İstanbul Üniv. Fen Fak. Mat. Dergisi 55 - 56 (1996 - 1997), 85-97

ON GAUSSIAN SUMS OVER FINITE FIELDS

NEŞE YELKENKAYA

Abstract

In this paper, it has been determined the sings of normed Gaussian sums over finite fields.

INTRODUCTION

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

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

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 elementary abelian group. On the other hand $F_q^* = F_q \setminus \{0\}$, the multiplicative group of the field F_q, is cyclic of order $q-1$ and $F_q^* =< \rho >$ for some generator p. Let $K :=< \rho^2 >$ then

$$F_q^* = K \cup \rho K \quad (disjoint).$$

Now $r := \rho^u$ is a generator of F^* where $u = (p^s-1)/(p-1)$, i.e., $F^* =< r >$. Let $\Psi = \Psi_{h_1,\ldots,h_s}$ be a non-trivial irreducible character of additive group of F_q which is also called additive character such that $0 \le h_1, \ldots, h_s \le p-1$; $(h_1, \ldots, h_s) \neq (0, \ldots, 0)$,

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

where $\beta = k_1 1_F + k_2\theta + \ldots + k_s\theta^{s-1}$; $0 \le k_i \le p-1$, $i = 1, \ldots, s$; $\varepsilon = \cos(2\pi/p) + i\sin(2\pi/p)$ and by abuse of notation we may also write $k_1, \ldots, k_s \in F$. On the other hand, let ζ be the irreducible character of the multiplicative group F_q^* which is also called multiplicative character with

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

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 F_q with respect to ζ, Ψ and θ. If $s = 1$ then $\tau_1(\zeta;\Psi)$ becomes the usual Gaussian sum $\tau_{h_1} = \sum_{1\leq x\leq p-1} \left(\frac{x}{p}\right) \varepsilon^{h_1 x}$, where $\left(\frac{x}{p}\right)$ is the Legendre symbol and ζ turns out to be the so called Legendre symbol.

Lemma 1. $\tau_{(s)}^2(\zeta;\Psi) = (-1)^{(q-1)/2}q$.

Proof.

1. $\zeta(-1) = (-1)^{(q-1)/2}$.
2. As ζ is a non-trivial irreducible multiplicative character of F_q^*, we have $\sum_{0\neq\beta\in F_q} \zeta(\beta) = 0$.
3. As Ψ is non-trivial irreducible additive character of F_q, we also have $\sum_{0\neq\beta\in F_q} \Psi(\beta) = -1$.
4. Now taking $\beta\delta = \gamma$

$$\begin{aligned}
\tau_{(s)}^2(\zeta;\Psi) &= \sum_{0\neq\beta,\gamma\in F_q} \zeta(\beta\gamma)\Psi(\beta+\gamma) = \sum_{0\neq\beta,\delta\in F_q} \zeta(\delta)\Psi[\beta(1+\delta)] \\
&= \zeta(-1)(q-1) + \sum_{0,-1\neq\delta\in F_q} \zeta(\delta) \sum_{0\neq\beta\in F_q} \Psi[\beta(1+\delta)] \\
&= (-1)^{(q-1)/2}q - \zeta(-1) - \sum_{0,-1\neq\delta\in F_q} \zeta(\delta) \\
&= (-1)^{(q-1)/2}q - \sum_{0\neq\delta\in F_q} \zeta(\delta) = (-1)^{(q-1)/2}q
\end{aligned}$$

as desired.

Note. By Lemma 1, $\tau_{(s)}^2(\zeta;\Psi)$ is independent of the choice of $\Psi \neq \Psi_{0,\ldots,0}$ and θ. And $\tau_{(s)}(\zeta;\Psi)$ is determined uniquely up to factor ±1.

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

Lemma 2. $\{x_{(s)}(\Psi), y_{(s)}(\Psi)\} = \{-\frac{1}{2}(-\eta\sqrt{q}+1), -\frac{1}{2}(\eta\sqrt{q}+1)\}$
where $\eta = \begin{cases} +1\ ; \text{if} \quad q \equiv 1 \pmod 4 \\ +\mathrm{i}\ ; \text{if} \quad q \equiv 3 \pmod 4 \end{cases}$; $\mathbf{i} = \sqrt{-1}$.
Note that we shall keep this notation for η throughout this paper.

