FERMAT'S LAST THEOREM

Ramanand Raman

Guest Faculty (Math)
Dept. of Math., T.N.B. College, Bhagalpur, T.M. Bhagalpur University, Bhagalpur, Bihar.

ABSTRACT : In 1637, Format stated the Diophantine equation $x^n + y^n = z^n$ has no non-trivial solution, If n is an integer greater than 2 there do not exist integers x, y, z all different from zero. In this paper we study the Fermat's last theorem, the most famous of all Diophantine problems.

Keywords : Fermat's last theorem, Diophantine problems, harmonic progression, geometric progression, non-zero positive integers.

Introduction

In this paper we study the Fermat's last theorem, the most famous of all Diophantine problems. In 1637, Format stated the following theorem without giving any proof of it.

If n is an integer greater than 2 there do not exist integers x, y, z all different from zero such that

$$x^n + y^n = z^n \quad (1)$$

This theorem was stated by Fermat on the margin of his copy of Diophantus. He added that he had discovered a truely remarkable proof of the theorem, but that the margin of the book was too narrow to contain it.

No general proof of this theorem has yet been found. For various special values of n proofs have been given.

In the study of equation (1) it is convenient to make the following observations.

If there exists a solution of (1) there exists also a solution in which x, y, z are relatively prime pairwise. This can be seen as follows.

If any two of the numbers x, y, z have the greatest common factor, $d > 1$ then from (1) it follows that the third number of the set has also the same factor. Hence the equation may be divided through by d^n.

In the resulting equation the numbers x, y, z are relatively prime pairwise. Hence in dealing with the impossibility of (1) it is sufficient to treat only the case in which x, y, z are relatively prime pairwise.

Again, since n is greater than 2,it must contain the factor 4 or an odd prime factor p. If n contains the factor 4, we may write $n = 4m$, whence we have

$$(x^m)^4 + (y^m)^4 = (z^m)^4 \quad (2)$$

But we know that$x^4 + y^4 = z^4$ is impossible, hence it follows that the equation (2) is impossible. Hence if equation (1) is true then n does not contain the factor 4.

Now, if n contains the odd prime factor p, we may write $n = pm$ for which we have

$$(x^m)^p + (y^m)^p = (z^m)^p$$

Therefore in order to prove the impossibility of the equation (1) it is sufficient to prove the impossibility of the equation

$$x^p + y^p = z^p \quad (3)$$

where p is an odd prime.

Many great Mathematicians have worked on this problem, but they only found particular solutions of this problem. A brief account of the results known so far are stated here.

(a) Legendre [1] has shown that the equation $x^p + y^p = z^p$ can not be satisfied by integers x, y, z each of which is prime to p if $p < 192$.
(b) Mailet [2] has shown that same is true if $p < 223$.
(c) L. E. Dickson [3] has proved that the equation is without a solution in integers prime to p if $p < 6857$.
(d) Kummer [4] in 1850 made the greatest contribution to the subject. He introduced the Algebric number arising from the p^{th} root of unity and this was beginning of algebric number theory which was later generalized by Dedekind and Kronecker.
(e) The work of H. Vandiver [5] and D. H. Lehmer [6] has settled the insolvebility for $p < 2000$.
(f) J. L. Selfridge, C. A. Nicol and H. S. Vandiver [7] have settled in 1955 the impossibility for $p < 4002$.
(g) In 1967 J. L. Selfridge [8] again attempted this problem. The calculation has been carried out on the high speed computer SWAC. Now it is known to hold for $p < 25000$.

The Academy of Sciences of Gottingen announces a sum of 1,00,000 German marks which is to be awarded as a prize to the person who first presents a rigirous proof of this theorem. No complete proof of this theorem submitted so far has been declared valid for the prize.

In this book 'A Chapter in the Theory of Number' L. J. Mordell who devoted his life in solving Diophantine equations declared that "There are easier methods of earning money than by proving Fermat's last theorem."

