SEVENTH POWER MOMENTS OF KLOOSTERMAN SUMS

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

June, 2008

2000 *Mathematics Subject Classification*: 11L05, 11F23, 11F30

Key Words: power moment, Kloosterman sum, newform, nebentypus, Hecke eigenvalue, symmetric power.

Abstract

Evaluations of the n-th power moments S_n of Kloosterman sums are known only for $n \leqslant 6$. We present here substantial evidence for an evaluation of S_7 in terms of Hecke eigenvalues for a weight 3 newform on $\Gamma_0(525)$ with quartic nebentypus of conductor 105. We also prove some congruences modulo 3, 5 and 7 for the closely related quantity T_7, where T_n is a sum of traces of n-th symmetric powers of the Kloosterman sheaf.

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

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

and their n-th power moments

$$(1.2) \qquad S_n = \sum_{a=0}^{p-1} K(a)^n, \quad n \in \mathbb{N}.$$

It is well-known [5, §4.4] that

$$(1.3) \qquad S_1 = 0, \quad S_2 = p^2 - p, \quad S_3 = (\frac{p}{3})p^2 + 2p, \quad S_4 = 2p^3 - 3p^2 - 3p.$$

The work in [8], [9] shows that S_5 can be expressed in terms of the p-th eigenvalue for a weight 3 newform on $\Gamma_0(15)$. The work in [4] shows that S_6 can be expressed in terms of the p-th eigenvalue for a weight 4 newform on $\Gamma_0(6)$. See also [1].

In Conjecture 1.1 below, we propose an evaluation of S_7 in terms of the p-th eigenvalue for a weight 3 newform on $\Gamma_0(525)$. This conjecture is based on substantial numerical evidence.

Write

$$(1.4) \qquad K(a) = -g(a) - h(a), \quad a \neq 0,$$

where $g(a)$, $h(a)$ are the two Frobenius eigenvalues for the Kloosterman sheaf at a, given by

$$(1.5) \qquad g(a) = p^{1/2}\exp(i\theta_p(a)), \quad h(a) = p^{1/2}\exp(-i\theta_p(a)),$$

with $\theta_p(a) \in [0, \pi]$. (In fact, $\theta_p(a) \in (0, \pi)$; see [2, Theorem 6.1].) By (1.2) and (1.4),

$$(1.6) \qquad S_n = (-1)^n + (-1)^n \sum_{a=1}^{p-1} (g(a) + h(a))^n.$$

As noted in [5, p. 63], one should study the "more natural" related expressions

$$T_n = \sum_{a=1}^{p-1} (g(a)^n + g(a)^{n-1}h(a) + \cdots + h(a)^n). \tag{1.7}$$

The summand in (1.7) is the trace of the n-th symmetric power of the Kloosterman sheaf at a, and equals

$$p^{n/2} U_n(2\cos\theta_p(a)), \tag{1.8}$$

where U_n is the n-th Chebyshev polynomial of the second kind. We have the bound [3, Theorem 0.2], [6]

$$|1 + T_n| \leqslant \left[\frac{n-1}{2}\right] p^{(n+1)/2}, \qquad \text{if } \ p > n > 0, \tag{1.9}$$

whose proof is based on Deligne's theory of exponential sums for varieties over $\mathbb{F}_p$. (A slightly weaker bound which holds for all $p > 2$ is given in [5, Theorem 4.6].)

The expressions S_n and T_n are related by the formula

$$(-1)^n S_n - 1 = \sum_{k=0}^{[n/2]} \left\{ \binom{n}{k} - \binom{n}{k-1} \right\} p^k T_{n-2k}. \tag{1.10}$$

In [1, (1.11)], it is proved that S_n is an integer multiple of p satisfying

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

From (1.10)–(1.11), it follows by induction that

$$T_n \equiv -1 (\text{mod } p^2), \quad n > 0. \tag{1.12}$$

By (1.3) and (1.10), we have

$$T_0 + 1 = p, \;\; T_1 + 1 = T_2 + 1 = 0, \;\; T_3 + 1 = -\left(\frac{p}{3}\right) p^2, \;\; T_4 + 1 = -p^2. \tag{1.13}$$

By [1, (1.8)], we have for $p > 5$,

$$a_p := \frac{-1 - T_5}{p^2} = \begin{cases} 2p - 12u^2, & \text{if} \quad p = 3u^2 + 5v^2 \\ 4x^2 - 2p, & \text{if} \quad p = x^2 + 15y^2 \\ 0, & \text{if} \quad (\frac{p}{15}) = -1. \end{cases} \tag{1.14}$$

Define

$$c_p := (-1 - T_7)/p^2. \tag{1.15}$$

By (1.12), a_p and c_p are integers, and by (1.9), we have

$$|a_p| \leqslant 2p, \quad |c_p| \leqslant 3p^2. \tag{1.16}$$

Putting $n = 7$ in (1.10) yields

$$S_7 = p^2 c_p + 6p^3 a_p + 14\left(\frac{p}{3}\right)p^4 + 14p^3 + 14p^2 + 6p. \tag{1.17}$$

Hence by (1.16),

$$|S_7| \leqslant 29p^4 + 14p^3 + 14p^2 + 6p. \tag{1.18}$$

In view of (1.14) and (1.17), an evaluation of c_p would yield an evaluation of S_7. Hence we focus on c_p in Conjecture 1.1 below, and in the sequel.

