For a reducible polynomial $P \in \boldsymbol{Z}[x, y]$, we first factorize it into irreducible polynomials, and obtain a lower estimate as above for each of their values. Using these estimates and Gel'fond's Lemma, we obtain the desired lower estimate for $|P(\omega, \omega_1)|$. This completes the proof of the theorem.

Acknowledgement. The author would like to express his gratitude to the referee for his valuable comments.

References

[1] P.-G. Becker-Landeck, *Transcendence measure by Mahler's transcendence method*, Bull. Austral. Math. Soc. 33 (1986), 59–65.

[2] P.-G. Becker and K. Nishioka, *Measures for the algebraic independence of the values of Mahler type functions*, C.R. Math. Rep. Acad. Sci. Canada 11 (1989), 89–93.

[3] G. V. Chudnovsky, *Contributions to the Theory of Transcendental Numbers*, Math. Surveys Monographs, no. 19, Providence, R.I., 1984.

[4] G. Diaz, *Grands degrés de transcendance pour des familles d'exponentielles*, J. Number Theory 31 (1989), 1–23.

[5] A. I. Galochkin, *Transcendence measure of values of functions satisfying certain functional equations*, Mat. Zametki 27 (1980); English transl. in Math. Notes 27 (1980), 83–88.

[6] K. K. Kubota, *On the algebraic independence of holomorphic solutions of certain functional equations and their values*, Math. Ann. 227 (1977), 9–50.

[7] J. H. Loxton and A. J. van der Poorten, *Arithmetic properties of certain functions in several variables II*, J. Austral. Math. Soc. Ser. A 24 (1977), 393–408.

[8] —,—, *Algebraic independence properties of the Fredholm series*, ibid. 26 (1978), 31–45.

[9] K. Mahler, *Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen*, Math. Z. 32 (1930), 545–585.

[10] W. Miller, *Transcendence measures by a method of Mahler*, J. Austral. Math. Soc. Ser. A 32 (1982), 68–78.

[11] Yu. V. Nesterenko, *On algebraic independence of algebraic powers of algebraic numbers*, Mat. Sb. 123 (165) (1984); English transl. in Math. USSR-Sb. 51 (1985), 429–454.

[12] —, *On a measure of the algebraic independence of the values of certain functions*, Mat. Sb. 128 (170) (1985); English transl. in Math. USSR-Sb. 56 (1987), 545–567.

[13] K. Nishioka, *On an estimate for the orders of zeros of Mahler type functions*, Acta Arith. 56 (1990), 249–256.

[14] —, *New approach in Mahler's method*, to appear in J. Reine Angew. Math.

[15] —, *Algebraic independence measures of the values of Mahler functions*, to appear.

[16] P. Philippon, *Critères pour l'indépendance algébrique*, Publ. IHES 64 (1986), 5–52.

[17] V. G. Sprindžuk, *Achievements and problems in Diophantine approximation theory*, Uspekhi Mat. Nauk 35 (1980); English transl. in Russian Math. Surveys 35(4) (1980), 1–80.

[18] M. Waldschmidt, *Nombres Transcendants*, Lecture Notes in Math. 402, Springer, Berlin 1974.

DEPARTMENT OF MATHEMATICS
GUMMA UNIVERSITY
Aramaki-cho 4, Maebashi 371
Japan

Received on 23.3.1990
and in revised form on 24.9.1990 (2021)

ACTA ARITHMETICA
LIX.1 (1991)

On Fermat's equation with prime power exponents

by

CUI-XIANG ZHONG (Vancouver, B.C.)

1. Introduction. There are many important and interesting results for the general equation

$$x^{p^n} + y^{p^n} + z^{p^n} = 0.$$

One is the following: In 1933, using the method of singular integers, Moriya [5] extended the theorem of Furtwängler to the Fermat equation with power exponent p^n to show that:

Suppose that the equation $x^{p^n} + y^{p^n} + z^{p^n} = 0$ with $n \geqslant 1$ and p an odd prime has a non-trivial solution x, y, z such that some integer r satisfies one of the following conditions: (i) $r|x$, $p \nmid x$, (ii) $r|x-y$, $p \nmid x^2 - y^2$. *Then* $r^{p-1} \equiv 1 \pmod{p^{n+1}}$.

