# ON THE DIOPHANTINE EQUATION $x^p+y^p=cz^p$

TARO MORISHIMA AND TAKEO MIYOSHI

1. When $p$ is a regular prime, that is, prime to the class number of the cyclotomic field $k(\zeta)$ defined by a primitive $p$th root of unity, $\zeta=e^{2\pi i/p}$, then E. Maillet [1], H. S. Vandiver [2], P. Dénes [3], and others, have obtained a number of results concerning the Diophantine equation

$$x^p + y^p = cz^p, \tag{1}$$

where $x$, $y$, $z$ are nonzero rational integers and $c$ is an integer satisfying several conditions.

If in (1), $c$ is equal to 1, this equation is the so-called Fermat relation.

In the present paper we shall investigate the equation (1) for an arbitrary odd prime $p$ and for an integer $c$ with $(\phi(c), p)=1$, where $\phi(c)$ stands for the Euler's function of $c$ and $(\phi(c), p)$ stands for the greatest common divisor of $\phi(c)$ and $p$.

To study the equation (1), it is convenient to divide the discussion into three cases as follows,

*Case* I. $x$, $y$, $z$ are prime to $p$,

*Case* II. $x$ or $y$ is divisible by $p$,

*Case* III. $z$ is divisible by $p$.

In Case II, we obtain easily the following result:

THEOREM. *Let $p$ be an odd prime and $c$ an arbitrary integer. If $c^{p-1}\not\equiv 1 \pmod{p^2}$, then the equation* (1) *is impossible in integers $x$, $y$, $z$ in Case* II.

The main purpose of this paper is to give two criteria for an integral solution of the equation (1) in Case I with conditions $(\phi(c), p)=1$ and $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$.

2. Let $p$ be an odd prime. Suppose then that

$$x^p + y^p = cz^p \tag{1'}$$

with $x$, $y$, $z$ prime to $p$ and $(\phi(c), p)=1$. It can be shown that with no loss in generality we may suppose that $c$ is prime to $p$ and is $p$th power free, and that $x$, $y$, $z$ are relatively prime in pairs.

Let $k(\zeta)$ denote the cyclotomic field defined by $\zeta=e^{2\pi i/p}$, and put

Received by the editors April 14, 1964.

$1-\zeta=\lambda$. For integers $\alpha$, $\beta$ in $k(\zeta)$ such that $(\alpha, \beta, \lambda)=1$ and $\alpha\equiv\beta \equiv 1 \pmod{\lambda}$, we have the law of reciprocity for $p$th power residues [4]

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{L}, \qquad L = \sum_{n=1}^{p-1} (-1)^{n} l_{n}(\alpha) l_{p-n}(\beta), \tag{2}$$

where

$$l_{n}(\alpha) = \left[\frac{d^{n} \log \alpha(e^{v})}{dv^{n}}\right]_{v=0} \qquad \text{for } 1 \leqq n \leqq p-2$$

and

$$l_{p-1}(\alpha) \equiv -\frac{N(\alpha)-1}{p} \pmod{p},$$

$N(\alpha)$ denoting norm of $\alpha$.

Let us write the equation (1′) as

$$(x+y)(x^{p-1} - x^{p-2}y + \cdots + y^{p-1}) = cz^{p}. \tag{3}$$

First we prove the following lemma:

LEMMA. *If* $(\phi(c), p)=1$, *the first factor* $x+y$ *on the left hand side of* (3) *is divisible by* $c$.

PROOF. Suppose that $x+y$ is not divisible by $c$. Since $(x, c)=1$, there exists an integer $u$ such that $xu\equiv -1 \pmod{c}$, $(u, c)=1$. From (1′) and the hypothesis, it follows that $(xu)^{p}+(yu)^{p}\equiv 0 \pmod{c}$ and $xu+yu\not\equiv 0 \pmod{c}$, consequently $(yu)^{p}\equiv 1 \pmod{c}$ and $yu\not\equiv 1 \pmod{c}$. On the other hand $(yu)^{\phi(c)}\equiv 1 \pmod{c}$. Hence we have $\phi(c)\equiv 0 \pmod{p}$, contrary to $(\phi(c), p)=1$.

Using (3) and the fact that $(cz, p)=1$, it is easily seen that

$$\left(\frac{x+y}{c}, x^{p-1} - x^{p-2}y + \cdots + y^{p-1}\right) = 1.$$

Hence the second factor on the left hand side of (3) can be written as

$$\prod_{m=1}^{p-1} (x+\zeta^{m}y) = w^{p},$$

where $w$ is a factor of $z$, $\zeta$ a primitive $p$th root of unity.

Since each two of the ideals $[x+\zeta^{m}y]$ $(m=1, 2, \cdots, p-1)$, are relatively prime, it follows that each of them must be the $p$th power of an ideal in $k(\zeta)$. In particular $[x+\zeta y]=\mathfrak{A}^{p}$, $\mathfrak{A}$ being an ideal in $k(\zeta)$.

