Method of Infinite Descent and proof of Fermat's last theorem for $\mathbf{n=3}$

R.A.D.Piyadasa

Department of Mathematics, University of Kelaniya

Abstract

The first proof of Fermat's last theorem for the exponent $n=3$ was given by Leonard Euler using the famous mathematical tool of Fermat called the method of infinite decent. However, Euler did not establish in full the key lemma required in the proof. Since then, several authors have published proofs for the cubic exponent but Euler's proof may have been supposed to be the simplest. Paulo Ribenboim [1] claims that he has patched up Euler's proof and Edwards [2] also has given a proof of the critical and key lemma of Euler's proof using the ring of complex numbers. Recently, Macys in his recent article [3, Eng.Transl.] claims that he may have reconstructed Euler's proof for the key lemma. However, none of these proofs is short nor easy to understand compared to the simplicity of the theorem and the method of infinite decent The main objective of this paper is to provide a simple, short and independent proof for the theorem using the method of infinite decent. It is assumed that the equation $z^3 = y^3 + x^3$, $(x,y)=1$ has non trivial integer solutions for (x,y,z) and their parametric representation [5] is obtained with one necessary condition that must be satisfied by the parameters. Using this necessary condition, an analytical proof of the theorem is given using the method contradiction. The proof is based on the method of finding roots of a cubic formulated by Tartagalia and Cardan [4], which is very much older than Fermat's last theorem.

Parametric solution of the equation

Let us assume that the equation

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

has a non trivial integer solution for (x,y,z). Now, the parametric representation of (x,y,z) is obtained using the following three simple lemmas.

Lemma.1

If $a^3 - b^3 \equiv 0(\text{mod } 3^m)$, $(m \neq 0)$ and $(a,3)=(b,3)=1$, then $a \equiv b(\text{mod } 3^{m-1})$ and $m \geq 2$.

If we assume $a^3 - b^3 = 3^{3m}t^3$ and $(a,b)=1$ in addition to $(a,3)=(b,3)=1$, then $a-b = 3^{3m-1}u^3$, where u is a factor of t.

We assume this lemma without proof which is straightforward.

Lemma.2

If the equation

$$z^3 = y^3 + x^3, \ (x, y) = 1 \tag{2}$$

has a non trivial integer solution for (x, y, z), then $xyz \equiv 0(\text{mod}3)$.We assume this lemma as well without proof. If we assume $y \equiv 0(\text{mod}3)$,

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

Lemma.3

$z - x = 3^{3m-1} u^3$, where u is a factor of t and $(3, u) = 1$.

This follows at once from Lemma.1 and the equation (3) can, now, be written as

$$z^3 = 3^{3m} u^3 e^3 + x^3 \tag{4}$$

where $(3, u) = (3, e) = (u, e) = 1$.

Let us now assume the parametric solution of Fermat equation and a necessary condition that must be satisfied by the parameters as in [5]. That is

$$x = 3^m ugh + h^3 \tag{5}$$

$$y = 3^m ugh + 3^{3m-1} u^3 \tag{6}$$

$$z = 3^m ugh + 3^{3m-1} u^3 + h^3 \tag{7}$$

In addition to this, we have $x + y = g^3$ and therefore from (5) and (6), we get

$$g^3 - h^3 - 2.3^m ugh – 3^{3m-1} u^3 = 0 \tag{8}$$

Proof if the theorem

Let us first assume that all $x, y, z > 0$ and $y \equiv 0(\text{mod}3)$. Then we can use the necessary condition

$$g^3 - h^3 - 2.3^m ugh – 3^{3m-1} u^3 = 0 \tag{9}$$

satisfied by the parameters to prove the theorem.

In this equation, u, g, h ,3 are co-prime numbers , and let us fix the parameters u, m of y and find g, a factor of z in (1), for different h which is a factor of x. It is clear from Lemma.1 and (9) that $g - h = 3^{m-1} j$, or $g = 3^{m-1} j + h$, where $(j, 3) = 1$ and $m \geq 2$ unless $uh = 0$ since $g^3 \equiv h^3 (\text{mod } 3^m)$.

