arXiv:1012.0964v1 [math.NT] 5 Dec 2010

Some Congruences of Kloosterman Sums and their Minimal Polynomials

Faruk Göloğlu*, Gary McGuire*, Richard Moloney†
School of Mathematical Sciences
University College Dublin
Ireland

Abstract

We prove two results on Kloosterman sums over finite fields, using Stickelberger's theorem and the Gross-Koblitz formula. The first result concerns the minimal polynomial over $\mathbb{Q}$ of a Kloosterman sum, and the second result gives a characterisation of ternary Kloosterman sums modulo 27.

1 Introduction

Let p be an odd 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.

Obviously $\mathcal{K}_q(a)$ is an algebraic integer lying in the cyclotomic field $\mathbb{Q}(\zeta)$. It is well known that

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

*Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006
†Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006, and the Irish Research Council for Science, Engineering and Technology

and it is easy to show (see [5]) 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

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

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 [11] showed that $e_a = 1$ if $\mathrm{Tr}(a) \neq 0$.

Moisio [8] 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 minimal polynomial $m_a(x)$ modulo p^2. In Section 3, we prove the following result about the constant term.

Theorem 1. *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 $\pm p \bmod p^2$.

In the case that $p = 3$, Theorem 1 becomes the following theorem.

Theorem 2. *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 [2]. The second result of this paper, see Corollary 18 in Section 4, is to extend this result to a modulo 27 characterisation of the ternary Kloosterman sum.

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 taking their values in an algebraic extension of $\mathbb{Q}_p$. Let ξ be a primitive $(q-1)^{\text{th}}$ 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 p-th 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 [7, 12]) 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-ary 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 $n \geq 1$ 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

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

Definition 4. 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 $\widehat{\tau}_S : \mathbb{F}_q \to \mathbb{Q}_p(\xi)$ by

$$\widehat{\tau}_S(c) := \sum_{s \in S} \omega^s(c) \,.$$

Remark 5. For the set $W = \{p^i \mid i \in \{0, \ldots, n-1\}\}$, τ_W is the usual trace function.
Remark 6. By the definition of the Teichmüller character, for any set S we have $\widehat{\tau}_S \equiv \tau_S \pmod{p}$. Thus we may consider $\widehat{\tau}_S$ to be a *lift* of τ_S, and this explains the notation. For the set W defined in the previous remark, we let $\widehat{\mathrm{Tr}}$ denote the function $\widehat{\tau_W}$. 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:

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

2.3 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

$$\pi \equiv \zeta - 1 \pmod{\pi^2} \,.$$

Wan [11] noted that the following improved version of Stickelberger's theorem is a direct consequence of the Gross-Koblitz formula (Theorem 8).

Theorem 7. *[11] Let $1 \leq j < q-1$ 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 [3, 10]) 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 7 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

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

A generalisation of Stickelberger's theorem is the Gross-Koblitz formula.
Theorem 8. *(Gross-Koblitz formula) [3].*

Let $1 \le j < q-1$ be an integer. Then

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

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

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.

2.4 The p-adic gamma function

The p-adic gamma function Γ_p, introduced in [9], 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 10 below.

The following are two classical results (they appear in [1]) which can be rephrased in terms of the p-adic gamma function. Theorem 10 appears in this form in [9].
Theorem 9 (Wilson's theorem)**.** *Let p be an odd prime. Then*

$$\Gamma_p(p-1) \equiv 1 \pmod{p}.$$

Theorem 10 (Generalised Wilson's theorem)**.** *Let p be a prime, and suppose $x \equiv y \pmod{p^k}$ for some integer k. If $p^k \neq 4$, then*

$$\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^k}.$$

2.5 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 $\widehat{f}(a) = \mathcal{K}_{p^n}(a)$. By Fourier analysis [4, 6] we have for any d

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

and hence

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

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

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

We will use this in Section 4.

3 Proof of Theorem 1

Moisio [8] considered the reduction of the minimal polynomial $m_a(x)$ modulo p, and proved the following.

