PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 112, Number 1, May 1991

ON THE DIOPHANTINE EQUATION $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$

SUN QI AND DAQING WAN

(Communicated by William Adams)

ABSTRACT. Let $d_1, \ldots, d_n$ be n positive integers. The purpose of this note is to study the number of solutions and the least solutions of the following diophantine equation:

$$\frac{x_1}{d_1} + \cdots + \frac{x_n}{d_n} \equiv 0 \pmod 1, \qquad 1 \le x_i \le d_i - 1, \tag{1}$$

which arises from diagonal hypersurfaces over a finite field. In particular, we determine all the d_i's for which (1) has a unique solution.

Let F_q be a finite field of q elements, c_i $(i = 1, \ldots, n)$ be nonzero elements of F_q. Suppose that d_i divides $q - 1$ for all i. Let N be the number of solutions of the equation:

$$c_1 x_1^{d_1} + \cdots + c_n x_n^{d_n} = 0, \qquad x_i \in F_q. \tag{2}$$

It is well known (see [1]) that

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

where $I(d_1, \ldots, d_n)$ is the number of solutions of equation (1). Recently, it has been proven in [3] that

$$\operatorname{ord}_q(N - q^{n-1}) \ge L(d_1, \ldots, d_n) - 1, \tag{4}$$

where $L(d_1, \ldots, d_n)$ is the least positive integer represented by $\sum_{i=1}^{n} x_i/d_i$ $(1 \le x_i \le d_i - 1)$ and ord_q is the additive q-adic valuation normalized such that $\operatorname{ord}_q q = 1$.

Thus, the archimedean estimate of N is reduced to give a good upper bound on the total number $I(d_1, \ldots, d_n)$ of solutions of equation (1); while the q-adic estimate of N is reduced to give a good lower bound for the least solution of equation (1), i.e., $L(d_1, \ldots, d_n)$. In a previous article [2], we answered the question when equation (1) is unsolvable. In the present paper, we study I and L. In particular, we are able to characterize all the d_i's for which equation (1) has a unique solution. We note that there is a combinatorial formula for

Received by the editors January 2, 1990 and, in revised form, March 12, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D41; Secondary 11D61, 11D85.

$I(d_1, \ldots, d_n)$ (see [2]). Unfortunately, this formula does not tell much about I and L.

Our first result is the following reduction theorem, on which our other results are based.

Theorem 1.

(i) *For each* i, *define* $u_i = \gcd(d_i, d_1 \cdots d_n/d_i)$. *Then we have the following two equalities*:

$$I(d_1, \ldots, d_n) = I(u_1, \ldots, u_n), \tag{5}$$

$$L(d_1, \ldots, d_n) = L(u_1, \ldots, u_n). \tag{6}$$

(ii) *For each* i, *define* $v_i = \gcd(u_i, u_1 \cdots u_n/u_i)$. *Then we have* $v_i = u_i$ *for all* i.

Part (i) of the theorem says that there is a reduction process for I and L. Part (ii) of the theorem says that this process terminates at the second step.

Proof. Consider the equation:

$$\frac{y_1}{u_1} + \cdots + \frac{y_n}{u_n} \equiv 0 \pmod 1, \qquad 1 \le y_i \le u_i - 1. \tag{7}$$

We claim that $x_i = y_i d_i/u_i$ gives a one-one correspondence between the solutions of equation (1) and the solutions of equation (7). Part (i) of the theorem then follows from this correspondence. To prove the claim, it is sufficient to prove that any solution $(x_1, \ldots, x_n)$ of equation (1) satisfies $x_i = y_i d_i/u_i$ for suitable integers y_i $(1 \le i \le n)$.

Let $b_1, \ldots, b_n$ be a solution of (1). Thus, there is a positive integer z such that

$$\frac{b_1}{d_1} + \cdots + \frac{b_n}{d_n} = z. \tag{8}$$

Multiply both sides of (8) by $d_1 \cdots d_n/u_1$, we have

$$\frac{b_1}{u_1} d_2 \cdots d_n + \sum_{i=2}^{n} b_i \frac{d_1}{u_1} \frac{d_2 \cdots d_n}{d_i} = z \frac{d_1}{u_1} d_2 \cdots d_n. \tag{9}$$

Since $(d_1/u_1, d_2 \cdots d_n/u_1) = 1$, from (9) we have

$$b_1 \equiv 0 \pmod{\frac{d_1}{u_1}}.$$

Similarly, we have

$$b_i \equiv 0 \pmod{\frac{d_i}{u_i}}.$$

Thus, $b_i = d_i y_i/u_i$ for some integers y_i $(1 \le i \le n)$, and the claim is proved.

