CONGRUENCES FOR SUMS OF POWERS OF KLOOSTERMAN SUMS

H. Timothy Choi
Department of Mathematics
University of California at Irvine
Irvine, CA 92717
tchoi@math.uci.edu

Ronald Evans
Department of Mathematics, 0112
University of California at San Diego
La Jolla, CA 92093-0112
revans@ucsd.edu

2000 Mathematics Subject Classification: 11L05

Key words: power moments of Kloosterman sums, Kloosterman sheaves, newform, eta and theta functions, Sturm bound, Jacobi symbol, congruences, Kummer's theorem for binomial coefficients.

January 17, 2009

Abstract

The n-th power-moments S_n of classical Kloosterman sums (mod p) are known explicitly only for $n \le 6$. In 2002, we conjectured formulas for $S_n(\text{mod } 4)$ for each $n > 1$, valid for all primes $p > n$. Here we prove these formulas, and give conjectural congruences for S_n modulo some higher powers of 2 for a few small values of n. For example, we conjecture that if $p \equiv 17 \pmod{120}$, so that $p = 3s^2 + 5t^2$, then

$$S_{10} \equiv \begin{cases} 15 \pmod{64}, & \text{if } \ t \equiv \pm 1 \pmod{12} \\ 47 \pmod{64}, & \text{if } \ t \equiv \pm 5 \pmod{12}. \end{cases}$$

1 Introduction

For an odd prime p, let $\mathbb{F}_p$ denote a field of p elements, and write $\zeta_p = \exp(2\pi i/p)$. Consider the Kloosterman sums $K(a)$ defined by

$$K(a) = \sum_{x=1}^{p-1} \zeta_p^{x+a/x}, \quad a \in \mathbb{F}_p. \tag{1.1}$$

For $n > 1$, let S_n denote the power-moment

$$S_n = \sum_{a=0}^{p-1} K(a)^n. \tag{1.2}$$

Define $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ by $\sigma_t(\zeta_p) = \zeta_p^t$, where $(t, p) = 1$. We have $\sigma_t(K(a)) = K(at^2)$; to see this, replace x by x/t in (1.1). Thus each σ_t fixes S_n, so $S_n \in \mathbb{Z}$. It is not difficult to show moreover that for each $p > n$,

$$S_n \equiv \begin{cases} 0 \pmod 2), & \text{if } n \text{ is a power of 2}, \\ 1 \pmod 2), & \text{otherwise.} \end{cases} \tag{1.3}$$

The primary purpose of this paper is to determine $S_n(\mathrm{mod}\ 4)$ for all $p > n$. This is accomplished in Theorems 2.1 and 2.2 for odd and even n, respectively. We conjectured these results in 2002 [2].

While Theorems 2.1 and 2.2 evaluate $S_n(\mathrm{mod}\ 4)$, it appears to be a much more difficult task to obtain general congruences for $S_n(\mathrm{mod}\ 2^r)$ for any fixed value of $r > 2$. In Section 5, we present conjectural congruences for some small values of $n > 5$ and $r > 2$. The formulas are especially intriguing for even n, as they depend on parameters occurring in multifarious binary quadratic forms representing the primes p.

We proceed to discuss further facts and conjectures concerning the sums S_n. For a study of sums of powers of certain Kloosterman sums over rings, see [6].

Explicit formulas for S_n are known for $n \le 6$. Indeed, Salié [11] proved that

$$S_2 = p^2 - p, \tag{1.4}$$

$$S_3 = \left(\frac{p}{3}\right) p^2 + 2p, \tag{1.5}$$

and

$$S_4 = 2p^3 - 3p^2 - 3p. \tag{1.6}$$

Proofs may also be found in [8] (but replace $-p$ by $-3p$ in [8, (4.25)]). For $p > 5$, it follows from the work in [10] and [9] that

$$S_5 = \left(\frac{p}{3}\right) 4p^3 + (a_p + 5)p^2 + 4p, \tag{1.7}$$

where a_p is the integer with $|a_p| < 2p$ defined for $p > 5$ by

$$a_p = \begin{cases} 2p - 12u^2, & \text{if} \quad p = 3u^2 + 5v^2 \\ 4x^2 - 2p, & \text{if} \quad p = x^2 + 15y^2 \\ 0, & \text{if} \quad p \equiv 7, 11, 13, \text{or } 14 \pmod{15}. \end{cases} \tag{1.8}$$

