**Доклади на Българската академия на науките**
**Comptes rendus de l'Académie bulgare des Sciences**
*Tome 75, No 5, 2022*

*MATHEMATICS*
*Number theory*

# A NOTE ON THE IRRATIONALITY OF ANGLES OF KLOOSTERMAN SUMS OVER FINITE FIELD

**Lyubomir Borissov, Yuri Borissov**

*Received on January 19, 2022*
*Presented by V. Drensky, Member of BAS, on January 27, 2022*

**Abstract**

We prove that the angles of Kloosterman sums over arbitrary finite field are incommensurable with the constant $\pi$.

**Key words:** Kloosterman sum over finite field, angle of Kloosterman sum, Weil bound

**2020 Mathematics Subject Classification:** 11L05, 11T71

**1. Introduction.** Let $\mathbb{F}_q$ be the finite field of characteristic $p$ and order $q = p^m$. As usual, denote by $\mathbb{F}_q^*$ the set of non-zero elements of $\mathbb{F}_q$, and by $\zeta_n$ the primitive $n$-th root of unity $e^{\frac{2\pi i}{n}}$.

Throughout this note we will use the following form of the definition of Kloosterman sum over a finite field.

**Definition 1.** For each $u \in \mathbb{F}_q$, the *Kloosterman sum* $\mathcal{K}_q(u)$ is a special kind exponential sum defined by

$$\mathcal{K}_q(u) = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{\,\mathrm{Tr}(x+u/x)},$$

and the *trace* $\mathrm{Tr}(a)$ over $\mathbb{F}_p$ of an element $a \in \mathbb{F}_q$ is defined as

$$\mathrm{Tr}(a) = a + a^p + \cdots + a^{p^{m-1}}.$$

A preliminary abstract version of this paper was published in the Proc. of the Sixth International Workshop "Boolean Functions and their Applications", Rosendal, Norway, September 6–10, 2021. This work is partially supported by the Bulgarian NSF under Contract KP-06-Russia/33/17.12.2020 and Contract KP-06-N32/2-2019.

DOI:10.7546/CRABS.2022.05.03

It can be easily shown that $\mathcal{K}_q(u)$ is a real non-zero number. Recall, as well, that the Weil bound [1] states:

$$|\mathcal{K}_q(u)| \leq 2\sqrt{q}. \tag{1}$$

This inequality implies the existence of a unique real number $\theta_u$ such that

$$\frac{\mathcal{K}_q(u)}{2\sqrt{q}} = \cos\theta_u, \quad 0 \leq \theta_u \leq \pi, \quad \theta_u \neq \pi/2. \tag{2}$$

The angle $\theta_u$ is referred to as *angle* of the Kloosterman sum $\mathcal{K}_q(u)$.

The behaviour of the angles of Kloosterman sums has been studied by many authors. Here, we only refer to some of these works [2–5], and that list of references is definitely far from being complete.

It is worth pointing out the existence of some successful attempts to show that inequality (1) is always strict for the angles of the simplest Kloosterman sums $\mathcal{K}_p(u)$, $u \in \mathbb{F}_p$ (see [6], Theorem 8) which means that $\theta_u \neq 0, \pi$ in this particular case.

In the present article, based on deep facts from Algebraic Number Theory (see, e.g., [7]), we prove a more general result that for any $u \in \mathbb{F}_q$ the ratio $\theta_u/\pi$ takes only irrational values, thus establishing additional constraints of the same type as the strictness of inequality (1). (As an immediate consequence a new proof for the strictness of that bound is obtained.) Our result resembles the result with respect to the so-called Frobenius angles obtained in [8] but it seems no transparent logical connection between the two results can be found out.

This short note is organized as follows. In the next section we recall some background from Algebraic Number Theory. Then in Section 3 we give several necessary lemmas. In Section 4 the main result is exposed and illustrated in two examples.

**2. Some background from algebraic number theory.** We need some notions from Algebraic Number Theory as *algebraic number*, *minimal polynomial of an algebraic number* and *algebraic integer* (see, e.g., [9]).

