ON FERMAT'S LAST THEOREM

BY

J. M. GANDHI

Introduction. D. E. Stone [4] proved the following two theorems pertaining to Fermat's Last Theorem (FLT) :

Theorem (A). *If p and $2p+1$ are odd primes and*

$$a^p + b^p + c^p = 0, \tag{1}$$

where a, b, c are non-zero, pairwise prime integers, then precisely one of the integers a, b, c is divisible by $2p+1$.

Theorem (B). *Under the same hypothesis as in Theorem A, precisely one of the integers a, b, c is divisible by p.*

Gandhi [2] proved the

Theorem (C). *If p and $4p+1$ are odd primes and a, b, c are non-zero pairwise prime integers, then one of the integers in (1) must be divisible by $4p+1$.*

In this paper we prove the following Theorems :

Theorem 1. *Under the same hypothesis as in Theorem C, precisely one of the integers a, b, c is divisible by p.*

In view of Theorem *B* and Theorem 1, in proving the following theorems we shall assume that

$$c \equiv 0 \pmod{p}. \tag{2}$$

Then we prove

Theorem 2. *Let p and $2p+1$ be odd primes. If (1) has at all any solutions, then one of the following four congruences must be satisfied*

$$\begin{array}{lll} & a \equiv \pm 1, & a \equiv 0, \\ (3) & b \equiv \mp 1, \pmod{2p+1} \qquad & b \equiv \pm 2, \pmod{2p+1}. \\ & c \equiv 0, & c \equiv \mp 1. \end{array}$$

However if p is such a prime so that $2^p \not\equiv 1 \pmod{2p+1}$, then the necessary conditions for solution of (1) will be only the first two congruences of (3).

Theorem 3. *If p and $4p+1$ are odd primes then the necessary condition for the solution of (1) is that the following two congruences should be satisfied:*

$$
(4) \qquad \begin{array}{ll} a^2 \equiv \pm 1, & a \equiv -b, \\ b^2 \equiv \pm 1, & c \equiv 0, \end{array} \pmod{4p+1}.
$$

Proofs. Firstly let us assume that p and $4p+1$ are odd primes.

Now in view of theorem C, it is known that exactly one of the integers a, b, c is divisible by $4p+1$. Assume that $(abc, p) = 1$, so that it suffices to consider only one case. Thus, let c be divisible by $4p+1$ so that from (1) we have

$$a^p + b^p \equiv \pmod{4p+1}.$$

Now

$$
(5) \qquad a^p + b^p = (a+b)(a^{p-1} - a^{p-2}b + \dots - ab^{p-2} + b^{p-1}) \equiv 0 \pmod{4p+1}.
$$

Legendre has shown (see [2], p. 734) for the case $(abc, p) = 1$ that the integers a, b, c must satisfy the following relations

$$
\begin{array}{llll}
(6a) & a + b = c_0^p, & (7a) & a^{p-1} - a^{p-2}b + \dots + b^{p-1} = -c_1^p, \\
(6b) & c + b = a_0^p, & (7b) & c^{p-1} - c^{p-2}b + \dots + b^{p-1} = -a_1^p, \\
(6c) & c + a = b_0^p, & (7c) & c^{p-1} - c^{p-2}b + \dots + a^{p-1} = -b_1^p,
\end{array}
$$

where $a = a_0 a_1$, $b = b_0 b_1$, $c = c_0 c_1$ and where the integers a_0, a_1, b_0, b_1, c_0, c_1 are pairwise prime. Since $(a, 4p+1) = (b, 4p+1) = 1$, we know that

$$a_0^{2p} \equiv b_0^{2p} \equiv \pm 1 \pmod{4p+1}.$$

Thus, since $4p+1$ divides c, we have from (6b) and (6c)

$$
(8) \qquad a^2 \equiv \pm 1, \quad b^2 \equiv \pm 1 \pmod{4p+1}
$$

so that either $a^2 - b^2 = (a+b)(a-b) \equiv 0, \pmod{4p+1}$, or $a^2 + b^2 \equiv 0, \pmod{4p+1}$. When $a - b$ is divisible by $4p+1$, we see from (5) that $2a^p \equiv 0 \pmod{4p+1}$.

