Fermat's Last Theorem and Cyclotomic Fields

Sankar Sitaraman, Howard University

Early History

In a margin of a book by the ancient Greek geometer Diophantus, Pierre de Fermat wrote (late 1630s):

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere. Cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Statement of the theorem:

$$x^n + y^n = z^n \text{ has no integer solutions for } n > 2,\ xyz \neq 0.$$

Can assume $(x, y, z) = 1$.

When $n = 2$, there exist infinitely many solutions. In fact, all primitive [i.e,$\{x, y, z\}$ such that $(x, y, z) = 1$] solutions are given by integer pairs $\{m, n\}$ satisfying $(m, n) = 1,\ m \not\equiv n\ (mod\ 2)$ by taking

$$x = 2mn,\ y = m^2 - n^2,\ z = m^2 + n^2,$$

The case $n = 4$ was proved by Fermat himself. If $x^{mn} + y^{mn} = z^{mn}$, then $\{x^m, y^m, z^m\}$ is a solution for $X^n + Y^n = Z^n$. So from now on it is enough to consider only $n = p$, where p is an odd prime.

The case $p = 3$ was proved (almost) by Euler (1753). Dirichlet and Legendre proved (independently, 1825) the case $p = 5$. Lamé proved (1839) the case $p = 7$. These proofs depended heavily on clever algebraic manipulations using identities for $x^3 + y^3, x^5 + y^5$, etc., and were often ad hoc, and not easily extended to all primes.

More general proofs: Use of Algebraic Number Theory

First case and second case

The later results on FLT mostly dealt with general p. It was found that the case when $(xyz, p) = 1$ required a different treatment from the case when $p|xyz$. The former began to be called the First case and the latter the Second case. In fact it would turn out that the First case was easier to prove than the second.

The following result by Sophie Germain (1823) was the first to provide a proof of FLT for general p :

If p is an odd prime such that $2p + 1$ is also a prime, then case I of FLT is true for p.

Using this and similar results, whose main ingredient was congruence relations, she was able to verify that if $p < 100$, then FLT is true for case I, i.e, $x^p + y^p = z^p \Rightarrow p|xyz$.

Algebraic number theory

Early use of Algebraic Number Theory was made by Gauss, who gave a proof for $p = 3$ using the "integers" from the field $\mathbf{Q}[\zeta_3]$ (the set of algebraic integers $\{a + b\zeta_3 \mid a, b \in \mathbf{Z}\}$) where ζ_3 is a cube root of unity.

[In this notation, ζ_p is a complex p-th root of 1 and $\mathbf{Q}[\zeta_p]$ is the p-th cyclotomic field.]

After Gauss, various results from algebraic number theory, especially cyclotomic field theory, were applied to the proof of FLT with varying degree of success by Cauchy, Kummer, and many others. Not only were they able to prove it for large categories of primes, they also developed many criterion for FLT to be true in various cases. The development of algebraic number theory owes a tremendous debt to the work of Kummer. The foundations he laid eventually led to the modern techniques used by Wiles.

Situation by 1993

By 1993 FLT was known to be true for many types of primes. It was also verified to be true numerically for a large number of primes, using the criteria developed by Kummer, Wieferich, et al.

Using computers, Buhler, Crandall, Ernvall, and Metsankyla verified it to be true upto 4 million in 1996. (By 1992, a year before Wiles' announcement, this was known upto 1 million). The first case, actually, was verified for primes upto 714,591,416,091,389, by Granville and Monagan around 1987.

There were also results showing that FLT was true for infinitely many primes. Granville had shown in 1985 that the set of primes for which FLT is true has asymptotic density one.

Adleman, Fouvry and Heath-Brown proved in 1985 using delicate estimates from analytic number theory as well as results similar to that of Sophie Germain that the First Case of FLT is true for infinitely many primes.

By Faltings' proof of the Mordell-Weil theorem (1983), we know that a non-singular curve C over a number field K of genus bigger than 1 has only finitely many K-rational points. Since genus of $x^n + y^n - z^n$ is $(n-1)(n-2)/2$, we have that for each p, $x^p + y^p = z^p$ has only finitely many solutions.

