Journal of Number Theory 133 (2013) 1596–1607

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Some congruences of Kloosterman sums and their characteristic polynomials

Faruk Göloğlu [1], Gary McGuire [*,1], Richard Moloney [1,2]

School of Mathematical Sciences, University College Dublin, Ireland

ARTICLE INFO

Article history:
Received 20 June 2012
Revised 10 September 2012
Accepted 22 September 2012
Available online 23 December 2012
Communicated by D. Wan

Keywords:
Kloosterman sums
Stickelberger's theorem
Gross–Koblitz formula

ABSTRACT

Text. We prove two congruence results concerning Kloosterman sums over finite fields. The first result concerns the coefficients of the characteristic polynomial over $\mathbb{Q}$ of a Kloosterman sum, and the second result gives a characterisation of ternary Kloosterman sums modulo 27. We use methods from algebraic number theory such as Stickelberger's theorem and the Gross–Koblitz formula, as well as Fourier analysis.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=VJcB6W_PQ0s.

1. Introduction

Let p be a prime, let $n \geqslant 1$ be an integer, let $q = p^n$ and let ζ be a complex primitive pth root of unity. We let $\mathbb{F}_q$ denote the finite field with q elements, and let Tr denote the absolute trace function $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$, defined by $\mathrm{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{n-1}}$. The q-ary Kloosterman sum is defined by

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

for any $a \in \mathbb{F}_q$, where we interpret 0^{-1} as 0. We remark that in some papers the summation is over all nonzero $x \in \mathbb{F}_q$.

* Corresponding author.
E-mail addresses: farukgologlu@gmail.com (F. Göloğlu), gary.mcguire@ucd.ie (G. McGuire), richard.moloney@ucd.ie (R. Moloney).

[1] Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.
[2] R. Moloney's research supported also by the Irish Research Council for Science, Engineering and Technology.

0022-314X/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2012.09.026

1.1. Characteristic polynomials of Kloosterman sums

For $p = 2$ and $p = 3$, Kloosterman sums are always integers, while if $p > 3$ Kloosterman sums are not necessarily integers (also they are never 0, as was recently shown in [17]). Thus it is of interest to study the characteristic polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$. It is clear that $\mathcal{K}_q(a)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta)$, because ζ is an algebraic integer and the algebraic integers form a ring. The Galois group of this extension is

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

and it is easy to show (see [17]) that the Galois automorphism $\zeta \mapsto \zeta^i$ has the effect $\mathcal{K}_q(a) \mapsto \mathcal{K}_q(i^2 a)$, for any integer i. If we let

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

it follows that $c_a(x)$ 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 $\frac{p-1}{2}$. For most a we have $e_a = 1$.

Moisio [23] 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 paper, our first result concerns the reduction of the characteristic polynomial $c_a(x)$ modulo p^2. We prove the following result.

Theorem 1. *Let p be an odd prime, and let $(\frac{\cdot}{p})$ be the Legendre symbol. Then*

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

One corollary is that the constant term of the characteristic polynomial, which is

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

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

These results are similar to those of Wan [28], who showed that the coefficients of the minimal polynomial $\sum_{i=0}^{k} a_i x^i$ of a Gauss sum over $\mathbb{F}_p$ are divisible by p, and that a_0, a_{k-2} are not divisible by p^2.

1.2. Divisibility by the characteristic prime

Divisibility properties of exponential sums by rational primes are often of interest. Different techniques are normally used depending on whether the prime under consideration is the characteristic or not. We previously used the methods of this paper to characterise divisibility by powers of 2 for binary Kloosterman sums in [9]. The second result of this paper is to prove a ternary analogue. We give a modulo 27 characterisation of the ternary Kloosterman sum using some simple finite field functions which are generalisations of the well-known trace function (see Section 2.2 for definitions of the finite field functions T_X and T_Y).

Theorem 2. *Let $n \geqslant 3$, and let $q = 3^n$.*

$$\mathscr{K}_q(a) \equiv \begin{cases} 0 \pmod{27} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } \mathrm{T}_Y(a) + 2\mathrm{T}_X(a) = 0, \\ 3 \pmod{27} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } \mathrm{T}_Y(a) = 2, \\ 6 \pmod{27} & \text{if } \mathrm{Tr}(a) = 2 \text{ and } \mathrm{T}_Y(a) + \mathrm{T}_X(a) = 2, \\ 9 \pmod{27} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } \mathrm{T}_Y(a) + 2\mathrm{T}_X(a) = 1, \\ 12 \pmod{27} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } \mathrm{T}_Y(a) = 0, \\ 15 \pmod{27} & \text{if } \mathrm{Tr}(a) = 2 \text{ and } \mathrm{T}_Y(a) + \mathrm{T}_X(a) = 0, \\ 18 \pmod{27} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } \mathrm{T}_Y(a) + 2\mathrm{T}_X(a) = 2, \\ 21 \pmod{27} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } \mathrm{T}_Y(a) = 1, \\ 24 \pmod{27} & \text{if } \mathrm{Tr}(a) = 2 \text{ and } \mathrm{T}_Y(a) + \mathrm{T}_X(a) = 1. \end{cases}$$