Since p is an odd prime and since $(a, 4p+1) = 1$, this congruence cannot be satisfied. Thus $(a - b, 4p+1) = 1$.

Then consider that $(a+b)$ is divisible by $4p+1$, so that from (6a) we find that c_0 is divisible by $4p+1$. In this case since $(c_0, c_1) = 1$, we see from (7a) that

$$pa^{p-1} \equiv b^{p-1} \equiv -c_1^p \pmod{4p+1}.$$

Squaring both sides of these congruences we get

$$p^2 a^{2p-2} \equiv c_1^{2p} \equiv \pm 1 \pmod{4p+1}$$

is

$$p^2 \equiv \pm a^2 \equiv \pm 1 \pmod{4p+1},$$

which is impossible if p and $4p+1$ are odd primes.

Lastly consider the case

$$a^2 + b^2 \equiv 0 \pmod{4p+1}$$

(originally I missed to discuss this case and it was brought to my attention by the courtesy of Professor L. J. Mordell).

Squaring (6a) and using the last congruence we get

$$2ab \equiv c_0^{2p} \pmod{4p+1}.$$

Since $(ab, 4p+1) = 1$, $c_0 \not\equiv 0 \pmod{4p+1}$, as $c = c_0 c_1 \equiv 0 \pmod{4p+1}$ and $c_0 \equiv 0 \pmod{4p+1}$, hence $c_1 \equiv 0 \pmod{4p+1}$ and therefore from (7a) we get

$$a^{p-1} - a^{p-2}b + \dots + b^{p-1} \equiv 0 \pmod{4p+1},$$

which can be written as

$$
(9) \qquad \begin{array}{l} (a^{p-1} + a^{p-3}b^2 + a^{p-5}b^4 + \dots + b^{p-1}) - \\ \quad - ab(a^{p-1} + a^{p-3}b^2 + \dots + b^{p-3}) \equiv 0 \pmod{4p+1}. \end{array}
$$

Now two cases are to be considered. Firstly when $(p+1)/2$ is odd and nextly when $(p + 1/2$ is even. Let $(p+1)/2$ be odd.

Then using the congruence $a^2 \equiv -b^2 \pmod{4p+1}$ we at once see that the first bracketed term of congruence (9) is exactly divisible by $4p+1$ (as there are even number of terms and every term cancels with the next). While from the second bracketed term we get $-ab^{p-2} \equiv 0 \pmod{4p+1}$ which is also impossible as $(ab, 4p+1) = 1$. This contradiction shows that $(abc, p) \neq 1$. A similar contradiction is obtained when we consider $(p+1)/2$ to be even. Thus, since the integers a, b, c are pairwise prime, exactly one of them must be divisible by p, thereby Theorem 1 is being proved.

Proof of Theorem 2. Let p and $2p+1$ be odd primes, then in view of theorems A and B, we know that one of the integers a, b, c in (1) must be divisible by p and one of them must be divisible by $2p+1$.

Let us then assume that c is divisible by p. So that from (1) we must have [3]:

$$
\begin{array}{llll}
(9a) & a + b = p^{p-1} c_0^p, & (10a) & a^{p-1} - a^{p-2}b + \dots + b^{p-1} = -pc_1^p, \\
(9b) & b + c = a_0^p, & (10b) & c^{p-1} - c^{p-2}b + \dots + b^{p-1} = -a_1^p,
\end{array}
$$

(9c) $\quad c + a = b_0^p,$ $\qquad$ (10c) $\quad c^{p-1} - c^{p-2}a + \dots + a^{p-1} = - b_1^p,$

where $a = a_0 a_1$, $b = b_0 b_1$, $c = pc_0 c_1$.