Wiles' Proof

In 1985, Frey conjectured that FLT could be proved using a special elliptic curve and a modular form which was conjectured to be associated to it.

Elliptic Curves

Let p be any odd prime. Frey considered $y^2 = x(x - a^p)(y + b^p)$, where a, b, c satisfy $a^p + b^p = c^p$, and $(a, b, c) = 1$ as before.

In addition we may assume a is even and $b \equiv -1 \pmod{p}$.

This curve is an elliptic curve, say E_{Frey}, over $\mathbf{Q}$. By reducing the coefficients of its defining equation modulo a prime q, one gets an elliptic curve over the finite field $\mathbf{F}_q$. This elliptic curve may be singular, with a node or a cusp, depending on whether the cubic $x(x-a^p)(x+b^p)$ has 2 or 3 equal roots in $\mathbf{F}_q$. In this case, the roots are $0, a^p, -b^p$. If $a^p \equiv b^p \equiv 0 \pmod{q}$, then $q|a$, and $q|b$ also, which is prevented by the hypothesis on a, b, c. Thus the curve E_{Frey} is either non-singular or has a node on reduction modulo any prime q, but no cusp [The case q=2 is taken care of by the additional assumptions]. Such an elliptic curve is said to have **semistable reduction**.

Modular Forms

Let N be a positive integer.

$\Gamma_0(N) \stackrel{def}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \equiv 0 \ (mod\ N) \right\}$. This group acts on the upper half plane H by $\gamma z = \frac{az+b}{cz+d}$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

If $k > 0$, $k \in \mathbf{Z}$, a modular form (a cusp form f of weight 2) is an analytic function $f : H \to \mathbf{C}$ such that

(a) $f(\gamma z) = (cz + d)^2 f(z)$ for $z \in H, \gamma \in \Gamma_0(N)$.

(b) f vanishes at the cusps.

[Vaguely speaking, cusps are the finitely many points added to the quotient space $\Gamma_0(N)/H$ to make it a compact Riemmann surface]

Letting $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, we get $f(z+1) = f(z)$. So f can be expanded in a Fourier series $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} = \sum_{n=1}^{\infty} a_n q^n$. The modular forms of level N (N as defined above) form a vector space which is equipped with linear operators called *Hecke operators* and the eigenvectors of these operators which are further normalized with $a_1 = 1$ are called *eigenforms*, with the coefficients a_n being the eigenvalues.

Connecting elliptic curves and modular forms

The modular form is a purely analytical object. The elliptic curve is a geometric object endowed with a group structure as well as associated Galois representations [representations of the Galois group of the extension of $\mathbf{Q}$ obtained by attaching coefficients of the torsion points in the group of rational points of the elliptic curve].

The Shimura-Taniyama-Weil conjecture produces a connection between them. Let E be an elliptic curve. For a given prime q, and the finite field $\mathbf{F}_q$, let $b_q = q+1-\#(E(\mathbf{F}_q))$, where $\#(E(\mathbf{F}_q))$ is the number of $\mathbf{F}_q$-rational points of the reduced elliptic curve.

The Shimura-Taniyama-Weil conjecture

For every elliptic curve, there exists an eigenform such that, for all but a finite number of primes, the coefficients $a_q = b_q$.

Proof of Fermat's Last Theorem

Frey claimed (1985) that the curve E_{Frey} cannot be modular. Serre showed (1985) that this claim will follow from a certain conjecture (the epsilon conjecture), as part of his more general *Serre's conjectures.* Ribet (1985) gave the proof of this epsilon conjecture, and Wiles announced in 1993 the outline of his proof that every semistable elliptic curve has to be modular. This completed the proof that E_{Frey} cannot exist, i.e, that $a^p + b^p = c^p$ is not possible for integers a, b, c. (The final, complete proof of Wiles' result was given in 1995, with the help of Richard Taylor).

Kummer et al and the classical approach

p is an odd prime. ζ a complex p-th root of 1, unless specified otherwise.

