On the number of solution of the equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$, and of diagonal equations in finite fields*

Andrew Granville, *Shuguang Li*
(Department of Mathematics, University of Georgia, Athens, GA 30602, USA)
Sun Qi
(Department of Mathematics, Sichuan University, Chengdu, Sichuan 610064)

Dedicated to Prof. Ko Chao on the occasion of his 85th birthday

Abstract Let $I(d_1,\cdots,d_n)$ denote the number of solutions to equation

$$\frac{x_1}{d_1}+\frac{x_2}{d_2}+\cdots+\frac{x_n}{d_n}\equiv 0 \pmod 1,\quad 1\leqslant x_i\leqslant d_i-1,\quad i=1,\cdots,n.$$

We investigate the numbers $I(d_1,\cdots,d_n)$ which provide bounds for the number of solutions $x_1,\cdots,x_n$ to diagonal equations $c_1x_1^{d_1}+\cdots+c_nx_n^{d_n}=0$ where $c_1,\cdots,c_n$ are given elements of a finite field and $d_1,\cdots,d_n$ are given positive integers. We obtain sharp general lower bounds for $I(d_1,\cdots,d_n)$.

Key words Finite field, diagonal equation, congruences
(1991 MSC: 11D79, 11T99)

Let F_q be a finite field of q elements, where $q=p^l$, $l\geqslant 1$, p is an odd prime. Let $c_i(i=1,\cdots,n)$ be nonzero elements of F_q. Suppose that $d_1,\cdots,d_n$ are fixed positive integers and d_i divides $q-1$ for all i. Let $N=N(d_1,\cdots,d_n;c_1,\cdots,c_n)$ be the number of solutions $(x_1,\cdots,x_n)\in F_q^{(n)}$ to the diagonal equation

$$c_1x_1^{d_1}+\cdots+c_nx_n^{d_n}=0. \tag{1}$$

It is well known (for example, see page 147 of [1]) that $|N-q^{n-1}|\leqslant I(d_1,\cdots,d_n)(q-1)q^{(n-2)/2}$, where $I(d_1,\cdots,d_n)$ denotes the number of solutions of the equation

$$\frac{x_1}{d_1}+\frac{x_2}{d_2}+\cdots+\frac{x_n}{d_n}\equiv 0 \pmod 1,\ 1\leqslant x_i\leqslant d_i-1,\ i=1,\cdots,n. \tag{2}$$

Thus $I(d_1,\cdots,d_n)$ and its estimations play an important role in studying diagonal equations over a finite field.

A trivial upper bound for $I(d_1,\cdots,d_n)$ is given by

Received September, 13, 1994

$$I(d_1,\cdots,d_n) \leqslant (d_1-1)(d_2-1)\cdots(d_n-1).$$

In 1991, sun Qi and D. Wan proved that

$$I(d_1,\cdots,d_n) = I(u_1,\cdots,u_n), \tag{3}$$

where $u_j = \gcd(d_j,\ d_1\cdots d_n/d_j)$, $j = 1,\cdots,n$, so that for all $j(1 \leqslant j \leqslant n)$

$$I(d_1,\cdots,d_n) \leqslant \prod_{i\neq j}(u_i - 1) \tag{4}$$

(see Theorems 1 and 2 in [3]).

Recently Sun Qi and P. Yuan(see [4]) gave the following identity for $N(d_1,\cdots,d_n;\ c_1,\cdots,c_n)$:

$$N(d_1,\cdots,d_n;\ c_1,\cdots,c_n) = N(u_1,\cdots,u_n;\ c_1,\cdots,c_n) \tag{5}$$

In this paper we obtain the following theorems and corollaries.

Theorem 1 (i) If $w_i = \gcd(d_i,\ \mathrm{lcm}[d_1,\cdots,d_{i-1},\ d_{i+1},\cdots,d_n])$ for $i = 1,\cdots,n$, then

$$I(d_1,\cdots,d_n) = I(w_1,\cdots,w_n), \tag{6}$$

(ii)
$$w_i = \gcd(w_i,\ \mathrm{lcm}[w_1,\cdots,w_{i-1},\ w_{i+1},\cdots,w_n]). \tag{7}$$

Part (i) of the theorem says that there is a reduction process for $I(d_1,\cdots,d_n)$. Part (ii) of the theorem says that this reduction terminates at the second step.

