ACTA ARITHMETICA
148.3 (2011)

Binary Kloosterman sums using Stickelberger's theorem and the Gross–Koblitz formula

by

Faruk Göloğlu, Gary McGuire and Richard Moloney (Dublin)

1. Introduction. Let $\mathcal{K}_{p^n}(a)$ denote the p-ary Kloosterman sum defined by

$$\mathcal{K}_{p^n}(a) := \sum_{x\in\mathbb{F}_{p^n}} \zeta^{\mathrm{Tr}(x^{p^n-2}+ax)},$$

for any $a \in \mathbb{F}_{p^n}$, where ζ is a primitive pth root of unity and Tr denotes the absolute trace map $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined as usual as

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

Finding explicit zeros (explicit a's with $\mathcal{K}_{p^n}(a) = 0$) of Kloosterman sums is considered difficult. Recent research on Kloosterman sums is generally concentrated on proving divisibility results and characterisation of Kloosterman sums modulo some integer (see [15, 12, 2, 1, 13]).

It is easy to see that binary Kloosterman sums are divisible by $4 = 2^2$, i.e., for all $a \in \mathbb{F}_{2^n}$,

$$\mathcal{K}_{2^n}(a) \equiv 0 \pmod 4. \tag{1}$$

They also satisfy (see [8])

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

and take every value which is congruent to 0 modulo 4 in that range.

Helleseth and Zinoviev proved the following result which improved (1) one level higher, i.e., modulo 2^3, in the sense of describing the a for which $\mathcal{K}_{2^n}(a)$ is 0 or 4 modulo 8.

Theorem 1.1 ([5]). *For $a \in \mathbb{F}_{2^n}$,*

$$\mathcal{K}_{2^n}(a) \equiv \begin{cases} 0 \pmod 8 & \text{if } \mathrm{Tr}(a) = 0,\\ 4 \pmod 8 & \text{if } \mathrm{Tr}(a) = 1.\end{cases}$$

2010 *Mathematics Subject Classification*: Primary 11L05.
Key words and phrases: Kloosterman sums, Stickelberger's theorem, Gross–Koblitz formula.

DOI: 10.4064/aa148-3-4

This paper will improve Theorem 1.1 to higher levels, i.e., modulo 2^4, in the sense of describing the residue class of $\mathcal{K}_{2^n}(a)$ modulo 2^4 in terms of a. We will define the quadratic sum

$$Q(a) := \sum_{0 \le i < j < n} a^{2^i + 2^j}.$$

While the trace map $\mathrm{Tr}(a)$ is the sum of all linear powers of a, the sum $Q(a)$ is the sum of all quadratic powers of a. Using Stickelberger's theorem we will improve the Helleseth–Zinoviev result one level further to the modulus 2^4. We will prove the following theorem.

THEOREM 1.2. *For $a \in \mathbb{F}_{2^n}$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{16} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } Q(a) = 0, \\ 4 \pmod{16} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } Q(a) = 1, \\ 8 \pmod{16} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } Q(a) = 1, \\ 12 \pmod{16} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } Q(a) = 0. \end{cases}$$

We mention a recent result due to Lisoněk [12] that gives a description of the elements $a \in \mathbb{F}_{2^n}$ for which $\mathcal{K}(a) \equiv 0 \pmod{16}$:

THEOREM 1.3. *Let $n \ge 4$. For any $a \in \mathbb{F}_{2^n}$, $\mathcal{K}(a)$ is divisible by 16 if and only if $\mathrm{Tr}(a) = 0$ and $\mathrm{Tr}(y) = 0$ where $y^2 + ay + a^3 = 0$.*

In Sections 2 and 3, we introduce the techniques we use. In Section 4 we give an alternative proof of Theorem 1.1 using our techniques. We prove Theorem 1.2 in Section 5. In Section 6 we combine Theorem 1.2 with the result concerning Kloosterman sums modulo 3 to achieve the complete characterisation modulo 48. Finally, in Section 7 we employ the Gross–Koblitz formula to characterize the values of Kloosterman sums modulo 64 in terms of the *lifted trace* that we introduce in Section 5.

