PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 100, Number 2, June 1987

# ON THE SOLVABILITY OF THE EQUATION $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$ AND ITS APPLICATION

SUN QI AND WAN DAQING

ABSTRACT. In this paper, we obtain a necessary and sufficient condition under which the equation of the title is unsolvable. More precisely, for the equation

$$\frac{x_1}{d_1} + \frac{x_2}{d_2} + \cdots + \frac{x_n}{d_n} \equiv 0 \pmod 1, \qquad x_i \text{ integral}, 1 \le x_i < d_i \ (1 \le i \le n),$$

where $d_1, \ldots, d_n$ are fixed positive integers, we prove the following result: The above equation is unsolvable if and only if

1. For some $d_i$, $(d_i, d_1 d_2 \cdots d_n/d_i) = 1$, or

2. If $d_{i_1}, \ldots, d_{i_k}$ $(1 \le i < \cdots < i_k \le n)$ is the set of all even integers among $\{d_1, \ldots, d_n\}$, then $2 \nmid k, d_{i_1}/2, \ldots, d_{i_k}/2$ are pairwise prime, and $d_{i_j}$ is prime to any odd number in $\{d_1, \ldots, d_n\}$ $(j = 1, \ldots, k)$.

**1. Introduction.** Let $d_1, \ldots, d_n$ be fixed positive integers. It is well known that the solvability and the number $I(d_1, \ldots, d_n)$ of solutions of the equation

$$\frac{x_1}{d_1} + \frac{x_2}{d_2} + \cdots + \frac{x_n}{d_n} \equiv 0 \pmod 1, \qquad x_j \text{ integers}, 1 \le x_j < d_j \ (j = 1, \ldots, n), \tag{1}$$

play an important role in the study of diagonal equations over finite fields. In fact, if $N$ denotes the number of solutions of the equation

$$\sum_{i=1}^{n} a_i x_i^{d_i} = 0, \quad \text{where } d_i | q - 1 \ (i = 1, \ldots, n) \tag{2}$$

over a finite field $F_q$, then (see [3, 291; 4, 169])

$$|N - q^{n-1}| \le I(d_1, \ldots, d_n)(q-1)q^{(n-2)/2}. \tag{3}$$

Note that the number $I(d_1, \ldots, d_n)$ can also be interpreted as the degree of the numerator of the zeta-function of

$$f = \sum_{i=1}^{n} a_i x_i^{d_i}.$$

Hence, the value of $I(d_1, \ldots, d_n)$ heavily affects the estimate of the number $N$ of solutions of the equation (2).

A trivial upper bound of $I(d_1, \ldots, d_n)$ is given by

$$I(d_1, \ldots, d_n) \le (d_1 - 1)(d_2 - 1) \cdots (d_n - 1);$$

Received by the editors October 11, 1985 and, in revised form, March 10, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D41; Secondary 11D61, 11D85.

this result is unsatisfactory in practice. In some special cases, simple explicit formulas of $I(d_1,\dots,d_n)$ are known. For the case $d_1 = d_2 = \cdots = d_n = d$, it is proved that

$$I(d,\dots,d) = \frac{d-1}{d}\left((d-1)^{n-1} + (-1)^n\right); \tag{4}$$

see Schmidt [**4**,169] and Small [**5**]. For the more general case $d_1|d_2|\cdots|d_n$, we proved [**6**]

(5)

$$I(d_1,\dots,d_n) = \prod_{j-1}^{n-1}(d_j-1) - \prod_{j=1}^{n-2}(d_j-1) + \cdots + (-1)^{n-1}(d_2-1)(d_1-1) + (-1)^n(d_1-1).$$

Recently, a complicated formula for $I(d_1,\dots,d_n)$ was obtained independently by Lidl and Niederreiter [**3**], R. Stanly (see Small [**5**]) and us [**6**] with not completely identical methods. The formula can be stated as follows:

$$I(d_1,\dots,d_n) = (-1)^n + \sum_{r=1}^{n}(-1)^{n-r} \sum_{1\le i_1<\cdots<i_r\le n} \frac{d_{i_1}\cdots d_{i_r}}{\operatorname{lcm}(d_{i_1},\dots,d_{i_r})}. \tag{6}$$

Note that both (4) and (5) can be deduced from (6).

Form (3), we find it is interesting to determine when $I(d_1,\dots,d_n) = 0$, for if $I(d_1,\dots,d_n) = 0$, then (2) has exactly $q^{n-1}$ solutions. Some partial results have been obtained along these lines by Joly [**2**] (see also [**3**, **4**, **5**]; he proved that if for some $d_i$,

$$(d_i, d_1\cdots d_n/d_i) = 1, \quad \text{or} \quad 2 \nmid n \text{ and } d_j = 2 \ (j = 1,\dots,n),$$

then $I(d_1,\dots,d_n) = 0$.