Let χ_5 denote the quartic Dirichlet character (mod 5) defined by $\chi_5(2) = -i$, and let ψ denote the quartic character of conductor 105 defined by

$$\psi(d) = \left(\frac{d}{21}\right)\chi_5(d), \quad d \in \mathbb{Z}. \tag{1.19}$$

Conjecture 1.1. *For $p > 7$,*

$$c_p = \left(\frac{p}{105}\right)(-p^2 + b(p)^2\ \overline{\psi}(p)) = \left(\frac{p}{105}\right)(-p^2 + |b(p)|^2), \tag{1.20}$$

where $b(p)$ is the p-th Hecke eigenvalue for a weight 3 newform f on $\Gamma_0(525)$ with nebentypus ψ and eigenfield $\mathbb{Q}(i, \sqrt{6}, \sqrt{14})$.

In Section 2, we motivate Conjecture 1.1 and discuss the evidence for it. In Section 3, we examine the integers c_p modulo 3, 5, and 7, proving in the process some observations of Katz [7]. Section 4, the Appendix, records a Sage [11] session which exhibits numerical evidence for Conjecture 1.1.

2 Motivation and evidence for Conjecture 1.1

The following conjecture has been verified for each of the 396 primes p in the interval $7 < p \le 2741$.

Conjecture 2.1. *Let $p > 7$, and define the signature $\alpha_p := \left(\left(\frac{p}{3}\right), \left(\frac{p}{5}\right), \left(\frac{p}{7}\right)\right)$. Then*

$$\left(\frac{p}{105}\right) c_p + p^2 = x(p)^2 \tag{2.1}$$

for a nonnegative number $x(p)$ of the form:

$2m\sqrt{7}$ *with* $m \equiv \pm 1 \pmod{10}$, $3 \nmid m$, *if* $\alpha_p = (1, -1, -1)$;
$4m\sqrt{3}$ *with* $m \equiv \pm 1 \pmod{10}$, *if* $\alpha_p = (-1, -1, 1)$;
$2m\sqrt{42}$ *with* $m \equiv \pm 1 \pmod{5}$, *if* $\alpha_p = (1, -1, 1)$;
$6m\sqrt{2}$ *with* $m \equiv \pm 2 \pmod{5}$, *if* $\alpha_p = (-1, -1, -1)$;
$2m$ *with* $m \equiv \pm(3 - 2\chi_5(p)) \pmod{10}$, $3 \nmid m$, *if* $\alpha_p = (1, 1, 1)$;
$4m\sqrt{21}$ *with* $m \equiv \pm(1 + \chi_5(p)) \pmod{5}$, *if* $\alpha_p = (-1, 1, -1)$;
$2m\sqrt{6}$ *with* $m \equiv \pm(2 - 2\chi_5(p)) \pmod{5}$, *if* $\alpha_p = (1, 1, -1)$;
$6m\sqrt{14}$ *with* $m \equiv \pm(2 - 2\chi_5(p)) \pmod{5}$, *if* $\alpha_p = (-1, 1, 1)$

where m is a positive integer.

The values of $x(p)$ for $7 < p < 100$ are given in Table 2.1 below.

p	11	13	17	19	23	29	31
$x(p)$	0	$2\sqrt{7}$	$18\sqrt{2}$	$8\sqrt{6}$	$4\sqrt{3}$	$6\sqrt{14}$	$10\sqrt{6}$

p	37	41	43	47	53	59	61
$x(p)$	$2\sqrt{42}$	$12\sqrt{21}$	$8\sqrt{42}$	$12\sqrt{2}$	$36\sqrt{3}$	$20\sqrt{21}$	$30\sqrt{6}$

p	67	71	73	79	83	89	97
$x(p)$	$12\sqrt{42}$	$30\sqrt{14}$	$38\sqrt{7}$	50	$78\sqrt{2}$	$20\sqrt{21}$	$38\sqrt{7}$

Table 2.1

Motivated by our Conjecture 2.1, Katz [7] proposed the following scenario. For $p > 7$, the number c_p/p^2 (which lies in $[-3, 3]$ by (1.16)) is the trace of

Frob_p in a representation towards O(3) (the orthogonal group with respect to a trace form). This Frob_p has determinant $(\frac{p}{105})$, so $(\frac{p}{105})c_p/p^2$ is the trace of Frob_p in a representation towards SO(3). For some Dirichlet character χ, this representation is $\overline{\chi}(p) \otimes \mathrm{Sym}^2(V)$ for a 2–dimensional representation V, where Frob_p in V has eigenvalues $\alpha,\ \beta$ with $|\alpha| = |\beta| = 1$ and $\alpha\beta = \chi(p)$. After equating traces, we obtain

$$\chi(p)\left(\frac{p}{105}\right)c_p/p^2 = \chi(p) + \alpha^2 + \beta^2,$$

so

$$\chi(p)\left\{\left(\frac{p}{105}\right)c_p + p^2\right\} = p^2(\alpha+\beta)^2.$$