We give a few remarks about the ternary case. It is easy to see that ternary Kloosterman sums are divisible by 3, i.e., for all $a \in \mathbb{F}_{3^n}$,

$$\mathcal{K}_{3^n}(a) \equiv 0 \pmod{3}. \tag{2}$$

Ternary Kloosterman sums satisfy (see Katz and Livné [7])

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

and take every value which is congruent to 0 modulo 3 in that range.

In a recent paper, we used Stickelberger's theorem to prove the following result on ternary Kloosterman sums, which improved (2) one level higher.

THEOREM 1.4 ([3]). *For $a \in \mathbb{F}_{3^n}$,*

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

2. Stickelberger's theorem. Let p be a prime (in Section 4 we set $p = 2$) and let $q = p^n$. We consider multiplicative characters taking their values in an algebraic extension of the p-adic numbers $\mathbb{Q}_p$. 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 $\omega : \mathbb{F}_q^\times \to \mathbb{Q}_p(\xi)$, which, for a fixed generator t of $\mathbb{F}_q^\times$, is defined by

$$\omega(t^j) = \xi^j.$$

We extend ω to $\mathbb{F}_q$ by setting $\omega(0)$ to be 0.

Let ζ be a 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 [11, 18]) of a character $\chi \in \widehat{\mathbb{F}_q^\times}$ is defined as

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

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. Just for shorthand notation we define

$$g(j) := \tau(\omega^{-j}) = \tau(\bar{\omega}^j).$$

Let π be the unique $(p-1)$th root of $-p$ in $\mathbb{Q}_p(\xi,\zeta)$ satisfying

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

Wan [17] noted that the following improved version of Stickelberger's theorem is a direct consequence of the Gross–Koblitz formula [4, 16].

THEOREM 2.1 ([17]). *Let $1 \le j < q-1$ 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 $\pi^{\mathrm{wt}_p(j)+1}$. Note that when $p = 2$, which is the case in this paper, Theorem 2.1 is the same as this original Stickelberger theorem.

We know (see [4]) 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 $\mathbb{Q}_p(\zeta)$, a totally ramified (degree $p-1$) extension of $\mathbb{Q}_p$, it follows that $(\pi)^{p-1} = (p)$ and $\nu_p(\pi) = 1/(p-1)$. Here ν_p denotes the p-adic valuation.

Therefore Theorem 2.1 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

$$\nu_p(g(j)) = \frac{\mathrm{wt}_p(j)}{p-1}. \tag{3}$$

In this paper we have $p = 2$. In that case, $\pi = -2$ and equation (3) becomes

$$\nu_2(g(j)) = \mathrm{wt}_2(j). \tag{4}$$

3. Fourier analysis. 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 a similar Fourier analysis argument to that in Katz [6] or Langevin–Leander [9], for any d we have

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

and hence

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

We will use this to obtain congruence information about Kloosterman sums. Putting $d = -1 = p^n - 2$, the previous congruence becomes

$$\mathcal{K}(a) \equiv -\sum_{j=1}^{q-2} (g(j))^2 \omega^j(a) \pmod{q}. \tag{5}$$

Equation (4) gives the 2-adic valuation of the Gauss sums $g(j)$, and the 2-adic valuation of each term in equation (5) follows. Our proofs will consider (5) at various levels, i.e., modulo 2^3, 2^4 and 2^6.

4. Binary Kloosterman sums modulo 8. Let $q = 2^n$ for some integer $n \geq 2$.

To warm up we shall give a new proof of the following result due to Helleseth and Zinoviev [5]. This is equivalent to Theorem 1.1.

THEOREM 4.1. *For $a \in \mathbb{F}_q$, $\mathcal{K}(a) \equiv 0 \pmod{8}$ if and only if* $\mathrm{Tr}(a) = 0$.