The classical approach, using algebraic number theory, and specifically cyclotomic field theory, starts with a factorization of $x^p + y^p$.

$$x^p + y^p = (x + y)(x + \zeta y)(x + \zeta^2 y) \dots (x + \zeta^{p-1} y).$$

If the set $\mathbf{Z}[\zeta]$ of algebraic integers of $\mathbf{Q}[\zeta]$ has unique factorization into irreducible elements, one gets from the above equation:

In case I,

$$x + \zeta y = \gamma \beta^p,$$

where γ is a unit and β is an algebraic integer.

In case II, assuming that p divides z,

$$\frac{x + \zeta y}{1 - \zeta} = \nu \rho^p,$$

where ν is a unit and ρ is an algebraic integer.

In case II, one gets a contradiction from the above by an infinite descent argument. We produce another couple of p-th powers which add upto a p-th power (modulo some unit elements) that are somehow "smaller" than the triple $\{x, y, z\}$.

In case I, a contradiction can be obtained directly using some algebraic manipulations (in the Precalculus sense) of the equation $x + \zeta y = \gamma \beta^p$. But it is more interesting to get the contradiction by using logarithmic derivatives, which were first defined by Kummer, as follows:

Logarithmic Derivatives

Definition and Properties

Let $1 - \zeta = \lambda$.

For any $f \in \mathbf{Z}[x], f(1) \not\equiv 0 \ (mod\ p)$ and any integer $k \geq 1$ define the (*formal*) logarithmic derivative $\Delta^{(k)}$ with values in $\mathbf{Q}$ by

$$\Delta^{(k)}(f) = \frac{d^k}{dv^k} log(f(e^v))\Big|_{v=0}.$$

Let $\alpha \in A = \mathbf{Z}[\zeta]$ be such that $(\lambda) \not| (\alpha)$. Write $\alpha = f(\zeta)$, with $f \in \mathbf{Z}[x]$. Then $f(1) \not\equiv 0 \ (\ mod\ p)$ and $\Delta^{(n)}(f)$ is defined. For $1 \leq k < l - 1$, set $\Delta^{(k)}(\alpha) = \Delta^{(k)}(f)$. This definition is independent modulo p of the choice of f by the following:

LEMMA 1

For $1 \leq k < l - 1,\ G(x), F(x)\ \in \mathbf{Z}[x]$ *with* $G(1) \not\equiv 0 \ (mod\ p)$,

$$F(\zeta) = G(\zeta) \Rightarrow \Delta^{(k)}(F) \equiv \Delta^{(k)}(G) \ (mod\ p).$$

For $\alpha \in A$, let $\overline{\alpha}$ denote the complex conjugate of α.

Let $\alpha \in A$ *such that* $\lambda \not| \alpha$. *Then for positive integers* $1 \leq k < l - 1, i \geq 1$, *we have*

(a) $\Delta^{(k)}(\alpha^i) \equiv i\Delta^{(k)}(\alpha) \ (mod\ p)$.
(b) $\Delta^{(k)}(\overline{\alpha}) \equiv (-1)^k \Delta^{(k)}(\alpha) \ (mod\ p)$.
(c) $\Delta^{(k)}(\alpha^\sigma) \equiv r^k \Delta^{(k)}(\alpha) \ (mod\ p)$

LEMMA 2

Let $\eta \in A^*$. (i.e, η is a unit element).
For $1 < k < l - 1$, k *odd, we have*

$$\Delta^{(k)}(\eta) \equiv 0 \ (mod\ p).$$

Note: $\Delta^{(1)}(\zeta^k) \equiv k \ (mod\ p)$.

Lemma 1 and (a) are straightforward. Property (b) follows from (c). Property (c) is a consequence of a lemma proved by Vandiver [V4, p. 619]. Lemma 2 follows from Property (b) and the fact that any unit of A is a product of a root of unity and a real unit.

