Jiang And Wiles Proofs On Fermat Last Theorem(2)

Abstract

D.Zagier (1984) and K.Inkeri(1990) said[7]: Jiang mathematics is true, but Jiang determinates the irrational numbers to be very difficult for prime exponent p>2. In 1991 Jiang studies the composite exponents n=15,21,33,…,3p and proves Fermat last theorem. In 1986 Gerhard Frey places Fermat last theorem at the elliptic curve that is Frey curve. Andrew Wiles studies Frey curve. In 1994 Wiles proves Fermat last theorem. Conclusion:Jiang proof is direct and simple,but Wiles proof is indirect and complex.

Automorphic Functions And Fermat's Last Theorem（2）

Chun-Xuan Jiang

P. O. Box 3924, Beijing 100854, P. R. China

Jiangchunxuan@vip.sohu.com

Abstract

In 1637 Fermat wrote: "*It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into powers of like degree: I have discovered a truly marvelous proof, which this margin is too small to contain.*"

This means: $x^n + y^n = z^n (n > 2)$ has no integer solutions, all different from 0(i.e., it has only the trivial solution, where one of the integers is equal to 0). It has been called Fermat's last theorem (FLT). It suffices to prove FLT for exponent 4. and every prime exponent P. Fermat proved FLT for exponent 4. Euler proved FLT for exponent 3.

In this paper using automorphic functions we prove FLT for exponents $6P$ and P, where P is an odd prime. The proof of FLT must be direct .But indirect proof of FLT is disbelieving.

In 1974 Jiang found out Euler formula of the cyclotomic real numbers in the cyclotomic fields

$$\exp\left(\sum_{i=1}^{2n-1} t_i J^i\right) = \sum_{i=1}^{2n} S_i J^{i-1} \qquad (1)$$

where J denotes a $2n$ th root of unity, $J^{2n} = 1$, n is an odd number, t_i are the real numbers.

S_i is called the automorphic functions(complex hyperbolic functions) of order $2n$ with $2n-1$ variables [5,7].

$$S_i = \frac{1}{2n}\left[e^{A_1} + 2\sum_{j=1}^{\frac{n-1}{2}} (-1)^{(i-1)jB_j} \cos\left(\theta_j + (-1)^j \frac{(i-1)j\pi}{n}\right)\right]$$

$$+\frac{(-1)^{(i-1)}}{2n}\left[e^{A_2} + 2\sum_{j=1}^{\frac{n-1}{2}} (-1)^{(i-1)j} e^{D_j} \cos\left(\phi_j + (-1)^{j+1} \frac{(i-1)j\pi}{n}\right)\right], \qquad (2)$$

where $i = 1, \ldots, 2n$;

$$A_1 = \sum_{\alpha=1}^{2n-1} t_\alpha, \quad B_j = \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{\alpha j} \cos\frac{\alpha j\pi}{n}, \theta_j = (-1)^{(j+1)} \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{\alpha j} \sin\frac{\alpha j\pi}{n},$$

$$A_2 = \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^\alpha, \quad D_j = \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{(j-1)\alpha} \cos\frac{\alpha j\pi}{n},$$

$$\phi_j = (-1)^j \sum_{\alpha=1}^{2n-1} t_\alpha (-1)^{(j-1)\alpha} \sin\frac{\alpha j\pi}{n}, A_1 + A_2 + 2\sum_{j=1}^{\frac{n-1}{2}} (B_j + D_j) = 0 \qquad (3)$$

From (2) we have its inverse transformation[5,7]

$$e^{A_1} = \sum_{i=1}^{2n} S_i, \quad e^{A_2} = \sum_{i=1}^{2n} S_i (-1)^{1+i}$$

$$e^{B_j} \cos\theta_j = S_1 + \sum_{i=1}^{2n-1} S_{1+i} (-1)^{ij} \cos\frac{ij\pi}{n},$$

$$e^{B_j}\sin\theta_j=(-1)^{(j+1)}\sum_{i=1}^{2n-1} S_{1+i}(-1)^{ij}\sin\frac{ij\pi}{n},$$

$$e^{D_j}\cos\phi_j=S_1+\sum_{i=1}^{2n-1} S_{1+i}(-1)^{(j-1)i}\cos\frac{ij\pi}{n}$$

$$e^{D_j}\sin\phi_j=(-1)^{j}\sum_{i=1}^{2n-1} S_{1+i}(-1)^{(j-1)i}\sin\frac{ij\pi}{n} \tag{4}$$