Proof of theorem 1: Consider the equation

$$\frac{y_1}{w_1} + \cdots + \frac{y_n}{w_n} \equiv 0 \pmod 1,\ 1 \leqslant y_i \leqslant w_i - 1,\ i = 1,\cdots,n. \tag{8}$$

We claim that $x_i = y_id_i/w_i$ gives an one-one correspondence between the solutions of equation (2) and the solutions of equation (8). Part (i) of theorem 1 follows from this correspondence. To prove the claim, it is sufficient to prove that any solution $(x_1,\cdots,x_n)$ of equation (2) satisfies $x_i = y_id_i/w_i$ for some integers $y_i(1 \leqslant i \leqslant n)$.

Let $(b_1,\ b_2,\cdots,b_n)$ be a solution of (2). Thus, there is a positive integer Z such that

$$\frac{b_1}{d_1} + \cdots + \frac{b_n}{d_n} = Z. \tag{9}$$

Multiply both sides of (9) by $d_1\mathrm{lcm}\ [d_2,\cdots,d_n]/w_1$, we have

$$\frac{\mathrm{lcm}[d_2,\cdots,d_n]}{w_1}b_1 + \frac{d_1\mathrm{lcm}[d_2,\cdots,d_n]}{w_1}\frac{b_2}{d_2} + \cdots + \frac{d_1\mathrm{lcm}[d_2,\cdots,d_n]}{w_1}\frac{b_n}{d_n} = \frac{d_1\,\mathrm{lcm}[d_2,\cdots,d_n]}{w_1}Z. \tag{10}$$

Since $\gcd\ (d_1/w_1,\ \mathrm{lcm}[d_2,\cdots,d_n]/w_1) = 1$ and each $\mathrm{lcm}\ [d_2,\cdots,d_n]/d_k$ is an integer, $k \geqslant 2$, we have $b_1 \equiv 0 \pmod{d_1/w_1}$ by(10). In the same way we have $b_i \equiv 0 \pmod{d_i/w_i}$, $i = 2,\cdots,n$. Thus $b_i = d_iy_i/w_i$ for some integers $y_i(1 \leqslant i \leqslant n)$. Since $0 < b_i < d_i$ thus $0 < y_i < w_i$ for all i, and claim is proved.

Now let us consider the second part of the theorem. Let l be a prime number dividing d_i to the exact power of l^{k_i}. Suppose that the exact powers of l dividing $d_1,\cdots,d_n$ are in descending order, $k_1 \geqslant k_2 \geqslant k_3 \geqslant \cdots \geqslant k_n$. Then the exact power of l dividing w_i is $l^{\min(k_i,k_2)}$. The sequences of powers of l dividing $w_1,\cdots,w_n$ are thus, in descending order, $k_2 \geqslant k_2 \geqslant k_3 \geqslant \cdots \geqslant k_n$. So if l^{j_i} is the exact power of l dividing w_i then $l^{\min(j_i,k_2)} = l^{j_i}$ divides $\gcd\ (w_i,\ \mathrm{lcm}[w_1,\cdots,w_{i-1},\ w_{i+1},\cdots,w_n])$ and the result follows.

Theorem 2 (i) For all j $(1 \leqslant j \leqslant n)$

$$I(d_1, \cdots, d_n) \leqslant \prod_{i \neq j} (w_i - 1). \tag{11}$$

(ii)

$$N(d_1, \cdots, d_n; c_1, \cdots, c_n) = N(w_1, \cdots, w_n; c_1, \cdots, c_n). \tag{12}$$

Proof To prove (11), it is sufficient to show that there is at most one y_j satisfying equation (8) for each choice of $\{y_i;\ 1 \leqslant i \leqslant n, i \neq j\}$. Given a set of y_i $(1 \leqslant y_i \leqslant w_i - 1,\ i = 2, \cdots, n)$, assuming that there are two choices for y_1, say y_1 and z_1, satisfying (8), then we have

$$(y_1 - z_1)/w_1 \equiv 0 \pmod 1,$$

so that $y_1 \equiv z_1 \pmod{w_1}$. Since $1 \leqslant y_1, z_1 \leqslant w_1 - 1$, thus $y_1 = z_1$ and so (11) holds.

