Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 83–87*

On Kloosterman sums over finite fields of characteristic 3[1]

L. A. Bassalygo bass@iitp.ru
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

Abstract. We study the divisibility by 3^k of Kloosterman sums $K(a)$ over finite fields of characteristic 3. We give a simple recurrent algorithm for finding the largest k, such that 3^k divides the Kloosterman sum $K(a)$. This gives a simple description of zeros of such Kloosterman sums.

1 Introduction

Let $\mathbb{F} = \mathbb{F}_{3^m}$ be a field of characteristic 3 of order 3^m, where $m \geq 2$ is an integer and let $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. By $\mathbb{F}_3$ denote the field, consisting of three elements. For any element $a \in \mathbb{F}^*$ the *Kloosterman sum* can be defined as

$$K(a) \;=\; \sum_{x \in \mathbb{F}} \omega^{Tr(x+a/x)}, \tag{1}$$

where $\omega = \exp 2\pi i/3$ is a primitive 3-th root of unity and

$$Tr(x) \;=\; x + x^3 + x^{3^2} + \cdots + x^{3^{m-1}}. \tag{2}$$

Recall that under x^{-i} we understand x^{3^m-1-i}, avoiding by this way a division into 0. Divisibility of ternary Klosterman sums $K(a)$ by 9 and by 27 was considered in [1-5]. In [6] an efficient deterministic (recursive) algorithm was given proving divisibility of Klosterman sums by 3^k.

Here we simplified some of results, given in the above papers. In particular, we give a simple test of divisibility of $K(a)$ by 27. We suggest also a recursive algorithm of finding the largest divisor of $K(a)$ of the type 3^k which does not need solving of cubic equation as in [6], but only implementation of arithmetic operation in $\mathbb{F}$. For the case when $m = g\,h$ we derive the exact connection between the divisibility by 3^k of $K(a)$ in $\mathbb{F}_{3^g}$, $a \in \mathbb{F}_{3^g}$, and the divisibility by $3^{k'}$ of $K(a)$ in $\mathbb{F}_{3^{gh}}$.

[1]This work has been partially supported by the Russian fund of fundamental researches (under the project No. 12 - 01 - 00905).

2 Known results

In this section we state the known results [1 - 5] about Kloosterman sums $K(a)$ over finite fields $\mathbb{F}_q$ of characteristic 3. Our interest is the divisibility of such sums by the maximal possible number of type 3^k (i.e. 3^k divides $K(a)$, but 3^{k+1} does not divide $K(a)$; in addition, when $K(a) = 0$ we assume that 3^m divides $K(a)$, but 3^{m+1} does not divide).

For a given $\mathbb{F}$ and any $a \in \mathbb{F}^*$ define the elliptic curve $E(a)$ as follows:

$$E(a) \;=\; \{(x,y) \in \mathbb{F} \times \mathbb{F} : \; y^2 = x^3 + x^2 - a\}. \tag{3}$$

The set of $\mathbb{F}$-rational points of the curve $E(a)$ over $\mathbb{F}$ forms a finite abelian group, which can be represented as a direct product of a cyclic subgroup $G(a)$ of order 3^t and a certain subgroup $H(a)$ of some order s (which is not multiple to 3): $E(a) = G(a) \times H(a)$, such that

$$|E(a)| \;=\; 3^t \cdot s$$

for some integers $t \geq 2$ and $s \geq 1$ (see [7]), where $s \not\equiv 0 \pmod 3$.

Moisio [3] showed that

$$|E(a)| \;=\; 3^m + K(a), \tag{4}$$

where $|A|$ denotes the cardinality of a finite set A. Therefore a Kloosterman sum $K(a)$ is divisible by 3^t, if and only if the number of points of the curve $E(a)$ is divisible by 3^t. Lisonek [2] observed, that $|E(a)|$ is divisible by 3^t, if and only if the group $E(a)$ contains an element of order 3^t.

Since $|E(a)|$ is divisible by $|G(a)|$, which is equal to 3^t, then generator elements of $G(a)$ and only these elements are of order 3^t.