Employing the law of reciprocity in (2) we obtain the following theorems just as in the Fermat relation [5].

THEOREM 1. *Let $p$ be an odd prime and $c$ an integer with $(\phi(c), p)=1$. If the equation (1′) is satisfied in integers prime to $p$, then we have for any factor $r$ of $x$ or $y$*

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

THEOREM 2. *If the equation (1′) is satisfied in integers prime to $p$ with $(\phi(c), p)=1$, provided $x-y$ is prime to $p$, we have for a factor $r$ of $x-y$*

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

We also have the following theorem:

THEOREM 3. *Under the same conditions as in Theorem 2, we have for a factor $r$ of $x+y$*

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

PROOF. $\alpha=(x+\zeta^2 y)(x+\zeta y)^{p-1}$ is prime to $r$ and its ideal is equal to the $p$th power of an ideal in $k(\zeta)$. Hence we have

$$\left(\frac{\alpha}{r}\right)\left(\frac{r}{\alpha}\right)^{-1} = \left(\frac{\alpha}{r}\right) = \zeta^{K}, \qquad K = y(r^{p-1}-1)/(x+y)p. \tag{4}$$

Since $x+y\equiv 0 \pmod{r}$,

$$\left(\frac{\alpha}{r}\right) = \left(\frac{1+\zeta}{r}\right) = \zeta^{-l_1(1+\zeta)\, l_{p-1}(r)}. \tag{5}$$

From (4) and (5) we have $r^{p-1}\equiv 1 \pmod{p^2}$.

We are now in a position to give criteria for an integral solution of (1′) in Case I with conditions $(\phi(c), p)=1$ and $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$.

THEOREM 4. *If the equation (1′) is satisfied in integers $x, y, z$ prime to $p$ and if $(\phi(c), p)=1$ and $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$, then we have*

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{6}$$

PROOF. If $x$ or $y$ is divisible by 2, then the theorem follows immediately from Theorem 1. If $x\equiv y\equiv 1 \pmod 2$, then $x-y$ is divisible by 2. Moreover $x-y$ is prime to $p$, because if $x-y$ is divisible by $p$, then $c^{p-1}\equiv 2^{p-1} \pmod{p^2}$, contrary to the hypothesis. Hence by Theorem 2 we obtain $2^{p-1}\equiv 1 \pmod{p^2}$.

THEOREM 5. *Under the same conditions as in Theorem 4, we have*

(7) $$3^{p-1} \equiv 1 \pmod{p^2}.$$

PROOF. Since one of $xy$, $x-y$, $x+y$ is divisible by 3, the theorem follows at once from Theorems 1, 2, 3 respectively.

The only primes $p$ less than $10^6$ for which the congruence (6) is satisfied are $p=1093$ and $p=3511$ [6], and $3^{1092} \not\equiv 1 \pmod{1093^2}$, $3^{3510} \not\equiv 1 \pmod{3511^2}$ [7]. Hence by Theorems 4 and 5 we obtain the following theorem:

THEOREM 6. *If* $(\phi(c), p)=1$ *and* $c^{p-1} \not\equiv 2^{p-1} \pmod{p^2}$, *then the equation*

$$x^p + y^p = cz^p$$

*is impossible in integers* $x, y, z$ *prime to* $p$ *for all odd primes* $p$ *less than* $10^6$.

We shall give here some examples of $c$ which satisfy the conditions in Theorem 6.

(1) Choose $c$ such that $c=2+kp$, $(k, p)=1$, and $(\phi(c), p)=1$.

(2) (i) $c=2^{n+1}$, $(n, p)=1$, $p \neq 1093, 3511$;

(ii) $c=2(k_1p^2+2)^{n_1}(k_2p^2+2)^{n_2} \cdots (k_ip^2+2)^{n_i}$, where each of the factors is a prime, $n_1+n_2+\cdots+n_i \not\equiv 0 \pmod{p}$ and $p \neq 1093, 3511$.

## REFERENCES

1. E. Maillet, *Sur les équations indéterminées de la forme* $x^\lambda+y^\lambda=cz^\lambda$, Acta Math. **24** (1901), 247–256.

2. H. S. Vandiver, *On trinomial diophantine equations connected with the Fermat relation*, Monatsh. Math. Phys. **43** (1936), 317–320.

3. P. Dénes, *Ueber die diophantische Gleichung* $x^l+y^l=cz^l$, Acta Math. **88** (1952), 241–251.

4. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. II, Jber. Deutsch. Math. Verein. **6** (1930), 110.

5. ———, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. II, Jber. Deutsch. Math. Verein. **6** (1930), 120–121.

6. M. Hausner and D. Sachs, *On the congruence* $2^p \equiv 2(p^2)$, Amer. Math. Monthly **70** (1963), 996.

7. H. Riesel, *Note on the congruence* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comput. **18** (1963), 149–150.

TOKYO COLLEGE OF SCIENCE, TOKYO, JAPAN