Using Jacobi sums (see [2]), we have

$$N(d_1, \cdots, d_n;\ c_1 \cdots, c_n) = q^{n-1} + \sum_{\substack{x_1/d_1 + \cdots + x_n/d_n \equiv 0 \pmod 1 \\ 1 \leqslant x_j \leqslant d_j - 1, j = 1, \cdots, n}} \chi_1^{x_1}(c_1^{-1}) \cdots \chi_n^{x_n}(c_n^{-1})\ J_0(\chi_1^{x_1}, \cdots, \chi_n^{x_n})$$

and

$$N(w_1, \cdots, w_n;\ c_1, \cdots, c_n) = q^{n-1} + \sum_{\substack{y_1/w_1 + \cdots + y_n/w_n \equiv 0 \pmod 1 \\ 1 \leqslant y_j \leqslant w_j - 1,\ j = 1, \cdots, n}} \lambda_1^{y_1}(c_1^{-1}) \cdots \lambda_n^{y_n}(c_n^{-1}) J_0(\lambda_1^{y_1}, \cdots, \lambda_n^{y_n})$$

where $J_0(\chi_1, \cdots, \chi_n) = \sum_{\substack{a_1 + \cdots + a_n = 0 \\ a_j \in F_q,\ j = 1, \cdots, n}} \chi_1(a_1) \cdots \chi_n(a_n)$ is the Jacobi sum with $\chi_j(a) = e^{(2\pi i \operatorname{ind}(a))/d_j}$ and $\lambda_j(a) = e^{(2\pi i \operatorname{ind}(a))/w_j}$ for $a \in F_q^*$, $j = 1, \cdots, n$. In the proof of Theorem 1 we know that $x_i = y_i d_i / w_i$ gives an one to one correspondence between the solutions of (2) and the solutions of (8). Similarly we find that

$$\chi_j^{x_j}(a) = e^{(2\pi i \operatorname{ind}(a))/d_j) x_j} = e^{(2\pi i \operatorname{ind}(a) y_j / w_j)} = \lambda_j^{y_j}(a),\ a \in F_q^*,\ j = 1, \cdots, n.$$

Therefore $N(d_1, \cdots, d_n;\ c_1, \cdots, c_n) = N(w_1, \cdots, w_n;\ c_1, \cdots, c_n)$, which complates the proof.

Corollary If $I(d_1, \cdots, d_n) = 1$, then $2 \mid n$ and

$$N(d_1, \cdots, d_n;\ c_1, \cdots, c_n) = N(\underbrace{2, \cdots, 2}_{n\ 2's}; c_1, \cdots, c_n).$$

Proof In [3] Sun Qi and D. Wan proved that $I(d_1, \cdots, d_n) = 1$ if and only if $2 \mid n$, for some j, $d_j = 2^t m_j (t > 0)$ and $d_i = 2m_i$, $i \neq j$, $1 \leqslant i \leqslant n$, where $m_1, \cdots, m_n$ are odd integers and pairwise coprime.

Thus if $I(d_1, \cdots, d_n) = 1$, then $2 \mid n$ and $w_i = 2$, $i = 1, \cdots, n$. So

$$N(d_1, \cdots, d_n;\ c_1, \cdots, c_n) = N(w_1, \cdots, w_n;\ c_1, \cdots, c_n) = N(\underbrace{2, \cdots, 2}_{n\ 2's}; c_1, \cdots, c_n).$$

The corollary is proved.

Now, we may assume that $I(d_1, \cdots, d_n) > 0$.

By theorem 1 we may assume that d_j divides lcm $[d_i:\ i \neq j]$ without loss of generality. Note that if $d_1 = 2$ then $x_1 = 1$. So $I(2, 2, d_3, d_4, \cdots, d_n) = I(d_3, d_4, \cdots, d_n)$. Thus we need only to consider the cases where $I(d_1, \cdots, d_n)$, $d_j \mid \operatorname{lcm}[d_i: i \neq j]$, $d_j \geqslant 3$, $j = 1, 2, \cdots, n$, and $I(2, d_1, \cdots, d_n)$, $d_j/2 \mid \operatorname{lcm}[d_i: i \neq j]$, if d_i are odd for all i except d_j is even and $d_j \equiv 2 \pmod 4$ for one j; $d_j \mid \operatorname{lcm}[d_i: i \neq j]$, otherwise, where $d_j \geqslant 3$, $j = 1, 2, \cdots, n$. We shall prove