Proof. As Ψ is a non-trivial irreducible additive character of F_q, we already know that

$$-1 = \sum_{0\neq\beta\in F_q} \Psi(\beta) = x_{(s)}(\Psi) + y_{(s)}(\Psi). \tag{1}$$

On the other hand by Lemma 1, $\tau_{(s)}(\zeta;\Psi)=\sigma\sqrt{q}$ with $\sigma=\mp\eta$. Thus

$$\sigma\sqrt{q}=\tau_{(s)}(\zeta;\Psi)=x_{(s)}(\Psi)-y_{(s)}(\Psi). \tag{2}$$

Therefore (1) and (2) yield the desired result:

$$x_{(s)}(\Psi)=-\frac{1}{2}(-\eta\sqrt{q}+1) \quad\text{and}\quad y_{(s)}(\Psi)=-\frac{1}{2}(\eta\sqrt{q}+1).$$

This completes the proof of the Lemma.

From now on we fix $\Psi=\Psi_{1,0,\dots,0}$ 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 finite field F_q. Note that $\tau_{(1)}=\tau$ is the usual normed Gaussian sum. To determine σ is an important problem which should be dealt with, next.

Lemma 3.(Gauss) If $s=1$ then $\sigma=\eta$; i.e. $\tau=\eta\sqrt{p}$,

$$x=x_{(1)}=-\frac{1}{2}(-\eta\sqrt{p}+1) \quad\text{and}\quad y=y_{(1)}=-\frac{1}{2}(\eta\sqrt{p}+1).$$

The concept -Gaussian sum- has been introduced by Gauss himself in order to prove his theorem on quatratic reciprocity and Gauss has also gave a proof of Lemma 3. There are some other proofs of this important theorem, but all of them are either long or require some deep results belonging to algebraic number theory. We give here the proof due to Kronecker stated in Borevich & Shafarevich, Number Theory, p.355 as exercises 13-16.

Assertion I. Let p be an odd prime and set $\varepsilon=\cos\frac{2\pi}{p}+\mathrm{i}\sin\frac{2\pi}{p}$. Let $\delta=\prod_{x=1}^{(p-1)/2}(\varepsilon^x-\varepsilon^{-x})$ then $\delta^2=(-1)^{(p-1)/2}p$. Thus δ^2 coincides with the square τ^2 of the Gaussian sum

$$\tau=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\varepsilon^x\,.$$

Proof. Since $\varepsilon^x-\varepsilon^{-x}=\mathrm{i}2\sin(2\pi x/p)$ for $x=1,\dots,(p-1)/2$

$$\delta=\mathrm{i}^{(p-1)/2}2^{(p-1)/2}\prod_{x=1}^{(p-1)/2}\sin(2\pi x/p)=\mathrm{i}^{(p-1)/2}|\delta|\,, \tag{3}$$

3-87

where $|\delta|$ denotes the absolute value of $\delta \in \mathbb{C}$. Thus

$$\delta^2 = (-1)^{(p-1)/2}|\delta^2| .$$

On the other hand,

$$|\delta^2| = \delta\bar{\delta} = \prod_{x=1}^{(p-1)/2} (\varepsilon^x - \varepsilon^{-x})(\varepsilon^{-x} - \varepsilon^x) = \prod_{x=1}^{(p-1)/2} (1 - \varepsilon^{-2x})(1 - \varepsilon^{2x}) .$$

Since $p \not| 2$ then $\mp 2, \mp 2.2, \ldots, \mp 2.(p-1)/2$ is a complete residue system with a complete resid system $\bmod(p)$, $1, 2, \ldots, p-1$. So that

$$|\delta^2| = \prod_{i=1}^{(p-1)} (1 - \varepsilon^i) = f(1) = p \qquad ($$

where $f(y) = y^{p-1} + y^{p-2} + \ldots + y + 1$. Thus we obtain the desired result

$$\delta^2 = (-1)^{(p-1)/2} p .$$

Assertion II. With the same notations, we have

$$(i) \quad \left(\frac{-2}{p}\right)\delta = \begin{cases} \sqrt{p} \text{ ; for } & q \equiv 1 \pmod 4 \\ +\mathrm{i}\sqrt{p} \text{ ; for } & q \equiv 3 \pmod 4 \end{cases} \quad ; \quad \mathrm{i} = \sqrt{-1} .$$

Further, setting $\lambda = 1 - \varepsilon$, we have that the congruence

$$(ii) \quad \left(\frac{-2}{p}\right)\delta = \left(\frac{p-1}{2}\right)! \lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}$$

holds in the order $\mathbb{Z}[\varepsilon]$.