Proof. If $f(x) = \mu(x^d)$ let

$$M_d = \min_{j \in \{1,\ldots,2^n-2\}} [\mathrm{wt}_2(j) + \mathrm{wt}_2(-jd)],$$

and let

$$J_d = \{j \in \{1,\ldots,2^n-2\} : \mathrm{wt}_2(j) + \mathrm{wt}_2(-jd) = M_d\}.$$

Lemma 1 of [10] states that if $f(x) = \mu(x^d)$, then

$$2^{M_d+1} \mid \widehat{f}(a) \ \Leftrightarrow\ \sum_{j \in J_d} a^{-jd} = 0. \tag{6}$$

Let $d = -1$. Then $\widehat{f}(a)$ is the Kloosterman sum $\mathcal{K}(a)$ on $\mathbb{F}_q$, $M_{-1} = 2$, and

$$J_{-1} = \{j \in \{1,\ldots,2^n-2\} : \mathrm{wt}_2(j) = 1\}.$$

It follows that

$$\sum_{j \in J_{-1}} a^j = \mathrm{Tr}(a),$$

and (6) implies that 8 divides $\mathcal{K}(a)$ if and only if $\mathrm{Tr}(a) = 0$. ■

5. Binary Kloosterman sums modulo 16. Again $q = 2^n$. For $i = 1, 2, \ldots,$ let

$$W_i = \{j \in \{1,\ldots,2^n-2\} : \mathrm{wt}_2(j) = i\}.$$

Then we may write

$$\mathrm{Tr}(a) = \sum_{j \in W_1} a^j.$$

Recall that $\omega : \mathbb{F}_q \to \mathbb{Q}_2(\xi)$ is the Teichmüller character.

We define the *lifted trace* $\widehat{\mathrm{Tr}} : \mathbb{F}_q \to \mathbb{Q}_2(\xi)$ by

$$\widehat{\mathrm{Tr}}(a) = \sum_{j \in W_1} \omega(a^j)$$

and note that $\widehat{\mathrm{Tr}}(a) \equiv \mathrm{Tr}(a) \pmod 2$.

We define the *quadratic trace* $Q : \mathbb{F}_q \to \mathbb{F}_2$ by

$$Q(a) = \sum_{j \in W_2} a^j$$

and define the *lifted quadratic trace* $\widehat{Q} : \mathbb{F}_q \to \mathbb{Q}_2(\xi)$ by

$$\widehat{Q}(a) = \sum_{j \in W_2} \omega(a^j).$$

Then $\widehat{Q}(a) \equiv Q(a) \pmod 2$.

Next we prove our theorem on $\mathcal{K}(a)$ mod 16.

THEOREM 5.1. *Let $q = 2^n$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{16} & \text{if } \operatorname{Tr}(a) = 0 \text{ and } Q(a) = 0, \\ 4 \pmod{16} & \text{if } \operatorname{Tr}(a) = 1 \text{ and } Q(a) = 1, \\ 8 \pmod{16} & \text{if } \operatorname{Tr}(a) = 0 \text{ and } Q(a) = 1, \\ 12 \pmod{16} & \text{if } \operatorname{Tr}(a) = 1 \text{ and } Q(a) = 0. \end{cases}$$

Proof. Let $q = 2^n$ and let $a \in \mathbb{F}_q$. As in the proof of Theorem 4.1, $\mathcal{K}(a) = \widehat{f}(a)$, where $f(x) = \mu(x^{-1})$. Stickelberger's theorem implies $g(j) \equiv 2^{\mathrm{wt}_2(j)} \pmod{2^{\mathrm{wt}_2(j)+1}}$, so squaring gives

$$g(j)^2 \equiv 2^{2\,\mathrm{wt}_2(j)} \pmod{2^{2\,\mathrm{wt}_2(j)+2}}.$$

It follows that $g(j)^2 \equiv 4 \pmod{16}$ for j of weight 1, and $g(j)^2 \equiv 0 \pmod{16}$ for j of weight at least 2. Thus congruence (5) modulo 16 gives

$$\mathcal{K}(a) \equiv -\sum_{j \in W_1} g(j)^2 \omega^j(a) \pmod{16}$$

or in other words

$$\mathcal{K}(a) \equiv -4\,\widehat{\operatorname{Tr}}(a) \pmod{16}.$$

It remains to determine $\widehat{\operatorname{Tr}}(a) \bmod 4$.

