TOKYO J. MATH.
VOL. 13, NO. 2, 1990

Generalization of Lucas' Theorem for Fermat's Quotient II

Nobuhiro TERAI

Waseda University
(Communicated by T. Kori)

Introduction.

Let p be an odd prime number and let m be a positive integer prime to p. We define Fermat's quotient $q_p(m)$ by $q_p(m)=\frac{m^{p-1}-1}{p}$. Lucas ([2], [5]) proved that $q_p(2)$ is a square only for $p=3$ and 7. To generalize Lucas' theorem, we consider whether the equation

$$(*)\qquad q_p(m)=x^l$$

has solutions or not, where l is a prime and x is a positive integer.

In the previous paper [9], we considered the three cases of $(*)$:

$$(\mathrm{I})\qquad q_p(m)=x^2 \qquad (p>3)$$

$$(\mathrm{II})\qquad q_p(r)=x^r \qquad (r \text{ is an odd prime})$$

$$(\mathrm{III})\qquad q_p(2)=x^l \qquad (l \text{ is an odd prime})$$

and we obtained the following three theorems:

THEOREM A. *If m is odd, then the equation* (I) *has the only solution* $(p, m, x)=(5, 3, 4)$.

THEOREM B. *If the equation* (II) *has solutions, then p and r satisfy the congruences*

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

THEOREM C. *The equation* (III) *has the only solution $p=3$.*

In this paper, we treat more general cases of $(*)$. In §1, we discuss the equation $(*)$ when m is even and $p>3$. Then it is proved that if Catalan's conjecture holds, namely, if the only solution in integers $m>1$,

Received October 5, 1989

$n>1$, $x>1$ and $y>1$ of the equation

$$x^m - y^n = 1$$

is $(m, n, x, y)=(2, 3, 3, 2)$, then the equation $(*)$ has the only solution $(p, m, x, l)=(7, 2, 3, 2)$ (Theorem 1).

In §2 and §3, we consider the equation $(*)$ when m is odd $\geqq 3$. The following is our main result:

If l is a prime >3 and $m \pm 1 \not\equiv 0 \pmod{2^{l-2}}$, then the equation $(*)$ has no solutions (p, m, x, l) (Theorem 2).

In particular, if m is even, the equation (I) has the only solution $(p, m, x)=(7, 2, 3)$ by Theorem 1 and Remark. The equation (II) has no solutions by Theorem 4. Combining these with the previous results in [9], the equations (I), (II) and (III) have been solved completely.

§1. The equation $q_p(m)=x^l$ (m is even).

In this section we treat the equation $q_p(m)=x^l$ when m is even. Then we prove the following:

THEOREM 1. *Suppose Catalan's conjecture holds. If p is a prime >3 and m is even, then the equation*

$$q_p(m)=x^l \tag{1.1}$$

has the only solution $(p, m, x, l)=(7, 2, 3, 2)$.

PROOF. By the equation (1.1), we have

$$(m^{(p-1)/2}+1)(m^{(p-1)/2}-1)=px^l .$$

Since m is even, we have the following two cases;

$$(m^{(p-1)/2}+1,\ m^{(p-1)/2}-1)=\begin{cases}(y^l,\ pz^l) & \text{(a)}\\ (py^l,\ z^l) & \text{(b)}\end{cases}$$

where y and z are positive integers with $x=yz$.

We first consider the case (a). Then we have

$$y^l - m^{(p-1)/2}=1 . \tag{1.2}$$

If Catalan's conjecture holds, then the equation (1.2) has the only solution $(p, m, y, l)=(7, 2, 3, 2)$. Thus from $m^{(p-1)/2}-1=pz^l$, $z=1$ and so $x=3$.

We next consider the case (b). Then we have

$$m^{(p-1)/2}-z^l=1 . \tag{1.3}$$

If Catalan's conjecture holds, then the equation (1.3) has the only solution $(p, m, z, l)=(5, 3, 2, 3)$. But this solution can not satisfy $m^{(p-1)/2}+1=py^l$. This completes the proof of Theorem 1. □

REMARK. It was proved that if $\min.(m, n)\leqq 3$, the only solution integers $m>1$, $n>1$, $x>1$ and $y>1$ of the equation

$$x^m-y^n=1$$

is $(m, n, x, y)=(2, 3, 3, 2)$ (cf. Lebesgue [3], Chao Ko [1] and Nagell [6]). Therefore we see that Theorem 1 unconditionally holds for $l=2$ and 3.