Proof. (i). By (3) and (4) in the proof of Assertion I, $\delta = \mathrm{i}^{(p-1)/2}\sqrt{p}$, to prove (i), it enough to show that

$$u := \left(\frac{-2}{p}\right)\mathrm{i}^{(p-1)/2} = \begin{cases} +1 \text{ ; for } & p \equiv 1 \pmod 4 \\ +\mathrm{i} \text{ ; for } & p \equiv 3 \pmod 4 \end{cases}$$

If $p \equiv 1 \pmod 4$ then $p = 4n + 1$ for some $n \in \mathbb{N}$. In this case

$$u = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8}\mathrm{i}^{(p-1)/2} = +1 .$$

If $p \equiv 3 \pmod 4$ then $p = 4n + 3$ for some $n \in \mathbb{N} \cup \{0\}$. In this case

$$u = +\mathrm{i} .$$

(*ii*) Let $\lambda := 1 - \varepsilon$ then $\varepsilon = 1 - \lambda$ and $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\lambda]$. On the other hand,

$$f(y) = y^{p-1} + y^{p-2} + \ldots + y + 1 = \prod_{i=1}^{p-1}(y - \varepsilon^i) \text{ and } p = f(1) = \prod_{i=1}^{p-1}(1 - \varepsilon^i)\ .$$

Let $g(y) := \prod_{i=2}^{p-1}(1 - (1 - y)^i) \in \mathbb{Z}[y]$, $p = \lambda g(y)$; i.e. $p \equiv 0 \pmod{\lambda}$. By Euler's criterion

$$\left(\frac{-2}{p}\right) \equiv (-2)^{(p-1)/2} \pmod{p}$$

and

$$\left(\frac{-2}{p}\right) \underset{\mathbb{Z}[\lambda]}{\equiv} (-2)^{(p-1)/2} \pmod{\lambda}\ .$$

Thus,

$$\begin{aligned}
\left(\frac{-2}{p}\right)\delta &\underset{\mathbb{Z}[\lambda]}{\equiv} (-2)^{(p-1)/2} \prod_{x=1}^{(p-1)/2} ((1-\lambda)^x - (1-\lambda)^{p-x}) \\
&\underset{\mathbb{Z}[\lambda]}{\equiv} (-2)^{(p-1)/2} \prod_{x=1}^{(p-1)/2} ((p - 2x)\lambda + (\ldots)\lambda^2 + \ldots) \\
&\underset{\mathbb{Z}[\lambda]}{\equiv} (-2)^{2(p-1)/2} \left(\frac{p-1}{2}\right)!\lambda^{(p-1)/2} \\
&\underset{\mathbb{Z}[\lambda]}{\equiv} \left(\frac{p-1}{2}\right)!\lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}\ .
\end{aligned}$$

Because, $(-2)^{2(p-1)/2} \equiv 1 \pmod{p}$; i.e. $(-2)^{2(p-1)/2} \equiv 1 \pmod{\lambda}$,
$p = (1-\varepsilon)(1-\varepsilon^2)\ldots(1-\varepsilon^{p-1}) = \lambda^{p-1}h(\lambda)$ and $\left(\frac{p+1}{2}\right) = \left(\frac{p-1}{2}\right) + 1$.

Assertion III. We have the following congruence

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\varepsilon^x = \tau \equiv \left(\frac{p-1}{2}\right)!\lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}$$

in the ring $\mathbb{Z}[\varepsilon]$.

