146. Generalized Fermat's Last Theorem and Regular Primes

By J. M. GANDHI

(Comm. by Kinjirô KUNUGI, M. J. A., Sept. 12, 1970)

1. Introduction.

According to Fermat's Last Theorem (FLT) the equation

$$x^n+y^n=z^n, \qquad n>2 \tag{1}$$

has no integral solution in non-zero integers. Gandhi [3] generalizing FLT, conjectured that the equation

$$x^n+y^n=cz^n \tag{2}$$

has no solution if $c\leq n$. Here x, y, z are non-zero unequal integers, c and n are also integers. Gandhi [3] proved his conjectures for several even powers and quoted a mass of results from literature to support his conjecture. The purpose of the present paper is to prove

Theorem 1. *The equation*

$$x^l+y^l=cz^l \tag{3}$$

has no integral solutions, where c is any integer prime to the regular prime $l>3$, $(\phi(c), l)=1$ *and*

$$c^{l-1}\not\equiv 1 \pmod{l^2} \qquad 2^{l-1}\not\equiv c^{l-1} \pmod{l^2}.$$

Here and in what follows $\phi(c)$ *denotes Euler's function.*

Consider $n=l$ in (2), l being a regular prime. Let $(c, l)=1$ and $(\phi(c), l)=1$. Then $c<l$ satisfies the condition $(\phi(c), l)=1$ hence in view of Theorem 1 and Maillet's result [9] that the equation $x^l+y^l=lz^l$ is impossible, Gandhi's conjecture is verified for a regular prime l for all such values of c, which satisfy

$$2^{l-1}\not\equiv c^{l-1} \pmod{l^2},\ c^{l-1}\not\equiv 1 \pmod{l^2}$$

Note that the truth of the theorem does not depend on particular values of x, y and z.

To prove Theorem 1, we shall discuss it under three cases.

First Case xyz prime to l
Second Case $xy\equiv 0 \pmod{l}$
Third Case $z\equiv 0 \pmod{l}$.

We note that the following theorem due to Györy [4], contains our theorem for the first two cases, hence we need to prove our theorem for third case only.

Theorem (Györy). *Let p be an arbitrary odd prime* >3. *If* $(\phi(c), p)=1$, $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$ *then* $x^p+y^p=cz^p$, $p\nmid z$ *has a solution only if* $r^{p-1}\equiv 1 \pmod{p^2}$ *for an arbitrary divisor r of c.*

For other results for the diophantine equation $x^n+y^n=cz^n$, refer-

ence may be made to Maillet [9], Lubelski [8], Dénis [1], Vandiver [13], Morishima and Miyoshi [10], Miyoshi [11] and others [2] and it will be observed that several results from them support Gandhi's conjecture. Especially we like to quote the following theorem due to Lubelski [8].

Theorem (Lubelski). *The equation*

$$x^p+y^p=cz^p \qquad (c,p)=1,$$

where p is an arbitrary prime $p\geq 3$ and c is an integral rational number, which has no prime factors of the form $pt+1$ and which is either p^{th} power residue (mod p^2) *or such a p^{th} power non residue for which simultaneously $c/2$ is a p^{th} power non residue* (mod p^2); *has a solution in rational integral x, y, z not divisible by p, then*

$$2^{p-1}\equiv 1 \pmod{p^2}.$$

We note that all values of $c<p$ satisfies the condition that c has no prime factors of the form $pt+1$.

Also the conditions $(\phi(c),p)=1$ and that c does not contain prime factors of the form $pt+1$, are equivalent.

For similar theorems see also [10, 11]. We will like to state the following theorem due to Vandiver [13].

Theorem (Vandiver). *The Equation*

$$x^l+y^l=cz^l \tag{4}$$

where c is a given integer prime to the regular prime $l>3$ and containing only prime factors belonging to even exponents modulo l, has no integral solution if

$$c^{l-1}\not\equiv 1 \pmod{l^2}$$
$$2^{l-1}\not\equiv c^{l-1} \pmod{l^2}.$$

Since a number containing prime factors of the form $pt+1$ belong to an odd exponent mod p, hence Vandiver's theorem cannot cover any other values of c other than those covered by our theorem. Moreover all values of $c<p$ satisfies the conditions of our Theorem 1 i.e., c does not contain prime factors of the form $pt+1$, while it is not necessary that all values of $c<p$ will have prime factors belonging to an even exponent (for example 2 belongs to 3 modulus 7) and hence our theorem contains Vandiver's theorem.

2. Proof of the Theorem.

As mentioned before we need to consider the case $z\equiv 0 \pmod{l}$. We shall prove the theorem for this case following Vandiver [13]. We take (3) in the generalized form

$$\alpha^l+\beta^l=c\xi\lambda^{2lm}\gamma^l\,;\ m>0 \tag{5}$$

where α, β and γ are nonzero integers in the field $K(\zeta+\zeta^{-1})$ prime to each other, ζ being the l^{th} root of unity and ξ is a unit in that field. we need

Lemma 1 (Morishima and Miyoshi).

Under the conditions $(c,l)=1$, $(\phi(c),l)=1$, $\alpha+\beta$ *in* (5) *is divisible by* c.

In other words if c does not contain prime factors of the form $lt+1$ then c cannot have prime ideals of the first degree and hence $\alpha+\zeta^a\beta$ $a>0$ is a prime to c or $\alpha+\beta$ is divisible by c.