For $p > 5$, a_p is the coefficient of p^{-s} in the Hecke L-function

$$L(s, \chi) = 1 + \frac{1}{2^s} - \frac{3}{3^s} - \frac{3}{4^s} + \frac{5}{5^s} - \frac{3}{6^s} + \cdots$$

where χ is the Hecke character of conductor (1) whose values on integral ideals of $\mathbb{Q}(\sqrt{-15})$ are as follows. For every principal ideal (α), $\chi((\alpha)) = \alpha^2$; for a nonprincipal prime ideal P of norm p, $\chi(P) = -3$ when $p = 3$ and otherwise $\chi(P) = \beta$, where β is that generator of the principal ideal P^2 whose real part is congruent modulo 3 to the Legendre symbol $(p/3)$. For example, $\chi(P) = (1 + \sqrt{-15})/2$ when $p = 2$.

By the Hecke correspondence, a_p is the Fourier coefficient of q^p in the q-expansion of a newform $F(z)$ on $\Gamma_0(15)$ of weight 3 with quadratic nebentypus of conductor 15, where $q = \exp(2\pi i z)$. Amazingly, $F(z)$ can be expressed explicitly as

$$F(z) := \eta(z)\eta(3z)\eta(5z)\eta(15z)\ (\theta_2(q)\theta_2(q^{15}) + \theta_3(q)\theta_3(q^{15})),$$

where η is the Dedekind eta function and θ_2, θ_3 are the classical Jacobi theta functions. This can be proved by squaring both sides (to get forms of weight 6 with trivial nebentypus) and then matching the corresponding Fourier coefficients up to the Sturm bound.

For $p > 6$, it follows from the work in [7] that

$$S_6 = 5p^4 - 10p^3 - (b_p + 9)p^2 - 5p, \tag{1.9}$$

where b_p is the integer with

$$|b_p| < 2p^{3/2} \tag{1.10}$$

defined to be the coefficient of q^p in the q-expansion of the newform of weight 4, level 6 given by

$$(\eta(6z)\eta(3z)\eta(2z)\eta(z))^2.$$

For $p > 7$, S_7 has been evaluated conjecturally [4] in terms of the coefficient of q^p in the q-expansion of a certain newform of weight 3, level 525.

For any $n > 1$, we have

$$S_n \equiv p(n-1)(-1)^{n-1} \pmod{p^2} \tag{1.11}$$

for all $p > n$ (in agreement with the rightmost terms in (1.4) – (1.7) and (1.9)). To see (1.11), first note that

$$S_n/p = \sum_{\bar{x}_1+\cdots+\bar{x}_n=0} \zeta_p^{x_1+\cdots+x_n} \equiv U_n := \sum_{\bar{x}_1+\cdots+\bar{x}_n=0} 1 \pmod{p}, \tag{1.12}$$

where $x_i \in \mathbb{F}_p^*$ and $\overline{x_i} x_i = 1$ in $\mathbb{F}_p$. The congruence

$$\sum_{\bar{x}_1+\cdots+\bar{x}_n=1} 1 \equiv U_n + (-1)^{n-1} \pmod{p} \tag{1.13}$$

yields the recursion

$$U_n \equiv (-1)^{n-1} - U_{n-1} \pmod{p}. \tag{1.14}$$

This in turn implies

$$U_n \equiv (-1)^{n-1}(n-1) \pmod{p}, \tag{1.15}$$

which proves (1.11).

We remark that the first equality in (1.12) yields the formula

$$S_n = p(N_0 - N_1), \tag{1.16}$$

where

$$N_a := \left\{(x_1, \ldots, x_n) \in (\mathbb{F}_p^*)^n : \ \Sigma x_i = 0, \ \Sigma \overline{x_i} = a\right\}. \tag{1.17}$$

See also [8, pp. 61–62].

By (1.9) and (1.10),

$$S_6 \sim 5p^4 \quad \text{as} \quad p \to \infty. \tag{1.18}$$

In fact, (1.18) is a special case of the asymptotic formula

$$S_{2k} \sim \binom{2k}{k} \frac{1}{k+1}\, p^{k+1} \quad \text{as} \quad p \to \infty, \tag{1.19}$$

which can be proved for each fixed integer $k > 0$ using the work of Katz on Kloosterman sheaves [8, p. 64]. Note that the estimate

$$S_{2k} < 4^k p^{k+1}$$

follows immediately from (1.2) and the Weil bound [8, (4.19)].

