ISSN 2304-1579. Visnyk Odesk. Nats. Univers. Mat. i Mekh.–2014 .–V.19,Is.3(23).–P.57–65

Mathematical Subject Classification: 94B05, 11T71
UDC 519.725 + 511.321

Tran The Vinh
Odesa I. I. Mechnikov National University

DISTRIBUTION OF THE WEIGHTS OF THE KLOOSTERMAN CODE

Чан Тхе Вінь. Розподілення ваг Клостерманівського коду. Вивчаються p-арні Клостерманівські коди довжини p^2-1 в алфавіті $\mathbb{F}_q$, які є циклічними кодами, дуальними до кодів Меласа довжини p^2-1. Ми отримуємо вагове розподілення кодів Меласа в термінах одновимірних сум Клостермана над кільцем цілих гаусових чисел. Знайдено нетривіальну оцінку суми Клостерманівських сум $k(1,\alpha z^2;p)$, $\alpha \in G_p$, коли α пробігає приведену систему вичетів за модулем p в $\mathbb{Z}$.
Ключові слова: суми Клостермана, коди Меласа, цілі гаусові числа.

Чан Тхе Винь. Распределение весов Клостермановского кода. Изучаются p-арные Клостермановы коды длины p^2-1 в алфавите $\mathbb{F}_q$, которые являются циклическими кодами, дуальными кодам Меласа длины p^2-1. Мы получаем весовое распределение кодов Меласа в терминах одномерных сумм Клостермана над кольцом целых гауссовых чисел. Найдена нетривиальная оценка суммы Клостермановых сумм $k(1,\alpha z^2;p)$, $\alpha \in G_p$, когда α пробегает приведенную систему вычетов по модулю p в $\mathbb{Z}$.
Ключевые слова: суммы Клостермана, коды Меласа, целые гауссовы числа.

Tran The Vinh. Distribution of the weights of the Kloosterman code. Studied p-ary Kloosterman codes of length p^2-1 in alphabet $\mathbb{F}_q$ which are the cyclic codes of the dual Melas code of length p^2-1. We obtain the weight distribution of the Melas codes in terms of one-dimensional Kloosterman sums over the ring of Gaussian integers. Derived the non-trivial bound of sum of the Kloosterman sums $k(1,\alpha z^2;p)$, $\alpha \in G_p$, when α runs the system of reduced residues modulo p in $\mathbb{Z}$.
Key words: Kloosterman sums, Melas codes, Gaussian integers.

Introduction. Let $\mathbb{F}_q$ be the field with $q=p^m$ elements and let θ be a primitive element of $\mathbb{F}_q$ over $\mathbb{F}_p$. Let $m_i(x)$ denotes the minimal polynomial of θ^i over $\mathbb{F}_p$.

Definition 1. *The simplex code $S(\theta)$ is the dual of the cyclic code over $\mathbb{F}_q$ of length $n=q-1$ generated by minimal polynomial $m_1(x)\in\mathbb{F}_p[x]$ for the primitive element θ.*

Definition 2. *The Melas $M(\theta)$ code is the cyclic code $[n,2m]$ over $\mathbb{F}_p$ generated by $m_1(x)m_{-1}(x)$.*

The code $M(\theta)$ has a parity matrix

$$\begin{pmatrix} 1 & \theta & \theta^2 & \dots & \theta^{q-2} \\ 1 & \theta^{-1} & \theta^{-2} & \dots & \theta^{-(q-2)} \end{pmatrix}$$

considered as a matrix over $\mathbb{F}_p$.

Definition 3. *Let C be a code over $\mathbb{F}_q$ of length n. Then*

$$C\big|_{\mathbb{F}_q} := C \bigcap \mathbb{F}_p$$

is called the subfield of C (or restriction of C to $\mathbb{F}_p$).

$C\big|_{\mathbb{F}_q}$ is a code over $\mathbb{F}_q$. Its minimal distance cannot be better than the minimal distance of C.

