4.27 Structure of Fermat triples

R.A.D.Piyadasa
Department of Mathematics , University of Kelaniya
(Dedicated to late Prof. S.B.P.Wichramasuriya)

ABSTRACT

The structure of Fermat's triples can be immensely useful in finding a simple proof of Fermata's Last Theorem. In this contribution, the structure of Fermat's triples is determined using Fermat's little theorem producing a new lower bound for the triples.
Fermat's last theorem can be stated as the equation

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

has no non-trivial integral solutions for x, y, z any prime $n > 2$ .Due to the famous work of Germain Sophie , if we assume the existence of non trivial integral triples (x, y, z) for any prime $n > 2$ satisfying (1),there may be two kinds of solutions , namely, one of (x, y, z) is divisible by n and none of (x, y, z) is divisible by n ,and the well known lower bound for positive x, y, z is n, that is, if x is the least, then $x > n$ [1].

Let us first consider the triples satisfying $xyz \neq 0(\bmod n)$. Then $(z - x) = y_\alpha^n$, $z - y = x_\alpha^n$, $x + y = z_\alpha^n$, where $x_\alpha, y_\alpha, z_\alpha$ are the factors of x, y, z respectively.

$$z_\alpha^n - y_\alpha^n - x_\alpha^n = x + y - (z - x) - (z - y) = 2(x + y - z) \tag{2}$$

$$x + y - z = z_\alpha^n - z_\alpha \xi = z_\alpha (z_\alpha^{n-1} - \xi) = z_\alpha (z_\alpha^{n-1} - 1 + 1 - \xi) \tag{3}$$

,where $z = z_\alpha \xi$ .Since $x + y - z \equiv 0(\bmod n)$,which follows from (1) and Fermat's little theorem, and also $z_\alpha^{n-1} - 1 = 0(\bmod n)$ .Hence $1 - \xi \equiv 0(\bmod n)$and $\xi = (nk + 1)$, where k is an integer which is non negative since $\xi \neq 0$.Therefore , we conclude in a similar manner that

$z = z_\alpha (nk + 1)$
$y = y_\alpha (nl + 1)$
$x = x_\alpha (nm + 1)$

where k, l, m are positive integers and $x_\alpha \geq 1$, in particular. Also, $x + y - z = x - x_\alpha^n \equiv 0(\bmod n)$, from which it follows at once that $x. \geq n + x_\alpha^n > n$, which first obtained in a different manner by Grunert in 1891[1].In this contribution , it is shown that x very well greater than n^2.
Proof.

$$2(x + y - z) = z_\alpha^n - y_\alpha^n - x_\alpha^n = (z - z_\alpha nk)^2 - (y - y_\alpha nl)^n - (x - x_\alpha nm)^2 = n^2 L \tag{4}$$

due to $z^n = y^n + x^n$ and hence $2(x + y - z) = n^2 L$.
where L is an integer, Hence, $x + y - z \equiv 0(\bmod n^2)$. It is easy to check that

$$x + y - z \equiv 0(\bmod z_\alpha y_\alpha x_\alpha n^2) \tag{5}$$

But $x+y-z=x-x_\alpha^n$ and all numbers $z_\alpha, y_\alpha, x_\alpha, n$ co-prime to one another, and hence

$$x > n^2 z_\alpha y_\alpha x_\alpha + x_\alpha^n \tag{6}$$

and note also that $z_\alpha, y_\alpha > 1$ which guarantees that x is very well greater than n^2. We deduce that

$$z^n - z \equiv 0(\bmod n^2) \tag{a}$$

$$y^n - y \equiv 0(\bmod n^2) \tag{b}$$

$$x^n - x \equiv 0(\bmod n^2) \tag{c}$$

since $x+y-z=(z-nkz_\alpha)-z=z^n-z+n^2H$, where H is an integer, from which (a) follows, and (b) and (c) follows in a similar manner. Now it is easy to deduce that

$$(x+y)^n - z^n \equiv 0(\bmod n^3) \tag{7}$$

In case of (7), one has to use the simple result that if $ab \neq 0(\bmod n)$ and $a - b \equiv 0(\bmod n^\mu)$,then $a^n - b^n \equiv 0(\bmod n^{\mu+1})$, where $n \geq 3$ is a prime.

Now assume that $xyz \equiv 0(\bmod n)$, and suppose that $y \equiv 0(\bmod n)$, for example.

Then, since y is of the $n^{n\beta}\alpha^n\gamma^n$, it follows from the above result that $z-x=n^{n\beta-1}\alpha^n$, where α may takes positive values including $\alpha=1$. Now the equation (4)takes the form

$$z_\alpha^n - n^{n\beta-1}\alpha^n - x_\alpha^n = 2(x+y-z) \tag{8}$$

Now, since $x+y-z \equiv 0(\bmod n^2)$, it follows that $z_\alpha^n - x_\alpha^n \equiv 0(\bmod n^2)$, and it is easy to deduce

$$x+y-z \equiv 0(\bmod z_\alpha.n^{n\beta}\alpha.x_\alpha) \tag{9}$$

Hence $x-\delta^n \equiv 0(\bmod z_\alpha.n^{n\beta}\alpha.x_\alpha)$ and from which we deduce that $x > z_\alpha.n^{n\beta}\alpha.x_\alpha$, where $\beta \geq 2$. The equations (a), (b),(c) can be obtained exactly in the same manner as before. It is easy to understand that above equations hold even if one assumes $z \equiv 0(\bmod n)$.

References

(1)Rebenboim, Paulo,13 Lectures on Fermat's last theorem, Springer-Verlag, New York, 1979,pp226.