Serdica J. Computing **5** (2011), 1–14

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

THE DIVISIBILITY MODULO 4 OF KLOOSTERMAN SUMS OVER FINITE FIELDS OF CHARACTERISTIC 3

Changhyon Sin

Abstract. Recently Garashuk and Lisonek evaluated Kloosterman sums $K(a)$ modulo 4 over a finite field $\mathbf{F}_{3^m}$ in the case of even $K(a)$. They posed it as an open problem to characterize elements a in $\mathbf{F}_{3^m}$ for which $K(a) \equiv 1 \pmod 4$ and $K(a) \equiv 3 \pmod 4$. In this paper, we will give an answer to this problem. The result allows us to count the number of elements a in $\mathbf{F}_{3^m}$ belonging to each of these two classes.

1. Introduction.

Let $\mathbf{F}_q$ denote the finite field with q elements. From now on, let m be a positive integer and $q = 3^m$.
Let $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_3}(x)$ be the *trace* function from $\mathbf{F}_q$ onto $\mathbf{F}_3$ defined by

$$\mathbf{Tr}_{\mathbf{F}_q/\mathbf{F}_3}(x) = \sum_{j=0}^{m-1} x^{3^j}.$$

We will often write simply **Tr**for $\mathbf{Tr}_{\mathbf{F}_q/\mathbf{F}_3}$ if $\mathbf{F}_q/\mathbf{F}_3$ is understood.

ACM Computing Classification System (1998): F.2.1.
Key words: Kloosterman sums, Divisibility, Exponential sum.

The *Kloosterman sum* $K(a)$ over $\mathbf{F}_q$ is defined for any $a \in \mathbf{F}_q$ by

$$K(a) = \sum_{x \in \mathbf{F}_q^*} \omega^{\mathbf{Tr}(x^{-1}+ax)},$$

where $\omega = e^{2\pi i/3}$ is a complex primitive cubic root of unity.

Kloosterman sums have been studied extensively because they are interesting mathematical objects as well as powerful tools to investigate coding theory and cryptography; see for example [8, 9].

Moreover Kloosterman sums are linked to the weight distribution of some codes, the number of rational points on an elliptic curve and the number of irreducible polynomials with prescribed coefficients (see e.g. [1, 3]).

It is very difficult to find exact values of Kloosterman sums and usually we have to be satisfied with only estimating it. Recently, congruences in terms of Kloosterman sums are widely studied (see e.g. [2, 4, 5]). Moreover Garaschuk and Lisonek [4] characterized elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 0 (\mathrm{mod} 4)$ and $K(a) \equiv 2 \pmod 4$. They posed it as an open problem to characterize elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 1 \pmod 4$ and $K(a) \equiv 3 \pmod 4$. In this paper we will give an answer to this problem. Our strategy is to obtain a congruence between $K(a^2)$ and an exponential sum using the property of elements $b \in \mathbf{F}_q$ such that the polynomial $x^4 - bx^3 + a^2$ has only one root in $\mathbf{F}_q$.

The rest of the paper is organized as follows. In section 2 some necessary definitions and propositions are recalled. In section 3 the number of roots of the polynomial $x^4 - bx^3 + a$ over $\mathbf{F}_q$ is considered. In section 4 congruences modulo 4 for $K(a^2)$ are obtained and elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 1 \pmod 4$ and $K(a) \equiv 3 \pmod 4$ are completely characterized. Finally in section 5 the number of elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 1 \pmod 4$ is given.

2. Preliminaries. In this section we recall some definitions and propositions for Kloosterman sums needed in the sequel.

Let $a \in \mathbf{F}_q$. If there exists an $x \in \mathbf{F}_q$ such that $a = x^2$ then we say that a is a *square*, otherwise we say that a is a *non-square*. For each square $a \in \mathbf{F}_q$, let $\sqrt{a}$ denote an $x \in \mathbf{F}_q$ such that $x^2 = a$. If $a \neq 0$, then we are making a choice between x and $-x$; this choice can be arbitrary as long as it is the same in each occurrence of $\sqrt{a}$.

The following results were obtained in [4].