As a corollary we get an if and only if criterion for $\mathscr{K}_{3^n}(a)$ to be divisible by 27, namely, that $\mathrm{Tr}(a) = 0$ and $\mathrm{T}_Y(a) + 2\mathrm{T}_X(a) = 0$.

1.3. Further remarks

Kloosterman sums are fascinating exponential sums with a large literature and many interesting properties. Weil showed that $\mathscr{K}_q(a)$ satisfies $|\mathscr{K}_q(a)| \leqslant 2\sqrt{q}$. If $p = 2$ Kloosterman sums are integers and can take any value within the Weil interval that is divisible by 4 (see Lachaud and Wolfmann [18]). If $p = 3$ they take any value divisible by 3 (see Katz and Livné [16]). For $p > 3$, generalising the results of Lachaud and Wolfmann and Katz and Livné is an interesting open problem.

Kloosterman sums have applications in coding theory [18] and cryptography. They have found applications to sum-product estimates [13], and to proving existence of primitive elements in finite fields with certain properties [4].

One open problem for Kloosterman sums over finite fields is a characterisation of Kloosterman zeros, which are the a such that $\mathscr{K}_q(a) = 0$. As well as being part of the general p-divisibility of exponential sums question, determining when $\mathscr{K}_q(a)$ is divisible by powers of various primes also gives insight into the Kloosterman zeros question. There are many divisibility results concerning binary and ternary Kloosterman sums. For binary Kloosterman sums modulo powers of 2 see [14,27,2,21,11,9], modulo 3 (and multiples of 3, i.e., $3 \cdot 2^i$) see [3,6,22]. For ternary Kloosterman sums modulo 3 and 9 see [27,21,10], modulo 2 and 4 see [5,8]. We state again that one of the results in this paper is a characterisation of ternary Kloosterman sums modulo 27.

This paper is set out as follows. In Section 2 we present all the background we need. This section has few parts because we are combining a few results from different areas. Section 3 has the proof of Theorem 1, and Section 4 has the proof of Theorem 2.

2. Background

In this section we present the background information that is used in our proofs.

2.1. Teichmüller characters and Gauss sums

Consider multiplicative characters of $\mathbb{F}_q$ taking their values in an algebraic extension of $\mathbb{Q}_p$. Let ξ be a primitive $(q-1)$th root of unity in a fixed algebraic closure of $\mathbb{Q}_p$. The group of multiplicative characters of $\mathbb{F}_q$ (denoted $\widehat{\mathbb{F}_q^\times}$) is cyclic of order $q-1$. The group $\widehat{\mathbb{F}_q^\times}$ is generated by the Teichmüller character $\omega : \mathbb{F}_q \to \mathbb{Q}_p(\xi)$, which, for a fixed generator t of $\mathbb{F}_q^\times$, is defined by $\omega(t^j) = \xi^j$. We set $\omega(0)$ to be 0. An equivalent definition is that ω satisfies $\omega(a) \equiv a \pmod{p}$ for all $a \in \mathbb{F}_q$.

Let ζ be a fixed primitive pth root of unity in the fixed algebraic closure of $\mathbb{Q}_p$. Let μ be the canonical additive character of $\mathbb{F}_q$, $\mu(x) = \zeta^{\mathrm{Tr}(x)}$.

The Gauss sum (see [20,30]) of a character $\chi \in \widehat{\mathbb{F}_q^\times}$ is defined as

$$\tau(\chi) = -\sum_{x\in\mathbb{F}_q} \chi(x)\mu(x).$$

We define $g(j) := \tau(\omega^{-j})$. For any positive integer j, let $\mathrm{wt}_p(j)$ denote the p-weight of j, i.e., $\mathrm{wt}_p(j) = \sum_i j_i$ where $\sum_i j_i p^i$ is the p-adic expansion of j.

