МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2021
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2021
Proceedings of the Fiftieth Spring Conference
of the Union of Bulgarian Mathematicians
2021

ON THE DISTINCTNESS OF SOME TERNARY KLOOSTERMAN SUMS*

Lyubomir Borissov

In this note we prove that the Kloosterman sums $\mathcal{K}_{3^n}(1)$ and $\mathcal{K}_{3^n}(2)$ are distinct for an arbitrary degree n of an extension of the field $\mathbb{F}_3$.

1. Introduction. The Kloosterman sums on finite fields play an important role in the algebraic and combinatorial coding theory and cryptography. For instance, they are related to some notable coding-theoretical and combinatorial objects such as Kloosterman and Melas codes, (hyper-)bent functions, etc. For more details about those links the reader is directed to the surveys [5] and [10].

The issue of distinctness of Kloosterman sums was studied for the first time by B. Fischer in [3]. In particular, his first result concerns the distinctness of the simplest Kloosterman sums, i.e., those for the non-zero elements of the prime field $\mathbb{F}_p$.

Recently, in [1], we have extended that result of Fischer for degrees of the field extensions which are powers of 2. In a private e-mail, Prof. D. Wan announced that a much more general statement is valid, namely, for degrees of the extension which are co-prime with the characteristic p. His proof of the latter claim makes use of Theorem 5.1 from [8] which in turn is based on a very deep fact from the algebraic number theory, namely "the finer form of the Stickelberger congruence which is an immediate consequence of the Gross-Koblitz formula [4]", see [8, Ch.5].

In the present paper we investigate the case $p = 3$ and obtain the result of distinctness for all degrees of the extension based on much *lighter* knowledge.

2. Preliminaries. Let $\mathbb{F}_q$ be the finite field of characteristic p and order $q = p^m$ and $\mathbb{F}_q^*$ be the multiplicative group of non-zero elements of $\mathbb{F}_q$.

Definition 2.1. *For each $u \in \mathbb{F}_q$, the* Kloosterman sum $\mathcal{K}_q(u)$ *is a special kind of exponential sum defined by*

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

where $\omega = e^{\frac{2\pi i}{p}}$ is a primitive $p-$th root of unity, and the trace $Tr(a)$ *over $\mathbb{F}_p$ of an element $a \in \mathbb{F}_q$ is defined as*

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

*This work is supported in part by the Bulgarian National Science Fund under Contract KP-06-Russia/33/17.12.2020.

2020 Mathematics Subject Classification: 11L05, 11T71.

Key words: Kloosterman sum on finite field, distinctness of Kloosterman sums.

The Kloosterman sum $\mathcal{K}_{q^n}(u), u \in \mathbb{F}_q$ where $\mathbb{F}_{q^n}$ is the finite field of order $q^n, n > 1$, will be referred as a lifted one (or a lift of $\mathcal{K}_q(u)$).

Example 2.2. In Table 1 of the Appendix, we present the values of the ternary Kloosterman sums $\mathcal{K}_{3^n}(1)$ and $\mathcal{K}_{3^n}(2)$ for $1 \leq n \leq 6$.

We need as well the notions of *algebraic number, minimal polynomial, degree of an algebraic number* and *algebraic integer.* Here we recall the concise definitions and facts given in [7, pp. 28-29]. An algebraic number is one that satisfies some equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{2.1}$$

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 *degree of* α (over the field of rational numbers $\mathbb{Q}$) is defined as the degree of this minimal polynomial of α. The minimal polynomial of α is irreducible over the rational numbers; it is a divisor of any other polynomial with rational coefficients having α as a zero, and it is the only monic polynomial having these properties. If an algebraic number α satisfies some equation of type (2.1) with integer coefficients, we say that α is an *algebraic integer.* It is easy to see that the minimal polynomial of an algebraic integer is also monic with integer coefficients.

We shall make use of previously known facts stated hereinafter as two lemmas.

The first is due to L. Carlitz (see, [2, Eq. 1.5]).