This can be done in terms of the $\mathbb{F}_q$-sums $\operatorname{Tr}(a)$ and $Q(a)$ by noting that

$$\begin{aligned} \widehat{\operatorname{Tr}}(a)^2 &= \sum_{j \in W_1} \sum_{k \in W_1} \omega(a^j)\omega(a^k) = \sum_{j,k \in W_1} \omega(a^{j+k}) \\ &= 2 \sum_{i \in W_2} \omega(a^i) + \sum_{j \in W_1} \omega(a^j) = 2\widehat{Q}(a) + \widehat{\operatorname{Tr}}(a). \end{aligned}$$

However

$$\begin{aligned} \widehat{\operatorname{Tr}}(a)^2 \equiv 0 \pmod 4 \ &\Leftrightarrow\ \widehat{\operatorname{Tr}}(a) \equiv 0 \pmod 2 \ \Leftrightarrow\ \operatorname{Tr}(a) = 0, \\ \widehat{\operatorname{Tr}}(a)^2 \equiv 1 \pmod 4 \ &\Leftrightarrow\ \widehat{\operatorname{Tr}}(a) \equiv 1 \pmod 2 \ \Leftrightarrow\ \operatorname{Tr}(a) = 1. \end{aligned}$$

Recalling that $\widehat{Q}(a) \equiv Q(a) \pmod 2$, and observing that we only require $\widehat{Q}(a) \bmod 2$, we get

$$\widehat{\operatorname{Tr}}(a) \equiv \begin{cases} 0 \pmod 4 & \text{if } \operatorname{Tr}(a) = 0 \text{ and } Q(a) = 0, \\ 1 \pmod 4 & \text{if } \operatorname{Tr}(a) = 1 \text{ and } Q(a) = 0, \\ 2 \pmod 4 & \text{if } \operatorname{Tr}(a) = 0 \text{ and } Q(a) = 1, \\ 3 \pmod 4 & \text{if } \operatorname{Tr}(a) = 1 \text{ and } Q(a) = 1, \end{cases}$$

which proves the result. ■

6. Binary Kloosterman sums modulo 48. We combine the results above with the result on the divisibility modulo 3 of binary Kloosterman sums from [1, 2, 14, 15] to fully characterise the congruence modulo 48 of binary Kloosterman sums.

6.1. Case n odd

THEOREM 6.1. *Let $q = 2^n$ and let $a \in \mathbb{F}_q^\times$ where n is odd and $n \geq 5$.*

(1) *If* $\mathrm{Tr}(a^{1/3}) = 0$ *then*

$$\mathcal{K}(a) \equiv \begin{cases} 4 \pmod{48} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } Q(a) = 1, \\ 16 \pmod{48} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } Q(a) = 0, \\ 28 \pmod{48} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } Q(a) = 0, \\ 40 \pmod{48} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } Q(a) = 1. \end{cases}$$

