Finite Fields and Their Applications **7,** 189–196 (2001)
doi.10.1006/ffta.2000.0316, available online at http://www.idealibrary.com on IDEAL®

On Diagonal Equations over Finite Fields*

JiaGui Luo and Qi Sun

Department of Mathematics, Sichuan University, Chengdu 610064, People's Republic of China

Communicated by Peter Jan-Shyong Shiue

Received October 12, 1999; revised August 31, 2000

DEDICATED TO PROFESSOR CHAO KO ON THE OCCASION OF HIS 90TH BIRTHDAY

In this paper, we obtain a sufficient condition for the diagonal equation to have only the trivial solution over finite fields. This result improves a theorem of Sun (*J. Sichuan Normal Univ. Nat. Sci. Ed.* **26** (1989), 55–59) greatly and proves that the conjecture posed by Powell (*J. Number Theory* **18** (1984), 34–40) holds for general $n \in N$ as well. © 2000 Academic Press

1. INTRODUCTION

Let Z, N, Q denote the sets of integers, positive integers, and rational numbers respectively.

The diagonal equation

$$a_1 x_1^d + a_2 x_2^d + \cdots + a_n x_n^d = 0 \quad d, n \in N, a_j \in Z$$

$$a_j \neq 0, j = 1, 2, \ldots, n, \tag{1}$$

have been investigated in many papers.

In 1954, Ankeny and Erdös [1] proved that Eq. (1) is almost always unsolvable provided that all distinct subsets of the set of number $\{a_1, a_2, \ldots, a_n\}$ have different sums.

In 1992, Granville [2] obtained fairly general results in this direction.

For the general Fermat equation

$$ax^d + by^d = cz^d, \tag{2}$$

*This project was supported by the National Natural Science Foundation of China.

1071-5797/00 $35.00

where $a, b, c \in Z$ with $abc(a \pm b)(a \pm c)(b \pm c)(a \pm b \pm c) \neq 0$, Powell [4] suggested the following.

Conjecture. Let $m \in N$ be a given even integer. If $d \in N$ is sufficiently large for which $md + 1 = p$ with p being a prime, equation (2) has no integral solution $xyz \neq 0$.

Qi Sun [5] and Granville [3] proved the conjecture.

In [1], Ankeny and Erdös obtained a slightly weaker version of the generalized Powell conjecture, i.e.,

THEOREM 1 (Ankeny and Erdös). *If $a_1, a_2, \ldots, a_n$ satisfy the condition*

(3) *For every selection of $\varepsilon_j = 0$ or $\pm 1 (j = 1, 2, \ldots, n)$, except $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = (0, 0, \ldots, 0)$, we have $\sum_{j=1}^{n} a_j \varepsilon_j \neq 0$.*

Then for a given d there exist no nontrivial solutions of (1) *provided we can find a rational prime p such that*

$$d \mid p - 1, \quad md = p - 1, \ 4 \nmid m$$

$$\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p}.$$

In [2], Granville gave the following two propositions.

PROPOSITION 1. *For any polynomial*

$$f(X_1, X_2, \ldots, X_n) = \sum_{j=1}^{r} a_i X_1^{e_{i,1}} X_2^{e_{i,2}} \cdots x_n^{e_{i,n}},$$

where each a_i is a nonzero integer, and each $e_{i,j}$ is a nonnegative integer, there exists a finite set of integers $B(f)$ with the following property: If m is a positive integer that is not divisible by any element of $B(f)$, then the Diophantine equation $f(x_1^d, \ldots, x_n^d) = 0$ has no solutions in nonzero integers $x_1, \ldots, x_n$, whenever $q = md + 1$ is a sufficiently large prime.