(3) and (4) have the same form.
From (3) we have

$$\exp\left[A_1+A_2+2\sum_{j=1}^{\frac{n-1}{2}}(B_j+D_j)\right]=1 \tag{5}$$

From (4) we have

$$\exp\left[A_1+A_2+2\sum_{j=1}^{\frac{n-1}{2}}(B_j+D_j)\right]=\begin{vmatrix} S_1 & S_{2n} & \cdots & S_2 \\ S_2 & S_1 & \cdots & S_3 \\ \cdots & \cdots & \cdots & \cdots \\ S_{2n} & S_{2n-1} & \cdots & S_1 \end{vmatrix}$$

$$=\begin{vmatrix} S_1 & (S_1)_1 & \cdots & (S_1)_{2n-1} \\ S_2 & (S_2)_1 & \cdots & (S_2)_{2n-1} \\ \cdots & \cdots & \cdots & \cdots \\ S_{2n} & (S_{2n})_1 & \cdots & (S_{2n})_{2n-1} \end{vmatrix} \tag{6}$$

where $(S_i)_j=\dfrac{\partial S_i}{\partial t_j}$ [7]..

From (5) and (6) we have circulant determinant

$$\exp\left[A_1+A_2+2\sum_{j=1}^{\frac{n-1}{2}}(B_j+D_j)\right]=\begin{vmatrix} S_1 & S_{2n} & \cdots & S_2 \\ S_2 & S_1 & \cdots & S_3 \\ \cdots & \cdots & \cdots & \cdots \\ S_{2n} & S_{2n-1} & \cdots & S_1 \end{vmatrix}=1 \tag{7}$$

If $S_i \neq 0$, where $i=1,2,3,\ldots,2n$, then (7) have infinitely many rational solutions.

Let $n=1$. From (3) we have $A_1=t_1$ and $A_2=-t_1$. From (2) we have

$$S_1=\operatorname{ch}t_1 \qquad S_2=\operatorname{sh}t_1 \tag{8}$$

we have Pythagorean theorem

$$\operatorname{ch}^2 t_1-\operatorname{sh}^2 t_1=1 \tag{9}$$

(9) has infinitely many rational solutions.

Assume $S_1 \neq 0, S_2 \neq 0, S_i \neq 0$, where $i = 3,...,2n$. $S_i = 0$ are $(2n-2)$ indeterminate equations with $(2n-1)$ variables. From (4) we have

$$e^{A_1} = S_1 + S_2, \quad e^{A_2} = S_1 - S_2, e^{2B_j} = S_1^2 + S_2^2 + 2S_1S_2(-1)^j \cos\frac{j\pi}{n},$$
$$e^{2D_j} = S_1^2 + S_2^2 + 2S_1S_2(-1)^{j+1} \cos\frac{j\pi}{n} \qquad (10)$$

Example. Let $n = 15$. From (3) and (10) we have Fermat's equation

$$\exp[A_1 + A_2 + 2\sum_{j=1}^{7} (B_j + D_j)] = S_1^{30} - S_2^{30} = (S_1^{10})^3 - (S_2^{10})^3 = 1 \qquad (11)$$

From (3) we have

$$\exp(A_1 + 2B_3 + 2B_6) = [\exp(\sum_{j=1}^{5} t_{5j})]^5 \qquad (12)$$

From (10) we have

$$\exp(A_1 + 2B_3 + 2B_6) = S_1^5 + S_2^5 \qquad (13)$$

From (12) and (13) we have Fermat's equation

$$\exp(A_1 + 2B_3 + 2B_6) = S_1^5 + S_2^5 = [\exp(\sum_{j=1}^{5} t_{5j})]^5 \qquad (14)$$

Euler prove that (19) has no rational solutions for exponent 3 [8]. Therefore we prove that (14) has no rational solutions for exponent 5.

