方程式$X_1^2+X_2^2+\cdots X_n^2=a$在有限體上之解的個數

(Number of Solutions of The Equation $X_1^2+X_2^2+\cdots+X_n^2=a$ in a Finite Field)

李 嘉 淦

一、引言

本文想以初等方法證明在有限體K上的方程式

(1) $x_1^2+x_2^2+\cdots\cdots+x_n^2=a$, $a\in K$

在K內的解的個數。

設有限體K的標數 (Characteristic) 爲質數p，則K必爲單體 (Simple field) $Z_p=\{0,1,\cdots\cdots,p-1\}$ (mod. p) 的有限擴張體，故其元數必爲$p^r=q$。

設(1)在上述有限體K之解之個數爲$S_n(a)$。已知$p=2$時，$S_n(a)=q^{n-1}$，但$p\neq 2$時，其解較爲複雜。本文主要目的爲討論$p\neq 2$時，$S_n(a)$之公式。其結果爲

(2)
$$\begin{cases} S_{2m}(0)=q^{2m-1}+\varepsilon q^m-\varepsilon q^{m-1} \\ S_{2m}(a)=q^{2m-1}\qquad\quad -\varepsilon q^{m-1} \qquad (a\neq 0) \end{cases}$$

(3)
$$\begin{cases} S_{2m+1}(0)=q^{2m} \\ S_{2m+1}(a)=q^{2m}+\varepsilon q^m \qquad (0\neq a,\ \exists\, c\in K \text{使} a=c^2) \\ S_{2m+1}(b)=q^{2m}-\varepsilon q^m \qquad (0\neq b,\text{但} b\neq c^2,\ \forall c\in K) \end{cases}$$

其中$\varepsilon=(-1)^{m\left(\frac{q-1}{2}\right)}$，$m$爲正整數，但(3)式中可爲$m=0$。以下證明其結果。

二、預備定理

定理1：若$0\neq a$，$b\in K$，而$b/a=c^2$，$c\in K$，則$S_n(a)=S_n(b)$.

證明：設 $x_1^2+x_2^2+\cdots+x_n^2=a$ 之一組解爲 $(d_1, d_2, \cdots, d_n)$ ，$d_i \in K$

即 $d_1^2+d_2^2+\cdots+d_n^2=a$

則 $(cd_1)^2+(cd_2)^2+\cdots+(cd_n)^2=c^2a=b$

故 $(cd_1, cd_2, \cdots, cd_n)$ 必爲

$x_1^2+x_2^2+\cdots+x_n^2=b$

之一組解。其逆亦眞，故 $S_n(a)=S_n(b)$

系：設 $S=\{a \in K : a \neq 0, \exists c \in K \text{使} a=c^2\}$

$N=\{b \in K : b \neq 0, b \neq c^2, \forall c \in K\}$

則 $a \in S \Rightarrow S_n(a)=S_n(1)$

$b, b' \in N \Rightarrow S_n(b)=S_n(b')$

證明：由定理 1 ，易知

$$c^2=a=\frac{a}{1}, \quad S_n(a)=S_n(1)$$

因 $K-\{0\}$ 爲 K 的乘法群，而 S 爲其部分群，其個數爲 $\frac{q-1}{2}$

故 N 爲其陪集（Coset），即 $N=Sb$ ，$b \in N$

若 $b, b' \in N$ ，則 $b/b'=c^2 \in S$ ，$\therefore S_n(b)=S_n(b')$

定理 2 ：$S_2(a) \geq 1$ ，$\forall a \in K$

證明：$S_2(0) \geq 1$ ，$S_2(1) \geq 1$ ，$\therefore a \in S \quad S_2(a) \geq 1$ 。

由是若 $S_2(b)=0$ ，則 $b \in N$ ，故由定理 1 ，系得 $b \in N$ $S_2(b)=0$ 。即 N 之元素不能爲 K 之二元素之平方和，換言之 $\{0\} \cup S$ 對於 K 的加法有封閉性，而 S 對於 K 的乘法成群，故 $\{0\} \cup S$ 爲 K 的部分體。但其元素個數爲

$\frac{q+1}{2}=\frac{p^r+1}{2}>p^{r-1}$ ，故矛盾。$\therefore S_2(b) \geq 1$ ；$\forall b \in N$

定理 3 ：若 $0 \neq a, b \in K$ ，則 $S_{2m}(a)=S_{2m}(b)$

證明：由定理 2 知，$\exists c, d \in K$ ，使 $c^2+d^2=b/a$

現令 $\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\triangle$，而對於 $x_1^2+x_2^2+\cdots+x_{2m}^2=a$ 之解作其矩陣爲

$$\begin{pmatrix} \triangle & 0 & \cdots & 0 \\ 0 & \triangle & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \triangle \end{pmatrix}$$