Consider the trace mapping $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p^n$ such that for $\alpha \in \mathbb{F}_q$ we have

$$\mathrm{Tr}(\alpha) := (\mathrm{tr}(\alpha), \mathrm{tr}(\alpha\theta), \ldots, \mathrm{tr}(\alpha\theta^{n-1})), \tag{1}$$

where $\mathrm{tr}(\beta) = \beta + \beta^p + \beta^{p^2} + \cdots + \beta^{p^{m-1}} \in \mathbb{F}_p$.

If C is a code over $\mathbb{F}_q$ then

$$\mathrm{Tr}(C) := \big\{\mathrm{tr}(c)\big|c \in C\big\} \subset \mathbb{F}_p^n$$

is called the trace code of C.

Delsarte [7] proved that for a code C over $\mathbb{F}_q$ the following equation

$$(C\big|_{\mathbb{F}_p})^\perp = \mathrm{Tr}(C^\perp)$$

holds.

This Delsarte statement is often used for study the dual codes.

From Definition 2 it follows that the Melas code may be defined as a restriction of a cyclic code over $\mathbb{F}_q$ on $\mathbb{F}_p$ with two zeros θ and θ^{-1}. Thus by Delsarte theorem, we conclude that the dual of Melas code $M(\theta)$ is the direct sum (as vectorial subspace) of two simplex code $S(\theta)$ and $S(\theta^{-1})$, i.e.

$$M(\theta)^\perp = \big\{\mathrm{tr}(\alpha x_1 + \beta x_1^{-1}), \ldots, \mathrm{tr}(\alpha x_n + \beta x_n^{-1})\big|\alpha, \beta \in \mathbb{F}_q\big\}$$

(here we fixed some sorting of non-zero element from $\mathbb{F}_q$).

Obviously, that $M(\theta)^\perp$ contains q^2 codewords. The code $M(\theta)^\perp$ we will call the Kloosterman code over $\mathbb{F}_p$.

In the works [5, 6, 8] the weights of dual code of $M(\theta)$ and other codes are given for $q = 2$ using properties of the Kloosterman sums over a finite fields of characteristic 2. In [11] J. Wolfmann determined the weight distribution of $M(\theta)^\perp$ for $p = 3$. G. van der Geer, R. Schoof and M. van der Vlugt (see [6]) derived a formula for the frequencies of the weights in ternary Melas codes.

Our aim is to investigate the distribution of weights for the p-ary dual Melas codes, where p is a prime number, $p \equiv 3 \pmod 4$, and $m = 2$, i.e. $n = p^m - 1 = p^2 - 1$.

Notation. In this article we denote:

$\mathbb{Z}, G$ — the ring of rational integers and Gaussian integers, respectively;

$\mathbb{Z}_p, G_p$ — the classes of residues in $\mathbb{Z}$ (respectively, in G) modulo p;

$\mathbb{Z}_p^*, G_p^*$ — the classes of reduced residues in $\mathbb{Z}_p$ (respectively, in G_p);

$\mathrm{wt}(a)$ — the Hamming weight of vector $a \in \mathbb{F}_q^n$;

$C^\perp$ — the dual code of C;

x^{-1} — the multiple inverse to $x \in G_p^*$ modulo p, i.e. $x \cdot x^{-1} \equiv 1 \pmod p$.

Also we consider "$\ll$" and "O" as equivalent symbols.

Auxiliary arguments. Let $m(\alpha, \beta)$ denotes a codeword of dual Melas code $M^\perp(\theta)$ associated with pair $(\alpha, \beta) \in G_p^2$, and let $\mathrm{wt}(m(\alpha, \beta))$ denotes a weight of $m(\alpha, \beta)$. Clearly that $\mathrm{wt}(m(\alpha, \beta)) = n - z(\alpha, \beta)$ with

$$z(\alpha, \beta) = \#\{x \in G_p^* \big| \mathrm{tr}(\alpha x + \beta x^{-1}) = 0\}. \tag{2}$$

For considered case we have $\mathrm{tr}(\gamma) = \gamma + \overline{\gamma}$, where $\overline{\gamma}$ is a complex conjugate to γ, so $\mathrm{tr}(\gamma) = 2\Re\gamma$.