By (1.7) and (1.8),

$$|S_5| \le (6 + 9/p)p^3 < 8p^3, \quad \text{for} \;\; p > 5. \tag{1.20}$$

This is a special case of the estimate

$$|S_{2k+1}| \le \left(4^k - \binom{2k+1}{k} + \left(\binom{2k+1}{k} - 1\right)/p\right) p^{k+1} \tag{1.21}$$

for $p > 2k+1$, which again can be proved for each fixed integer $k > 0$ using [8, p. 64].

By (1.5), $(p/3)S_3 > 0$ for all $p > 3$. It can also be shown (using the estimates of Katz) that $(p/3)S_5 > 0$ for all $p > 5$. On the other hand, S_7, S_9, S_{11}, and S_{13} are each negative when, e.g., $p = 2161$.

2 Theorems and preliminaries

Theorem 2.1 *Let $n > 1$ be odd, with binary expansion*

$$1 + 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}, \quad 0 < a_1 < a_2 < \cdots < a_m.$$

Write

$$M_n = \Pi(2^{a_m} \pm 2^{a_{m-1}} \pm \cdots \pm 2^{a_1} \pm 1), \tag{2.1}$$

where the product is over all 2^m *choices of signs. Then for each prime* $p > n$,

$$S_n \equiv -\left(\frac{p}{M_n}\right) \pmod 4, \tag{2.2}$$

where the symbol on the right is the Jacobi symbol.

Example: For $n = 21$, we have $M_{21} = \Pi(2^4 \pm 2^2 \pm 1) = 21 \cdot 19 \cdot 13 \cdot 11 = 57057$, so

$$S_{21} \equiv -\left(\frac{p}{57057}\right) \pmod 4$$

for all $p > 21$.

Theorem 2.2 *Let* $n > 1$ *be even, with binary expansion*

$$2^{a_1} + \cdots + 2^{a_m}, \quad 0 < a_1 < \cdots < a_m.$$

Then for each prime $p > n$,

$$S_n \equiv \begin{cases} 1-p \pmod 4, & \text{if} \quad m = 1 \\ -1 \pmod 4, & \text{if} \quad m = 2 \\ 1 \pmod 4, & \text{if} \quad m > 2. \end{cases} \tag{2.3}$$

Example: For $p > 14$, we have $S_{14} \equiv 1 \pmod 4$, $S_6 \equiv S_{10} \equiv S_{12} \equiv -1 \pmod 4$, and $S_2 \equiv S_4 \equiv S_8 \equiv 1 - p \pmod 4$.

For the proofs of Theorems 2.1 and 2.2, we will need the following result of Kummer (see [5]) for binomial coefficients $\binom{N}{M}$.

Theorem (Kummer, 1852) *Let* q *be a prime. Then*

$$q^c \| \binom{N}{M},$$

where c *is the number of carries resulting from the addition of* M *and* $N - M$ *in base* q.

We will also need the simple facts

$$K(0) = -1 \tag{2.4}$$

and, for nonzero $a \pmod p$,

$$K(a) \equiv \begin{cases} \zeta_p^{2b} + \zeta_p^{-2b} \pmod 2, & \text{if} \quad a \equiv b^2 \pmod p \\ 0 \pmod 2, & \text{if} \quad \left(\frac{a}{p}\right) = -1. \end{cases} \tag{2.5}$$

To prove (2.5), first note that the term $\zeta_p^{x+a/x}$ in (1.1) remains unchanged when x is replaced by a/x, then note that $x \not\equiv a/x \pmod p$ unless $x \equiv \pm b \pmod p$ with $a \equiv b^2 \pmod p$.

Finally, for the quadratic character ϕ on $\mathbb{F}_p$ (defined by $\phi(r) = (r/p)$), recall that the quadratic Gauss sum

$$G(\phi) := \sum_{x=1}^{p-1} \phi(x)\zeta_p^x = \sum_{b=0}^{p-1} \zeta_p^{b^2} \tag{2.6}$$

satisfies the elementary formula [1, p. 12]

$$G(\phi)^2 = \phi(-1)p. \tag{2.7}$$

3 Proof of Theorem 2.1

Assume that $p > n$, where

$$n = 1 + 2^{a_1} + \cdots + 2^{a_m}, \quad 0 < a_1 < \cdots < a_m. \tag{3.1}$$

Our objective is to prove (2.2). If $n = 3$, then (2.2) follows from (1.5), so assume that $n \geq 5$. For brevity, write

$$N = n - 1. \tag{3.2}$$

For nonzero $a \pmod p$, (2.5) yields

$$K(a)^N \equiv \begin{cases} \left(\zeta_p^{2b} + \zeta_p^{-2b}\right)^N \pmod 4, & \text{if} \quad a \equiv b^2 \pmod p \\ 0 \pmod 4, & \text{if} \quad \left(\frac{a}{p}\right) = -1. \end{cases} \tag{3.3}$$