1. Devid E. Stone [9] has proved a theorem which pertains to Fermat's last theorem. The theorem is

Theorem 1. If p and $2p + 1$ are odd primes and $x^p + y^p + z^p = 0$, where x, y, z are non-zero pairwise prime integers then precisely one of the integers x, y, z is divisible by p.

In the present section we shall prove theorems which some pertain to Fermat's last theorem.

Theorem 2. If x, y, z are positive integers and

$$x^n + y^n = z^n;\ n > 2 \quad (4)$$

then x, y, z can not be in arithmatic progression.

Proof. Let x, y, z be in arithmatic progression, then we may take them without loss of generality as $X - K, X, X + K$, where K is positive integer and $(X, K) = 1$

Then we have

$$(X-K)^n + X^n = (X+K)^n \tag{5}$$

Now expanding (5) by the Binomial theorem we get

$$X^n = 2K\left[\binom{n}{1}X^{n-1} + \binom{n}{3}X^{n-3}K^2 + \ldots\right] + K^n - (-1)^n K^n. \tag{6}$$

$\equiv 0 \pmod 2$, whether n is odd or even.

Hence $x^n = 2Km$ for some positive integers m.

For integral solution X should be divided by K, but $(X, K) = 1$ therefore $K = 1$.

The equation (6) becomes

$$X^n = 2\left[\binom{n}{1}X^{n-1} + \binom{n}{3}X^{n-3} + \ldots\right] + 1 - (-1)^n. \tag{7}$$

If n were odd, then $2|X^n$, hence X is even and so 2^{n-1} will divide the odd number,

$$\binom{n}{1}X^{n-1} + \binom{n}{3}X^{n-3} + \ldots + \binom{n}{n-2}X^2 + 1,$$

which is impossible.

Now let n be even and greater than 4, then (7) will be written as

$$X^{n-1} = 2\left[\binom{n}{1}X^{n-2} + \binom{n}{3}X^{n-4} + \ldots + \binom{n}{n-2}\right], \tag{8}$$

Since $\frac{X}{2}$ is even, we have

$$\left(\frac{X}{2}\right)^{n-1} = 2\left[\binom{n}{1}\left(\frac{X}{2}\right)^{n-2} 2^{n-2} + \ldots + \binom{n}{n-2}\left(\frac{X}{2}\right)^2 2^2 + \binom{n}{n-1}\right], \tag{9}$$

Hence $\frac{X}{2}$ divides $\binom{n}{n-1}$ i.e. n. But from (9)

$$\left(\frac{X}{2}\right)^{n-1} 2^{n-2} > \binom{n}{1}\left(\frac{X}{2}\right)^{n-2} 2^{n-2}$$

i.e. $\frac{X}{2} > n$. But $\frac{X}{2}$ divides n, so that $\frac{X}{2} \le n$.

Thus $\frac{X}{2} > n \ge \frac{X}{2}$

This is a contradiction. Hence the theorem follows.

Theorem 3. If $x^n + y^n = z^n$ where x, y, z are non-zero positive integers and n greater than 2 then x, y, z can not be in geometric progression.

Proof. Let us suppose that x, y, z are non-zero positive integers and they are in geometric progression.

Let $x = a, y = ar, z = ar^2$

where a and r are positive integers other than zero.

Therefore $a^n + (ar)^n = (ar^2)^n$

or $1 + r^n = r^{2n}$, for $a^n > 0$

Hence $r^{2n} - r^n - 1 = 0$

The discriminate of the quadratic equation in r^n is 5 which is not a perfect square. Hence r^n and so r can not be a rational number. This proves the theorem.

Theorem 4. If $x^n + y^n = z^n$ where x, y, z are non-zero positive rationals and n greater than 2 then x, y, z can not be in harmonic progression.

Proof. Let x, y, z be in harmonic progression. Then we may take them as

$$\frac{1}{X-K}, \frac{1}{X}, \frac{1}{X+K},$$

where X, K are positive integers and X greater than K. Now we are to show that

$$\left(\frac{1}{X-K}\right)^n + \left(\frac{1}{X}\right)^n + \left(\frac{1}{X+K}\right)^n \tag{10}$$

is impossible.