Next we will express the Hamming weight $\mathrm{wt}(m(\alpha, \beta))$ by means of the Kloosterman sum over G_p^*

$$k(\alpha, \beta; p) := \sum_{x \in G_p^*} e^{\pi i \mathrm{tr}\left(\frac{\alpha x + \beta x^{-1}}{p}\right)}. \tag{3}$$

It well-known that

$$k(\alpha, \beta; p) = \begin{cases} p^2 - 1 & if \quad \alpha = \beta = 0, \\ -1 & if \quad \alpha = 0,\ \beta \neq 0 \\ & or \quad \alpha \neq 0,\ \beta = 0, \\ \varepsilon(\alpha, \beta) \cdot p & if \quad \alpha\beta \neq 0, \end{cases} \tag{4}$$

here $|\varepsilon(\alpha, \beta)| \leq 2$.

Since $k(\alpha, \beta; p) = k(1, \alpha\beta; p)$ if $\alpha \neq 0$, we consider the h-th moment $K^{(h)}$ of the Kloosterman sum $k(1, \gamma)$ that is given by

$$K^{(h)} := \sum_{\gamma \in G_p} (k(1, \gamma; p))^h. \tag{5}$$

In terms of $K^{(h)}$ we will study the distribution of weight of the $M(\theta)^\perp$ code.

Lemma 1. *Let θ is a generated element of the group G_p^*. Then*

$$wt(m(\alpha, \beta)) = \begin{cases} 0 & if \quad \alpha = \beta = 0, \\ p^2 - 1 & if \quad \alpha = 0,\ \beta \neq 0, \\ & or \quad \alpha \neq 0,\ \beta = 0, \\ \frac{(p^2-1)(p-1)}{p} - \frac{1}{p} \sum\limits_{z \in \mathbb{Z}_p^*} k(1, \alpha\beta z^2; p) & if \quad \alpha\beta \neq 0. \end{cases} \tag{6}$$

Proof. The case $\alpha\beta = 0$ is trivial. Let $\alpha\beta \neq 0$. Then we have

$$z(\alpha,\beta) = \sum_{x\in G_p^*}\frac{1}{p}\sum_{z\in\mathbb{Z}_p} e^{\pi i \mathrm{tr}\left(\frac{\alpha x+\beta x^{-1}}{p}z\right)} =$$

$$= \sum_{x\in G_p^*}\frac{1}{p}\sum_{z=0}^{p-1} e^{2\pi i\frac{\Re(\alpha x+\beta x^{-1})}{p}z} =$$

$$= \frac{p^2-1}{p} + \frac{1}{p}\sum_{z=1}^{p-1} e^{\pi i\frac{\mathrm{tr}(x+\alpha\beta z^2x^{-1})}{p}} =$$

$$= \frac{p^2-1}{p} + \frac{1}{p}\sum_{z=1}^{p-1} k(1,\alpha\beta z^2;p).$$

Hence,

$$\mathrm{wt}(m(\alpha,\beta)) = n - z(\alpha,\beta) = p^2 - 1 - \left(\frac{p^2-1}{p} + \frac{1}{p}\sum_{z=1}^{p-1} k(1,\alpha\beta z^2;p)\right) =$$

$$= (p^2-1)(1-\frac{1}{p}) - \frac{1}{p}\sum_{z=1}^{p-1} k(1,\alpha\beta z^2;p).$$

■

Cosequence 1. *For* $\alpha\beta \neq 0$

$$wt(m(\alpha,\beta)) = p^2 + 3p\cos\varphi,\ 0 \leq \varphi < 2\pi.$$

The following Lemma shows that an estimate of $\mathrm{wt}(m(\alpha,\beta))$ can be improved.