An algebraic number is one that satisfies some equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{3}$$

with rational coefficients. (A polynomial having leading coefficient 1 is called monic.) Any algebraic number $\alpha$ satisfies a unique monic polynomial equation of smallest degree, called the minimal polynomial of $\alpha$, and the algebraic degree of $\alpha$ (over the field of rational numbers $\mathbb{Q}$) is defined as the degree of its minimal polynomial. If an algebraic number $\alpha$ satisfies some equation of type (3) with integer coefficients, we say that $\alpha$ is an *algebraic integer*. The minimal polynomial of an algebraic integer is also with integer coefficients.

Recall as well that the set of all algebraic numbers forms a number field while the set of all algebraic integers constitutes only a ring which contains the square root of each own element.

For more sophisticated concepts of Algebraic Number Theory we direct the readers to [7] or [10]. Herein, in the amount of knowledge needed for this paper we recall some basic facts concerning those notions.

Let $\alpha$ be an algebraic number with minimal polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$. The $n$ roots of $f(x)$, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are called conjugates of $\alpha$. The *absolute norm* $\mathcal{N}(\alpha)$ of $\alpha$ is defined as $\mathcal{N}(\alpha) = \prod_{i=1}^{n} \alpha_i$. Evidently, $\mathcal{N}(\alpha) = (-1)^n a_n$.

In general, given a finite extension of number fields $L/K$, the norm $\mathcal{N}_{L/K}(\gamma)$ of an arbitrary $\gamma \in L$ can be defined which in case $K = \mathbb{Q}$ and $L = \mathbb{Q}(\gamma)$ coincides with $\mathcal{N}(\gamma)$. ($\mathbb{Q}(\gamma)$ stands for the number field obtained by adjoining $\gamma$ to $\mathbb{Q}$. In particular, $\mathbb{Q}(\zeta_n)$ is the so-called cyclotomic field generated by $\zeta_n$.)

We shall make use of the following properties of norm:

$\mathcal{P}1$: If $L \supset \mathbb{Q}(\alpha)$, then $\mathcal{N}_{L/\mathbb{Q}}(\alpha) = \mathcal{N}^e(\alpha)$, where $e$ is the degree of extension $L/\mathbb{Q}(\alpha)$.

Particularly, if $\alpha$ is an algebraic integer, then $\mathcal{N}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

$\mathcal{P}2$: (the multiplicative property of norm) For arbitrary $\alpha, \beta \in L$ it holds:

$$\mathcal{N}_{L/K}(\alpha\beta) = \mathcal{N}_{L/K}(\alpha)\mathcal{N}_{L/K}(\beta).$$

**3. Several necessary lemmas.** We shall make use of five facts stated herein as lemmas.

Definition 1 easily implies the following lemma.

**Lemma 1.** *The Kloosterman sum $\mathcal{K}_q(u)$ is an algebraic integer which belongs to the cyclotomic field $\mathbb{Q}(\zeta_p)$.*

**Lemma 2.** *For an arbitrary prime $p$ and positive integer $m$, the number $\sqrt{p^m}$ is an algebraic integer that belongs to the cyclotomic field $\mathbb{Q}(\zeta_n)$, where*

$$n = \begin{cases} 8, & \text{if } p = 2 \\ p, & \text{if } p \equiv 1 \pmod 4 \\ 4p, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

**Proof.** The case of even $m$ is trivial. Consider, now, the case $m = 1$. If $p = 2$, then the evident $\sqrt{2} = 2\cos\pi/4 = \zeta_8 + \zeta_8^{-1}$ implies the claim. If $p > 2$, the assertion is an immediate consequence of Proposition 6.4.3 in [11]. Finally, $\sqrt{p^m} = (\sqrt{p})^m \in \mathbb{Q}(\zeta_n)$ completes the proof when $m$ is odd $> 1$. □

**Lemma 3.** *For any $r = k/n \in \mathbb{Q}$ with relative primes $k$ and $n > 0$, the trigonometric value $2\cos(2\pi r)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_n)$.*

**Proof.** Indeed, $2\cos(2\pi r) = \zeta_n^k + \zeta_n^{n-k}$. □

**Remark 1.** Lemma 3 is a part of LEHMER's work [12] (Theorem 1) which in addition to that describes the minimal polynomial of trigonometric value $2\cos(2\pi r)$.

We also need the following obvious lemma.

