First Case of Fermat's Last Theorem

Student Research Seminar - 4

Gaurish Korpal*
gaurish4math.wordpress.com

August 20, 2016

Abstract

Fermat's Last Theorem (FLT) states that $x^n + y^n = z^n$ has no integer solution for $n > 2$. It is easy to show that if the theorem is true when n equals some integer r, then it is true when n equals any multiple of r. Since every integer greater than 2 is divisible by 4 or an odd prime, it is sufficient to prove the theorem for $n = 4$ and every odd prime. On 19^{th} September 1994, Andrew Wiles announced that he had finally completed the proof of FLT. Today we will see an *elementary proof* by Sophie Germain (1823) which can be extended to prove FLT for all prime exponents less than 1700.

1 Introduction

It is believed that Fermat knew the proof for $n = 4$. In 1760, Leonhard Euler gave elementary proof for $n = 3$ (apart from an ingenious algebraic proof in 1770) but it was incomplete and was completed by Adrien-Marie Legendre.

In 1823, Sophie-Marie Germain[1] proved FLT (using elementary methods) for all prime exponents $2 < p < 100$ by giving a prime q for which following theorem applies.

> Let p, q be distinct odd primes, and assume the following two conditions:
>
> 1. $p \not\equiv a^p \pmod{q}$ for any $a \in \mathbb{Z}$
> 2. If x, y, z are integers and if $x^p + y^p + z^p \equiv 0 \pmod{q}$ then q divides x, y or z.
>
> Then FLT holds for exponent p such that $p \nmid xyz$.

For example, if $p = 7$, $q = 29$, then both the conditions of the Germain's theorem are satisfied[1] and hence FLT is proved for $p = 7$.

In 1985, Étienne Fouvry[2], Leonard M. Adleman and David R. Heath-Brown[3] used a refinement of Germain's criterion together with difficult analytic estimates to prove that there are infinitely many primes p such that first case of FLT is true.

2 The Proof

I will follow the proof given on pp. 55 of [2].

On the contrary, assume that there exist relatively prime integers x, y, z which satisfy FLT, hence $x^p + y^p + z^p = 0$. Then by condition 2. it follows that q divides one of the integers x, y or z. Say, $q \mid x$ and $q \nmid yz$.

---

*3^{rd} year Integrated M. Sc. student at NISER, Bhubaneswar (Jatni), India

[1] Since women were not allowed in French Academy of Sciences, Adrien-Marie Legendre communicated the results and credited Germain for them.

[2] "Théorème de Brun-Titchmarsh; application au théorème de Fermat." *Inventiones Mathematicae* 79, no. 2 (1985), 383–407. http://dx.doi.org/10.1007/bf01388980

[3] Adleman, L. M. and Heath-Brown, D. R. "The first case of Fermat's last theorem." *Inventiones Mathematicae* 79, no. 2 (1985), 409–416. http://doi.org/10.1007/bf01388981

Exercise (Barlow-Abel relations)**.** *If pairwise relatively prime integers x, y, z are not multiples of p and satisfy FLT, $x^p + y^p + z^p = 0$, then for some integers t, t_1, r, r_1, s, s_1:*

$$\begin{aligned} x + y = t^p, &\quad \tfrac{x^p+y^p}{x+y} = t_1^p, &\quad z = -tt_1; \\ y + z = r^p, &\quad \tfrac{y^p+z^p}{y+z} = r_1^p, &\quad x = -rr_1; \\ z + x = s^p, &\quad \tfrac{z^p+x^p}{z+x} = s_1^p, &\quad y = -ss_1; \end{aligned}$$

such that $\gcd(t, t_1) = \gcd(r, r_1) = \gcd(s, s_1) = 1$, $p \nmid tt_1$, $p \nmid rr_1$, $p \nmid ss_1$, t_1, r_1, s_1 *are odd and greater than* 1.

Hint: All these statements are symmetrical so we just have to prove one of them and others follow. Since $x + y + z \equiv x^p + y^p + z^p = 0 \pmod p$, it follows that $-z \equiv x + y \pmod p$, so $p \nmid (x + y)$. Now

$$(-z)^p = x^p + y^p = \left(\sum_{k=0}^{p-1} x^k (-y)^{p-k-1} \right) (x + y) = Q_p(x, y) \cdot (x + y)$$

Note that $\gcd\left(Q_p(x, y), (x + y)\right) = \gcd\left(p, (x + y)\right) = 1$. By unique factorization of integers, $Q_p(x, y)$ and $(x + y)$ are p^{th} powers.