Let us first consider that $a \equiv 0 \pmod{2p+1}$ since $a = a_0 a_1$ and hence either

(i) $$a_0 \equiv 0 \pmod{2p+1} \text{ or } a_1 \equiv 0 \pmod{2p+1}.$$

Let then $a_0 \equiv 0 \pmod{2p+1}$ and $a_1 \equiv 0 \pmod{2p+1}$. So that from (9a), (9b) and (9c) we get $p(a+b) \equiv p^p c_0^p \equiv \pm 1 \pmod{2p+1}$ or

(11a) $$pb \equiv \pm 1 \pmod{2p+1},$$

(11b) $$b \equiv -c \pmod{2p+1},$$

(11c) $$c \equiv b_0^p \equiv \pm 1 \pmod{2p+1}.$$

Combining (11b) and (11c) from (11a) we get $\pm p \equiv \pm 1 \pmod{2p+1}$, which is impossible as such $a_0 \not\equiv 0 \pmod{2p+1}$.

Let us then consider that $a_1 \equiv 0 \pmod{2p+1}$ and $a_0 \not\equiv 0 \pmod{2p+1}$. So that from (9a), (9b) and (9c) we get $p(a+b) \equiv p^p c_0^p \equiv \pm 1 \pmod{2p+1}$ or

12a) $$pb \equiv \pm 1 \pmod{2p+1},$$

12b) $$b + c \equiv \pm 1 \pmod{2p+1},$$

12c) $$c \equiv \pm 1 \pmod{2p+1}.$$

Hence $b \equiv \pm 2, 0$ and $c \equiv \pm 1 \pmod{2p+1}$ as b is a prime to $2p+1$ and hence

(12d) $$b \equiv \mp 2 \text{ and } c \equiv \pm 1 \pmod{2p+1}$$

while (10b) gives

$$1 + 2 + 2^2 + \dots + 2^{p-1} \equiv 0 \pmod{2p+1},$$

$$\text{that is } 2^p - 1 \equiv 0 \quad \text{or} \quad 2^p \equiv 1 \pmod{2p+1}.$$

Hence if $2^p \not\equiv 1 \pmod{2p+1}$, equation (1) will have no solution under the present assumptions. However if p is such a prime so that $2^p \equiv 1 \pmod{2p+1}$, then (1) may have solutions, provided

(13) $$a \equiv 0; \quad b \equiv \mp 2; \quad c \equiv \pm 1 \pmod{2p+1}.$$

It is observed that congruence (13) gives consistent results when we substitute those congruences in (10a) and (10c).

Since a and b are symmetrical it was immaterial whether we consider $a \equiv 0 \pmod{2p+1}$ or $b \equiv 0 \pmod{2p+1}$. However we have to consider the case when $c \equiv 0 \pmod{2p+1}$, as $c \equiv 0 \pmod{p}$ while $ab \not\equiv 0 \pmod{p}$. Since $c = c_0 c_1$ and hence if $c \equiv 0 \pmod{2p+1}$ then either

$$c_0 \equiv 0 \pmod{2p+1} \quad \text{or} \quad c_1 \equiv 0 \pmod{2p+1}.$$

Let then $c_0 \equiv 0 \pmod{2p+1}$ and $c_1 \not\equiv 0 \pmod{2p+1}$ so that from (9a), (9b) and (9c) we get

(15) $$a + b \equiv 0; \quad b \equiv \pm 1; \quad a \equiv \mp 1 \pmod{2p+1}.$$

It is observed that when congruences (15) are substituted in equations (10a), (10b) and (10c) give consistent results.

Finally let us consider the case when

(16) $$c \not\equiv 0 \pmod{2p+1} \text{ and } c_1 \equiv 0 \pmod{2p+1}.$$

Then from (9a), (9b) and (9c) we get

(17) (a) $\quad p(a+b) \equiv \pm 1; \quad$ (b) $b \equiv \pm 1; \quad$ (c) $a \equiv \pm 1 \pmod{2p+1}$.