**Lemma 4.** *The cyclotomic fields $\mathbb{Q}(\zeta_k)$ and $\mathbb{Q}(\zeta_l)$ can be embedded in the cyclotomic field $\mathbb{Q}(\zeta_m)$, where $m$ is the least common multiple of $k$ and $l$.*

The next lemma can be easily derived by Lemma 11 in [13]. Herein, we recall this fact for the reader's convenience.

$\mathcal{F}$: Let $g(x) = x^t - g_1x^{t-1} + g_2x^{t-2} - \cdots + (-1)^t g_t \in \mathbb{Z}[x]$ be the minimal polynomial of $\mathcal{K}_q(u)$, $u \neq 0$. Then, for $k = 1, \ldots, t$, we have $g_k \equiv (-1)^k \binom{t}{k} \pmod p$.

**Lemma 5.** *For any $u \in \mathbb{F}_q$, the absolute norm of Kloosterman sum $\mathcal{K}_q(u)$ satisfies the congruence:*

$$\mathcal{N}(\mathcal{K}_q(u)) \equiv (-1)^t \pmod p,$$

*where $t$ is the algebraic degree of $\mathcal{K}_q(u)$.*

**Proof.** The case $u = 0$ is trivial since $\mathcal{K}_q(0) = -1$. If $u \in \mathbb{F}_q^*$, the claim follows by fact $\mathcal{F}$ for $k = t$. □

**4. Main result.** Now, we are in position to prove the main result of this note.

**Theorem 1.** *For any $u \in \mathbb{F}_q$, the angle $\theta_u$ of the Kloosterman sums $\mathcal{K}_q(u)$ is not rational multiple of $\pi$.*

**Proof.** Rewriting Eq. (2), we have:

$$\mathcal{K}_q(u) = \sqrt{q} * 2\cos\theta_u. \tag{4}$$

Assume the contrary that $\theta_u = 2\pi r$ for some $r \in \mathbb{Q}$. Lemmas 1, 2 and 3 show that the algebraic integers $\mathcal{K}_q(u)$, $\sqrt{q} = p^{m/2}$ and $2\cos 2\pi r$ belong to cyclotomic fields. Now, Lemma 4 implies that the number fields $\mathbb{Q}(\mathcal{K}_q(u))$, $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(2\cos 2\pi r)$ can be embedded in a common (cyclotomic) field $L$ with extension degrees, say, $e_1$, $e_2$ and $e_3$, respectively.

Further, by $\mathcal{P}1$ and Lemma 5 we easily get:

$$\mathcal{N}_{L/\mathbb{Q}}(\mathcal{K}_q(u)) = \mathcal{N}^{e_1}(\mathcal{K}_q(u)) \equiv \pm 1 \pmod p. \tag{5}$$

But, on the other hand, by Eq. (4) and properties $\mathcal{P}2$ and $\mathcal{P}1$ we consecutively obtain:

$$\begin{aligned}\mathcal{N}_{L/\mathbb{Q}}(\mathcal{K}_q(u)) &= \mathcal{N}_{L/\mathbb{Q}}(\sqrt{q} * 2\cos\theta_u)\\ &= \mathcal{N}_{L/\mathbb{Q}}(\sqrt{q})\mathcal{N}_{L/\mathbb{Q}}(2\cos\theta_u)\\ &= \mathcal{N}^{e_2}(\sqrt{q})\mathcal{N}^{e_3}(2\cos 2\pi r).\end{aligned}$$

And, the apparent fact:

$$\mathcal{N}(\sqrt{q}) = \begin{cases} p^{m/2}, & \text{if } m \equiv 0 \pmod 2 \\ -p^m, & \text{if } m \equiv 1 \pmod 2 \end{cases}$$

alongside with $\mathcal{N}(2\cos 2\pi r) \in \mathbb{Z}$ (which follows by Lemma 3), imply that

$$\mathcal{N}_{L/\mathbb{Q}}(\mathcal{K}_q(u)) \equiv 0 \pmod p.$$

The latter contradicts Congr. (5) and completes the proof. □

As an application of Theorem 1 we get the next corollary (see also the remark after Theorem 3 in [14]).