2.2. 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 3. Let p be a prime, let $n \geqslant 1$ 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 $\mathrm{T}_S : \mathbb{F}_q \to \mathbb{F}_p$ by

$$\mathrm{T}_S(c) := \sum_{s\in S} c^s.$$

Definition 4. Let p be a prime, let $n \geqslant 1$ 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 $\widehat{\mathrm{T}}_S : \mathbb{F}_q \to \mathbb{Q}_p(\xi)$ by

$$\widehat{\mathrm{T}}_S(c) := \sum_{s\in S} \omega^s(c)$$

where ω is the Teichmüller character.

Remark 5. For the set $W = \{p^i \mid i \in \{0,\ldots,n-1\}\}$, T_W is the usual trace function.

Remark 6. By the definition of the Teichmüller character, for any set S we have

$$\widehat{\mathrm{T}}_S \equiv \mathrm{T}_S \pmod{p}.$$

Thus we may consider $\widehat{\mathrm{T}}_S$ to be a *lift* of T_S, and this explains the notation. For the set W defined in the previous remark, we let $\widehat{\mathrm{Tr}}$ denote the function $\widehat{\mathrm{T}}_W$. Sometimes we call $\widehat{\mathrm{Tr}}$ the lifted trace.

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

$$X := \left\{r \in \{0,\ldots,q-2\} \,\middle|\, r = 3^i + 3^j\right\} \quad (i, j \text{ not necessarily distinct}),$$
$$Y := \left\{r \in \{0,\ldots,q-2\} \,\middle|\, r = 3^i + 3^j + 3^k,\ i, j, k \text{ distinct}\right\},$$
$$Z := \left\{r \in \{0,\ldots,q-2\} \,\middle|\, r = 2\cdot 3^i + 3^j,\ i, j \text{ distinct}\right\}.$$

2.3. The p-adic gamma function

The p-adic gamma function Γ_p, introduced in [25], is defined over $\mathbb{N}$ by

$$\Gamma_p(k) = (-1)^k \prod_{\substack{t<k \\ (t,p)=1}} t,$$

and extends to $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p$ according to Theorem 8 below.

The following are two classical results which can be rephrased in terms of the p-adic gamma function.

Theorem 7 *(Wilson's theorem). (See [7].) Let p be an odd prime. Then $\Gamma_p(p-1) \equiv 1 \pmod{p}$.*

Theorem 8 *(Generalised Wilson's theorem). (See [7,25].) Let p be a prime, and suppose $x \equiv y \pmod{p^k}$ for some integer k. If $p^k \neq 4$, then $\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^k}$.*

2.4. Stickelberger's theorem and the Gross–Koblitz formula

Let π be the unique $(p-1)$th root of $-p$ in $\mathbb{Q}_p(\xi, \zeta)$ satisfying $\pi \equiv \zeta - 1 \pmod{\pi^2}$. We will first give the Gross–Koblitz formula and then a generalised version of Stickelberger's theorem.

Theorem 9 *(Gross–Koblitz formula). (See [12].) Let $1 \leqslant j < q-1$ be an integer. Then*

$$g(j) = \pi^{\mathrm{wt}_p(j)} \prod_{i=0}^{n-1} \Gamma_p\left(\left\{\frac{p^i j}{q-1}\right\}\right)$$

where $\{x\}$ is the fractional part of x, and Γ_p is the p-adic gamma function.

Wan [29] noted that the following generalisation of Stickelberger's theorem is a direct consequence of the Gross–Koblitz formula (Theorem 9).

Theorem 10 *(More general version of Stickelberger's theorem). (See [29].) Let $1 \leqslant j < q-1$ be an integer and let $j = j_0 + j_1 p + \cdots + j_{n-1} p^{n-1}$. Then*

$$g(j) \equiv \frac{\pi^{\mathrm{wt}_p(j)}}{j_0! \cdots j_{n-1}!} \pmod{\pi^{\mathrm{wt}_p(j)+p-1}}.$$

Stickelberger's theorem, as usually stated, is the same congruence modulo $\pi^{\mathrm{wt}_p(j)+1}$.

We have (see [12,26]) that (π) is the unique prime ideal of $\mathbb{Q}_p(\zeta, \xi)$ lying above p. Since $\mathbb{Q}_p(\zeta, \xi)$ is an unramified extension of $\mathbb{Q}_p(\zeta)$, which is a totally ramified (degree $p-1$) extension of $\mathbb{Q}_p$, it follows that $(\pi)^{p-1} = (p)$ and $\nu_p(\pi) = \frac{1}{p-1}$. Here ν_p denotes the p-adic valuation.