Again with the same method, Inkeri [2] proved the following generalization of a theorem due to Vandiver [8]:

With the same assumption as in the last theorem,

$$x^p \equiv x \pmod p, \quad y^p \equiv y \pmod p, \quad z^p \equiv z \pmod p.$$

However, this is far from perfect. The author will improve this result in the next section by making use of the recent result of Azuhata [1] of Science University of Tokyo who proved in 1984 that:

If p is an odd prime and there exist pairwise relatively prime integers x, y, z satisfying one of the following conditions: (i) $r|x$, $p \nmid x$, (ii) $r|x-y$, $p \nmid x^2 - y^2$, (iii) $r|x^2 - yz$, $p \nmid xy + yz + zx$, (iv) $r|x^2 + yz$, $p \nmid x(y-z)(x^2+yz)$, *then*

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

This is a considerable generalization of Moriya's theorem. The result of the author is the following

THEOREM. *If p is an odd prime and there are relatively prime integers x, y, z satisfying $x^{p^n} + y^{p^n} + z^{p^n} = 0$, then*

$$x^p \equiv x \pmod{p^{3n}}, \quad y^p \equiv y \pmod{p^{3n}}, \quad z^p \equiv z \pmod{p^{3n}},$$

and $x + y + z \equiv 0 \ (p^{3n})$. Moreover, if $p|z$ then $p^{3n}|z$.

Furthermore, this result can be used as a key to give a series of important estimates on the variables x, y, z such that $x^{p^n}+y^{p^n}=z^{p^n}$. These estimates can be summarized in the following corollaries that are proved in another paper of the author:

COROLLARY 1. *If p is an odd prime, $0<x<y<z$ are relatively prime integers, $p\nmid xyz$ and $x^{p^n}+y^{p^n}=z^{p^n}$, then*

$$x>\left(\frac{2p^{3n}+p^n}{\log(3p^n)}\right)^{p^n} \quad \text{and} \quad z-x>4^{p^n}p^{2np^n}.$$

COROLLARY 2. *If p is an odd prime and there exist pairwise relatively prime integers x, y, z such that $0<x<y<z$, $p|xyz$ and $x^{p^n}+y^{p^n}=z^{p^n}$, then*

$$x>p^{3np^n-4n}, \quad y>\tfrac{1}{2}p^{3np^n-n}, \quad z-x>\tfrac{1}{4}p^{3np^n-n-1}.$$

COROLLARY 3. *Let $M>0$ be a given real number, p an odd prime and $0<x<y<z$ relatively prime integers satisfying $x^{p^n}+y^{p^n}=z^{p^n}$. If*

$$y-x<M(z-x)^{1-1/\sqrt{p^n}}$$

then

$$p\leqslant\sqrt{\tfrac{1}{4}(\log M)^2}.$$

In fact, these estimates are generalizations of some important estimates for x, y, z satisfying $x^p+y^p=z^p$, obtained by Inkeri [3], van der Poorten [4], Stewart [7], and others.

2. Proof of the theorem. We divide the proof into two cases:

(a) If $p\nmid xyz$ then under the assumption of the theorem,

$$x^{p^n}+y^{p^n}=(x+y)Q_p(x,y)Q_p(x^p,y^p)\dots Q_p(x^{p^{n-1}},y^{p^{n-1}})$$

where $Q_p(x,y)=(x^p+y^p)/(x+y)$. Since $p\nmid xyz$, we have

$$(1)\qquad \begin{aligned}(x+y,\,Q_p(x,y))&=(x^p+y^p,\,Q_p(x^p,y^p))=\dots\\&=(x^{p^{n-1}}+y^{p^{n-1}},\,Q_p(x^{p^{n-1}},y^{p^{n-1}}))=1\end{aligned}$$

and so

$$x+y=t^{p^n},\quad Q_p(x,y)=t_1^{p^n},\quad Q_p(x^p,y^p)=t_2^{p^n},\quad\dots,\quad Q_p(x^{p^{n-1}},y^{p^{n-1}})=-t_n^{p^n}$$

for some integers $t, t_1, t_2, \dots, t_n$. From (1) it follows that if q is a prime with $q|t_1t_2\dots t_n$ then $q\equiv 1 \pmod p$. Since $q^{p-1}\equiv 1 \pmod{p^{2n}}$ by Azuhata's theorem, we have $q^p\equiv q \pmod{p^{2n}}$ and so

$$q\equiv q^p\equiv 1 \pmod{p^2},\quad\dots,\quad q\equiv q^{p^n}\equiv 1 \pmod{p^{2n}}.$$