Proposition 1. *For all $a \in \mathbf{F}_q, K(a)$ is an integer satisfying $K(a) \equiv 2 \pmod 3$.*

Proposition 2. *$K(a)$ is odd if and only if $a = 0$ or a is a square and $\mathrm{Tr}(\sqrt{a}) \neq 0$.*

Proposition 3. *$K(a)$ is odd for $\frac{1}{3}q + 1$ elements $a \in \mathbf{F}_q$.*

It is sufficient to consider $K(a^2)$ in order to arrive at the goal of this paper by proposition 2. We have easily $K(0) = -1$. Hence we only consider $K(a^2)$ with $a \neq 0$.

We know the following result by [6, p. 19].

Proposition 4. *Let $f(x) = x^3 - bx - c \in \mathbf{F}_q[x]$ with $b \neq 0$. Then*
(1) *$f(x)$ has no multiple roots.*
(2) *$f(x)$ has only one root in $\mathbf{F}_q$ if and only if b is a non-square.*
(3) *$f(x)$ has three roots in $\mathbf{F}_q$ if and only if b is a square and $\mathbf{Tr}(c\sqrt{b}^{-3}) = 0$.*
(4) *$f(x)$ is irreducible over $\mathbf{F}_q$ if and only if b is a square and $\mathbf{Tr}(c\sqrt{b}^{-3}) \neq 0$.*

We need also the following well-known result (see Theorem 5.4 in [7]).

Proposition 5. *Let $a \in \mathbf{F}_q$. Then*

$$\sum_{x \in \mathbf{F}_q} \chi(ax) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{if } a \neq 0, \end{cases}$$

where χ is the canonical additive character of $\mathbf{F}_q$.

3. The number of roots of a polynomial with degree 4. In this section we consider the number of roots of the polynomial $x^4 - bx^3 + a$.

Lemma 1. *Let $f(x) = x^3 + ax^2 + bx + c \in \mathbf{F}_q[x]$ with $a \neq 0$ and $B = c + \frac{b^3}{a^3} - \frac{b^2}{a} \neq 0$. Then*
(1) *$f(x)$ has no multiple roots.*
(2) *$f(x)$ has only one root in $\mathbf{F}_q$ if and only if $-aB^{-1}$ is a non-square.*
(3) *$f(x)$ has three roots in $\mathbf{F}_q$ if and only if $-aB^{-1}$ is a square and*

$$\mathbf{Tr}(B^{-1}\sqrt{-aB^{-1}}^{-3}) = 0.$$

(4) *$f(x)$ is irreducible over $\mathbf{F}_q$ if and only if $-aB^{-1}$ is a square and*

$$\mathbf{Tr}(B^{-1}\sqrt{-aB^{-1}}^{-3}) \neq 0.$$

P r o o f. We have

$$f(x) = \left(x - \frac{b}{a}\right)^3 + a\left(x - \frac{b}{a}\right)^2 + B.$$

Since $x^3 + ax^2 + B$ is the reciprocal polynomial of $B\left(x^3 + \frac{a}{B}x + \frac{1}{B}\right)$, the lemma follows immediately from Proposition 4. □

Lemma 2. *Let $f(x) = x^4 - bx^3 + a \in \mathbf{F}_q[x]$ with $a \neq 0$. Then*
(1) *$f(x)$ has no multiple roots.*
Assume that $f(x)$ has at least one root in $\mathbf{F}_q$. Then
(2) *$f(x)$ has exactly two roots in $\mathbf{F}_q$ if and only if a is a non-square.*
(3) *$f(x)$ has four roots in $\mathbf{F}_q$ if and only if a is a square and $\mathbf{Tr}(b^2\sqrt{a}^{-1}) = 0$.*
(4) *$f(x)$ has only one root in $\mathbf{F}_q$ if and only if a is a square and $\mathbf{Tr}(b^2\sqrt{a}^{-1}) \neq 0$.*

P r o o f. We have

$$f'(x) = 4x^3 - 3bx^2 = x^3.$$

Therefore $f(x)$ and $f'(x)$ are relatively prime which proves the first part of the lemma.

Assume that $t \in \mathbf{F}_q$ is a root of $f(x)$. Then we have

$$f(x) = (x - t)\left(x^3 - \frac{a}{t^3}x^2 - \frac{a}{t^2}x - \frac{a}{t}\right).$$

Calculating B of $x^3 - \frac{a}{t^3}x^2 - \frac{a}{t^2}x - \frac{a}{t}$ with the notation of Lemma 1, we have

$$B = -\frac{a}{t} + t^3 + \frac{a}{t} = t^3 \neq 0.$$

By Lemma 1-(2), it follows that $f(x)$has exactly two roots in $\mathbf{F}_q$ if and only if

$$-\left(-\frac{a}{t^3}\right)B^{-1} = \frac{a}{t^6}$$

is a non-square which proves the second part of the lemma.

