Fermat's Last Theorem for the Case $n = 3$

Ananya V, Prasad H M
Department of Mathematics,Center for PG Studies and Research, St Philomena College, Puttur.
Email: ananyabhat42@gmail.com

Abstract: *Fermat's Last Theorem is one of the most difficult and famous problems in mathematics which was unsolved for more than 350 years. Fermat himself proved the theorem for the case n=4. Leonardo Euler gave the proof for the first odd prime number 3. But his proof was not complete. It contained a fallacious argument which he didn't recognize. To correct it by the most direct method, that of supplying an alternative proof of the statement for which Euler's proof is fallacious is not at all simple. Here in this paper we show how the proof can be corrected in a less direct way by bringing in arguments which Euler used to prove other propositions of Fermat. Thus we get a complete proof of the theorem for the case n=3.*

Key words: *Divisors, Factors, Cube, Prime, etc.*

Introduction

Fermat's last theorem was one of the very famous theorems which attracted the famous mathematicians of all times. Among all the famous theorems in the number theory Fermat's last theorem stands first being a theorem stated by a non mathematician by profession, Pierre De Fermat and proved by Andrew Wiles, three centuries after it was stated. Fermat's last theorem was recorded in Guinness Book of records as the "most difficult mathematical problems" being the theorem having largest number of unsuccessful proofs. The unsolved problem stimulated the development of algebraic number

theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among the most notable theorems in the history of mathematics. Fermat's last theorem states that, no three positive integers a, b, and c satisfy the equation $x^n + y^n = z^n$ for any integer value of n greater than 2. This theorem was first conjectured by Pierre De Fermat in 1637 in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin.

Euler was one of the great mathematicians of the times and he had interest in every field of mathematics. And here in this paper we study the contributions of Euler for the proof of Fermat's Last Theorem. The basic method of Euler's proof of the case $n = 3$ Fermat's method of infinite descent. He shows that if positive whole numbers x, y, z could be found for which $x^3 + y^3 = z^3$ then smaller positive whole numbers could be found with the same property, thus it would be possible to find a sequence of such triples of positive integers which continually decreased and never terminated, which is manifestly impossible. Therefore no such x, y, z can be found.

Euler's Proof of the Case n = 3

Let

$$x^3 + y^3 = z^3 \tag{1}$$

Step 1: Any factor which divided two of the numbers x, y, z would, by virtue of this equation, also divide the third. Therefore all common factors can be removed and one can assume at the outset that the numbers x, y, z are pairwise relatively prime. In particular, then, at the most one of the three numbers x, y, z is even. On the other hand, at least one is even because if x, y are both odd then z is even. Therefore exactly one is even.

Case 1: x, y are odd and z is even.

Then $x + y$ and $x - y$ are both even, say $2p$ and $2q$ respectively

$$\Rightarrow x = p + q, \qquad y = p - q$$

.

We have

$$\begin{aligned} & x^3 + y^3 = (x + y)(x^2 - xy + y^2) \\ \Rightarrow \quad & x^3 + y^3 = 2p[(p + q)^2 - (p + q)(p - q) + (p - q)^2] \\ & \qquad = 2p(p^2 + 3q^2) \end{aligned}$$

Since $p + q$ and $p - q$ are odd, p and q are of opposite parities. And they are relatively prime because any factor they had in common would divide both $x = p+q$ and $y = p-q$, and therefore could only be 1.

Moreover, p and q can both be assumed to be positive.

Therefore the assumption that $x^3 + y^3 = z^3$ is possible with x, y both odd, which implies that there exist relatively prime positive integers p, q of opposite parity such that

$$2p(p^2 + 3q^2) = cube$$

.