Lemma 2.3. *For any $u \in \mathbb{F}_q^*$, the lifted Kloosterman sum $\mathcal{K}_{q^n}(u)$ can be expressed as*

$$\mathcal{K}_{q^n}(u) = -(\alpha^n + \beta^n),$$

where α, β are the roots of the quadratic equation:

$$z^2 + \mathcal{K}_q(u) z + q = 0. \tag{2.2}$$

The Weil bound (find it in [9]) implies that the roots of Eq. (2.2) are conjugate complex numbers. The next corollary immediately follows from the above Lemma and de Moivre formula by representing these roots in polar form.

Corollary 2.4. *For any $u \in \mathbb{F}_q^*$, the lifted Kloosterman sum $\mathcal{K}_{q^n}(u)$ can be expressed as*

$$\mathcal{K}_{q^n}(u) = -2q^{n/2} \cos n\theta,$$

where $\theta = \arg(\alpha)$ is the argument of the root α of Eq. (2.2) *lying above or on the real axis.*

The second fact is due to D. H. Lehmer [6].

Lemma 2.5. *Let $r = k/n$, where $n > 0$, be a rational number with the integers k and n relatively prime. Then $2\cos(2\pi r)$ is an algebraic integer.*

Sketch of Proof. The cases $n = 1, 2$ are trivial. If $n > 2$ the assertion is part of [6, Theorem 1]. □

Remark. In fact, D. H. Lehmer has proved much more, i.e., if $n > 2$ the algebraic integer $2\cos(2\pi k/n)$ with co-primes k and n is of degree $\phi(n)/2$ whose minimal polynomial is $\psi(y) = x^{-\phi(n)/2}\Phi_n(x)$, where $y = x + x^{-1}$ and $\phi(n), \Phi_n(x)$ are Euler's totient function and the $n-$th cyclotomic polynomial, respectively. Note that the algebraic degree depends only on the denominator n.

Example 2.6. In Table 2 of the Appendix, we show the minimal polynomials of the trigonometric values of interest whose algebraic degree equals 2.

3. The proof of the main result. We are now in a position to prove the following theorem.

Theorem 3.1. *For any degree n of the field extension, the ternary Kloosterman sums $\mathcal{K}_{3^n}(1)$ and $\mathcal{K}_{3^n}(2)$ are distinct.*

Proof. Obviously, $\mathcal{K}_3(1) = -1$ and $\mathcal{K}_3(2) = 2$. Further, making use of Corollary 2.4 for arbitrary n, we obtain:

$$\mathcal{K}_{3^n}(1) = -2 * 3^{n/2} \cos n\theta_1 \tag{3.1}$$

and

$$\mathcal{K}_{3^n}(2) = -2 * 3^{n/2} \cos n\theta_2 \tag{3.2}$$

where θ_1 and θ_2 are the arguments of the corresponding quadratic equation roots. Notice that $\theta_2 \neq \theta_1$. As easily seen, it also holds:

$$\cos\theta_1 = \frac{1}{2\sqrt{3}}, \quad \sin\theta_1 = \frac{\sqrt{11}}{2\sqrt{3}}; \tag{3.3}$$

and

$$\cos\theta_2 = -\frac{1}{\sqrt{3}}, \quad \sin\theta_2 = \frac{\sqrt{2}}{\sqrt{3}}. \tag{3.4}$$