Proof. By Euler's criterion

$$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \pmod p$$

and by Wilson's theorem

$$\left(\frac{p-1}{2}\right)!(-1)^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (p-1)! \equiv -1 \pmod p \ ;$$

i.e.

$$\left(\frac{x}{p}\right) \underset{\mathbb{Z}\,[\lambda]}{\equiv} x^{(p-1)/2} \pmod{\lambda^{p-1}} \tag{5}$$

and

$$(-1)\frac{(-1)^{(p-1)/2}}{\left(\frac{p-1}{2}\right)!} \underset{\mathbb{Z}\,[\lambda]}{\equiv} \left(\frac{p-1}{2}\right)! \pmod{\lambda^{p-1}} \ . \tag{6}$$

$$\begin{aligned} \text{Set } \ g_m(y) &= y(y-1)\dots(y-m+1) \\ &= y^m + a_{m,m-1}y^{m-1} + \ldots + a_{m,1}y + a_{m,0} \in \mathbb{Z}\,[y] \end{aligned}$$

for $m = 1, 2, \ldots, x$; $a_{m,m} = 1$.

As we already know that

$$\sum_{x=1}^{p-1} x^m \equiv \begin{cases} 0 & \pmod p \quad \text{for} \quad 0 < m < p-1 \\ -1 & \pmod p \quad \text{for} \quad m = p-1 \ . \end{cases}$$

Now decomposing the sum $\sum\limits_{x=1}^{p-1} x^{(p-1)/2}(1-\lambda)^x$ into powers of λ, by (5) we have

$$\begin{aligned} \tau &\underset{\mathbb{Z}\,[\lambda]}{\equiv} \sum_{x=1}^{p-1} x^{(p-1)/2}(1-\lambda)^x \\ &\underset{\mathbb{Z}\,[\lambda]}{\equiv} \sum_{x=1}^{p-1} x^{(p-1)/2}[1 + (-1)\frac{x}{1}\lambda + \ldots (-1)^m \frac{g_m(x)}{m!}\lambda^m + \ldots] \ . \end{aligned}$$

Thus

$$\begin{aligned} \tau &\underset{\mathbb{Z}\,[\lambda]}{\equiv} \sum_{x=1}^{p-1} x^{(p-1)/2} + (-1)\sum_{x=1}^{p-1} x^{(p+1)/2}\lambda + \ldots + \\ &\quad +[(-1)^m \frac{1}{m!}\sum_{i=0}^{m} a_{m,i} \sum_{x=1}^{p-1} x^{\frac{p-1}{2}+i}]\lambda^m + \ldots \pmod{\lambda^{(p+1)/2}} \ ; \end{aligned}$$

6 - 30

i.e.

$$\tau \underset{\mathbb{Z}[\lambda]}{\equiv} (-1)^{(p-1)/2} \frac{1}{\left(\frac{p-1}{2}\right)!} a_{\frac{p-1}{2},\frac{p-1}{2}} \sum_{x=1}^{p-1} x^{p-1} \lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}$$

Then we obtain by (6) that

$$\tau \underset{\mathbb{Z}[\lambda]}{\equiv} \left(\frac{p-1}{2}\right)! \lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}} \ .$$

Assertion IV. Using two preceding assertions we get

$$\tau = \begin{cases} \sqrt{p}\,; \text{for} & q \equiv 1 \pmod 4 \\ +\mathrm{i}\sqrt{p}\,; \text{for} & q \equiv 3 \pmod 4 \end{cases} \quad ; \quad \mathrm{i} = \sqrt{-1} \, .$$

Proof. By Assertion I, $\tau^2 = \delta^2 = \left[\left(\frac{-2}{p}\right)\delta\right]^2$ so that

$$\tau \in \left\{ \left(\frac{-2}{p}\right)\delta, - \left(\frac{-2}{p}\right)\delta \right\} \ .$$

If $\tau = \left(\frac{-2}{p}\right)\delta$, by Assertion II, we obtain the desired result.