Theorem 10 implies that $\nu_\pi(g(j)) = \mathrm{wt}_p(j)$, and because $\nu_p(g(j)) = \nu_\pi(g(j)) \cdot \nu_p(\pi)$ we get

$$\nu_p\big(g(j)\big) = \frac{\mathrm{wt}_p(j)}{p-1}. \tag{1}$$

Our proof in Section 3 studies the π-adic expansion of the Kloosterman sum, and uses the Gross–Koblitz formula to get information on the coefficients.

2.5. Fourier coefficients

Recall that $\mu(x) = \zeta^{\mathrm{Tr}(x)}$. The Fourier transform of a function $f : \mathbb{F}_q \to \mathbb{C}$ at $a \in \mathbb{F}_q$ is defined to be

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_q} f(x)\mu(ax).$$

The complex number $\widehat{f}(a)$ is called the Fourier coefficient of f at a.

Consider monomial functions defined by $f(x) = \mu(x^d)$. When $d = -1$ we have $\widehat{f}(a) = \mathscr{K}_{p^n}(a)$. By Fourier analysis [15,19] we have for any d

$$\widehat{f}(a) = \frac{q}{q-1} + \frac{1}{q-1}\sum_{j=1}^{q-2} \tau\left(\bar{\omega}^j\right)\tau\left(\omega^{jd}\right)\bar{\omega}^{jd}(a)$$

and hence

$$\widehat{f}(a) \equiv -\sum_{j=1}^{q-2} \tau\left(\bar{\omega}^j\right)\tau\left(\omega^{jd}\right)\bar{\omega}^{jd}(a) \pmod{q}.$$

Putting $d = -1 = p^n - 2$, this congruence becomes

$$\mathscr{K}_q(a) \equiv -\sum_{j=1}^{q-2} \big(g(j)\big)^2 \omega^j(a) \pmod{q}. \tag{2}$$

We will use this in Section 4.

3. Proof of first theorem

Moisio considered the reduction of the minimal polynomial $m_a(x)$ modulo p, and proved the following.

Theorem 11. *(See [23].) For $a \in \mathbb{F}_q$, let $m_a(x)$ be the minimal polynomial of $\mathscr{K}_q(a)$ over $\mathbb{Q}$ and let t be the degree of m_a. Then $m_a(x) \equiv x^t \pmod{p}$.*

Our first result (Theorem 1 in Section 1) concerns the reduction of the characteristic polynomial $c_a(x)$ modulo p^2.

Theorem 1. *Let p be an odd prime, and let $(\frac{\cdot}{p})$ be the Legendre symbol. Then*

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

Proof. For $j \in \{1, \ldots, q-2\}$, Theorem 10 implies that

$$\nu_\pi\left(g(j)^2\right) = 2\,\mathrm{wt}_p(j), \tag{3}$$

so taking Eq. (2) mod π^4 gives

$$\mathcal{K}_q(a) \equiv -\sum_{\mathrm{wt}_p(j)=1} g(j)^2\,\omega^j(a) \pmod{\pi^4}$$
$$\equiv -g(1)^2\widehat{\mathrm{Tr}}(a) \pmod{\pi^4}.$$

Eq. (3) implies that $\nu_\pi(g(1)^2)=2$. Therefore we can write $\mathcal{K}_q(a)$ π-adically as

$$\mathcal{K}_q(a) = a_1\pi^2 + a_2\pi^4 + \cdots,$$

where

$$a_1 = -\left(\frac{g(1)}{\pi}\right)^2 \widehat{\mathrm{Tr}}(a)$$
$$= -\left(\prod_{i=0}^{n-1} \Gamma_p\left(\frac{p^i}{q-1}\right)\right)^2 \widehat{\mathrm{Tr}}(a)$$

by Theorem 9. Reducing this expression modulo p gives that

$$a_1 \equiv -\left(\Gamma_p\left(\frac{1}{q-1}\right)\right)^2 \mathrm{Tr}(a) \pmod{p}$$
$$\equiv -\big(\Gamma_p(p-1)\big)^2\,\mathrm{Tr}(a) \pmod{p}$$
$$\equiv -\mathrm{Tr}(a) \pmod{p},$$

by Theorems 8 and 7. Since $\pi^{p-1} = -p$ we certainly have $a_1 \equiv -\mathrm{Tr}(a) \pmod{\pi^4}$. Thus

$$\mathcal{K}_q(a) \equiv -\pi^2\,\mathrm{Tr}(a) \pmod{\pi^4}.$$

We can rewrite this as an equation

$$\mathcal{K}_q(a) = -\pi^2\,\mathrm{Tr}(a) + X(a)\pi^4,$$

where $X(a)$ is some element of $\mathbb{Q}_p(\xi,\zeta)$ that will drop out in the end, and $\mathrm{Tr}(a)$ is considered as an integer. Then we get equations