§2. The equation $q_p(m)=x^l$ (m is odd and l is a prime >3).

In this section we treat the equation $q_p(m)=x^l$ when m is odd and l is a prime >3. We use the following lemma to prove Theorem 2.

LEMMA 1 (Störmer [10]). *The Diophantine equation*

$$x^2+1=2y^n$$

has no solutions in integers $x>1$, $y\geqq 1$ and n odd $\geqq 3$.

THEOREM 2. *Let m be odd $\geqq 3$ and l be an odd prime >3. If $m\pm 1\not\equiv 0 \pmod{2^{l-2}}$, then the equation*

$$q_p(m)=x^l \tag{2.1}$$

has no solutions (p, m, x, l).

PROOF OF THEOREM 2. By the equation (2.1), we have

$$(m^{(p-1)/2}+1)(m^{(p-1)/2}-1)=px^l\ .$$

Since m is odd, we have the following four cases;

$$(m^{(p-1)/2}+1,\ m^{(p-1)/2}-1)=\begin{cases}(2y^l,\ 2^{l-1}pz^l) & \text{(a)}\\ (2^{l-1}y^l,\ 2pz^l) & \text{(b)}\\ (2^{l-1}py^l,\ 2z^l) & \text{(c)}\\ (2py^l,\ 2^{l-1}z^l) & \text{(d)}\end{cases}$$

where y and z are positive integers with $x=2yz$. Then we put $n=\dfrac{p-1}{2}$.

We first consider the case (a). Then we have

$$m^n+1=2y^l\ . \tag{2.2}$$

If n is even, it follows from Lemma 1 that the equation (2.2) has no solutions. Suppose n is odd. We also have the equation

$$m^n - 1 = 2^{l-1} p z^l .$$

Hence we obtain the congruence $m-1 \equiv 0 \pmod{2^{l-1}}$, since m and n are odd. This contradicts our assumption.

We next consider the case (b). Then we have

$$m^n + 1 = 2^{l-1} y^l .$$

If n is even, we have $(m^{n/2})^2 \equiv -1 \pmod 4$, which is impossible. If n is odd, we obtain the congruence $m+1 \equiv 0 \pmod{2^{l-1}}$, which contradicts our assumption.

The case (c) also yields a contradiction as in the case (b). Finally, we consider the case (d). Then we have

$$m^n - 1 = 2^{l-1} z^l . \tag{2.3}$$

If n is odd, we obtain $m-1 \equiv 0 \pmod{2^{l-1}}$, which is a contradiction by our assumption. Suppose n is even. Then we show that $n \not\equiv 0 \pmod 4$. Suppose the contrary, say $n=4k$ for some positive integer k. Then by the equation (2.3), we have the following two cases;

$$(m^{2k}+1,\ m^{2k}-1) = \begin{cases} (2z_1^{\,l},\ 2^{l-2} z_2^{\,l}) & \text{(d1)} \\ (2^{l-2} z_1^{\,l},\ 2z_2^{\,l}) & \text{(d2)} \end{cases}$$

where z_1 and z_2 are positive integers with $z = z_1 z_2$. In the case (d1), we have

$$m^{2k} + 1 = 2 z_1^{\,l} . \tag{2.4}$$

It follows from Lemma 1 that the equation (2.4) has no solutions. In the case (d2), we have

$$m^{2k} + 1 = 2^{l-2} z_1^{\,l} .$$

Since $l > 3$, we obtain $(m^k)^2 \equiv -1 \pmod 4$, which is impossible. Therefore $n \not\equiv 0 \pmod 4$. Thus we can put $n = 2k$ for some odd k, since n is even. Then by the equation (2.3), we have the following two cases;

$$(m^k+1,\ m^k-1) = \begin{cases} (2z_3^{\,l},\ 2^{l-2} z_4^{\,l}) & \text{(d3)} \\ (2^{l-2} z_3^{\,l},\ 2z_4^{\,l}) & \text{(d4)} \end{cases}$$

where z_3 and z_4 are positive integers with $z = z_3 z_4$. In the case (d3), we have

$$m^k - 1 = 2^{l-2} z_4{}^l .$$

Since k is odd, we obtain $m-1 \equiv 0 \pmod{2^{l-2}}$, which gives a contradiction by our assumption. In the case (d4), we have

$$m^k + 1 = 2^{l-2} z_3{}^l .$$

Hence we obtain $m+1 \equiv 0 \pmod{2^{l-2}}$, which gives a contradiction. This completes the proof of Theorem 2. □

Using Theorem 2, we show the following corollaries:

COROLLARY 1. *Let m be odd $\geqq 3$ and l be an odd prime >3. If $m \equiv 3, 5 \pmod 8$, then the equation*

$$q_p(m) = x^l$$

has no solutions (p, m, x, l).