Theorem. Let $n = 3P$ where P is an odd prime. From (7) and (8) we have Fermat's equation

$$\exp(A_1 + A_2 + 2\sum_{j=1}^{\frac{3P-1}{2}} (B_j + D_j)] = S_1^{6P} - S_2^{6P} = (S_1^{2P})^3 - (S_2^{2P})^3 = 1 \qquad (15)$$

From (3) we have

$$\exp\left(A_1 + 2\sum_{j=1}^{\frac{P-1}{2}} B_{3j}\right) = \left[\exp\left(\sum_{j=1}^{5} t_{jP}\right)\right]^P \qquad (16)$$

From (10) we have

$$\exp\left(A_1 + 2\sum_{j=1}^{\frac{P-1}{2}} B_{3j}\right) = S_1^P + S_2^P \qquad (17)$$

From (16) and (17) we have Fermat's equation

$$\exp\left(A_1 + 2\sum_{j=1}^{\frac{P-1}{2}} B_{3j} \right) = S_1^P + S_2^P = \left[\exp\left(\sum_{j=1}^{5} t_{jP} \right) \right]^P \tag{18}$$

Euler prove that (15) has no rational solutions for exponent 3[8]. Therefore we prove that (18) has no rational solutions for prime exponent P [5,7].

Remark. It suffices to prove FLT for exponent 4. Let $n = 4P$, where P is an odd prime. We have the Fermat's equation for exponent $4P$ and the Fermat's equation for exponent P [2,5,7]. This is the proof that Fermat thought to have had. In complex hyperbolic functions let exponent n be $n = \Pi P$, $n = 2\Pi P$ and $n = 4\Pi P$. Every factor of exponent n has the Fermat's equation [1-7]. In complex trigonometric functions let exponent n be $n = \Pi P$, $n = 2\Pi P$ and $n = 4\Pi P$. Every factor of exponent n has Fermat's equation [1-7]. Using modular elliptic curves Wiles and Taylor prove FLT [9, 10]. This is not the proof that Fermat thought to have had. The classical theory of automorphic functions, created by Klein and Poincare, was concerned with the study of analytic functions in the unit circle that are invariant under a discrete group of transformation. Automorphic functions are the generalization of trigonometric, hyperbolic, elliptic, and certain other functions of elementary analysis. The complex trigonometric functions and complex hyperbolic functions have a wide application in mathematics and physics.

Acknowledgments. We thank Chenny and Moshe Klein for their help and suggestion.

References

[1] Jiang, C-X, Fermat last theorem had been proved, Potential Science (in Chinese), 2.17-20 (1992), Preprints (in English) December (1991). http://www.wbabin.net/math/xuan47.pdf.

[2] Jiang, C-X, Fermat last theorem had been proved by Fermat more than 300 years ago, Potential Science (in Chinese), 6.18-20(1992).

[3] Jiang, C-X, On the factorization theorem of circulant determinant, Algebras, Groups and Geometries, 11. 371-377(1994), MR. 96a: 11023, http://www.wbabin.net/math/xuan45.pdf

[4] Jiang, C-X, Fermat last theorem was proved in 1991, Preprints (1993). In: Fundamental open problems in science at the end of the millennium, T.Gill, K. Liu and E. Trell (eds). Hadronic Press, 1999, P555-558. http://www.wbabin.net/math/xuan46.pdf.

[5] Jiang, C-X, On the Fermat-Santilli theorem, Algebras, Groups and Geometries, 15. 319-349(1998)

[6] Jiang, C-X, Complex hyperbolic functions and Fermat's last theorem, Hadronic Journal Supplement, 15. 341-348(2000).

[7] Jiang, C-X, Foundations of Santilli's Isonumber Theory with applications to new cryptograms, Fermat's theorem and Goldbach's Conjecture. Inter. Acad. Press. 2002. MR2004c:11001, http://www.wbabin.net/math/xuan13.pdf. http://www.i-b-r.org/docs/jiang.pdf

[8] Ribenboim,P, Fermat last theorem for amateur, Springer-Verlag, (1999).

[9] Wiles A, Modular elliptic curves and Fenmat's last theorem, Ann of Math, (2) 141 (1995), 443-551.

[10] Taylor, R. and Wiles, A., Ring-theoretic properties of certain Hecke algebras, Ann. of Math., (2) 141(1995), 553-572.