$$\mathcal{K}_q\big(i^2a\big) = -\pi^2\,\mathrm{Tr}\big(i^2a\big) + X\big(i^2a\big)\pi^4$$

for $i = 1, 2, \ldots, (p-1)/2$. We may also write

$$\mathcal{K}_q\big(i^2a\big) = -\pi^2 i^2\,\mathrm{Tr}(a) + X\big(i^2a\big)\pi^4$$

because of the mod p congruence this equation comes from. Multiplying these equations together and taking the result modulo π^{p+1}, only the lowest degree term in π survives, and we obtain

$$\prod_{i=1}^{\frac{p-1}{2}}\left(\mathscr{K}_q\left(i^2a\right)\right) \equiv \prod_{i=1}^{\frac{p-1}{2}} \pi^2\left(-i^2\operatorname{Tr}(a)\right) \pmod{\pi^{p+1}}$$

$$\equiv -p\operatorname{Tr}(a)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}}\left(-i^2\right) \pmod{\pi^{p+1}}$$

since $\pi^{p-1} = -p$. But $\prod_{i=1}^{\frac{p-1}{2}}(\mathscr{K}_q(i^2a)) \in \mathbb{Z}$ by the remarks in Section 1, so we may raise the modulus and write

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

Using Wilson's theorem (as usually stated), we have that

$$\prod_{i=1}^{\frac{p-1}{2}}\left(-i^2\right) = \prod_{i=1}^{p-1} i \equiv -1 \pmod{p}.$$

Thus

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

Corollary 12. *The constant term of the characteristic polynomial $c_a(x)$ is always congruent to either 0 or $\pm p$ mod p^2.*

The following result is due to Wan.

Theorem 13. *(See [29].) Let $a \in \mathbb{F}_q$. If $\operatorname{Tr}(a) \neq 0$, then $m_a(x)$ has degree $\frac{p-1}{2}$, and so $m_a(x) = c_a(x)$.*

Corollary 14. *Let $a \in \mathbb{F}_q$. If $\operatorname{Tr}(a) \neq 0$, then the constant term of $m_a(x)$ is $\equiv p(\frac{\operatorname{Tr}(a)}{p}) \pmod{p^2}$, and so is always congruent to either 0 or $\pm p$ mod p^2.*

The same statement can be made in the case that $\deg(m_a(x)) = \frac{p-1}{2}$ where $\operatorname{Tr}(a) = 0$.

If $\operatorname{Tr}(a) = 0$ and $\deg(m_a(x)) < \frac{p-1}{2}$, then the result in Theorem 1 is implied by Theorem 11. In this case, our result gives us no extra information about the constant term of the minimal polynomial.

3.1. The $p = 5$ case

When $p = 5$ we will give the other (nontrivial) coefficient modulo 25 of the characteristic polynomial of 5-ary Kloosterman sums. The details of the following can be found in the PhD thesis of the third author [24]. For $p > 5$ computing the other coefficients modulo p^2 is an open problem.

In the case of 5-ary Kloosterman sums, the characteristic polynomial of $\mathscr{K}_q(a)$ is

$$x^2 - \left(\mathscr{K}_q(a) + \mathscr{K}_q(-a)\right)x + \mathscr{K}_q(a)\mathscr{K}_q(-a).$$

By Theorem 1 we have

$$\mathcal{K}_q(a)\mathcal{K}_q(-a) \equiv 5\big(\mathrm{Tr}(a)\big)^2 \pmod{25}.$$

Detailed calculations (see [24]) show

$$\mathcal{K}_q(a) + \mathcal{K}_q(-a) \equiv 5\big(\mathrm{Tr}(a)\big)^2 + 10\,\mathrm{Tr}\big(a^2\big) \pmod{25}.$$

To show a few concrete examples we give the characteristic polynomial of $\mathcal{K}_q(a)$, computed using Magma [1], for the following elements of $\mathbb{F}_{5^4}$, with generator t satisfying $t^4 + 4t^2 + 4t + 2 = 0$.

a	$c_a(x)$	$\mathrm{Tr}(a)$	$\mathrm{Tr}(a^2)$
t^{112}	$x^2 + 30x + 205$	1	4
t^{453}	$x^2 + 20x - 305$	2	1
t^{371}	$x^2 + 40x + 355$	4	3
t^{297}	$x^2 + 30x - 495$	1	4
t^{432}	$x^2 - 15x + 45$	3	2

4. Proof of second theorem

In this section we will use the same techniques (Gross–Koblitz formula, etc.) to improve the modulo 9 Kloosterman sum characterisation previously proved in [10,27] to a modulo 27 characterisation. The modulo 9 characterisation states that $\mathcal{K}_{3^n}(a) \equiv 3\,\mathrm{Tr}(a) \pmod 9$. We remark that in the case that $p = 3$, Theorem 1 reduces to this modulo 9 characterisation.

