 2. Marie-Sophie Germain (1776 ～1831 : 프랑스)

Germain은 100이하의 모든 소수 $p$에 대하여 페르마의 정리가 참 임을 확립했던 새로운 종류의 정리를 증명했다. 그녀의 정리는 특정한 $n$값이 아니고 모든 $n$값에 적용될 수 있는 어떤 일반적인 사실을 밝혔고 그 뒤로 정수론 학자들은 그녀의 아이디어를 도입하여 개개의 소숫값에 대하여 페르마의 마지막 정리를 증명해 나가기 시작했다.
Dirichlet와 Legendre는 Germain이 제안했던 방법을 이용하여 $n=5$일 때를 증명했고, 라메(G. Lame)가 1839년에 $n=7$일 때 정수해가 없음을 증명해냈다.

## 3. Ernst Eduard Kummer (1810～1893 : 독일)

“모든 정수는 소인수 분해될 수 있으며 하나의 정수를 소인수 분해하는 방법은 단 한가지뿐이다. 그러나 허수가 있는 시스템에서는 더 이상 소인수분해 이론이 맞지 않는다.”

Kummer는 자신의 이론이 대부분의 소수 $n$에 대하여 소인수분해하는 방법의 수가 유일하지 않기 때문에 야기되는 문제를 해결할 수 있음을 보였다.

자세히 설명해 보면 $n$에 31이하의 소수인 경우에는 Kummer의 논리가 잘 적용되어 아무런 문제가 없었으나, 그의 이론 역시 모든 소수에 대해 성립하지는 않는데 특히 $n=37$일 때는 맞지 않았다. 100이하의 소수들 중에서 $n=59$와 $n=67$인 경우 역시 맞지 않았기 때문에 Kummer는 페르마의 마지막 정리가 증명되기 어렵다. 이러한 소수들을 가리켜 '비정규 소수(irregular primes)'라고 했다. “$p>2$가 정규소수(regular prime)이면 페르마의 마지막 정리는 지수 $p$에 대하여 참이다”라는 사실을 지적한 이후에 모든 불규칙 소수에 대하여 페르마의 마지막 정리가 성립하는 방법을 찾지 못하였다.

Kummer는 소인수 분해가 늘 성립하지 않는다는 것 등의 대수학에 새로운 경지를 열었으나 지나치게 대수학적으로 접근하여 페르마의 마지막 정리를 증명하지 못했다.

## 4. Lewis Mordell (1888～1972 : 영국)

1보다 큰 종수(genus)를 가진 어떠한 방정식도 무한히 많은 유리수 해를 가질 수 없다고 추측하였다. 이것은 2보다 큰 지수의 모든 값에 대해서 페르마 방정식 $x^n+y^n=z^n$은 많아야 유한개의 해를 가질 수 있다는 사실을 나타낸다.

## 5. Gerd Faltings (1954～ : 독일)

정수론 분야에 남아 있는 미해결 문제들을 이미 알고 있는 미분기하학적 문제로 변환하여 해답을 찾는 방법을 도입하여 타원 방정식, 곡면의 분류이론을 이용하여 타원곡선이 페르마의 마지막 정리와 관계 있음을 밝힘으로써 유명한 ‘Mordell의 추즉’을 증명하였다. Faltings는 페르마의 마지막 정리를 증명하

지는 못했지만 해의 개수가 무한히 많지 않다는 사실을 증명한 것이다.

## 6. Yutaka Taniyama(일본)와 G. Shimura(일본)

1955년 Taniyama는 임으로 주어진 타원 곡선과 모듈러 곡선사이에 어떤 관계 - "유리수 체 위의 모든 타원 곡선은 모듈러이다" - 가 존재하여 그 관계가 주어진 곡선의 성질을 알려줄 것이라고 추측했다.

## 7. Gerhard Frey(독일)과 K. Ribet(미국)

1984년 Frey는 만약 정수 $a, b, c, n$이 존재해서 $a^n + b^n = c^n$이 성립하면 Taniyama가 제안한 방법대로 방정식 $y^2 = x(x-a^n)(x+b^n)$에 의해 정의된 타원곡선은 맞지 않다고 생각했다.
Taniyama의 추론을 증명하면 페르마의 마지막 정리를 증명하는 것이 된다.

