Journal of İstanbul Kültür University
2002/1, pp. 31-36

On Gaussian Sums over Finite Fields II

Neşe Yelkenkaya*

Abstract
Let F_q:=GF(q) be a finite field of order q=p^s for some $s \in \mathbf{N}$, where p is an odd prime, and F_q=F(θ), where F=F_p. Let F_q^* =F_q-{0}=$\langle \rho \rangle$ and K:=$\langle \rho^2 \rangle$. Let $\Psi = \Psi_{h_1,\ldots,h_s}$ be a non-trivial irreducible character of the additive group of F_q such that $0 \leq h_1,\ldots,h_s \leq p-1$; $(h_1,\ldots,h_s) \neq (0,\ldots,0)$ and $\Psi(\beta) = \varepsilon^{k_1h_1+\ldots+k_sh_s}$ where $\beta = k_1 + k_2\theta + \ldots + k_s\theta^{s-1}$; $0 \leq k_1,\ldots,k_s \leq p-1$; ε=cos(2π/p)+ **sin** (2π/p) and ζ be the irreducible character of the multiplicative group F_q^* with $\zeta(\rho^i) = (-1)^i$ for any $i \in \mathbf{Z}$.
In this paper, the values of $\tau_{(s)}(\zeta;\Psi) := \sum_{0 \neq \beta \in F_q} \zeta(\beta)\Psi(\beta)$; $x_{(s)}(\Psi) := \sum_{\beta \in K} \Psi(\beta)$ and $y_{(s)}(\Psi) := \sum_{\beta \in \rho K} \Psi(\beta)$ have been detemined for the irreducible additive character $\Psi = \Psi_{0,\ldots,0,1}$, by counting square elements satisfying certain conditions in F_q^*.

Özet
p bir tek asal sayı olmak üzere F_q:=GF(q), mertebesi q=p^s olan bir sonlu cisim ve F_q=F(θ) olsun; burada $s \in \mathbf{N}$, F=F_p dir. F_q^* =F_q-{0}=$\langle \rho \rangle$ ve K:=$\langle \rho^2 \rangle$ olsun. $\Psi = \Psi_{h_1,\ldots,h_s}$ ile F_q nun toplam grubunun $\Psi(\beta) = \varepsilon^{k_1h_1+\ldots+k_sh_s}$ şeklindeki trivial olmayan indirgenemez karakterini gösterelim; burada $0 \leq h_1,\ldots,h_s \leq p-1$; $(h_1,\ldots,h_s) \neq (0,\ldots,0)$; $\beta = k_1 + k_2\theta + \ldots + k_s\theta^{s-1}$; $0 \leq k_1,\ldots,k_s \leq p-1$; ε=cos(2π/p)+ isin(2π/p) dir. ζ, F_q^* çarpım grubunun $\zeta(\rho^i) = (-1)^i$, $i \in \mathbf{Z}$ şeklindeki indirgenemez karakterini göstersin.
Bu çalışmada $\tau_{(s)}(\zeta;\Psi) := \sum_{0 \neq \beta \in F_q} \zeta(\beta)\Psi(\beta)$; $x_{(s)}(\Psi) := \sum_{\beta \in K} \Psi(\beta)$ ve $y_{(s)}(\Psi) := \sum_{\beta \in \rho K} \Psi(\beta)$ nin $\Psi = \Psi_{0,\ldots,0,1}$ karakteri için aldığı değerler, F_q^* içinde belirli koşulları sağlayan kare elemanlar sayılarak, hesaplanmıştır.

Keyword: Gauss sums.

* Department of Matematics, İstanbul Kültür Üniversity 34510 Şirinevler/İSTANBUL

Introduction

Let p be an odd prime number and F_q:=GF(q) be a finite field of order $q=p^s$ for some $s\in\mathbf{N}$. Then $F_q=F(\theta)$ with $f(\theta)=0$, where $F=F_p$;

$$f(x)=\mathrm{Irr}(\theta,x,F)=x^s+a_{s-1}x^{s-1}+\ldots+a_1x+a_0$$

is the minimal polynomial of θ over F. Thus

$$F_q=F\oplus F\theta\oplus\ldots\oplus F\theta^{s-1}$$

becomes an additive abelian group. $F_q^*=F_q-\{0\}$, the multiplicative group of the field F_q, is cyclic of order q-1. Let $F_q^*=\langle\rho\rangle$, for some generator ρ.

$$F_q^*=K\cup\rho K \qquad \text{(disjoint)}$$

where $K=\langle\rho^2\rangle$. $r:=\rho^u$ is a generator of F^* where $u=(p^s-1)/(p-1)$.