Theorem 3

$$I(d_1,\cdots,d_n) \text{ and } I(2,d_1,\cdots,d_n) \geqslant \frac{d_1\cdots d_n}{\mathrm{lcm}[d_1,\cdots,d_n]}\frac{1}{3^{n/2}}.$$

Proof Write $d_i = \prod_{m=1}^{M} p_m^{e_{im}}$, the factorization of d_i into powers of distinct primes. Let $q_i^{f_i}$ be the largest prime power dividing d_i that is $q_i^{f_i} = \max_{1\leqslant m\leqslant M} p_m^{e_{im}}$ for each i. Since $d_i \geqslant 3$ thus $q_i^{f_i} \geqslant 3$ for each i. In $I(d_1,\cdots,d_n)$ and $I' = I(2,d_1,\cdots,d_n)$ we count solutions to

$$\frac{x_1}{d_1}+\frac{x_2}{d_2}+\cdots+\frac{x_n}{d_n} \in Z \text{ and } Z+\frac{1}{2}$$

respectively, with each x_k satisfying $1\leqslant x_k \leqslant d_k - 1$.

To get a lower bound we select x_k by the Chinese Remainder Theorem so that

$$x_k \equiv x_{km}\prod_{j\neq m} p_j^{e_{kj}} \pmod{p_m^{e_{km}}},\ \text{for } 1\leqslant m\leqslant M,$$

where

$$\frac{x_{1m}}{p_m^{e_{1m}}}+\frac{x_{2m}}{p_m^{e_{2m}}}+\cdots+\frac{x_{nm}}{p_m^{e_{nm}}} \in Z, \tag{13}$$

(or $Z + 1/2$ if $p_m = 2$ and we are looking at I'). We only allow that

$$0\leqslant x_{km}\leqslant p_m^{e_{km}}-1,\quad \text{if } p_m^{e_{km}}\neq q_k^{f_k}, \tag{14}$$

$$1\leqslant x_{km}\leqslant p_m^{e_{km}}-1,\quad \text{if } p_m^{e_{km}} = q_k^{f_k}. \tag{15}$$

(this guarantees that $x_k \equiv 0 \pmod{d_k}$).

For each m let $E_m = \max_{1\leqslant j\leqslant n} e_{jm}$. Since d_j divides $\mathrm{lcm}[d_i; ,i\neq j]$, we can select distinct j_1 and j_2 so that $e_{j_1m} = e_{j_2m} = E_m$ (the only possible exception is if $p_m^{E_m} = 2$ and we are looking at I' and there is just one even d_j — in that case we must have x_j odd). So if $j\neq j_1$, j_2 choose x_{jm} to be any value in the ranges (14) or (15). If (13) is to be satisfied, that means that $x_{j_1m}+x_{j_2m} \equiv$ (fixed value) (mod $p_m^{E_m}$). Thus x_{j_2m} can take any value (mod $p_m^{E_m}$) which determines x_{j_1m}, except 0 if we have the range (15) for x_{j_2m}, and also except the value that forces $x_{j_1m} = 0$ if we have the range (15) for x_{j_1m}.

Therefore the total number of such sets $\{x_{jm}\}$ for a given p_m is at least

$$\prod_{k=1}^{n} p_m^{e_{km}}\cdot \prod_{\substack{k=1\\ p_m^{e_{km}}=q_k^{f_k}}}^{n}\left(1-\frac{1}{q_k^{f_k}}\right)\cdot\frac{1}{p_m^{E_m}}\begin{cases}\dfrac{p_m^{E_m}(p_m^{E_m}-2)}{(p_m^{E_m}-1)^2} & \text{if } p_m^{E_m} = q_{j_1}^{f_{j_1}} = q_{j_2}^{f_{j_2}},\\ 1 & \text{otherwise.}\end{cases} \tag{16}$$

Therefore taking the product over all primes p_m, $1\leqslant m\leqslant M$ and since $\mathrm{lcm}[d_1,\cdots,d_n] = \prod_{m=1}^{M} p_m^{E_m}$ we have (checking the one special case for I' with $p_m^{E_m} = 2$).