First let us prove a lemma on evaluations of the p-adic gamma function. This lemma will allow us to evaluate Gauss sums for higher moduli and find Kloosterman congruences modulo 27.

Lemma 15. *Let $n \geqslant 3$, $q = 3^n$, and let i be an integer in the range $0, \ldots, n-1$. Then*

$$\Gamma_3\left(\left\{\frac{3^i}{q-1}\right\}\right) \equiv \begin{cases} 13 \pmod{27} & \text{if } i = 1, \\ 1 \pmod{27} & \text{if } i > 1. \end{cases}$$

Proof. For any $3 \leqslant j \leqslant n$, we have $3^j \leqslant q$, and

$$\left\{\frac{3^i}{q-1}\right\} = \frac{3^i}{q-1} \equiv 3^i\big(3^j - 1\big) \pmod{3^j},$$

so

$$\Gamma_3\left(\left\{\frac{3^i}{q-1}\right\}\right) \equiv \Gamma_3\big(26 \cdot 3^i\big) \pmod{27}.$$

If $i \geqslant 3$, then $26 \cdot 3^i \equiv 0 \pmod{27}$, and $\Gamma_3(\{\frac{3^i}{q-1}\}) \equiv 1 \pmod{27}$. Now $\Gamma_3(26 \cdot 3) \equiv \Gamma_3(24) \pmod{27}$ using Theorem 8. And $\Gamma_3(24) \equiv 13 \pmod{27}$. Similarly $\Gamma_3(26 \cdot 9) \equiv 1 \pmod{27}$. □

Lemma 15 allows us to compute the square of a Gauss sum modulo 27:

Lemma 16. *Let $n \geqslant 3$ and let $q = 3^n$. Then*

$$g(j)^2 \equiv \begin{cases} 6 \pmod{27} & \text{if } \mathrm{wt}_p(j) = 1, \\ 9 \pmod{27} & \text{if } \mathrm{wt}_p(j) = 2, \\ 0 \pmod{27} & \text{if } \mathrm{wt}_p(j) \geqslant 3. \end{cases}$$

Proof. Suppose $\mathrm{wt}_3(j) = 1$. By Theorem 9 and Lemma 15, $g(j) \equiv 13\pi \pmod{27}$. Let $g(j) = 27A + 13\pi$ for some $A \in \mathbb{Z}_3[\zeta, \xi]$. Then

$$\begin{aligned} g(j)^2 &= 27^2 A^2 + 2 \cdot 27 \cdot 13A + 169\pi^2 \\ &\equiv 169\pi^2 \pmod{27} \\ &\equiv 6 \pmod{27} \end{aligned}$$

since $\pi^2 = -3$. Now suppose $\mathrm{wt}_3(j) = 2$. By Theorem 9, $g(j) \equiv -3 \pmod 9$. Thus $g(j) = 9B - 3$ for some $B \in \mathbb{Z}_3[\zeta, \xi]$, so $g(j)^2 = 81B^2 - 54B + 9 \equiv 9 \pmod{27}$.

It is clear from Theorem 9 that if $\mathrm{wt}_3(j) > 2$, then $27 | \pi^{2\,\mathrm{wt}_3(j)} | g(j)^2$. □

Now we are ready to prove our result on Kloosterman sums modulo 27.

Theorem 17. *Let $n \geqslant 3$, $q = 3^n$ and let $\widehat{\mathrm{Tr}}$ and $\widehat{\mathrm{T}}_X$ be as defined in Section 2.2. Then*

$$\mathscr{K}_{3^n}(a) \equiv 21\widehat{\mathrm{Tr}}(a) + 18\widehat{\mathrm{T}}_X(a) \pmod{27}. \tag{4}$$

Proof. Using (2) and Lemma 16, we get

$$\begin{aligned} \mathscr{K}_q(a) &\equiv -\sum_{j=1}^{q-2} g(j)^2\, \omega^j(a) \pmod{q} \\ &\equiv -\sum_{\mathrm{wt}_3(j)=1} g(j)^2 \omega^j(a) - \sum_{\mathrm{wt}_3(j)=2} g(j)^2 \omega^j(a) \pmod{27} \\ &\equiv -6 \sum_{\mathrm{wt}_3(j)=1} \omega^j(a) - 9 \sum_{\mathrm{wt}_3(j)=2} \omega^j(a) \pmod{27} \\ &\equiv 21\widehat{\mathrm{Tr}}(a) + 18\widehat{\mathrm{T}}_X(a) \pmod{27}. \end{aligned}$$

