Irrationality of the Angles of Kloosterman Sums over Finite Field

Lyubomir Borissov

Institute of Mathematics and Informatics Bulgarian Academy of Sciences

Yuri Borissov (✉ youri@math.bas.bg)

Institute of Mathematics and Informatics Bulgarian Academy of Sciences <https://orcid.org/0000-0002-7036-5529>

Research Article

Keywords: Kloosterman sum over finite field, angle of the Kloosterman sum, Weil bound.

Posted Date: January 7th, 2022

DOI: <https://doi.org/10.21203/rs.3.rs-989563/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Irrationality of the Angles of Kloosterman Sums over Finite Field

Lyubomir Borissov¹ and Yuri Borissov¹

¹ Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G. Bontchev Str., 1113 Sofia, Bulgaria.

lubobs90@math.bas.bg, your@math.bas.bg

Dedicated to Prof. Vincent Rijmen's 50th Birthday

Abstract. We prove that the angles of Kloosterman sums over arbitrary finite field are incommensurable with the constant π . In particular, this implies that the Weil bound for Kloosterman sums over finite fields cannot be reached.

keywords: Kloosterman sum over finite field, angle of the Kloosterman sum, Weil bound.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of characteristic p and order $q = p^m$. As usually, 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 $e^{\frac{2\pi i}{n}}$.

First, for reader's convenience, we recall the notion of classical Kloosterman sum over $\mathbb{F}_q$.

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

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

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

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

It can be easily shown that $\mathcal{K}_q(u)$ is a real non-zero number. Recall, as well, that the Weil bound (see [14]) states:

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

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

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

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 [1][4][7][11][13], 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 the inequality (1) is always strict for the angles of the simplest Kloosterman sums $\mathcal{K}_p(u)$, $u \in \mathbb{F}_p$ (see [5, 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., [9, Chapter 2]), we prove more general result that for any $u \in \mathbb{F}_q$ the ratio θ_u/π takes only irrational values, thus establishing additional constraints of the same type as the strictness of the inequality (1). Our result resembles the result with respect to the so-called Frobenius angles obtained in [2] but it seems a transparent logical connection between the two results cannot be found out.

This paper 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 (ANT) as *algebraic number*, *minimal polynomial of an algebraic number* and *algebraic integer* (see, e.g., [12, Chapter 3]). An algebraic number is one that satisfies some equation of the form

$$x^n + a_1x^{n-1} + \dots + a_n = 0 \quad (3)$$

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. 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.

Also remind that the set of all algebraic numbers forms a number field, i.e. the sum, difference, product and ratio of algebraic numbers are algebraic numbers, too. However, the set of all algebraic integers constitutes only a ring which contains the square root of each own element.

For more sophisticated concepts of ANT we direct the readers to [9, Chapter 2] or [3, Chapter 6]. Herein, in the amount of knowledge needed for this paper, we recall some basic facts concerning those notions.

Let α be an algebraic number with minimal polynomial $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{Q}[x]$. The n roots of $f(x)$, $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ 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 $\mathcal{N}_{L/\mathbb{Q}}(\alpha) = \mathcal{N}^e(\alpha)$, where e is the degree of extension $L/\mathbb{Q}(\alpha)$.

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:

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

3 Several Necessary Lemmas

We also make use of five facts stated hereinafter as lemmata.

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 $\sqrt[p^m]{p}$ 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 [6, Proposition 6.4.3]. Finally, $\sqrt[p^m]{p} = (\sqrt[p]{p})^m \in \mathbb{Q}(\zeta_n)$ completes the proof when m is odd > 1 . $\square$

Lemma 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 $\mathbb{Q}(\zeta_n)$.

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

Remark 1. Lemma 3 is a part of D. H. Lehmer's work [8, Theorem 1] which in addition to that describes the minimal polynomial of trigonometric value $2 \cos(2\pi r)$.

Also, we 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 is deduced by a result which is due to M. Moissio and D. Wan (see [10, Lemma 11]), and given below as the following position.

Proposition 1. Let $g(x) = x^t - g_1 x^{t-1} + g_2 x^{t-2} - \dots + (-1)^t g_t \in \mathbb{Z}[x]$ be the minimal polynomial of $\mathcal{K}_q(u)$. Then, for $k = 1, \dots, t$, 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. Follows by Proposition 1 for $k = t$. □

Remark 2. Since $\mathcal{K}_q(0) = -1$ then $\mathcal{N}(\mathcal{K}_q(0)) = -1$ which means that Lemma 5 is still valid for $u = 0$.

4 Main Result

Now, we are in position to prove the main result of this work.

Theorem 1. All angles θ_u of the Kloosterman sums $\mathcal{K}_q(u)$, $u \in \mathbb{F}_q$ are incommensurable with the constant π .

Proof. By Eq. (2) we have:

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

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

Lemmata 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, on the one hand by $\mathcal{P}1$ and Lemma 5, we easily get:

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

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

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

Finally, the apparent fact $\mathcal{N}(\sqrt{q}) = (-p)^m$ alongside with $\mathcal{N}(2 \cos 2\pi r) \in \mathbb{Z}$ which is derived by Lemma 3 and $\mathcal{P}1$, imply $\mathcal{N}_{L/\mathbb{Q}}(\mathcal{K}_q(u)) \equiv 0 \pmod{p}$. The latter contradicts Congr. (5) and completes the proof. □

As an immediate consequence of Theorem 1, we obtain the following corollary.

Corollary 1. *The Weil bound cannot be reached 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. $\square$

Let us illustrate the claim of Theorem 1 by the following two examples.

Example 1. Let $p = 3$, 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 $x^2 - \frac{1}{3}$ and $x^2 - \frac{4}{3}$, 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. 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 $\frac{\theta_u}{\pi} \notin \mathbb{Q}$.

Acknowledgments

This work is supported in part by the Bulgarian NSF under Contract KP-06-N32/2-2019.

References

1. A. Adolphson, "On the distribution of angles of Kloosterman sums", *Journal für die reine und angewandte Mathematik*, 395(1989), 214-220.
2. O. Ahmadi, I. Shparlinski, "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.
3. Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press Inc., New York, San Francisco, London (1966).
4. 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.
5. G. Harcos, "Weil's bound for Kloosterman sums", preprint.
6. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, (1990).
7. N. M. Katz, *Gaus sums, Kloosterman sums and monodromy groups*, Princeton Univ. Press, Princeton, NJ (1988).
8. D. H. Lehmer, "A note on trigonometric algebraic numbers", *The American Mathematical Monthly*, vol. 40.3 (1933), 165-166.
9. D. A. Marcus, *Number Fields*, 2nd ed., Springer International Publishing AG, part of Springer Nature (2018).
10. M. Moisio, "On certain values of Kloosterman sums", *IEEE IT*, vol. 55.8 (2009), 3563-3564.
11. H. Niederreiter, "The distribution of values of Kloosterman sums", *Arch. Math.* 56, (1991), 270-277.
12. I. Niven, *Irrational Numbers*, The Math. Assoc. of America, second printing, distributed by John Wiley and Sons, 1963.
13. I. Shparlinski, "On the distribution of Kloosterman sums", *Proc. of the Amer. Math. Soc.* 136 (2008), 419-425.
14. A. Weil, "On some exponential sums", *Proc. Nat. Acad. Sci. USA* 34 (1948), 204-207.