That is, every prime factor q of any integer among $t_1, t_2, \dots, t_n$ is congruent to 1 modulo p^{2n}. Similarly, we can prove that

$$z+x=s^{p^n},\quad Q_p(z,x)=s_1^{p^n},\quad Q_p(z^p,x^p)=s_2^{p^n},\quad\dots,\quad Q_p(z^{p^{n-1}},x^{p^{n-1}})=-s_n^{p^n},$$

and

$$z+y=r^{p^n},\quad Q_p(z,y)=r_1^{p^n},\quad Q_p(z^p,y^p)=r_2^{p^n},\quad\dots,\quad Q_p(z^{p^{n-1}},y^{p^{n-1}})=-r_n^{p^n},$$

and moreover if q is a prime and $q|ss_1\dots s_nrr_1r_2\dots r_n$ then we also have $q\equiv 1 \pmod{p^{2n}}$. Hence

$$\begin{aligned}x&=-rr_1\dots r_n\equiv -r \pmod{p^{2n}},\\ y&=-ss_1\dots s_n\equiv -s \pmod{p^{2n}},\\ z&=-tt_1\dots t_n\equiv -t \pmod{p^{2n}},\end{aligned}$$

and so

$$x^{p^n}+y^{p^n}+z^{p^n}\equiv -(r^{p^n}+s^{p^n}+t^{p^n})\equiv 0 \pmod{p^{3n}}.$$

Again

$$\begin{aligned}x&=(-r^{p^n}+s^{p^n}+t^{p^n})/2\equiv -r^{p^n} \pmod{p^{3n}},\\ y&=(r^{p^n}-s^{p^n}+t^{p^n})/2\equiv -s^{p^n} \pmod{p^{3n}},\\ z&=(r^{p^n}+s^{p^n}-t^{p^n})/2\equiv -t^{p^n} \pmod{p^{3n}},\\ x^p&=[-(rr_1)^{p^n}+(ss_1)^{p^n}+(tt_1)^{p^n}]/2\equiv -r^{p^n} \pmod{p^{3n}},\\ y^p&=[(rr_1)^{p^n}-(ss_1)^{p^n}+(tt_1)^{p^n}]/2\equiv -s^{p^n} \pmod{p^{3n}},\\ z^p&=[(rr_1)^{p^n}+(ss_1)^{p^n}-(tt_1)^{p^n}]/2\equiv -t^{p^n} \pmod{p^{3n}}.\end{aligned}$$

Combining the last two groups of congruences, we obtain the conclusion of the theorem.

(b) If $p|xyz$, there is no loss of generality in assuming that $p|z$. Under the assumption of the theorem, we have

$$\begin{aligned}&x+y=p^{mp^n-n}t^{p^n}, && Q_p(x,y)=pt_1^{p^n}, && \dots, && Q_p(x^{p^{n-1}},y^{p^{n-1}})=-pt_n^{p^n};\\ &z+x=s^{p^n}, && Q_p(z,x)=s_1^{p^n}, && \dots, && Q_p(z^{p^{n-1}},x^{p^{n-1}})=-s_n^{p^n};\\ &y+z=r^{p^n}, && Q_p(z,y)=r_1^{p^n}, && \dots, && Q_p(z^{p^{n-1}},y^{p^{n-1}})=-r_n^{p^n}.\end{aligned}$$

With the same method as in (a), we can prove that if q is a prime and $q|ss_1\dots s_nrr_1\dots r_n$, then $q\equiv 1 \pmod{p^{2n}}$. Hence we have

$$x=-rr_1\dots r_n\equiv -r \pmod{p^{2n}},\quad y=-ss_1\dots s_n\equiv -s \pmod{p^{2n}},$$