Lemma 2. *Let* $\alpha \in G_p^*$. *Then*

$$\sum_{z=1}^{p-1} k(1,\alpha z^2;p) = 2p^2\cos\varphi_0 + 1.$$

Proof. We have

$$\sum_{z=1}^{p-1} k(1,\alpha z^2;p) = \sum_{z=1}^{p-1}\sum_{z\in G_p^*} e^{\pi i\mathrm{tr}\left(\frac{x+\alpha z^2x^{-1}}{p}\right)} =$$

$$= \sum_{x\in G_p^*} e^{\pi i\mathrm{tr}\left(\frac{\alpha x}{p}\right)}\left(\sum_{z=0}^{p-1} e^{\pi i\frac{\mathrm{tr}(x^{-1})\cdot z^2}{p}} - 1\right) =$$

$$= \sum_{x\in G_p^*} e^{\pi i\mathrm{tr}\left(\frac{\alpha x}{p}\right)}\left(\left(\frac{\mathrm{tr}(x^{-1})}{p}\right)G(1,p^2) - 1\right),$$

where $G(1,p^2)$ is the Gauss sum over $\mathbb{F}_{p^2}$, $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Take into account that $G(1,p^2)=p$ if $p\equiv 3 \pmod 4$, we yield

$$\sum_{z=1}^{p-1} k(1,\alpha z^2;p) = p\sum_{x\in G_p^*}\left(\frac{\mathrm{tr}(x^{-1})}{p}\right) e^{\pi i \mathrm{tr}\left(\frac{\alpha x}{p}\right)} + 1.$$

The sum in right-hand side in last equation is the Kloosterman sum $k_\chi(\alpha,\beta;p)$ with the quadratic character χ. The Kloosterman sum with character admits the same estimate as the Kloosterman sum $k(\alpha,\beta;p)$ over G_p^*. Thus we obtain

$$\sum_{z=1}^{p-1} k(1,\alpha z^2;p) = 2p^2\cos\varphi_0 + 1,\ 0\le\varphi_0<2\pi.$$

■

Cosequence 2. *For* $\alpha\beta\neq 0$

$$wt(m(\alpha,\beta)) = p^2 - p - 1 + 2p\cos\varphi, \tag{7}$$

where $0\le\varphi<2\pi$.

Main Results

1. Distribution of the Hamming weight for the Melas code. We will determine the weight distributions of the Melas code as follows: first, we study the duals of the codes $M(\theta)$ and then by the MacWilliams identities related the weight distribution of the dual codes to the weight distribution of the Melas codes themselves, we will obtain the weight distribution of the codes $M(\theta)$.

We need two more of lemmas.

Lemma 3 (V. Pless [10])**.** *Let C be a p-ary linear code of length n and of dimension k and let A_i (respectively, $A_i^\perp$) denotes the number of codewords of weight i in C (respectively, in $C^\perp$). Then for $h=0,1,2,\ldots$, we have*

$$\sum_{i=0}^{n}(n-i)^h A_i = \sum_{i=0}^{\min(h,n)} A_i^\perp \sum_{j=i}^{h} j!S(h,j)p^{k-j}\begin{pmatrix} n-i \\ n-j \end{pmatrix}, \tag{8}$$

where

$$S(h,j) = \frac{1}{j!}\sum_{i=0}^{j}(-1)^{j-i}\begin{pmatrix} j \\ i \end{pmatrix} i^h$$

is a Stirling number of the second kind.

Denote

$$\overline{k}(\gamma) := \sum_{z=1}^{p-1} k(1, \gamma z^2; p),$$

$$\overline{K}^{(\ell)} := \sum_{\gamma \in G_p^*} \overline{k}(\gamma)^\ell, \ \ell = 0, 1, 2, \ldots.$$