We can re-write the *Barlow-Abel relations* as

$$\begin{aligned} x &= -r^p + \tfrac{r^p+s^p+t^p}{2} = \frac{-r^p + s^p + t^p}{2}; \\ y &= -s^p + \tfrac{r^p+s^p+t^p}{2} = \frac{r^p - s^p + t^p}{2}; \\ z &= -t^p + \tfrac{r^p+s^p+t^p}{2} = \frac{r^p + s^p - t^p}{2}; \end{aligned}$$

where $r, s, t \in \mathbb{Z}$. Therefore we have

$$-r^p + s^p + t^p = 2x \equiv 0 \pmod q$$

But the condition 2. it follows that q divides r, s or t. Also, clearly $q \mid r$ and $q \nmid st$. By *Barlow-Abel relations* following congruences hold

$$\begin{aligned} y &\equiv -z \pmod q \\ t_1^p &\equiv y^{p-1} \pmod q \quad \text{because} \quad (x + y)t_1^p = x^p + y^p \\ r_1^p &\equiv pt_1^p \pmod q \quad \text{because} \quad r_1^p = \frac{y^p + z^p}{y + z} = \sum_{k=0}^{p-1} y^k (-z)^{p-k-1} \equiv py^{p-1} \equiv pt_1^p \pmod q \end{aligned}$$

Since $q \nmid t_1$, we have an integer t' such that $t't_1 \equiv 1 \pmod q$, then $(t'r_1)^p \equiv p \pmod q$. This contradicts the condition 1.

3 Birth of Cases

For primes p and $q = 2p + 1$ with $p \nmid xyz$, we will check that the conditions for above theorem holds. If $p \equiv a^p \pmod q$, then by using Euler's Criterion of quadratic residue and Fermat's Little Theorem:

$$a^{(q-1)/2} = a^p \equiv \pm 1 \pmod q \qquad \text{and} \qquad a^p \equiv p \pmod q$$

so $p \equiv \pm 1 \pmod q$ and this is impossible.

Now, suppose $x^p + y^p + z^p \equiv 0 \pmod q$ and $q \nmid xyz$. Since $p = (q - 1)/2$, using Euler's Criterion we can say that

$$x^p \equiv \pm 1 \pmod q, \qquad y^p \equiv \pm 1 \pmod q, \qquad z^p \equiv \pm 1 \pmod q$$

So, $0 = x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \pmod q$, which is impossible. Therefore we conclude that

For a prime p if $2p+1$ is also prime and $p \nmid xyz$, then there is no integer solution of $x^p + y^p = z^p$.

Based on this result, the statement of FLT is generally subdivided into two cases, with Germain's condition being the first case:

1. For the prime exponent p when there do not exist integers x, y, z such that $p \nmid xyz$ and $x^p + y^p = z^p$.

2. For the prime exponent p when there do not exist integers x, y, z all different from zero, such that $p|xyz$, $\gcd(x, y, z) = 1$ and $x^p + y^p = z^p$.

Interestingly, there doesn't exist an elementary proof for second case of FLT.

4 Sophie Germain Primes

If she could prove that there are infinitely many such primes p such that $2p + 1$ is also prime, now called *Sophie Germain primes*, then she would have been able to prove first case of FLT for infinite number of prime exponents. This year, 1^{st} April 2016, was Sophie Germain's 240th Birthday and 239 is 17th Sophie Germain prime (the next one is 251). But,

Nobody knows that whether there are infinitely many Sophie Germain primes.

Euler proved that if p is of the form $4k + 3$, then $2p + 1$ divides the Mersenne number, $M_p = 2^p - 1$. Thus, large Sophie Germain primes of the form $4k + 3$ lead to the largest known composite Mersenne numbers[6]. It has not yet been shown that there are infinitely many Mersenne composites. It is generally believed that there are an infinite number of Sophie Germain primes. In fact there is good reason to believe that there are about the same number of Germains as twin primes (prime numbers p such that $p + 2$ is also a prime). In both cases we have linear polynomials $2X + 1$, $X + 2$ respectively, and the question is whether they infinitely often assume prime values at primes[3].

5 But Why?

In 1970, Yuri Matiyasevich, following works of Martin Davis, Hilary Putnam and Julia Robinson proved that there is no hope of producing a complete theory of the subject of Diophantine Equations. Thus, there doesn't exist a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers. But the reason behind why equations of form $x^n + y^n = z^n$ and $ax^n + bz^n = c$ (especially for $a = c = 1, n = 2$) were (and are) still studied is their frequent occurrence in Algebraic Number Theory, a branch of number theory initially motivated by study of higher reciprocity laws.

References

[1] Dickson, L. E. "Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers." *Annals of Mathematics*, Second Series 18, no. 4 (1917): 161–187. http://dx.doi.org/10.2307/2007234

[2] Ribenboim, P. *13 Lectures on Fermat's Last Theorem.* New York: Springer-Verlag, 1979. pp. 55. http://dx.doi.org/10.1007/978-1-4684-9342-9

[3] Ribenboim, P. "1093." *The Mathematical Intelligencer* 5, no. 2 (1983): 28–34. http://dx.doi.org/10.1007/BF03023623

[4] Sampson, J. H. "Sophie Germain and the Theory of Numbers." *Archive for History of Exact Sciences* 41, no. 2 (1990): 157–161. https://dx.doi.org/10.1007/BF00411862

[5] Dalmédico, A. D. "Sophie Germain." *Scientific American* 265, no. 6 (December 1991): 116–122. https://dx.doi.org/10.1038/scientificamerican1291-116.

[6] Dubner, H. "Large Sophie Germain Primes" *Mathematics of Computation* 65, no. 213 (1996): 393–396 http://dx.doi.org/10.1090/s0025-5718-96-00670-9