**Corollary 1.** *The Weil bound cannot be attained by the sums $\mathcal{K}_q(u)$, $u \in \mathbb{F}_q$.*

**Proof.** Suppose for some $u \in \mathbb{F}_q$ it holds $|\mathcal{K}_q(u)| = 2\sqrt{q}$. Then, evidently, either $\theta_u = 0$ or $\theta_u = \pi$ which contradicts the assertion of Theorem 1. □

**Remark 2.** It is well known that in case $m = 1$ the estimate $2\sqrt{p}$ is essentially best possible (see, e.g., [15] or [16] for brief explanation of the relevant reasoning). In addition, Corollary 1 shows the non-existence of a prime $p$ such that $2\sqrt{p}$ is an admissible value for some $|\mathcal{K}_p(u)|$, $u \in \mathbb{F}_p^*$.

Just for illustration we give the following two examples.

**Example 1.** Let $q = 3$, so $\mathcal{K}_3(1) = -1$ and $\mathcal{K}_3(2) = 2$. Thus, the minimal polynomials for $2\cos\theta_1$ and $2\cos\theta_2$ are $x^2 - 1/3$ and $x^2 - 4/3$, and therefore these trigonometric values are not algebraic integers.

**Example 2.** Let $u \in \mathbb{F}_q^*$ with $q = p^m$ ($p \in \{2, 3\}$) be a Kloosterman zero (see, e.g., [17] about the definition and conditions for existence). Then $2\cos\theta_u = -1/p^{m/2}$ and its minimal polynomial is: $x^2 - 1/p^m$ in case $m$ odd; $x + 1/p^{m/2}$ in case $m$ even. So, $2cos\theta_u$ is not an algebraic integer and therefore $\theta_u/\pi \notin \mathbb{Q}$.

## REFERENCES


[1] Weil A. (1948) On some exponential sums, Proc. Nat. Acad. Sci. USA, **34**, 204–207.

[2] Adolphson A. (1989) On the distribution of angles of Kloosterman sums, J. für die Reine und Angew. Math., **395**, 214–220.

[3] Fouvry É., P. Michel, J. Rivat, A. Sárközy (2004) On the pseudorandomness of the signs of Kloosterman sums, J. Aust. Math. Soc., **77**, 425–436.

[4] Niederreiter H. (1991) The distribution of values of Kloosterman sums, Arch. Math., **56**, 270–277.

[5] Shparlinski I. (2008) On the distribution of Kloosterman sums, Proc. AMS, **136**, 419–425.

[6] Harcos G. (2015) Weil's bound for Kloosterman sums, preprint, available on `https://users.renyi.hu/~gharcos/weil.pdf`, 14 pp.

[7] Marcus D. A. (2018) Number Fields, 2nd ed., Springer International Publishing AG, Part of Springer Nature, 9–28.

[8] Ahmadi O., I. Shparlnski (2010) On the distributions of the number of points on algebraic curves in extensions of finite fields, Math. Res. Lett., **17**(4), 689–699.
[9] Niven I. (1963) Irrational Numbers, The Math. Assoc. of America, 2nd printing, distributed by John Wiley and Sons, 28–29.
[10] Borevich Z. I., I. R. Shafarevich (1966) Number Theory, New York, San Francisco, London, Academic Press Inc., 390–415.
[11] Ireland K., M. Rosen (1990) A Classical Introduction to Modern Number Theory, 2nd ed., New York, Springer-Verlag, 66–73.
[12] Lehmer D. H. (1933) A note on trigonometric algebraic numbers, Am. Math. Monthly, **40**(3), 165–166.
[13] Moisio M. (2009) On certain values of Kloosterman sums, IEEE Trans. on IT, **55**(8), 3563–3564.
[14] Conrad K. (2002) On Weil's proof of the bound for Kloosterman sums, J. Number Theory, **97**, 439–446.
[15] Heath-Brown D. R. (2000) Arithmetic applications of Kloosterman sums, NAW, **5/1**(4), 380–384.
[16] Tolev D. I. (2016) Lectures on Elementary and Analytic Number Theory – Part I, Sofia, St. Kliment Ohridski University Press, 337 pp (in Bulgarian).
[17] Lisonek P., M. Moisio (2011) On zeros of Kloosterman sums, Designs, Codes and Cryptography, **59**(3), 223–230.

*Institute of Mathematics and Informatics*
*Bulgarian Academy of Sciences*
*Akad. G. Bonchev St, Bl. 8*
*1113 Sofia, Bulgaria*
*e-mails*: lubobs90@math.bas.bg
youri@math.bas.bg