Now (10) may be written as

$$X^{2n}\left[\left(1+\frac{K}{X}\right)^n - \left(1-\frac{K}{X}\right)^n + \left(1-\frac{K^2}{X^2}\right)^n\right] = 0$$

As $X > 0$ and $n > 2$ we have

$$\left(1+\frac{K}{X}\right)^n - \left(1-\frac{K}{X}\right)^n + \left(1-\frac{K^2}{X^2}\right)^n = 0 \tag{11}$$

Since $\frac{K}{X} < 1$, hence using the Binomial theorem in (11), we get

$$1+\binom{n}{1}\left(\frac{K}{X}\right)+\binom{n}{2}\left(\frac{K}{X}\right)^2+\ldots+\binom{n}{r}\left(\frac{K}{X}\right)^r+\ldots-\left[1-\binom{n}{1}\left(\frac{K}{X}\right)+\binom{n}{2}\left(\frac{K}{X}\right)^2+\ldots+(-1)^r\binom{n}{r}\left(\frac{K}{X}\right)^r+\ldots\right]$$

$$+\left[1-\binom{n}{1}\left(\frac{K^2}{X^2}\right)+\binom{n}{2}\left(\frac{K^2}{X^2}\right)^2+\ldots+(-1)^r\binom{n}{r}\left(\frac{K^2}{X^2}\right)^r+\ldots\right]=0$$

Considering r^{th} term of three expansions we have

$$\binom{n}{r}\left[\left(\frac{K}{X}\right)^r-(-1)^r\left(\frac{K}{X}\right)^r+(-1)^r\left(\frac{K^2}{X^2}\right)^r\right]$$

when r is odd we get

$$\binom{n}{r}\left[\left(\frac{K}{X}\right)^r+\left(\frac{K}{X}\right)^r+\left(1-\frac{K^r}{X^r}\right)\right]$$

Since $\frac{K}{X}<1$,

hence $1-\frac{K^r}{X^r}>0$ for all values of $r \le n$.

When r is even we get

$$\binom{n}{r}\left[\left(\frac{K}{X}\right)^r-\left(\frac{K}{X}\right)^r+\left(\frac{K^r}{X^r}\right)\right]=\binom{n}{r}\left(\frac{K^2}{X^2}\right)^r>0\,.$$

Hence R.H.S. of (11) is always positive for all values of $r \le n$, $n > 2$, which is a contradiction. Hence the theorem follows.

Theorem 5. If x, y, z are positive integers such that $z \ge \min(x^2, y^2)$ then for any integer $n \ge 3$ the equation $x^n + y^n = z^n$ is impossible.

Proof. Here we have

$$x^n + y^n = z^n$$

or $$x^n = z^n - y^n = (z - y)(z^{n-1} + z^{n-2}y + \ldots + y^{n-1})$$

We know that the arithmatic mean of n positive numbers is greater than their geometric mean. Applying this result we get

$$\frac{z^{n-1}+z^{n-2}y+\ldots+y^{n-1}}{n}>(zy)^{\frac{n-1}{2}}$$

$$z^{n-1}+z^{n-2}y+\ldots+y^{n-1}>n(zy)^{\frac{n-1}{2}}>(zy)^{\frac{n-1}{2}},\quad n\ge 3$$

Again $(z - y) \ge 1$, we have

$$x^n>(zy)^{\frac{n-1}{2}}$$

or $$x>(zy)^{\frac{1}{2}-\frac{1}{2n}}$$

or $$x>(zy)^{\frac{1}{3}}$$

On account of symmetry in x, y we have

$$y>(zx)^{\frac{1}{3}}$$

Now $x^9 > z^3y^3 > z^3zx = z^4x$

or $z^4 < x^8$

or $z < x^2$,

similarly $z < y^2$

Hence $z < \min(x^2, y^2)$ which contradicts the assumption. Hence the theorem follows.