PROPOSITION 2. *For any polynomial f as in Proposition* 1, *there exists a finite set of integers $B(f)$ with the following property: There exist mth roots of unity $\xi_1, \xi_2, \ldots, \xi_n$ satisfying $f(\xi_1, \xi_2, \ldots, \xi_n) = 0$ if and only if m is divisible by some elements of $B(f)$.*

In 1989, *Qi Sun* [5] *obtained the following result.*

THEOREM 2. *Let $m \in N, m > 2, d = (p^f - 1)/m$, where p is a prime, and $f = \operatorname{ord}_m p (\operatorname{ord}_m p$ be the smallest positive integer f with $p^f \equiv 1 (\operatorname{mod} m)$). If $a_1, a_2, \ldots, a_n$ satisfy condition* (3),

(4) $\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p^f}$, *where $\varphi(m)$ is the Euler function,*

(5) $A_0 + A_1\xi + \cdots + A_{m-1}\xi^{m-1} \neq 0$, *where* $A_j = \sum_{k\in s_j} a_k$ $(j = 0, \ldots, m-1)$, *and* s_j *is a* (*possibly void*) *subset of the set of numbers* $\{1, 2, \ldots, n\}$, *and* $\xi = e^{2\pi i/m}$, *then Eq.* (1) *has no integral solutions except* $x_j = 0, j = 1, \ldots, n$.

In this paper, we improve Theorem 1 by removing Condition $4 \dagger m$ and so prove that the conjecture posed by Powell holds for general $n \in N$ as well. We also improve the result of [6] greatly by removing condition (5). Our main results are the following.

THEOREM 3. *Let* $m \in N, m > 1$, $d = (p^f - 1)/m$, *where* p *is a prime*, $f = \mathrm{ord}_m p$. *If* $a_1, a_2, \ldots, a_n$ *satisfy* (3) *and* (4), *then Eq.* (1) *has no nonzero solutions over the finite field* F_q, *where* $q = p^f$.

COROLLARY 1. *Let the hypothesis be as in Theorem* 3. *Then Eq.* (1) *has only the trivial integral solution* $x_j = 0, j = 1, 2, \ldots, n$.

COROLLARY 2. *Let* $m \in N$, $m > 1$, $md + 1 = p$ *with* p *being a prime. If* $a_1, a_2, \ldots, a_n$ *satisfy* (3) *and*

(6) $d > [(\sum_{j=1}^{n} |a_j|)^{\varphi(m)} - 1]/m$,

then Eq. (1) *has no integral solutions except* $x_j = 0, j = 1, 2, \ldots, n$.

2. LEMMA

In order to prove the results, we need the following.

LEMMA. *Let* $a_1, a_2, \ldots, a_n$ *satisfy* (3). *Then for any nonnegative integers* $k_1, k_2, \ldots, k_n$, *we have*

$$\sum_{j=1}^{n} a_j \xi_m^{k_j} \neq 0, \tag{7}$$

where $m \in N, m > 1, \xi_m = e^{2\pi i/m}$.

Proof. When $4 \dagger m$, the result has been proved by Ankeny and Erdös [1]. Now assume that $4 | m$. The proof is by induction on n. If $n = 1$, the result is clearly true.

Suppose now that $n > 1$ and that we have proved the result for all positive integers less than n. The assumption that (7) is false leads to a relation

$$\sum_{j=1}^{n} a_j \xi_m^{k_j} = 0. \tag{8}$$

By the inductive hypothesis we must have that $k_1, k_2, \ldots, k_n$ are distinct. Without the loss of generality we may assume $k_1 > k_2 > \cdots > k_n$. Let