Now assume that $a$is a square. By Lemma 1-(3) it follows that

$$0 \neq \mathbf{Tr}\left(B^{-1}\sqrt{\frac{a}{t^6}}^{-3}\right) = \mathbf{Tr}\left(\frac{t^6}{\sqrt{a}^3}\right) = \mathbf{Tr}(\sqrt{a}^{-1}t^2)$$

$$\begin{aligned}\mathbf{Tr}(\sqrt{a}^{-1}t^2) &= \mathbf{Tr}(\sqrt{a}^{-1}t^2) + 2\mathbf{Tr}(\sqrt{a}\,t^{-2}) + \mathbf{Tr}(\sqrt{a}\,t^{-2}) \\ &= \mathbf{Tr}(\sqrt{a}^{-1}t^2) + 2\mathbf{Tr}(\sqrt{a}\,t^{-2}) + \mathbf{Tr}(\sqrt{a}^{3}t^{-6}) \\ &= \mathbf{Tr}(\sqrt{a}^{-1}(t^2 + 2at^{-2} + a^2t^{-6})) \\ &= \mathbf{Tr}(\sqrt{a}^{-1}(t + at^{-3})^2) \\ &= \mathbf{Tr}(\sqrt{a}^{-1}b^2),\end{aligned}$$

which completes the proof. □

Lemma 3. *Let $f(x) = x^4 - bx^3 + a \in \mathbf{F}_q[x]$ with $a \neq 0$. Then*
(1) *$f(x)$ has only one root in $\mathbf{F}_q$ if and only if a is square and $\mathbf{Tr}(b^2\sqrt{a}^{-1}) \neq 0$.*
(2) *If a is a square then the number of roots of $f(x)$ in $\mathbf{F}_q$ is*

$$|\{x \in \mathbf{F}_q^* | b = x + ax^{-3}\}| = \begin{cases} 1 & \text{if } \mathbf{Tr}(b^2\sqrt{a}^{-1}) \neq 0 \\ 0 \text{ or } 4 & \text{if } \mathbf{Tr}(b^2\sqrt{a}^{-1}) = 0. \end{cases}$$

P r o o f. (1) By Lemma 2-(4) it is sufficient to show that if a is a square and $\mathbf{Tr}(b^2\sqrt{a}^{-1}) \neq 0$ then $f(x)$ has at least one root in $\mathbf{F}_q$.

Assume that $f(x)$ has no root in $\mathbf{F}_q$. Then $f(x)$ is irreducible over $\mathbf{F}_q$ or $f(x)$ factors into two irreducible polynomials with degree 2. Hence $f(x)$ has four roots in an extension field $\mathbf{F}_{q^4}$ of $\mathbf{F}_q$. By Lemma 2-(3) we have

$$0 = \mathbf{Tr}_{\mathbf{F}_{q^4}/\mathbf{F}_3}(b^2\sqrt{a}^{-1}) = \mathbf{Tr}_{\mathbf{F}_q/\mathbf{F}_3}(4b^2\sqrt{a}^{-1}) = \mathbf{Tr}_{\mathbf{F}_q/\mathbf{F}_3}(b^2\sqrt{a}^{-1}),$$

a contradiction.

(2) If $\mathbf{Tr}(b^2\sqrt{a}^{-1}) = 0$ and $|\{x \in \mathbf{F}_q^* | b = x + ax^{-3}\}| \neq 0$ then by Lemma 2-(3) we have

$$|\{x \in \mathbf{F}_q^* | b = x + ax^{-3}\}| = 4,$$

which completes the proof. □

4. Congruence modulo 4 for $K(a^2)$.

In this section we will show some congruences modulo 4 for $K(a^2)$.

Although the following lemma is proved easily by using techniques in [4, Lemma 1.2], we also prove it here for the convenience of the reader.

