Conspectus materiae tomi LIV, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires à l'adresse ci-dessus
The authors are requested to submit papers in two copies to the above address
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit an die obige Adresse
Рукописи статей редакция просит предлагать в двух экземплярах на вышеуказанный адрес

ISBN 83-01-09228-9 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
LIV (1989)

On a diophantine equation of a modified Fermat type

by

KUSTAA INKERI (Turku)

1. Introduction and preliminaries. In this paper we deal with the diophantine equation

$$x^{l^n}+y^{l^n}=cz^{l^m}, \tag{1}$$

where l is an odd prime, m and n are positive integers with $l^n > 3$ and c is an integer, which will be restricted by certain conditions. The case $c = 1$ has been discussed in detail in [1] by Azuhata and in [5] by Inkeri.

We shall prove some theorems and corollaries in which certain results presented in our earlier papers [3] and [4] have been generalized and improved on.

For brevity let

$$Q_0(x, y) = x+y, \quad Q_n(x, y) = \frac{x^{l^n}+y^{l^n}}{x^{l^{n-1}}+y^{l^{n-1}}} \quad (n = 1, 2, \dots).$$

Let x and y be any integers with $x+y \neq 0$ and $\gcd(x, y) = 1$. Then the numbers Q_n ($n = 0, 1, \dots$) have fulfilled the following conditions (see e.g. [2], [6]):

(a) If $l \nmid x+y$, then the numbers Q_n are pairwise relatively prime integers and none of Q_n is divisible by l.

(b) If $l \mid x+y$, then the same holds for the numbers $\frac{1}{l} Q_n$ and in addition $l^2 \nmid Q_n$ for $n = 1, 2, \dots$ (every Q_n is divisible by l).

(c) For $n = 1, 2, \dots$ all the prime divisors of Q_n different from l, are of the form kl^n+1.

Our scrutiny will be based on the following result proved in our recent paper ([5], Theorem 2).

THEOREM 1. *If the nonzero integers x, y, z satisfy the equation*

$$Q_n(x, y) = l^e z^{l^m}, \tag{2}$$

where m and n are positive integers, $e = 0$ or 1, and $x+y \neq 0$, $(x, y, z) = 1$, $l \nmid z$, then for a prime p

(3) $$p^{l-1} \equiv 1 \pmod{l^{m+n}}$$

in the following two cases

(i) $p|x$, $l\nmid x$;

(ii) $p|x^2-y^2$, $l\nmid x^2-y^2$.

2. Theorems and corollaries. The following theorem is an almost immediate issue from the preceding theorem.

THEOREM 2. *Let c be an integer containing no prime divisors of the form kl^n+1. If the integers x, y, z satisfy the equation* (1) *with $(x, y) = 1$, then the congruence* (3) *holds for a prime p in both of the cases* (i) *and* (ii).

Proof. Clearly the trivial cases $xyz = 0$ and $x+y = 0$ are excluded both in (i) and (ii). By the assumption also $(x, y, cz) = 1$. By (a) and (b) we see easily that

$$\gcd(x^{l^{n-1}}+y^{l^{n-1}}, Q_n(x, y)) = 1 \text{ or } l$$

according as $l\nmid cz$ or $l|cz$. Moreover $l^2\nmid Q_n(x, y)$. Noting in addition (c) we infer by the assumption concerning c, that $(Q_n, c) = 1$ or l. Since (1) can be written

$$(x^{l^{n-1}}+y^{l^{n-1}})Q_n(x, y) = cz^{l^m},$$

it follows that

$$Q_n(x, y) = l^e z_1^{l^m},$$

where $z_1|z$, $(x, y, z_1) = 1$, $l\nmid z_1$ and $e = 0$ or 1. The results follow now from Theorem 1.

Theorem 2 implies the following

COROLLARY 1. *If the assumptions of Theorem 2 are valid and if none of the numbers x, y and x^2-y^2 is divisible by $2l$ or by $3l$, then*

$$2^{l-1} \equiv 1 \quad \text{or} \quad 3^{l-1} \equiv 1 \pmod{l^{m+n}},$$

respectively.