Theorem 6. If $x^n + y^n = z^n$, where x, y, z are non-zero pairwise prime integers and for any integer $n > 2$, $3n + 1$ is a prime, then one of the integers x, y, z is divisible by $3n + 1$.

Proof. Suppose that none of the integers x, y, z is divisible by $3n + 1$, then xyz is not divisible by $3n + 1$ and so $(xyz, 3n + 1) = 1$, then $(3n + 1, x) = 1$, $(3n + 1, y) = 1$, $(3n + 1, z) = 1$, since x, y, z are relatively prime pairwise.

By Fermat's theorem

$$x^{3n} \equiv y^{3n} \equiv z^{3n} \equiv 1 \pmod{3n+1} \qquad (12)$$

Again since $x^n + y^n = z^n$

We have $$x^{3n} + y^{3n} + 3x^ny^nz^n = z^{3n} \qquad (13)$$

From (12) and (13) we have

$$3x^ny^nz^n \equiv -1 \pmod{3n+1}$$

Hence we have $27x^{3n}y^{3n}z^{3n} \equiv -1 \pmod{3n+1}$

Now using (12) we get

$$27 \equiv -1 \pmod{3n+1}$$

i.e. $$28 \equiv 0 \pmod{3n+1}$$

which is impossible since only prime divisor of 28 is 7 corresponding to $n = 2$, but $n > 2$ by assumption hence the theorem follows.

Theorem 7. If $x^p + y^p = z^p$ has positive integral solutions for any prime $p > 2$, then $z > \min(x, y) > p$.

Proof. We may suppose that x, y, z are relatively prime pairwise.

Since $x^p + y^p = z^p$, therefore it is obvious that

$$z > \min(x, y).$$

Let us suppose $p >$ rain (x, y). On account of symmetry we may suppose that $x > y$ and $p > y$. The following two cases arise.

(i) $p > x > y$

(ii) $x > p > y$

In case (i) since $y^p = z^p - x^p$, we have

$$y^p \geq (x + 1)^p - x^p > px^{p-1}$$

Hence $$y > p\left(\frac{x}{y}\right)^{p-1} > p$$

So that $y > P$ and this contradicts (i). Similarly in case (ii) we have a contradiction. This proves the theorem.

Theorem 8. If x, y, z are positive integers and $x^n + y^n = z^n$, then each of x, y, z is greater than n, where n is a positive integer.

Proof. We may suppose that $z > x > 0$. We now only show that $x > n$.

Here we have

$$x^n = z^n - y^n = (x - y)(z^{n-1} + z^{n-2y} + \ldots + y^{n-1})$$

Since $z > y$, therefore $z - y = k > 0$

$$x^n > kny^{n-1}$$

$$x > kn\left(\frac{y}{x}\right)^{n-1} > kn \text{ as } y > x.$$

Thus $x > n$. The theorem follows.

Theorem 9. If $x^n + y^n = z^n$ has a positive integral solutions for any odd number $n > 2$ and x, y, z are positive integers then Mobius function $\mu(x + y) = 0$.

Proof. Since n is odd, therefore $(x + y) \mid (x^n + y^n)$, i.e. $(x + y) \mid z^n$. If the prime factor of $(x + y)$ be q then $q \mid z^n$.

Therefore $q \mid z$.

Thus every factor of $(x + y)$ divides z. Now let us suppose

$$\mu(x + y) \neq 0, \text{ then } (x + y) \mid z.$$

Therefore $(x + y) < z$ or $(x + y)^n < z^n$

or $$\binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-1}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} < 0.$$

This is impossible as x, y are positive integers and $n > 2$. This is a contradiction, hence $\mu(x + y) = 0$.

Theorem 10. If x, y, z are positive integers such that

$$x^n + y^n = z^n \text{ where } n > 4 \text{ then}$$

$$\sqrt{2}\min(x, y) > (\sqrt{x}, \sqrt{y})(1 + (2n\log 2n)^{-1}).$$

To prove this theorem we need the following lemma.