Lemma 4. *Let $f(x)$ be a function from $\mathbf{F}_q^*$ to $\mathbf{F}_q$ (then $f(x)$ will become a polynomial function over $\mathbf{F}_q$). For $u \in \mathbf{F}_3$, let N_u denote $|\{x \in \mathbf{F}_q^* | \mathbf{Tr}(f(x)) = u\}|$. If $f(x) = -f(-x)$ for any $x \in \mathbf{F}_q^*$, then*

$$L := \sum_{x \in \mathbf{F}_q^*} \chi(f(x)) = q - 1 - 3N_1.$$

P r o o f. The bijection $x \mapsto -x$ shows that $N_1 = N_{-1}$. Since $\omega + \omega^{-1} = -1$, we get $L = N_0 - N_1$. Then from $N_0 = q-1-2N_1$ we get $L = q-1-3N_1$. □

Theorem 5. *Let $a \in \mathbf{F}_q^*$ and $S_a = \{b \in \mathbf{F}_q | \mathbf{Tr}(b) = 1,\ \mathbf{Tr}(b^2 a^{-1}) \neq 0\}$. Then*

$$K(a^2) \equiv (-1)^m - 1 + |S_a| \pmod 4.$$

P r o o f. By the Frobenius automorphism and the properties of the trace function, we have

$$\begin{aligned} K(a^2) &= \sum_{x \in \mathbf{F}_q^*} \chi(x + a^2 x^{-1}) = \sum_{x \in \mathbf{F}_q^*} \chi(x^3 + a^2 x^{-3}) = \sum_{x \in \mathbf{F}_q^*} \chi(x^3)\chi(a^2 x^{-3}) \\ &= \sum_{x \in \mathbf{F}_q^*} \chi(x)\chi(a^2 x^{-3}) = \sum_{x \in \mathbf{F}_q^*} \chi(x + a^2 x^{-3}). \end{aligned}$$

By Lemma 4 we have

$$K(a^2) \equiv (-1)^m - 1 + |\{x \in \mathbf{F}_q^* | \mathbf{Tr}(x + a^2 x^{-3}) = 1\}| (\mathrm{mod} 4),$$

using $q \equiv (-1)^m \pmod 4$.

By Lemma 3-(2) we also get

$$|\{x \in \mathbf{F}_q^* | \mathbf{Tr}(x + a^2 x^{-3}) = 1\}| \equiv |\{b \in \mathbf{F}_q | \mathbf{Tr}(b) = 1,\ \mathbf{Tr}(b^2 a^{-1}) \neq 0\}| (\mathrm{mod} 4),$$

which completes the proof. □

Now we consider the following exponential sums to calculate $|S_a|$.

Let η denote the quadratic character of $\mathbf{F}_q^*$. i is a complex number such that $i^2 = -1$.

Lemma 6. Let $a,\ b \in \mathbf{F}_q$ Then

(1) $\sum_{x \in \mathbf{F}_q^*} \chi(ax^2) = -1 + (-1)^{m-1} i^m \eta(a) \sqrt{q}.$

(2) If $a \neq 0$, $\sum_{x\in\mathbf{F}_q^*} \chi(ax^2+bx) = \chi\left(\frac{-b^2}{a}\right)(-1)^{m-1}i^m\eta(a)\sqrt{q}\ -1.$

P r o o f. (1) By [7, Theorem 5.30, 5.15] we have

$$\sum_{x\in\mathbf{F}_q^*} \chi(ax^2) = -1 + G(\eta)\ \cdot \eta(a), \quad G(\eta) = (-1)^{m-1}i^m\sqrt{q},$$

where $G(\eta) = \sum_{x\in F_q^*} \chi(x)\eta(x)$ is the Gauss sum of η. This completes the first part of the lemma.

(2) We have

$$\sum_{x\in\mathbf{F}_q^*}\chi(ax^2+bx) = \sum_{x\in\mathbf{F}_q^*}\chi\left(a\left(x-\frac{b}{a}\right)^2-\frac{b^2}{a}\right) = \chi\left(\frac{-b^2}{a}\right)\sum_{x\in\mathbf{F}_q^*}\chi\left(a\left(x-\frac{b}{a}\right)^2\right) =$$

$$= \chi\left(\frac{-b^2}{a}\right)\left[\sum_{x\in\mathbf{F}_q^*}\chi(ax^2)+1-\chi(\frac{b^2}{a})\right] = \chi\left(\frac{-b^2}{a}\right)(-1)^{m-1}i^m\eta(a)\sqrt{q}\ -1,$$