Define $b(p) := p(\alpha+\beta)$, so that $|b(p)| \leqslant 2p$ and $b(p)/p$ is the trace of Frob_p in V. In the notation of (2.1), it follows that

$$\chi(p)x(p)^2 = b(p)^2, \quad p > 7. \tag{2.2}$$

Assuming the validity of Katz's scenario, we hoped to find a Dirichlet character χ, a level N, and a weight 3 newform

$$f(z) = \sum_{m=1}^{\infty} \widehat{f}(m)e^{2\pi imz}, \quad \widehat{f}(p) = b(p) \tag{2.3}$$

on $\Gamma_0(N)$ with nebentypus χ such that $x(p) = |b(p)|$ for $p > 7$. The equality $x(p) = |b(p)|$ is equivalent to (2.2), by [5, (6.57)]. Our search for N, χ, f culminated with the discovery of a weight 3 newform (2.3) on $\Gamma_0(525)$ with nebentypus ψ and eigenfield $\mathbb{Q}(i, \sqrt{6}, \sqrt{14})$ such that $x(p) = |b(p)|$ for $7 < p < 100$. Equivalently,

$$\psi(p)x(p)^2 = b(p)^2, \quad 7 < p < 100,$$

which is powerful evidence that (1.20) in fact holds for *all* $p > 7$.

We proceed to describe how this newform f of level 525 was discovered. While browsing William Stein's *Modular Forms Explorer* found in his *Modular Forms Database* [10], we had encountered a weight 3 newform $g(z)$ on $\Gamma_0(168)$ with quadratic nebentypus of conductor 168 and eigenfield $\mathbb{Q}(i\sqrt{2}, \sqrt{3},\ i\sqrt{7})$. For each p with $7 < p < 100$, $|\widehat{g}(p)|$ appeared to be an integer multiple of one of $\sqrt{1}, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{7},\ \sqrt{14}, \sqrt{21}, \sqrt{42}$, just as was the case for $x(p)$ (cf. Table 2.1). Moreover, analogous to the situation in Conjecture 2.1, the particular choice of square root occurring in $|\widehat{g}(p)|$ seemed to be completely determined by the signature $((\frac{p}{3}), (\frac{p}{7}), (\frac{-8}{p}))$. The product of the conductors of the three quadratic characters in this signature is $3 \cdot 7 \cdot 8 = 168$, which equals the conductor of the nebentypus of g. It seemed reasonable to guess by analogy that the product of the conductors of the three quadratic characters in α_p, namely $3 \cdot 5 \cdot 7 = 105$, should be the conductor of the nebentypus χ of the newform f that we were seeking. Since f has odd weight, χ is odd. The simplest odd character of conductor 105 is the quartic character ψ defined in (1.19). Thus we took $\chi = \psi$ as a first guess, and the evidence strongly suggests that this was the right choice.

As a first guess for the level N, we took $N = 105$, hoping that the level would equal the conductor of the nebentypus as was the case for the newform g on $\Gamma_0(168)$. However, for newforms f on $\Gamma_0(105)$, there were already small primes $p > 7$ for which $|\widehat{f}(p)|$ failed to equal $x(p)$. Our next guess was that the level equals 105 times a small prime factor. The levels $2 \cdot 105$ and $3 \cdot 105$ each failed, but the level $5 \cdot 105 = 525$ provided a happy ending. Indeed the Sage session in the Appendix shows the existence of a weight 3 newform f on $\Gamma_0(525)$ with nebentypus ψ and eigenfield $\mathbb{Q}(i, \sqrt{6}, \sqrt{14})$ such that $|\widehat{f}(p)| = x(p)$ for all p with $7 < p < 100$. As was noted above, this is powerful evidence for Conjecture 1.1.

3 Congruences for c_p

Let $p > 7$. It follows from [1, Theorem 2.1] that $S_7 \equiv -(\frac{p}{105}) \pmod 4$. Thus, by (1.17),

(3.1) $$2 \nmid c_p.$$

Katz [7] observed that numerical evidence moreover suggests

(3.2) $$5 \nmid c_p$$

and

(3.3) $$7 \nmid c_p.$$

On the other hand, we conjecture that for every prime $q \notin \{2, 5, 7\}$, one has $q \mid c_p$ for infinitely many primes p.

In Theorem 3.1, we prove (3.3). In Theorem 3.2, we give an evaluation of c_p (mod 5) which in particular proves (3.2). In Theorem 3.3, we evaluate c_p (mod 3).