and so

$$x^{p^n}+y^{p^n}+z^{p^n}\equiv -(r^{p^n}+s^{p^n})\equiv 0 \pmod{p^{3n}}.$$

Again since

$$\begin{aligned}x&=(-r^{p^n}+s^{p^n}+p^{mp^n-n}t^{p^n})/2\equiv -r^{p^n} \pmod{p^{3n}},\\ y&=(r^{p^n}-s^{p^n}+p^{mp^n-n}t^{p^n})/2\equiv -s^{p^n} \pmod{p^{3n}}\end{aligned}$$

and

$$x^p = [-(rr_1)^{p^n} + (ss_1)^{p^n} + p^{mp^n - n + 1}(tt_1)^{p^n}]/2 \equiv -r^{p^n} \pmod{p^{3n}},$$

$$y^p = [(rr_1)^{p_n} - (ss_1)^{p^n} + p^{mp^n - n + 1}(tt_1)^{p^n}]/2 \equiv -s^{p^n} \pmod{p^{3n}},$$

so we obtain

$$x^p \equiv x \pmod{p^{3n}}, \quad y^p \equiv y \pmod{p^{3n}}.$$

Noticing that

$$z = (r^{p^n} + s^{p^n} - p^{mp^n - n} t^{p^n})/2 \equiv 0 \pmod{p^{3n}},$$

we also have

$$z^p \equiv z \pmod{p^{3n}}.$$

That completes the proof of the theorem.

References

[1] T. Azuhata, *On Fermat's Last Theorem*, Acta Arith. 45 (1985), 19–27.

[2] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. AI, 1946, No. 33, 60 pages.

[3] –, *Abschätzungen für eventuelle Lösungen der Gleichung in Fermatschen Problem*, Ann. Univ. Turku, Ser. A 1 (1953), 3–9.

[4] K. Inkeri and A. J. van der Poorten, *Some remarks on Fermat's conjecture*, Acta Arith. 36 (1980), 107–111.

[5] M. Moriya, *Über die Fermatsche Vermutung*, J. Reine Angew. Math. 169 (1933), 92–97.

[6] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, 1978, 225–240.

[7] C. C. Stewart, *A note on the Fermat equation*, Mathematika 224 (1977), 130–132.

[8] H. S. Vandiver, *A property of cyclotomic integers and its relation to Fermat's Last Theorem*, Ann. of Math. 21 (1919), 73–80.

MATHEMATICS DEPARTMENT
THE UNIVERSITY OF BRITISH COLUMBIA
121–1984 Mathematics Road
Vancouver, B.C.
Canada, V6T 1Y4

Received on 2.5.1990
and in revised form on 21.8.1990 (2036)

ACTA ARITHMETICA
LIX.1 (1991)

Arcs containing no three lattice points

by

JAVIER CILLERUELO (Madrid)

1. Introduction. In [1], A. Córdoba and myself developed a method to study the location of lattice points on circles centered at the origin. There we proved the following theorem:

THEOREM A. *On a circle of radius R centered at the origin, an arc whose length is not greater than*

$$\sqrt{2}R^{1/2 - 1/(4[m/2]+2)}$$

contains at most m lattice points.

We could not decide whether the exponent

$$\frac{1}{2} - \frac{1}{4[m/2]+2}$$

is sharp for each m. In particular, we do not know if the number of lattice points on arcs of length $R^{1/2}$ is bounded uniformly in R or not. Probably it is not.

Obviously, Theorem A is sharp for $m = 1$. The case $m = 2$ was first proved by A. Schinzel and used by Zygmund [2] to prove a Cantor–Lebesgue theorem in two variables.

It is not too hard to prove that the exponent 1/3 cannot be improved.

In this paper we get the best constant C, such that an arc of length $CR^{1/3}$ cannot contain three lattice points.

THEOREM 1. (i) *On a circle of radius R centered at the origin, an arc whose length is not greater than $2\sqrt[3]{2}R^{1/3}$ contains at most two lattice points.*

(ii) *For every $\varepsilon > 0$, there exist infinitely many circles $x^2 + y^2 = R_n^2$ with arcs of length $2\sqrt[3]{2}R_n^{1/3} + \varepsilon$ containing three lattice points.*

2. Preliminary lemma and notation. Let us denote by $r(n)$ the number of representations of the integer n as a sum of two squares, i.e. $r(n)$ is the number of lattice points on the circle $x^2 + y^2 = n$. Therefore we shall associate lattice points with Gaussian integers: $a^2 + b^2 = n$ determines a Gaussian integer