which completes the proof. □

Lemma 7. *With notations as above, we have*

$$9|S_a|\ = 2q + i^m\eta(a)\sqrt{q}[(-1)^m+1+(-1)^{m-1}\chi(-a)-\chi(a)].$$

P r o o f. By Lemma 6 we have

$$\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}\right) = -1+(-1)^{m-1}i^m\eta(a^{-1})\sqrt{q} = -1+(-1)^{m-1}i^m\eta(a)\sqrt{q},$$

$$\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}\right) = \sum_{x\in\mathbf{F}_q^*}\bar{\chi}\left(\frac{x^2}{a}\right) = -1+(-1)^{m-1}(-i)^m\eta(a)\sqrt{q} = -1-i^m\eta(a)\sqrt{q},$$

$$\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}+x\right) = \chi(-a)(-1)^{m-1}i^m\eta(a)\sqrt{q}-1,$$

$$\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}-x\right) = -\chi(a)i^m\eta(a)\sqrt{q}-1,$$

$$\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}+x\right) = \sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}-x\right), \quad \sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}-x\right) = \sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}+x\right),$$

$$\bar{\omega}\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}+x\right)+\omega\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}-x\right)=\bar{\omega}\chi(-a)(-1)^{m-1}i^m\eta(a)\sqrt{q}\ -\bar{\omega}$$

$$-\omega\chi(a)i^m\eta(a)\sqrt{q}\ -\omega=1+i^m\eta(a)\sqrt{q}\cdot[\bar{\omega}\chi(-a)(-1)^{m-1}\ -\omega\chi(a)],$$

$$\omega\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}-x\right)+\bar{\omega}\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}+x\right)=\omega\chi(-a)(-1)^{m-1}i^m\eta(a)\sqrt{q}\ -\omega$$

$$-\bar{\omega}\chi(a)i^m\eta(a)\sqrt{q}\ -\bar{\omega}=1+i^m\eta(a)\sqrt{q}\cdot[\omega\chi(-a)(-1)^{m-1}\ -\bar{\omega}\chi(a)].$$

Let ψ be the canonical additive character of $\mathbf{F}_3$. Let $z\in\mathbf{F}_q$ satisfying $\mathbf{Tr}(z)=1$.

By proposition 5 we have

$$9|S_a|=\sum_{x\in\mathbf{F}_q^*}\left[\sum_{u\in\mathbf{F}_3}\psi(\mathbf{Tr}(x-z)u)\sum_{v\in\mathbf{F}_3}\psi(\mathbf{Tr}(\frac{x^2}{a}-z)v)\right]$$

$$+\sum_{x\in\mathbf{F}_q^*}\left[\sum_{u\in\mathbf{F}_3}\psi(\mathbf{Tr}(x-z)u)\sum_{v\in\mathbf{F}_3}\psi(\mathbf{Tr}(\frac{x^2}{a}+z)v)\right],$$

$$9\cdot\left(\frac{q}{3}-|S_a|\right)=\sum_{x\in\mathbf{F}_q^*}\left[\sum_{u\in\mathbf{F}_3}\psi(\mathbf{Tr}(x-z)u)\sum_{v\in\mathbf{F}_3}\psi(\mathbf{Tr}\left(\frac{x^2}{a}\right)v)\right]$$

$$=\sum_{x\in\mathbf{F}_q^*}[1+\chi(x-z)+\chi(z-x)]\left[1+\chi\left(\frac{x^2}{a}\right)+\chi\left(\frac{-x^2}{a}\right)\right]$$

$$=\sum_{x\in\mathbf{F}_q^*}\Bigg[1+\chi(x-z)+\chi(z-x)+\chi\left(\frac{x^2}{a}\right)+\chi\left(\frac{-x^2}{a}\right)$$

$$+\chi\left(\frac{x^2}{a}+x-z\right)+\chi\left(\frac{-x^2}{a}-x+z\right)+\chi\left(\frac{x^2}{a}-x+z\right)+\chi\left(\frac{-x^2}{a}+x-z\right)\Bigg]$$

$$=q-1+\bar{\omega}\sum_{x\in\mathbf{F}_q^*}\chi(x)+\omega\sum_{x\in\mathbf{F}_q^*}\chi(-x)+\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}\right)+\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}\right)$$

$$+\bar{\omega}\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}+x\right)+\omega\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}-x\right)$$

$$+\omega\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{x^2}{a}-x\right)+\bar{\omega}\sum_{x\in\mathbf{F}_q^*}\chi\left(\frac{-x^2}{a}+x\right)$$