Our proofs will make use of the simple fact that

$$n \mid S_n, \quad \text{for prime } n. \tag{3.4}$$

To justify (3.4), note that

$$S_n = \sum_{a=0}^{p-1} \left(\sum_{x=1}^{p-1} \zeta_p^{x+a/x} \right)^n \equiv \sum_{x=1}^{p-1} \sum_{a=0}^{p-1} \zeta_p^{n(x+a/x)} \equiv 0 \pmod{n}.$$

Theorem 3.1. *For each $p > 7$, we have $7 \nmid c_p$.*

Proof. By (1.17),

$$p^2 c_p \equiv S_7 + p^3 a_p + p \pmod{7}.$$

Since $7 \mid S_7$ by (3.4),

$$p^2 c_p \equiv \left(\frac{p}{7}\right) a_p + p \pmod{7}. \tag{3.5}$$

It remains to prove that

$$\left(\frac{p}{7}\right) a_p + p \not\equiv 0 \pmod{7}. \tag{3.6}$$

We may assume that $a_p \neq 0$, since otherwise (3.6) is clear. By (1.14), either

$$a_p = 10v^2 - 6u^2 \quad \text{with} \quad p = 3u^2 + 5v^2. \tag{3.7}$$

or

$$a_p = 2x^2 - 30y^2 \quad \text{with} \quad p = x^2 + 15y^2. \tag{3.8}$$

In the case (3.7),

$$(\frac{p}{7})a_p + p = u^2(3 - 6(\frac{p}{7})) + v^2(5 + 10(\frac{p}{7})) \not\equiv 0 \pmod{7},$$

since $(-3+6(\frac{p}{7}))(5+10(\frac{p}{7}))$ is a nonsquare (mod 7). In the case (3.8),

$$(\frac{p}{7})a_p + p = x^2(1+2(\frac{p}{7})) + y^2(15-30(\frac{p}{7})) \not\equiv 0 \pmod 7,$$

since $(1+2(\frac{p}{7}))(-15+30(\frac{p}{7}))$ is a nonsquare (mod 7). □

Theorem 3.2. *For $p > 7$,*

$$c_p \equiv p + p\left(\frac{p}{5}\right) + \left(\frac{p}{21}\right) \pmod 5.$$

In particular, $5 \nmid c_p$.

Proof. All congruences in this proof are modulo 5. By (1.17),

$$p^2 c_p \equiv S_7 - p^3 a_p + \left(\frac{p}{3}\right)p^4 + p^3 + p^2 - p.$$

Since $p^2 \equiv \left(\frac{p}{5}\right)$, we have

$$c_p \equiv \left(\frac{p}{5}\right)S_7 - pa_p + \left(\frac{p}{15}\right) + p + 1 - \left(\frac{p}{5}\right)p. \tag{3.9}$$

It remains to prove

$$a_p \equiv \left(\frac{p}{3}\right)p + \left(\frac{p}{5}\right)p \tag{3.10}$$

and

$$S_7 \equiv 2p + \left(\frac{p}{105}\right), \tag{3.11}$$

since the theorem follows from (3.9)–(3.11).

By (1.10) and (1.13),

$$p^2 a_p = S_5 - 4p^3\left(\frac{p}{3}\right) - 5p^2 - 4p. \tag{3.12}$$

Thus

$$a_p \equiv \left(\frac{p}{5}\right) S_5 + \left(\frac{p}{3}\right) p + \left(\frac{p}{5}\right) p. \tag{3.13}$$

This proves (3.10), since $5 \mid S_5$ by (3.4).

To prove (3.11), observe that

$$\begin{aligned}
S_7 = \sum_{a=0}^{p-1} K(a)^7 &\equiv \sum_{a=0}^{p-1} K(a)^2 \sum_{x=1}^{p-1} \zeta_p^{5(x+a/x)} \\
&= \sum_{a=0}^{p-1} K(a)^2 K(25a) \\
&= \sum_{a=0}^{p-1} \sum_{x,y,z\neq 0} \zeta_p^{x+y+z+a(\frac{1}{x}+\frac{1}{y}+\frac{25}{z})} \\
&= p \sum_{\substack{x,y,z\neq 0 \\ \frac{1}{x}+\frac{1}{y}+\frac{25}{z}=0}} \zeta_p^{x+y+z} \\
&= p \sum_{\substack{x,y\neq 0 \\ x+y\neq 0}} \zeta_p^{x+y-25xy/(x+y)}.
\end{aligned}$$

With the change of variables

$$r = x + y, \qquad s = xy,$$

this becomes

$$\begin{aligned}
S_7 &\equiv p \sum_{r,s\neq 0} \zeta_p^{r-25s/r} \left\{ 1 + \left(\frac{r^2-4s}{p}\right) \right\} \\
&= p \sum_{r,s\neq 0} \zeta_p^{r(1-25s)} \left\{ 1 + \left(\frac{1-4s}{p}\right) \right\},
\end{aligned}$$

where in the last step we replaced s by sr^2. Replacing s by $(1-s)/4$, we obtain

$$
\begin{aligned}
S_7 &\equiv p \sum_{r\neq 0, s\neq 1} \zeta_p^{r(\frac{-21}{4}+\frac{25s}{4})}\big\{1+\big(\frac{s}{p}\big)\big\} \\
&= 2p - p^2 + p\sum_{r,s} \zeta_p^{r(\frac{-21}{4}+\frac{25s}{4})}\big\{1+\big(\frac{s}{p}\big)\big\} \\
&= 2p - p^2 + p^2\big\{1+\big(\frac{21}{p}\big)\big\} = 2p + p^2\big(\frac{p}{21}\big) \equiv 2p + \big(\frac{p}{105}\big).
\end{aligned}
$$

This completes the proof of (3.11). □

Theorem 3.3. *For $p > 7$,*

$$
c_p \equiv 1 + \big(\frac{p}{3}\big) + \big(\frac{p}{35}\big) \pmod 3.
$$

In particular, $3 \mid c_p$ *if and only if* $\left(\dfrac{p}{3}\right) = \left(\dfrac{p}{35}\right) = 1$.