Wiles' proof of Fermat's Last Theorem

From Wikipedia, the free encyclopedia
Jump to: navigation, search

Sir Andrew John Wiles

Wiles' proof of Fermat's Last Theorem is a proof of the modularity theorem for semistable elliptic curves, which, together with Ribet's theorem, provides a proof for Fermat's Last Theorem. Wiles first announced his proof in June 1993 in a version that was soon recognized as having a serious gap. The widely accepted version of the proof was released by Andrew Wiles in September 1994, and published in 1995. The proof uses many techniques from algebraic geometry and number theory, and has many ramifications in these branches of mathematics. It also uses standard constructions of modern algebraic geometry, such as the category of schemes and Iwasawa theory, and other 20th century techniques not available to Fermat.

The proof itself is over 100 pages long and consumed seven years of Wiles' research time. Among other honors for his accomplishment, he was knighted.

Contents

[hide]

[edit] Progress of the previous decades

Fermat's Last Theorem states that no nontrivial integer solutions exist for the equation

$$a^n + b^n = c^n$$

if n is an integer greater than two.

In the 1950s and 1960s a connection between elliptic curves and modular forms was conjectured by the Japanese mathematician Goro Shimura based on some ideas that Yutaka Taniyama posed. In the West it became well known through a 1967 paper by André Weil. With Weil giving conceptual evidence for it, it is sometimes called the Shimura-Taniyama-Weil conjecture. It states that every rational elliptic curve is modular.

On a separate branch of development, in the late 1960s, when Yves Hellegouarch came up with the idea of associating solutions (a, b, c) of Fermat's equation with a completely different mathematical object: an elliptic curve.[1] The curve consists of all points in the plane whose coordinates (x, y) satisfy the relation.

$$y^2 = x(x - a^n)(x + b^n)$$

Such an elliptic curve would enjoy very special properties, which are due to the appearance of high powers of integers in its equation and the fact that $a^n + b^n = c^n$ is a nth power as well.

In 1982-1985, Gerhard Frey called attention to the unusual properties of the same curve as Hellegouarch, now called a Frey curve. This provided a bridge between Fermat and Taniyama by showing that a counterexample to Fermat's Last Theorem would create such a curve that would not be modular. Again, the conjecture says that each elliptic curve with rational coefficients can be constructed in an entirely different way, not by giving its equation but by using modular functions to parametrize coordinates x and y of the points on it. Thus, according to the conjecture, any elliptic curve over **Q** would have to be a modular elliptic curve, yet if a solution to Fermat's equation with non-zero a, b, c and p greater than 2 existed, the corresponding curve would not be modular, resulting in a contradiction. The link between Fermat's Last Theorem and the Taniyama–Shimura conjecture is a little subtle: in order to derive the former from the latter, one needs to know a small amount more, or as mathematicians would have it, "an epsilon more".

In 1985, Jean-Pierre Serre proposed that a Frey curve could not be modular and provided a partial proof of this. This showed that a proof of the semistable case of the Taniyama-Shimura conjecture would imply Fermat's Last Theorem. Serre did not provide a complete proof and what was missing became known as the epsilon conjecture or ε-conjecture. Serre's main interest was in an even more ambitious conjecture, Serre's conjecture on modular Galois representations, which would imply the Taniyama–Shimura conjecture. Although in the preceding twenty or thirty years a lot of evidence had been accumulated to form conjectures about elliptic curves, the main reason to believe that these various conjectures were true lay not in the numerical confirmations, but in a remarkably coherent and attractive mathematical picture that they presented. Moreover, it could have happened that one or more of these conjectures were actually false.

In the summer of 1986, Ken Ribet succeeded in proving the epsilon conjecture. (His article was published in 1990.) He demonstrated that, just as Frey had anticipated, a special case of the Taniyama–Shimura conjecture (still unproven at the time), together with the now proven epsilon conjecture, implies Fermat's Last Theorem. Thus, if the Taniyama–Shimura conjecture holds for a class of elliptic curves called semistable elliptic curves, then Fermat's Last Theorem would be true.

[edit] General approach of proof

Given an elliptic curve E over the field Q of rational numbers $E(\bar{Q})$, for every prime power l^n, there exists a homomorphism from the absolute Galois group

$$\mathrm{Gal}(\bar{Q}/Q)$$

to

$$GL_2(Z/l^nZ),$$

the group of invertible 2 by 2 matrices whose entries are integers $(\mathrm{mod}\ l^n)$. This is because $E(\bar{Q})$, the points of E over $\bar{Q}$, form an abelian group, on which $\mathrm{Gal}(\bar{Q}/Q)$acts; the subgroup of elements x such that $l^n x = 0$ is just $(Z/l^nZ)^2$, and an automorphism of this group is a matrix of the type described.

