Some Results on Kloosterman Sums and their Minimal Polynomials

Faruk Gölöglu, Gary Mcguire, Richard Moloney

Some Results on Kloosterman Sums and their Minimal Polynomials

Faruk Göloğlu, Gary McGuire, and Richard Moloney

School of Mathematical Sciences
University College Dublin
Ireland

Abstract. This paper introduces two new results on Kloosterman sums and their minimal polynomials. We characterise ternary Kloosterman sums modulo 27. We also prove a congruence concerning the minimal polynomial over $\mathbb{Q}$ of a Kloosterman sum. This paper also serves as a survey of our recent results on binary Kloosterman sums modulo $16, 32, 64$ and 128 with Petr Lisoněk.

1 Introduction

Throughout the paper let p be a prime, $n \geq 1$ an integer, $q = p^n$ and ζ a primitive p^{th} root of unity. We let $\mathbb{F}_q$ denote the finite field with q elements, and let Tr denote the absolute trace function $\text{Tr} : \mathbb{F}_q \to \mathbb{F}_p$,

$$\text{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{n-1}}.$$

The Kloosterman sum of $a \in \mathbb{F}_q$ is defined to be

$$\mathcal{K}_q(a) = \sum_{x \in \mathbb{F}_q} \zeta^{\text{Tr}(x^{-1} + ax)}$$

where we interpret 0^{-1} as 0. We remark that some authors do not include 0 in the definition of Kloosterman sum.

Kloosterman sums are Walsh transform values of the inverse function over $\mathbb{F}_q$, therefore have a cryptographic significance as the inverse function is used in AES (the Advanced Encryption Standard) and Walsh transform values of a function is related to linear cryptanalysis. Exponential sums and in particular Kloosterman sums have coding theoretical and combinatorial significance. Kloosterman and Melas codes, bent functions are the best known examples (see [10] for an excellent survey).

Kloosterman sums are real numbers. Binary and ternary Kloosterman sums are always integers. If $p > 3$ there are Kloosterman sums that are not integers. An interesting problem is to find the 'smallest' ring to which all the Kloosterman

sums over $\mathbb{F}_q$ belong. The Lachaud-Wolfmann result [13] does that for the binary case and states that Kloosterman sums satisfy

$$-2^{n/2+1} \leq \mathcal{K}_{2^n}(a) \leq 2^{n/2+1},$$

and take every value which is congruent to 0 modulo 4 in that range. Hence, all binary Kloosterman sums are precisely the integers in $4\mathbb{Z}$ within the *Weil bound*. For the ternary case, Kloosterman sums satisfy (see Katz and Livné [11])

$$-2\sqrt{3^n} < \mathcal{K}_{3^n}(a) < 2\sqrt{3^n}$$

and take every value which is congruent to 0 modulo 3 in that range. For $p > 3$ a similar congruence result is unknown.

A related question is the existence of a Kloosterman zero, i.e., an element $a \in \mathbb{F}_q^*$ (non-zero elements of $\mathbb{F}_q$) such that $\mathcal{K}_q(a) = 0$. The results of Lachaud and Wolfmann [13] (resp. Katz and Livne [11]) guarantees the existence of binary (resp. ternary) Kloosterman zeroes. Kononen, Rinta-aho and Väänänen have proved recently [12] that if $p > 3$ then no Kloosterman zero exists. Kloosterman zeroes for the binary and ternary case are linked to existence of *bent functions* [2, 8].

Characterising Kloosterman zeroes seems to be difficult. Lisoněk and Moisio showed that other than $p = 2$, $n = 4$ and $a = 1$ if a belongs to a proper subfield of $\mathbb{F}_q$ then $\mathcal{K}_q(a)$ cannot be zero. Another way of approaching this problem is to give congruences of Kloosterman sum modulo some integers. This was done for binary Kloosterman sums for moduli $3, 8, 24$ in [17, 9, 1, 3, 15]. In the next section we survey our recent results for moduli $16, 32, 64, 128$ with Petr Lisoněk. For the ternary case, Lisoněk proved a result for divisibility by 9 in [14]. We have recently given a complete modulo 9 characterisation [7] (we should note here this result was implicit in [17]). In this paper we give a modulo 27 characterisation. For $p > 3$, since Kloosterman sums are not necessarily integers, we resort to the analysis of the minimal polynomial of Kloosterman sums over $\mathbb{Q}$. What we prove in Section 3 can be seen as a generalisation of our ternary result of [7] to arbitrary p.