## 8. Andrew Wiles (영국)

Andrew Wiles는 열 살 때 고향의 공공도서관에서 수학에 대한 어떤 책 한권을 읽었다. 그 책에 페르마의 마지막 정리에 대한 내용이 나와 있었다. 정리는 묘사된 대로 간단해 보였고 어떤 아이라도 이해할 수 있을 것 같았다. 그는 1970년대에 대학에 들어갔고, 학사학위를 받고 케임브리지 대학 수학과 대학원생이 되었다. 지도교수는 John Coates였다. Wiles는 페르마의 마지막 정리를 증명하려던 어린 시절의 꿈을 포기해야했다. 그 문제는 시간 낭비이고, 어느 대학원생도 감당할 수 없었다. 정리는 1970년대에 어울리는 주제가 아니었고, 그 시절의 인기 있는 주제인 타원곡선에 관한 논문으로 박사학위를 받은 뒤 프리스턴 대학 수학과에 자리를 얻어 미국으로 이주해서도 타원곡선에 대해 연구를 계속했다.

무더운 여름 저녁시간에 Andrew Wiles는 친구와 대화 도중에 갑자기 "K.Ribet이 입실론 추론[4]을 막 증명했다는 소식을 들었나?" 라는 말에 Wiles는

4) 입실론 추론이란 페르마의 마지막 정리와 Shimura-Taniyama 추론 사이의 관계에 대한 Frey의 추론을 세르가 수정한 것에 대하여 정수론 학자들이 비공식적으로 부르는 말이다.

감전된 듯이 놀랐고, 인생의 전환점이 다가왔다는 것을 알았다. 페르마의 마지막 정리 증명에 대하여 가졌던 어린 시절의 꿈이 강렬히 되살아났고 귀가하여 Shimura-Taniyama 추론을 어떻게 증명할 것인가를 생각하기 시작했고, 다락방에 틀어박혀 다른 연구 프로젝트는 포기하고 완전히 페르마에 투자했다.
Wiles가 알고 있기로 Shimura-Taniyama 추론을 증명하자면 모든 타원곡선이 모듈라한다는 것을 증명해야했다. 그가 최선의 방법이라고 생각한 것은 타원곡선의 숫자를 세어보고, 모듈라한 타원곡선의 숫자를 세어보고 나서 그 '숫자'가 같다는 것을 보이는 것 이였다. 이 작업은 타원곡선과 모듈라한 타원곡선이 동일하고, 따라서 모든 타원곡선이 사실 모듈라하기 때문에 Shimura-Taniyama 추론이 주장한 바와 같다는 것을 증명하는 것이었다.

Wiles는 두 가지를 알아냈다. 하나는 Shimura-Taniyama 추론 전체를 증명할 필요는 없고, 특별한 경우, 즉 계수가 유리수인 준안정 타원곡선에 대해서만 증명하면 된다는 것이었다. 다른 사실은, 그가 무한집합을 취급하기 때문에 이 경우에는 '숫자 세기'가 통하지 않는다는 것이었다. 준안정 타원곡선의 집합은 무한했다. 어떤 유리수 $\frac{a}{b}$ ($a, b$는 정수) 별개의 타원곡선을 제공할 것이다.

$\frac{a}{b}$가 각각 $1, 2, 3, 4\cdots$로 계속되어 무한대 까지 가는 무한히 많은 숫자 가운데 하나이기 때문에 유리수 $\frac{a}{b}$의 개수는 무한하며, 무한히 많은 타원 곡선이 존재하므로, 우리가 알고 있는 방식에 의한 개수 세기는 통하지 않는다. 갈루아 이론을 이용하여 복잡한 체로부터 군으로 변환시키면 종종 군은 유한한 집합의 원소에 의하여 생성되므로 무한한 집단으로부터 유한한 집합으로 옮겨갈 수 있다. 원소의 유한한 집합은 무한집합보다 취급하기가 훨씬 쉽기 때문에 그 접근법은 타원곡선의 몇 가지 집합에 대해서 잘 될 것 같아서 좋은 돌파구였으나, Wiles는 또 다시 난관에 봉착했다.