If we assume $a \equiv 1$ and $b \equiv -1$ or $a \equiv -1$ and $b \equiv +1 \pmod{2p+1}$. Then (17a) gives inconsistent results. Hence let us assume that

(18) $$a \equiv +1 \text{ and } b \equiv +1, \text{ or } a \equiv -1 \text{ and } b \equiv -1 \pmod{2p+1}.$$

Using (18), from (10a) we get $+1 \equiv 0 \pmod{2p+1}$, which is impossible. Thus our assumption (16) is invalid.

Now combining the congruences (13) and (15) we get the proof of Theorem 2.

Proof of Theorem 2. In view of Theorems (C) and 1, we know that if p and $4p+1$ are both primes then one of a, b, c must be divisible by p and one of them must be divisible by $4p+1$. Let us assume that $c \equiv 0 \pmod{p}$ so that the integers a, b and c satisfy equations (9) and (10). Again it is immaterial whether we assume that a or $b \equiv 0 \pmod{4p+1}$, but since c is divisible by p, we have to consider the case separately when $c \equiv 0 \pmod{4p+1}$.

Let us first consider the case when $a \equiv 0 \pmod{4p+1}$. Since $a = a_0 a_1$ and $(a_0, a_1) = 1$ hence either

(19a) $$a_0 \equiv 0 \pmod{4p+1}, \quad a_1 \not\equiv 0 \pmod{4p+1}$$

or

(19b) $$a_0 \not\equiv 0 \pmod{4p+1}, \quad a_1 \equiv 0 \pmod{4p+1}.$$

Let us firstly consider the condition (19a). Under this case, equations (9a), (9b) and (9c) yield

(20) (a) $\quad b \equiv p^{p-1} c_0^p; \quad$ (b) $b + c \equiv 0; \quad$ (c) $c \equiv b_0^p \pmod{4p+1}$

(20d) $$\therefore b \equiv -c \pmod{4p+1}; \quad c^2 \equiv b_0^{2p} \equiv \pm 1 \pmod{4p+1};$$

$$\therefore b^2 \equiv \pm 1 \pmod{4p+1}.$$

So that squaring (20a) we get $b^2 p^2 \equiv p^{2p} c^{2p} \equiv \pm 1$, which in view of (20d) becomes $p^2 \equiv \pm 1 \pmod{4p+1}$.

Since p and $4p+1$ are odd primes, the last congruence is impossible and as such equation (1) is impossible under condition (19a). Let us then consider the condition (19b). Under this condition from equations (9a), (9b) and (9c) we get

(21) (a) $b^2 p^2 \equiv \pm 1$; (b) $(b+c)^2 \equiv \pm 1$; (c) $c^2 \equiv \pm 1 \pmod{4p+1}$.

From (21) b) we get $b^2 + c^2 + 2bc \equiv \pm 1 \pmod{4p+1}$; using (21a) and (21c) we get $\pm 1 \pm p^2 + 2bcp^2 \equiv \pm p^2 \pmod{4p+1}$, which gives either

(22) (a) $2bcp^2 \equiv \pm 1 \pmod{4p+1}$ or (b) $2bcp^2 \equiv \pm 2p^2 \pm 1 \pmod{4p+1}$;

squaring (22a) and using (21a) and (21c) we get $4p^2 \equiv \pm 1 \pmod{4p+1}$ which is impossible, hence it remains to deal with (22b).

Squaring (22b) and using (21a) and (21b) we get $\pm 4p^2 \equiv (1 \pm 2p^2)^2 \pmod{4p+1}$, which yield either

(23) (a) $4p^4 + 1 \equiv 0 \pmod{4p+1}$ or (b) $4p^4 \pm 8p^2 + 1 \equiv 0 \pmod{4p+1}$.