(2) *If* $\mathrm{Tr}(a^{1/3}) = 1$, *let* β *be the unique element satisfying* $\mathrm{Tr}(\beta) = 0$, $a^{1/3} = \beta^4 + \beta + 1$. *Then*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{48} & \text{if } \mathrm{Tr}(a) = 0,\ Q(a) = 0,\ n + \mathrm{Tr}(\beta^3) \equiv 5, 7\ (8), \\ 8 \pmod{48} & \text{if } \mathrm{Tr}(a) = 0,\ Q(a) = 1,\ n + \mathrm{Tr}(\beta^3) \equiv 1, 3\ (8), \\ 12 \pmod{48} & \text{if } \mathrm{Tr}(a) = 1,\ Q(a) = 0,\ n + \mathrm{Tr}(\beta^3) \equiv 5, 7\ (8), \\ 20 \pmod{48} & \text{if } \mathrm{Tr}(a) = 1,\ Q(a) = 1,\ n + \mathrm{Tr}(\beta^3) \equiv 1, 3\ (8), \\ 24 \pmod{48} & \text{if } \mathrm{Tr}(a) = 0,\ Q(a) = 1,\ n + \mathrm{Tr}(\beta^3) \equiv 5, 7\ (8), \\ 32 \pmod{48} & \text{if } \mathrm{Tr}(a) = 0,\ Q(a) = 0,\ n + \mathrm{Tr}(\beta^3) \equiv 1, 3\ (8), \\ 36 \pmod{48} & \text{if } \mathrm{Tr}(a) = 1,\ Q(a) = 1,\ n + \mathrm{Tr}(\beta^3) \equiv 5, 7\ (8), \\ 44 \pmod{48} & \text{if } \mathrm{Tr}(a) = 1,\ Q(a) = 0,\ n + \mathrm{Tr}(\beta^3) \equiv 1, 3\ (8). \end{cases}$$

Note that we consider $\mathrm{Tr}(\beta^3)$ *to be an integer in the final congruences.*

Proof. Follows from Theorem 5.1 above, and Theorem 3 of [1], which implies that $\mathcal{K}(a) \equiv 1 \pmod 3 \Leftrightarrow \mathrm{Tr}(a^{1/3}) = 0$, and otherwise, $\mathcal{K}(a) \equiv 0 \pmod 3$ if and only if either $\mathrm{Tr}(\beta^3) = 0$ and $n \equiv 5$ or $7 \pmod 8$, or $\mathrm{Tr}(\beta^3) = 1$ and $n \equiv 1$ or $3 \pmod 8$. ∎

6.2. Case n even. By a similar argument (with a few more cases) we can combine Theorem 5.1 above with Theorem 11 of [15] to classify the congruence modulo 48 of the Kloosterman sum on $\mathbb{F}_{2^n}$ where n is even. We omit the details.

7. Binary Kloosterman sums modulo 64. So far in this paper we have used the lifted trace modulo 2 (the usual finite field trace) and the lifted quadratic trace modulo 2 to characterise the Kloosterman sums modulo 16. Further information can be obtained using the lifted traces modulo higher powers of 2. We will now show how the values taken by the lifted trace modulo 16 determine the congruence modulo 64 of binary Kloosterman sums, using the Gross–Koblitz formula.

The first part of this section, down to Theorem 7.1, is a restatement of Section 8 of [10] (with a correction when $q = 4$).

For a field $\mathbb{F}_q = \mathbb{F}_{2^n}$, and a residue j modulo $q-1$, the *Gross–Koblitz formula* [16] states that

$$\tau(\bar{\omega}^j) = (-2)^{\mathrm{wt}_2(j)} \prod_{i=0}^{n-1} \Gamma_2\left(\left\langle \frac{2^i j}{q-1} \right\rangle\right) \tag{7}$$

where $\langle x \rangle$ is the fractional part of x, and Γ_2 is the 2-adic Gamma function.

The *p-adic Gamma function* Γ_p is defined over $\mathbb{N}$ by

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

By the generalised Wilson's theorem, $\Gamma_p(p^k) \equiv 1 \pmod{p^k}$, unless $p^k = 4$, in which case $\Gamma_2(4) \equiv -1 \pmod 4$.

Suppose $x \equiv y \pmod{2^k}$. Observe that $(-1)^{x+2^k} = (-1)^x$, and that the product

$$\prod_{\substack{x \le t < x+2^k \\ (t,2)=1}} t \bmod 2^k$$

consists of 2^{k-1} distinct elements, and hence is congruent to $\Gamma_2(2^k)$. It follows that $\Gamma_2(x) \equiv \Gamma_2(y) \pmod{2^k}$ unless $k = 2$, in which case $\Gamma_2(x) \equiv -\Gamma_2(y) \pmod 4$.