Proof. It is evident that one of the numbers x, y, x^2-y^2 is divisible by 2 and one by 3, but this number is non-divisible by l because of the assumption. We establish at once that the validity of the congruences follows directly from Theorem 2.

Remark. For $m = n = c = 1$ this corollary gives, as may easily be verified, Wieferich's and Mirimanoff's well-known criteria concerning the first case of Fermat's last theorem.

The following corollary is a simple extension of Theorem 2.

COROLLARY 2. *Let t be an integer with $0 \leqslant t < n$ and let c be an integer containing no prime divisors of the form $kl^{n-t}+1$. If x, y, z satisfy* (1) *with $(x, y) = 1$ and $l\nmid x^2-y^2$, and if for a prime p*

$$p|x^{2l^t}-y^{2l^t},$$

then

(4) $$p^{l-1} \equiv 1 \pmod{l^{m+n-t}}.$$

Proof. Putting $u = x^{l^t}$, $v = y^{l^t}$ we have by (1)

$$u^{l^{n-t}}+v^{l^{n-t}} = cz^{l^m}.$$

Obviously $(u, v) = 1$ and $l\nmid u^2-v^2$. Since furthermore $p|u^2-v^2$ and c has no prime divisors of the form $kl^{n-t}+1$, Theorem 2 shows that the congruence (4) holds.

COROLLARY 3. *Suppose the integers x, y, z satisfy* (1) *with $(x, y) = 1$. If c has no prime divisors of the form kl^n+1 and if $l\nmid x$ or $l\nmid y$, then*

(5) $$x^l \equiv x \quad \text{or} \quad y^l \equiv y \pmod{l^{m+n}},$$

respectively. If further $l|x-y$, in addition to these congruences also

$$x \equiv y \pmod{l^{m+n}}$$

holds. If c has no prime divisors of the form $kl+1$, and $l|y$, then even $l^{m+n}|y$, i.e.

$$y^l \equiv y \pmod{l^{m+n}}.$$

Proof. We verify immediately that the corollary is true for the trivial solutions x, y, z of (1).

The first part is clear by Theorem 2.

For $l|x-y$ obviously $l\nmid cxyz$. Therefore, by the preceding case,

$$x^l \equiv x, \quad y^l \equiv y \pmod{l^{m+n}}.$$

Subtracting gives

$$(x-y)((x^l-y^l)/(x-y)-1) \equiv 0 \pmod{l^{m+n}}.$$

But here the quotient is divisible by l and hence $l^{m+n}|(x-y)$.

For the last case we infer that $l\nmid cxz$ and, since the proof for the case $n = 1$ may be found in [4], Cor. 5, we may suppose that $n \geqslant 2$. Clearly,

$$\prod_{s=0}^{n} Q_s(x, y) = cz^{l^m}.$$

Here the divisors of the left product are pairwise relatively prime. Recalling the assumption concerning c and the fact (c), mentioned at the beginning, we

establish that $c|Q_0(x, y) = x+y$. Consequently

$$Q_1(x, y) = \frac{x^l+y^l}{x+y} = b^{l^m}, \tag{6}$$

where $b \equiv 1 \pmod{l}$. But on account of Corollary 2 every prime divisor p of b satisfies (for $n \geqslant 2$) the congruence

$$p^{l-1} \equiv 1 \pmod{l^{m+n-1}},$$

whence $b^l \equiv b \pmod{l^{m+n-1}}$. Now

$$(b-1)((b^l-1)/(b-1)-1) \equiv 0 \pmod{l^{m+n-1}}$$

and $(b^l-1)/(b-1)$ is divisible by l because of (b). Therefore $b \equiv 1 \pmod{l^{m+n-1}}$, so that (6) gives

$$x^l+y^l \equiv x+y \pmod{l^{2m+n-1}}.$$

Since $x^l \equiv x \pmod{l^{m+n}}$, we have from this

$$y^l \equiv y \pmod{l^{m+n}},$$

i.e. $y \equiv 0 \pmod{l^{m+n}}$. This finishes the proof.