$$\begin{aligned}
&= q-1+\bar{\omega}\cdot(-1)+\omega\cdot(-1)-1+(-1)^{m-1}i^m\eta(a)\sqrt{q}-1-i^m\eta(a)\sqrt{q}\\
&\quad +1+i^m\eta(a)\sqrt{q}\cdot[\bar{\omega}\chi(-a)(-1)^{m-1}-\omega\chi(a)]\\
&\quad +1+i^m\eta(a)\sqrt{q}\cdot[\omega\chi(-a)(-1)^{m-1}-\bar{\omega}\chi(a)]\\
&= q-1+1+i^m\eta(a)\sqrt{q}[(-1)^{m-1}-1-\chi(-a)(-1)^{m-1}+\chi(a)]\\
&= q-i^m\eta(a)\sqrt{q}[(-1)^m+1+(-1)^{m-1}\chi(-a)-\chi(a)],
\end{aligned}$$

which completes the proof. □

Theorem 8. *Let $a\in\mathbf{F}_q^*$. Then*

$$K(a^2)\equiv-(-1)^m-1+i^m\eta(a)\sqrt{q}[(-1)^m+1+(-1)^{m-1}\chi(-a)-\chi(a)](\mathrm{mod}\,4).$$

P r o o f. By Theorem 5 and Lemma 7 we have

$$\begin{aligned}
K(a^2)\equiv{}&(-1)^m-1+2(-1)^m\\
&+i^m\eta(a)\sqrt{q}[(-1)^m+1+(-1)^{m-1}\chi(-a)-\chi(a)](\mathrm{mod}\,4),
\end{aligned}$$

which completes the proof. □

The next corollary answers the open problem posed in Garashcuk and Lisonek [4].

Corollary 9. *Let $a\in\mathbf{F}_q^*$. Then*

(1) *In the case of m even,*

$K(a)\equiv 1\,(\mathrm{mod}\,4)$ *if and only if a is a square,* $\mathbf{Tr}(\sqrt{a})\neq 0$ *and $\sqrt{a}$ is a square.*

$K(a)\equiv 3\,(\mathrm{mod}\,4)$ *if and only if a is a square,* $\mathbf{Tr}(\sqrt{a})\neq 0$ *and $\sqrt{a}$ is a non-square.*

(2) *In the case of m odd,*

$K(a)\equiv 3\,(\mathrm{mod}\,4)$ *if and only if there exists an element $t\in\mathbf{F}_q^*$ such that $a=t^2$,* $\mathbf{Tr}(t)=1$ *and t is a square.*

$K(a) \equiv 1 \pmod 4$ *if and only if there exists an element* $t \in \mathbf{F}_q^*$ *such that* $a = t^2$, $\mathbf{Tr}(t) = 1$ *and* t *is a non-square.*

P r o o f. By Proposition 2 we only consider $a \in \mathbf{F}_q^*$ such that a is a square and $\mathbf{Tr}(\sqrt{a}) \neq 0$.

By Theorem 8 we have

$$K(a) \equiv 2 + i^m \eta(\sqrt{a})\sqrt{q}[2 - \chi(-\sqrt{a}) - \chi(\sqrt{a})] (\mathrm{mod}\, 4).$$

Since $\mathbf{Tr}(\sqrt{a}) \neq 0$ we also get

$$\chi(-\sqrt{a}) + \chi(\sqrt{a}) = \omega + \bar{\omega} = -1.$$

Therefore we obtain

$$K(a) \equiv 2 - (-1)^{m/2}\eta(\sqrt{a})\sqrt{q} \equiv 2 - (-1)^{m/2}\eta(\sqrt{a})(-1)^{m/2} \equiv 2 - \eta(\sqrt{a}) (\mathrm{mod}\, 4),$$

which completes the first part of the corollary.

(2) Let t be a square root of a. Since $\mathbf{Tr}(t) \neq 0$ and $\mathbf{Tr}(t) + \mathbf{Tr}(-t) = 0$, suppose without loss of generality that $\mathbf{Tr}(t) = 1$.