Less obvious is that given a modular form of a certain special type, a Hecke eigenform with eigenvalues in Q, one also gets a homomorphism from the absolute Galois group

$$\mathrm{Gal}(\bar{Q}/Q) \to GL_2(Z/l^nZ).:$$

This goes back to Eichler and Shimura. The idea is that the Galois group acts first on the modular curve on which the modular form is defined, thence on the Jacobian variety of the curve, and finally on the points of l^n power order on that Jacobian. The resulting representation is not usually 2-dimensional, but the Hecke operators cut out a 2-dimensional piece. It is easy to demonstrate that these representations come from some elliptic curve but the converse is the difficult part to prove.

Instead of trying to go directly from the elliptic curve to the modular form, one can first pass to the $\pmod{l^n}$ representation for some l and n, and from that to the modular form. In the case l=3 and n=1, results of the Langlands-Tunnell theorem show that the (mod 3) representation of any elliptic curve over Q comes from a modular form. The basic strategy is to use induction on n to show that this is true for l=3 and any n, that ultimately there is a single modular form that works for all n. To do this, one uses a counting argument, comparing the number of ways in which one can lift a $\pmod{l^n}$ Galois representation to $\pmod{l^{n+1}}$ and the number of ways in which one can lift a $\pmod{l^n}$ modular form. An essential point is to impose a sufficient set of conditions on the Galois representation; otherwise, there will be too many lifts and most will not be modular. These conditions should be satisfied for the representations coming from modular forms and those coming from elliptic curves. If the original (mod 3) representation has an image which is too small, one runs into trouble with the lifting argument, and in this case, there is a final trick, which has since taken on a life of its own with the subsequent work on the Serre Modularity Conjecture. The idea involves the interplay between the (mod 3) and (mod 5) representations. See Chapter 5 of the Wiles paper for this 3/5 switch.

[edit] Wiles' proof

Shortly after learning of the proof of the epsilon conjecture, it was clear that a proof that all rational semistable elliptic curves are modular would also constitute a proof of Fermat's Last Theorem. Wiles decided to conduct his research exclusively towards finding a proof for the Taniyama-Shimura conjecture. Many mathematicians thought the Taniyama-Shimura conjecture was inaccessible to proof because the modular forms and elliptic curves seem to be unrelated.

Wiles opted to attempt to "count" and match elliptic curves to counted modular forms. He found that this direct approach was not working, so he transformed the problem by instead matching the Galois representations of the elliptic curves to modular forms. Wiles denotes this matching (or mapping) that, more specifically, is a ring homomorphism:

$$R_n \to T_n.$$

R is a deformation ring and T is a Hecke ring.

Wiles had the insight that in many cases this ring homomorphism could be a ring isomorphism. (Conjecture 2.16 in Chapter 2, §3) Wiles had the insight that the map between R and T is an isomorphism if and only if two abelian groups occurring in the theory are finite and have the same cardinality. This is sometimes referred to as the "numerical criterion". Given this result, one can see that Fermat's Last Theorem is reduced to a statement saying that two groups have the same order. Much of the text of the proof leads into topics and theorems related to ring theory and commutation theory. The Goal is to verify that the map $R \to T$ is an isomorphism and ultimately that $R=T$. This is the long and difficult step. In treating deformations, Wiles defines four cases, with the flat deformation case requiring more effort to prove and is treated in a separate article in the same volume entitled "Ring-theoretic properties of certain Hecke algebra".

Gerd Faltings, in his bulletin, on p. 745. gives this commutative diagram:

```
  --> T -> T/m
 /         ^
R          |
 \         |
  --> Z3 -> F3
```

or ultimately that $R = T$, indicating a complete intersection. Since Wiles cannot show that $R=T$ directly, he does so through $Z3$, $F3$ and T/m via lifts.