By (2.4) and (3.3),

$$\begin{aligned} S_n &\equiv (-1)^n + \frac{1}{2} \sum_{b=1}^{p-1} K(b^2)^n \\ &\equiv -1 + \frac{1}{2} \sum_{b=1}^{p-1} \left(\zeta_p^{2b} + \zeta_p^{-2b}\right)^N K(b^2) \pmod 4. \end{aligned} \tag{3.4}$$

The lower limit $b = 1$ on the far right may be replaced by $b = 0$, since $8|2^N$. Thus

$$
\begin{aligned}
(3.5) \qquad S_n + 1 &\equiv \frac{1}{2} \sum_{k=0}^{N} \binom{N}{k} \sum_{b=0}^{p-1} K(b^2)\, \zeta_p^{2b(2k-N)} \\
&= \frac{1}{2} \sum_{k=0}^{N} \binom{N}{k} \sum_{x=1}^{p-1} \zeta_p^{x} \sum_{b=0}^{p-1} \zeta_p^{b^2/x+2b(2k-N)} \\
&= \frac{1}{2} \sum_{k=0}^{N} \binom{N}{k} \sum_{x=1}^{p-1} \zeta_p^{x-x(2k-N)^2} \sum_{b=0}^{p-1} \zeta_p^{(b+x(2k-N))^2/x} \\
&= G(\phi)\frac{1}{2} \sum_{k=0}^{N} \binom{N}{k} \sum_{x=1}^{p-1} \phi(x)\zeta_p^{x(n-2k)(2k+2-n)} \\
&= G^2(\phi)\frac{1}{2} \sum_{k=0}^{N} \binom{N}{k} \phi(n-2k)\phi(2k+2-n) \pmod 4,
\end{aligned}
$$

where the last equality follows because $(n-2k)(2k+2-n) \not\equiv 0 \pmod p$, in view of the fact that n is an odd integer $< p$. The right side of (3.5) is an integer, and $G(\phi)^2 \equiv 1 \pmod 4$ by (2.7). Thus

$$
\begin{aligned}
(3.6) \qquad S_n + 1 &\equiv \frac{1}{2} \sum_{k=0}^{N} \binom{N}{k} \phi(n-2k)\phi(2k+2-n) \\
&= \frac{1}{2}\binom{N}{N/2} + \sum_{0 \le k < N/2} \binom{N}{k} \phi(n-2k)\phi(2k+2-n) \\
&\equiv \frac{1}{2}\binom{N}{N/2} + \sum_{0 \le k < N/2} \binom{N}{k} (-1-\phi(n-2k)-\phi(2k+2-n)) \\
&= \binom{N}{N/2} - 2^{N-1} - \sum_{0 \le k < N/2} \binom{N}{k} \{\phi(n-2k)+\phi(2k+2-n)\} \\
&\equiv \binom{N}{N/2} - \sum_{\substack{0 \le k < N/2 \\ \binom{N}{k} \text{ odd}}} \binom{N}{k} \{\phi(n-2k)+\phi(2k+2-n)\} \pmod 4,
\end{aligned}
$$

where the last congruence holds because the expression in braces is even.