之形式之變換。則其結果必爲 $x_1^2+x_2^2+\cdots+x_{2m}^2=b$ 之解，而此變換成爲前方程式所有之解至後方程式所有之解的 $1-1$ 對應。

故 $S_{2m}(a)=S_{2m}(b)$

註：若 $(\alpha_1,\alpha_2,\cdots,\alpha_{2m})$ 爲 $x_1^2+x_2^2+\cdots+x_{2m}^2=a$ 之解

則 $$\begin{pmatrix} \triangle & 0 & \cdots & 0 \\ 0 & \triangle & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \triangle \end{pmatrix}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2m} \end{pmatrix}=\begin{pmatrix} c\alpha_1 & +d\alpha_2 \\ -d\alpha_1 & +c\alpha_2 \\ c\alpha_3 & +d\alpha_4 \\ -d\alpha_3 & +c\alpha_4 \\ \cdots\cdots & \cdots\cdots \\ c\alpha_{2m-1} & +d\alpha_{2m} \\ -d\alpha_{2m-1} & +c\alpha_{2m} \end{pmatrix}$$

$$(c\alpha_1+d\alpha_2)^2+(-d\alpha_1+c\alpha_2)^2+(cd_3+d\alpha_4)^2+(-d\alpha_3+c\alpha_4)^2+\cdots\cdots+(c\alpha_{2m-1}+d\alpha_{2m})^2+(-d\alpha_{2m-1}+c\alpha_{2m})^2$$

$$=(c^2+d^2)(\alpha_1^2+\alpha_2^2+\cdots+\alpha_{2m}^2)$$

$$=(c^2+d^2)a=b$$

定理4：$\sum_{c\in k} S_n(c)=q^n$

證明：$(\alpha_1,\alpha_2,\cdots,\alpha_n)\in K^n \quad \alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2\in K$

$\therefore \sum_{c\in k} S_n(c)=q^n$

定理5：若 $S_{2m}(0)=q^{2m-1}+\varepsilon q^m-\varepsilon q^{m-1}$ 爲眞

則 $S_{2m}(a)=q^{2m-1}-\varepsilon q^{m-1}$，$a\neq 0$ 亦必爲眞。

證明：由定理3，知 $\sum_{0\neq c\in k} S_{2m}(c)=(q-1)S_{2m}(a), a\neq 0$

由定理4知 $q^{2m}=\sum_{c\in k} S_{2m}(c)$

$$=S_{2m}(0)+(q-1)S_{2m}(a),\ a\neq 0$$

$$S_{2m}(0)=q^{2m-1}+\varepsilon q^{m}-\varepsilon q^{m-1}$$

$$\therefore S_{2m}(a)=\frac{1}{q-1}(q^{2m}-q^{2m-1}-\varepsilon q^{m}+\varepsilon q^{m-1})$$

$$=q^{2m-1}-\varepsilon q^{m-1}$$

定理6：$S_n(d)=\sum_{c\in k} S_{n-r}(c)S_r(d-c)$，$1\leq r\leq n-1$

證明：若 $\alpha_1^2+\alpha_2^2+\cdots+\alpha_n^2=d$

則 $\alpha_1^2+\alpha_2^2+\cdots+\alpha_r^2=d-(\alpha_{r+1}^2+\cdots+\alpha_n^2)$

$c=\alpha_{r+1}^2+\cdots+\alpha_n^2\in K$

故上列結果顯然成立。

三、公式的證明

利用以上各預備定理及數學歸納法證明(2)及(3)之公式。

首先證明(2)

（I） $m=1$ 之情形

(a) 若 $q-1\equiv 0\pmod 4$，則 $\varepsilon=1$

因 $\exists c\in K$，使 $c^2=-1$，

故 $x_1^2+x_2^2=0$ 之解爲（0，0），及（d，$\pm cd$），$0\neq d\in K$

故 $S_2(0)=2q-1$，即 $m=1$ 時(2)的第一式能成立。故由預備定理5知其第二式亦成立。

即 $S_2(a)=q-1$，$a\neq 0$

(b) 若 $q-1\equiv 0\pmod 4$ 則 $\varepsilon=-1$

此時在 K 中無適合 $c^2=-1$ 的 $c\in K$ 存在（因 $p>2$ 爲質數，故 p 爲奇數，故 $q-1=p^r-1$ 爲偶數，$K-\{0\}$ 爲乘法群，