In Section 2 we give a brief survey on binary Kloosterman sums modulo some powers of 2. The characterisations use help from some functions from finite fields. Proofs of the results of Section 2 can be found in [4]. In Section 3 we give our first new and unpublished result on the minimal polynomial of p-ary Kloosterman sums. Our second new result is in Section 4. We give a characterisation of ternary Kloosterman sums modulo 27 using trace-like functions on finite fields. Our proof methods use algebraic number theory: Stickelberger's theorem and Gross-Koblitz formula and Fourier analysis (see [6]).

2 Binary Kloosterman sums

In this section let $p = 2$ and $q = 2^n$. Furthermore let $a \in \mathbb{F}_q$, and consider the characteristic polynomial of a;

$$\prod_{i=0}^{n-1}(x - a^{2^i}) = x^n + \bar{e}_1 x^{n-1} + \bar{e}_2 x^{n-2} + \cdots + \bar{e}_n \,.$$

Each of the $\bar{e}_i$ is in $\mathbb{F}_2$, $\bar{e}_1$ is the trace of a and $\bar{e}_2$ is sometimes called the subtrace (or quadratic trace). For $i > n$, set $\bar{e}_i = 0$.

Let $e_i \in \{0, 1\}$ denote $\bar{e}_i$ viewed as an integer.

Note that the only reason we restrict the integers e_i to the set $\{0, 1\}$ is so that we can identify e_i^2 with e_i, allowing us to eliminate exponents and reduce the length of certain expressions in e_i.

For any positive integer j, let $\mathrm{wt}_2(j)$ denote the binary weight of j, i.e.,

$$\mathrm{wt}_2(j) = \sum_i j_i$$

where $\sum_i j_i 2^i$ is the binary expansion of j. With this notation, we can write $\bar{e}_i$ for $0 \le i \le n$ as

$$\bar{e}_i = \sum_{\mathrm{wt}_2(j)=i} a^j.$$

2.1 Survey of results on Kloosterman sums modulo powers of 2

Using this notation we rephrase the known results.

The first result is usually attributed to Helleseth and Zinoviev [9], but it also appears in an earlier paper by van der Geer and van der Vlugt [17].

Theorem 1 *Let $q \ge 8$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}_q(a) \equiv 4e_1 \pmod 8.$$

This gives a condition for divisibility by 8.

Corollary 2 *Let $q \ge 8$ and let $a \in \mathbb{F}_q$. Then $\mathcal{K}_q(a) \equiv 0 \pmod 8$ if and only if $e_1 = 0$.*

The following theorem is in [5].

Theorem 3 *Let $q \ge 16$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}_q(a) \equiv 12e_1 + 8e_2 \pmod{16}.$$

Again, this gives a divisibility condition.

Corollary 4 *[5] Let $q \geq 16$ and let $a \in \mathbb{F}_q$. Then $\mathcal{K}_q(a) \equiv 0 \pmod{16}$ if and only if $e_1 = 0$ and $e_2 = 0$.*

Note that this mod 16 divisibility criterion was stated earlier in a different but equivalent form in [14].

Now we give a congruence for Kloosterman sums mod 32, and then a necessary and sufficient condition for divisibility mod 32:

Theorem 5 *[4] Let $q \geq 32$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_8$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then*

$$\mathcal{K}_q(a) \equiv 28e_1 + 8e_2 + 16(e_1e_2 + e_1e_3 + e_4) \pmod{32}.$$

Corollary 6 *[4] Let $q \geq 32$ and let $a \in \mathbb{F}_q$. Let $\bar{e}_1, \ldots, \bar{e}_4 \in \mathbb{F}_2$ be the coefficients of the characteristic polynomial of a. Then $\mathcal{K}_q(a) \equiv 0 \pmod{32}$ if and only if*

$$e_1 = 0,\ e_2 = 0,\ \text{and } e_4 = 0.$$

Next, a mod 64 congruence and characterisation:

Theorem 7 *[4] Let $q \geq 64$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_8$ be the coefficients of the characteristic polynomial of a viewed as integers as described above. Then*

$$\begin{aligned}\mathcal{K}_q(a) \equiv & 28e_1 + 40e_2 + \\ & 16(e_1e_2 + e_1e_3 + e_4) + \\ & 32(e_1e_4 + e_1e_5 + e_1e_6 + e_1e_7 + e_2e_3 + e_2e_4 + \\ & e_2e_6 + e_3e_5 + e_1e_2e_3 + e_1e_2e_4 + e_8) \pmod{64}.\end{aligned}$$

Corollary 8 *[4] Let $q \geq 64$ and let $a \in \mathbb{F}_q$. Let $\bar{e}_1, \ldots, \bar{e}_8 \in \mathbb{F}_2$ be the coefficients of the characteristic polynomial of a. Then $\mathcal{K}_q(a) \equiv 0 \pmod{64}$ if and only if the conditions of Corollary 6 are satisfied, and furthermore,*

$$e_8 = e_3e_5.$$

Finally we have a mod 128 congruence and characterisation:

Theorem 9 *[4] Let $q \geq 128$ and let $a \in \mathbb{F}_q$. Let $e_1, \ldots, e_{16} \in \{0, 1\}$ be the coefficients of the characteristic polynomial of a viewed as integers as described*

above. Then

$$\begin{aligned}\mathcal{K}_q(a) \equiv & 92e_1 + 40e_2 + 16(e_1e_2 + e_4) + 80e_1e_3 + 32(e_1e_2e_3 + e_1e_7 + e_2e_6 + e_8) + \\ & 96(e_1e_2e_4 + e_1e_4 + e_1e_5 + e_1e_6 + e_2e_3 + e_2e_4 + e_3e_5) + \\ & 64(e_1e_2e_3e_4 + e_1e_2e_3e_5 + e_1e_2e_5 + e_1e_2e_6 + e_1e_2e_{10} + e_1e_2e_{11} + e_1e_2e_{12} + e_1e_3e_7 + \\ & e_1e_3e_{11} + e_1e_4e_6 + e_1e_4e_7 + e_1e_4e_8 + e_1e_4e_{10} + e_1e_5e_7 + e_1e_5e_9 + e_1e_6e_8 + \\ & e_1e_8 + e_1e_9 + e_1e_{10} + e_1e_{11} + e_1e_{12} + e_1e_{13} + e_1e_{14} + e_1e_{15} + e_2e_3e_5 + e_2e_3e_8 + \\ & e_2e_3e_9 + e_2e_4e_5 + e_2e_4e_6 + e_2e_4e_8 + e_2e_5e_7 + e_2e_7 + e_2e_8 + e_2e_{10} + e_2e_{12} + e_2e_{14} + \\ & e_3e_4e_5 + e_3e_4e_6 + e_3e_4 + e_3e_7 + e_3e_{10} + e_3e_{13} + e_3 + e_4e_6 + e_4e_8 + \\ & e_4e_{12} + e_5e_6 + e_5e_{11} + e_6e_{10} + e_7e_9 + e_{16}) \pmod{128}.\end{aligned}$$

Corollary 10 *[4] Let $q \geq 128$ and let $a \in \mathbb{F}_q$. Let $\bar{e}_1, \ldots, \bar{e}_{16} \in \mathbb{F}_2$ be the coefficients of the characteristic polynomial of a. Then $\mathcal{K}_q(a) \equiv 0 \pmod{128}$ if and only if the conditions of Corollary 8 are satisfied, and furthermore,*

$$\begin{aligned}e_{16} \equiv & e_3 + e_3(e_7 + e_{10} + e_{13}) + e_5(e_6 + e_{11}) + \\ & e_6e_{10} + e_7e_9 \pmod 2.\end{aligned}$$

3 Minimal polynomials of *p*-ary Kloosterman sums

As we mentioned before when $p > 3$ the Kloosterman sum is not necessarilly an integer. In this section, we give a result previously unpublished which proves a congruence for the minimal polynomial of p-ary Kloosterman sums over $\mathbb{Q}$.