Suppose on the contrary that for some n, we have: $\mathcal{K}_{3^n}(1) = \mathcal{K}_{3^n}(2)$. Then Eqs. (3.1) and (3.2) imply the equality $\cos n\theta_1 = \cos n\theta_2$, i.e., $\cos n\theta_2 - \cos n\theta_1 = 0$, which by the well-known formula for difference of cosines leads to: $\sin\frac{n}{2}(\theta_1 + \theta_2) * \sin\frac{n}{2}(\theta_2 - \theta_1) = 0$. This means that $\sin\frac{n}{2}(\theta_1 + \theta_2) = 0$ or $\sin\frac{n}{2}(\theta_2 - \theta_1) = 0$. We shall consider only the case when $\sin\frac{n}{2}(\theta_1 + \theta_2) = 0$ (the other is treated in a similar way). The last equality easily implies that for some integer k it holds: $\frac{n}{2}(\theta_1 + \theta_2) = k\pi$ or $\theta_1 + \theta_2 = 2\pi k/n$. Taking cosine from both sides of the latter, we get the equality: $\cos(\theta_1 + \theta_2) = \cos 2\pi k/n$. Further, applying the formula for cosine of sum on the left hand side of the latter equality and taking into account Eqs. (3.3) and (3.4), we obtain $\gamma := \frac{-1 - \sqrt{22}}{3} = 2\cos 2\pi k/n$. Finally, computing the minimal polynomial of γ, i.e., $x^2 + \frac{2}{3}x - \frac{7}{3}$, we see that γ is not an algebraic integer. This is a contradiction to Lemma 2.5, and the proof is completed. □

Remark. In the case $\sin\frac{n}{2}(\theta_2 - \theta_1) = 0$ instead of γ we obtain $\gamma' = \frac{-1 + \sqrt{22}}{3}$ which is the algebraic conjugate of γ, so they have the same minimal polynomial.

4. Conclusion. In this note, we show the distinctness of the lifted ternary Kloosterman sums $\mathcal{K}_{3^n}(1)$ and $\mathcal{K}_{3^n}(2)$ for an arbitrary degree n of the field extension. However, the case of an arbitrary characteristic p (especially when the degree of the extension is a multiple of p) looks more complicated and still remains an open problem.

Appendix A. Some numerical results.

Table 1. Values of $\mathcal{K}_{3^n}(u)$ for $1 \leq n \leq 6$ and $u = 1, 2$

n	1	2	3	4	5	6
$\mathcal{K}_{3^n}(1)$	-1	5	8	-7	-31	-10
$\mathcal{K}_{3^n}(2)$	2	2	-10	14	2	-46

Table 2. Minimal polynomials of trigonometric values $2\cos(2\pi r)$ whose algebraic degree is 2 (r is an irreducible fraction)

denominator of r	minimal polynomial
5	$y^2 + y - 1$
8	$y^2 - 2$
10	$y^2 - y - 1$
12	$y^2 - 3$

REFERENCES

[1] Y. Borissov, L. Borissov. A note on the distinctness of some Kloosterman sums. *Cryptogr. Commun.* **12**, No 5 (2020), 1051–1056.

[2] L. Carlitz. Kloosterman sums and finite field extensions. *Acta Arithmetika* **XVI**, No 2 (1969), 179–193.

[3] B. Fischer. Distinctness of Kloosterman sums. *Contemporary Mathematics*, **133** (1992), 81–102.

[4] B. H. Gross, N. Koblitz. Gauss sums and the p-adic $\Gamma-$function. *Ann. of Math.* **109** (1979), 569–581.

[5] N. E. Hurt. Exponential sums and coding theory: a review. *Acta Appl. Math.*, **46**, No 1 (1997), 49–91.

[6] D. H. Lehmer. A note on trigonometric algebraic numbers. *The American Mathematical Monthly*, **40**, No 3 (1933), 165–166.

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

[8] D. Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, **1** (1995), 189–203.

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

[10] *V. A. Zinoviev.* On classical Kloosterman sums. *Cryptogr. and Commun.*, **11**, No 3 (2019), 461–496.

Lyubomir Borissov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Block 8
1113 Sofia, Bulgaria
e-mail: lubobs90@math.bas.bg

ВЪРХУ РАЗЛИЧИЕТО НА НЯКОИ ТРОИЧНИ СУМИ НА КЛОСТЕРМАН

Любомир Борисов

В този доклад доказваме, че сумите на Клостерман $\mathcal{K}_{3^n}(1)$ и $\mathcal{K}_{3^n}(2)$ са различни за произволна степен n на разширение на полето $\mathbb{F}_3$.