Let $Q = (\xi, *) \in E(a)$. Then the point $P = (x, *) \in E(a)$, such that $Q = 3P$ exists, if and only if the equation

$$x^9 - \xi x^6 + a(1-\xi)x^3 - a^2(a+\xi) \;=\; 0.$$

has a solution in $\mathbb{F}$. This equation is equivalent to equation

$$x^3 - \xi^{1/3}x^2 + (a(1-\xi))^{1/3}x - (a^2(a+\xi))^{1/3} \;=\; 0. \tag{5}$$

The equation (5) is solvable in $\mathbb{F}$ if and only if

$$Tr\left(\frac{a\sqrt{\xi^3+\xi^2-a}}{\xi^3}\right) \;=\; 0\;. \tag{6}$$

Since the point $(a^{1/3}, a^{1/3})$ belongs to $G(a)$ and has order 3, then solving the recursive equation

$$x_i^3 - x_{i-1}^{1/3}x_i^2 + (a(1-x_{i-1}))^{1/3}x_i - (a^2(a+x_{i-1}))^{1/3} \;=\; 0, \quad i = 0, 1, ... \tag{7}$$

with initial value $x_0 = a^{1/3}$, we obtain that the point $(x_i, *) \in G(a)$ for $i = 0, 1, \ldots, t-1$, and the point $(x_{t-1}, *)$ is a generator element of $G(a)$. Such algorithm of finding of cardinality of $G(a)$ was given in [6].

Similar method was presented in our previous paper [8] for finite fields of characteristic 2. Besides, some another results have been obtained in [8] for the case $p = 2$. Our purpose here is to generalize these results for finite fields of characteristic 3.

3 New results

We begin with simple result. It is known [1, 4], that 9 divides $K(a)$ if and only if $Tr(a) = 0$. In this case a can be presented as follows: $a = z^{27} - z^9$, where $z \in \mathbb{F}$, and, hence $x_0 = a^{1/3} = z^9 - z^3$ (see (7)). We found the expression for the next element x_1, namely:

$$x_1 = z^2(z+1)(z^2+1)(z-1)^4$$

and, therefore, from condition (6), the following result holds.

Statement 1. *Let $a \in \mathbb{F}^*$ and $Tr(a) = 0$, i.e. a can be presented in the form: $a = z^{27} - z^9$. Then $x_0 = z^9 - z^3$, $x_1 = z^2(z+1)(z^2+1)(z-1)^4$, and, therefore, $K(a)$ is divisible by 27, if and only if*

$$\mathrm{Tr}\left(\frac{z^5(z-1)(z+1)^7}{(z^2+1)^3}\right) \;=\; 0, \tag{8}$$

This condition (8) is less bulky than the corresponding condition from the paper [5], where it is proven that $K(a)$ is divisible by 27, if $Tr(a) = 0$ and

$$2 \sum_{1 \le i,j \le m-1} a^{3^i+3^j} \;+\; \sum_{1 \le i \ne j \ne k \le m-1} a^{3^i+3^j+3^k} \;=\; 0.$$

Similar to the case $p = 2$ [8], we give now also another algorithm to find the maximal divisor of $K(a)$ of the type 3^t, which does not require solving of the cubic equations (5), but only consequent implementation of arithmetic operations in $\mathbb{F}$.

Let $a \in \mathbb{F}^*$ be an arbitrary element and let $u_1, u_2, \ldots, u_\ell$ be a sequence of elements of $\mathbb{F}$, constructed according to the following recurrent relation (compare with (7):

$$u_{i+1} \;=\; \frac{(u_i^3 - a)^3 \;+\; a u_i^3}{(u_i^3 - a)^2}, \quad i = 1, 2, \ldots, \tag{9}$$

where $(u_1, *) \in E(a)$ and

$$Tr\left(\frac{a\sqrt{u_1^3 + u_1^2 - a}}{u_1^3}\right) \;\ne\; 0\;. \tag{10}$$

Then the following result is valid.

Theorem 1. *Let $a \in \mathbb{F}^*$ and let $u_1, u_2, \ldots, u_\ell$ be a sequence of elements of $\mathbb{F}$, which satisfies the recurrent relation (9), where the element u_1 satisfies (10). Then there exists an integer $k \le m$ such that one of the two following cases takes place:*
(i) either $u_k = a^{1/3}$, but all the previous u_i are not equal to $a^{1/3}$;
(ii) or $u_{k+1} = u_{k+1+r}$ for a certain r and all u_i are different for $i < k+1+r$.
In the both cases the Kloosterman sum $K(a)$ is divisible by 3^k and is not divisible by 3^{k+1}.