The equation (9) is of the form

$$g^3 - 3vwg - v^3 - w^3 = 0 \tag{10}$$

where $3^{3m-1}u^3 + h^3 = v^3 + w^3$, $2.3^{m-1}uh = vw$, and using the method of Tartagalia and Cardan [4], its roots can be written as

$$v + w, v\omega + w\omega^2, \; v\omega^2 + w\omega. \tag{11}$$

ω being the cube root of unity. v^3, w^3 are the roots of the equation

$$t^2 + Gt - H^3 = 0 \tag{12}$$

where $H = -2.3^{m-1}uh$ and $G = -3^{3m-1}u^3 - h^3$ [4]. Discriminant of (12) is 27Δ, where Δ given by $\Delta = -[G^2 + 4H^3] = -[3^{6m-2}u^6 - 14.3^{3m-3}u^3h^3 + h^6] = -[(3^{3m-1}u^3 - h^3)^2 + 4.3^{3m-3}u^3h^3]$. It is clear that Δ is negative when $uh > 0$. Therefore v, w are real and distinct and (9) has only one real root [4], namely, $g = v + w$. Assume that v, w are integers. Since $(u,3) = (g,3) = 1$ and $vw = 2uh3^{m-1}$, we can write

$$g = 3^{m-1}v_1 + w_1 = 3^{m-1}j + h \tag{13}$$

where $(3, w_1) = (3, v_1) = 1$, $v_1w_1 = 2uh$. If g is even, then both h, u are odd which follows from the fact that z of the Fermat equation is even and u, h are the factors of odd y and x respectively. Since $v_1w_1 = 2uh$ and u, h are odd, v_1, w_1 should be opposite parity since either v_1 and w_1 mist carry the only even factor 2. Therefore g cannot be even. Now, assume that one of u, h even. In general, the both u, h may be composite. Assume that u is even, and let $g = 3^{m-1}2u_1h_1 + u_2h_2 = 3^{m-1}j + h$, where u_1, u_2 are co-prime factors such that $u_1u_2 = u$ and u_1 is even. Also, $h_1h_2 = h$ and $(h_1, h_2) = 1$. Then, we must have

$$3^{3m-1}u^3 + h^3 = 8..3^{3m-3}u_1^3h_1^3 + u_2^3h_2^3 = 3^{3m-3}v_1^3 + w_1^3 \tag{14}$$

Since $3^{3m-1}u^3 = 8.3^{3m-3}u^3 + 3^{3m-3}u^3 = 8.3^{3m-3}u_2^3u_1^3 + 3^{3m-3}u_1^3u_2^3$, it follows from (14) that

$$3^{3m-1}u^3 + h^3 = 8.3^{3m-3}u_1^3u_2^3 + 3^{3m-3}u_1^3u_2^3 + h_1^3h_2^3 = 8.3^{3m-3}u_1^3h_1^3 + u_2^3h_2^3 \tag{15}$$

$$(h_1^3 - u_2^3)(3^{3m-3}.8.u_1^3 - h_2^3) = 3^{3m-3}u_2^3u_1^3 \tag{16}$$

It follows, at once, from (16) that $(h_1^3 - u_2^3) = 3^{3m-3}u_1^3$ and $3^{3m-3}.8.u_1^3 - h_2^3 = u_2^3$. In other words, we must have

$$h_1^3 = 3^{3m-3}u_1^3 + u_2^3 \tag{17a}$$

$$3^{3m-3}.2^3.u_1^3 = u_2^3 + h_2^3 \tag{17b}$$

If we assume, $g = 3^{m-1}u_3h_3 + 2u_4h_4$, where u_4 is even, $u = u_3u_4, h = h_3h_4, (u_3, u_4) = (h_3, h_4)$, in exactly the same manner, we are lead to the equations

$$(8u_4^3 - h_3^3)(h_4^3 - 3^{3m-3}u_3^3) = 3^{3m-3}u_4^3u_3^3 \tag{18}$$

$$h_4^3 = 3^{3m-3}u_3^3 + u_4^3 \tag{19a}$$

$$2^3u_4^3 = 3^{3m-3}u_3^3 + h_3^3 \tag{19b}$$

Let $z = 3^m ugh + 3^{3m-1}u^3 + h^3$ is the least of all integral z satisfying (1), then we have $h_1, h_4, 3^{m-1}2, u_1, 2u_4 < z$ for all z values of Fermat equations (17a),(17b),(19a),(19b) of $n = 3$ leading to a contradiction. Then it follows from the method of infinite decent that (1) has no solutions integers. Proof of the theorem for even h and odd u follows exactly the same way as before. If $z \equiv 0(\text{mod} 3)$ the proof can be done in exactly the sane way as above

References

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

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

(3) J.J.Macys, On Euler's Hypothetical Proof, Math. Notes , Vol.82, No.3, (2007) p.352-356.

(4) J.W.Archbold, Algebra, Sir Issac Pitman & Sons LTD., London, 1961, p.174-176.

(5) R.A.D.Piyadasa, Simple analytical proofs of Fermat's last theorem for $n = 3$, CMNSEM, Vol.1 No.3, April 2010, p.64-70.