In order to perform this matching, Wiles had to create a class number formula (CNF). He first attempted to use horizontal Iwasawa theory but that part of his work had an unresolved issue such that he could not create a CNF. At the end of the summer of 1991, he learned about a paper by Matthias Flach, using ideas of Victor Kolyvagin to create a CNF, and so Wiles set his Iwasawa work aside. Wiles extended Flach's work in order to create a CNF. By the spring of 1993, his work covered all but a few families of elliptic curves. In early 1993, Wiles reviewed his argument beforehand with a Princeton colleague, Nick Katz. His proof involved the Kolyvagin-Flach method,[2] which he adopted after the Iwasawa method failed.[3] In May 1993 while reading a paper by Mazur, Wiles had the insight that the 3/5 switch would resolve the final issues and would then cover all elliptic curves (again, see Chapter 5 of the paper for this 3/5 switch). Over the course of three lectures delivered at Isaac Newton Institute for Mathematical Sciences on June 21, 22, and 23 of 1993, Wiles announced his proof of the Taniyama - Shimura conjecture, and hence of Fermat's Last Theorem. There was a relatively large amount of press coverage afterwards.[4]

After announcing his results, Katz was a referee on his manuscript and he asked Wiles a series of questions that led Wiles to recognize that the proof contained a gap. There was an error in a critical portion of the proof which gave a bound for the order of a particular group: the Euler system used to extend Flach's method was incomplete. Wiles and his former student Richard Taylor spent almost a year resolving it.[5][6] Wiles indicates that on the morning of September 19, 1994 he realized that the specific reason why the Flach approach would not work directly suggested a new approach with the Iwasawa theory which resolved all of the previous issues with the latter and resulted in a CNF that was valid for all of the required cases. On 6 October Wiles sent the new proof to three colleagues including Faltings. The new proof was published and, despite its size, widely accepted as likely correct in its major components.[7][8]

In his 1995 108 page article, Wiles divides the subject matter up into the following chapters (preceded here by page numbers):

Gerd Faltings provided some simplifications to the 1995 proof, primarily in switch from geometric constructions to rather simpler algebraic ones.[9][10] The book of the Cornell conference also contained simplifications to the original proof.[11]

[edit] Culmination of the work of many

Because Wiles had incorporated the work of so many other specialists, it had been suggested in 1994 that only a small number of people were capable of fully understanding at that time all the details of what Wiles has done.[12] The number is likely much larger now with the 10-day conference and book organized by Cornell et al.,[11] which has done much to make the full range of required topics accessible to graduate students in number theory. The paper provides a long Bibliography and Wiles mentions the names of many mathematicians in the text. The list of some of the many other mathematicians whose work the proof incorporates includes Felix Klein, Robert Fricke, Adolf Hurwitz, Erich Hecke, Barry Mazur, Dirichlet, Richard Dedekind, Robert Langlands, Jerrold B. Tunnell, Jun-Ichi Igusa, Martin Eichler, André Bloch, Tosio Kato, Ernst S. Selmer, John Tate, P. Georges Poitou, Henri Carayol, Emil Artin, Jean-Marc Fontaine, Karl Rubin, Pierre Deligne, Vladimir Drinfel'd and Haruzo Hida and to those mathematicians who have searched (or continue to search) for a more elementary proof.

[edit] Aftermath

In 1998, the full modularity theorem was proven by Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor using many of the methods that Andrew Wiles used in his 1995 published papers.

A computer science challenge given in 2005 is "Formalize and verify by computer a proof of Fermat's Last Theorem, as proved by A. Wiles in 1995."[13]

[edit] Reading and notation guide

The Wiles paper is over 100 pages long and often uses the peculiar symbols and notations of group theory, algebraic geometry, commutative algebra, and Galois theory.

One might want to first read the 1993 email of Ken Ribet,[14][15] Hesselink's quick review of top-level issues gives just the elementary algebra and avoids abstract algebra.[16], or Daney's web page which provides a set of his own notes and lists the current books available on the subject. Weston attempts to provide a handy map of some of the relationships between the subjects.[17] F. Q. Gouvêa provides an award-winning review of some of the required topics.[18][19][20][21] Faltings' 5-page technical bulletin on the matter is a quick and technical review of the proof for the non-specialist. For those in search of a commercially available book to guide them, he recommended that those familiar with abstract algebra read Hellegouarch, then read the Cornell book,[11] which is claimed to be accessible to "a graduate student in number theory". Note that not even the Cornell book can cover the entirety of the Wiles proof.[4]

The work of almost every mathematician who helped to lay the groundwork for Wiles did so in specialized ways, often creating new specialized concepts and yet more new jargon. In the equations, subscripts and superscripts are used extensively because of the numbers of concepts that Wiles is sometimes dealing with in an equation.