In our recent communication with him, Professor Niederreiter said though there is the formula (6) for the number $I(d_1,\dots,d_n)$ it cannot be deduced readily when $I(d_1,\dots,d_n) = 0$ from the formula. The main purpose of this paper is to solve the problem, that is, to determine when equation (1) has no solutions.

**2. The main theorem.** For $n = 2$, the solvable condition of (1) can be easily obtained (see the lemma below). We suppose $n > 2$.

THEOREM. *Let $n > 2$; then (1) has no solutions if and only if one of the following conditions holds.*

1. *For some $d_i$, $(d_i, d_1\cdots d_n/d_i) = 1$, or*
2. *If $d_{i_1},\dots,d_{i_k}$ $(1 \le i_1 < \cdots < i_k \le n)$ is the set of all even integers among $\{d_1,\dots,d_n\}$, then $2 \nmid k, d_{i_1}/2,\dots,d_{i_k}/2$ are pairwise prime, and $d_{i_j}$ is prime to any odd number in $\{d_1,\dots,d_n\}$ $(j = 1,\dots,k)$ if $k < n$.*

For convenience, we first introduce two lemmas.

LEMMA 1. *Let $(d_1,d_2) = d > 1$; then $x_1/d_1 + x_2/d_2 = 1$, $1 \le x_i < d_i$ $(i = 1,2)$ has a solution. Moreover, we can take $x_1 \ne d_1/2$ if $d > 2$.*

PROOF. Put $x_1 = d_1/d, x_2 = d_2(d-1)/d$; then $x_1, x_2$ is a desired solution. Remark: $x_1 = d_1a/d, x_2 = d_2(d-a)/d, a = 1,2,\dots,d-1$, actually furnish all $d-1$ solutions to the equation in the lemma. Therefore, for $n = 2$, (1) has no solutions if and only if $(d_1,d_2) = 1$.

DEFINITION. If

$$\frac{a_1}{d_1}+\frac{a_1}{d_2}+\cdots+\frac{a_m}{d_m}\equiv 0 \pmod 1, \qquad a_i \text{ integral, } 1\le a_i<d_i \ (1\le i\le m),$$

we simply say that $\{d_1,\dots,d_m\}$ has a solution and $\{a_1,\dots,a_m\}$ is a solution of $\{d_1,\dots,d_m\}$.

LEMMA 2. *Let $\{d_1,\dots,d_{m-1}\}$ have a solution but $\{d_1,\dots,d_m\}$ have none. If $(d_i,d_m)>1$ for some $i<m$, then $(d_i,d_m)=2$.*

PROOF. Let $\{a_1,\dots,a_{m-1}\}$ be a solution of $\{d_1,\dots,d_{m-1}\}$, and $\{b_i,b_m\}$ be a solution of $\{d_i,d_m\}$ which has the property described in Lemma 1. If $d_i\nmid a_i+b_i$, then $a_1,\dots,a_{i-1}$, $\langle a_i+b_i\rangle_{d_i}$, $a_{i+1},\dots,a_{m-1},b_m$ is a solution of $\{d_1,\dots,d_m\}$; if $d_i\nmid a_i-b_i$, then $a_1,\dots,a_{i-1}$, $\langle a_i-b_i\rangle_{d_i}$, $a_{i+1}$, $d_m-b_m$ is a solution of $\{d_1,\dots,d_m\}$, where the symbol $\langle x\rangle_m$ denotes the smallest nonnegative residue of $x \pmod m$. Both cases contradict the hypothesis of the lemma. Thus, $d_i|a_i+b_i, d_i|a_i-b_i$, and $d_i|2a_i, d_i|2b_i$; from this, it follows that $a_i=b_i=d_i/2$. In terms of Lemma 1 and the property of the chosen $b_i$, we must have $(d_i,d_m)=2$.