PROOF. If $m \equiv 3, 5 \pmod 8$, $m \pm 1 \equiv 2, 4\ 6 \pmod 8$ and so $m \pm 1 \not\equiv 0 \pmod 8$. Thus we obtain $m \pm 1 \not\equiv 0 \pmod{2^{l-2}}$, since l is an odd prime >3. Hence by Theorem 2, the equation

$$q_p(m) = x^l$$

has no solutions (p, m, x, l). This completes the proof of the corollary. □

COROLLARY 2. *Let m be odd $\geqq 3$ and l be an odd prime >3. If m is a biquadratic number, then the equation*

$$q_p(m) = x^l$$

has no solutions (p, m, x, l).

PROOF. By the proof of Theorem 2, it follows that in the case (a), (b) and (c), the equation $q_p(m) = x^l$ has no solutions when n is even, and in the case (d) the equation $q_p(m) = x^l$ has no solutions when $n \equiv 0 \pmod 4$. If m is a biquadratic number, it implies that $n \equiv 0 \pmod 4$, in the proof of Theorem 2. Therefore the equation $q_p(m) = x^l$ has no solutions (p, m, x, l) if m is a biquadratic number. Hence the proof of the corollary is complete. □

§3. The equation $q_p(m) = x^3$ (m is odd).

In this section we consider the equation $q_p(m) = x^3$, where m is odd $\geqq 3$. Then in view of the proof of Theorem 2, we have the following four cases;

(a) $$m^n+1=2y^3 \quad \text{and} \quad m^n-1=4pz^3\,,$$

(b) $$m^n+1=4y^3 \quad \text{and} \quad m^n-1=2pz^3\,,$$

(c) $$m^n+1=4py^3 \quad \text{and} \quad m^n-1=2z^3\,,$$

(d) $$m^n+1=2py^3 \quad \text{and} \quad m^n-1=4z^3\,,$$

where $n=\frac{p-1}{2}$.

Now we prepare the three lemmas which we use in this section. The following lemma is well known (cf., e.g., Nagell [8]):

LEMMA 2. *The Diophantine equation*

$$x^3+y^3=2^n z^3 \qquad (n=0,\ 1,\ 2)$$

has no solutions in integers x, y and z with $xyz\neq 0$ other than $x^3=y^3=z^3$ when $n=1$.

LEMMA 3 (Nagell [7]). *The Diophantine equation*

$$Ax^3+By^3=C$$

($C=1$ or 3; $3\nmid AB$ if $C=3$; A, B, C positive integers) has at most one solution in nonzero integers (x, y). There is the unique exception for the equation $2x^3+y^3=3$, which has exactly the two integral solutions $(x, y)=(1, 1)$ and $(4, -5)$.

LEMMA 4 (Ljunggren [4]). *The Diophantine equation*

$$\frac{x^n-1}{x-1}=y^3\,,$$

where $n\geqq 3$ with $n\not\equiv -1 \pmod 6$ and $|x|>1$, has the only integral solution $(x, y, n)=(18$ or $-19, 7, 3)$.

We start with the following proposition:

PROPOSITION 1. (1) *The Diophantine equation*

$$x^2-1=4y^3$$

has no solutions in integers x and y with $y\neq 0$.

(2) *The Diophantine equation*

$$x^3+6y^3=1$$

has no solutions in integers x and y with $y \neq 0$.

PROOF. (1) Since we have $(x+1)(x-1)=4y^3$ and $(x+1, x-1)=2$, there exist integers u and v with $y=uv\neq 0$ such that

$$x+1=2u^3 \quad \text{and} \quad x-1=2v^3 .$$

Therefore we obtain $1^3=u^3+(-v)^3$. By Lemma 2, the equation has no solutions.