Lemma 4. *Let M_i denote the number of code words of weight i for the Melas code $M(\theta)$ over $\mathbb{Z}_p$. Then for every positive integer h, the moment $K^{(h)}$ of the Kloosterman sum $k(1, \gamma; p)$ is given by*

$$(p^2-1)(p-1)^h \overline{K}^{(h)} = f(M_0, \ldots, M_h) + g(\overline{K}^{(0)}, \overline{K}^{(1)}, \ldots, , \overline{K}^{(h-1)}), \tag{9}$$

where

$$f(M_0, M_1, \ldots, M_h) = p^4 \sum_{i=0}^{h} M_i \sum_{j=1}^{h} j! S(h, j) p^{h-1} \left(\begin{array}{c} p^2-1-i \\ p^2-1-j \end{array} \right) \tag{10}$$

$$g(K_0^{(0)}, \ldots, K^{(h-1)}) = -(p^2-1)(p^h(p^2-1)). \tag{11}$$

Proof. We purpose a scheme of proof the Theorem 13 in [9]. Take $C = M(\theta)^\perp$ in Lemma 3, and consider the left-hand side of the identity (8). By Lemma 1 for each pair $(\alpha, \beta) \in G_p^2$ with $\alpha\beta = 0$, but α or β is not zero, the weight $\mathrm{wt}(m(\alpha, \beta)) = p^2 - 1$ (all together we have $2(p^2-1)$ such pairs). For every from other pairs (α, β) there exist $\gamma \in G_p^*$ such that $\alpha\beta = \gamma$. More over, the same γ corresponds exactly (p^2-1) pairs $(\alpha, \beta) \in G_p^*$ with weight $(p^2-1)\left(1 - \frac{1}{p}\right) - \frac{1}{p} \sum\limits_{z=1}^{p-1} k(1, \gamma z^2; p)$ by Lemma 1.

Thus the left-hand side of the identity (8) equals

$$\begin{aligned}
\sum_{i=0}^{p^2-1} (p^2-1-i)^h M_i^\perp &= \sum_{\alpha, \beta \in G_p} (p^2 - 1 - \mathrm{wt}(m(\alpha, \beta)))^h = \\
&= (p^2-1)^h + (p^2-1) \sum_{\gamma \in G_p^*} \left(\frac{p^2-1}{p} - \frac{1}{p} \overline{k}(\gamma) \right)^h = \\
&= (p^2-1)^h + \frac{(p^2-1)}{p^h} \sum_{\gamma \in G_p^*} \sum_{i=0}^{h} (p^2 - 1 - \overline{k}(\gamma))^h = \\
&= (p^2-1)^h + \frac{p^2-1}{p^h} \sum_{i=0}^{h} \left(\begin{array}{c} h \\ i \end{array} \right) (p^2-1)^{h-i} \overline{K}^{(i)}.
\end{aligned}$$

Since in our case the dimension of $M(\theta)$ is $k = 4$, the right-hand side of (8) equals

$$\sum_{i=1}^{h} M_i \sum_{j=i}^{h} j! S(h, j) p^{4-j} \left(\begin{array}{c} p^2-1-i \\ p^2-1-j \end{array} \right). \tag{12}$$

Hence, Lemma 4 is proved completely. ■

Lemma 4 establishes link between the number of codewords of weight i in $M(\theta)$ and values of $\overline{K}^{(j)}$. But it is easy to show that $\overline{K}^{(j)}$ can be expressed by values of the ℓ-th power moment $K^{(\ell)}$ of Kloosterman sums $k(1,\alpha;p)$, where

$$K^{(\ell)} := \sum_{\alpha\in G_p} (k(1,\alpha;p))^{\ell},\ \ell = 0,1,2,\ldots.$$

Thus below we give estimates for $K^{(\ell)}$ over G_p.

2. Moments of Kloosterman sum over G_p. Evaluations of the n-th power moments $K^{(n)}$ of Kloosterman sums represent a big interest not only for the studying the distribution of weight of special linear codes, but also for investigation of individual values $k(1,\alpha;p)$. Relatively, easily derive the formulas for the first four moments of Kloosterman sums over $\mathbb{Z}_p$

$$K^{(1)} = 1,\ K^{(2)} = p^2-p-1,\ K^{(3)} = \left(\frac{p}{3}\right)p^2+2p+1,\ K^{(4)} = 2p^3-3p^2-p-1, \quad (13)$$

(see [4, §4.4]).