PROOF OF THE THEOREM. First, the conditions are sufficient. In fact, if condition 1 is satisfied, (1) having no solutions has been proved by Joly [**2**]. We now suppose condition 2 is satisfied. If (1) had a solution, we would prove that the equation

$$\frac{x_{i_1}}{d_{i_1}}+\cdots+\frac{x_{i_k}}{d_{i_k}}\equiv 0 \pmod 1, \qquad 1\le x_{i_j}<d_{i_j} \ (j=1,\dots,k) \tag{7}$$

has a solution. Let $k<n$, $x_i=a_i$ $(i=1,\dots,n)$ be a solution of (1), and $B$ denote the product of all odd numbers among $\{d_1,\dots,d_n\}$. From

$$\frac{a_1}{d_1}+\cdots+\frac{a_n}{d_n}\equiv 0 \pmod 1$$

we have

$$\frac{Ba_{i_1}}{d_{i_1}}+\cdots+\frac{Ba_{i_k}}{d_{i_k}}\equiv 0 \pmod 1. \tag{8}$$

Because of $(B,d_{i_j})=1$ $(j=1,\dots,k)$, this reduces to $a_{i_1}/d_{i_1}+\cdots+a_{i_k}/d_{i_k}\equiv 0 \pmod 1$. That is, equation (7) has a solution. But $d_{i_i}/2,\dots,d_{i_k}/2$ are pairwise prime; this together with $1\le a_{i_j}<d_j$ $(j=1,\dots,k)$ implies $a_{i_j}=d_{i_j}/2$ $(j=1,\dots,k)$. Then from (8), we have

$$k/2\equiv 0 \pmod 1.$$

This contradicts with $2\nmid k$, hence (1) has no solutions. If $k=n$, the above proof also shows (1) has no solutions. Therefore, the sufficiency of the conditions of the theorem is proved.

Next, we prove that the conditions are also necessary. Let (1) have no solutions. If for some $d_i$, $(d_i,d_1\cdots d_n/d_i)=1$, then condition 1 is satisfied. Otherwise, we have $(d_i,d_1\cdots d_n/d_i)>1$ $(i=1,\dots,n)$, hence $(d_1,d_j)>1$ for some $j$; according to Lemma 1 $\{d_1,d_j\}$ has a solution. Therefore, there exists a subset $S$ of $\{d_1,\dots,d_n\}$ having maximal cardinal number such that $S$ has a solution in the sense of our definition. $S$ will turn out to be a subset of $\{d_1,\dots,d_n\}$ of cardinality $n-1$ obtained by deleting any even element $d_j$.

Without loss of generality, we let $S = \{d_1, \ldots, d_t\}$; we prove $t = n-1$. Suppose $a_1, \ldots, a_t$ is a solution of $\{d_1, \ldots, d_t\}$; we first prove that $d_{t+1}, \ldots, d_n$ are pairwise prime. Otherwise, we may suppose $(d_{t+1}, d_{t+2}) > 1$. From Lemma 1 we know $\{d_{t+1}, d_{t+2}\}$ has solution $\{b_{t+1}, b_{t+2}\}$; then $a_1, \ldots, a_t, b_{t+1}, b_{t+2}$ is a solution of $d_1, \ldots, d_{t+2}$; but $t$ is maximal according to our choice. This is impossible, so $\{d_{t+1}, \ldots, d_n\}$ are pairwise prime. From $(d_i, d_1 \cdots d_n/d_i) > 1$ $(i = 1, \ldots, n)$, we know $d_{t+j}$ $(j = 1, \ldots, n-t)$ is not prime to some of $\{d_1, \ldots, d_t\}$; we may therefore suppose there exists $i \leq t$ depending on $j$ for which $(d_{t+j}, d_i) > 1$. By Lemma 2 we have $(d_{t+j}, d_i) = 2$. Hence $2 | d_{t+j}$ $(j = 1, \ldots, n-t)$, but we have proved that $d_{t+1}, \ldots, d_n$ are pairwise prime, so this forces $t = n-1$ and $2 | d_n$.

Now we prove that among $\{d_1, \ldots, d_n\}$ any odd number and any even number are relatively prime. Let $d_j$ $(j \leq n)$ be an odd number and $d_i$ be an even number. If $i = n$, then $(d_j, d_i) = 1$; this is proved above. We now suppose $i < n$; then Lemma 2 implies that $(d_i, d_n) = 2$ and $\{d_i/2, d_n/2\}$ is a solution of $\{d_i, d_n\}$. If $d_i \nmid a_i + d_i/2$, then $a_1, \ldots, a_{i-1}, \langle a_i + d_i/2 \rangle_{d_i}, a_{i+1}, \ldots, a_{n-1}, d_n/2$ is a solution of $\{d_1, \ldots, d_n\}$; this contradicts the insolvability of (1). Hence, $d_i | a_i + d_i/2$ and $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n-1}, d_n/2$ is a solution of $\{d_1, \ldots, d_{i-1}, d_{i+1}, \ldots, d_n\}$. Lemma 2 shows that if $(d_j, d_i) > 1$, then $(d_j, d_i) = 2$; but $2 \nmid d_j$, so $(d_j, d_i) = 1$, and among $\{d_1, \ldots, d_n\}$ any odd number and any even number are relatively prime. We have also proved that any two even numbers of $\{d_1, \ldots, d_n\}$ have 2 as their greatest common divisor, that is $d_{i_1}/2, \ldots, d_{i_k}/2$ are pairwise prime.

