Chin. Ann. of Math.
7B (2) 1986

ON THE DIOPHANTINE EQUATION $\sum_{i=1}^{n}\frac{x_i}{d_i}\equiv 0$ (mod 1) AND ITS APPLICATIONS

SUN QI(孙琦)* WAN DAQING(万大庆)* MA DEGANG(马德刚)*

Abstract

The number $A(d_1, \cdots, d_n)$ of solutions of the equation

$$\sum_{i=1}^{n}\frac{x_i}{d_i}\equiv 0 \pmod 1,\ 0<x_i<d_i (i=1, 2, \cdots, n), \tag{1}$$

where all the $d_i's$ are positive integers, is of significance in the estimation of the number $N(d_1, \cdots, d_n)$ of solutions in a finite field F_q of the equation

$$\sum_{i=1}^{n}a_i x_i^{d_i}=0,\ x_i\in F_q (i=1,2, \cdots, n), \tag{2}$$

where all the $a_i's$ belong to F_q^*, the multiplication group of F_q[1, 2]. In this paper, applying the inclusion-exclusion principle, a general formula to compute $A(d_1 \cdots, d_n)$ is obtained. For some special cases more convenient formulas for $A(d_1, \cdots, d_n)$ are also given, for example, if $d_i | d_{i+1}$, $i=1, \cdots, n-1$, then

$$A(d_1, \cdots, d_n)=(d_{n-1}-1)\cdots(d_1-1)-(d_{n-2}-1)\cdots(d_1-1)+\cdots$$
$$+(-1)^{n-1}(d_2-1)(d_1-1)+(-1)^n(d_1-1).$$

For a polynomial equation of the type

$$a_1x_1^{d_1}+a_2x_2^{d_2}+\cdots+a_nx_n^{d_n}=0, \tag{1}$$

where $a_i\in F_q^*$ and $d_i>0 (i=1, 2, \cdots, n)$, a lot of study has been made[1, 2]. Let N be the number of solutions $(x_1, \cdots, x_n)$ in F_{q^n} of the equation (1), where $x_i\in F_q$, $i=1, \cdots, n$. By using exponential (character) sums it can be proved that

$$|N-q^{n-1}|\leqslant A(d_1, \cdots, d_n)\left(1-\frac{1}{q}\right)q^{\frac{n}{2}}.$$

Here $A(d_1, \cdots, d_n)$ is the number of the solutions of the Diophantine equation

$$\sum_{i=1}^{n}\frac{x_i}{d_i}\equiv 0 \pmod 1, \tag{2}$$

where $0<x_i<d_i$, $d_i>1$, $i=1, \cdots, n$. For the special case $d=d_1=\cdots=d_n$, it was proved that[2]

$$A(d, \cdots, d)=A_n(d)=\frac{d-1}{d}[(d-1)^{n-1}-(-1)^{n-1}],$$

but for the general $d_1, \cdots, d_n$, there is no formula for $A(d_1, \cdots, d_n)$. In this paper

Manuscript received January 18, 1984. Revised April 11, 1984.

* Department of Mathematics, Sichuan University, Chengdu, Sichuan, China.

we shall give a general formula for $A(d_1, \cdots, d_n)$, which, in several special cases, is also very convenient for calculating. In other words, we are now giving a more convenient estimate of the number N of solutions of the equation (1).

Theorem 1. *Let $B(d_1, \cdots, d_n)$ be the number of the solutions $(x_1, \cdots, x_n)$ in F_q^* of the equation*

$$\sum_{i=1}^{n}\frac{x_i}{d_i}\equiv 0 \pmod 1, \tag{3}$$

where $0\leqslant x_i<d_i$, $d_i>1$, $i=1, \cdots, n$. Let $A(d_1, \cdots, d_n)$ be as noted above. Then

$$B(d_1, \cdots, d_n)=[d_1, \cdots, d_n]^{-1}d_1\cdots d_n, \tag{4}$$

$$A(d_1, \cdots, d_n)=\sum_{k=1}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}\frac{d_{i_1}\cdots d_{i_k}}{[d_{i_1}, \cdots, d_{i_k}]}+(-1)^n. \tag{5}$$