By Theorem 8 we have

$$K(t^2) \equiv i^m \eta(t)\sqrt{q}[\chi(-t) - \chi(t)] (\mathrm{mod}\, 4),$$

$$\chi(-t) - \chi(t) = \bar{\omega} - \omega = -i\sqrt{3},$$

$$K(t^2) \equiv -(-1)^{(m+1)/2}\eta(t)\sqrt{3q}$$
$$\equiv -(-1)^{(m+1)/2}\eta(t)(-1)^{(m+1)/2} \equiv -\eta(t) \pmod 4.$$

The proof is now complete. □

5. The number of elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 1 \pmod 4$. In this section we consider the number of elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 1 \pmod 4$, which lead to the number of elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 3 \pmod 4$ because we know the number of elements $a \in \mathbf{F}_q$ for which $K(a) \equiv 1 \pmod 2$.

For the convenience we denote by $A_{r,M}$ the number of elements $a \in \mathbf{F}_q^*$ for which $K(a) \equiv r \pmod M$ for any positive integer M and any integer $r = 0, 1, \ldots, M-1$, i.e.

$$A_{r,M} = |\{a \in \mathbf{F}_q^* | K(a) \equiv r (\mathrm{mod} M)\}|.$$

By proposition 3 we have

$$A_{1,4} + A_{3,4} = A_{1,2} = \frac{q}{3},$$

since $K(0) = -1$.

5.1. Case of m even. By Corollary 9 we have

$$A_{1,4} = |\{a \in \mathbf{F}_q^* | \exists\, t \in \mathbf{F}_q^*,\, a = t^4,\, \mathbf{Tr}(t^2) \neq 0\}|.$$

By Lemma 3-(2) it follows that if the polynomial $x^4 - a \in \mathbf{F}_q[x]$ with $a \neq 0$ has a root in $\mathbf{F}_q$ then it has four distinct roots in $\mathbf{F}_q$. Therefore we obtain

$$A_{1,4} = \frac{1}{4}|\{t \in \mathbf{F}_q^* | \mathbf{Tr}(t^2) \neq 0\}|.$$

Let α be a primitive element of $\mathbf{F}_q$. Then $\delta = \alpha^{(q-1)/4}$ is a primitive fourth root of unity in $\mathbf{F}_q$ since m is even. The bijection $t \mapsto \delta\, t$ shows that

$$|\{t \in \mathbf{F}_q^* | \mathbf{Tr}(t^2) = 1\}| = |\{t \in \mathbf{F}_q^* | \mathbf{Tr}(t^2) = -1\}|.$$

Hence we have

$$A_{1,4} = \frac{1}{2}|\{t \in \mathbf{F}_q^* | \mathbf{Tr}(t^2) = 1\}|.$$

Let $z \in \mathbf{F}_q$ satisfying $\mathbf{Tr}(z) = 1$. Let ψ be the canonical additive character of $\mathbf{F}_3$.

By Proposition 5 we have

$$|\{t \in \mathbf{F}_q^* | \mathbf{Tr}(t^2) = 1\}| = \frac{1}{3} \sum_{x \in \mathbf{F}_q^*} \sum_{u \in \mathbf{F}_3} \psi(\mathbf{Tr}(x^2 - z)u)$$

$$= \frac{1}{3} \sum_{x \in \mathbf{F}_q^*} (1 + \chi(x^2 - z) + \chi(-x^2 + z))$$

$$= \frac{1}{3}(q - 1 + \bar{\omega} \sum_{x \in \mathbf{F}_q^*} \chi(x^2) + \omega \sum_{x \in \mathbf{F}_q^*} \chi(-x^2)). \tag{1}$$

By Lemma 6 we also get

$$\sum_{x \in \mathbf{F}_q^*} \chi(x^2) = -1 - i^m\sqrt{q} = \sum_{x \in \mathbf{F}_q^*} \chi(-x^2).$$

Therefore we obtain

$$A_{1,4} = \frac{1}{6}[q - 1 + (\omega + \bar{\omega})(-1 - i^m\sqrt{q})]$$

$$= \frac{1}{6}(q + i^m\sqrt{q}) = \frac{1}{6}(3^m + (-1)^{m/2}3^{m/2}).$$

By Proposition 3 we also get

$$A_{3,4} = \frac{q}{3} - A_{1,4} = \frac{1}{6}(q - i^m\sqrt{q}) = \frac{1}{6}(3^m - (-1)^{m/2}3^{m/2}).$$

5.2. Case of m odd. By Corollary 9 we now get

$$A_{3,4} = |\{a \in \mathbf{F}_q^* | \exists\, t \in \mathbf{F}_q^*,\ a = t^2,\ \mathbf{Tr}(t) = 1,\ t \text{ is a square}\}|.$$