Congruence (23a) is impossible. Let us then deal with (23b); we have

$$4p^2 \pm 8p^3 + (4p+1) - 4p \equiv 0 \pmod{4p+1}$$

or

$$4p\,(p^3 \pm 2p - 1 \equiv 0 \pmod{4p+1},$$

or

$$p^3 \pm 2p - 1 \equiv 0 \pmod{4p+1},$$

$$p^3 \pm 2p - (4p+1) + 4p \equiv 0 \pmod{4p+1},$$

which gives

$$p^3 + 6p \equiv 0 \pmod{4p+1} \text{ and } p^3 + 2p \equiv 0 \pmod{4p+1} \text{ i. e.}$$

$$p^2 + 6 \equiv 0 \pmod{4p+1}; \quad p^2 + 2 \equiv 0 \pmod{4p+1}.$$

Since the last two congruences are impossible hence equation (1) is impossible under condition (19b)

Let us then consider that

$$c \equiv 0 \pmod{4p+1}.$$

Since $c = c_0 c_1$ and $(c_0, c_1) = 1$ the following two cases arise

(24a) $c_0 \equiv 0 \pmod{4p+1}$, $c_1 \not\equiv 0 \pmod{4p+1}$,

(24b) $c_0 \equiv 0 \pmod{4p+1}$, $c_1 \not\equiv 0 \pmod{4p+1}$.

Firstly let us consider the case (24a). Then from (9a), (9b) and (9c) we get

(25) $a + b \equiv 0 \pmod{4p+1}$; $b^2 \equiv \pm 1 \pmod{4p+1}$; $a^2 \equiv \pm 1 \pmod{4p+1}$.

When the congruences (25) are substituted in equations (10a), (10b) and (10c), they give consistent results. As such if (1) has any solutions congruences (25) must be satisfied.

Finally let us consider the case (24b). Using (24b), equations (9a), (9b) and (9c) yield

(26) (a) $p^2 (a+b)^2 \equiv \pm 1$; (b) $b^2 \equiv \pm 1$; (c) $a^2 \equiv \pm 1 \pmod{4p+1}$,

while (10a) gives

(27) $a^{p-1} - a^{p-2} b + .. + a^2 b^{p-3} - ab^{p-2} + b^{p-1} \equiv 0 \pmod{4p+1}$.

We then show that (26b), (26c) and (27) are inconsistent.

We have to consider the following three cases:

$$\text{28)} \quad \begin{aligned} &\text{(a)} \quad b^2 \equiv +1, \quad a^2 \equiv +1 \pmod{4p+1}, \\ &\text{(b)} \quad b^2 \equiv -1, \quad a^2 \equiv -1 \pmod{4p+1}, \\ &\text{(c)} \quad b^2 \equiv \pm 1, \quad a^2 \equiv \mp 1 \pmod{4p+1}, \end{aligned}$$

we can rewrite (27) as

(29) $$(a^{p-1} + a^{p-3} b^2 + \dots + a^2 b^{p-3} + b^{p-1}) -$$
$$- ab\,(a^{p-3} + a^{p-5} b^2 + \dots + b^{p-3}) \equiv 0 \bmod 4p+1),$$

so that in the bracketed terms we have only expressions which are powers of a^2 and b^2. Moreover the first bracket contains $(p+1)/2$ terms while the second bracket contains $(p-1)/2$ terms.

Consider the congruence (28 a). Then (29) yields

$$\frac{(p+1)}{2} \equiv ab \frac{(p-1)}{2} \pmod{4p+1}, \text{ or}$$

$$(p+1)^2 \equiv (p-1)^2 \pmod{4p+1}; \quad 4p \equiv 0 \pmod{4p+1}$$

which is impossible.

Exactly the same condition will be obtained when we consider congruences (28 b). Last let us consider the congruences (28c) so that $b^2 \equiv -a^2 \pmod{4p+1}$. Then we have to treat two cases namely (a) when $(p-1)/2$ is odd, (b) when $(p-1)/2$ is even. Under case (a) we find that the first bracketed term in (2a) is divisible by $4p+1$ while the second bracketed term yield

$$-ab^{p-2} \equiv 0 \pmod{4p+1}$$

which is impossible, since $(ab, 4p+1) = 1$.