Proof

(i) It can be easily seen that

$$\begin{aligned}B(d_1, \cdots, d_n)&=\frac{1}{[d_1, \cdots, d_n]}\sum_{a=1}^{[d_1, \cdots, d_n]}\sum_{x_1=0}^{d_1-1}\sum_{x_2=0}^{d_2-1}\cdots\sum_{x_n=0}^{d_n-1}e^{2\pi i a\left(\sum_{i=1}^{n}\frac{x_i}{d_i}\right)}\\&=\frac{1}{[d_1, \cdots, d_n]}\sum_{a=1}^{[d_1, \cdots, d_n]}\sum_{x_1=0}^{d_1-1}\cdots\sum_{x_n=0}^{d_n-1}\prod_{i=1}^{n}\exp\left(a\frac{x_i}{d_i}\right)\\&=\frac{1}{[d_1, \cdots, d_n]}\sum_{a=1}^{[d_1, \cdots, d_n]}\prod_{i=1}^{n}\sum_{x_i=0}^{d_i-1}\exp\left(a\frac{x_i}{d_i}\right)\\&=[d_1, \cdots, d_n]^{-1}d_1\cdots d_n.\end{aligned}$$

The last equality holds because of the fact that

$$\sum_{x_i=0}^{d_i-1}\exp\left(a\frac{x_i}{d_i}\right)=\begin{cases}d_i, & d_i\mid a,\\ 0, & d_i\nmid a.\end{cases}$$

(ii) Let $P=\left\{(x_1, \cdots, x_n)\;\middle|\;\sum_{i=1}^{n}\frac{x_i}{d_i}\equiv 0 \pmod 1,\ 0\leqslant x_i<d_i,\ i=1, \cdots, n\right\}$,

$$P_j=\{(x_1, \cdots, x_n)\mid (x_1, \cdots, x_n)\in P,\ x_j=0\},\ j=1, 2, \cdots, n,$$

then we have

$$|P|=B(d_1, \cdots, d_n),$$

$$|P_j|=B(d_1, \cdots, d_{j-1}, d_{j+1}, \cdots, d_n)$$

and

$$A(d_1, \cdots, d_n)=\left|P-\bigcup_{j=1}^{n}P_j\right|.$$

Applying the inclusion-exclusion principle, we get

$$\begin{aligned}A(d_1, \cdots, d_n)&=\left|P-\bigcup_{j=1}^{n}P_j\right|=\sum_{k=0}^{n}(-1)^k\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}|P_{i_1}\cap P_{i_2}\cap\cdots\cap P_{i_k}|\\&=\sum_{k=1}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}B(d_{i_1}, \cdots, d_{i_k})+(-1)^n\\&=\sum_{k=1}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<\cdots\leqslant i_k\leqslant n}\frac{d_{i_1}\cdots d_{i_k}}{[d_{i_1}, \cdots, d_{i_k}]}+(-1)^n.\end{aligned}$$

The Theorem is proved.

Without loss of generality, we assume that $d_1\leqslant d_2\leqslant\cdots\leqslant d_n$, and $A(d_1, \cdots, d_n)$ is the same as in Theorem 1.

Theorem 2.

1) *If there exists some* i *such that* $1\leqslant i\leqslant n$ *and* $(d_i,\ d_1\cdots d_{i-1}d_{i+1}\cdots d_n)=1$. *Then* $A(d_1,\ \cdots,\ d_n)=0$;

2) *For the case* $n=2$ *we have* $A(d_1,\ d_2)=d-1$, *where* $(d_1,\ d_2)=d$;

3) *If* $d_i\mid d_{i+1}$, $i=1,\ \cdots,\ n-1$, *then*

$$A(d_1,\ \cdots,\ d_n)=(d_{n-1}-1)\cdots(d_1-1)-(d_{n-2}-1)\cdots(d_1-1)+\cdots$$
$$+(-1)^{n-1}(d_2-1)(d_1-1)+(-1)^n(d_1-1);$$

4) *If* $n=3$, $(d_1,\ d_2)=1$, $(d_1,\ d_3)=t_1$, $(d_2,\ d_3)=t_2$, *then*

$$A(d_1,\ d_2,\ d_3)=(t_1-1)(t_2-1).$$

Proof

(i) Without loss of generality, we assume $(d_1,\ d_2\cdots d_n)=1$, so we have $[d_1,\ d_2,\ \cdots,\ d_n]=d_1[d_2,\ \cdots,\ d_n]$.

