New Proof of Fermat's last Theorem by Final - Main HM Theorem

Seyyed Mohammad Reza Hashemi Moosavi

Abstract

In this article by providing an elliptic curve **HM** (Non – Singular cubic curve **HM**), we prove that Fermat's Last Theorem (**FLT**) for every odd number except one is a special case of an elliptic curve of **HM** and in fact this (flexibility) reduction of Fermat's equation (in the form of an elliptic curve) has helped to prove **FLT** in short and cross – cut and brought to fruition the idea of elliptic curve short and understand able for final proof of **FLT** for every odd number greater than one. We know about the history of **FLT** and proving special cases of $n=3$ and $n=4$ in an independent way and about trends of a controversial and wanderful ideas of general case of $n \geq 3$ in which the most important ones are Wiles' Theorem and Taylor – Wiles regarding proving Taniyama – Shimura – Weil conjecture for elliptic curves.

Key Words: Equation – Theorem – Elliptic – Curve – Conjecture

- **Introduction**

  We know about the history of Fermat's Last Theorem and proving special cases of $n = 3$ and $n = 4$ in an independent way and about trends of controversial and wonderful ideas of general case of $n \geq 3$ in which the most important ones are Wile's Theorem and Taylor – Wiles regarding proving Taniyama – Shimura – Weil conjecture for elliptic curves.

- **Introduction to Fermat's Last Theorem & Elliptic curves**

  The announcement of year 1993 the Fermat's Last Theorem was an exciting event for the entire mathematics community. This Introduction will discuss the mathematical history of Fermat's Last Theorem (which we will abbreviate throughout as **FLT**), broken up into the following periods:

  1. Diophantus to Euler (250-1783 A.D.)
  2. Euler to Frey (1783 – 1982 A.D.)
  3. Frey to Wiles (1982 – 1993 A.D.)

  We will give only an Introduction to the story of **FLT**, and out account is by no means definitive. I hope that the Introduction succeeds in conveying the flavor of this truly wonderful mathematics.

  Hence the basic claim of **FLT** is that the equation $x^n + y^n = z^n$ has no solutions when x, y, z are nonzero integers and $n > 2$.

1. Diophantus to Euler

Generations of mathematical historians have debated over whether Fermat really did have a Proof, though many experts doubt that he did.

For one thing, the equation $x^n + y^n = z^n$ was atypical for Fermat – the vast majority of the other equations he studied dealt with $\text{exponents} \leq 4$.

Also, in his correspondence, he only stated **FLT** for the exponent $n=3$. As for Fermat's "marvelous proof ", it probably used the technique of infinite descent. His descent argument for $n=4$ is actually known; it can be found in Fermat's proof that the area of a right triangle with integral sides cannot be a square. This proof is given in one of his marginal notes, although even here, Fermat complains that there isn't enough room to give 3the proof "with all detail". It seems likely that Fermat thought that his proofs for $n=3$ and $n=4$ generalized, and they almost certainly didn't.

2. **Euler to Frey.** This section is only a sketch of more than two hundred years of beautiful and wonderful number theory. Here are some of the highlights of the 19th century work on **FLT**:

- By the early 1800s, all of Fermat's problems were solved except for **FLT** (thus justifying the name, **FLT**).
- 1816 – The French Academy announces a prize for a solution to **FLT**.
- In the 1820's Sophie Germain shows that if p and $2p+1$ are prime, then $x^P+y^P=z^P$ has no solution with $p\nmid xyz$. This is the so – called case I of **FLT**. (Case II is where $p\mid xyz$ and is usually regarded as being much harder).
- 1825 – Dirichlet and Legendre prove **FLT** for $n=5$.
- 1832 – Dirchlet, after trying to prove it for $n=7$ (proves **FLT** for $n=14,21,28,\ldots,7k$).
- 1839 – Lame' prove **FLT** for $n=7$.
- 1847 – Lame' and Cauchy present false proofs of **FLT** for general n.
- 1844 – 1857 – kummer's work on **FLT**:
  - 1847 – Theorem: **FLT** hold for p if $p\nmid h$ (such p are called regular primes).

