Shadini, A.M.D.M., R.A.D.Piyadasa & B.B.U.P.Perera
Department of Mathematics, University of Kelaniya

Paper: Diversity

Uniqueness of roots of a cubic and proof of Fermat's last theorem for n=3

Fermat's last theorem, even for the smallest exponent i.e. $n=3$ has generated a lot of interest and has produced a number of proofs. The first, a proof by Leonard Euler, appeared in a book published in 1770. Euler did not establish in full a lemma required in the proof. Rebenboim [1999], Edwards (1977) claim that they have patched up Euler's proof using the ring of complex numbers of the form $a+b\sqrt{-3}$, where a and b are integers. Recently, Macys (2007) [English Transl.] claims that he may have reconstructed Euler's proof by establishing that key lemma, using elementary mathematics. However, in this authors' point of view, none of these proofs is short or easy to understand when compared to the simplicity of the wording of the theorem and the meaning of it.

Parametric solution of Fermat's equation for n=3

We first obtain the parametric solution of the equation

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

assuming that this equation has non-trivial integer solution for (x,y,z).

Lemma.1

If $a^3 \equiv b^3 (\mathrm{mod}\, 3^m)$, $(m \neq 0)$ and $(a,3)=(b,3)=1$, then $a \equiv b(\mathrm{mod}\, 3^{m-1})$ and $m \geq 2$. If we assume still further that $(a,b)=1$ and $a^3 - b^3 = 3^{3m}t^3$, where $(3,t)=1$, then

Lemma.2

If the equation (1) has a non trivial integer solution for (x,y,z), then $xyz \equiv 0(\mathrm{mod}\, 3)$.

We assume these two lemmas without proof.

Since x, y, z in (1) can be replaced by $-x$, $-y$, $-z$, without loss of generality, we can assume that $y \equiv 0(\mathrm{mod}\, 3)$.

Then (1) takes the form

$$z^3 - x^3 = 3^{3m}t^3, (3,x)=(3,t)=1 \qquad (2)$$

Lemma.3

$z - x = 3^{3m-1}h^3$, where h is a factor of t and $(3,h)=1$. This follows at once from the Lemma.1 since $(z,3)=(x,3)=(z,x)=1$.

Using these Lemmas parametric solution of (2) can be written as.

$$x = 3^m hcl + l^3 \qquad (a)$$

$$y = 3^m hcl + 3^{3m-1}h^3 \qquad (b)$$

$$z = 3^m hcl + 3^{3m-1}h^3 + l^3 \qquad (c)$$

, where $(3,h),(3,c),(h,c),(h,l)=1$.

In addition to this, we have $x + y = c^3$ and therefore from (a) and (b), we get

$$c^3 - l^3 - 2.3^m hcl - 3^{3m-1}h^3 = 0 \qquad (d)$$

Proof of Fermat's last theorem for n=3 : In the equation[d], h,l,c, 3are co-prime numbers, and let us fix the parameters h,m of y and find c, a factor of z in (1), for given l which is a factor of x. It is clear from Lemma.1 and (d) that $c - l = 3^{m-1}e$, or $c = l + 3^{m-1}e$, where $(e,3)=1$ and $m \geq 2$, unless $hcl = 0$. The equation (d) is of the form,

$$x^3 - 3uvx - u^3 - v^3 = 0 \qquad (3)$$

, where $l^3 + 3^{3m-1}h^3 = u^3 + v^3$, $2.3^{m-1}hl = uv$ and its roots are given [1]] by

$$u+v,\ u\omega + v\omega^2,\ u\omega^2 + v\omega. \qquad (4)$$

where ω is the cube root of unity and u^3, v^3 are the roots of the equation

$$x^2 + Gx - H^3 = 0 \qquad (5)$$

where $H = -2.3^{m-1}hl$ and $G = -3^{3\beta-1}h^3 - l^3$.

$\Delta = G^2 + 4H^3 = 3^{6m-2}h^6 - 14.3^{3m-3}h^3l^3 + l^6 = (3^{3m-1}h^3 - l^3)^2 + 4.3^{3m-3}h^3l^3 > 0$. Therefore the representation of the roots is unique. Since $x = u + v = 3^{m-1}e + l$ is the real root, l^3 is a root of (5) and hence

$$x^2 - (3^{3m-1}h^3 + l^3)x + 8.3^{3m-3}h^3l^3 = 0 \qquad (6)$$

This is possible only if $l^3 = 0$ or $-3^{3m-3}h^3 = 0$, giving $x = 0$, or $y = 0$. Hence $xyz \neq 0$ is not satisfied and (1) has no non-trivial integer solutions for (x, y, z).

References

[1]Archbold J.W. (1961).Algebra (Sir Issac Pitman & Sons LTD., London.

[2]Edwards H.M. (1977) Fermat's last theorem; A Genetic Introduction to Algebraic Number Theory. (Springer -Verlag).

[3]Macys J.J. (2007) On Euler's Hypothetical Proof .Math. Notes; Vol.82, No.3. p.352.

[4] Ribenboim P. (1999).Fermat's last theorem for amateurs. (Springer-Verlag, New York).