For the case $h = 5$, we have (see, [11])

$$K^{(5)} = \left(\frac{p}{3}\right)4p^3 + b(p)p^2 + 4p + 1 \ \ if\ p > 5 \quad (14)$$

where $|b(p)| < 2p + 5$.

For $h = 6$ H. Salié and H. Davenport independently proved that $K^{(6)} = O(p^4)$. For $h = 7$ R.J. Evans [**?**] obtained the estimate $|K^{(7)}| \le 29p^4 + 14p^3 + 14p^2 + 6p$, and Ping Xi, Yian Yi [11] constructed an asymptotic representation for $K^{(n)}$, $n > 7$, when p grows to infinity.

The behaviour of $K^{(h)}$ over G also represents a certain interest. It is easy to show that

$$K^{(1)} = 1,\ K^{(2)} = p^4 - p^2 - 1,\ |K^{(3)}| \le cp^4,\ 0 < c < 3. \quad (15)$$

In greater details the case of $h = 3$ we consider now.

We have

$$\begin{aligned} K^{(3)}(p) &= \sum_{\alpha\in G_p^*}(k(1,\alpha;p))^3 = \sum_{\alpha\in G_p^*}\sum_{x,y,z\in G_p^{-1}} e^{\pi i \mathrm{tr}\left(\frac{\alpha(x+y+z)+x^{-1}+y^{-1}+z^{-1}}{p}\right)} = \\ &= \sum_{x,y,z\in G_p^*} e^{\pi i \mathrm{tr}\left(\frac{x^{-1}+y^{-1}+z^{-1}}{p}\right)}\left(\sum_{\alpha\in G_p} e^{2\pi i\frac{\alpha(x+y+z)}{p}} - 1\right) = \quad (16) \\ &= N(p) \sum_{\substack{x,y,z\in G_p^* \\ x+y+z\equiv 0 \pmod p}} e^{pii\mathrm{tr}\left(\frac{x^{-1}+y^{-1}+z^{-1}}{p}\right)} + 1 = \end{aligned}$$

The exponential sum in right-hand side of (19) can be estimated by the following theorem.

Theorem. *Let $\mathbb{F}_q$ be a finite field with q elements and let $f(x,y,z) \in \mathbb{F}_q[x,y,z]$ and V be an algebraic manifold produced by the polynomial $f(x,y,z)$. If for given $\alpha,\beta,\gamma \in \mathbb{F}_q$ and all $\tau \in \overline{\mathbb{F}}_q$ except $O(1)$ values, the polynomial*

$$F_\tau(x,y) = f(x,y,\tau)\gamma^{-1} - \alpha\gamma^{-1}x - \beta\gamma^{-1}y$$

is absolutely irreducible polynomial, then the following bound

$$\sum_{(x,y,z)\in V\bigcup \mathbb{F}_q^3} e^{\pi i t r\left(\frac{\alpha x+\beta y+\gamma z}{p}\right)} \ll q \tag{17}$$

holds.

This statement is a generalization of the result of C. Hooley from [3].

We apply this theorem to construction of bound $K^{(3)}(p)$. We have

$$\sum_{\substack{x,y,z\in G_p^*\\ x+y+\tau\equiv 0 \pmod p}} e^{\pi i \mathrm{tr}\left(\frac{x^{-1}+y^{-1}+z^{-1}}{p}\right)} = \sum_{\substack{x,y,z\in G_p^*\\ x^{-1}+y^{-1}+z^{-1}\equiv 0 \pmod p}} e^{\pi i \mathrm{tr}\left(\frac{x+y+z}{p}\right)}.$$