- 1847 – Theorem: p is regular if p doesn't divide the numerator of the Bernoulli numbers $B_2, B_4, \ldots, B_{P-3}$. (We can define the Bernoulli numbers by the power series: $\frac{x}{e^x - 1} = \sum_{n=1}^{\infty} \frac{Bn}{n!} x^n$).
  - A corollary of this result is that for $p < 100$, only 37, 59 and 67 are irregular.
  - 1850 – The French Academy offers a second prize for a solution to **FLT**.
  - 1856 – At Cauchy's suggestion, the Academy withdraws the prize and then awards a medal to kummer.
- 1857 – kummer develops complicated criteria for proving **FLT** for certain irregular primes. There are some gaps in his proofs which are later filled in by Vandiver in the 1920s. These results establish **FLT** for $p < 100$.

Here are some highlights of the history of **FLT** after kummer's.

- 1908 – The Wolfskehl prize for a solution to **FLT** is announced. Later inflation in the German mark reduces the value of this prize considerably, but does not reduce the flow of crank solutions submitted.
- 1909 – Wieferich proves $x^P + y^P = z^P$ and $p \nmid xyz$ (case I of **FLT**),

  then $2^{P-1} \overset{P^2}{\equiv} 1$. This is a strong congruence which is particularly easy to check on a computer.
- 1953 – Inkeri proves that if $x^P + y^P = z^P$ and $x < y < z$, then $x > \left(\left(2p^3 + p\right)/\log\left(3p\right)\right)^p$ in case I and $x > p^{3p-4}$ in case II.
- 1971 – Brillhart, Tonascia and Weinberger show that case I of **FLT** is true for all primes less than 3.10^9.
- 1976 – Wagstaff shows that **FLT** is true for all primes less than $125{,}000$.

There results imply that any counterexample to **FLT** must involve $p \geq 125{,}003$ and $z > y > x > \left(125{,}003\right)^{375{,}005} \approx 4.5 \cdot 10^{1{,}911{,}370}$ (In 1992, as a byproduct of other computations, the lower bound on the exponent was raised to $p > 4{,}000{,}000$).

3. **Frey to Wiles.** In 1983, Fatlings proved the Morell's Conjecture, which implies that a polynomial equation with rational coefficients $Q\left(x,y\right)=0$ has only finitely many rational solutions when the curve has $genus \geq 2$ (for a definition of genus, see the sidebar "The genus of an algebraic curve"). Since $x^n + y^n = 1$ has $genus \geq 2$ for $n \geq 4$, there are only finitely many rational solutions by the Mordell's Conjecture. Then clearing denominators, it follows easily that $x^n + y^n = z^n$ has only finitely many relatively prime integer solutions.

Attention (The genus of an algebraic curve)

- The genus of a curve given by a polynomial equation $p(x,y)=0$ of degree n can be defined in a variety of ways. When the equation is sufficiently smooth (which is true for the Fermat's curve $x^n + y^n = 1$), then the genus is $g = \left(n-1\right)\left(n-2\right)/2$. This $is \geq 2$ when $n \geq 4$.
- Topologically, the solutions of $p\left(x,y\right)=0$ over the complex numbers form a compact Riemann surface minus a finite set of points, and then the genus is just the usual genus of this compact real 2 – dimensional manifold.
- Analytically, a Riemann surface is a compact complex 1-dimensional manifold, and one can define the notion of a holomorphic 1-form. Then the genus is the maximum number of linearly independent holomorphic 1 – forms on the surface.

- For example, the Riemann sphere has genus Zero, so that there are no holomorphic 1- form, while the elliptic curve

$$y^2 = Ax^3 + Bx^2 + Cx + D$$

has genus 1, and up to a constant, dx/y is the only holomorphic 1-form.