Proof of case I [For $p > 3$], when $\mathbf{Z}[\zeta]$ has unique factorization

$$\Delta^{(3)}(x + \zeta y) \equiv \Delta^{(3)}(\gamma) + \Delta^{(3)}(\beta^p) \quad (mod\ p) \quad (\text{ by Lemma 1})$$

$$\Delta^{(3)}(x + \zeta y) \equiv p\Delta^{(3)}(\beta) \equiv 0\ (mod\ p) \text{ by Lemma 2 and (a)}$$

$$\Delta^{(3)}(x + \zeta y) = \left.\frac{d^3}{dv^3} log(x + e^v y)\right|_{v=0} = \frac{xy(x-y)}{(x+y)^3}.$$

Since $p \not| xyz$, we get $x - y \equiv 0\ (mod\ p)$. We had $x^p + y^p = z^p$. Note that the roles of x, y, z can be taken by $x, -z, y$ or $y, -z, x$ in this equation as well as the arguments above. Hence we also get $x + z \equiv y + z \equiv 0\ (mod\ p)$. Thus $x \equiv y \equiv -z\ (mod\ p)$. Reducing $x^p + y^p = z^p$ modulo p, we get $x + y - z \equiv 0\ (mod\ p)$. This gives $3x \equiv 3y \equiv 3z \equiv 0\ (mod\ p)$. Since $p > 3$, we have a contradiction.

[For $p = 3$, the proof is even simpler: Reduce everything mod 9 to get $x^3 + y^3 \equiv \pm 1 + \pm 1 \equiv \pm 1\ (mod\ 3)$, which is impossible.]

When Unique Factorization Fails

In 1847 Cauchy and Lamé (apparently) tried to prove FLT along these lines, and Kummer pointed out that Lamé assumed that the elements of $\mathbf{Z}[\zeta]$ have unique factorization property. This is true for primes upto 19, but fails for $p = 23$. (But the argument outlined above remained the basic line of attack for most work on FLT using cyclotomic fields. One simply tries to come up with the same type of equation as $x + \zeta y = \gamma\beta^p$ *without* the help of unique factorization in $\mathbf{Z}[\zeta]$.)

Dedekind domains and Unique Factorization into Ideals

Kummer set out to rectify this by introducing the "ideal numbers." Starting with elements in $\mathbf{Z}[\zeta]$ (which he called cyclotomic integers) he considered all multiples of a given number as an ideal number and also considered sets generated by two or more cyclotomic integers as "divisors." These were the precursors of **ideals**, with the former now called principal ideals.

It turned out that the *Ideals of the ring of algebraic integers of any number field (finite extension of* $\mathbf{Q} \subset \mathbf{C}$ *) factor uniquely into products of prime ideals.*

[So now we can deduce $(x + \zeta y) = I^p$ in case I or $\frac{x+\zeta y}{\lambda} = I^p$ in case II.]

In fact, it turned out that the ring of algebraic integers are an example of *Dedekind domains,* (Noetherian, integrally closed, and every prime ideal is a maximal ideal) in which ideals not only unique factor into prime ideals but also form a multiplicative group called the **Ideal Class Group** with the class of principal ideals as the identity element. Kummer proved that the ideal class group of a cyclotomic number field is always *finite.*

Moreover, *A Dedekind ring is a UFD iff it is a PID*

The Ideal Class Group, Regular and irregular primes

To fix notations,

p is an odd prime, ζ is a primitive p-th root of unity, and $\lambda = 1 - \zeta$.

$K = \mathbf{Q}(\zeta)$ is the cyclotomic field, $A = \mathbf{Z}[\zeta]$ its ring of integers, and A^* the group of units in A.

$G = Gal(K/\mathbf{Q})$, σ is a generator of G and $\sigma(\zeta) = \zeta^r$, where r is a primitive generator of $(\mathbf{Z}/l\mathbf{Z})^*$.

C is the ideal class group of K, h the order of C, and C_p its p-Sylow subgroup.

$K^+ = \mathbf{Q}(\zeta + \zeta^{-1}) =$ Maximal real subfield of K . A^+, C^+, h^+, and C_p^+ are defined similarly.

If I is an ideal in A, then $[I]$ is its ideal class in C.