Similarly assuming $(p-1)/2$ to be even we get impossible congruences, so that equation (1) is impossible under the present situation.

Thus the necessary condition for the solution of (1) under the present situation is

$$a + b \equiv 0 ; \quad b^2 \equiv \pm 1 ; \quad a^2 \equiv \pm 1 ; \quad c \equiv 0 \pmod{4p+1},$$

whereby Theorem 3 has been proved.

REFERENCES

1. Dickson E. — *History of Theory of Numbers.* Vol. II, Chelsea Publishing Company, 1952.
2. Gandhi M. — *On Fermat's Last Theorem.* American Math. Monthly 73 (1966), pp. 1106–1107.
3. Mordell J. — *Three Lectures on Fermat's Last Theorem.* Chelsea Publishing Company, 1955.
4. Stone E. D. — *On Fermat's Last Theorem.* American Math. Monthly, 70 (1963). pp. 976–977.

DESPRE ULTIMA TEOREMĂ A LUI FERMAT

Rezumat

Se demonstrează că dacă p şi $4p+1$ sînt numere prime impare şi a, b, c întregi primi între ei doi cîte doi, care satisfac (1), atunci unul şi numai unul din întregii a, b, c este divizibil prin p. Dacă p şi $2p+1$ sînt prime impare şi deci (1) are o soluţie, atunci are loc una din cele 4 relaţii (3): dacă p şi $4p+1$ sînt prime impare, atunci pentru ca (1) să admită soluţie este necesar ca cele 2 congruenţe (4) să fie satisfăcute.

SUR LES ALGÈBRES TERNAIRES

PAR

ION CREANGĂ

Communication présentée à la session scientifique de l'Université „Al. I. Cuza" de 26 – 28 octobre 1969

Soit l'espace linéaire $\mathcal{L}$ doté d'une loi de composition interne, ternaire, ainsi que, par trois vecteurs $x, y, z \in \mathcal{L}$, on détermine, d'une manière unique, un quatrième élément $u \in \mathcal{L}$, à la seule condition que si l'un des facteurs est nul, le produit est nul. C'est une application du produit cartésien $\mathcal{L} \times \mathcal{L} \times \mathcal{L}$ dans $\mathcal{L}$, qui a parmi les préimages de $\mathcal{O}$, les ternes qui contiennent au moins un zéro.

On désigne le produit ternaire des vecteurs x, y, z par $\overline{xyz}$.

Les algèbres binaires sont de même considérées par nous comme des applications du produit cartésien $\mathcal{L} \times \mathcal{L}$ dans $\mathcal{L}$, qui a aussi parmi les préimages de zéro, les couples de vecteurs qui contiennent au moins un zéro. On constate que les algèbres binaires sont aussi des algèbres ternaires et dans une algèbre ternaire on peut avoir des familles d'algèbres binaires, qui sont des sous-algèbres d'algèbre ternaire.

On dit qu'une algèbre $\mathcal{A}$ ternaire est totalement homogène de degré un, par rapport aux scalaires du corps de base et par rapport à chacun des facteurs si l'on a:

$$\alpha\overline{xyz} = \overline{(\alpha . x)yz} = \overline{x(\alpha y)z} = \overline{xy(\alpha z)}. \tag{1}$$

De même l'algèbre $\mathcal{A}$ est totalement distributive si les conditions suivantes sont remplies:

$$\begin{aligned} &(D_1) \quad \overline{(x+y)uv} = \overline{xuv} + \overline{yuv}, \\ &(D_2) \quad \overline{u(x+y)v} = \overline{uxv} + \overline{uyv}, \\ &(D_3) \quad \overline{uv(x+y)} = \overline{uvx} + \overline{uvy}. \end{aligned} \tag{2}$$