In this section we let p be an odd prime. Obviously $\mathcal{K}_q(a)$ is an algebraic integer lying in the cyclotomic field $\mathbb{Q}(\zeta)$. It is well known that

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\zeta \mapsto \zeta^i \mid i \in (\mathbb{Z}/p\mathbb{Z})^*\},$$

and it is easy to show (see [12]) that the Galois automorphism $\zeta \mapsto \zeta^i$ has the effect $\mathcal{K}_q(a) \mapsto \mathcal{K}_q(i^2a)$, for any integer i. If we let

$$c_a(x) = \prod_{i=1}^{\frac{p-1}{2}} (x - \mathcal{K}_q(i^2a))$$

it follows that $c_a(x)$ (which has degree $(p-1)/2$) is the characteristic polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$. If $m_a(x)$ is the minimal polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$, then

$$c_a(x) = m_a(x)^{e_a}$$

for some e_a dividing $\frac{p-1}{2}$. Most of the time, it is true that $e_a = 1$. For example, Wan [18] showed that

Theorem 11 *[18] Let $a \in \mathbb{F}_q$. If $\mathrm{Tr}(a) \neq 0$, the minimal polynomial of $\mathcal{K}_q(a)$ has degree $\frac{p-1}{2}$.*

Moisio [16] considered the reduction of the minimal polynomial $m_a(x)$ modulo p. He showed that all coefficients, apart from the leading coefficient, are divisible by p.

In this section, our new result concerns the reduction of the minimal polynomial $m_a(x)$ modulo p^2.

Theorem 12 *Let p be an odd prime, and let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. Then*

$$\prod_{i=1}^{\frac{p-1}{2}} \mathcal{K}_q(i^2 a) \equiv p \left(\frac{\mathrm{Tr}(a)}{p}\right) \pmod{p^2}.$$

As a consequence, the constant term of the characteristic polynomial, which is

$$(-1)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} (\mathcal{K}_q(i^2 a)),$$

is always congruent to either 0 or $\pm p \bmod p^2$.

Thus if $\mathrm{Tr}(a) \neq 0$, the minimal polynomial $m(x)$ of $\mathcal{K}_q(a)$ is precisely the characteristic polynomial $c(x)$. In this case (and in the case that $\deg(m(x)) = \frac{p-1}{2}$ where $\mathrm{Tr}(a) = 0$) Theorem 12 gives a statement about the constant term of $m(x) \bmod p^2$.

If $\mathrm{Tr}(a) = 0$ and $\deg(m(x)) < \frac{p-1}{2}$, then the result in Theorem 12 is already known. In this case, our result gives us no extra information about the constant term of the minimal polynomial.

4 Ternary Kloosterman sums modulo 27

In the case that $p = 3$, Theorem 12 becomes the following theorem.

Theorem 13 *Let $n > 1$. For $a \in \mathbb{F}_{3^n}$,*

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod 9 \text{ if } \mathrm{Tr}(a) = 0, \\ 3 \pmod 9 \text{ if } \mathrm{Tr}(a) = 1, \\ 6 \pmod 9 \text{ if } \mathrm{Tr}(a) = 2. \end{cases}$$

This is precisely the modulo 9 characterisation of the ternary Kloosterman sum which we previously proved in [7].

The second previously unpublished result of this paper is to extend this result to a modulo 27 characterisation of ternary Kloosterman sums.

4.1 Trace and similar objects

Consider again the trace function $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$,

$$\mathrm{Tr}(c) = c + c^p + c^{p^2} + \cdots + c^{p^{n-1}}.$$

We wish to generalise this definition to a larger class of finite field sums, which includes the usual trace function as a special case.

Definition 14 *Let p be a prime, let $n \geq 1$ be an integer and let $q = p^n$. For any $S \subseteq \mathbb{Z}/(q-1)\mathbb{Z}$ satisfying $S^p = S$ where $S^p := \{s^p \mid s \in S\}$, we define the function $\tau_S : \mathbb{F}_q \to \mathbb{F}_p$ by*

$$\tau_S(c) := \sum_{s \in S} c^s .$$

Remark 15 *For the set $W = \{p^i \mid i \in \{0, \ldots, n-1\}\}$, τ_W is the usual trace function.*

Other than the set W, for the case $p = 3$, we will be particularly concerned with the following sets:

$$\begin{aligned} X &:= \{r \in \{0, \ldots, q-2\} | r = 3^i + 3^j\}, \ (i, j \text{ not necessarily distinct}) \\ Y &:= \{r \in \{0, \ldots, q-2\} | r = 3^i + 3^j + 3^k, i, j, k \text{ distinct}\}, \\ Z &:= \{r \in \{0, \ldots, q-2\} | r = 2 \cdot 3^i + 3^j, i \neq j\}. \end{aligned}$$

4.2 Result modulo 27

We use Gross-Koblitz formula and Fourier analysis (cf. [5]) to evalulate Gauss sums modulo 27 which gives us the following result.