Let $\Psi=\Psi_{h_1,\ldots,h_s}$ be a non-trivial irreducible additive character of the additive group F_q such that $0\le h_1,\ldots,h_s\le p-1$, $(h_1,\ldots,h_s)\neq(0,\ldots,0)$ and

$$\Psi(\beta)=\varepsilon^{k_1h_1+\ldots+k_sh_s},$$

where $\beta=k_1+k_2\theta+\ldots+k_s\theta^{s-1}$, $0\le k_1,\ldots,k_s\le p-1$; $\varepsilon=\cos(2\pi/p)+\mathbf{i}\sin(2\pi/p)$. Let ζ be the irreducible character of the multiplicative group F_q^* with

$$\zeta(\rho^i)=(-1)^i \text{ for any } i\in\mathbf{Z}.$$

Now define

$$\tau_{(s)}(\zeta;\Psi):=\sum_{0\neq\beta\in F_q}\zeta(\beta)\Psi(\beta);$$

which is called a **Gaussian sum** over the field Fq with respect to ζ, Ψ and θ. Let

$$x_{(s)}(\Psi):=\sum_{\beta\in K}\Psi(\beta) \text{ and } y_{(s)}(\Psi):=\sum_{\beta\in\rho K}\Psi(\beta).$$

Property 1 (See [1]). $\tau_{(s)}=(\zeta,\Psi)=\sigma\sqrt{q}$, $x_{(s)}(\Psi)=-\frac{1}{2}(-\sigma\sqrt{q}+1)$ and $y_{(s)}(\Psi)=-\frac{1}{2}(\sigma\sqrt{q}+1)$ with $\sigma=\pm\eta$, where

$$\eta=\begin{cases}+1,\text{if } q\equiv 1\pmod 4\\ +\mathbf{i},\text{if } q\equiv 3\pmod 4\end{cases} \qquad ;\mathbf{i}=\sqrt{-1}$$

we shall keep this notation for η throughout this paper.

From now on we fix $\Psi=\Psi_{0,\ldots,0,1}$ and write $\tau_{(s)}$, $x_{(s)}$, $y_{(s)}$ instead of $\tau_{(s)}=(\zeta;\Psi)$, $x_{(s)}(\Psi)$, $y_{(s)}(\Psi)$ and we call $\tau_{(s)}$ the **normed Gaussian sum** over the field F_q with respect to $\Psi=\Psi_{0,\ldots,0,1}$.

Property 2 (Gauss) (See [1]). If s=1 then $\sigma=\eta$, i.e., $\tau_{(1)}=\eta\sqrt{p}$, $x_{(1)}=-\frac{1}{2}(-\eta\sqrt{p}+1)$ and $y_{(1)}=-\frac{1}{2}(\eta\sqrt{p}+1)$.

Lemma 1. Let s=2n+1 for some $n\in\mathbf{N}$. Then $\tau_{(s)}=\sigma\sqrt{q}$, $x_{(s)}=-\frac{1}{2}(-\sigma\sqrt{q}+1)$, $y_{(s)}=-\frac{1}{2}(\sigma\sqrt{q+1})$ is equivalent to $u=\frac{1}{2}(p^{2n}-1)$, $v=\frac{1}{2}p^{n}(\overline{\eta}\sigma+p^{n})$, $w=\frac{1}{2}p^{n}(-\overline{\eta}\sigma+p^{n})$ where u, v and w are the numbers of the square elements $0\neq\beta=\sum_{i=1}^{s}b_i\theta^{i-1}$ with $b_s=0$, $b_s=1$ and $b_s=r$ respectively and $\overline{\eta}$ denotes the complex conjugate of η.

Proof. It can be shown by using the same idea in the proof of Lemma 4 in [1].

Lemma 2. Let

$$P_n:=\{(\lambda_0,\lambda_1,\ldots,\lambda_n;\mu_1,\ldots,\mu_n)\in F^{(2n+1)}:\lambda_0^2+2\sum_{i=1}^{n}\lambda_i\mu_i+\sum_{0\le j<k\le n}a_{jk}\lambda_j\mu_k+\sum_{i=1}^{n}d_i\mu_i^2+\sum_{1\le j<k\le n}c_{jk}\mu_j\mu_k=1\}$$

where a_{jk}, $c_{jk}\in F$ $(1\le j<k\le n)$; $d_i\in F$ (i=1,…,n) and $F^{(2n+1)}=F\times\ldots\times F$, $n\in\mathbf{N}$, here the number of product is 2n+1 times. Then $|P_n|=p^n(p^n+1)$.

Proof. (Induction on n)

1. Let n=1. Then we have the equation,

$$\lambda_0^2+2\lambda_1\mu_1+a_{01}\lambda_0\mu_1+d_1\mu_1^2=1$$

defined over F. Then

$|P_1|=|\{(\lambda_0,\lambda_1,\mu_1)\in P_1:\mu_1=0,\lambda_1\in F\}|+|\{(\lambda_0,\lambda_1,\mu_1)\in P_1:\mu_1\neq 0,\lambda_0\in F\}|=$
2p+p(p-1)=p(p+1) as required.