Assume that $\tau \neq \left(\frac{-2}{p}\right)\delta$. In this case by Assertion II and Assertion III

$$2\left(\frac{p-1}{2}\right)! \lambda^{(p-1)/2} \underset{\mathbb{Z}[\lambda]}{\equiv} 2\tau \underset{\mathbb{Z}[\lambda]}{\equiv} 0 \pmod{\lambda^{(p+1)/2}}$$

i.e. there is a polynomial $k(y) \in \mathbb{Z}[y]$ such that

$$2\left(\frac{p-1}{2}\right)! = \lambda k(\lambda) \ .$$

Thus,$\mathrm{N}(2\left(\frac{p-1}{2}\right)!) = \mathrm{N}(\lambda)\mathrm{N}(k(\lambda))$, since $\mathrm{N}(\lambda) = \mathrm{N}(1-\varepsilon) = f(1) = p$, $\mathrm{N}(k(\lambda)) \in \mathbb{Z}$ and $\mathrm{N}(2\left(\frac{p-1}{2}\right)!) = \left[2\left(\frac{p-1}{2}\right)!\right]^{p-1}$ we arrive at a contradiction $2\left(\frac{p-1}{2}\right)! \equiv 0 \pmod p$ where $\mathrm{N}(a) = \mathrm{N}_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(a)$ for $a \in \mathbb{Q}(\varepsilon) = \mathbb{Q}(\lambda)$.

Lemma 4. Let $s = 2n+1$ for some $n \in \mathbb{N}$. Then

$$\tau_s := \sigma\sqrt{q} \quad ; \quad x_{(s)} := -\frac{1}{2}[-\sigma\sqrt{q} + 1] \quad ; \quad y_{(s)} := -\frac{1}{2}[\sigma\sqrt{q} + 1]$$

⑦-31

is equivalent to

$$u = \frac{1}{2}(p^{2n} - 1) \quad ; \quad v = \frac{1}{2}p^n(\overline{\eta}\sigma + p^n) \quad ; \quad w = \frac{1}{2}p^n(-\overline{\eta}\sigma + p^n) \; ;$$

where u, v and w are the numbers of square elemets $0 \neq \beta = \sum_{i=1}^{s} b_i\theta^{i-1}$ with $b_1 = 0$, $b_1 = 1$ and $b_1 = r$ respectively and $\overline{\eta}$ denotes the complex conjugate of η.

Proof. 1. Since s is odd r is not a square in F_q; i.e. $r \notin < p^2 >$
2. By making use of 1, we have

$$\frac{1}{2}(q-1) \;=\; |K| = u + \frac{1}{2}(p-1)(v+w) \tag{7}$$

and

$$x(s) = -\frac{1}{2}[-\sigma\sqrt{q} + 1] = u + w(-1) + (v - w)\left[-\frac{1}{2}(-\eta\sqrt{p} + 1)\right] \tag{8}$$

hold since $x_{(1)} + y_{(1)} = -1$ and by Lemma 3, $x_{(1)} = -\frac{1}{2}(-\eta\sqrt{p} + 1)$. But then " (7) and (8) " is equivalent to

$$u = \frac{1}{2}(p^{2n} - 1) \quad ; \quad v = \frac{1}{2}p^n(\overline{\eta}\sigma + p^n) \quad ; \quad w = \frac{1}{2}p^n(-\overline{\eta}\sigma + p^n)$$

which can easily be checked.

Lemma 5: Let

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

where $0 \neq a, b_i, c_{jk}, d_{jk} \in F$; $(i = 1, 2, \ldots, n)$, $(1 \leq j < k \leq n)$ and $F^{(2n+1)} = F \times \ldots \times F$, $n \in \mathbb{N}$, here the number of product is $2n+1$ times. Then $|P_n| = p^n(p^n + 1)$.

Proof. (Induction on n)
1. Let $n = 1$ and consider the equation $\lambda_0^2 + a\lambda_1\mu_1 + b_1\mu_1^2 = 1$ defined over F. Then

$$\begin{aligned} |P_1| \;&=\; |\{(\lambda_0, \lambda_1, \mu_1) \in P_1 : \; \mu_1 = 0; \; \lambda_1 \in F\}| + \\ &+ |\{(\lambda_0, \lambda_1, \mu_1) \in P_1 : \; \mu_1 \neq 0; \; \lambda_0 \in F\}| = 2p + p(p-1) = p(p+1) \end{aligned}$$

as required.

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

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

as desired.
Note. The assertion in Lemma 5 remains true if we replace 1 in the equation by any $d \in < r^2 >$.