- Granville and Heath – Brown, aided by an observation of Filaseta, used the above finiteness result to show that FLT holds for "most" exponents, in the sense that if you look at all exponents – prime and composite – from 3 to n, the percentage where FLT could fail approaches Zero as n increases.
- Adelman and Heath – Brown showed that case I of FLT was true for infinitely many prime exponents.
- By the end of the 1980's, there were several conjectures in number theory which, if proved, would imply FLT, though sometimes only for sufficiently large exponents (see the sidebar "Conjectures that imply Fermat's Last Theorem "). This showed that FLT was not an isolated oddity, but rather was intimately connected to other parts of number theory. Frey showed that nontrivial Solution to FLT give rise to very special elliptic curves, which we shall call Frey curves. His basic insight was that Frey curves were so special that they couldn't be modular. Hence, if the Taniyama – Shimura conjecture were true, Frey curves couldn't exist, and FLT would follow.

  If $a^P + b^P = c^P$ is a solution to FLT, then the associated Frey curve is (Δ_F : The minimal discriminant of the Frey curve)

$$y^2 = x\left(x - a^P\right)\left(x + b^P\right),\ \Delta_F = 2^{-8}\left(abc\right)^{2P}$$

  As usual, we assume a, b, c, are nonzero relatively prime integers and P is an odd prime. This is an elliptic curve over the rational numbers Q, similar to the equation

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

Considered by Fermat. In general, an elliptic curve over Q is given by an equation of the form

$$y^2 = Ax^3 + Bx^2 + Cx + D$$

Where A, B, C, D are rational and the cubic polynomial in x on the right hand side of the equation has distinct roots. Elliptic curves are a large and important part of modern number theory.

- **Attention (Elliptic curves).** The Taniyama – Shimura Conjecture states that all elliptic curves over rational numbers are modular. As we will explain, the work of Frey, Sere and Rabbet shows that this Conjecture implies FLT for all exponents.

- **Elliptic curves**

Elliptic curves are a special kind of algebraic curves which have a very rich arithmetical structure.

There are several fancy ways of defining them. But for our purposes we can just define them as the set of points satisfying a polynomial equation of a certain form. To be specific, consider an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Where the a_i are integers (There is a reason for the strange choice of indices on the a_i, but we won't go into it here). We want to consider the set of points (x, y) which satisfy this equation.

To make things easier, let us focus on the special case in which the equation is of the form

$$y^2 = x^3 + Ax^2 + Bx + C = g(x) \quad (*)$$

With $g(x)$ a cubic polynomial (in other words, we're assuming $a_1 = a_3 = 0$). In this case (*), it's very easy to determine when there can be singular points, and even what sort of singular points they will be. If we put

$$f(x,y) = y^2 - g(x),$$

Then we have

$$\frac{\partial f}{\partial x}(x,y) = -g'(x) \text{ And } \frac{\partial f}{\partial y}(x,y) = 2y,$$

We know, the curve will be smooth if there are no common solutions of the equations

$$f(x,y) = 0 \ , \ \frac{\partial f}{\partial x}(x,y) = 0 \ , \ \frac{\partial f}{\partial y}(x,y) = 0 \quad (**)$$

Attention

We know, from elementary analysis, that an equation $f(x,y) = 0$ defines a smooth curve exactly when there are no points on the curve at which both partial derivatives of f vanish.

In other words, the curve will be smooth if there are no common solutions of the equations (**).

And the condition for a point to be "bad" be comes

$$y^2 = g(x) \ , \ -g'(x) = 0 \ , \ 2y = 0$$

Which boils down to $y = g(x) = g'(x) = 0$. In other words, a point will be "bad" exactly when its y - coordinate is Zero and its x - coordinate is a double root of the polynomial $g(x)$. Since $g(x)$ is of degree 3, this gives us only three possibilities:

- $g(x)$ has no multiple roots, and the equation defines an elliptic curve (Three distinct roots), (For example, elliptic curve $y^2 = x^3 + x$ has three distinct roots).
- $g(x)$ has a double root (curve has a node), (For example, curve $y^2 = x^3 + x^2$ has a node).
- $g(x)$ has a triple root (curve has a cusp), (For example, curve $y^2 = x^3$ has a cusp).