Finally, we prove that $2 \nmid k$. If $d_1, \ldots, d_n$ are all even, then $2 \nmid n$, otherwise (1) has a solution $x_i = d_i/2$ $(i = 1, \ldots, n)$, which is impossible. Below we let $k < n$, $d_{u_1}, \ldots, d_{u_l}$ $(l \geq 1)$ be all odd numbers of $\{d_1, \ldots, d_n\}$, $E = \prod_{j=1}^{k} d_{i_j}$. From $2 | d_n$, we have $k \geq 1$, $\{d_{u_1}, \ldots, d_{u_l}\} \subseteq \{d_1, \ldots, d_{n-1}\}$. From

$$\frac{a_1}{d_1} + \cdots + \frac{a_{n-1}}{d_{n-1}} \equiv 0 \pmod 1, \qquad 1 \leq a_j < d_j \ (j = 1, \ldots, n-1)$$

we have

$$\frac{Ea_{u_1}}{d_{u_1}} + \cdots + \frac{Ea_{u_l}}{d_{u_l}} \equiv 0 \pmod 1$$

but $(E, d_{u_1} \cdots d_{u_l}) = 1$, so

$$\frac{a_{u_1}}{d_{u_1}} + \cdots + \frac{a_{u_l}}{d_{u_l}} \equiv 0 \pmod 1.$$

If $2 | k$, $\{d_{i_1}, \ldots, d_{i_k}\}$ would have a solution $f_1, \ldots, f_k$,

$$\frac{f_1}{d_{i_1}} + \cdots + \frac{f_k}{d_{i_k}} \equiv 0 \pmod 1;$$

then $(a_{u_1}, \ldots, a_{u_l}, f_1, \ldots, f_k)$ would be a solution of $\{d_{u_1}, \ldots, d_{u_l}, d_{i_1}, \ldots, d_{i_k}\} = \{d_1, \ldots, d_n\}$. This contradicts our hypothesis, therefore $2 \nmid k$ and the theorem is completely proved.

**3. Some applications.** We now present several examples which indicate equation (2) has exactly $q^{n-1}$ solutions.

EXAMPLE 1. From the theorem we see that for $d_1 = 2m_i, 2 \nmid n$ and $\{m_1, \ldots, m_n\}$ pairwise prime, $I(d_1, \ldots, d_n) = 0$. Then it follows from (3) that in this case (2) has exactly $q^{n-1}$ solutions.

EXAMPLE 2. For $d_1 = \cdots = d_k = 2$, $2 \nmid k$, and $2 \nmid d_j$, $j = k+1, \ldots, n$, we also have $I(d_1, \ldots, d_n) = 0$. This is a generalization of a result of Joly.

EXAMPLE 3. Let $\{d_1, \ldots, d_n\}$ denote a block of $n$ consecutive positive integers. If $n \leq 16$, then condition 1 holds, so $I(d_1, \ldots, d_n) = 0$. However, for each $n \geq 17$, we can find a block $\{d_1, \ldots, d_n\}$ for which condition 1 fails to hold and so by the Theorem, $I(d_1, \ldots, d_n) \neq 0$ (see [**1**]).

## REFERENCES

1. R. J. Evans, *On blocks of N consecutive integers*, Amer. Math. Monthly **76** (1969), 48–49.
2. J. R. Joly, *Nombre de solutions de certaines équations diagonales sur un corps fini*, C. R. Acad. Sci. Paris Ser. A–B **272** (1971), 1549–1552.
3. R. Kidl and H. Niederreiter, *Finite fields*, Encyclopedia of Math. and Its Appl., vol. 20, Addison-Wesley, Reading, Mass, 1983.
4. W. M. Schmidt, *Equations over finite fields*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin and New York, 1976.
5. C. Small, *Diagonal equations over large finite fields*, Canad. J. Math. **36** (1984), 249–262.
6. Sun Qi, Wan Daqing and Ma Degang, *On the equation* $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$, Chinese Ann. of Math. (to appear).

DEPARTMENT OF MATHEMATICS, SICHUAN UNIVERSITY, CHENGDU, SICHUAN, PEOPLE'S REPUBLIC OF CHINA (Current address of Sun Qi)

*Current address* (Daqing Wan): Department of Mathematics, University of Washington, Seattle, Washington 98195