$$I(d_1,\cdots,d_n) \text{ and } I(2,d_1,\cdots,d_n)$$

$$\geqslant \frac{d_1\cdots d_n}{\mathrm{lcm}[d_1,\cdots,d_n]}\prod_{k=1}^{n}\left(1-\frac{1}{q_k^{f_k}}\right)\prod_{\substack{p\mid d_1,\cdots,d_n\exists\, j_1,j_2\\ \text{such that } p^E = q_{j_1}^{f_{j_1}} = q_{j_2}^{f_{j_2}}}}\left(1-\frac{1}{(p^E-1)^2}\right) \tag{17}$$

We now examine these products. Since each $q_k^{f_k}\geqslant 3$ thus $1 - 1/q_k^{f_k} \geqslant 2/3$. If $q_{j_1}^{f_{j_1}} = q_{j_2}^{f_{j_2}}$, Then our factor is $1 - 2/q_k^{f_k} \geqslant 1/3$. thus the factor corresponding to d_k is $\geqslant 1/\sqrt{3}$. The result follows.

With the same hypothesis as above $d_1\cdots d_n \geqslant \mathrm{lcm}[d_1,\cdots,d_n]^2$, and so we get

Corollary

$$I(d_1,\cdots,d_n) \text{ and } I(2,\ d_1,\cdots,d_n) \geqslant \left(\frac{d_1\cdots d_n}{3^n}\right)^{1/2}.$$

Let us revise our estimate above corresponding to prime p. Suppose that $p^{e_j} \| d_j$, $1 \leqslant j \leqslant n$ and $E = \max\{e_i; 1 \leqslant i \leqslant n\}$. Rearrange the $d'_j s$ so that $E = e_1 = e_2$. Then the factor arising from p in the right side of (16) is

$$\geqslant (p^E - 2) \prod_{j=3,p^{e_j}\geqslant 3}^{n} (p^{e_j} - 1) \prod_{j=3,p^{e_j}=2}^{n} p^{e_j}$$

$$\geqslant \left(\prod_{j=1}^{n} p^{e_j}\right)^{1/2}\cdot\left(1 - \frac{2}{p^E}\right) \prod_{j=3,p^{e_j}\geqslant 3}^{n} \left(\frac{(p^{e_j}-1)^2}{p^{e_j}}\right)^{1/2} \left(\prod_{j=3,p^{e_j}=2}^{n} p^{e_j}\right)^{1/2}.$$

Now if $p^{e_j} \geqslant 3$ then $(p^{e_j} - 1)^2/p^{e_j} \geqslant 4/3 > 1$. So the above is $\geqslant \left(\prod_{j=1}^{n} p^{e_j}\right)^{1/2}(1 - 2/p^E)$ in general.

When $E = 1$ and p is an odd prime, we can improve this estimation as follows. Without loss generality, let us suppose that $p \| d_i$, $i = 1,\cdots,s$ and p does not divide d_i, $i > s$, Then (13) becomes

$$\frac{x_1}{p} + \frac{x_2}{p} + \cdots + \frac{x_s}{p} \in Z,$$

which has solutions at least $(p-1)^{s-2}(p-2)$ when $s \geqslant 3$, or $p-1$ when $s = 2$. For $s \geqslant 3$,

$$(p-1)^{s-2}(p-2) = p^{s/2}[(p + 1/p - 2)^{(s-2)/2}(1 - 2/p)]$$

$$\geqslant \begin{cases} p^{s/2}, & \text{if } p \geqslant 3, \text{ or } p = 3 \text{ and } s \geqslant 10, \\ \dfrac{2}{3\sqrt{3}} p^{s/2}, & \text{if } p = 3 \text{ and } s \leqslant 9. \end{cases}$$

Therefore by denoting $\triangle = \mathrm{lcm}[d_1,\cdots,d_n]$,

$$I(2,\ d_1,\cdots,d_n) \text{ and } I(d_1,\cdots,d_n)$$

$$\geqslant \prod_{E\geqslant 2,p^E \| \triangle} \left(\left(\prod_{j=1}^{n} p^{e_j}\right)^{1/2}\left(1 - \frac{2}{p^E}\right)\right) \frac{2}{3\sqrt{3}} \left(\prod_{j=1,\text{odd } p \| \triangle}^{n} p^{e_j}\right)^{1/2}\cdot \prod_{\substack{\text{odd} p \| \triangle \\ \#\{i,p|d_i\}=2}} \left(1 - \frac{1}{p}\right) \frac{1}{\sqrt{2}} \quad (18)$$

(the last $1/\sqrt{2}$ occurs in the case of $I(2,d_1,\cdots,d_n)$ where exactly one d_j is even).