Kummer defined the **regular primes** as those for which $p|h$.

He proved (1850) that FLT is true for all regular primes.

(The regular primes are believed to form about 61% of all primes, but it is an open problem to show that they form an infinite set. But the irregular primes are known to be infinite! [Jensen, 1915])

For the first case, for instance, we already have $(x + \zeta y) = I^p$. From this we get $[I^p] = 0$. $p \not| h$, so this means $[I] = 0$. So I is principal and we can complete the proof as before.

h, h^+, and the Bernoulli numbers

Kummer found a formula for h as a product of two numbers, both positive integers, one of which turned out to be h^+. Let $h^- = h/h^+$. He expressed h^- in terms of *Bernoulli numbers* and h^+ in terms of logarithms of certain special units. He seemed to have believed that p never divides h^+. This statement is now known as the *Kummer-Vandiver conjecture.*

We actually have $p|h^+ \rightarrow p|h^-$. So in particular, if p is regular then p does not divide h^+. This helped him to prove the second case of FLT for regular primes.

The Bernoulli numbers

The Bernoulli numbers B_m are defined by $\dfrac{t}{e^t-1} = \sum_{m=0}^{\infty} B_m \dfrac{t^m}{m!}$.

Some examples are $B_0 = 1,\ B_1 = -1/2,\ B_2 = 1/6,$
$B_4 = -1/30,\ B_6 = 1/42,\ B_8 = -1/30,\ B_{10} = 5/66,\ B_{12} = -691/2730, ...$ and all odd Bernoulli numbers are zero for $n > 1$.

Kummer proved that $p|h^-$ *iff* p *divides the numerator of one of the Bernoulli numbers* $B_2, B_4, B_6, \ldots B_{p-3}$.

The irregular primes

The first irregular prime is 37. Proving FLT for irregular primes remained, and still is, very difficult, using the same techniques. Only special cases have been proved using cyclotomic fields.

Cauchy proved that case I is true if p does not divide B_{p-3}. This was extended by Kummer and others later, using the following result of Kummer:

If $x^p + y^p + z^p = 0$, *and* p *doesn't divide* z, *and* $(x, y, z) = 1$, *then* $\Delta^{(p-2s)}(x + \zeta y)B_{2s} \equiv 0\ (mod\ p)$ *for* $2s = 2, 4, ..., p - 3$.

Using this and its refinement by Mirimanoff, Wieferich and others were able to prove the following criterion which was used to verify FLT numerically as mentioned in the beginning:

If the first case were false, then $q^{p-1} \equiv 1\ (mod\ p)$ *for the primes* $q = 3, 5, 7, ..., 41, 43$.

For irregular primes, Kummer was able to prove FLT only under further conditions and he verified that these conditions were met by 37, 59, and 67. The rest of the primes under 100 are regular, so Kummer was able to prove FLT only upto 100.

Vandiver proved that if p divided only one of $B_2, B_4, ..., B_{p-3}$ and this Bernoulli number is not divisible by p^3, then FLT holds for p. Using this and similar theorems, he was able to verify FLT upto $p = 269$. He also claimed that the first case of FLT is true if p did not divide h^+, but his proof was found to be flawed.

Obviously, to use the cyclotomic approach further, one needed more information about the field and its class group. This was provided by the development of Class Field Theory by Hilbert, Hasse, Furtwangler, Takagi and others. While this yielded more results about FLT, a complete proof proved far out of reach. But these new theories led to the rapid development of number theory, culminating in the proof of the Shimura-Taniyama-Weil conjecture.

The generalized Bernoulli numbers and the finer structure of the class group

The Teichmüller character $\omega : \mathbf{Z}_p \to \mathbf{Z}_p^*$ is given by $\omega(x) \equiv x \pmod p$, where $\omega(x)$ is a $p-1$-st root of unity, and $x \in \mathbf{Z}_p$.

It generates the group of (Dirichlet) characters of $(\mathbf{Z}/p\mathbf{Z})^*$ to which $Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$ is isomorphic.