其元素個數爲$q-1$，故$c\neq 0$，$c\in K$　$c^{q-1}=1$，$q-1\equiv 0\ (\mathrm{mod.}\ 4)$）於是$x_1^2+x_2^2=0$僅有一解（0，0）即$S_2(0)=1$，故滿足(2)的第一式，由定理5知第二式亦能滿足，即

$$S_2(a)=q+1,\quad a\neq 0$$

(Ⅱ) 假設對於整數m，(2)式能成立，欲推證$m+1$的情形。

利用預備定理6，設其$r=2$，

仍然設$\varepsilon=(-1)^{m\left(\frac{q-1}{2}\right)}$，另設$\varepsilon'=(-1)^{\frac{q-1}{2}}$，由預備定理3知

$$S_{2m+2}(0)=\sum_{c\in k} S_{2m}(c)S_2(-c)$$

$$\begin{aligned}
&=S_{2m}(0)S_2(0)+(q-1)S_{2m}(1)S_2(1)\\
&=(q^{2m-1}+\varepsilon q^m-\varepsilon q^{m-1})(q+\varepsilon' q-\varepsilon')\\
&+(q-1)(q^{2m-1}-\varepsilon q^{m-1})(q-\varepsilon')\\
&=(q^{2m-1}-\varepsilon q^{m-1})(q+\varepsilon' q-\varepsilon'+q^2-q-\varepsilon' q+\varepsilon')+\varepsilon q^m(q+\varepsilon' q-\varepsilon')\\
&=(q^{2m-1}-\varepsilon q^{m-1})q^2+\varepsilon q^m(q+\varepsilon' q-\varepsilon')\\
&=q^{2m+1}+\varepsilon\varepsilon' q^{m+1}-\varepsilon\varepsilon' q^m\\
&=q^{2m+1}+(-1)^{(m+1)\left(\frac{q-1}{2}\right)}q^{m+1}\\
&\quad-(-1)^{(m+1)\left(\frac{q-1}{2}\right)}q^m
\end{aligned}$$

故(2)之第一式對於$m+1$時亦成立。

由定理5知第二式亦必成立。

其次證明(3)

顯然

$S_1(0)=1$

$S_1(a)=2$　若$0\neq a\in K$，而$\exists c\in K$使$a=c^2$

$S_1(b)=0$　若$0\neq b\in K$，而$b\neq c^2$，$\forall c\in K$

以上結果滿足(3)式中$m=0$的情形，故$m=0$時(3)式成立。

由定理6知

$$S_{2m+1}(d)=\sum_{c\in k} S_{2m}(c)S_1(d-c)$$

故 $S_{2m+1}(0)=S_{2m}(0)S_1(0)+\sum_{a\in s} S_{2m}(-a)S_1(a)$

$$=S_{2m}(0)S_1(0)+\frac{q-1}{2}S_{2m}(1)S_1(1)$$

$$=(q^{2m-1}+\varepsilon q^m-\varepsilon q^{m-1})+(q-1)(q^{2m-1}-\varepsilon q^{m-1})$$

$$=q^{2m}$$

若 $0\neq b\in K$，$b\neq c^2$，$c\in K$時

$$S_{2m+1}(b)=\sum_{c\in k} S_{2m}(c)S_1(b-c)$$

$$=S_{2m}(1)\Big(\sum_{0\neq c\in k} S_1(b-c)\Big)$$

（因 $c=0$，則 $S_1(b-c)S_1(b)=0$，$c\neq 0$，$S_{2m}(c)=S_{2m}(1)$）

$$\therefore S_{2m+1}(b)=(q^{2m-1}-\varepsilon q^{m-1})\left(1+\frac{q-1}{2}\cdot 2\right)$$

$$=q^{2m-1}-\varepsilon q^m$$

若 $0\neq a=c$，$c\in K$，由定理 1 系知 $S_{2m+1}(a)=S_{2m+1}(1)$ 再利用定理 5 得

$$S_{2m+1}(1)=S_{2m}(0)S_1(1)+S_{2m}(1)S_1(0)+\sum_{\substack{c\in k\\ c\neq 0,1}} S_{2m}(c)S_1(1-c)$$

$$=2S_{2m}(0)+S_{2m}(1)+\left(\frac{q-1}{2}-1\right)S_{2m}(1)S_1(1)$$

（因 $S_1(b)=0$，$b\neq c^2$，$c\in k$）

$$=2S_{2m}(0)+S_{2m}(1)+(q-3)S_{2m}(1)$$

$$=2(q^{2m-1}+\varepsilon q^m-\varepsilon q^{m-1})+(q-2)$$

$$(q^{2m-1}-\varepsilon q^{m-1})$$
$$=q^{2m}+\varepsilon q^{m}$$

由上列可知(3)式成立。

以上結果可利用到$x_1, x_2, \cdots, x_n$之二次齊次多項式等於一常數$a\in k^*$的方程式在有限體k之解的個數問題上。

參考資料

1. A. Weil: Number of solutions of equations in finite fields. Bull American Math. Soc. 55 (1949), 497-508
2. L. Carlitz: The number of solutions of some special equations in a finite field. Pacific, J. Math. 4 (1954), 207-217.
3. I. N. Herstein: Topies in Algebra. University of Chicago (1969). 167-215.