On the irrationality of the angles of Kloosterman sums over $\mathbb{F}_p$

Lyubomir Borissov* and Yuri Borissov*

*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

Abstract

We prove that for arbitrary prime p the angles of Kloosterman sums over the field $\mathbb{F}_p$ are incommensurable with the constant π.

1 Introduction

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

Let us recall the notion of classical Kloosterman sum over $\mathbb{F}_q$.

Definition 1.1 *For each $u \in \mathbb{F}_q$, the* Kloosterman sum $\mathcal{K}_q(u)$ *is a special kind exponential sum defined by*

$$\mathcal{K}_q(u) = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{\;Tr(x+ux^{-1})},$$

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

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

It can be easily shown that $\mathcal{K}_q(u)$ is a real non-zero number. Recall, as well, that the Weil bound (see, [12]) states:

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

This inequality implies the existence of a unique real number θ_u such that

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

The angle θ_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 (see, [1][2][5][9][11]), and that list is certainly far from being complete.

The simplest kind of Kloosterman sum is that over the prime field $\mathbb{F}_p$, i.e., of the form $\mathcal{K}_p(u) = \sum_{x \in \mathbb{F}_p^*} \zeta_p^{x+ux^{-1}}$. It is worth pointing out the existence of some successful attempts to prove that the inequality (1) is always strict for the angles of $\mathcal{K}_p(u), u \in \mathbb{F}_p$, so $\theta_u \neq 0, \pi$ (see [3, Theorem 8]).

In the present paper, we show that for any $u \in \mathbb{F}_p$ the ratio θ_u/π takes only irrational values, thus establishing additional constraints of the same type as the strictness of the inequality (1).

2 Preliminaries

We need some notions from Algebraic Number Theory (ANT) as *algebraic number*, *minimal polynomial of an algebraic number* and *algebraic integer* (see, e.g. [10, Chapter 3]). An algebraic number is one that satisfies some equation of the form

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

with rational coefficients. (A polynomial having leading coefficient 1 is called monic.) Any algebraic number α satisfies a unique monic polynomial equation of smallest degree, called the minimal polynomial of α, and the algebraic degree of α (over the field of rational numbers $\mathbb{Q}$) is defined as the degree of its minimal polynomial. Remind, as well, that the set of all algebraic numbers forms a number field, i.e. the sum, difference, product and ratio of algebraic numbers are algebraic, too. If an algebraic number α satisfies some equation of type (3) with integer coefficients we say that α is an *algebraic integer*. The minimal polynomial of an algebraic integer is also with integer coefficients.

For more sophisticated concepts of ANT we direct the readers to [7, Chapter 2]. Herein, in the amount of knowledge needed for this paper, we recall some basic facts concerning those notions (possibly with slight abuses).

Let α be an algebraic number with minimal polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Q}[x]$. The n roots of $f(x), \alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are called conjugates of α. The *absolute norm* $\mathcal{N}(\alpha)$ of α 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, it can be defined the norm $\mathcal{N}_{L/K}(\gamma)$ of an arbitrary $\gamma \in L$, 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 γ to $\mathbb{Q}$. In particular, $\mathbb{Q}(\zeta_n)$ is the so-called cyclotomic field generated by ζ_n.)
We shall make use of the following properties of norm:

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

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

We also use previously known facts stated here as several lemmata.

Definition 1.1 easily implies the following lemma.

Lemma 2.1 *The Kloosterman sum $\mathcal{K}_q(u)$ is an algebraic integer which belongs to the cyclotomic field $\mathbb{Q}(\zeta_p)$.*

The second one is an immediate consequence of [4, Proposition 6.4.3].

Lemma 2.2 *For arbitrary odd prime p, the number $\sqrt{p}$ is an algebraic integer that belongs to the cyclotomic field $\mathbb{Q}(\zeta_n)$ where*

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

Lemma 2.3 *For any $r = \frac{k}{n} \in \mathbb{Q}$ with relatively primes k and $n > 0$, the trigonometric value $2\cos(2\pi r)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_n)$.*

Remark 2.4 *Lemma 2.3 is a part of D. H. Lehmer's work [6, Theorem 1].*

We shall need, as well, the next simple lemma.

Lemma 2.5 *The cyclotomic fields $\mathbb{Q}(\zeta_k)$ and $\mathbb{Q}(\zeta_l)$ can be embedded in a common cyclotomic field, e.g., $\mathbb{Q}(\zeta_{LCM(k,l)})$ where $LCM(k,l)$ stands for the least common multiple of k and l.*

The last lemma is derived by [8, Lemma 11].

Lemma 2.6 *For any $u \in \mathbb{F}_q^*$, the absolute norm of Kloosterman sum $\mathcal{K}_q(u)$ satisfies the congruence $\mathcal{N}(\mathcal{K}_q(u)) \equiv (-1)^d \pmod{p}$ where d is the algebraic degree of $\mathcal{K}_q(u)$.*

Remark 2.7 *Since $\mathcal{K}_q(0) = -1$ then $\mathcal{N}(\mathcal{K}_q(0)) = -1$ which means that Lemma 2.6 is still valid for $u = 0$.*

3 Results and their proofs

We will prove the following theorem.