COROLLARY 4. *If c has no prime factors of the form kl^n+1 and if* (1) *has a solution in integers x, y, z with $(x, y) = 1$, $l|x-y$, then*

$$c^{l-1} \equiv 2^{l-1} \pmod{l^{m+1}}.$$

Proof. Corollary 3 shows $x \equiv y \pmod{l^{m+n}}$. Hence

$$x^{l^n} \equiv y^{l^n} \pmod{l^{m+2n}},$$

so that from (1)

$$2x^{l^n} \equiv cz^{l^m} \pmod{l^{m+2n}}.$$

Since $l \nmid x$, $x^{l-1} \equiv 1 \pmod{l^{m+n}}$ by Corollary 3. Thus

$$x^{l^n(l-1)} \equiv 1 \pmod{l^{m+2n}}$$

and

$$2^{l-1} \equiv c^{l-1} z^{l^m(l-1)} \pmod{l^{m+2n}}.$$

According to Euler's theorem $z^{l^m(l-1)} \equiv 1 \pmod{l^{m+1}}$ and so we obtain the result required, which, unfortunately, is much weaker than other congruences in our proof.

COROLLARY 5. *Suppose that* (1) *has a solution in integers x, y, z such that $(x, y) = 1$ and $l|y$ (or $l|x$).*

(i) *If c has no prime divisors of the form kl^n+1, then*

$$c^{l-1} \equiv 1 \pmod{l^{m+1}}.$$

(ii) *If c has no prime divisors of the form $kl+1$, then*

$$c^{l-1} \equiv 1 \pmod{l^{m+n}}, \quad z^{l-1} \equiv 1 \pmod{l^n}.$$

Proof. Clearly, $l \nmid cxz(x^2-y^2)$. By Corollary 3,

$$x^{l-1} \equiv 1 \pmod{l^{m+n}}.$$

Thus $x^{l^n(l-1)} \equiv 1 \pmod{l^{m+2n}}$. We deduce from (1)

$$1 \equiv c^{l-1} z^{l^m(l-1)} \pmod{l^{m+2n}}, \tag{7}$$

because $l^{m+1}|y$, by Corollary 3, and $(m+1)l^n \geqslant (m+1)(2n+1) > m+2n$.

(i) Again by Euler's theorem we have from (7)

$$c^{l-1} \equiv 1 \pmod{l^{m+1}}.$$

(ii) Since in this case $c|x+y$, $l \nmid x^2-y^2$, Theorem 2 shows that

$$c^{l-1} \equiv 1 \pmod{l^{m+n}}.$$

From (7) it now follows that

$$z^{l^m(l-1)} \equiv 1 \pmod{l^{m+n}}.$$

But

$$z^{l^m(l-1)}-1 = (z^{l-1}-1) \prod_{s=1}^{m} Q_s(z^{l-1}, -1) \equiv 0 \pmod{l^{m+n}}$$

and, by (b), $l \| Q_s$, so that $l^n|z^{l-1}-1$. This completes the proof.

COROLLARY 6. *If c has no prime factors of the form $kl+1$ and the integers x, y, z satisfy* (1) *with $l \nmid x^2-y^2$ and $(x, y) = 1$, then for every prime factor p of c or of z*

$$p^{l-1} \equiv 1 \pmod{l^{m+n}} \quad \text{or} \quad p^{l-1} \equiv 1 \pmod{l^M},$$

respectively. Here $M = n$ for $m \geqslant n$ and $M = [(m+n+1)/2]$ for $m < n$. Thus

$$c^{l-1} \equiv 1 \pmod{l^{m+n}}, \quad z^{l-1} \equiv 1 \pmod{l^M}.$$

Proof. Clearly, $l \nmid cz$ and $c|x+y$. Using Theorem 2 we infer that the assertions concerning c are valid.