(2) We write the equation as

$$(x-1)(x^2+x+1)=6(-y)^3 .$$

The greatest common divisor of the two factors on the left is 1 or 3. It is easily seen that x^2+x+1 is odd and is not divisible by 9. Hence we obtain the following two cases;

$$x-1=2u^3 \qquad \text{and} \quad x^2+x+1=3v^3 ,$$

or

$$x-1=2*3^3*u^3 \quad \text{and} \quad x^2+x+1=3v^3 ,$$

for some nonzero integers u and v. Thus it suffices to show that the equation

$$X^2+X+1=3Y^3$$

has no solutions in integers X and Y with $X\neq 1, -2$. Since the above equation can be written as

$$\left(\frac{X+2}{3}\right)^3+\left(\frac{1-X}{3}\right)^3=Y^3 , \tag{3.1}$$

we see that the equation (3.1) has no solutions in integers X and Y with $X\neq 1, -2$, by Lemma 2. □

Now we may assume that n is odd in the cases (a), (b), (c) and (d), by the proof of Theorem 2 and Proposition 1 (1).

We first treat the case $p=3$. Then we have the following:

PROPOSITION 2. *Let m be odd $\geqq 3$. Then the equation*

$$q_3(m)=x^3$$

has the only solution $(m, x)=(5, 2)$.

PROOF. As easily seen, the four cases (a), (b), (c) and (d) when $p=3$, are reduced to the following two cases;

$$X^3+6Y^3=1\ , \tag{3.2}$$

$$2X^3+3Y^3=1\ , \tag{3.3}$$

with nonzero integers X and Y.

By Proposition 1 (2), the equation (3.2) has no solutions (X, Y). By Lemma 3, the equation (3.3) has the only solution $(X, Y)=(-1, 1)$. Hence the equation $q_3(m)=x^3$ has the only solution $(m, x)=(5, 2)$. □

Further, we may assume that $n=\frac{p-1}{2}$ is odd $\geqq 3$, since we considered the case $p=3$. Therefore from the cases (a), (b), (c) and (d), we have only to treat the equations

$$X^n-1=2Y^3\ , \tag{3.4}$$

$$X^n-1=4Y^3\ , \tag{3.5}$$

where n is odd $\geqq 3$ and X, Y are integers with $|X|>1$. Then we show the following:

PROPOSITION 3. (1) *Suppose X is an integer satisfying the following two conditions;*

(i) $\frac{X-1}{2}$ *is not a cube, or*

if $\frac{X-1}{2}$ *is a cube, then* $X\not\equiv 1$, 5 *and* 6 (mod 7).

(ii) $\frac{X-1}{2}$ *is not of the form* q^2a^3, *where a is an integer and q is an odd prime* >3.

Then the equation (3.4) *has no solutions in integers X, Y and n with* $|X|>1$ *and n odd* $\geqq 3$.

(2) *Suppose X is an integer satisfying the following two conditions;*

(i) $\frac{X-1}{4}$ *is not a cube, or*

if $\frac{X-1}{4}$ *is a cube, then* $X\not\equiv 1$, 2 *and* 3 (mod 7).

(ii) $\frac{X-1}{4}$ *is not of the form* q^2a^3, *where a is an integer and q is an odd prime* >3.

Then the equation (3.5) *has no solutions in integers* X, Y *and* n *with* $|X|>1$ *and* n *odd* $\geqq 3$.

PROOF. (1) We may assume that n is an odd prime, say q. Suppose $q=3$. Then the equation (3.4) becomes

$$X^3-1=2Y^3 . \tag{3.6}$$

The equation (3.6) has no solutions in integers X and Y with $|X|>1$, by Lemma 2. Thus we may suppose that $q>3$.

It is easily seen that $\dfrac{X^q-1}{X-1}$ is odd, and the greatest common divisor d of $X-1$ and $\dfrac{X^q-1}{X-1}$ is 1 or q, and $\dfrac{X^q-1}{X-1}\equiv q \pmod{q^2}$, if $d=q$. If $d=1$, then we obtain by the equation (3.4)

$$\frac{X-1}{2}=a^3 \quad\text{and}\quad \frac{X^q-1}{X-1}=b^3 \tag{3.7}$$

for some integers a and b. When $q\not\equiv -1 \pmod 6$, it follows from Lemma 4 that the second equation in (3.7) has no solutions in integers X, b and q with $|X|>1$, since $q>3$. When $q\equiv -1 \pmod 6$, we put $q=6k-1$ for some integer k. Then by the equation (3.4), we have

$$X^{6k-1}-1=2Y^3 ,$$

so

$$X^{6k}-X=2XY^3 .$$

Taking the equation modulo 7, we obtain

$$1-X\equiv 2XY^3 \pmod 7 .$$

Since $X\not\equiv 1$, 5 and 6 (mod 7), we have

$$Y^3\equiv 2,\ 4 \text{ and } 5 \pmod 7 ,$$

which is impossible.