그는 오랫동안 해왔던 것처럼 계속해서 비밀에 부칠 것인지, 정수론을 잘 아는 누군가에게 이야기해야 할 것인지에 대한 결단을 내려야 했다. 1993년 1월, 6년 동안 혼자 연구한 끝에 Wiles는 프린스턴 대학 수학과 동료이던 완전히 믿

을 만한 Nick Katz 교수를 불렀다. Katz는 Wiles와 함께 일하면서 프로젝트가 끝날 때까지 완벽하게 입을 다물었지만 여전히 Wiles는 누군가가 눈치채지 않을까 걱정해서 그는 1993년 봄 학기에 새로운 강좌를 수학과 대학원에 개설하여 닉 카츠를 수강생으로 받아들임으로써 다른 사람들의 의심 없이 함께 연구할 수 있게 되었다. 몇 주 만에 대학원생들은 방향이 정해져 있지 않은 강의를 따라갈 수 없어서 모두 다 빠져 나가서 Nick Katz만이 유일한 학생이 되었다. 유수공식(Class Number Formula)은 성립하는 것 같았고, Wiles는 페르마 문제 해결을 향한 본 궤도에 진입했다. Wiles는 마지막 난관에 대한 직관을 더 얻기 위해 또 다른 한 사람에게 이야기할 때가 되었다고 느꼈고 프린스턴 대학 수학과 동료인 Peter Sarnak에게 도움을 청했다. 이제 두 동료는 Wiles가 증명을 마무리 하도록 도와주게 되었다.

1993년 5월, Wiles는 책상 앞에 앉아 좌절감을 느꼈는데, 그 이유는 타원들이 모듈라하다는 것을 증명하지 못하고 있었고, 그것이 증명이 되어야 페르마의 마지막 정리가 해결되기 때문에 필요했다. 준안정 타원 곡선의 대부분에 대하여 모듈라하다는 것을 보인 자체로도 훌륭한 수학적인 업적이었지만 목표에는 미치지 못했다. 그는 아무런 결과도 나오지 않는 탐구로부터 좀 쉬려고 위대한 대가인 하버드 대학의 Barry Mazur가 쓴 오래된 논문을 들었다. 아이젠슈타인 아이디얼에 대한 Mazur의 논문에서 Wiles의 주의를 끄는 내용이 한 줄 있었는데 “한 세트의 타원곡선을 다른 것으로 교체하는 것이 가능하다. 교체는 소수 사이에 행해져야했다.”였다. Mazur가 말하는 것은, 어떤 사람이 3이라는 소수를 바탕으로 하는 타원곡선을 취급한다면, 3대신 5라는 소수를 사용하여 연구할 수 있도록 타원곡선을 취급한다면, 3대신 5라는 소수를 사용하여 연구할 수 있도록 변환하는 것이 가능하다는 것이었다. 이 3대 5교체는 바로 Wiles가 필요로 하던 것이었다. 그는 3이라는 소수에 기초한 타원곡선이 모듈라하다는 것을 증명할 수 없어서 난관에 봉착했다. 그런데 Mazur는 5라는 소수에 바탕을 둔 곡선으로 교체할 수 있다고 말하고 있었다. 그러나 5에 바탕을 둔 이 곡선은 Wiles가 이미 모듈라하다고 증명해 놓은 것이었다. 그래서 3대 5교체는 결정적인 비결이 있었다. 그것은 3에 바탕을 둔 어려운 타원곡선을 떠맡아서 5에 바탕을 둔 것으

로 변환시키는데 이미 모듈라하다고 알려져 있었다. 다시 한번 다른 수학자들의 훌륭한 아이디어는 Wiles가 해결할 수 없을 것으로 보였던 장애물을 극복하도록 도와주었고 결국 그는 해냈다.

다음 달인 6월에 지도교수였던 John Coates가 정수론에 대한 학회를 주관할 예정이었고, 그 학회에는 정수론 거물들이 참가하는데, 그의 고향인 케임브리지에서 페르마의 마지막 정리에 대한 증명을 발표하면 완벽하겠다는 것이 그의 생각이였다.

Wiles는 Shimura-Taniyama 추론이 준안정 타원곡선에 대하여 성립한다는 증명 전체를 주워 모아야 했고, 다 써놓고 나니 증명은 200쪽이나 되었고 영국행 비행기를 타야 할 시간에 임박해서야 가까스로 끝낼 수 있었다. 그곳에서 마지막 강의가 끝났을 때 사람들의 박수갈채, 플래시 터뜨리는 카메라, 기자들을 향하여 의기양양한 태도를 갖는다.