Lemma 1. For any integer $n > 4$

$$2^{\frac{1}{2}} > 1 + (n\log n)^{-1} \tag{14}$$

$$n > \frac{1}{e\log 2}.$$

Proof. If $n > 4$ then

From which we get $\log n > (\log 2)^{-1}$ which implies

$$(n \log n)^{-1} < n^{-1} \log 2.$$

But $$\log\{1 + (n \log n)^{-1}\} < (n \log n)^{-1}$$

or $$\log\{1 + (n \log n)^{-1}\} < (n^{-1}\log 2 = \log 2^{\frac{1}{n}}.$$

Therefore $2^{\frac{1}{n}} > 1 + (n \log n)^{-1}$.

Proof of the theorem. It is well known that

$$x^n + y^n > 2\left(\frac{x+y}{2}\right)^n$$

Since $x^n + y^n = z^n$, it follows that

$$Z^n > 2^{1-n}(x + y)^n$$

$$z > 2^{\frac{1}{n}-1}(x + y).$$

We have already proved in Theorem 5 that

$$z \geq \min(x^2, y^2)$$

Therefore $x^2 > 2^{\frac{1}{n}-1}(x + y) = m(x + y)$

where $m = 2^{\frac{1}{n}-1}$ and $y^2 > m(x + y)$; this implies

$$x > \frac{m + \sqrt{m^2 + 4my}}{2}.$$

Hence we find $x > my$, so that $\frac{\sqrt{2}x}{\sqrt{2}} > 2^{\frac{1}{2n}}$.

Therefore $\frac{\sqrt{2}x}{\sqrt{2}} > 1+(2n\log 2n)^{-1}$. Similarly

$$\frac{\sqrt{2}x}{\sqrt{2}} > 1+(2n\log 2n)^{-1}.$$

Hence we get $\sqrt{2}\min(x,y) > \max(\sqrt{x},\sqrt{y})[1+(2n\log 2n)^{-1}$.

This proves the theorem.

Theorem 11. If $x^n + y^n = z^n$ has positive integral solutions for infinitely many primes p, then there exist sequences $\{x_n\}$, $\{y_n\}$, $\{z_n\}$ of positive integers and a sequence $\{p_n\}$ of prime such that

(i) $x_n^{p_n} + y_n^{p_n} = z_n^{p_n}$ and

(ii) z_n □ $\max(x_n, y_n)$ or more precisely

$z_n = \max(x_n, y_n)(1+0(n\log n)^{-1})$.

Proof. Let us suppose that $x^p + y^p = z^p$ has positive integral solutions for infinitely many primes p, then there is a sequence of primes $\{p_n\}$ such that for each p_n there exists integers x_n, y_n, z_n such that

$$x_n^{p_n} + y_n^{p_n} = \frac{z_n}{x_n} \qquad (15)$$

Let x_n, y_n, z_n be the least of the sets of positive integers $\{x_n\}$, $\{y_n\}$, $\{z_n\}$ satisfying (15) for a given p_n. Now suppose that $x_n > y_n$ then from (i) we have

$$x_n^{p_n} < 2x_n^{p_n} or \frac{z_n}{x_n} < 2^{\frac{1}{p_n}}$$

Now it is easy to see that

$$2^{\frac{1}{m}} < 1+\frac{1}{m}, \text{ for any integer } m > 1.$$

Hence we get $1 < \frac{x_n}{z_n} < 1+\frac{1}{p_n}$.

If Q_n is the n^{th} prime, then plainly $p_n > Q_n$.

But it is known that $Q_n = 0$ ($n \log n$).

Hence it follows that

$$\frac{z_n}{x_n} = 1+0(n\log n)^{-1}$$

Similarly we can prove

$$\frac{z_n}{y_n} = 1+0(n\log n)^{-1}, \quad \text{if } x_n < y_n.$$

Hence we get $z_n = \max(x_n, y_n)[1+0(n\log n)^{-1}]$.

Theorem 12. If p and $4p + 1$ are primes with $P > 3$ and $x^p + y^p + z^p = 0$, where x, y, z are non-zero pairwise prime integers than precisely of the integers x, y, z is divisible by $4p + 1$.