Lemma 11. *[8] For $a \in \mathbb{F}_q$, let $m(x)$ be the minimal polynomial of $\mathcal{K}_q(a)$ over $\mathbb{Q}$ and let t be the degree of m. Then*

$$m(x) \equiv x^t \pmod{p}.$$

Our first result concerns the reduction of the minimal polynomial $m_a(x)$ modulo p^2.

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

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

Proof: For $j \in \{1, \ldots, q-2\}$, Theorem 7 implies that

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

so taking equation (2) mod π^4 gives

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

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

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

where

$$\begin{aligned}a_1 &= -\left(\frac{g(1)}{\pi}\right)^2 \widehat{\mathrm{Tr}}(a) \\ &= -\left(\prod_{i=0}^{n-1} \Gamma_p\left(\left\langle \frac{p^i}{q-1} \right\rangle\right)\right)^2 \widehat{\mathrm{Tr}}(a) \text{ (by Theorem 8).}\end{aligned}$$

Reducing this expression modulo p gives that

$$\begin{aligned}a_1 &\equiv -\left(\Gamma_p\left(\frac{1}{q-1}\right)\right)^2 \mathrm{Tr}(a) \pmod{p} \\ &\equiv -\left(\Gamma_p(p-1)\right)^2 \mathrm{Tr}(a) \pmod{p} \text{ (by Theorem 10)} \\ &\equiv -\mathrm{Tr}(a) \pmod{p} \text{ (by Theorem 9),}\end{aligned}$$

and thus

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

So

$$\prod_{i=1}^{\frac{p-1}{2}}(\mathcal{K}_q(i^2a)) \equiv \pi^{p-1}\prod_{i=1}^{\frac{p-1}{2}}(-i^2\,\mathrm{Tr}(a)) \pmod{\pi^{p+1}}$$

$$\equiv -\,p\,\mathrm{Tr}(a)^{\frac{p-1}{2}}\prod_{i=1}^{\frac{p-1}{2}}(-i^2) \pmod{\pi^{p+1}}.$$

But $\prod_{i=1}^{\frac{p-1}{2}}(\mathcal{K}_q(i^2a)) \in \mathbb{Z}$ by the remarks in Section 1, so

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

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

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

Thus

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

□

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

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 1 gives a statement about the constant term of $m(x)$ mod p^2.

If $\mathrm{Tr}(a) = 0$ and $\deg(m(x)) < \frac{p-1}{2}$, then the result in Theorem 1 is implied by Lemma 11. 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 this section we use the same techniques to improve the modulo 9 Kloosterman sum characterisation in [2] to a modulo 27 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 14. *Let $n \geq 3$ $q = 3^n$ and let i be an integer in the range $0, \ldots n-1$. Then*

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

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

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

so

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

If $i \geq 3$, then $26 \cdot 3^i \equiv 0 \pmod{27}$, and

$$\Gamma_3\left(\left\langle \frac{3^i}{q-1} \right\rangle\right) \equiv 1 \pmod{27},$$

Now $\Gamma_3(26 \cdot 3) \equiv \Gamma_3(24) \pmod{27}$ using Theorem 10. And $\Gamma_3(24) \equiv 13 \pmod{9}$. Similarly:

$$\Gamma_3(26 \cdot 9) \equiv 1 \pmod{27}.$$

□

Lemma 14 allows us to compute Gauss sums modulo 27:

Lemma 15. *Let $n \geq 3$ and let $q = 3^n$. Then*

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

Proof. Suppose $\mathrm{wt}_3(j) = 1$. By Theorem 8 and Lemma 14,

$$g(j) \equiv 13\pi \pmod{27}.$$

Let

$$g(j) = 27A + 13\pi$$

for some $A \in \mathbb{Z}_3[\zeta, \xi]$. Then

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

since $\pi^2 = -3$. Now suppose $\mathrm{wt}_3(j) = 2$. By Theorem 8,

$$g(j) \equiv -3 \pmod{9}.$$

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 8 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 16. *Let $n \geq 3$, $q = 3^n$ and let $\widehat{\mathrm{Tr}}$ and $\widehat{\tau_X}$ be as defined in Section 2.2. Then*