Proof. By (1.17),

$$
c_p \equiv S_7 + \big(\frac{p}{3}\big) + p + 1 \pmod 3.
$$

Thus it remains to show that

$$
S_7 \equiv \left(\frac{p}{35}\right) - p \pmod 3. \tag{3.14}
$$

We have

$$
\begin{aligned}
S_7 &\equiv \sum_{a=0}^{p-1} K(a)\Bigg(\sum_{x=1}^{p-1} \zeta_p^{3(x+a/x)}\Bigg)^2 \\
&= \sum_{a=0}^{p-1} K(a)K(9a)^2 \\
&= \sum_{a=0}^{p-1} \sum_{x,y,z\neq 0} \zeta_p^{x+y+z+a(\frac{9}{x}+\frac{9}{y}+\frac{1}{z})} \pmod 3.
\end{aligned}
$$

The rest of the proof of (3.14) proceeds as in the proof of (3.11). □

4 Appendix

The Sage session below shows the existence of a weight 3 newform f on $\Gamma_0(525)$ with nebentypus ψ and eigenfield $\mathbb{Q}(i, \sqrt{6}, \sqrt{14})$, such that the p-th Fourier coefficients $b(p)$ of f satisfy (1.20) for $7 < p < 100$.

The session begins by setting `G` equal to the group of 16 Dirichlet characters modulo 525 of order dividing 4. The elements of `G` are placed into a list `X`, whose last element `Y` = `X[15]` equals the quartic character ψ of conductor 105 defined in (1.19).

Let `M` denote a modular symbols space of level 525, weight 3, with character ψ. This is a vector space of dimension 160 over $\mathbb{Q}(i)$. It has a "cuspidal subspace" `S` of dimension 148, and `S` in turn has a "new subspace" `N` of dimension 92. The space `N` is decomposed into 10 further subspaces, each invariant under Hecke operators, and `D` denotes a sorted list of these 10 subspaces. For more information about these spaces, see the Sage documentation at [11, `/doc/html/ref/module-sage.modular.modsym.space.html`].

Our desired eigenfunction f lies in the fifth invariant subspace `D[4]`, and `f` gives the first 97 terms of its q-expansion. Finally, `parent(f)` tells us that the Fourier coefficients of our eigenfunction all lie in the eigenfield $\mathbb{Q}($`zeta4`, `alpha`$)$, where `zeta4` $= i$ and `alpha` is a zero of

$$x^4 + (-8i - 8)x^3 + 98ix^2 + (-264i + 264)x - 1425.$$

We may take `alpha` $= 2\sqrt{2}z - \sqrt{3}z - 2\sqrt{7}z^7$, where $z = \exp(2\pi i/8)$. Then the eigenfield is easily seen to be $\mathbb{Q}(i, \sqrt{6}, \sqrt{14})$. Simplifying the q-expansion `f`, we obtain the following table of Fourier coefficients of f corresponding to primes $7 < p < 100$:

p	11	13	17	19	23	29	31
$b(p)$	0	$2\sqrt{7}z^7$	$18\sqrt{2}z^3$	$8\sqrt{6}$	$4\sqrt{3}z^3$	$6\sqrt{14}$	$10\sqrt{6}z^2$

p	37	41	43	47	53	59	61
$b(p)$	$2\sqrt{42}z^3$	$12\sqrt{21}z^4$	$8\sqrt{42}z^5$	$12\sqrt{2}z^7$	$36\sqrt{3}z^7$	$20\sqrt{21}z^2$	$30\sqrt{6}z^2$

p	67	71	73	79	83	89	97
$b(p)$	$12\sqrt{42}z^3$	$30\sqrt{14}z^6$	$38\sqrt{7}z^3$	$50z^2$	$78\sqrt{2}z$	$20\sqrt{21}z^6$	$38\sqrt{7}z$

Table 4.1

Comparison of Tables 2.1 and 4.1 shows that $x(p) = |b(p)|$ and so (1.20) holds for $7 < p < 100$.