Hence

$$A(d_1,\ \cdots,\ d_n)=\sum_{k=1}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}\frac{d_{i_1}\cdots d_{i_k}}{[d_{i_1}\cdots d_{i_k}]}+(-1)^n$$
$$=(-1)^{n-1}+\Big[(-1)^{n-1}\sum_{2\leqslant i_1\leqslant n}\frac{d_{i_1}}{d_{i_1}}+(-1)^{n-2}\sum_{1\leqslant i_2\leqslant n}\frac{d_1d_{i_2}}{d_1d_{i_2}}\Big]$$
$$+\Big[(-1)^{n-2}\sum_{1<i_1<i_2\leqslant n}\frac{d_{i_1}d_{i_2}}{[d_{i_1},\ d_{i_2}]}+(-1)^{n-3}\sum_{1<i_2<i_3\leqslant n}\frac{d_1d_{i_2}d_{i_3}}{d_1[d_{i_2},\ d_{i_3}]}\Big]$$
$$+\Big[(-1)^{n-3}\sum_{1<i_1<i_2<i_3\leqslant n}\frac{d_{i_1}d_{i_2}d_{i_3}}{[d_{i_1},\ d_{i_2},\ d_{i_3}]}$$
$$+(-1)^{n-4}\sum_{1<i_2<i_3<i_4\leqslant n}\frac{d_1d_{i_2}d_{i_3}d_{i_4}}{[d_{i_2},\ d_{i_3},\ d_{i_4}]d_1}+\cdots$$
$$+\Big[-\sum_{1<i_1<i_2<\cdots<i_{n-1}\leqslant n}\frac{d_{i_1}\cdots d_{i_n}}{[d_{i_1},\ \cdots,d_{i_n}]}+\frac{d_1d_{i_1}\cdots d_{i_n}}{d_1[d_{i_1}\cdots d_{i_n}]}\Big]+(-1)^n$$
$$=(-1)^{n-1}+(-1)^n=0.$$

(ii) Using formula (5), we obtain

$$A(d_1,\ d_2)=-(1+1)+\frac{d_1d_2}{[d_1,\ d_2]}+1=d-1.$$

(iii) $$A(d_1,\ \cdots,\ d_n)=\sum_{k=1}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n}\frac{d_{i_1}\cdots d_{i_k}}{[d_{i_1},\ \cdots,\ d_{i_k}]}+(-1)^n$$
$$=\sum_{k=1}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n}\frac{d_{i_1}\cdots d_{i_k}}{d_{i_k}}+(-1)^n$$
$$=\sum_{k=1}^{n-1}(-1)^{n-k}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n-1}\frac{d_{i_1}\cdots d_{i_k}}{d_{i_k}}+(-1)^{n-1}$$
$$+\sum_{k=2}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<\cdots<i_{k-1}\leqslant n-1}d_{i_1}\cdots d_{i_{k-1}}+(-1)^n,$$

$$A(d_1,\ \cdots,\ d_{n-1})=\sum_{k=1}^{n-1}(-1)^{n-1-k}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n-1}\frac{d_{i_1}\cdots d_{i_k}}{d_{i_k}}+(-1)^{n-1},$$

$$A(d_1, \cdots, d_{n-1})+A(d_1, \cdots, d_n)=\sum_{k=2}^{n}(-1)^{n-k}\sum_{1\leqslant i_1<\cdots<i_{k-1}\leqslant n-1} d_{i_1}\cdots d_{i_{k-1}}+(-1)^{n-1}$$

$$\overset{k-2=t}{=\!=}\sum_{t=1}^{n-1}(-1)^{n-1-t}\sum_{1\leqslant i_1<\cdots<i_t\leqslant n-1} d_{i_1}\cdots d_{i_t}+(-1)^{n-1}$$