Theorem 3.1 *Let p be an odd prime. Then, for each $u \in \mathbb{F}_p$, the angle θ_u of the Kloosterman sum $\mathcal{K}_p(u)$ and π are incommensurable, i.e., their ratio θ_u/π is an irrational number.*

Proof: By Eq. (2) we have:

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

Assume, on the contrary, $\theta_u = 2\pi r$ for some $r \in \mathbb{Q}$.

Lemmata 2.1, 2.2 and 2.3 show that $\mathcal{K}_p(u)$, $\sqrt{p}$ and $2\cos 2\pi r$, respectively, belong to some cyclotomic fields. Now, Lemma 2.5 implies that the number fields: $\mathbb{Q}(\mathcal{K}_p(u)), \mathbb{Q}(\sqrt{p})$ 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, on the one hand, by $\mathcal{P}1$ and Lemma 2.6 (with $q = p$) we easily get:

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

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

$$\mathcal{N}_{L/\mathbb{Q}}(\mathcal{K}_p(u)) = \mathcal{N}_{L/\mathbb{Q}}(\sqrt{p} * 2\cos\theta_u) =$$

$$\mathcal{N}_{L/\mathbb{Q}}(\sqrt{p})\mathcal{N}_{L/\mathbb{Q}}(2\cos\theta_u) = \mathcal{N}^{e_2}(\sqrt{p})\mathcal{N}^{e_3}(2\cos 2\pi r).$$

Hence, by the apparent $\mathcal{N}(\sqrt{p}) = -p$ and by $\mathcal{N}(2\cos 2\pi r) \in \mathbb{Z}$ which is deduced from Lemma 2.3, it follows $\mathcal{N}_{L/\mathbb{Q}}(\mathcal{K}_p(u)) \equiv 0 \pmod{p}$. The latter congruence contradicts Congr. (5) which completes the proof. $\square$

Remark 3.2 *In case $p = 2$, we have: $2\cos\theta_1 = \mathcal{K}_2(1)/\sqrt{2} = \frac{1}{\sqrt{2}}$. Thus, $2\cos\theta_1$ is a root of $x^2 - \frac{1}{2} = 0$, so it is not an algebraic integer. Now, Lemma 2.3 implies the counterpart of Theorem 3.1 for binary case.*

Example 3.3 *Hereinafter, we present two examples illustrating the main statement.*

- *Let $p = 3$, so $\mathcal{K}_3(1) = -1$ and $\mathcal{K}_3(2) = 2$. Thus, $x^2 - \frac{1}{3}$ and $x^2 - \frac{4}{3}$ are minimal for $2\cos\theta_1$ and $2\cos\theta_2$, so these trigonometric values are not algebraic integers.*
- *Let $u \in \mathbb{F}_q^*$ with $q = p^m$ ($p = 2, 3$) be a Kloosterman zero. Then $2\cos\theta_u = -\frac{1}{p^{m/2}}$ and its minimal polynomial is: $x^2 - \frac{1}{p^m}$ in case m odd; $x + \frac{1}{p^{m/2}}$ in case m even. So, $2\ cos\theta_u$ is not an algebraic integer and therefore $\theta_u/\pi \in \mathbb{R} \setminus \mathbb{Q}$.*

Remark 3.4 *The assertion of Theorem 3.1 seems to be valid in more general settings. However, the precise statement and proof of this result are postponed to a forthcoming extended version of that paper.*

As an immediate consequence of Theorem 3.1, we obtain the following corollary.

Corollary 3.5 *The Weil bound cannot be attained by the sums $\mathcal{K}_p(u), u \in \mathbb{F}_p$.*

Proof: Suppose for some $u \in \mathbb{F}_p$ it holds $\mathcal{K}_p(u) = \pm 2\sqrt{p}$. Then, evidently, either $\theta_u = 0$ or $\theta_u = \pi$ which contradicts the assertion of Theorem 3.1. $\square$

Acknowledgments

We are grateful to the anonymous referees for their comments and suggestions.
This work is supported in part by the Bulgarian NSF under Contract KP-06-N32/2-2019.

References

[1] O. Ahmadi, I. Shparlnski, "On the distributions of the number of points on algebraic curves in extensions of finite fields", Math. Res. Lett. 17 (2010), no.4, 689-699.

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

[3] G. Harcos, "Weil's bound for Kloosterman sums", preprint.

[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, (1990).

[5] N. M. Katz, *Gaus sums, Kloosterman sums and monodromy groups*, Princeton Univ. Press, Princeton, NJ (1988).

[6] D. H. Lehmer, "A note on trigonometric algebraic numbers", The American Mathematical Monthly, vol. 40.3 (1933), 165-166.

[7] D. A. Marcus, *Number Fields*, 2nd ed., Springer International Publishing AG, part of Springer Nature (2018).

[8] M. Moisio, "On certain values of Kloosterman sums", *IEEE IT*, vol. 55.8 (2009), 3563-3564.

[9] H. Niederreiter, "The distribution of values of Kloosterman sums", Arch. Math. 56, (1991), 270-277.

[10] I. Niven, *Irrational Numbers*, The Math. Assoc. of America, second printing, distributed by John Wiley and Sons, 1963.

[11] I. Shparlinski, "On the distribution of Kloosterman sums", Proc. of the Amer. Math. Soc. 136 (2008), 419-425.

[12] A. Weil, "On some exponential sums", Proc. Nat. Acad. Sci. USA 34 (1948), 204-207.