Let T denote the set of 2^{m-1} subsums of the sum $2^{a_{m-1}} + \cdots + 2^{a_1}$. If $m = 1$, interpret $T = \{0\}$. For $0 \le k < N/2$, Kummer's Theorem gives

$$\binom{N}{k} \text{ is odd if and only if } \; k \in T. \tag{3.7}$$

Also by Kummer's theorem,

$$2^m \,\Big\|\, \binom{N}{N/2}. \tag{3.8}$$

Suppose first that $m = 1$. By (3.6) – (3.8),

$$S_n \equiv 1 - \phi(n) - \phi(2-n) \equiv -\phi(n(2-n)) \pmod 4. \tag{3.9}$$

By (2.1), $M_n = n(n-2) \equiv 3 \pmod 4$, so (3.9) yields, in view of quadratic reciprocity,

$$S_n \equiv -\left(\frac{p}{M_n}\right) \pmod 4.$$

This completes the proof of (2.2) in the case $m = 1$, so suppose now that $m > 1$. By (3.6) – (3.8),

$$-S_n \equiv 1 + \sum_{k \in T} (\phi(n-2k) + \phi(2k+2-n)) \pmod 4. \tag{3.10}$$

The right side of (3.10) is the sum of $2|T| + 1 = 2^m + 1$ terms in $\{\pm 1\}$. It is easily proved that any sum of t terms in $\{\pm 1\}$ with $t \equiv 1 \pmod 4$ is congruent (mod 4) to the product of these same t terms. Thus

$$S_n \equiv -\prod_{k \in T} \phi((n-2k)(n-2k-2)) \pmod 4. \tag{3.11}$$

By (3.1) and the definition of T,

$$M_n = \prod_{k \in T} (n-2k)(n-2k-2). \tag{3.12}$$

Note that $M_n \equiv (-1)^{|T|} = 1 \pmod 4$. By (3.11) – (3.12) and quadratic reciprocity,

$$S_n \equiv -\phi(M_n) = -\left(\frac{p}{M_n}\right) \pmod 4 \tag{3.13}$$

and the proof of (2.2) is complete. $\square$

4 Proof of Theorem 2.2

As might be expected from the relative simplicity of (2.3) compared to (2.2), Theorem 2.2 has a considerably shorter proof than Theorem 2.1. Assume that $p > n$, where

$$n = 2^{a_1} + \cdots + 2^{a_m}, \quad 0 < a_1 < \cdots < a_m. \tag{4.1}$$

If $n = 2$ or 4, then (2.3) follows from (1.4) and (1.6), so assume that $n \geq 6$. By (2.4) and (3.3),

$$\begin{aligned} S_n &\equiv (-1)^n + \frac{1}{2} \sum_{b=1}^{p-1} K(b^2)^n \\ &\equiv 1 + \frac{1}{2} \sum_{b=1}^{p-1} \left(\zeta_p^{2b} + \zeta_p^{-2b}\right)^n \\ &\equiv 1 + \frac{1}{2} \sum_{b=0}^{p-1} \left(\zeta_p^{2b} + \zeta_p^{-2b}\right)^n \\ &\equiv 1 + \frac{1}{2} \sum_{k=0}^{n} \binom{n}{k} \sum_{b=0}^{p-1} \zeta_p^{2b(2k-n)} \pmod 4. \end{aligned} \tag{4.2}$$

As $p > n$, we have $2k - n \equiv 0 \pmod p$ if and only if $k = n/2$. Thus

$$S_n \equiv 1 + \frac{p}{2}\binom{n}{n/2} \pmod 4. \tag{4.3}$$

By (4.3) and (3.8),

$$S_n \equiv \begin{cases} 1 \pmod 4, & \text{if} \quad m > 2 \\ -1 \pmod 4, & \text{if} \quad m = 2. \end{cases}$$

This completes the proof of (2.3) when $m > 1$. Finally, assume $m = 1$, so that $n = 2^a$ for some $a \geq 3$. We have

$$\begin{aligned} \binom{n}{n/2} &= \prod_{u=1}^{2^{a-1}} \frac{(2^{a-1} + u)}{u} \\ &\equiv \prod_{v=1}^{4} \left(\frac{2^{a-1} + v2^{a-3}}{v2^{a-3}}\right) = \prod_{v=1}^{4} \left(\frac{4+v}{v}\right) \equiv -2 \pmod 8. \end{aligned} \tag{4.4}$$

By (4.3) and (4.4),

$$S_n \equiv 1 - p \pmod 4,$$

which completes the proof of (2.3). □

5 Conjectural congruences

In this section, we conjecture congruences for S_7, S_9 and S_{11} (mod 16), as well as for S_6 (mod 2^5), S_8 (mod 2^7), S_{10} (mod 2^6), and S_{12} (mod 2^6). These congruences have been verified for at least the first 360 primes.