Lemma 6. Let $s = 2n+1, n \in \mathbb{N}$. Then the number v of the square elements $\beta = \sum\limits_{i=1}^{s} b_i\theta^{i-1}$ with $b_1 = 1$ equals $\frac{1}{2}p^n(p^n+1)$.

Proof. For any element $0 \neq \gamma \in F_q$ we can write

$$\gamma = \lambda_0 + \sum_{i=1}^{n}\lambda_i\theta^{n+1-i} + \sum_{j=1}^{n}\mu_j\theta^{n+j}$$

with $(\lambda_0, \lambda_1, \ldots, \lambda_n; \mu_1, \ldots, \mu_n) \neq (0, 0, \ldots, 0)$. Set $\gamma^2 = \sum\limits_{i=1}^{s} c_i\theta^{i-1}$. Then we have

$$c_1 = \lambda_0^2 + (-2a_0)\sum_{i=1}^{n}\lambda_i\mu_i + \sum_{i=1}^{n} b_i\mu_i^2 + \sum_{1\leq j<k\leq n} c_{jk}\lambda_j\mu_k + \sum_{1\leq j<k\leq n} d_{jk}\mu_j\mu_k$$

for some $b_i, .c_{jk}, d_{jk} \in F$; $(i = 1, \ldots, n)$; $(1 \leq j < k \leq n)$ by making use of $\theta^s = \theta^{2n+1} = -a_0 - a_1\theta - \ldots - a_{2n}\theta^{2n}$; $a_0 \neq 0$. For any $0 \neq \gamma \in F_q$ we have $\gamma \neq -\gamma$ and $\gamma^2 = (-\gamma)^2$ and this enables us to obtain

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

with P_n defined in Lemma 5.

Corollary 7. If $s = 2n+1,\ n \in \mathbb{N}$ then $\tau_{(s)} = \eta\sqrt{q}$, $x_{(s)} = -\frac{1}{2}(-\eta\sqrt{q}+1)$, $y_{(s)} = -\frac{1}{2}(\eta\sqrt{q}+1)$ where

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

Proof. Since $s = 2n+1,\ n \in \mathbb{N}$ then by Lemma 4 and Lemma **6** $\overline{\eta}\sigma = 1$; i.e. $\sigma = \eta$ and $\tau_{(s)} = \eta\sqrt{q}$, $x_{(s)} = -\frac{1}{2}(-\eta\sqrt{q}+1)$, $y_{(s)} = -\frac{1}{2}(\eta\sqrt{q}+1)$.

Now we shall discuss the remaining case $s = 2n$, $n \in \mathbb{N}$.

Lemma 8. Let $s = 2n$, $n \in \mathbb{N}$. Then $\eta = 1$ and $\sigma = \pm 1$;

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

is equivalent to

$$u = \frac{1}{2p}[(q-p)+\sigma(p-1)\sqrt{q}] \quad \text{and} \quad v = \frac{1}{2p}[q-\sigma\sqrt{q}]$$

where u and v are the numbers of the square elements $0 \neq \beta = \sum_{i=1}^{s-1} b_i\theta^{i-1}$ with $b_1 = 0$ and $b_1 = 1$ respectively.

Proof. 1. By Lemma 1, and s is even, i.e. $q \equiv 1 \pmod 4$ we get $\eta = 1$ and $\sigma = \pm 1$.

2. As $s = 2n$, $n \in \mathbb{N}$ and for $r = p^{(q-1)/(p-1)}$, $< r >= F^*$ it follows that r is a square in F_q^*.

3. By 2 we have the following

$$|K| = \frac{1}{2}(q-1) = u + (p-1)v \tag{9}$$

and

$$x_{(s)} = -\frac{1}{2}(-\sigma\sqrt{q}+1) = u - v \tag{10}$$

is equivalent to

$$u = (1/2p)[(q-p)+\sigma(p-1)\sqrt{q}] \quad \text{and} \quad v = (1/2p)[q-\sigma\sqrt{q}]$$

which can easly be verified.