Attention

If x_1, x_2 and x_3 are the roots of the polynomial $g(x)$, the discriminant for the equation $y^2 = g(x)$ turns out to be $\left(g(x) = 0\right)$

$$\Delta = k(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

where k is a constant.

This does just what we want:

If two of the roots are equal, it is Zero, and if not, not. Furthermore, it is not too hard to see that Δ is actually a polynomial in the coefficients of $g(x)$, which is what we claimed. In other words, all that the discriminant is doing for us is giving a direct algebraic procedure for determining whether there are singular points.

While this analysis applies specifically to curves of the form $y^2 = g(x)$, it actually extends to all equations of the sort we are considering there is at most one singular point, and it is either a node or a cusp.

Attention

With some examples in hand, we can proceed to deeper waters. In order to understand the connection we are going to establish between elliptic curves and Fermat's Last Theorem, we need to review quite a large portion of what is known about the rich arithmetic structure of these curves.

Conclusion

Elliptic curve of the form

$$y^2 = x^3 + Ax^2 + Bx + C = g(x)$$

is a elliptic curve of Non – Singular if $g(x)$ has not a double root or

a triple root. In fact below equation

$$g(x) = x^3 + Ax^2 + Bx + C = 0$$

has three distinct roots, if

$$\Delta_{HM} = \left(AB - 9C\right)^2 - 4\left(A^2 - 3B\right)\left(B^2 - 3AC\right) \neq 0$$

Attention

If $\Delta_{HM} \neq 0$ then $g(x)$ has no multiple roots, and $y^2 = g(x)$ is a

Non –Singular cubic elliptic curve.

Here now, we offer Main & Final HM theorems.

- **Main HM Theorem (Reducing Fermat's equation to equation hm)**
  If $(h,m) = 1$ and Fermat's equation

  $$p > 2 \ , \ abc \neq 0 \ ; \ a^P + b^P = c^P \ \ (*)$$

  have non-Zero answers, then generalized equation hm should have answer like this

  $$(h,m) = 1 \ , \ x^h + y^h = z^m \ \ (**)$$

  Reverse, if equation (**) for $h = p$ for at least one $m \geq 2$ has no answer, then Fermat's equation (*) for p has no answer.
- **Final HM Theorem (Reducing (*) to cubic elliptic curve)**

Fermat's equation (*) with the condition of $(m,p) = 1$ is reducable to

$$\left|\begin{array}{l} \text{I. } x^{m}+y^{m+1}=z^{m^2+m+1} \\ \text{II. } x^{m}+y^{m^2+m+1}=z^{m+1} \\ \text{III. } x^{m+1}+y^{m^2+m+1}=z^{m} \end{array}\right. \quad (***)$$

If for $m \geq 2$ with the condition of $(m,p)=1$ one equation (***) has no answer then FLT is established.

For example, for $m=2$ and (odd numbers) $p \geq 3$ with the condition $(2,p)=1$ is always true and equation (*) is reducable to an elliptic curve of cubic like this $u^2-v^3+kw^3=0$ or $F(H,M)=H^2-M^3-AM^2-BM-C=0$.

Conclusion

Fermat's equation (*) for every (odd numbers) $p \geq 3$ is reducable to a cubic curve.