2. Assume n≥2 and suppose the claim is true for (n-1). Then

$$\begin{aligned}|P_n|&=|\{(\lambda_0,\ldots,\lambda_n;\mu_1,\ldots,\mu_n)\in P_n:\mu_n\neq 0;\lambda_0,,\ldots,\lambda_{n-1};\mu_1,\ldots,\mu_{n-1}\in F\}|+\\&|\{(\lambda_0,\ldots,\lambda_n;\mu_1,\ldots,\mu_n)\in P_n:\mu_n=0;\lambda_n\in F;(\lambda_0,,\ldots,\lambda_{n-1};\mu_1,\ldots,\mu_{n-1})\in P_{n-1}\}|\\&=(p-1)p^{2n-1}+p|P_{n-1}|=p^n(p^n+1)\end{aligned}$$

any $d\in<r^2>$.

Note: The assertion in Lemma 2 remains true if 1 in the equation, replaced by

Lemma 3. Let s=2n+1, $n\in\mathbf{N}$. Then the number of square elements $\beta=\sum_{i=1}^{s}b_i\theta^{i-1}$, with $b_s=1$ equals $\frac{1}{2}p^n(p^n+1)$.

Proof. Any element $0 \neq \gamma \in F_q$ can be written in the form

$$\gamma = \lambda_n + \sum_{i=0}^{n-1} \lambda_i \theta^{n-i} + \sum_{j=1}^{n} \mu_j \theta^{n+j}$$

with $(\lambda_0, \lambda_1, \ldots, \lambda_n; \mu_1, \ldots, \mu_n) \neq (0,0,\ldots,0)$. Set $\gamma^2 = \sum_{i=1}^{s} c_i \theta^{i-1}$. Then by making use of $\theta^s = \theta^{2n+1} = -a_0 - a_1\theta - \ldots - a_{2n}\theta^{2n}$, $a_0 \neq 0$; we have

$$c_s = \lambda_0^2 + 2\sum_{i=1}^{n} \lambda_i \mu_i + \sum_{0 \le j < k \le n} a_{jk} \lambda_j \mu_k + \sum_{i=1}^{n} d_i \mu_i^2 + \sum_{1 \le j < k \le n} c_{jk} \mu_j \mu_k$$

for some $a_{jk}, c_{jk} \in F$ $(1 \le j < k \le n)$; $d_i \in F$ (i=1,…,n). If $0 \neq \gamma \in F_q$ then $\gamma \neq -\gamma$ but $\gamma^2 = (-\gamma)^2$. Then we have

$$\text{v} = \frac{1}{2}\left|P_n\right| = \frac{1}{2} p^n (p^n + 1)$$

with P_n defined in Lemma 2.

Corollary 4. If s=2n+1, n∈**N** then $\tau_{(s)} = \eta\sqrt{q}$, $\text{x}_{(s)} = -\frac{1}{2}(-\eta\sqrt{q} + 1)$, $\text{y}_{(s)} = -\frac{1}{2}(\eta\sqrt{q} + 1)$ where

$$\eta = \begin{cases} +1, \text{if } q \equiv 1 \pmod 4 \\ +\mathbf{i}, \text{if } q \equiv 3 \pmod 4 \end{cases} \quad ; \mathbf{i} = \sqrt{-1}.$$

Now we shall discuss the remaining case s=2n, n∈**N**.

Lemma 5. Let s=2n. Then $\eta = 1$ and $\sigma = \pm 1$; $\tau_{(s)} = \sigma\sqrt{q}$, $\text{x}_{(s)} = -\frac{1}{2}(-\sigma\sqrt{q} + 1)$, $\text{y}_{(s)} = -\frac{1}{2}(\sigma\sqrt{q + 1})$ is equivalent to $\text{u} = \frac{1}{2p}\left[(q-p) + \sigma(p-1)\sqrt{q}\right]$ and $\text{v} = \frac{1}{2p}\left[q - \sigma\sqrt{q}\right]$,

where u and v are the numbers of the square elements $0 \neq \beta = \sum_{i=1}^{s} b_i \theta^{i-1}$ with b_s=0 and b_s=1 respectively.

Proof. It can be shown by using the same idea in the proof of Lemma 8 in [1].