Lemma 9. Let $P_n := \{(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}; \mu_0, \ldots, \mu_{n-1}) \in F^{(2n)} \backslash (0, \ldots, 0) : \lambda_0^2 + a\sum_{i=1}^{n-1} \lambda_i\mu_i + (-b)\mu_0^2 + \sum_{i=1}^{n-1} b_i\mu_i^2 + \sum_{1 \le j < k \le n-1} c_{jk}\lambda_j\mu_k + \sum_{0 \le j < k \le n-1} d_{jk}\mu_j\mu_k = 0\}$ where $0 \neq a, 0 \neq b$; $b_i, c_{jk} \in F$; $(i = 1, 2, \ldots, n-1)$, $(1 \le j < k \le n-1)$, $d_{jk} \in F$, $(0 \le j < k \le n-1)$, and $n \in \mathbb{N}$. Then

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

where $\left(\frac{b}{p}\right)$ is the Legendre symbol.

Proof. (Induction on n)

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

$$\lambda_0^2 + (-b)\mu_0^2 = 0$$

defined over F. Thus $|P_1| = 0$, if $\left(\frac{b}{p}\right) = -1$ and $|P_1| = 2(p-1)$ if $\left(\frac{b}{p}\right) = +1$. Therefore $|P_1| = p - 1 + (p-1)\left(\frac{b}{p}\right)$ as desired.

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

$$\begin{aligned}
|P_n| \;=\; & |\{(\lambda_0, \ldots, \lambda_{n-1}; \mu_0, \ldots, \mu_{n-1}) \in P_n : \\
& \mu_{n-1} \neq 0; \lambda_0, \ldots, \lambda_{n-2}; \mu_0, \ldots, \mu_{n-2} \in F\}| + \\
& +|\{(\lambda_0, \ldots, \lambda_{n-1}; \mu_0, \ldots, \mu_{n-1}) \in P_n : \\
& \mu_{n-1} = 0; \lambda_{n-1} \neq 0; \lambda_i = \mu_i = 0 \text{ for all } i = 0, 1, \ldots, n-2\}| + \\
& +|\{(\lambda_0, \ldots, \lambda_{n-1}; \mu_0, \ldots, \mu_{n-1}) \in P_n : \\
& \mu_{n-1} = 0; \lambda_{n-1} \in F;\ (\lambda_0, \ldots, \lambda_{n-2}; \mu_0, \ldots, \mu_{n-2}) \neq (0, \ldots, 0)\}| \\
=\; & (p-1)p^{2n-2} + (p-1) + p|P_{n-1}| = p^{2n-1} - 1 + (p-1)p^{n-1}\left(\frac{b}{p}\right)
\end{aligned}$$

as desired.

Lemma 10. Let $s = 2n$, $n \in \mathbb{N}$. Then the number u of the square elements $0 \neq \beta = \sum_{i=1}^{s} b_i\theta^{i-1}$ with $b_1 = 0$ equals

$$\frac{1}{2}\left[p^{2n-1} - 1 + (p-1)p^{n-1}\left(\frac{a_0}{p}\right)\right]$$

where $\theta^s = \theta^{2n} = -a_0 - a_1\theta - \ldots - a_{2n-1}\theta^{2n-1}$; $a_0 \neq 0$.

Proof. For any element $0 \neq \gamma \in F_q$ we have

$$\gamma = \lambda_0 + \sum_{i=1}^{n-1} \lambda_i\theta^{n-i} + \sum_{i=0}^{n-1} \mu_i\theta^{n+i} \quad \text{with} \quad (\lambda_0, \ldots, \lambda_{n-1}; \mu_0, \ldots, \mu_{n-1}) \neq (0, \ldots, 0)$$

Set $\gamma^2 = \sum_{i=1}^{n-1} c_i\theta^{i-1}$. Then we get

$$c_1 = \lambda_0^2 + (-2a_0)\sum_{i=1}^{n-1} \lambda_i\mu_i + (-a_0)\mu_0^2 + \sum_{i=1}^{n-1} b_i\mu_i^2 + \sum_{1 \leq j < k \leq n-1} c_{jk}\lambda_j\mu_k + \sum_{0 \leq j < k \leq n-1} d_{jk}\mu_j\mu_k$$

for some $b_i, c_{jk} \in F$, $(i = 1, \ldots, n-1)$, $(1 \leq j < k \leq n-1)$, $d_{jk} \in F$, $(0 \leq j < k \leq n-1)$. If $0 \neq \gamma$ then $\gamma \neq -\gamma$ but $\gamma^2 = (-\gamma)^2$. Thus

$$u = \frac{1}{2}|P_n| = \frac{1}{2}\left[p^{2n-1} - 1 + (p-1)p^{n-1}\left(\frac{a_0}{p}\right)\right]$$

with P_n defined in Lemma 9.