> **Theorem.** The equation $a^P+b^P=c^P$ has no solutions with a,b,c nonzero for p an prime.
>
> **Proof.** Suppose there were a solution $a^P+b^P=c^P$, with our usual assumptions about p and a,b,c. Then we have a Frey curve and according to corollary of "The Frey curve is modular" has a cusp form F of weight **2** and level N, where N is the conductor. The Frey curve also has a Galois representation p on the points of order p on the curve (we won't define precisely what this means). The cusp form F is linked to the representation p in an especially nice way.
>
> Serre's level reduction conjecture deals with the pair (p,F), and according to the hypotheses of the conjecture are satisfied for all odd primes l dividing N. In such a case, the conjecture asserts that there is a cusp form F' of weight **2** and level N/l with

$$F' \overset{P}{\equiv} F$$

and F' is also an eigen – form for the appropriate Hecke algebra (it takes some work to define what it means for modular forms to be congruent modulo p). This congruence means that F' is linked to p in the same way F was, except that F' has smaller level N/l . But then, if l' is another odd prime dividing N, we can apply the level reduction conjecture to the pair (P, F') and get a cusp form F'' with even smaller level N/ll', and then apply it again to (P, F''), etc. Eventually we get a cusp form $\tilde{F}$ of weight 2 and level 2 (b is even). Here is a diagram of the argument so far:

Solution of FLT
→ Frey curve
→ Cusp form of level N
→ Cusp form of level N/l
→ Cusp form of level N/ll'
□
→ Cusp form of level 2

But it is well known that there are no cusp forms of weight 2 and level 2 (see the sidebar "The modular curve $X_0(N)$"). Hence the above diagram self – destructs, and Fermat's Last Theorem is proved! Q.E.D. This brings us to the end of **FLT**, but certainly not to the end of the story.

- There is a lot more to say about the mathematics involved in the proof of Fermat's Last Theorem!. We can now offer the new proof.

- **Final – Main HM Theorem**

For every odd number $p \geq 3$ Fermat's Last Theorem ($abc \neq 0$):

$$a^P + b^P = c^P$$

Special case is of an elliptic curve (Non – Singular Cubic Curve) HM:

$$H^2 = M^3 + \left(3S^P\right)M^2 + \left(3S^{2P}\right)M + \left(S^{3P} + S^P\right) \ (*)$$

- **Proof:**

It is enough in the below general elliptic curve:

$$y^2 = x^3 + Ax^2 + Bx + C \ (**)$$

Or elliptic curve HM (*) we assume:

$$\left|\begin{array}{l} y = H = \left(ac^{\frac{3P-5}{2}}\right)^P \\ x = M = \left(ac^{P-2}\right)^P - \left(a^2bc^{3P-6}\right)^P \\ A = 3\ S^P = 3\left(a^2bc^{3P-6}\right)^P \\ B = 3\ S^{2P} = 3\left(a^2bc^{3P-6}\right)^{2P} \\ C = S^{3P} + S^P = \left(a^2bc^{3P-6}\right)^{3P} + \left(a^2bc^{3P-6}\right)^P \end{array}\right.$$

Then after replacing in (*) or (**):

$$\text{(odd numbers) } p \geq 3 \ : \ a^P + b^P = c^P$$

Attention

- Elliptic curve (*) is Non – Singular.
- First Fermat's equation is multiplied λ_{HM}.
- We assume $R = M + S^P \ \left(R^3 + S^P = H^2\right)$.
- We know that Proofed $x^3 + y^3 = z^3$ is an elliptic curve.

Because:

$$y^2 = x^3 + Ax^2 + Bx + C;$$

$$H^2 = M^3 + \left(3S^P\right)M^2 + \left(3S^{2P}\right)M + \left(S^{3P} + S^P\right);$$

$$H^2 = \left(M^3 + 3S^P M^2 + 3S^{2P}M + S^{3P}\right) + S^P;$$

$$H^2 = \left(M + S^P\right)^3 + S^P;$$

$$\left| \begin{array}{l} H = \left(ac^{\frac{3P-5}{2}}\right)^P \\ M = \left(ac^{P-2}\right)^P - \left(a^2bc^{3P-6}\right)^P \\ S = \left(a^2bc^{3P-6}\right) \end{array} \right.$$

$$M + S^P = \left(ac^{P-2}\right)^P - \left(a^2bc^{3P-6}\right)^P + \left(a^2bc^{3P-6}\right)^P = \left(ac^{P-2}\right)^P$$

$$H^2 = \left(ac^{P-2}\right)^{3P} + \left(a^2bc^{3P-6}\right)^P = \left(ac^{\frac{3P-5}{2}}\right)^{2P};$$