Since $\mathbf{Tr}(-t) = -\mathbf{Tr}(t)$ we obtain

$$A_{3,4} = |\{t \in \mathbf{F}_q^* |\ \mathbf{Tr}(t) = 1,\ t \text{ is a square}\}|$$

$$= \frac{1}{2}\,|\{x \in \mathbf{F}_q^* |\ \mathbf{Tr}(x^2) = 1\}|.$$

By (1) we have

$$|\{x \in \mathbf{F}_q^* |\ \mathbf{Tr}(x^2) = 1\}| = \frac{1}{3}(q - 1 + \bar{\omega}\sum_{x\in\mathbf{F}_q^*}\chi(x^2) + \omega\sum_{x\in\mathbf{F}_q^*}\chi(-x^2)).$$

By Lemma 6 we also get

$$\sum_{x\in\mathbf{F}_q^*}\chi(x^2) = -1 + i^m\sqrt{q},$$

$$\sum_{x\in\mathbf{F}_q^*}\chi(-x^2) = -1 - i^m\sqrt{q}.$$

Therefore we have

$$A_{3,4} = \frac{1}{6}(q - 1 + \bar{\omega}(-1 + i^m\sqrt{q}) + \omega(-1 - i^m\sqrt{q}))$$

$$= \frac{1}{6}(q - 1 + 1 + (\bar{\omega} - \omega)i^m\sqrt{q})$$

$$= \frac{1}{6}(q - i^{m+1}\sqrt{3q}) = \frac{1}{6}(3^m - (-1)^{(m+1)/2}3^{(m+1)/2}).$$

By Proposition 3 we also get

$$A_{1,4} = \frac{q}{3} - \frac{1}{6}(q - i^{m+1}\sqrt{3q}) = \frac{1}{6}(q + i^{m+1}\sqrt{3q}) = \frac{1}{6}(3^m + (-1)^{(m+1)/2}3^{(m+1)/2}).$$

We have proved the following theorem.

Theorem 10.

$$|\{a \in \mathbf{F}_q^* | K(a) \equiv 1 \,(\mathrm{mod} 4)\}| = \begin{cases} (3^m + (-1)^{m/2}3^{m/2})/6 & \textit{if } m \textit{ is even,} \\ (3^m + (-1)^{(m+1)/2}3^{(m+1)/2})/6 & \textit{if } m \textit{ is odd.} \end{cases}$$

$$|\{a \in \mathbf{F}_q^* | K(a) \equiv 3 \,(\mathrm{mod} 4)\}| = \begin{cases} (3^m - (-1)^{m/2}3^{m/2})/6 & \textit{if } m \textit{ is even,} \\ (3^m - (-1)^{(m+1)/2}3^{(m+1)/2})/6 & \textit{if } m \textit{ is odd.} \end{cases}$$

REFERENCES

[1] Moisio M. On the moments of Kloosterman sums and fibre products of Kloosterman curves. *Finite Field Appl.* **14** (2008), 515–531.

[2] Charpin P., T. Helleseth, V. Zinoviev. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd, *J.Combin.Theory*, Ser.A, **114** (2007), 322–338.

[3] Moisio M. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Arith.* **132** (2008), 329–350.

[4] Garaschuk K., P.Lisonek. On ternary Kloosterman sums modulo 12, *Finite Field Appl.* **14** (2008), 1083–1090.

[5] Moisio M. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even. *Finite Field Appl.* **15** (2009) 174–184.

[6] Hirschfeld W. P. Projective Geometries over Finite Fields. Second ed., Clarendon Press/Oxford Univ. Press, New York, 1998.

[7] Lidl R. H. Niederreiter. Finite Fields. Second ed., Encyclopedia Math. Appl., Vol. **20**, Cambridge Univ. Press, 1997.

[8] Charpin P., T. Helleseth, V. Zinoviev. Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums. *Finite Fields Appl.* **13** (2007), 366–381.

[9] Moisio M., K. Ranto. Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros. *Finite Fields Appl.* **13** (2007), 922–935.

Changhyon Sin
Faculty of Mathematics and Mechanics
KIM IL SUNG University
Pyongyang
Democratic People's Republic of Korea

Received June 22, 2010
Final Accepted November 5, 2010