Congruences for S_7 (mod 16) when $p > 7$

(5.1)
$$S_7 \equiv 1 \Leftrightarrow (p/5) = -1,\ (p/21) = 1,\ \text{and}$$
$$(2/p) = \begin{cases} 1, & \text{if} \quad (p/3) = 1 \\ -(-1/p), & \text{if} \quad (p/3) = -1. \end{cases}$$

(5.2)
$$S_7 \equiv 3 \Leftrightarrow (p/15) = (p/7) = -1 \quad \text{and} \quad (-1/p) = -(p/3).$$

(5.3)
$$S_7 \equiv 5 \Leftrightarrow (p/5) = 1,\ (p/21) = -1, \quad \text{and}$$
$$(2/p) = \begin{cases} -(-1/p), & \text{if} \quad (p/3) = 1 \\ 1, & \text{if} \quad (p/3) = -1. \end{cases}$$

(5.4)
$$S_7 \equiv 7 \quad \text{never occurs.}$$

(5.5)
$$S_7 \equiv 9 \Leftrightarrow (p/5) = -1,\ (p/21) = 1, \quad \text{and}$$
$$(2/p) = \begin{cases} -1, & \text{if} \quad (p/3) = 1 \\ (-1/p), & \text{if} \quad (p/3) = -1. \end{cases}$$

(5.6)
$$S_7 \equiv 11 \Leftrightarrow (p/15) = (p/7) = -1 \quad \text{and} \quad (p/3) = (-1/p).$$

(5.7)
$$S_7 \equiv 13 \Leftrightarrow (p/5) = 1,\ (p/21) = -1, \quad \text{and}$$
$$(2/p) = \begin{cases} (-1/p), & \text{if} \quad (p/3) = 1 \\ -1, & \text{if} \quad (p/3) = -1. \end{cases}$$

$$(5.8) \qquad S_7 \equiv 15 \Leftrightarrow (p/15) = (p/7) = 1.$$

Congruences for $S_9 \pmod{16}$ **when** $p > 9$

$$(5.9) \qquad S_9 \equiv 15 \quad \text{if} \quad (p/7) = 1 \quad \text{and} \quad (p/15) = 1.$$

$$(5.10) \qquad S_9 \equiv 7 \quad \text{if} \quad (p/7) = 1 \quad \text{and} \quad (p/15) = -1.$$

$$(5.11) \qquad S_9 \equiv 5 \quad \text{if} \quad (p/7) = -1 \quad \text{and} \quad (p/15) = -(2/p).$$

$$(5.12) \qquad S_9 \equiv 13 \quad \text{if} \quad (p/7) = -1 \quad \text{and} \quad (p/15) = (2/p).$$

Congruences for $S_{11} \pmod{16}$ **when** $p > 11$

$$(5.13) \qquad S_{11} \equiv 1 \Leftrightarrow (p/55) = (p/3) = -(p/7) \quad \text{and} \quad (2/p) = \begin{cases} 1, & \text{if} \quad (p/3) = 1 \\ (11/p), & \text{if} \quad (p/3) = -1. \end{cases}$$

$$(5.14) \qquad S_{11} \equiv 3 \Leftrightarrow (p/77) = (p/5) = -(p/3) \quad \text{and} \quad (p/3) = \begin{cases} (p/7), & \text{if} \quad (-1/p) = -1 \\ 1, & \text{if} \quad (-1/p) = 1. \end{cases}$$

$$(5.15) \qquad S_{11} \equiv 5 \Leftrightarrow (p/3) = (p/7) = -(p/55) \quad \text{and} \quad (2/p) = \begin{cases} -1, & \text{if} \quad (p/3) = 1 \\ (11/p), & \text{if} \quad (p/3) = -1. \end{cases}$$

$$(5.16) \qquad S_{11} \equiv 7 \Leftrightarrow (p/77) = (p/3) = (p/5) \quad \text{and} \quad (p/7) = (-1/p) = -1.$$

$$(5.17) \qquad S_{11} \equiv 9 \Leftrightarrow (p/55) = (p/3) = -(p/7) \quad \text{and} \quad (2/p) = \begin{cases} -1, & \text{if} \quad (p/3) = 1 \\ -(11/p), & \text{if} \quad (p/3) = -1. \end{cases}$$

(5.18) $$S_{11} \equiv 11 \Leftrightarrow (p/77) = (p/5) = -(p/3) \quad \text{and}$$
$$(p/3) = \begin{cases} -(p/7), & \text{if} \quad (-1/p) = -1 \\ -1, & \text{if} \quad (-1/p) = 1. \end{cases}$$