$u_j = k_j - k_n > 0$, $j = 1, 2, \ldots, n-1$. We get from (8) that

$$\sum_{j=1}^{n-1} a_j \xi_m^{u_j} + a_n = 0. \tag{9}$$

Let m_1 be the product of all distinct prime divisors of m and $m = m_1 m_2$. Write $u_j = t_j m_2 + s_j$, $0 \le s_j < m_2$, $j = 1, 2, \ldots, n-1$. Replace u_j by $t_j m_2 + s_j$ in (9), then

$$\sum_{j=1}^{n-1} a_j \xi_{m_1}^{t_j} \xi_m^{s_j} + a_n = 0. \tag{10}$$

We claim that $s_j = 0$, $j = 1, 2, \ldots, n-1$. Otherwise, we may assume that $s_1 = s_2 = \cdots = s_v = 0$, $s_j \neq 0$, $v < j \le n-1$, where $0 \le v \le n-2$. Since $m_2 \varphi(m_1) = \varphi(m) = [Q(\xi_m) : Q] = [Q(\xi_m) : Q(\xi_{m_1})] \varphi(m_1)$, we have $[Q(\xi_m) : Q(\xi_{m_1})] = m_2$. It follows that $1, \xi_m, \ldots, \xi_m^{m_2 - 1}$ are linearly independent over $Q(\xi_{m_1})$. We find from (10) that $\sum_{j=1}^{v} a_j \xi_{m_1}^{t_j} + a_n = \sum_{j=1}^{v} a_j \xi_m^{m_2 t_j} + a_n = 0$. But since $v + 1 < n$, by the induction hypothesis, $\sum_{j=1}^{v} a_j \xi_m^{m_2 t_j} + a_n \neq 0$, is a contradiction. Thus $s_j = 0$, $j = 1, 2, \ldots, n-1$. We get from (10) that

$$\sum_{j=1}^{n-1} a_j \xi_{m_1}^{t_j} + a_n = 0. \tag{11}$$

Obviously, $t_1, t_2, \ldots, t_{n-1}$ are not all zero under the assumption of the lemma.

If $m_1 = 2$, we find from (11) that $\sum_{j=1}^{n-1} a_j (-1)^{t_j} + a_n = 0$ which is impossible.

If $m_1 \neq 2$, we claim that there is at least one of the odd prime divisors of m_1, say p, such that $t_1, t_2, \ldots, t_{n-1}$ are not all divisible by p. Otherwise, $(m_1/2) \mid t_j$, $j = 1, 2, \ldots, n-1$. Then we find from (11) that $\sum_{j=1}^{n-1} (-1)^{2t_j/m_1} a_j + a_n = 0$, which is impossible. Since $\xi' = \xi_{m_1/p} \xi_p = \xi_{m_1}^{p + (m_1/p)}$ and $(p + m_1/p, m_1) = 1$, ξ' is also a primitive m_1th root of unity. We get from (11) that

$$\sum_{j=1}^{p-1} b_j \xi_p^j = 0,$$

where $b_0 = \sum_{k \in s_0} a_k \xi_{m_1/p}^{[t_k/p]} + a_n$ and $b_j = \sum_{k \in s_j} a_k \xi_{m_1/p}^{[t_k/p]}$, $(j = 1, \ldots, p-1)$, and s_j is a (possibly void) subset of the set of numbers $\{1, 2, \ldots, n-1\}$ such that $\bigcup_{j=0}^{p-1} s_j = \{1, 2, \ldots, n-1\}$. Since $t_1, t_2, \ldots, t_{n-1}$ are not all divisible by p, there is a $j (\neq 0)$ such that $b_j \neq 0$. And by the inductive hypothesis, for every $1 \le i \neq j \le p-1$, $b_i \neq b_j$. On the other hand, since $(p-1)\varphi(m_1/p) = \varphi(m_1) = [Q(\xi_{m_1/p}, \xi_p) : Q] = [Q(\xi_{m_1/p}, \xi_p) : Q(\xi_{m_1/p})] \varphi(m_1/p)$, we have $[Q(\xi_{m_1/p}, \xi_p) : Q(\xi_{m_1/p})] = p-1$. It follows that $x^{p-1} + \cdots + x + 1$ is the monic irreducible

polynomial for ξ_p over $Q(\xi_{m_1/p})$. Thus $b_0 = b_1 = b_2 = \cdots = b_{p-1}$ is a contradiction. Therefore $\sum_{j=1}^{n} a_j \xi_m^{k_j} \neq 0$. This establishes the lemma.