Lemma 6. Let $P_n := \{(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}; \mu_0, \ldots, \mu_{n-1}) \in F^{2n}$ -$\{(0,\ldots,0)\}$: $2\sum_{i=0}^{n-1} \lambda_i \mu_i + \sum_{0 \le j < k \le n-1} a_{jk} \lambda_j \mu_k + \sum_{i=0}^{n-1} d_i \mu_i^2 + \sum_{0 \le j < k \le n-1} c_{jk} \mu_j \mu_k = 0\}$ where $a_{jk}, c_{jk} \in F$ $(0 \le j < k \le n-1)$; $d_i \in F$ $(i = 0, \ldots, n-1)$ and n∈**N**. Then

$$\left|P_n\right| = \text{p}^{2n-1} - 1 + (\text{p}-1)\text{p}^{n-1}.$$

Proof. (Induction on n)

1. Let n=1. Then we have the equation

$$2\lambda_0\mu_0 + d_0\mu_0^2 = 0$$

defined over F. Then

$|P_1| = |\{(\lambda_0, \mu_0) \in P_1 : \mu_0 = 0, \lambda_0 \in F - \{0\}| + |\{(\lambda_0, \mu_0) \in P_1 : \mu_0 \neq 0\}| =$
(p-1)+(p-1)=2(p-1) as required.

2. Assume $n \geq 2$ and suppose the claim is true for (n-1). Then

$$|P_n| = |\{(\lambda_0,\ldots,\lambda_{n-1};\mu_0,\ldots,\mu_{n-1}) \in P_n : \mu_{n-1} \neq 0; \lambda_0,\ldots,\lambda_{n-2};\mu_0,\ldots,\mu_{n-2} \in F\}| +$$
$$|\{(\lambda_0,\ldots,\lambda_{n-1};\mu_0,\ldots,\mu_{n-1}) \in P_n : \mu_{n-1} = 0; \lambda_{n-1} \neq 0; \lambda_i = \mu_i = 0 \;\; for\ all\ i = 0,1,\ldots,n-2\}| +$$
$$|\{(\lambda_0,\ldots,\lambda_{n-1};\mu_0,\ldots,\mu_{n-1}) \in P_n : \mu_{n-1} = 0; \lambda_{n-1} \in F; (\lambda_0,\ldots,\lambda_{n-2};\mu_0,\ldots,\mu_{n-2}) \in P_{n-1}\}|$$

$=(p-1)p^{2n-2}+(p-1)+p|P_{n-1}| = (p-1)p^{2n-2}+(p-1)+p(p^{2n-3}-1+(p-1)p^{n-2})=$
$p^{2n-1}-1+(p-1)p^{n-1}$.

Lemma 7. Let s=2n, $n \in \mathbf{N}$. Then the number u of the square elements $0 \neq \beta = \sum_{i=1}^{s} b_i\theta^{i-1}$ with $b_s=0$ equals $\frac{1}{2}$ $[p^{2n-1}-1+(p-1)p^{n-1}]$, where $\theta^s = \theta^{2n} = -a_0 - a_1\theta - \ldots - a_{2n-1}\theta^{2n-1}$, $a_0 \neq 0$.

Proof. Any element $0 \neq \gamma \in F_q$ can be written in the form

$$\gamma = \sum_{i=0}^{n-1}\lambda_i\theta^{n-1-i} + \sum_{i=0}^{n-1}\mu_i\theta^{n+i}$$

with $(\lambda_0,\ldots,\lambda_{n-1};\mu_0,\ldots,\mu_{n-1}) \neq (0,0,\ldots,0)$. Set $\gamma^2 = \sum_{i=1}^{s} c_i\theta^{i-1}$. Then we have

$$c_s = 2\sum_{i=0}^{n-1}\lambda_i\mu_i + \sum_{0\leq j<k\leq n-1} a_{jk}\lambda_j\mu_k + \sum_{i=0}^{n-1} d_i\mu_i^2 + \sum_{0\leq j<k\leq n-1} c_{jk}\mu_j\mu_k = 0\}$$ for some $a_{jk}, c_{jk} \in F$ $(0 \leq j < k \leq n-1)$; $d_i \in F$ $(i = 0,\ldots,n-1)$. If $0 \neq \gamma \in F_q$ then $\gamma \neq -\gamma$ but $\gamma^2 = (-\gamma)^2$. Then we have

$u = \frac{1}{2}|P_n| = \frac{1}{2}$ $[p^{2n-1}-1+(p-1)p^{n-1}]$, with P_n defined in Lemma 6.

Corollary 8. If s=2n, $n \in \mathbf{N}$ then

$$\tau_{(s)} = \sqrt{q},\;\; x_{(s)} = -\frac{1}{2}(-\sqrt{q}+1),\;\; y_{(s)} = -\frac{1}{2}(\sqrt{q}+1).$$

Reference

[1] N.Yelkenkaya, (1996/97)"On Gaussian Sums Over Finite Fields" *İst.Üniv. Fen Fak. Mat. Derg.* **55/56** , (1996/97), 85-97.