□

Next we shall express the above result in terms of operations within $\mathbb{F}_q$ itself, i.e., using functions T_S directly, and not their lifts. Note that in (4) we only need $\widehat{\mathrm{Tr}}(a)$ modulo 9 and $\widehat{\mathrm{T}}_X(a)$ modulo 3. We have $\mathrm{T}_X(a) \equiv \widehat{\mathrm{T}}_X(a) \pmod 3$ so this takes care of the $\widehat{\mathrm{T}}_X(a)$ term. For the other term we need to find a condition for $\widehat{\mathrm{Tr}}(a)$ modulo 9 using functions from $\mathbb{F}_q$ to $\mathbb{F}_3$. We will do that in the proof of the following corollary.

Corollary 18. *Let $n \geqslant 3$, $q = 3^n$, $a \in \mathbb{F}_q$ and let T_X, T_Y and T_Z be as defined in Section 2.2. Let $\mathrm{Tr}(a)$ be the trace of a, but considered as an integer. Then*

$$\mathscr{K}_q(a) \equiv 21\,\mathrm{Tr}(a)^3 + 18\mathrm{T}_Z(a) + 9\mathrm{T}_Y(a) + 18\mathrm{T}_X(a) \pmod{27}.$$

Proof. First recall that $\widehat{\mathrm{T}}_X(a) \equiv \mathrm{T}_X(a) \pmod 3$.

To determine $\widehat{\mathrm{Tr}}(a) \bmod 9$, we compute

$$\begin{aligned}\widehat{\mathrm{Tr}}(a)^3 &= \sum_{i,j,k\in\{0,\ldots,n-1\}} \omega\left(a^{3^i+3^j+3^k}\right)\\ &= \widehat{\mathrm{Tr}}(a) + 3\widehat{\mathrm{T}}_Z(a) + 6\widehat{\mathrm{T}}_Y(a),\end{aligned}$$

and note the elementary fact that if $x \equiv y \pmod m$, then $x^m \equiv y^m \pmod{m^2}$. This means that $\widehat{\mathrm{Tr}}(a)^3 \bmod 9$ is given by $\widehat{\mathrm{Tr}}(a) \bmod 3 = \mathrm{Tr}(a)$, i.e. $\widehat{\mathrm{Tr}}(a)^3 \bmod 9 = \mathrm{Tr}(a)^3$. Since $\widehat{\mathrm{T}}_Z(a) \equiv \mathrm{T}_Z(a) \pmod 3$ and $\widehat{\mathrm{T}}_Y(a) \equiv \mathrm{T}_Y(a) \pmod 3$ we have that $\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a)^3 - 3\mathrm{T}_Z(a) - 6\mathrm{T}_Y(a) \pmod 9$, proving the result. □

Theorem 2 (see Section 1) combines Corollary 18 and Theorem 17 and enumerates the possible values of ternary Kloosterman sums mod 27.

Proof of Theorem 2. Note that $\mathrm{Tr}(a)\mathrm{T}_X(a) = \mathrm{Tr}(a) + 2\mathrm{T}_Z(a)$. Thus Corollary 18 can be rewritten as

$$\mathcal{K}_q(a) \equiv 21\,\mathrm{Tr}(a)^3 + 18\,\mathrm{Tr}(a) + 18\mathrm{T}_X(a) + 9\,\mathrm{Tr}(a)\mathrm{T}_X(a) + 9\mathrm{T}_Y(a) \pmod{27}. \tag{5}$$

The result is an enumeration of the cases in Eq. (5). □

We remark that a characterisation like in Theorem 2 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.

Supplementary material

The online version of this article contains additional supplementary material.
Please visit http://dx.doi.org/10.1016/j.jnt.2012.09.026.