3. PROOFS

The proof of Theorem 3 is as follows. Let D_m be the ring of integers of cyclotomic field $Q(\xi_m)$, $P \subseteq D_m$ be a prime ideal containing p. By the knowledge of cyclotomic field, we know that $D_m/P = F_q$, where $q = p^f$. Let G be the galois group of $Q(\xi_m)/Q$. It is well known that $|G| = \varphi(m)$, $\Pi_{\sigma \in G} \sigma(P) = (N(P)) = (p^f)$. Assume that Eq. (1) has a nonzero solution over F_q. Let $x_j = u_j$, $j = 1, 2, \ldots, n$, be a nonzero solution. We may assume that $x_{i_j} = u_{i_j} \in F_q^*$, $j = 1, 2, \ldots, s$, $1 \leq s \leq n$, where F_q^* is the multiplicative group of F_q. Then

$$u_{i_j}^d \equiv u_{i_j}^{(p^f - 1)/m} \equiv \left(\frac{u_{i_j}}{P}\right)_m \equiv \xi_m^{k_{i_j}} (\mathrm{mod}\, P),\ k_{i_j} \geq 0,\ j = 1, 2, \ldots, s.$$

Reducing (1) modulo P gives

$$\sum_{j=1}^{s} a_{i_j} \xi_m^{k_{i_j}} \equiv 0 (\mathrm{mod}\, P).$$

Then

$$\Pi_{\sigma \in G} \left(\sum_{j=1}^{s} a_{i_j} \sigma(\xi_m)^{k_{i_j}} \right) \equiv 0 (\mathrm{mod}\, p^f). \tag{12}$$

By the lemma, $\sum_{j=1}^{s} a_{i_j} \xi_m^{k_{i_j}}$ is a nonzero algebraic integer. Therefore, $\Pi_{\sigma \in G} (\sum_{j=1}^{s} a_{i_j} \sigma(\xi_m)^{k_{i_j}}) = N(\sum_{j=1}^{s} a_{i_j} \xi_m^{k_{i_j}})$ is a nonzero rational integer. We find from (12) that $p^f \leq |\Pi_{\sigma \in G} (\sum_{j=1}^{s} a_{i_j} \sigma(\xi_m)^{k_{i_j}})| \leq \Pi_{\sigma \in G} (\sum_{j=1}^{s} |a_{i_j}|) \leq (\sum_{j=1}^{n} |a_j|)^{\varphi(m)}$, which is impossible because $\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p^f}$. This completes the proof of Theorem 3. ■

Proof of Corollary 1. Suppose $x_j = u_j \in Z$, $j = 1, 2, \ldots, n$, not all zero, is a solution of Eq. (1). Without the loss of generality, we may assume $(u_1, u_2, \ldots, u_n) = 1$. Then there exists at least one of $u_1, u_2, \ldots, u_n$ not to be divisible by p. Let $x_{i_j} = u_{i_j} \in F_p^* \subseteq F_q$, $j = 1, 2, \ldots, s$, $1 \leq s \leq n$. It follows that $x_j = u_j$, $j = 1, 2, \ldots, n$ is a nonzero solution of Eq. (1) over F_q, which

contradicts with the result of Theorem 3. This completes the proof of Corollary 1. ■

Corollary 2 is an immediate consequence of Corollary 1.

4. APPLICATIONS

In this section, we give examples of applications of the results.

First, for any given positive integer n greater than 2, it is not hard to prove that there are nonzero integers $a_1, a_2, \dots, a_n$ such that

$$\sum_{k=1}^{j-1} |a_k| < |a_j|, \quad 2 \le j \le n. \tag{13}$$

It is easy to see that $a_1, \dots, a_n$ satisfy (3). For a given positive integer m greater than 1 and nonzero integers $a_1, \dots, a_n$, which satisfy inequality (13), how can one find a positive integer d sufficiently large enough for which $md + 1 = p^f$, p a prime, and $f = \mathrm{ord}_m p$ such that $\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p^f}$? We now give some examples.