The condition $x^{-1}+y^{-1}+z^{-1} \equiv 0 \pmod p$ is equivalent to $xy+xz+yz \equiv 0 \pmod p$. Let us $f(x,y,z) = xy+xz+yz$ and $z = \tau-(x+y)$. Then in notations of theorem we have $F_\tau(x,y) = xy+(x+y)(\tau-x-y)$. In order the polynomial $F_\tau(x,y)$ was absolutely irreducible modulo p it is sufficient the fulfilment of a condition the system of equations

$$\begin{cases} \frac{\partial K}{\partial x} = 2x+y+\tau w = 0, \\ \frac{\partial K}{\partial y} = x+2y+\tau w = 0, \\ \frac{\partial K}{\partial w} = x+y = 0, \end{cases} \tag{18}$$

where $K(x,y,w) = w^2 F_\tau\left(\frac{x}{w},\frac{y}{w}\right)$ has not solutions (x_0,y_0,w_0) with $w_0 \neq 0$ for all values $\tau \in \overline{\mathbb{F}}_q$ except $O(1)$ among them.

But the system (21) has not solutions (x_0,y_0,w_0) with $w_0 \neq 0$ if $\tau \neq 0$. Hence,

$$\sum_{\substack{x,y,z\in G_p^*\\ x+y+z\equiv 0 \pmod p}} e^{\pi i \mathrm{tr}\left(\frac{x^{-1}+y^{-1}+z^{-1}}{p}\right)} \ll p^2,$$

and consequently we proved that $K^{(3)} \ll p^2$.

Conclusion. Studied p-ary Kloosterman codes of length p^2-1 in alphabet $\mathbb{F}_q$ which are the cyclic codes of the dual Melas code of length p^2-1. We obtain the weight distribution of the Melas codes in terms of one-dimensional Kloosterman sums over the ring of Gaussian integers. Derived the non-trivial bound of sum of the Kloosterman sums $k(1,\alpha z^2;p)$, $\alpha \in G_p$, when α runs the system of reduced residues modulo p in $\mathbb{Z}$.

1. **Evans R. J.** Seventh power moments of Kloosterman sums / R. J. Evans // Israel J. Math. – 2010. – 175. – P. 349–362.

2. **Van der Geer G.** Weight Formulae for Ternary Melas Codes / G. van der Geer, R. Schoof, M. van der Vlugt // Mathem Comput. – 1992.– 58(198). – P. 781–792.

3. **Hooley C.** On another sieve method and the number that are a sum of two h-th powers / C. Hooley // Proc. London Math. Soc.(3). – 1981. – 43(1). – P. 73–109.

4. **Iwaniec H.** Topic in Classical Automorphic Forms / H. Iwaniec // Graduate Studies in Mathematics, American Math. Soc., Providence, R1. – 1997. – Vol. 17. – P. 259.

5. **Lachaud G.** Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2 / G. Lachaud, J. Wolfmann // C. R. Acad. Sci. Paris Sér. – 1987. – 305(1). – P. 881–883.

6. **Lachaud G.** The weights of the orthogonals of the extended quadratic binaryGoppa codes / G. Lachaud, J. Wolfmann // IEEE Transactions on Information Theory. – 1990. – 36(3). – P. 685–692.

7. **MacWilliams F. J.** The Theory of Error-Correcting Codes / F. J. MacWilliams, N. J. A. Sloane. – Elsevier: North-Holland, Amsterdam, 1977. – P. 762.

8. **Marko Moisio.** Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros / Marko Moisio, Kalle Ranto // Finite Fields and Their Applications. – 2007. – 13. – P. 922–935.

9. **Marko Moisio.** On the moments of Kloosterman sums and fibre products of Kloosterman curves / Marko Moisio // Finite Fields and Their Applications. – 2008. – 14(2). – P. 515–531.

10. **Pless V.** Power Moment Identities on Weight Distributions in Error Correcting Codes / V. Pless // Information and Control. – 1963. – 6. – P. 147–152.

11. **Ping Xi** A note the moments of Kloosterman sums / Ping Xi and Yuan Yi // arXiv:1108.0746v2 [math.NT], to appear in PAMS. – 2011. – 8 p.