SAGE SESSION

```
----------------------------------------------------------------------
| SAGE Version sage-2.11, Release Date: 2008-03-30                   |
| Type notebook() for the GUI, and license() for information.        |
----------------------------------------------------------------------

sage: G = DirichletGroup(525, CyclotomicField(4)); G
Group of Dirichlet characters of modulus 525 over Cyclotomic Field of order
4 and degree 2

sage: X = G.list(); X
[[1, 1, 1],
 [-1, 1, 1],
 [1, zeta4, 1],
 [-1, zeta4, 1],
 [1, -1, 1],
 [-1, -1, 1],
 [1, -zeta4, 1],
 [-1, -zeta4, 1],
 [1, 1, -1],
 [-1, 1, -1],
 [1, zeta4, -1],
 [-1, zeta4, -1],
 [1, -1, -1],
 [-1, -1, -1],
 [1, -zeta4, -1],
 [-1, -zeta4, -1]]

sage: Y = X[15]; Y.conductor(); Y.order()
105
4

sage: time M = ModularSymbols(Y, 3, sign=1)
CPU times: user 113.82 s, sys: 0.18 s, total: 114.01 s Wall time: 114.02

sage: M
Modular Symbols space of dimension 160 and level 525, weight 3, character
[-1, -zeta4, -1], sign 1, over Cyclotomic Field of order 4 and degree 2

sage: time S = M.cuspidal_subspace()
CPU times: user 7.04 s, sys: 0.21 s, total: 7.24 s Wall time: 7.24

sage: S
Modular Symbols subspace of dimension 148 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2

sage: time N = S.new_subspace()
CPU times: user 65.15 s, sys: 0.79 s, total: 65.94 s Wall time: 65.95
```

```
sage: N
Modular Symbols subspace of dimension 92 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2

sage: time D = N.decomposition()
CPU times: user 4195.14 s, sys: 58.98 s, total: 4254.12 s Wall time: 4252.91

sage: D
[
Modular Symbols subspace of dimension 2 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 2 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 4 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 4 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 4 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 4 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 8 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 8 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 16 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2,
Modular Symbols subspace of dimension 40 of Modular Symbols space of
dimension 160 and level 525, weight 3, character [-1, -zeta4, -1], sign 1,
over Cyclotomic Field of order 4 and degree 2
]

sage: time f = D[4].q_eigenform(98)
CPU times: user 378.18 s, sys: 1.32 s, total: 379.51 s Wall time: 379.52

sage: f
q + (1/62*zeta4*alpha^3 + (-3/31*zeta4 + 3/31)*alpha^2 + (-43/62)*alpha +
27/31*zeta4 + 27/31)*q^2 + (1/124*zeta4*alpha^3 + (-3/62*zeta4 +
3/62)*alpha^2 + (-105/124)*alpha + 27/62*zeta4 + 27/62)*q^3 - zeta4*q^4 +
((-1/62*zeta4 + 1/62)*alpha^3 + (-55/124)*alpha^2 + (105/62*zeta4 +
105/62)*alpha - 1239/124*zeta4)*q^6 + (1/124*alpha^3 + (25/124*zeta4 -
37/124)*alpha^2 + (105/124*zeta4 + 2)*alpha - 1201/124*zeta4 - 845/124)*q^7
+ (5/62*alpha^3 + (-15/31*zeta4 - 15/31)*alpha^2 + 215/62*zeta4*alpha -
135/31*zeta4 + 135/31)*q^8 + ((-1/62*zeta4 + 1/62)*alpha^3 + (-6/31)*alpha^2
+ (105/62*zeta4 + 105/62)*alpha - 333/31*zeta4)*q^9 + (1/124*alpha^3 +
(-3/62*zeta4 - 3/62)*alpha^2 + 105/124*zeta4*alpha - 27/62*zeta4 +
27/62)*q^12 + (1/62*zeta4*alpha^3 + (-3/31*zeta4 + 3/31)*alpha^2 +
```

```
(-105/62)*alpha + 89/31*zeta4 + 89/31)*q^13 + ((3/124*zeta4 - 3/124)*alpha^3
+ (1/4*zeta4 + 9/31)*alpha^2 + (-439/124*zeta4 - 191/124)*alpha +
267/31*zeta4 - 33/4)*q^14 + 11*q^16 + (18*zeta4 - 18)*q^17 + (5/62*alpha^3 +
(1/62*zeta4 + 1/62)*alpha^2 + (-33/62*zeta4)*alpha + 753/62*zeta4 -
753/62)*q^18 + ((-4/31*zeta4 - 4/31)*alpha^3 + 48/31*zeta4*alpha^2 +
(-172/31*zeta4 + 172/31)*alpha - 432/31)*q^19 + ((-15/124*zeta4 +
13/124)*alpha^3 + (3/31*zeta4 - 53/62)*alpha^2 + (249/124*zeta4 +
459/124)*alpha + 267/62*zeta4 - 306/31)*q^21 + (2/31*alpha^3 +
(-12/31*zeta4 - 12/31)*alpha^2 + 86/31*zeta4*alpha - 108/31*zeta4 +
108/31)*q^23 + ((-5/62*zeta4 - 5/62)*alpha^3 + 275/124*zeta4*alpha^2 +
(-525/62*zeta4 + 525/62)*alpha - 6195/124)*q^24 + ((-1/2)*alpha^2 + (2*zeta4
+ 2)*alpha - 33/2*zeta4)*q^26 + (1/124*alpha^3 + (-3/62*zeta4 -
3/62)*alpha^2 + 105/124*zeta4*alpha + 1089/62*zeta4 - 1089/62)*q^27 +
((-1/124*zeta4)*alpha^3 + (37/124*zeta4 + 25/124)*alpha^2 + (-2*zeta4 +
105/124)*alpha + 845/124*zeta4 - 1201/124)*q^28 + ((3/62*zeta4 -
3/62)*alpha^3 + 18/31*alpha^2 + (-315/62*zeta4 - 315/62)*alpha +
534/31*zeta4)*q^29 + ((-5/31*zeta4 + 5/31)*alpha^3 + (-60/31)*alpha^2 +