1. $m = 4$. Since there are infinitely many primes of the form $4d + 1$, we can always find a sufficiently large prime $p = 4d + 1$ so that

$$\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p^f} = \sqrt{p},$$

where $\varphi(m) = 2$, $f = \mathrm{ord}_m p = \mathrm{ord}_m 1 = 1$. Thus the equation

$$\sum_{j=1}^{n} a_j x_j^d = 0$$

has only the trivial integral solutions $x_j = 0$, $j = 1, 2, \dots, n$.

The equation

$$\pm x_1^{16384} \pm 2x_2^{16384} \pm 4x_3^{16384} \pm 8x_4^{16384} \pm 16x_5^{16384} \pm 32x_6^{16384}$$

$$\pm 64x_7^{16384} \pm 128x_8^{16384} = 0,$$

in particular, has only the trivial integral solutions $x_j = 0$, $j = 1, 2, \dots, 8$, where $p = 65537$.

2. $m = 10$. We can always find a sufficiently large prime p of the form $10r + 7$ so that

$$\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p^f} = p,$$

where $\varphi(m) = 4, f = \operatorname{ord}_m p = \operatorname{ord}_m 7 = 4$. Thus the equation

$$\sum_{j=1}^{n} a_j x_j^d = 0, \text{ where } d = (p^f - 1)/m,$$

has only the trivial integral solutions $x_j = 0, j = 1, 2, \ldots, n$.

The equation

$$\pm x_1^{5728976} \pm 3x_2^{5728976} \pm 5x_3^{5728976} \pm 10x_4^{5728976} \pm 22x_5^{5728976} \pm 45x_6^{5728976} = 0,$$

in particular, has only the trivial integral solutions $x_j = 0, j = 1, \ldots, 6$, where $p = 87$.

3. $m = 15$. We can always find a sufficiently large prime p of the form $15r + 2$ so that

$$\sum_{j=1}^{n} |a_j| < \sqrt[\varphi(m)]{p^f} = \sqrt{p},$$

where $\varphi(m) = 8, f = \operatorname{ord}_m p = \operatorname{ord}_m 2 = 4$. Thus the equation

$$\sum_{j=1}^{n} a_j x_j^d = 0, \text{ where } d = (p^f - 1)/m$$

has only the trivial integral solutions $x_j = 0, j = 1, \ldots, n$.

The equation

$$\pm x_1^{23485024} \pm 3x_2^{23485024} \pm 7x_3^{23485024} = 0,$$

in particular, has only the trivial integral solutions $x_1 = x_2 = x_3 = 0$, where $p = 137$.

ACKNOWLEDGMENT

The authors thank the referee for his valuable suggestions, especially, for pointing out references [1] and [2].

REFERENCES

1. N. C. Ankeny and P. Erdös, The insolubility of classes of Diophantine equations, *Amer. J. Math.* **76** (1954), 488–496.
2. A. Granville, Finding integers for k for which a given Diophantine equation has no solutions in kth powers of integers, *Acta Arith.* **60**, No. 3 (1992), 203–212.
3. A. Granville, "Diophantine Equations with Varying Exponent" Ph.D. thesis, Queen's University Kingston, 1987.
4. B. Powell, Proof of the impossibility of the Fermat equation $X^p + Y^p = Z^p$ for special values of p and of the more general equation $bX^n + cY^n = dZ^n$, *J. Number Theory* **18** (1984), 34–40.
5. Qi Sun, On a conjecture posed by Powell, *J. Sichuan Normal Univ. Nat. Sci. Ed.* **31** (1994), 145–147.
6. Qi Sun, On the Diophantine equation $a_1 x_1^d + \cdots + a_n x_n^d = 0$, *J. Sichuan Normal Univ. Nat. Sci. Ed.*, **26** (1989), 55–59.