***Case 2**: z is odd and x or y is even .*

Let x be even and y and z be odd.

$$\begin{aligned} & \Rightarrow x^3 = z^3 - y^3 = (z - y)(z^2 + zy + y^2) \\ & Then, \quad z - y = 2p, \quad z + y = 2q, \quad z = p + q, \quad y = q - p \\ & And \quad x^3 = 2p[(q + p)^2 + (q + p)(q - p) + (q - p)^2] \end{aligned}$$

which leads to the same conclusion that $2p(p^2 + 3q^2) = cube$ where p, q are relatively prime positive integers of opposite parity.

Similarly we can reach at same conclusion if x is odd and y is even.

Step 2: Since p and q are of opposite parity $(p^2 + 3q^2)$ is odd.

Any common factor of $2p$ and (p^2+3q^2) would be a common factor of p and (p^2+3q^2) and therefore a common factor of p, $3q^2$.
Since $gcd(p,q) - 1$, this implies that the only possible common factor is 3.
But if $3 \mid p \Rightarrow 3 \mid (p^2+3q^2)$,then $2p$ and (p^2+3q^2) are not relatively prime.
The proof therefore splits into two cases, the one in which $3 \nmid p$ and consequently $gcd(2p, p^2+3q^2) = 1$ and the other in which $3 \mid p$.

Case 1: $3 \nmid p$ and consequently $2p$ and $(p^2+3q^2)$are relatively prime
Assume that 3 does not divide p and that $2p$ and (p^2+3q^2) are both cubes.
First we show that there exists two values a and b such that
$p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ with $gcd(a,b) = 1$ and a and b are of opposite parity.
We have $(a^2+3b^2)(c^2+3d^2) = (ac-3bd)^2 + 3(ad+bc)^2$
Consider ,

$$(a^2+3b^2)^3 = (a^2+3b^2)(a^2+3b^2)(a^2+3b^2)$$
$$(a^2+3b^2)^3 = (a^2+3b^2)((a^2-3b^2)^2 + 3(ab+ba)^2)$$
$$(a^2+3b^2)^3 = (a(a^2-3b^2) - 3b(2ab))^2 + 3(a(2ab) + b(a^2-3b^2))^2$$
$$(a^2+3b^2)^3 = (a^3-9ab^2)^2 + 3(3a^2b-3b^3)^2$$

Which is of the form p^2+3q^2 where $p = a^3-9ab^2$ and $q = 3a^2b-3b^3$
$\therefore$ one way to find cubes of the form p^2+3q^2 is to choose a,b at random and set, $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$, so that

$$p^2 + 3q^2 = (a^2+3b^2)^3$$

.
The major gap to be filled in Euler's proof is the proof that *this is the only way that* p^2+3q^2 *can be a cube*, that is, if p^2+3q^2 is a cube then there must be a, b such that p and q are given by the above

equations.
Assuming this fact we can proceed further as follows:
We have $p = a(a-3b)(a+3b)$ and $q = 3b(a-b)(a+b) \Rightarrow gcd(a,b) = 1$
Moreover, $2p = 2a(a-3b)(a+3b) = cube.$
The parities of a and b must be opposite.
Therefore $a-3b$, $a+3b$ are both odd and the only possible common factor of $2a$, $a+3b$ would be common factors of a, $a+3b$ and therefore of a,$3b$. Similarly, any common factor of $a+3b$ and $a-3b$ would be a factor of a and $3b$.
The only possible common factor is 3.
But $3 \nmid a$ because if it did it would divide p, contrary to assumption.
Therefore $2a$, $a-3b$, $a+3b$ are relatively prime and all three of them must be cubes, say $2a = \alpha^3$,$a-3b = \beta^3$,$a+3b = \gamma^3$
Then $\beta^3 + \gamma^3 = 2a = \alpha^3$ and this gives a solution of $x^3 + y^3 = z^3$ in smaller numbers than the original solution.
Therefore the descent has been accomplished in the case where $3 \nmid p$.