1993년 6월 23일 뉴턴 연구소에서 열린 학술회의에서 Wiles는 반 안정적 타원곡선에 대해 Taniyama-시무라의 추론이 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 Wiles는 자신의 증명이 마지막 정리를 내포한다고 확신했고 그래서 그의 6월 발표는 페르마의 오래된 난문에 대한 증명이었다. 그러나 Wiles의 증명에서 몇 가지 논리적 비약이 발견되었다. Wiles가 해결할 수 없었던 한 가지 결함은 1994년 10월 케임브리지 대학교의 테일러와의 공동 논문을 통해 증명되었고, 1995년 5월 잡지 Annals of Mathmatics에 발표되었다. 그리고 볼프스켈의 유언에 따라 2년 동안의 심사 기간을 거친 뒤인 1997년 6월 27일에 볼프스켈 상[5]을 수상했다.

그는 4년마다 한 번’이라는 제약과 수상자의 연령이 40세보다 적어야 한다는 규정으로 인해 1993년에 최초에 증명을 내놓으나, 오류가 있음이 지적이 되어

5) 1906년 볼프스켈 상금 100,000(금)마르크는 당시 35.8423킬로그램의 금과 교환할 수 있었다. 이것은 오늘날 약 600.000DM(독일 마르크)의 가치가 있다. 즉, 이 상금은 오늘날 약 1,700,000달러의 구매력이 있다. 이 돈은 볼프스켈의 유언에 따라 비밀로 유지했다. 1997년 6월 27일 Wiles에게 볼프스켈 상이 수여될 때, 상금은 75,000DM가 되었다. 이것은 약 5%의 연이율 때문에 상금 총액이 지난 49년간 10배로 증가했음을 의미한다([13]).

1994년에 필즈 상을 수상하지 못했고, 증명을 마치고 난 다음 수상해인 1998년에는 그의 나이가 40세를 넘어 공로상을 받았다.
그는 정수론의 최첨단 이론을 모두 동원하여 Taniyama의 추측을 증명하였고, 단순한 수학적 테크닉으로 증명한 것보다는 수학의 또 다른 분야를 개척하였다는데 커다란 의의가 있다. 그것은 순수대수학과 위상수학, 기하학이 서로 독립된 분야가 아니라 하나의 커다란 이론적 유기체로서 상호의존적이라는 것을 보여주고 있다.
Wiles의 증명으로 인하여 현대 수학은 희망으로 가득 찬 차세대 수학으로 일대 도약을 일으켰다([1],[5],[10],[11],[12],[13],[14]).

# 제 6장. 결론

본 논문을 통해 우리는 페르마의 마지막 정리가 증명되는 과정을 알아보았다. 페르마의 마지막 정리는 360[6]여년이 지난 지금에야 증명되었다. 그러나 이 정리는 해가 존재하지 않는 방정식이 어디에 쓸모가 있겠는가? 라는 생각에 부정적인 결과라 생각한다. 실제로 1984년까지 페르마의 마지막은 증명된다고 해도 별 쓸모가 없는 순전히 호기심을 불러일으키는 문제일 뿐이였다. 사실, 페르마의 마지막 정리를 증명하려는 시도는 이 정리 하나만을 위한 연구가 아니었으며, 훨씬 더 큰 목표를 향한 연구 과정의 일부에 지나지 않았다. 그러나 이 문제가 타원함수에 대한 어떤 문제와 관계가 있다는 것이 밝혀지면서 이 문제는 많은 다른 문제를 풀 수 있는 출발점이 되었다. 페르마의 마지막 정리를 증명하는 것은 곧 20세기 수학에 한 획을 긋는 역사적인 일이었다.

수학적 관점에서 보면 이 페르마의 마지막 정리 문제는 단순히 그 문제를 해결하는데 의미가 있는 것이 아니라 페르마 시대부터 지금까지의 모든 수학적 분야를 총동원하여 해결했다는 것에 큰 의의가 있다.

---

6) 페르마는 1601년 8월 20일에 태어나 1665년 1월 12일에 사망했고, 1637년 그의 나이 37세에 페르마의 마지막 정리를 발견하였다. 그 뒤 수세기 동안 이 문제는 역사상 최대의 난제로 군림하였고, 약 357년가량이 지난 1994년에 영국의 수학자 앤드류 와일즈에 의해 해결되었다.