Since $\prod_{p_E \| \triangle, E\geqslant 2} (1 - 2/p^E) \geqslant \prod_{p \text{ prime}}(1 - 2/p^2)$ is convergent, we have

Theorem 4　Let $D = d_1\cdots d_n$. With the notations and hypothesis as above

$$I(2,\ d_1,\cdots,d_n) \text{ and } I(d_1,\cdots,d_n) \geqslant CD^{1/2} \prod_{p\|\triangle,\#\{i,p|d_i\}=2} \left(1 - \frac{1}{p}\right),$$

where $C = \frac{1}{3}\sqrt{2/3}\prod_{p\text{ prime}}(1 - 2/p^2) > 0.0878 > 5/57$.

Since $\#\{p \text{ prime}; p | \mathrm{lcm}[d_1,\cdots,d_n]\} \leqslant \frac{\log(\mathrm{lcm}[d_1,\cdots,d_n])}{\log 2} = L$, say, and $d_1\cdots d_n \geqslant \mathrm{lcm}[d_1,\cdots,d_n]^2/2$ (which implies that $\log_2 D \leqslant 2L - 1$), then, by using Mertens' Theorem,

$$\prod_{p\|\triangle,\#\{i,p|d_i\}=2} \left(1 - \frac{1}{p}\right) \geqslant \prod_{p|\triangle}\left(1 - \frac{1}{p}\right) \geqslant \prod_{i=1}^{L}\left(1 - \frac{1}{p_i}\right) > \frac{C_1}{\log L} \geqslant \frac{C_2}{\log\log D}$$

For some constants C_1, $C_2 > 0$, where $p_1 = 3 < p_2 < \cdots$ is the sequence of odd primes. Thus we have

Corollary With the same notations and hypothesis as in Theorem 4,

$$I(2,d_1,\cdots,d_n) \text{ and } I(d_1,\cdots,d_n) > \frac{C_3 D^{1/2}}{\log\log D},$$

for some explicitly computable constant $C_3 > 0$.

We note that this is just about best possible (up to the value of C_3) in general, for if $3 \leqslant p_1 < p_2 < \cdots < p_m$ are the sequence of odd primes then

$$I(p_1,p_1,p_2,p_2,p_3,p_3,\cdots,p_m,p_m) = \prod_{i=1}^{m}(p_i - 1) = D^{1/2}\prod_{i=1}^{m}(1 - \frac{1}{p_i}) \sim \frac{e^{-\gamma}D^{1/2}}{\log\log D}$$

where $D = (p_1\cdots p_m)^2$ and $\gamma \approx 0.0577$ is the Euler-Mascheroni constant.

Acknowledgment

This paper was written while Sun Qi was visiting the University of Georgia, who would like to take this opportunity to thank Carl Pomerance for his generous support.

References

1 Ireland K, Rosen M. A classical introduction to modern number theory-Graduate texts in Mathematics, vol 84, Springer-Verlag, New York, 1982

2 Lidl R, Niedrreiter H. Finite Fields, Encyclopedia of Mathematica, Vol 20, Addson-Wesley, 1983

3 Sun Qi, Wan D. In the Diophantine equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$, Proc. AMS, 1991 112: 25

4 Sun Qi, Yuan Ping-Zhi. On the number of solutions of diagonal equations over a finite field, to appear

关于方程 $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$ 的解的个数和有限域上的对角方程

G. Andrew 李曙光

(Georgia 大学数学系)

孙 琦

(四川大学数学系)

摘要 设 $I(d_1,\cdots,d_n)$ 代表方程 $x_1/d_1 + \cdots + x_n/d_n \equiv 0 \pmod 1$, $1 \leqslant x_i \leqslant d_i - 1, i = 1,2,\cdots,n$, 解的个数. 作者得到了一个计算 $I(d_1,\cdots,d_n)$ 的减缩定理: $I(d_1,\cdots,d_n) = I(w_1,\cdots,w_n)$, 这里 $w_j = \text{lcm}[w_i; i \neq j], j = 1,\cdots,n$. 还得到了 $I(d_1,\cdots,d_n)$ 的一个非平凡下界. 这些结果在有限域的对角方程零点个数的研究中, 有重要应用.

关键词 有限域, 对角方程, 同余式

中图法分类号 O156.7