***Case 2*:** $3 \mid p$ and consequently $2p$ and $(p^2+3q^2)$are not relatively prime.
Then $p = 3s$ for some positive integer s and $3 \nmid q$.
Consider,

$$\begin{aligned} 2p(p^2+3q^2) &= 3.2s(3^2s^2+3q^2) \\ &= 3^2.2s(3s^2+q^2) \end{aligned}$$

Where $gcd[(3^2.2s),(3s^2+q^2)] = 1$ thus $(3^2.2s)$ and $(3s^2+q^2)$ are cubes.
By the above assumed fact $3s^2+q^2$ can be a cube only if

$$q = a(a-3b)(a+3b) \quad and \quad s = 3b(a-b)(a+b)$$

.
Since $3^2.2s$ is a cube, $3^3.2b(a-b)(a+b)$ a cube.

$\therefore b(a-b)(a+b)$ is a cube.
And $gcd(2b,(a-b),(a+b))-1$ $\therefore$they are cubes.
Let $2b=\alpha^3$,$(a-b)=\beta^3$,$(a+b)=\gamma^3$
Remaining proof follows by case1 of step 2. To complete the proof it remains to show that if p, q are relatively prime integers such that p^2+3q^2 is a cube then there must be integers a and b such that $p=a^3-9ab^2$ and $q=3a^2b-3b^3$. To get the above conclusion Euler used the set $\{a+\sqrt{(-3)}b : a,b\in\mathbb{Z}\}$ which forms a ring with unit.

Euler's Argument for Sufficient Condition for p^2+3q^2 to be a Cube

The sufficient condition: By factorizing and applying conjugate we get that in order to find a cube of the form p^2+3q^2 it suffices to set $p+q\sqrt{(-3)}=(a+b\sqrt{(-3)})^3$. Using the binomial theorem, it follows that in order to write p^2+3q^2 as a cube it suffices to find integers a and b such that $p=a^3-9ab^2$ and $q=3a^2b-3b^3$.
Now it remains to prove the necessary condition.

Remainder of the Proof

Euler's idea of computing with numbers of the form $a+b\sqrt{(-c)}$ is closely related to the use of the formula

$$(x^2+cy^2)(u^2+cv^2)=(xu-cyv)^2+c(xv+yu)^2$$

To prove the lemma needed to prove Fermat's Last Theorem in the case n = 3 we require to prove few of the following Propositions,

Proposition 1. *If a number which is a sum of two squares is divisible by a prime which is a sum of two squares then the quotient is a sum of two squares.*

Proof: Suppose $a^2 + b^2$ is divisible by $p^2 + q^2$ and that $p^2 + q^2$ is prime, then $p^2 + q^2$ divides $(pb - aq)(pb + aq) = p^2b^2 - a^2q^2$
$\Rightarrow (pb - aq)(pb + aq) - p^2(a^2 + b^2) - a^2(p^2 + q^2)$.
Since it is prime it must divide either $pb - aq$ or $pb + aq$.
Suppose $p^2 + q^2 \mid pb + aq$, then it follows that $p^2 + q^2 \mid (ap - bq)^2$.
Therefore the equation can be divided by the square of $p^2 + q^2$ and the result is an expression of $(a^2 + b^2)/(p^2 + q^2)$ as a sum of two squares as required. The second case, in which $p^2 + q^2$ divides $pb - aq$, can be handled in the same way.

Proposition 2. *If a number of the form $a^2 + 3b^2$ is divisible by 2 then it must be divisible by 4, and its quotient by 4 must itself be of the form $c^2 + 3d^2$.*

Proof: If a and b have opposite parities then $a^2 + 3b^2$ is not divisible by 2. If a and b are both even, then $a^2 + 3b^2$ is divisible by 2^2 and the quotient is of the form $c^2 + 3d^2$ with $c = \frac{a}{2}, d = \frac{b}{2}$.
Consider the case where a and b are both odd.
Then $a = 4m \pm 1$ and $b = 4n \pm 1$ when m and n and the signs are properly chosen. Therefore either $a + b$ or $a - b$ is divisible by 4.
If $a + b$ is divisible by 4 then

$$\begin{aligned} 4(a^2 + 3b^2) &= (1^2 + 3.1^2)(a^2 + 3b^2) \\ &= (a - 3b)^2 + 3(a + b)^2 \end{aligned}$$

is divisible by 4^2 and it follows that $(a^2 + 3b^2)/4$ is of the form $c^2 + 3d^2$.
If $a - b$ is divisible by 4 then again we reach at same conclusion by making appropriate changes.