$$=(d_{n-1}-1)\cdots(d_1-1).$$

Hence

$$A(d_1, \cdots, d_n)=\prod_{i=1}^{n-1}(d_i-1)-A(d_1, \cdots, d_{n-1}).$$

From 2) we have

$$A(d_1, d_2)=d_1-1.$$

Then

$$A(d_1, \cdots, d_n)=\prod_{i=1}^{n-1}(d_i-1)-A(d_1, \cdots, d_{n-1})$$

$$=\prod_{i=1}^{n-1}(d_i-1)-\prod_{i=1}^{n-2}(d_i-1)+A(d_1, \cdots, d_{n-2})\cdots$$

$$=\prod_{i=1}^{n-1}(d_i-1)-\prod_{i=1}^{n-2}(d_i-1)+\cdots+(-1)^{n-1}(d_2-1)(d_1-1)$$

$$+(-1)^n(d_1-1).$$

This proves 3).

iv) When $n=3$, $(d_1, d_2)=1$, $(d_1, d_3)=t_1$, $(d_2, d_3)=t_2$, we have

$$[d_1, d_2]=d_1d_2,\ [d_1, d_3]=\frac{d_1d_3}{t_1},\ [d_2, d_3]=\frac{d_2d_3}{t_2},$$

$$[d_1, d_2, d_3]=[[d_1, d_2], d_3]=[d_1d_2, d_3]=\frac{d_1d_2d_3}{(d_1d_2, d_3)}=\frac{d_1d_2d_3}{(d_1, d_3)(d_2, d_3)}=\frac{d_1d_2d_3}{t_1t_2}.$$

Therefore

$$A(d_1, d_2, d_3)=(-1)^{3-1}3+(-1)^{3-2}\left(\frac{d_1d_2}{[d_1, d_2]}+\frac{d_1d_3}{[d_1, d_3]}+\frac{d_2d_3}{[d_2, d_3]}\right)$$

$$+(-1)^{3-3}\frac{d_1d_2d_3}{[d_1, d_2, d_3]}+(-1)$$

$$=3-1-(1+t_1+t_2)+\frac{d_1d_2d_3}{[d_1, d_2, d_3]}$$

$$=1-t_1-t_2+t_1t_2=(t_1-1)(t_2-1).$$

The proof is complete.

Let N be the number of solutions $(x_1, \cdots, x_n)$ in F_{q^n} of equation (1), obviously we have the following

Corollary 1. *If there exists some i, $1\leqslant i\leqslant n$, such that $(d_i, d_1\cdots d_{i-1}d_{i+1}\cdots d_n)=1$ then*

$$N=q^{n-1}.$$

Corollary 2. *If $d_i \mid d_{i+1}$ $(i=1, \cdots, n-1)$, then*

$$|N-q^{n-1}|\leqslant\left(\prod_{i=1}^{n-1}(d_i-1)-\prod_{i=1}^{n-2}(d_i-1)+\cdots+(-1)^n(d_1-1)\right)\left(1-\frac{1}{q}\right)q^{\frac{n}{2}}.$$

Corollary 3. $A(\underbrace{d, \cdots, d}_{\leftarrow n\rightarrow})=\frac{d-1}{d}((d-1)^{n-1}-(-1)^{n-1})).$

Proof

Theorem 2 gives us

$$A(\overbrace{d, \cdots, d}^{n}) = ((d-1)^{n-1} - (d-1)^{n-2} + \cdots + (-1)^n(d-1))$$
$$= \frac{d-1}{d}[(d-1)^{n-1} + (-1)^n],$$

this is a result of [2]

Corollary 4. *Assume that* $(d_1, d_2) = 1$, $(d_1, d_3) = t_1$, $(d_2, d_3) = t_2$, *then the number of solutions* (x_1, x_2, x_3) *in* F_{q^n} *of the Diophantine equation*

$$a_1x_1^{d_1} + a_2x_2^{d_2} + a_3x_3^{d_3} = 0,\ a_i \in F_q^*,\ d_i \mid q-1,\ i = 1, 2, 3,$$

satisfies

$$|N - q^2| \leqslant (t_1 - 1)(t_2 - 1)\left(1 - \frac{1}{q}\right)q^{\frac{3}{2}}.$$

References

[1] Ireland, K. and Rosen, M. I., A Classical Introduction to Modern Number Theory, Springer Graduate Text #84, New York, 1977.

[2] Schmidt, W. M., Equations over Finite Fields an Flementary Approach, Springer Lecture Notes #536, New York, 1976.