Theorem 7.1. *Let $q = 2^n$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 0 \pmod{16}, \\ 4 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 3 \pmod{16}, \\ 8 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 10 \pmod{16}, \\ 12 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 5 \pmod{16}, \\ 16 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 4 \pmod{16}, \\ 20 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 7 \pmod{16}, \\ 24 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 14 \pmod{16}, \\ 28 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 9 \pmod{16}, \\ 32 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 8 \pmod{16}, \\ 36 \pmod{64} & \text{if } \widehat{\mathrm{Tr}}(a) \equiv 11 \pmod{16}, \end{cases}$$

$$\mathcal{K}(a) \equiv \begin{cases} 40 \pmod{64} & \textit{if } \widehat{\mathrm{Tr}}(a) \equiv 2 \pmod{16}, \\ 44 \pmod{64} & \textit{if } \widehat{\mathrm{Tr}}(a) \equiv 13 \pmod{16}, \\ 48 \pmod{64} & \textit{if } \widehat{\mathrm{Tr}}(a) \equiv 12 \pmod{16}, \\ 52 \pmod{64} & \textit{if } \widehat{\mathrm{Tr}}(a) \equiv 15 \pmod{16}, \\ 56 \pmod{64} & \textit{if } \widehat{\mathrm{Tr}}(a) \equiv 6 \pmod{16}, \\ 60 \pmod{64} & \textit{if } \widehat{\mathrm{Tr}}(a) \equiv 1 \pmod{16}. \end{cases}$$

Proof. By the statements above, the following congruences hold for residues mod 8:

$$\begin{aligned} \Gamma_2(0) &\equiv 1 \pmod 8 \equiv 1 \pmod 4, \\ \Gamma_2(1) &\equiv 7 \pmod 8 \equiv -1 \pmod 4, \\ \Gamma_2(2) &\equiv 1 \pmod 8 \equiv 1 \pmod 4, \\ \Gamma_2(3) &\equiv 7 \pmod 8 \equiv -1 \pmod 4, \\ \Gamma_2(4) &\equiv 3 \pmod 8 \equiv -1 \pmod 4, \\ \Gamma_2(5) &\equiv 5 \pmod 8 \equiv 1 \pmod 4, \\ \Gamma_2(6) &\equiv 7 \pmod 8 \equiv -1 \pmod 4, \\ \Gamma_2(7) &\equiv 1 \pmod 8 \equiv 1 \pmod 4. \end{aligned}$$

If $j = j_0 + 2j_1 + 4j_2 + \cdots$ is the 2-adic expansion of j, then

$$\Gamma_2\left(\left\langle \frac{2^i j}{q-1} \right\rangle\right) \equiv \Gamma_2(7j_0 + 6j_1 + 4j_2) \pmod 8 \equiv (-1)^{j_2+j_1+j_0j_1} \pmod 4.$$

Feeding this into the Gross–Koblitz formula (7) gives

$$g(j) \equiv (-1)^{Q(j)+\mathrm{wt}_2(j)} 2^{\mathrm{wt}_2(j)} \pmod{2^{\mathrm{wt}_2(j)+2}} \tag{8}$$

where $Q(j) = j_0j_1 + j_1j_2 + \cdots + j_{n-1}j_0$. Squaring (8) gives

$$g(j)^2 \equiv 2^{2\,\mathrm{wt}_2(j)} \pmod{2^{2\,\mathrm{wt}_2(j)+4}}. \tag{9}$$

It follows that $g(j)^2 \equiv 4 \pmod{64}$ for j of weight 1, and $g(j)^2 \equiv 16 \pmod{64}$ for j of weight 2, and $g(j)^2 \equiv 0 \pmod{64}$ for j of weight greater than 2.