Under the action of $Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$ through this character, C_p decomposes as a direct sum of $C_p^{(i)}$, where $C_p^{(i)}$ is the eigenspace corresponding to ω^i. Let the order of $C_p^{(i)}$ be p^{h_i}.

The generalized Bernoulli numbers B_{m,ω^j} are defined by

$$\sum_{a=1}^{p-1} \frac{\omega^j(a) x e^{ax}}{e^{(p-1)x} - 1} = \sum_{m=0}^{\infty} B_{m,\omega^j} \frac{x^m}{m!}.$$

We have $B_{m,1} = B_m$ and also the following congruence:
If n is odd and $p-1$ doesn't divide $n+1$, then

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod p.$$

Not surprisingly, (j is odd),

$$h^- = 2p \prod_{j=1}^{p-2} B_{1,\omega^j}$$

Similar to the definition of $C_p^{(i)}$, if V_p is the $\mathbf{Z}/p\mathbf{Z}$ vector space C_p/C_p^p, let $V_p^{(i)}$ be the eigenspace consisting of elements on which G acts via ω^i. We have the following criterion due to Herbrand (1932) and Ribet (1976):

$$V_p^{(i)} \neq 0 \Leftrightarrow p|\mathbf{B}_{p-i}.$$

This was further refined in 1984 by Mazur and Wiles (and independently by Kolyvagin) who proved that

if j is odd and p doesn't divide $j-1$, then the exponent of p dividing $|C_p^{(j)}|$ and $B_{1,\omega^{-j}}$ are equal.

The following result of Kurihara is a consequence of the proof of the main conjecture for cyclotomic fields due to Mazur-Wiles [MW] (a cyclotomic proof of the main conjecture follows from the work of V. Kolyvagin [Ko]), the computation of $K_4(\mathbf{Z})$ by Lee and Sczcarba, and the surjectivity, due to C. Soulé, for $p > 2$ of the p-adic Chern class map $c_p : K_4(\mathbf{Z}) \otimes \mathbf{Z}_p \longrightarrow H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(3))$.

$C_p^{(p-3)} = 0$ and $C_p^{(3)}$ is cyclic.

[This was independently observed by R. Greenberg]

Using these results, one can prove:

For every $n \geq max(1, h_3)$, the equation $x^{p^n} + y^{p^n} + z^{p^n} = 0$ has no integral solutions (x, y, z) with $p \not| xyz$.

(After Wiles) the following for a fermat-type equation:

Let $p > 3$, and c an integer divisible only by primes of the form $kp - 1, (k, p) = 1$.

Assume p is irregular, and $p|B_{p-3}$. Let q be an odd prime such that $q \equiv 1 \ (mod\ p)$, and there is a prime ideal Q over q in $\mathbf{Q}(\zeta)$ whose ideal class generates $C_p^{(3)}$, which is known to be cyclic. If $x^p + y^p = pc\ z^p$ has nontrivial integer solutions, then $q \not| \frac{pc\ z^p}{x+y}$.

If p is regular, we can prove that this equation has no solutions using some results of Vandiver.

References

P. Ribenboim *Thirteen Lectures on Fermat's Last Theorem* Springer-Verlag, 1979

S. Sitaraman Ph.D Thesis, California Institute of Technology, 1994

S. Sitaraman, *Vandiver Revisited*, Journal of Number Theory, vol. 57, 1996.

S. Sitaraman, *On a Fermat-type diophantine equations*, to appear.

H.S. Vandiver *Fermat's last theorem and the second factor in the cyclotomic class number* Bull. of Amer. Math. Soc., 1934

L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag 1982

H. Edwards, *Fermat's Last Theorem*, Springer Verlag, 1977.

S. Lang, *Algebraic Number Theory* , Addison-Wesley, 1970.

D. Marcus, *Number Fields*, Springer Verlag.

A. Wiles *Modular Elliptic Curves and Fermat's Last Theorem* Annals of Math. vol 141, 1995

R. Taylor and A. Wiles *Ring theoretic properties of certain Hecke algebras* Annals of Math., vol 141 , 1995.