Proposition 3. *If a number of the form $a^2 + 3b^2$ is divisible by a prime of the form $p^2 + 3q^2$ then the quotient can be written in the form $c^2 + 3d^2$.*

Proof: We observe that

$$\begin{aligned}(pb - aq)(pb + aq) &= p^2b^2 + 3q^2b^2 - 3q^2b^2 - a^2q^2 \\ &= b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)\end{aligned}$$

is divisible by $p^2 + 3q^2$ and therefore, since $p^2 + 3q^2$ is prime, that either $pb - aq$ or $pb + aq$ is divisible by $p^2 + 3q^2$.
Therefore

$$\begin{aligned}(p^2 + 3q^2)(a^2 + 3b^2) - [p^2 + 3(\pm q)^2](a^2 + 3b^2) \\ = (pa \pm 3qb)^2 + 3(pb \pm aq)^2\end{aligned}$$

can be divided by $(p^2 + 3q^2)^2$ when the sign is chosen correctly and it follows that $(a^2 + 3b^2)/p^2 + 3q^2$ has the desired form.

Proposition 4. *If a number which can be written in the form* a^2+3b^2 *has an odd factor which is not of this form then the quotient has an odd factor which is not of this form.*

Proof: Let $xy = a^2 + 3b^2$ where x is odd. If y is even then by Porposition(1) it is divisible by 4 and $x(y/4) = c^2 + 3d^2$.
This process can be repeated until $y/4^k$ is odd.
Therefore $y = p_1p_2...p_n$ where each of the p's is either 4 or an odd prime.
If all of the odd primes in this factorization of y can be written in the form $c^2 + 3d^2$ then $xy = a^2 + 3b^2$ can be divided successively by each of the p's and proposition 2 imply that x can be written in the form $c^2 + 3d^2$. Therefore if x does not have this form then y must have an odd factor not of this form.

Proposition 5. *If a and b are relatively prime then every odd factor of* $a^2 + 3b^2$ *is of the form* $c^2 + 3d^2$.

Proposition 6. *If a and b are relatively prime and if* $a^2 + 3b^2$ *is cvcn thcn* $a + b\sqrt{(}-3)$ *can bc writtcn in thc form*

$$a + b\sqrt{(}-3) = (1 \pm \sqrt{(}-3))(u + v\sqrt{(}-3))$$

where the sign is appropriately chosen and where u and v are integers.

Proof: Since a^2+3b^2 is even, a and b must have the same parity, and since they are relatively prime they must both be odd.
Therefore each is of the form $4n \pm 1$ and either $a+b$ or $a-b$ must be divisible by 4.
If $a+b$ is divisible by 4 then the equation

$$\begin{aligned} 4(a^2+3b^2) &= (1^2+3.1^2)(a^2+3b^2) \\ &= (a-3b)^2+3(a+b)^2 \end{aligned}$$

is divisible by 4^2 because $a-3b=(a+b)-4b$ to put $(a^2+3b^2)/4$ is of the form u^2+3v^2.
where $u=(a-3b)/4$, $v=(a+b)/4$.
These equations can be solved for a and b in terms of u and v by noting that they are equivalent to

$$u+v\sqrt{(}-3)=(a+b\sqrt{-}3)(1+\sqrt{-}3)/4$$

which gives $(1-\sqrt{(}-3))(u+v\sqrt{(}-3))=a+b\sqrt{(}-3)$ as desired.
Similarly, if $a-b$ is divisible by 4 then

$$a+b\sqrt{(}-3)=(1+\sqrt{(}-3))(u+v\sqrt{(}-3))$$

for suitable u and v.
Note that u and v are relatively prime (otherwise a and b would not be relatively prime) and that $a^2+3b^2=4(u^2+3v^2)$.