Euler의 증명에서 쓰인 새로운 형태의 수들을 일종의 정수(integer)로 생각할 수 있으며, 이것을 대수적 정수(algebraic integer)라고 부른다. 이런 대수적 정수의 성질을 연구하는 분야가 대수적 정수론(algebraic number theory)이다. 실제로, Kummer는 페르마의 마지막 정리가 아니라 이른바 '상호 정리'(reciprocity theorem)를 증명하려고 시도했었다. 고차 상호 법칙을 증명하려는 Kummer의 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 공현을 했다. 그리고 Wiles의 연구도 오래 전부터 수학자에게 큰 과제를 제시한 디오판토스 방정식의 풀이와 관련이 있으며(이와 관련된 자세한 내용과 현재의 연구방법은 타원 곡선과 모듈러 형식(modular form) 및 갈루아 표현(Galois representation) 이론을 창조하고 이들 사이의 관계를 연구한 많은 수학자의 도움으로 이루어졌다. 사실, 이 분야에서 수학자들은 페르마의 마지막 정리가 아니라 훨씬 더 유용한 미해결 문제를 해결하기 위해 노력하고 있다.

아직도 수학에는 해결되지 않은 '리만가설', '포앙카레 예측', '골드바흐 예측' 등 어디선가 그 문제를 풀기 위해 노력할 것이다. 이처럼 끊임없이 탐구하고 연구하는 자세를 우리는 본받아야 한다고 생각하며, 이 글을 통해 조금이나마 자각을 하는 계기가 되었다.

이로써 페르마의 마지막 정리의 증명은 끝이 아니라 또 다른 시작이다. 증명을 얻기 위해 사용된 방법은 페르마의 마지막 정리 자체보다 훨씬 중요하다.
수학 문제의 해결은 당장 해결되는 것 보다는 오랜 수학이론의 발전과 더불어 해결된다고 보여지는데, 위대한 선각자들의 올바른 방향제시가 수학발전에 얼마나 중요한 것인가를 알려준다.

# 참고문헌

[1]. 사이먼 싱.『페르마의 마지막 정리』, 영림카디얼, 1998.

[2]. Paulo Ribenboim. 『페르마의 마지막 정리』, 교우사, 2000.

[3]. 김응태・박승안. 『정수론』제 5판, 경문사, 2002.

[4]. 김응태・박승안. 『현대대수학』제 5판, 경문사, 2005.

[5]. Amir D, Aczel. 『쉽게 읽는 페르마의 마지막 정리』, 경문사, 2006.

[6]. David M. Burton, 『Elementary Number Theory』, Allyn and Bacon, 1980.

[7]. 한국사전연구사. 『수학대사전(상)』, 한국사전연구사편집부, 1999.

[8]. 김소희, “Finite abelian groups related with Fermat numbers", 연세대학교 교육대학원 석사학위논문, 2005.

[9]. 김유찬, “페르마의 마지막 정리에 관한 수학사적 고찰, 한국외국어대학교 교육대학원 석사학위논문, 2004.

[10]. 류수정, “페르마 마지막 정리에 관련된 중등학교 수학 학습 자료 개발 연구, 경상대학교 교육대학원 석사학위논문, 2004.

[11]. 방성배, “페르마의 마지막 정리와 대수 교육", 홍익대학교 교육대학원 석사학위논문, 2004.

[12]. 정건회, “페르마의 마지막 정리에 대한 연구”, 한남대학교 교육대학원 석사학위논문, 2004.

[13]. 허민, “페르마의 마지막 정리 - 역사적 발전과정", 『한국수학교육학회지 시리즈 E 제 7집』. p. 69-79, 1998.

[14]. 편집부, “페르마의 마지막 정리”, 『한국수학교육학회 뉴스레터 제 14권 제 6호 통권 제 58호』, 1998.

# 저작물 이용 허락서

| 학 과 | 수학교육 | 학 번 | 20068066 | 과 정 | 석사 |
|---|---|---|---|---|---|
| 성 명 | 한글: 조 형 서 한문: 趙 亨 書 영문: Hyoung-Seo Cho | | | | |
| 주 소 | 광주광역시 남구 봉선동 금호2차 205동 1202호 | | | | |
| 연락처 | 011-9607-4222 E - MAIL : cuteseoya@naver.com | | | | |
| 논문제목 | 페르마의 마지막정리<br>- On Fermat's Last Theorem - | | | | |

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건 아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

2008년 10월 일

저작자: 조 형 서 (서명 또는 인)

조선대학교 총장 귀하