Corollary 11. If $s = 2n$, $n \in \mathbb{N}$. Then

$$\tau_{(s)} = \left(\frac{a_0}{p}\right)\sqrt{q}, \quad x_{(s)} = -\frac{1}{2}\left[-\left(\frac{a_0}{p}\right)\sqrt{q} + 1\right], \quad y_{(s)} = -\frac{1}{2}\left[\left(\frac{a_0}{p}\right)\sqrt{q} + 1\right] \ .$$

Proposition. 1. Let $s = 2n$, $n \in \mathbb{N}$ then $\left(\frac{a_0}{p}\right) = +1$, if and only if $\theta \in <\rho^2> = K$.
2. $F_q = F(\rho) = F(\rho^2)$; i.e. ρ and ρ^2 are primitive elements of F_q over F. Namely, θ can be chosen as ρ and ρ^2 for any $s \in \mathbb{N}$.
3. a) If $s = 2n+1$, $n \in \mathbb{N} \cup \{0\}$ then $\tau_{(s)}$, $x_{(s)}$ and $y_{(s)}$ are independent of the choice of the primitive element θ.
b) If $s = 2n$, $n \in \mathbb{N}$ then

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

for any primitive element $\theta \in <\rho^2> = K$ while

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

for any primitive element $\theta \in \rho K$.
c) For any $s \in \mathbb{N}$ and for any primitive element $\theta \in <\rho^2> = K$ we always have

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

where

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

Proof. 1. As we already know $Gal(F_q/F) = <\alpha>$ with $\alpha(\gamma) = \gamma^p$ for any $\gamma \in F_q$. And $s = 2n$, $n \in \mathbb{N}$ implies that $a_0 = \mathrm{N}_{F_q/F} = \theta\theta^p \ldots \theta^{p^{s-1}} = \theta^{(p^s-1)/(p-1)}$. Let $\theta = \rho^i$ for some $i \in \mathbb{N}$. Since $r = \rho^{(p^s-1)/(p-1)}$, $<r> = F^*$,
$\left(\frac{a_0}{p}\right) = +\mathbf{i} \iff a_0 = r^{2j}$ for some $j \in \mathbb{N} \iff a_0 = \rho^{[(p^s-1)/(p-1)]i} = \rho^{[(p^s-1)/(p-1)]2j} \iff$

$[(p^s-1)/(p-1)]i \equiv [(p^s-1)/(p-1)]2j \pmod{(p^s-1)} \Longleftrightarrow i \equiv 2j \pmod{(p-1)}$ $\Longleftrightarrow i \equiv 0 \pmod 2 \Longleftrightarrow \theta \in <\rho^2>= K$.

2. If $s=1$, then each non-zero element of F is trivially a primitive element over F. Suppose $s \geq 2$. As $F_q^* =<\rho>$ we have $F(p)=F_q$; i.e. ρ is a primitive element of F_q over F. Now we shall show that ρ^2 is also a a primitive element of F_q over F. Otherwise $F_{p^t}=F(\rho^2)<F_q$ for some $1 \leq t < s$. Then $1=(\rho^2)^{p^t-1}$ and thus $2(p^t-1) \equiv 0 \pmod{(p^s-1)}$. But then

$$p^s-1 \leq 2(p^t-1) < p(p^t-1) = p^{t+1}-p < p^s-1$$

which is a contradiction.

3. By Corollary 7 and Corollary 11 and from 1, 2 above we arrive at desired result.

References

[1] Borevich Z.I. and Shafarevich: Number Theory, New York Academic Press Inc. C. 1966.

N.Yelkenkaya
Department of Mathematics
Faculty of Science
University of Istanbul
Vezneciler 34459, Istanbul, Turkey