If $d=q$, then we obtain by the equation (3.4)

$$\frac{X-1}{2}=q^2c^3 \quad\text{and}\quad \frac{X^q-1}{X-1}=qd^3 \tag{3.8}$$

for some integers c and d. But the first equation in (3.8) contradicts the condition (ii).

(2) Similarly we can prove the case (2). □

PROPOSITION 4. *Let m be odd $\geqq 3$. If m is a cube, then the equation*

$$q_p(m)=x^3$$

has no solutions (p, m, x).

PROOF. Since m is a cube, it suffices to consider the equations

$$X^3-1=2Y^3$$

and

$$X^3-1=4Y^3 ,$$

respectively, where X and Y are integers with $|X|>1$. It follows from Lemma 2 that the equations have no solutions. □

Using Proposition 2 and Proposition 3, we immediately obtain the following:

PROPOSITION 5. *Let m be odd $\geqq 3$. If $m<50$, then the equation*

$$q_p(m)=x^3$$

has the only solution $(p, m, x)=(3, 5, 2)$.

PROOF. If $p=3$, we have the only solution $(p, m, x)=(3, 5, 2)$ by Proposition 2. If $p>3$, then $X=\pm m$ satisfy the conditions of Proposition 3 when $m<50$ except for $X=-15$. When $X=-15$, the congruence

$$X^{6k}-X\equiv 2XY^3 \pmod{13}$$

does not hold. Therefore the equation $q_p(m)=x^3$ has no solutions (p, m, x), if $p>3$. □

Now, by Corollary 1 in §2 and Proposition 5, we obtain the following:

THEOREM 3. *Let m be odd $\geqq 3$ and l be odd prime. If $m\equiv 3, 5 \pmod 8$ and $m<50$, then the equation*

$$q_p(m)=x^l$$

has the only solution $(p, m, x, l)=(3, 5, 2, 3)$.

Finally, we prove the following theorem on the equation

$$q_p(r)=x^r \qquad (r \text{ is odd } \geqq 3)$$

which we considered in [9].

THEOREM 4. *If r is odd $\geqq 3$, then the equation*

$$q_p(r)=x^r$$

has no solutions (p, r, x).

PROOF. We may clearly assume that l is odd $\geqq 3$ in Theorem 2 in §2. If $r>3$, the congruence $r\pm 1\not\equiv 0 \pmod{2^{r-2}}$ holds. Hence it follows from Theorem 2 that the equation $q_p(r)=x^r$ has no solutions (p, r, x), if $r>3$.

If $r=3$, the equation $q_p(r)=x^r$ has no solutions (p, r, x), by Proposition 5. □

References

[1] CHAO KO, On the Diophantine equation $x^2=y^n+1$, $xy\neq 0$, Scientia Sinica (Notes), **14** (1964), 457–460.

[2] L. E. DICKSON, *History of the Theory of Numbers, Vol. I*, reprinted by Chelsea, 1971.

[3] V. A. LEBESGUE, Sur l'impossibilité, en nombres entiers, de l'équation $x^m=y^2+1$, Nouv. Ann. Math. (1), **9** (1850), 178–181.

[4] W. LJUNGGREN, Noen setningen om ubestemte likninger av formen $\frac{x^n-1}{x-1}=y^q$, Norsk. Mat. Tidsskr., **25** (1943), 17–20.

[5] E. LUCAS, *Théorie des Nombres*, Gauthier-Villars, Paris, 1891, reprinted by A. Blanchard, Paris, 1961.

[6] T. NAGELL, Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$, Norsk. Mat. Forenings Skrifter, **I**, No. 2 (1921), 1–14.

[7] T. NAGELL, Solution complète de quelques équations cubiques a deux indéterminées, J. Math. Pures Appl. Ser. 9, **4** (1925), 209–270.

[8] T. NAGELL, *Introduction to Number Theory*, Chelsea, 1981.

[9] H. OSADA and N. TERAI, Generalization of Lucas' Theorem for Fermat's quotient, C. R. Math. Rep. Acad. Sci. Canada, **11** (1989), 115–120.

[10] C. STÖRMER, L'equation $m \operatorname{arctang} \frac{1}{x}+n \operatorname{arctang} \frac{1}{Y}=k\frac{\pi}{4}$, Bull. Soc. Math. France, **27** (1899), 160–170.

Present Address:
DEPARTMENT OF MATHEMATICS, SCHOOL OF SCIENCE AND ENGINEERING
WASEDA UNIVERSITY
OKUBO, SHINJUKU-KU, TOKYO 169, JAPAN