(5.19) $$S_{11} \equiv 13 \Leftrightarrow (p/3) = (p/7) = -(p/55) \quad \text{and}$$
$$(2/p) = \begin{cases} 1, & \text{if} \quad (p/3) = 1 \\ -(11/p), & \text{if} \quad (p/3) = -1. \end{cases}$$

(5.20) $$S_{11} \equiv 15 \Leftrightarrow (p/77) = (p/3) = (p/5) \quad \text{and}$$
$$(p/7), (-1/p) \quad \text{are not both} \quad -1.$$

Congruences for S_6 (mod 32) when $p > 6$

The congruences below depend on parameters in the following binary quadratic forms representing p:

(5.21) $$p = a^2 + 4b^2, \quad \text{when} \;\; p \equiv 1 \pmod 4,$$

(5.22) $$p = c^2 + 2d^2, \quad \text{when} \;\; p \equiv 3 \pmod 8,$$

(5.23) $$p = e^2 + 6f^2, \quad \text{when} \;\; p \equiv 7 \pmod{24},$$

and

(5.24) $$p = 6h^2 - g^2, \quad \text{when} \;\; p \equiv 23 \pmod{24}.$$

We have the following conjectures for S_6 (mod 32).

(5.25) $$\text{If} \quad p \equiv 1 \pmod{24}, \quad \text{then} \quad S_6 \equiv 11.$$

(5.26) $$\text{If} \quad p \equiv 5 \pmod{24}, \quad \text{then}$$
$$S_6 \equiv \begin{cases} 3, & \text{if} \quad a \equiv \pm b \pmod{12} \\ 19, & \text{otherwise.} \end{cases}$$

(5.27) $$\text{If} \quad p \equiv 7 \pmod{24}, \quad \text{then}$$
$$S_6 \equiv \begin{cases} 3, & \text{if} \quad e \equiv \pm 1 \pmod{12} \\ 19, & \text{otherwise.} \end{cases}$$

(5.28) If $p \equiv 11 \pmod{24}$, then

$$S_6 \equiv \begin{cases} 3, & \text{if} \quad \pm d \equiv 3 - 2(-1)^{(p-3)/8} \pmod{12} \\ 19, & \text{otherwise.} \end{cases}$$

(5.29) If $p \equiv 13 \pmod{24}$, then

$$S_6 \equiv \begin{cases} 11, & \text{if} \quad 3|b \\ 27, & \text{otherwise.} \end{cases}$$

(5.30) If $p \equiv 17 \pmod{24}$, then

$$S_6 \equiv \begin{cases} 11, & \text{if} \quad 4|b \\ 27, & \text{otherwise.} \end{cases}$$

(5.31) If $p \equiv 19 \pmod{24}$, then

$$S_6 \equiv \begin{cases} 3, & \text{if} \quad c \equiv \pm 1 \pmod{12} \\ 19, & \text{otherwise.} \end{cases}$$

(5.32) If $p \equiv 23 \pmod{24}$, then

$$S_6 \equiv \begin{cases} 11, & \text{if} \quad g \equiv \pm 1 \text{ or } \pm 5 \pmod{24} \\ 27, & \text{otherwise.} \end{cases}$$

Congruences for $S_8 \pmod{128}$ when $p > 8$

The congruences below again depend on parameters in (5.21) – (5.24).

(5.33) If $p \equiv 1 \pmod{24}$, then $S_8 \equiv 37 - p$.

(5.34) If $p \equiv 5 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 37 - p, & \text{if} \quad a \equiv \pm b \pmod{12} \\ 101 - p, & \text{otherwise.} \end{cases}$$

(5.35) If $p \equiv 7 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 61 - p, & \text{if} \quad e \equiv \pm 1 \pmod{12} \\ 125 - p, & \text{otherwise.} \end{cases}$$

(5.36) If $p \equiv 11 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 93 - p, & \text{if} \quad \pm d \equiv 3 - 2(-1)^{(p-3)/8} \pmod{12} \\ 29 - p, & \text{otherwise.} \end{cases}$$

(5.37) If $p \equiv 13 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 69 - p, & \text{if} \quad 3|b \\ 5 - p, & \text{otherwise.} \end{cases}$$

(5.38) If $p \equiv 17 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 37 - p, & \text{if} \quad 4|b \\ 101 - p, & \text{otherwise.} \end{cases}$$