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

Proof. Using (2) and Lemma 15, we get

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

□

Next we shall express the above result in terms of operations within $\mathbb{F}_q$ itself, i.e., using functions τ_S directly, and not their lifts. Note that in (4) we only need $\widehat{\mathrm{Tr}}(a)$ modulo 9 and $\widehat{\tau_X}(a)$ modulo 3. We have

$$\tau_X(a) \equiv \widehat{\tau_X}(a) \pmod 3$$

so this takes care of the $\widehat{\tau_X}(a)$ 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 17. *Let $n \geq 3$, $q = 3^n$, $a \in \mathbb{F}_q$ and let τ_X, τ_Y and τ_Z be as defined in Section 2.2. Let $\mathrm{Tr}(a)$ be the trace of a, but considered as an integer. Then*

$$\mathcal{K}_q(a) \equiv 21\,\mathrm{Tr}(a)^3 + 18\tau_Z(a) + 9\tau_Y(a) + 18\tau_X(a) \pmod{27}.$$

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

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

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

and note the elementary fact that if $x \equiv y \pmod m$, then $x^m \equiv y^m \pmod{m^2}$. This means that $\widehat{\mathrm{Tr}}(a)^3$ mod 9 is given by $\widehat{\mathrm{Tr}}(a)$ mod $3 = \mathrm{Tr}(a)$, i.e. $\widehat{\mathrm{Tr}}(a)^3$ mod $9 = \mathrm{Tr}(a)^3$.

Since

$$\widehat{\tau}_Z(a) \equiv \tau_Z(a) \pmod 3$$

and

$$\widehat{\tau}_Y(a) \equiv \tau_Y(a) \pmod 3\,,$$

we have that

$$\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a)^3 - 3\tau_Z(a) - 6\tau_Y(a) \pmod 9,$$

proving the result. □

The next corollary combines Corollary 17 and Theorem 16 and enumerates the possible values of ternary Kloosterman sums mod 27.

Corollary 18. *Let $n \geq 3$, and let $q = 3^n$. Let* Tr, τ_X *and* τ_Y *be as defined in Section 2.2. Then*

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

Proof. Note that

$$\mathrm{Tr}(a)\tau_X(a) = \mathrm{Tr}(a) + 2\tau_Z(a)\,.$$

Thus Corollary 17 can be rewritten as

$$\mathcal{K}_q(a) \equiv 21\,\mathrm{Tr}(a)^3 + 18\,\mathrm{Tr}(a) + 18\tau_X(a) + 9\,\mathrm{Tr}(a)\tau_X(a) + 9\tau_Y(a) \pmod{27}. \qquad (5)$$

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

We remark that a characterisation like in Corollary 18 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] C.F. Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, 1986.

[2] 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, 2010.

[3] Benedict H. Gross and Neal Koblitz. Gauss sums and the p-adic Γ-function. *Ann. of Math. (2)*, 109(3):569–581, 1979.

[4] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[5] 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.

[6] Philippe Langevin and Gregor Leander. Monomial bent functions and Stickelberger's theorem. *Finite Fields and Their Applications*, 14:727–742, 2008.

[7] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1986.

[8] M.J. Moisio. On certain values of Kloosterman sums. *IEEE Transactions on Information Theory*, 55(8):3563 –3564, Aug 2009.

[9] Yasuo Morita. A p-adic analogue of the Γ-function. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 22(2):255–266, 1975.

[10] Alain Robert. The Gross-Koblitz formula revisited. *Rendiconti del Seminario Matematico della Università di Padova*, 105:157 – 170, 2001.

[11] Da Qing Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, 1(2):189–203, 1995. Special issue dedicated to Leonard Carlitz.

[12] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1982.