Theorem 16 *Let $n \geq 3$, and let $q = 3^n$. Let* Tr*, τ_X and τ_Y be as defined in Section 4.1. Then*

$$\mathcal{K}_q(a) \equiv \begin{cases} 0 \pmod{27} \text{ if } \mathrm{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 0 \\ 3 \pmod{27} \text{ if } \mathrm{Tr}(a) = 1 \text{ and } \tau_Y(a) \qquad\quad = 2 \\ 6 \pmod{27} \text{ if } \mathrm{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 2 \\ 9 \pmod{27} \text{ if } \mathrm{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 1 \\ 12 \pmod{27} \text{ if } \mathrm{Tr}(a) = 1 \text{ and } \tau_Y(a) \qquad\quad = 0 \\ 15 \pmod{27} \text{ if } \mathrm{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 0 \\ 18 \pmod{27} \text{ if } \mathrm{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 2 \\ 21 \pmod{27} \text{ if } \mathrm{Tr}(a) = 1 \text{ and } \tau_Y(a) \qquad\quad = 1 \\ 24 \pmod{27} \text{ if } \mathrm{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 1. \end{cases}$$

We remark that a characterisation like in Theorem 16 of Kloosterman sums modulo p^3 for $p > 3$ does not seem to be straightforward. The estimates given by the Gross-Koblitz formula are weaker.

References

1. Pascale Charpin, Tor Helleseth, and Victor Zinoviev. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd. *Journal of Combinatorial Theory*, 114:332–338, 2007.
2. J. F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.
3. Kseniya Garaschuk and Petr Lisoněk. On binary Kloosterman sums divisible by 3. *Designs, Codes and Cryptography*, 49:347–357, 2008.
4. Faruk Göloğlu, Petr Lisoněk, Gary McGuire, and Richard Moloney. Binary Kloosterman sums modulo 128 and coefficients of the characteristic polynomial. submitted, 2010.
5. Faruk Göloğlu, Gary McGuire, and Richard Moloney. Binary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula. Acta Arithmetica, accepted, 2010.
6. Faruk Göloğlu, Gary McGuire, and Richard Moloney. Some congruences of Kloosterman sums and their minimal polynomials. preprint, 2010.
7. Faruk Göloğlu, Gary McGuire, and Richard Moloney. Ternary Kloosterman sums modulo 18 using Stickelberger's theorem. In Claude Carlet and Alexander Pott, editors, *Sequences and Their Applications . SETA 2010*, volume 6338 of *Lecture Notes in Computer Science*, pages 196–203. Springer Berlin / Heidelberg, 2010.
8. Tor Helleseth and Alexander Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory*, 52(5):2018–2032, 2006.
9. Tor Helleseth and Victor Zinoviev. On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums. *Designs, Codes and Cryptography*, 17:269–288, 1999.
10. Norman E. Hurt. Exponential sums and coding theory: a review. *Acta Appl. Math.*, 46(1):49–91, 1997.
11. Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.
12. K.P. Kononen, M.J. Rinta-aho, and K.O. Väänänen. On integer values of Kloosterman sums. *IEEE Transactions on Information Theory*, 56(8):4011–4013, Aug 2010.
13. G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, 1990.
14. Petr Lisoněk. On the connection between Kloosterman sums and elliptic curves. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008.
15. Marko Moisio. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even. *Finite Fields and Their Applications*, 15:174–184, 2009.
16. M.J. Moisio. On certain values of Kloosterman sums. *IEEE Transactions on Information Theory*, 55(8):3563 –3564, Aug 2009.
17. Gerard van der Geer and Marcel van der Vlugt. Kloosterman sums and the p-torsion of certain Jacobians. *Math. Ann.*, 290(3):549–563, 1991.
18. Da Qing Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, 1(2):189–203, 1995. Special issue dedicated to Leonard Carlitz.