Directly from Theorem 1 we obtain the following necessary and sufficient condition for an element $a \in \mathbb{F}^*$ to be a zero of the Kloosterman sum $K(a)$.

Corollary 1. *Let $a \in \mathbb{F}^*$ and $u_1, u_2, \ldots, u_\ell$ be the sequence of elements of $\mathbb{F}$, which satisfies the recurrent relation (9), where the element u_1 satisfies (10). Then $K(a) = 0$, if and only if $u_m = a^{1/3}$, and $u_i \ne a^{1/3}$ for all $1 \le i \le m-1$.*

Assume now that the field $\mathbb{F}_q$ of order $q = 3^m$ is embedded into the field $\mathbb{F}_{q^n}$ $(n \ge 2)$, and a is an element of $\mathbb{F}_q^*$. Recall that

$$Tr_{q^n \to q}(x) \;=\; x + x^q + x^{q^2} + \ldots + x^{q^{n-1}}, \quad x \in \mathbb{F}_{q^n},$$

and ω is a primitive 3-th root of unity. For any elements $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q^n}$ define

$$e(a) \;=\; \omega^{Tr(a)}, \quad e_n(b) \;=\; \omega^{Tr(Tr_{q^n \to q}(b))}.$$

For a given $a \in \mathbb{F}_q^*$ it is possible to consider the following two Kloosterman sums:

$$K(a) \;=\; \sum_{x \in \mathbb{F}_q} e\left(x + \frac{a}{x}\right), \quad K_n(a) \;=\; \sum_{x \in \mathbb{F}_{q^n}} e_n\left(x + \frac{a}{x}\right).$$

Denote by $H(a)$ the maximal degree of 3, which divides $K(a)$, and by $H_n(a)$ the maximal degree of 3, which divides $K_n(a)$. There exists a simple connection between $H(a)$ and $H_n(a)$.

Theorem 2. *Let $n = 3^h \cdot s$, $n \ge 2$, $s \ge 1$, where 3 and s are mutually prime, and $a \in \mathbb{F}_q^*$. Then*

$$H_n(a) \;=\; H(a) \;+\; h.$$

From Theorem 2 we immediately obtain the following known result [4].

Corollary 2. *Let $a \in \mathbb{F}_q^*$ and $n \ge 2$. Then $K_n(a)$ is not equal to zero.*

References.

[1] van der Geer G., van der Vlugt M., Kloosterman sums and the p-torsion of certain Jacobians, Math. Ann., 1991, vol. 290, no. 3, pp. 549 - 563.

[2] Lisonek P., On the connection between Kloosterman sums and elliptic curves. In: Proceedings of the 5th International Conference on Sequences and Their Applications (SETA 2008) (S. Golomb et al. Eds.), Lecture Notes in Computer Science, Springer, 2008, vol. 5203, pp. 182 - 187.

[3] Moisio M., Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, Acta Arith., 2008, vol. 132, 4, pp. 329 - 350.

[4] Lisonek P., Moisio M., On zeros of Kloosterman sums, Designs, Codes and Cryptography, 2011, vol. 59, no. 1 - 3, pp. 223- 230.

[5] G'ologlu F., McGuire G., & R. Moloney R., Some results on Kloosterman sums and their minimal polynomials, in: "Seventh International Workshop on Coding and Cryptography, WCC 2011", April 11-15, 2011, Paris, France, Proceedings (eds. D. Augot & A. Canteaut), 2011, pp. 403 - 412.

[6] Ahmadi O., Granger R. An efficient deterministic test for Kloosterman sum zeros, arXiv: 1104.3882v1 [math.NT] 19 Apr 2011.

[7] Enge A., Elliptic curves and their applications to cryptography: an introduction, Klumer Academic Publishers, Boston, 1999.

[8] Bassalygo L.A., Zinoviev V.A., On divisibility of exponential sums of polynomials of special type over fields of characteristic 2, Designs, Codes and Cryptography, 2012, to appear.