Taking this into account, reading congruence (5) modulo 64 gives

$$\mathcal{K}(a) \equiv -4\widehat{\mathrm{Tr}}(a) - 16\widehat{Q}(a) \pmod{64}.$$

As we have noted,

$$2\widehat{Q}(a) = \widehat{\mathrm{Tr}}(a)^2 - \widehat{\mathrm{Tr}}(a),$$

so the value of $\widehat{\mathrm{Tr}}(a) \bmod 16$ determines $\widehat{Q}(a) \bmod 8$, and so determines $16\widehat{Q}(a) \bmod 64$. Thus $\widehat{\mathrm{Tr}}(a) \bmod 16$ completely determines $\mathcal{K}(a) \bmod 64$. The possibilities are enumerated in the statement. ∎

Remark. Just as we did in Section 6, this theorem can be combined with the results on binary Kloosterman sums modulo 3 to yield a theorem characterizing binary Kloosterman sums modulo 192. We omit the details.

Acknowledgements. This research was supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006 and, in the case of the third author, the Irish Research Council for Science, Engineering and Technology.

References

[1] P. Charpin, T. Helleseth, and V. Zinoviev, *The divisibility modulo 24 of Kloosterman sums on* $\mathrm{GF}(2^m)$*, m odd*, J. Combin. Theory Ser. A 114 (2007), 322–338.

[2] K. Garaschuk and P. Lisoněk, *On binary Kloosterman sums divisible by* 3, Des. Codes Cryptogr. 49 (2008), 347–357.

[3] F. Göloğlu, G. McGuire, and R. Moloney, *Ternary Kloosterman sums modulo* 18 *using Stickelberger's theorem*, in: Sequences and Their Applications – SETA 2010, C. Carlet and A. Pott (eds.), Lecture Notes in Comput. Sci. 6338, Springer, Berlin, 2010, 196–203.

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

[5] T. Helleseth and V. Zinoviev, *On* $\mathbb{Z}_4$*-linear Goethals codes and Kloosterman sums*, Des. Codes Cryptogr. 17 (1999), 269–288.

[6] N. M. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Ann. of Math. Stud. 116, Princeton Univ. Press, Princeton, NJ, 1988.

[7] N. Katz et R. Livné, *Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3*, C. R. Acad. Sci. Paris Sér. I Math. 309 (1989), 723–726.

[8] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory 36 (1990), 686–692.

[9] P. Langevin and G. Leander, *Monomial bent functions and Stickelberger's theorem*, Finite Fields Appl. 14 (2008), 727–742.

[10] P. Langevin, G. Leander, G. McGuire, and E. Zălinescu, *Analysis of Kasami–Welch functions in odd dimension using Stickelberger's theorem*, J. Combin. Number Theory 2 (2010).

[11] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, Cambridge, 1986.

[12] P. Lisoněk, *On the connection between Kloosterman sums and elliptic curves*, in: Sequences and Their Applications – SETA 2008, S. W. Golomb, M. G. Parker, A. Pott, and A. Winterhof (eds.), Lecture Notes in Comput. Sci. 5203, Springer, Berlin, 2008, 182–187.

[13] P. Lisoněk and M. Moisio, *On zeros of Kloosterman sums*, to appear.

[14] M. Moisio, *Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm*, Acta Arith. 132 (2008), 329–350.

[15] —, *The divisibility modulo 24 of Kloosterman sums on* $\mathrm{GF}(2^m)$*, m even*, Finite Fields Appl. 15 (2009), 174–184.

[16] A. M. Robert, *The Gross–Koblitz formula revisited*, Rend. Sem. Mat. Univ. Padova 105 (2001), 157–170.

[17] D. Q. Wan, *Minimal polynomials and distinctness of Kloosterman sums*, Finite Fields Appl. 1 (1995), 189–203.
[18] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

Faruk Göloğlu, Gary McGuire, Richard Moloney
School of Mathematical Sciences
University College Dublin
Dublin, Ireland
E-mail: farukgologlu@gmail.com
gary.mcguire@ucd.ie
richard.moloney@ucd.ie

Received on 30.4.2010 (6370)