(215/31*zeta4 + 215/31)*alpha - 540/31*zeta4)*q^31 + ((-9/62*zeta4)*alpha^3
+ (27/31*zeta4 - 27/31)*alpha^2 + 387/62*alpha - 243/31*zeta4 - 243/31)*q^32
+ ((-9/31*zeta4 - 9/31)*alpha^3 + 108/31*zeta4*alpha^2 + (-387/31*zeta4 +
387/31)*alpha - 972/31)*q^34 + ((-1/62*zeta4 - 1/62)*alpha^3 +
6/31*zeta4*alpha^2 + (-105/62*zeta4 + 105/62)*alpha - 333/31)*q^36 +
((1/2*zeta4 - 1/2)*alpha^2 + 4*alpha - 33/2*zeta4 - 33/2)*q^37 +
(-24*zeta4 - 24)*q^38 + ((-1/62*zeta4 + 1/62)*alpha^3 + (-6/31)*alpha^2 +
(105/62*zeta4 + 105/62)*alpha - 612/31*zeta4)*q^39 + ((-3)*alpha^2 +
(12*zeta4 + 12)*alpha - 99*zeta4)*q^41 + ((-7/62*zeta4 + 3/62)*alpha^3 +
(17/124*zeta4 - 89/124)*alpha^2 + (315/62*zeta4 + 177/62)*alpha -
3405/124*zeta4 + 3939/124)*q^42 + ((-2*zeta4 - 2)*alpha^2 + 16*zeta4*alpha -
66*zeta4 + 66)*q^43 + 12*q^46 + (-12*zeta4 + 12)*q^47 +
(11/124*zeta4*alpha^3 + (-33/62*zeta4 + 33/62)*alpha^2 + (-1155/124)*alpha +
297/62*zeta4 + 297/62)*q^48 + ((-7/31*zeta4 - 7/31)*alpha^3 +
84/31*zeta4*alpha^2 + (-301/31*zeta4 + 301/31)*alpha - 35*zeta4 -
756/31)*q^49 + ((-9/62*zeta4 - 9/62)*alpha^3 + 54/31*zeta4*alpha^2 +
(-945/62*zeta4 + 945/62)*alpha - 486/31)*q^51 + (1/62*alpha^3 +
(-3/31*zeta4 - 3/31)*alpha^2 + 105/62*zeta4*alpha - 89/31*zeta4 +
89/31)*q^52 + ((-18/31)*alpha^3 + (108/31*zeta4 + 108/31)*alpha^2 +
(-774/31*zeta4)*alpha + 972/31*zeta4 - 972/31)*q^53 + ((-19/62*zeta4 -
19/62)*alpha^3 + 487/124*zeta4*alpha^2 + (-879/62*zeta4 + 879/62)*alpha -
5127/124)*q^54 + ((15/124*zeta4 + 15/124)*alpha^3 + (-45/31*zeta4 +
5/4)*alpha^2 + (955/124*zeta4 - 2195/124)*alpha + 165/4*zeta4 +
1335/31)*q^56 + (8/31*zeta4*alpha^3 + (-110/31*zeta4 + 110/31)*alpha^2 +
(-840/31)*alpha + 2478/31*zeta4 + 2478/31)*q^57 + ((-3/2*zeta4 -
3/2)*alpha^2 + 12*zeta4*alpha - 99/2*zeta4 + 99/2)*q^58 + (5*zeta4*alpha^2 +
(-20*zeta4 + 20)*alpha - 165)*q^59 + ((-15/31*zeta4 + 15/31)*alpha^3 +
(-180/31)*alpha^2 + (645/31*zeta4 + 645/31)*alpha - 1620/31*zeta4)*q^61 +
(-30*zeta4 + 30)*q^62 + ((-5/124*zeta4 - 14/31)*alpha^3 + (521/124*zeta4 +
461/124)*alpha^2 + (-912/31*zeta4 + 525/124)*alpha + 8985/124*zeta4 -
7293/124)*q^63 - 71*zeta4*q^64 + ((3*zeta4 - 3)*alpha^2 + 24*alpha -
99*zeta4 - 99)*q^67 + (18*zeta4 + 18)*q^68 + ((-2/31*zeta4 - 2/31)*alpha^3 +
55/31*zeta4*alpha^2 + (-210/31*zeta4 + 210/31)*alpha - 1239/31)*q^69 +
((15/62*zeta4 + 15/62)*alpha^3 + (-90/31*zeta4)*alpha^2 + (1575/62*zeta4 -
1575/62)*alpha + 2670/31)*q^71 + ((-25/62*zeta4)*alpha^3 + (-5/62*zeta4 +
5/62)*alpha^2 + (-165/62)*alpha + 3765/62*zeta4 + 3765/62)*q^72 +
((-19/62*zeta4)*alpha^3 + (57/31*zeta4 - 57/31)*alpha^2 + 1995/62*alpha -
1691/31*zeta4 - 1691/31)*q^73 + ((3/62*zeta4 - 3/62)*alpha^3 + 18/31*alpha^2
+ (-315/62*zeta4 - 315/62)*alpha + 534/31*zeta4)*q^74 + ((4/31*zeta4 -
4/31)*alpha^3 + 48/31*alpha^2 + (-172/31*zeta4 - 172/31)*alpha +
```

```
432/31*zeta4)*q^76 + (7/31*alpha^3 + (-53/62*zeta4 - 53/62)*alpha^2 +
177/31*zeta4*alpha + 267/62*zeta4 - 267/62)*q^78 + 50*zeta4*q^79 +
((-5/31*zeta4 - 5/31)*alpha^3 + 60/31*zeta4*alpha^2 + (-525/31*zeta4 +
525/31)*alpha - 819/31)*q^81 + ((-9/31)*alpha^3 + (54/31*zeta4 +
54/31)*alpha^2 + (-945/31*zeta4)*alpha + 1602/31*zeta4 - 1602/31)*q^82 +
(78*zeta4 + 78)*q^83 + ((-13/124*zeta4 - 15/124)*alpha^3 + (53/62*zeta4 +
3/31)*alpha^2 + (-459/124*zeta4 + 249/124)*alpha + 306/31*zeta4 +
267/62)*q^84 + ((-6/31*zeta4 - 6/31)*alpha^3 + 72/31*zeta4*alpha^2 +
(-630/31*zeta4 + 630/31)*alpha - 2136/31)*q^86 + (3/31*alpha^3 +
(-18/31*zeta4 - 18/31)*alpha^2 + 315/31*zeta4*alpha - 1836/31*zeta4 +
1836/31)*q^87 + ((-5*zeta4)*alpha^2 + (20*zeta4 - 20)*alpha + 165)*q^89 +
((-7/31*zeta4 + 7/31)*alpha^3 + (-84/31)*alpha^2 + (301/31*zeta4 +
301/31)*alpha - 756/31*zeta4 - 14)*q^91 + ((-2/31*zeta4)*alpha^3 +
(12/31*zeta4 - 12/31)*alpha^2 + 86/31*alpha - 108/31*zeta4 - 108/31)*q^92 +
((-10/31)*alpha^3 + (275/62*zeta4 + 275/62)*alpha^2 + (-1050/31*zeta4)*alpha
+ 6195/62*zeta4 - 6195/62)*q^93 + ((6/31*zeta4 + 6/31)*alpha^3 +
(-72/31*zeta4)*alpha^2 + (258/31*zeta4 - 258/31)*alpha + 648/31)*q^94 +
((9/62*zeta4 - 9/62)*alpha^3 + 495/124*alpha^2 + (-945/62*zeta4 -
945/62)*alpha + 11151/124*zeta4)*q^96 + ((-19/62)*alpha^3 + (57/31*zeta4 +
57/31)*alpha^2 + (-1995/62*zeta4)*alpha + 1691/31*zeta4 - 1691/31)*q^97 +
O(q^98)

sage: parent(f)
Power Series Ring in q over Univariate Quotient Polynomial Ring in alpha
over Cyclotomic Field of order 4 and degree 2 with modulus
x^4 + (-8*zeta4 - 8)*x^3 + 98*zeta4*x^2 + (-264*zeta4 + 264)*x - 1425
```