To prove the second part of the theorem, we need to verify

$$u_i = \gcd(u_i, u_1 \cdots u_n/u_i) \qquad (1 \le i \le n). \tag{10}$$

For any given prime number l, let $h_i = \operatorname{ord}_l(d_i)$ (for simplicity of notation, we suppress the dependence of h_i on l). Then, we have

$$\operatorname{ord}_l u_i = \min\left(h_i, \sum_{j\neq i} h_j\right),$$

$$\operatorname{ord}_l u_1 \cdots u_n/u_i = \sum_{j\neq i} \min\left(h_j, \sum_{k\neq j} h_k\right).$$

Thus, (10) holds if and only if the following inequality holds for all prime numbers l and all i $(1 \leq i \leq n)$,

$$\min\left(h_i, \sum_{j\neq i} h_j\right) \leq \sum_{j\neq i} \min\left(h_j, \sum_{k\neq j} h_k\right). \tag{11}$$

Case I. $h_i \leq h_j$ for some $j \neq i$. In this case, we have

$$\min\left(h_i, \sum_{j\neq i} h_j\right) = h_i \leq \min\left(h_j, \sum_{k\neq j} h_k\right). \tag{12}$$

Clearly, the right term of (12) is less than or equal to the right term of (11).

Case II. $h_i \geq \max_j h_j$ for all $j \neq i$. In this case,

$$\min\left(h_i, \sum_{j\neq i} h_j\right) \leq \sum_{j\neq i} h_j \leq \sum_{j\neq i} \min\left(h_j, \sum_{k\neq j} h_k\right). \tag{13}$$

Thus, (11) holds in this case, too. The theorem is proved.

As a corollary of Theorem 1, we have the following estimates for I and L.

Theorem 2. *For all* j $(1 \leq j \leq n)$, *the following two inequalities hold*:

$$I(d_1, \ldots, d_n) \leq \prod_{i\neq j} (u_i - 1), \tag{14}$$

$$L(d_1, \ldots, d_n) \geq \tfrac{1}{u_1} + \cdots + \tfrac{1}{u_n}. \tag{15}$$

Part (ii) of Theorem 1 shows that if one repeats the process of (5) and (6), one does not get a better bound.

Proof. Consider equation (7). (15) is trivial by Theorem 1. To prove (14), it suffices to show that for each choice of y_i $(i \neq j)$ there is at most one y_j satisfying equation (7). We may suppose that $j = 1$. If for a given y_i $(1 \leq y_i \leq u_i - 1,\ i = 2, 3, \ldots, n)$ there are two choices for y_1, say y_1 and z_1, satisfying (7), then one has

$$(y_1 - z_1)/u_1 \equiv 0 \pmod 1. \tag{16}$$

This implies that $y_1 = z_1$. Thus, (14) is true.

The next result describes all d_i's for which equation (1) has no solutions.

Theorem 3. *Let* $u_i = \gcd(d_i, d_1 \cdots d_n/d_i)$ $(1 \le i \le n)$. *The following conditions are equivalent.*

(a) $I(d_1, \ldots, d_n) = 0$.

(b) $L(d_1, \ldots, d_n) = +\infty$.

(c) *Either some* $u_i = 1$, *or let* u_{i_j} $(j = 1, \ldots, k)$ *be all the even integers among the* u_i*'s; then* k *is odd and* $u_{i_j} = 2$ *for all* j *except* $u_{i_l} = 2^t$ $(t > 0)$ *for one* l.

In [2], we gave a necessary and sufficient condition for $I = 0$ in terms of the d_i's. Unfortunately, that condition is not very simple. In contrast, the new condition (in terms of the u_i's) given in Theorem 3 is much simpler.