(5.39) If $p \equiv 19 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 93 - p, & \text{if} \quad c \equiv \pm 1 \pmod{12} \\ 29 - p, & \text{otherwise.} \end{cases}$$

(5.40) If $p \equiv 23 \pmod{24}$, then

$$S_8 \equiv \begin{cases} 93 - p, & \text{if} \quad g \equiv \pm 1 \text{ or } \pm 5 \pmod{24} \\ 29 - p, & \text{otherwise.} \end{cases}$$

Note the remarkable parallel between the congruences for S_6 and S_8. This does not persist for S_{10} and S_{12}, where additional quadratic forms come into play.

Congruences for S_{10} (mod 64) when $p > 10$

(5.41) If $p \equiv 71 \pmod{120}$, so $p = 60u^2 - v^2$, then

$$S_{10} \equiv \begin{cases} 15, & \text{if} \quad \pm v \equiv 5 - 3(-1)^{(p-7)/8} \pmod{15} \\ 47, & \text{if} \quad \pm v \equiv 5 + 3(-1)^{(p-7)/8} \pmod{15}. \end{cases}$$

(5.42) If $p \equiv 17 \pmod{120}$, so $p = 3s^2 + 5t^2$, then

$$S_{10} \equiv \begin{cases} 15, & \text{if} \quad t \equiv \pm 1 \pmod{12} \\ 47, & \text{if} \quad t \equiv \pm 5 \pmod{12}. \end{cases}$$

As the complete list of congruences for S_{10} (mod 64) is quite long, we refer the reader to [3] for the remaining congruences.

Congruences for S_{12} (mod 64) when $p > 12$

(5.43) If $p \equiv 71 \pmod{240}$, so $p = x^2 - 10y^2$, then

$$S_{12} \equiv \begin{cases} 3, & \text{if} \quad \pm y \equiv 3 - 2(-1)^{(p-7)/16} \pmod{12} \\ 35, & \text{if} \quad \pm y \equiv 3 + 2(-1)^{(p-7)/16} \pmod{12}. \end{cases}$$

(5.44) If $p \equiv 17 \pmod{240}$, so $p = 3s^2 + 5t^2$, then

$$S_{12} \equiv \begin{cases} 31, & \text{if} \quad \pm s \equiv 3 - 2(-1)^{(p-17)/16} \pmod{12} \\ 63, & \text{if} \quad \pm s \equiv 3 + 2(-1)^{(p-17)/16} \pmod{12}. \end{cases}$$

For the long list of remaining congruences for S_{12} (mod 64), see [3].

Acknowledgments: The authors are grateful to Nick Katz, Daqing Wan, Harold Stark, and William Stein for valuable suggestions. We are also grateful to Scott Ahlgren and Tim Kilbourn for informing us about the work in references [7], [9], and [10].

References

[1] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Wiley- Interscience, N.Y., 1998.

[2] H. T. Choi and R. J. Evans, *Sums of powers of Kloosterman sums*, San Diego AMS joint meeting, January 7, 2002, 973-U1-1062.

[3] H. T. Choi and R. J. Evans, *Conjectural congruences for sums of powers of Kloosterman sums*, (http://www.math.ucsd.edu/~revans/kloospowers).

[4] R. J. Evans, *Seventh power moments of Kloosterman sums*, to appear.

[5] A. Granville, *Arithmetic properties of binomial coefficients*, (http://www.dms.umontreal.ca/~andrew/Binomial).

[6] S. Gurak, *Polynomials for Kloosterman sums*, Canad. Math. Bulletin, to appear.

[7] K. Hulek, J. Spandaw, B. van Geemen, and D. van Straten, *The modularity of the Barth-Nieto quintic and its relatives*, Adv. Geom. **1** (2001), 263–289.

[8] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Math., vol. 17, Amer. Math. Soc., Providence, RI, 1997.

[9] R. Livné, *Motivic orthogonal two-dimensional representations of* Gal($\overline{\mathbf{Q}}/\mathbf{Q}$), Israel J. Math. **92** (1995), 149–156.

[10] C. Peters, J. Top, and M. van der Vlugt, *The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes*, J. Reine Angew. Math. **432** (1992), 151–176.

[11] H. Salié, *Über die Kloostermanschen Summen S(u,v;q)*, Math. Z. **34** (1931), 91-109.