(odd numbers) $p \geq 3 : \left(a^3 c^{3p-6}\right)^p + \left(a^2 b c^{3p-6}\right)^p = \left(a^2 c^{3p-5}\right)^p ;$

$$a^{3P} c^{3P^2-6P} + a^{2P} b^P c^{3P^2-6P} = a^{2P} c^{3P^2-5P} ;$$

$$a^{2P} c^{3P^2-6P} \left[a^P + b^P = c^P\right];$$

$$\left(\lambda_{HM} = a^{2P} c^{3P^2-6P}\right);$$

$$abc \neq 0 : a^P + b^P = c^P$$

Attention

- **Elliptic curve HM (*) is Non – Singular, because:**

$$M^3 + \left(3S^P\right)M^2 + \left(3S^{2P}\right)M + \left(S^{3P} + S^P\right) = 0 \ ;$$

$M_1 = -S^P - \sqrt[3]{S^P}$, $M_{2,3} = \alpha \pm i\beta$ **(Three distinct roots)**

- **References**

[1] Ezra Brown, Three Fermat Trails to Elliptic Curves, The College Mathematics Journal, 31 (2000), no. 3,167-172.

[2] David A. Cox, Introduction to Fermat's Last Theorem, American Mathematical Monthly, 101 (1994), no. 1, 3-14.

[3] Henri Darmon, A Proof of the Full Shimura – Taniyama – Weil Conjecture is announced, Notices of the American Mathematical Society, December 1999, 1397-1401.

[4] Harold M. Edwards, Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Springer – Verlag, New York, 1977.

[5] Fernando Q. Gouvea, A Marvelors Proof, American Mathematical Monthly, 101 (1994), no. 3, 203-222.

[6] Anthony W. Knapp, Elliptic Curves, Princeton University Press, Princeton, 1992.

[7] Barry Mazur, Number Theory as gadfly, American Mathematical Monthly 98 (1991), 593-610.

[8] Barry Mazur, on the Passage from local to global in number theory, Bulletin of the American Mathematical Society, 29 (1993), 14-50.

[9] Alf van der poorten, Notes on Fermat's Last Theorem, John Wiley & Sons, New York, 1996.

[10] Paulo Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer- Verlag, New York, 1979.

[11] Kenneth A. Ribet, and Brian Hayes, Fermat's Last Theorem, and Modern Arithmetic, American Scientist, 82 (1994), 144-156.

[12] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer- Verlag, New York, 1986.

[13] Joseph H. Silverman, and john H. Tatc, Rational Points on Elliptic Curves, Springer- Verlag, New York, 1992.

[14] Richard Taylor, and Andrew Wiles, Ring – theoretic Properties of certain Hecke algebras, Annals of Mathematics (2) 141 (1995), 553-572.

[15] Andrew Wiles, Modular elliptic curves and Fermat's last theorem Annals of Mathematics (2) 141 (1995), 443-551.

[16] Postnikov, Mikhail Mikhailovich, Fermat's Last Theorem (2000).

[17] S. M. R. Hashemi Moosavi, The Discovery of Prime Numbers Formula & It's Results (2003).

[18] S. M. R. Hashemi Moosavi, Generalization of Fermat's Last Theorem and Solution of Beal's Equation by HM Theorems (2016).

[19] S. M. R. Hashemi Moosavi, 31 Methods for Solving Cubic Equations and Applications (2016).