- See the glossaries listed in Lists of mathematics topics#Pure mathematics, such as Glossary of arithmetic and Diophantine geometry . Daney provides a proof-specific glossary.
- See Table of mathematical symbols and Table of logic symbols
- For the deformation theory, Wiles defines restrictions (or cases) on the deformations as Selmer (sel), ordinary(ord), strcit(str) or flat(fl) and he uses the abbreviations list here. He usually uses these as a subscript but he occasionally uses them as a superscript. There is also a fifth case: the implied "unrestricted" case but note that the superscript "unr" is not an abbreviation for unrestricted.
- Q^{unr} is the unramified extension of Q. A related but more specialized topic used is crystalline cohomology. See also Galois cohomology.
- Some relevant named concepts: Hasse-Weil zeta function, Mordell–Weil theorem, Deligne-Serre theorem
- Grab bag of jargon mentioned in paper: cover and lift, finite field, isomorphism, surjective function, decomposition group, j-invariant of elliptical curves, Abelian group, Grossencharacter, L-function, abelian variety, Jacobian[*disambiguation needed*], Néron model, Gorenstein ring, Torsion subgroup (including torsion points on elliptic curves here [22] and here [23]), Congruence subgroup, eigenform, Character (mathematics), Irreducibility (mathematics), Image (mathematics), dihedral, Conductor, Lattice (group), Cyclotomic field, Cyclotomic character, Splitting of prime ideals in Galois extensions (and decomposition group and inertia group), Quotient space, Quotient group

[edit] Notes

1. ^ Hellegouarch, Yves (2001). *Invitation to the Mathematics of Fermat-Wiles*. Academic Press. ISBN 978-0123392510.
2. ^ Singh, Simon. *Fermat's Last Theorem*, 2002, p. 259.
3. ^ Singh, Simon. *Fermat's Last Theorem*, 2002, p. 260.
4. ^ *a b* AMS book review Modular forms and Fermat's Last Theorem by Cornell et. al., 1999
5. ^ A Year Later, Snag Persists In Math Proof 1994-06-28
6. ^ June 26-July 2; A Year Later Fermat's Puzzle Is Still Not Quite Q.E.D. 1994-07-03
7. ^ NOVA Video, The Proof October 28, 1997, See also Solving Fermat: Andrew Wiles
8. ^ The Proof of Fermat's Last Theorem Charles Daney, 1996
9. ^ Fermat's Last Theorem at MacTutor
10. ^ Fermat's Last Theorem 1996
11. ^ *a b c* G. Cornell, J. H. Silverman and G. Stevens, *Modular forms and Fermat's Last Theorem*, ISBN 0-387-94609-8

12. ^ History of Fermat's Last Theorem Andrew Granville, Jun 24, 1993
13. ^ Computer verification of Wiles' proof of Fermat's Last Theorem
14. ^ FAQ: Wiles attack June 1993
15. ^ Fermat's Last Theorem a Theorem at last August 1993
16. ^ How does Wiles prove Fermat's Last Theorem? by Wim H. Hesselink
17. ^ Research Summary Topics
18. ^ A Marvelous Proof Fernando Gouvêa, The American Mathematical Monthly, vol. 101, 1994, pp. 203-222
19. ^ The Mathematical Association of America's Lester R. Ford Award
20. ^ Year of Award: 1995
21. ^ MAA Writing Awards, 1995
22. ^ http://mat.uab.es/~xarles/elliptic.html
23. ^ http://planetmath.org/encyclopedia/ArithmeticOfEllipticCurves.html