Suppose now $p|z$. Then $p|Q_t(x, y)$ for some t with $0 \leqslant t \leqslant n$. Since $Q_t(x, y)$ is a factor of $x^{l^t}+y^{l^t}$, we see from Corollary 2 that for $t < n$

$$p^{l-1} \equiv 1 \pmod{l^{m+n-t}}.$$

On the other hand p has the form kl^t+1 by (c) so that in addition (for $0 \leqslant t \leqslant n$)

$$p^{l-1} \equiv 1 \pmod{l^t}.$$

(For $t = 0$ this is trivial.) Combining these conditions we obtain for $t < n$

$$p^{l-1} \equiv 1 \pmod{l^{\max\{t, m+n-t\}}}.$$

Now we have surely $p^{l-1} \equiv 1 \pmod{l^M}$, where

$$M = \min\{n, \min\{\max\{t, m+n-t\} \mid 0 \leqslant t < n\}\}$$

or more explicitly $M = n$ or $[(m+n+1)/2]$ according as $m \geqslant n$ or $m < n$. This completes the proof.

Using the Corollaries 1, 4 and 6 we may prove the following theorem.

THEOREM 3. *If the positive constant c satisfies the conditions $(\varphi(c), l) = 1$ (φ the Euler's function) and*

$$c^{l-1} \not\equiv 2^{l-1} \pmod{l^{m+1}}, \tag{8}$$

then the equation (1) *has no solution in integers x, y, z with $(x, y) = 1$ and $l \nmid xyz$.*

Proof. Suppose such a solution exists. It is evident from the assumption $(\varphi(c), l) = 1$ that c contains no prime divisors of the form $kl+1$. Since $l \nmid \varphi(c)$, c must be non-divisible by l, for otherwise $l \| c$ and so, by $l \nmid z$, also $l \| x^{l^n} + y^{l^n}$, which, however, is a contradiction (cf. (a) and (b)).

If now $l \mid x-y$, then according to Corollary 4

$$c^{l-1} \equiv 2^{l-1} \pmod{l^{m+1}}, \tag{9}$$

which contradicts the assumption (8). Thus $l \nmid x-y$ and so also $l \nmid x^2-y^2$. Then, by Corollary 1, $2^{l-1} \equiv 1 \pmod{l^{m+n}}$ and, by Corollary 6, $c^{l-1} \equiv 1 \pmod{l^{m+n}}$. Hence it follows again that (9) holds contrary to the assumption (8). This completes the proof.

The following noteworthy result which has got its definitive form through the intuitive perception of J. M. Gandhi, is an immediate sequel from the preceding theorem.

COROLLARY 7. *If $(\varphi(c), l) = 1$ and $c^{l-1} \not\equiv 2^{l-1} \pmod{l^2}$, then the equation $x^l + y^l = cz^l$ has no solution in integers x, y, z prime to l.*

Proof. We see, as above, that $l \nmid c$, and so $l \nmid cxyz$. Furthermore, we may assume that c contains no divisors of the form a^l $(a > 1)$, because $a^{l(l-1)} \equiv 1 \pmod{l^2}$ and a^l can be absorbed in z^l, without loss of the assumptions in the corollary, in other words, "the new c" fulfills the conditions of the corollary.

In addition we can assume that $(x, y, z) = 1$. Then also $(x, y) = 1$. Now the validity of our corollary follows directly from Theorem 3.

References

[1] T. Azuhata, *On Fermat's last theorem*, Acta Arith. 45 (1984), 19–27.

[2] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. AI, 33 (1946), 1–60.

[3] — *Über die Lösbarkeit einiger Diophantischer Gleichungen*, ibid. 334 (1963), 1–15.

[4] — *On the unsolvability of some diophantine equations of a modified Fermat type*, Mathematika 27 (1980), 179–187.

[5] — *Generalizations of Furtwängler's criteria for Fermat's last theorem and some related results*, preprint, Univ. of Turku, Finland (to appear in Math. Scand.).

[6] E. Landau, *Vorlesungen über Zahlentheorie*, vol. III, Leipzig 1927. Chelsea Publ. Co., New York 1969.

[7] S. Lubelski, *Studien über den grossen Fermatschen Satz*, Prace Mat.-Fiz. 42 (1935), 1–34.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Turku, Finland

Received on 16.4.1987
and in revised form on 28.3.1988 (1720)