Proof. To prove the theorem let us assume that none of the x, y, z is divisible by $4p + 1$ so that $(xyz, 4p + 1) = 1$. Writing the equation as $x^p + y^p = - z^p$ and squaring get,

$$x^{2p} + y^{2p} + 2x^p y^p = z^{2p} \qquad (16)$$

Since $4p + 1$ is a prime and by assumption x, y, z are each prime to $4p + 1$, we have by Fermat's theorem

$$x^{4p} \equiv 1 (\text{mod } 4p + 1)$$

or $x^{4p}-1 \equiv 0 \text{ (mod } 4p + 1)$

or $(x^{2p} + 1)(x^{2p} - 1) \equiv 0 \text{ (mod } 4p + 1)$,

Only one of the factor of the left is divisible by $4p + 1$, for if both of them were divisible by $4p + 1$, so is there difference i.e. 2 which is impossible.

Now

$$x^{2p} \equiv 1(\text{mod } 4p+1) \text{ if } x = \infty$$
$$x^{2p} \equiv -1(\text{mod } 4p+1) \text{ if } x \neq \infty \qquad (17)$$

Simillarly when x is placed by y and z. Hence by using these relations in (16) we get

$$\pm 1 \pm 1\ 2x^p y^p = \pm 1 \text{ (mod } 4p + 1)$$

or $2x^p y^p = \pm 1, -1 + 3, \text{ or } -3 \text{ (mod } 4p + 1)$

Squaring the last congruence and (17) for x, y, we get

$$\pm 4 = 1 \text{ or } 9 \text{ (mod } 4p + 1)$$

Since p is prime > 3, the last congruent is impossible. This contradicts the assumption that $(xyz, 4p + 1) = 1$ and hence one of the integers x, y, z must be divisible by $4p + 1$.

Theorem 13. If p and $2p + 1$ are odd primes and x, y, z are non-zero pairwise prime integers such that $x^p + y^p + z^p = 0$, then exactly one of the integers x, y, z is divisible by p^2.

In order to prove the theorem we need the following lemma.

Lemma 2. If a and b are integers such that $a + b = 0 \text{ (mod } p)$ and

$$F(a,b) = \sum_{r=1}^{p} (-1)^{r-1} a^{p-r} b^{r-1}$$

Then $F(a, b) = pa^{p-1} \pmod{p^2}$

Proof. We have $a + b = 0 \pmod{p}$, therefore, $b = kp - a$ for some integers k, so that

$$F(a,b) = \sum_{r=1}^{p} (-1)^{r-1} a^{P-r} (kp-a)^{r-1} = pa^{p-1} \sum_{r=1}^{p} (-1)^{r-1} a^{P-r} (kp)^{r-1} \left[\sum_{n=r-1}^{p-1} \binom{n}{r-1} \right]$$

Now $$\sum_{r=1}^{p} (-1)^{r-1} a^{P-r} (kp)^{r-1} \left[\sum_{n=r-1}^{p-1} \binom{n}{r-1} \right] \equiv 0 \pmod{p^2}$$

Since when $r = 2$

$$\sum_{r=1}^{p} \binom{n}{1} = \binom{1}{1} + \binom{2}{2} + \ldots + \binom{p-1}{1} = \binom{p}{2} \equiv 0 \pmod{p}$$

Hence $F(a, b) \equiv pa^{p-1} \pmod{p^2}$

The lemma is proved.

Proof of the theorem. By Stone's theorem we may suppose that p divides z. Then we can write

$$z = p^s c \tag{18}$$

where s is a positive integer and c an integer such that $(p, c) = 1$. Now since $x^p + y^p = z^p$, it follows that $x^p + y^p = - p^{sp} c^p$ which implies

$$(x + y) F(x, y) = - p^{sp} c^p \tag{19}$$

But $(x, p) = (y, p) = 1$,

Therefore $x^p + y^p = (x + y) \pmod{p}$, (by Fermat's theorem)

So that we get $- z^p \equiv (x + y) \pmod{p}$

Since p divides z, it follows $x + y = 0 \pmod{p}$.