Acknowledgements:

We are very grateful to Nick Katz, who communicated many key ideas [7], and to William Stein, who wrote Sage code for commands used in the Appendix and provided us with hours of computing time with Magma and Sage on his machine. We are also grateful to Scott Ahlgren, Greg Anderson, Tim Kilbourn, and Daqing Wan for helpful comments and references.

References

[1] H. T. Choi and R. J. Evans, Congruences for sums of powers of Kloosterman sums, International Journal of Number Theory **3** (2007), 105–117.

[2] R. J. Evans, Twisted hyper-Kloosterman sums over finite rings of integers, Number Theory for the Millennium, Proc. Millennial Conf. Number Theory (Urbana, IL, May 21-26, 2000), Vol. **I**, pp. 429–448, M. A. Bennett et al. eds., A. K. Peters, Natick, MA, 2002.

[3] L. Fu and D. Wan, L–functions for symmetric products of Kloosterman sums, J. Reine Angew. Math. **589** (2005), 79–103

[4] 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.

[5] H.Iwaniec, Topics in Classical Automorphic Forms, Graduate studies in Mathematics, v. **17**, AMS, Providence, R.I. 1997.

[6] N. M. Katz, Gauss sums, Kloosterman sums, and Monodromy groups, Annals of Mathematics Studies, Princeton University Press, Princeton, N.J., 1988.

[7] N. M. Katz, Email correspondence, 2005-2006.

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

[9] 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.

[10] W. Stein, The Modular Forms Database, [`http://sage.math.washington.edu/`].

[11] Stein, William, *Sage: Open Source Mathematical Software (Version 2.11)*, The Sage Group, 2008, [`http://www.sagemath.org`].