17

On the use of Remainder Theorem in proving Fermat's last Theorem

P.P.D. Nayomi Kaushalya

Abstract: In this paper, we have verified the use of the Remainder Theorem in proving Fermat's last theorem for the primeindex three. In this respect, elementary mathematics is used. First, we have assumed that a parametric equation resulting from the equation corresponding to Fermat's last theorem for the prime index three and then we have used simple mathematics to justify the use of the Remainder Theorem in proving Fermat's last theorem for this index.

Key words: Fermat,Last theorem, prime, integer, root

1. Introduction

In a recent publication,ithas been proved[2] Fermat's last theorem [1],[4] using elementary Mathematics and in the proof of the theorem, the remainder theorem has been used on one occasion but it has not verified in it.The main objective of this article is to explain the use of the remainder theorem in proving Fermat's last theorem. It is sufficient to explain the use of the remainder theorem forthe case of prime index $p = 3$ since the generalization of the use of it for any odd prime is not difficult at all.

2. Methodology and the proof

Fermat's last theorem for$p = 3$ can be stated as that the equation

(1) $z^3 = y^3 + x^3, (x, y) = 1$

has no non- trivial integer solutions for x, y, z. Assume that the equation has non-trivial integer solutions for x, y, z. It is then well known that $xyz \equiv 0(mod 3)$ since $2.3 + 1 = 7$ and assume that

$y \equiv 0(mod3)$. Then it is easy to obtain a parametric equation in the form

(2) $g^3 - 2.3^m ugh - h^3 - 3^{3m-1}u^3 = 0$

where $h, 3^m u, g, h$ are factors of y, z, x respectively. This is a cubic equation in g and it has at least one real root since the order of the cubic is odd. It can actually be shown that the cubic has only one real root [3]. $g^3 - h^3 - 2.3^m \text{ u } gh - 3^{3m-1}u^3 = 0$, $g^3 - h^3 = (g-h)[(g-h)^2 + 3gh]$

(3)Therefore $g - h = 3^{m-1}q$, where $(3,q)1$ .Hence, $g = h + 3^{m-1}p$,where $(3,p) = 1$. This root must be an integer and it follows that it must be an integer factor of the term $h^3 +$ $3^{3m-1}u^3$.Now,(2) can be written as

(4)$(h + 3^{m-1}p)[(h + 3^{m-1}p)^2 - 2.3^m uh] = h^3 + 3^{3m-1}u^3$

We have to check whether the above result is true for any integer$h$, not equal to zero.

Therefore by the Remainder theorem,

(5)$-3^{3m-3}p^3 + 3^{3m-1}u^3 = 0$

This violates the condition $(3,p) = 1$and hence (2) has no integer roots for g.Therefore the equation (1) is not satisfied by non – trivial integer triples (x,y,z) .Hence, Fermat's last theorem for $p = 3$ is true.

Now, we obtain (4) in a different way

$$h^3 + 3^{3m-1}u^3 = [(h + 3^{m-1}p) - 3^{m-1}p]^3 + 3^{3m-1}u^3$$
$$= (h + 3^{m-1}p)A + B$$

where

$$A = [(h + 3^{m-1}p)^2)3^m p - 3^{2m-1}p^2]$$
$$B = -3^{3m-3}p^3 + 3^{3m-1}u^3 = -(g-h)^3 + (z-x)$$
$$B = -(x+y) + (z-y) + (z-x) + 3gh(g-h)$$
$$= 2[z - (x+y)] + 3gh.3^{m-1}p$$
$$= -2.3^m ugh + 3gh.3^{m-1}p = -3^m h(p-2)(h + 3^{m-1}p)$$

Therefore

$h^3 + 3^{3m-1}u^3 = (h + 3^{m-1}p)[(h + 3^{m-1}p)^2)3^m p - 3^{2m-1}p^2 - 3^m h(p-2)]$

(6) Hence, by the Remainder theorem $-3^{3m-3}p^3 + 3^{3m-1}u^3 = 0$

3. Summary and conclusions

In a recent publication, Fermat's last theorem has been proved by using elementary mathematics. However, the use of the remainder theorem in the proof has not been verified. We have explained how the use of the remainder theorem can be verified using the available literature and elementary mathematics. Even though we have justified the use of the remainder theorem in case of the odd prime number three , the result we have proved is applicable for any odd prime p in exactly same as in this paper.

References

[1] Edwards, H.M. Fermat's last theorem, A Genetic Introduction to Algebraic Number, Theory, Springer -Verlag, 1977.

[2] Piyadasa R.A.D.(2011)March A Simple and short analytical proof of Fermat's last theorem,CMNSEM,Vol.2,No.3,57-63

[3] Piyadasa R.A.D.(2010)September Method of infinite descent and proof of Fermat's last theorem for n= 3,CMNSEM, Vol.1,No.6,181-186

[4] Rihenboin P. (1991) Fermat's Last Theorem for amateurs, Springer-Verlag, New York