Hence by the above lemma

$$F(x, y) \equiv px^{p-1} \pmod{p^2}$$

which shows that

$F(x, y) \equiv 0 \pmod{p}$, but

$F(x, y) \not\equiv 0 \pmod{p^2}$.

Hence (19) implies $x + y = p^{sp-1} u$

and $F(x, y) = pv$

where $uv = -c^p$. (20)

Now we shall show that $(u, v) = 1$, for if q is a prime divisor of u and v, $y = tq - x$ for some integer t and hence

$$F(x, y) \equiv px^{p-1} \pmod{q},$$

which shows that $px^{p-1} \equiv 0 \pmod{q}$ and this is false.

Therefore from (20) it follows that $u = z_0^p$ and $v = -z_1^p$

where $z_0 z_1 = c$.

Again $[y + z, F(y, z)] = 1$, for if q_1 is prime divisor of $y + z$ and $F(y, z)$ we have $y = q_1 t_1 - z$ for some integer t_1, so that

$$0 \equiv F(y, z) = pz^{p-1} \pmod{q_1} \text{ and,}$$

hence $pz^{p-1} = 0 \pmod{q_1}$.

Therefore it follows that $q_1 = p$ or q_1 divides z.

If $q_1 = p$, then p divides $y + z$ which together with (18) shows that p divides y and thus we get $(y, z) \neq 1$, which contradicts the hypothesis of the theorem.

If q_1 divides z, it follows that $q1$ divides y and again $(y, z) \neq 1$ and this is false.

Likewise if fellows that $(z + x, F(z, x)) = 1$.

Hence we have the following relations

$$x + y = p^{sp-1} z_0^p \quad (21_1) \quad F(x, y) = -pz_1^p \tag{21}$$

$$y + z = x_0^p \quad (22_1) \quad F(y, z) = -x_1^p \tag{22}$$

$$z + x = x_0 x_1, \; y = y_0 y_1, \; c = z_0 z_1$$

and $x_0, x_1, y_0, y_1, z_0, z_1$ are pairwise prime integers.

Now (22) and (23) imply

$$x + y + 2z = (x_0 + y_0) F(x_0, y_0). \tag{24}$$

But $(p, x_0) = (p, y_0) = 1$, so that

$$x_0^p + y_0^p \equiv (x_0 + y_0) \pmod{p} \tag{25}$$

Since p divides z and also $x + y$, from (22) and (23) we get

$$x_0^p + y_0^p \equiv 0 \pmod{p},$$

hence (25) implies

$$(x_0 + y_0) \equiv 0 \pmod{p}$$

Which follows $F(x_0, y_0) \equiv 0 \pmod{p}$ by lemma.

Therefore (24) implies

$x + y + 2z \equiv 0 \pmod{p^2}$.

Using (21) it fallows that

$z \equiv 0 \pmod{p^2}$

Hence the theorem follows.

REFERENCES

[1] Lander, L. and Parkin, T. (1967) : *A counterexample to Euler's sum of powers conjecture*, Math. Comp., 21:101-103.
[2] Lang, S. (1991) : *Number Theory III: Diophantate Geometry*, Springer-Verlag, Berlin Heidelberg New York.
[3] Lang, S. (1990) : *Old and new conjectured diophantine inequalities*, bull, AMS 23, p. 37-75.
[4] Leech, J. (1957) : *Some solutions of Diophantine equations*, Proc. Cambridge Philos. Soc, 53:778-780.
[5] Martin, A. (1893) : Quart. J. Math., 26:225-227.
[6] Moessner, A. (1947) : *On equal sums of like powers*, Math. Student, 15:83-88.
[7] Mordell, L. J. (1969) : *Diophantine equation*, Academic Press, London and New York.
[8] Niven, I.; Zuckerman, H. S. and Montgomery, H. L. (2001) : *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc.
[9] Oystein, Ore (1976) : *Number Theory and Its History* : Dover Publications.