Proof. The equivalence of (a) and (b) is trivial. We now prove that (c) $\Rightarrow$ (a). If the first condition of (c) holds, i.e., some $u_i = 1$, then (7) has no solutions. Theorem 1 shows that $I(d_1, \ldots, d_n) = 0$. If the second condition of (c) holds, then for any solution y_i $(i = 1, \ldots, n)$ of (7), we must have $y_{i_j} = 1$ and k even. This contradicts the assumption that k is odd. Thus, $I(d_1, \ldots, d_n) = 0$. Next, we prove (a) $\Rightarrow$ (c). Assuming $I(d_1, \ldots, d_n) = 0$, the result in [2] shows that one of the following conditions holds:

(i) For some i, $\gcd(d_i, d_1 \cdots d_n/d_i) = 1$.

(ii) Let d_{i_j} $(j = 1, \ldots, k)$ be all the even integers among the d_i's; then k is odd, $d_{i_1}/2, \ldots, d_{i_k}/2$ are pairwise prime, and any d_{i_j} is prime to any odd numbers among the d_i's.

If (i) is true, then $u_i = 1$ and the first condition of (c) holds. We now suppose that (ii) is true. If $k = 1$, one checks that $u_{i_1} = 1$. Hence, the first condition of (c) holds. If $k > 1$, it is easy to see that the second condition of (c) is satisfied. This proves that (a) implies (c). Theorem 3 is proved.

The last result describes all d_i's for which equation (1) has a unique solution.

Theorem 4. *Let* $n > 1$. *Let* $u_i = \gcd(d_i, d_1 \cdots d_n/d_i)$ $(1 \le i \le n)$. *The following conditions are equivalent.*

(a) $I(d_1, \ldots, d_n) = 1$.

(b) n *is even and* $u_i = 2$ *for all* i *except* $u_j = 2^k$ $(k > 0)$ *for one* j.

Proof. First, (b) $\Rightarrow$ (a). Without loss of generality, we suppose that $u_1 = \cdots = u_{n-1} = 2$ and $u_n = 2^k$ for some $k > 0$. If $y_i = b_i$ $(1 \le i \le n)$ give a solution of (7), then one must have $b_1 = \cdots = b_{n-1} = 1$ and $b_n = 2^{k-1}$. Thus (7) has a unique solution.

Next, we prove (a) $\Rightarrow$ (b). Let $y_1, \ldots, y_n$ be the unique solution of equation (7). It is clear that $u_i - y_i$ $(1 \le i \le n)$ also satisfy (7). By uniqueness of solution, we have $y_i = u_i/2$ for all i. We claim that $\gcd(u_i, u_j) = 2$ for all $i \ne j$. To prove the claim, we let $d = \gcd(u_i, u_j) > 2$ for some $i \ne j$. Then

the equation

$$\frac{z_i}{u_i} + \frac{z_j}{u_j} \equiv 0 \pmod 1, \qquad 1 \le z_l \le u_l - 1, \tag{17}$$

has exactly $d - 1 > 1$ solutions. Furthermore, it is easy to see that one can choose a solution z_l such that $z_l \ne u_l/2$ $(l = i, j)$. Then $y_i + z_i \pmod{u_i}$, $y_j + z_j \pmod{u_j}$, y_l $(l \ne i, j)$ give rise to a new solution of (7) contradicting with the assumption on uniqueness.

By part (ii) of Theorem 1, we have

$$\gcd(u_i, u_1 \cdots u_n/u_i) = u_i \qquad (1 \le i \le n). \tag{18}$$

The above claim and (18) show that all the u_i's are powers of 2. One more application of the claim $\gcd(u_i, u_j) = 2$ implies that $u_i = 2$ for all i except $u_j = 2^k$ $(k > 0)$ for one j. Theorem 4 is proved.

From the first part of the proof of Theorem 4, we have

Corollary 5. *Assume the d_i's satisfy one of the equivalent conditions in Theorem* 4; then

$$L(d_1, \ldots, d_n) = n/2. \tag{19}$$

Acknowledgment

This paper was written while the first author was visiting the University of Washington. He would like to thank Neal Koblitz and Ralph Greenberg for their generous support.

References

1. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Math., vol. 84, Springer-Verlag, New York, 1982.
2. Sun Qi and Daqing Wan, *On the solvability of the equation* $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$ *and its application*, Proc. Amer. Math. Soc. **100** (1987), 220–224.
3. Daqing Wan, *Zeros of diagonal equations over finite fields*, Proc. Amer. Math. Soc. **103** (1988), 1049–1052.

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

Department of Mathematics, The University of Washington, Seattle, Washington 98195