[edit] References

- Aczel, Amir. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*, 1997. ISBN 978-1-56858-077-7
- John Coates (July 1996). "Wiles Receives NAS Award in Mathematics" (PDF). *Notices of the AMS* **43** (7): 760–763. http://www.ams.org/notices/199607/comm-wiles.pdf.
- Cornell, Gary (1998-01-01). *Modular Forms and Fermat's Last Theorem*. ISBN 0387946098. (Cornell, et al.)
- Daney, Charles (2003). "The Mathematics of Fermat's Last Theorem". http://cgd.best.vwh.net/home/flt/flt01.htm. Retrieved 2004-08-05.
- Darmon, H. (September 9, 2007). "Wiles' theorem and the arithmetic of elliptic curves". http://www.math.mcgill.ca/darmon/pub/Articles/Expository/03.BU-FLT/paper.pdf.
- Faltings, Gerd (July 1995). "The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles" (PDF). *Notices of the AMS* **42** (7): 743–746. ISSN 0002-9920. http://www.ams.org/notices/199507/faltings.pdf.
- Frey, Gerhard (1986). "Links between stable elliptic curves and certain diophantine equations". *Ann. Univ. Sarav. Ser. Math.* **1**: 1–40.
- Hellegouarch, Yves (2001-01-01). *Invitation to the Mathematics of Fermat-Wiles*. ISBN 0-12-339251-9. See review
- "The bluffer's guide to Fermat's Last Theorem". http://math.stanford.edu/~lekheng/flt/. (collected by Lim Lek-Heng)
- Mozzochi, Charles (2000-12-07). *The Fermat Diary*. American Mathematical Society. ISBN 978-0-821-82670-6. (see book review
- Mozzochi, Charles (2006-07-06). *The Fermat Proof*. Trafford Publishing. ISBN 1412022037.
- O'Connor, J. J.; Robertson, E. F. (1996). "Fermat's last theorem". http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html. Retrieved 2004-08-05.
- van der Poorten, Alfred (1996-01-01). *Notes on Fermat's Last Theorem*. ISBN 0471062618.

- Ribenboim, Paulo (2000-01-01). *Fermat's Last Theorem for Amateurs*. ISBN 0387985085.
- Ribet, Ken (1995). "Galois representations and modular forms" (PDF). http://math.stanford.edu/~lekheng/flt/ribet.pdf. Discusses various material which is related to the proof of Fermat's Last Theorem: elliptic curves, modular forms, Galois representations and their deformations, Frey's construction, and the conjectures of Serre and of Taniyama–Shimura.
- Singh, Simon (October 1998). *Fermat's Enigma*. New York: Anchor Books. ISBN 978-0-385-49362-8. ISBN 0-8027-1331-9
- Simon Singh "The Whole Story". http://www.simonsingh.net/FLT_the_whole_story.html. Edited version of ~2,000-word essay published in Prometheus magazine, describing Andrew Wiles' successful journey.
- Richard Taylor and Andrew Wiles (May 1995). "Ring-theoretic properties of certain Hecke algebras" (PDF). *Annals of Mathematics* (Annals of Mathematics) **141** (3): 553–572. doi:10.2307/2118560. ISSN 0003486X. OCLC 37032255. http://math.stanford.edu/~lekheng/flt/taylor-wiles.pdf.
- Wiles, Andrew (1995). "Modular elliptic curves and Fermat's Last Theorem" (PDF). *Annals of Mathematics* (Annals of Mathematics) **141** (3): 443–551. doi:10.2307/2118559. ISSN 0003486X. OCLC 37032255. http://math.stanford.edu/~lekheng/flt/wiles.pdf. See also this smaller and searchable PDF text version. The smaller PDF gets the volume number correct: it is 141, not 142.

[edit] External links

- Weisstein, Eric W., "Fermat's Last Theorem" from MathWorld.
- "The Proof". http://www.pbs.org/wgbh/nova/proof/. The title of one edition of the PBS television series NOVA, discusses Andrew Wiles' effort to prove Fermat's Last Theorem broadcast on BBC Horizon and UTV/Documentary series as Fermat's Last Theorem at Google Video (Adobe Flash video) 1996
- Wiles, Ribet, Shimura-Taniyama-Weil and Fermat's Last Theorem
- Are mathematicians finally satisfied with Andrew Wiles' proof of Fermat's Last Theorem? Why has this theorem been so difficult to prove?, *Scientific American*, October 21, 1999

- Discussion

Variants

Views

- Read
- Edit
- View history

Actions

Search

Special:Search

Search

Navigation

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia

Interaction

- Help
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia

Toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Cite this page

Print/export

- Create a book
- Download as PDF
- Printable version

- Contact us

- Privacy policy
- About Wikipedia
- Disclaimers