Proposition 7. *If a and b are relatively prime and if a^2+3b^2 is divisible by the odd prime P then P can be written in the form $P=p^2+3q^2$ with p and q positive integers and $a+b\sqrt{(}-3)$ can be written in the form*
$a+b\sqrt{(}-3)=[p\pm q\sqrt{(}-3)][u\pm v\sqrt{(}-3)]$ where the sign is appropriately chosen and where u and v are integers.

Proof: The first statement follows by previous propositions. To prove the second statement, we follow the method used in Proposition 1.

Proposition 8. *Let a and b be relatively prime. Then* $a + b\sqrt{-3}$ *can be written in the form*

$$a + b\sqrt{-3} = \pm(p_1 \pm q_1\sqrt{-3})(p_2 \pm q_2\sqrt{-3})...(p_n \pm q_n\sqrt{-3})$$

where the p's and q's are positive integers and $p_i^2 + 3q_i^2$ *is either 4 or an odd prime.*

Proposition 9. *Let a and b be relatively prime. Then the factors in the above factorization of* $a + b\sqrt{-3}$ *are completely determined, except for the choice of signs as indicated, by the fact that*

$$(p_1^2 + 3q_1^2)(p_2^2 + 3q_2^2)...(p_n^2 + 3q_n^2) = a^2 + 3b^2$$

is a factorization of $a^2 \mid 3b^2$ *into odd primes and 4's. Moreover, if the factor* $p + q\sqrt{-3}$ *occurs then the factor* $pq\sqrt{-3}$ *does not, and conversely.*

Using the above proved statements, the lemma needed to complete Euler's proof of the case n = 3 of Fermat's Last Theorem can now be deduced very easily.

Lemma 1. *Let a and b be relatively prime numbers such that* $a^2 + 3b^2$ *is a Cube. Then there exist integers p and q such that*

$$a + b\sqrt{-3} = \left(p + q\sqrt{-3}\right)^3$$

Proof: Let $a^2 + 3b^2 = P_1, P_2, ...P_n$, be a factorization into 4's and odd primes. If this factorization contains exactly k factors of 4 then 2^{2k} is the largest power of 2 which divides $a^2 + 3b^2$ and, since

$a^2 + 3b^2$ is a cube, it follows that $2k$ and hence k are multiples of 3. Moreover, any odd prime P in the factorization must occur with a multiplicity which is a multiple of 3.
Thus n is divisible by 3 and the factors$P_1, P_2, ...P_n$, can be arranged in such a way that $P_{(3k+1)} = P_{(3k+2)} = P_{(3k+3)}$.
It follows that in the factorization of $a+b\sqrt{-3}$ given by proposition 8 the factors corresponding to each group of three P's are identical because the only choice is the choice of sign $p\pm\sqrt{-3}$ and both signs cannot occur.
Taking one factor from each group of three and multiplying them together then gives a number $c + d\sqrt{(}-3)$ such that

$$a + b\sqrt{-3} = \pm\big(c + d\sqrt{-3}\big)^3$$

Since

$$-\big(c + d\sqrt{-3}\big)^3 = \big(-c - d\sqrt{-3}\big)^3$$

the desired conclusion follows.

References

Herald Edward, (1977). *A Genetic Introduction to Algebraic Number Theory,* Springer-Verlag.

David M Burton, (2007). *Elementary Number Theory*, Sixth Edition, New Delhi.

Jody Esmonde, M.Ram Murthy, (1999). *Problems in Algebraic Number Theory*, Newyork.

Dinesh S Thakur. *Fermat's Last Theorem for Regular Primes.*