References

[1] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system, I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[2] Pascale Charpin, Guang Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials, IEEE Trans. Inform. Theory 54 (9) (2008) 4230–4238.
[3] Pascale Charpin, Tor Helleseth, Victor Zinoviev, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd, J. Combin. Theory Ser. A 114 (2007) 332–338.
[4] Stephen D. Cohen, Kloosterman sums and primitive elements in Galois fields, Acta Arith. 94 (2) (2000) 173–201.
[5] Kseniya Garaschuk, Petr Lisoněk, On ternary Kloosterman sums modulo 12, Finite Fields Appl. 14 (4) (2008) 1083–1090.
[6] Kseniya Garaschuk, Petr Lisoněk, On binary Kloosterman sums divisible by 3, Des. Codes Cryptogr. 49 (2008) 347–357.
[7] Carl Friedrich Gauss, Disquisitiones Arithmeticae, Springer, 1986.
[8] Faruk Göloğlu, Ternary Kloosterman sums modulo 4, Finite Fields Appl. 18 (1) (2012) 160–166.
[9] Faruk Göloğlu, Petr Lisoněk, Gary McGuire, Richard Moloney, Binary Kloosterman sums modulo 256 and coefficients of the characteristic polynomial, IEEE Trans. Inform. Theory 58 (4) (2012) 2516–2523.
[10] Faruk Göloğlu, Gary McGuire, Richard Moloney, Ternary Kloosterman sums modulo 18 using Stickelberger's theorem, in: Claude Carlet, Alexander Pott (Eds.), Sequences and Their Applications, SETA 2010, in: Lecture Notes in Comput. Sci., vol. 6338, Springer, Berlin, Heidelberg, 2010, pp. 196–203.
[11] Faruk Göloğlu, Gary McGuire, Richard Moloney, Binary Kloosterman sums using Stickelberger's theorem and the Gross–Koblitz formula, Acta Arith. 148 (3) (2011) 269–279.
[12] Benedict H. Gross, Neal Koblitz, Gauss sums and the p-adic Γ-function, Ann. of Math. (2) 109 (3) (1979) 569–581.
[13] Derrick Hart, Alex Iosevich, Jozsef Solymosi, Sum-product estimates in finite fields via Kloosterman sums, Int. Math. Res. Not. IMRN (5) (2007), Art. ID rnm007, 14 p.
[14] Tor Helleseth, Victor Zinoviev, On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums, Des. Codes Cryptogr. 17 (1999) 269–288.
[15] Nicholas M. Katz, Gauss Sums, Kloosterman Sums, and Monodromy Groups, Ann. of Math. Stud., vol. 116, Princeton University Press, Princeton, NJ, 1988.

[16] Nicholas Katz, Ron Livné, Sommes de Kloosterman et courbes elliptiques universelles caractéristiques 2 et 3, C. R. Acad. Sci. Paris Sér. I Math. 309 (11) (1989) 723–726.
[17] Keijo Kononen, Marko Rinta-aho, Keijo Väänänen, On integer values of Kloosterman sums, IEEE Trans. Inform. Theory 56 (8) (2010) 4011–4013.
[18] Gilles Lachaud, Jacques Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory 36 (3) (1990) 686–692.
[19] Philippe Langevin, Gregor Leander, Monomial bent functions and Stickelberger's theorem, Finite Fields Appl. 14 (2008) 727–742.
[20] Rudolf Lidl, Harald Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1986.
[21] Petr Lisoněk, On the connection between Kloosterman sums and elliptic curves, in: Solomon W. Golomb, Matthew G. Parker, Alexander Pott, Arne Winterhof (Eds.), SETA, in: Lecture Notes in Comput. Sci., vol. 5203, Springer, 2008, pp. 182–187.
[22] Marko Moisio, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even, Finite Fields Appl. 15 (2009) 174–184.
[23] Marko Moisio, On certain values of Kloosterman sums, IEEE Trans. Inform. Theory 55 (8) (2009) 3563–3564.
[24] Richard Moloney, Divisibility properties of Kloosterman sums and division polynomials for Edwards curves, PhD thesis, University College Dublin, 2011.
[25] Yasuo Morita, A p-adic analogue of the Γ-function, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 22 (2) (1975) 255–266.
[26] Alain Robert, The Gross–Koblitz formula revisited, Rend. Sem. Mat. Univ. Padova 105 (2001) 157–170.
[27] Gerard van der Geer, Marcel van der Vlugt, Kloosterman sums and the p-torsion of certain Jacobians, Math. Ann. 290 (3) (1991) 549–563.
[28] Da Qing Wan, Some arithmetic properties of the minimal polynomials of Gauss sums, Proc. Amer. Math. Soc. 100 (2) (1987) 225–228.
[29] Da Qing Wan, Minimal polynomials and distinctness of Kloosterman sums, in: Special Issue Dedicated to Leonard Carlitz, Finite Fields Appl. 1 (2) (1995) 189–203.
[30] Lawrence C. Washington, Introduction to Cyclotomic Fields, Springer, 1982.