In view of Lemma 1, $\alpha+\zeta^a\beta$ is prime to c and hence [see Vandiver [12]]

$$\alpha+\zeta^a\beta=(1-\zeta^a)\xi_a\theta_a^l \tag{6}$$

where ξ_a is a real unit and θ_a is an integer in $K(\zeta)$ and

$$\alpha+\beta=c\xi_0\lambda^{l(2m-1)+1}\theta_0^l \tag{6a}$$

where ξ_0 is a unit and θ_0 an integer in $K(\zeta)$. Consider (6) for a fixed a and take $b\not\equiv\pm a \pmod{l}$. Since $l>3$ we obtain

$$\begin{aligned}(\alpha+\beta\zeta^a)(\alpha+\beta\zeta^{-a})&=(1-\zeta^a)(1-\zeta^{-a})\xi_a^2(\theta_a\theta_{-a})^l\\ (\alpha+\beta\zeta^b)(\alpha+\beta\zeta^{-b})&=(1-\zeta^b)(1-\zeta^{-b})\xi_b^2(\theta_b\theta_{-b})^l\\ (\alpha+\beta)^2&=c^2\xi_0^2\qquad\lambda^{2l(2m-1)+2}\theta_0^{2l}\end{aligned} \tag{7}$$

and also since $\alpha+\beta\equiv 0 \pmod{\lambda^{l(2m-1)+1}}$,

(7) gives

$$\xi_a^2/\xi_b^2\equiv j \pmod{\lambda^l}. \tag{8}$$

Where j is a rational integer. We need

Lemma 2 (Kummer [5]). *If* l *is a regular prime and* ε *is a unit of* $k(\zeta)$ *satisfying* $\varepsilon\equiv a \pmod{\lambda^l}a$ *being a rational number, then there exists a unit* ε_1 *such that* $\varepsilon=\varepsilon_1^l$.

In view of Lemma 2 left member in (8) is a l^{th} power of an unit in $K(\zeta)$. Eliminating α and β from equations (7) and employing (8) we find integers α_1, β_1, and γ_1 in $K(\zeta)$ and a unit δ_1 in $K(\zeta)$ such that

$$\alpha_1^l+\beta_1^l=c^2\delta_1\lambda_1^{S_1}\gamma_1^l;\ S_1=(4m-2)l$$

Also $\gamma_1=\theta_0^2$ and γ_1 therefore contains a less number of distinct ideal factors than γ unless

$$\frac{\alpha+\zeta^i\beta}{1-\zeta^i}$$

is a unit in $K(\zeta)$ where $i=1,2,\cdots,l-1$, whence, since ξ_a is real in (6)

$$\frac{\alpha+\zeta^a\beta}{1-\zeta^a}=\frac{\alpha+\zeta^{-a}\beta}{1-\zeta^{-a}}$$

and this gives $\alpha=-\beta$ which applied to (3) gives $z=0$, contrary to an assumption. Proceeding in this manner, we obtain a relation

$$\alpha_2^l+\beta_2^l=c^4\delta_2\lambda^{S_2}\gamma_2^l$$

in which δ_2 is a unit in $K(\zeta)$, $s_2>s_1$, γ_2 contains less distinct ideal prime factors than γ_1. Hence, we have an infinite reference of algebraic integers.

$$\gamma,\gamma_1,\gamma_2,\cdots$$

in each of which the number of distinct ideal prime factors is less than in the preceeding, which is impossible since the number of distinct

prime ideal factors of an integer in $K(\zeta)$ is finite. This disposes of the third case and the proof of theorem is complete.

My thanks are due to Professor L. Carlitz, Professor D. H. Lehmer, and Professor E. Lehmer for their kind encouragement and helpful discussions.

References

[1] Dénis, P.: Über die diophantische Gleichung $x^l+y^l=cz^l$. Acta Math., **88**, 241-251 (1952).

[2] Dickson, E.: History of Theory of Numbers, Vol. 2. Chelsea Pub. Co. (1952).

[3] Gandhi, J. M.: On Fermat's Last Theorem. Amer. Math. Monthly, **71**, 998-1006 (1964).

[4] György Kálmán: Über die diophantische gleichung $x^p+y^p=cz^p$. Pub. Math., **13**, 301-305 (1966).

[5] Kummer, E. E.: Jour. für Math., **44**, 93-138 (1850) and Jour. de Math., **16**, 454-498 (1851).

[6] ——: Abh. Akad. Wiss. Berlin, 41-74 (1857, 1858).

[7] Landau, E.: Vorlesungen über zahlentheorie, Vol. 3. Leipzig S. Hirzel (1927).

[8] Lubelski, S.: Studien über den groben Fermatschen Satz. Prace Matematyczne, Fiz., **42**, 11-44 (1935).

[9] Maillet, E.: Sur les equations indeterminees de la forme $x^\lambda+y^\lambda=cz^\lambda$. Acta Math., **24**, 247-256 (1901).

[10] Morishima, T., and Miyoshi, T.: On the Diophantine Equation $x^p+y^p=cz^p$. Proc. Amer. Math. Soc., **16**, 833-836 (1965).

[11] Miyoshi, T.: On the Diophantine Equation $x^l+y^l=cz^l$. II. TRU Maths., **2**, 53-54 (1966).

[12] Vandiver, H. S.: On the method of infinite descent for regular prime exponents in connection with Fermat's Last Theorem. Commentarii Mathematici Helvectici, **4**, 1-8 (1932).

[13] ——: On the trinomial Diophantine equation connected with Fermat's relation. Monotshefte für Mathphy, **43**, 317-320 (1936).