Canad. Math. Bull. Vol. **46** (3), 2003 pp. 344–355

Gauss and Eisenstein Sums of Order Twelve

S. Gurak

Abstract. Let $q = p^r$ with p an odd prime, and $\mathbf{F}_q$ denote the finite field of q elements. Let $\mathrm{Tr}\colon \mathbf{F}_q \to \mathbf{F}_p$ be the usual trace map and set $\zeta_p = \exp(2\pi i/p)$. For any positive integer e, define the (modified) Gauss sum $g_r(e)$ by

$$g_r(e) = \sum_{x\in\mathbf{F}_q} \zeta_p^{\mathrm{Tr}\, x^e}$$

Recently, Evans gave an elegant determination of $g_1(12)$ in terms of $g_1(3)$, $g_1(4)$ and $g_1(6)$ which resolved a sign ambiguity present in a previous evaluation. Here I generalize Evans' result to give a complete determination of the sum $g_r(12)$.

1 Introduction

Let $q = p^r$ with p an odd prime, and $\mathbf{F}_q$ denote the finite field of q elements. Fix a generator γ for the multiplicative group $\mathbf{F}_q^*$ of $\mathbf{F}_q$. Then $G = \gamma^{(q-1)/(p-1)}$ generates $\mathbf{F}_p^*$. Let $\mathrm{Tr}\colon \mathbf{F}_q \to \mathbf{F}_p$ be the usual trace map and set $\zeta_m = \exp(2\pi i/m)$ for any positive integer m. For a character χ of $\mathbf{F}_q^*$ define the Gauss sum $G_r(\chi)$ by

$$G_r(\chi) = \sum_{x\in\mathbf{F}_q^*} \chi(x)\zeta_p^{\mathrm{Tr}\, x} \tag{1}$$

which satisfies

$$G_r(\chi)G_r(\chi^{-1}) = \chi(-1)p^r \quad \text{for } \chi \neq 1 \tag{2}$$

(We will write $G(\chi)$ for $G_1(\chi)$.) For $r > 1$, the value of $G_r(\chi)$ can be expressed in terms of the Eisenstein sums

$$E_r(\chi) = \sum_{x\in\mathbf{F}_q^*,\, \mathrm{Tr}\, x=1} \chi(x); \tag{3}$$

namely (chiefly, Theorem 12.1.1 in [2]),

$$G_r(\chi) = \begin{cases} E_r(\chi)G(\chi^*) & \text{if } \chi^* \text{ is nontrivial} \\ -pE_r(\chi) & \text{if } \chi^* \text{ is trivial,} \end{cases} \tag{4}$$

where χ^* denotes the restriction of χ to $\mathbf{F}_p^*$.

Received by the editors October 15, 2001; revised January 2, 2002.
AMS subject classification: 11L05, 11T24.

When χ is nontrivial, the Davenport-Hasse Theorem on lifted Gauss sums can be applied to give a more refined result (chiefly, Theorem 12.1.3 in [2] or see [6]). Namely, if χ has order $k > 1$ and l is the least positive integer such that $k | p^l - 1$, then $l | r$ and χ is the lift of some character ψ on $\mathbf{F}_{p^l}^*$ (that is; $\chi = \psi \circ N_{\mathbf{F}_{p^r}/\mathbf{F}_{p^l}}$, where N is the relative norm map) and for $s = r/l$,

$$(5) \qquad \frac{E_r(\chi)}{E_l^s(\psi)} = \begin{cases} p^{s-1} & \text{if } \psi^* \text{ is trivial} \\ (-1)^s G^s(\chi^*)/p & \text{if } \psi^* \text{ is nontrivial and } \chi^* \text{ trivial} \\ (-1)^{s-1} G^s(\psi^*)/G(\psi^{s*}) & \text{if } \chi^* \text{ is nontrivial} \end{cases}$$

For any positive integer e, define the modified Gauss sum $g_r(e)$ by

$$(6) \qquad g_r(e) = \sum_{x \in \mathbf{F}_q} \zeta_p^{\mathrm{Tr}\, x^e}$$

(We write $g(e)$ for $g_1(e)$.) The modified Gauss sums are intimately related to the Gauss sums $G_r(\chi)$ for characters χ of order dividing e. Normalizing such characters χ so $\chi_j(\gamma) = \zeta_e^j$ for $1 \le j \le e$, one has

$$(7) \qquad g_r(e) = \sum_{i=1}^{e-1} G_r(\chi_i).$$

For small values of e, the sums $E_r(\chi)$ and $g_r(e)$ are known or easily derived using (4) and (7). (particularly for $e|6$ or $e|8$.) The modern treatment of Eisenstein sums $E_r(\chi)$ stems for the seminal work of Williams, Hardy and Spearman [6], in which they have tabulated the values of $E_r(\chi)$ for $e = 2, 3, 4, 6, 8$. See also [2], where Berndt, Evans and Williams give the value of $g(e)$ for $e = 2, 3, 4, 6, 8, 12$, and of $g_r(e)$ for $e = 2, 3, 4$, leaving the computation of $g_r(6)$ and $g_r(8)$ as exercises. Recently, Evans [3] gave an elegant determination of $g(12)$ in terms of $g(3)$, $g(4)$ and $g(6)$ which resolved a sign ambiguity present in a previous evaluation. Here I generalize Evans' result to give a complete determination of the modified Gauss sum $g_r(12)$.

2 Eisenstein Sums of Order 12

Before giving the evaluation of the Eisenstein sums $E_r(\chi)$ for χ having order 12, some comments concerning Jacobi sums are in order. Let χ and ψ be characters of $\mathbf{F}_q^*$, where $q = p^r$. The Jacobi sum $J_r(\chi, \psi)$ is defined by

$$(8) \qquad J_r(\chi, \psi) = \sum_{x \in \mathbf{F}_q^* - \{1\}} \chi(x)\psi(1-x),$$

and satisfies

$$(9) \qquad J_r(\chi, \psi) = \frac{G_r(\chi)G_r(\psi)}{G_r(\chi\psi)}$$

and

$$J_r(\chi,\psi) = \psi(-1)J_r(\chi^{-1}\psi^{-1},\psi) = \chi(-1)J_r(\chi^{-1}\psi^{-1},\chi) \tag{10}$$

if χ, ψ and $\chi\psi$ are all non-trivial (chiefly Theorem 2.1.4 and 2.1.5 in [2]). (We write as before $J(\chi,\psi)$ for $J_1(\chi\cdot\psi)$.) The explicit evaluation of $J(\chi,\psi)$ has been tabulated by Berndt, Evans and Williams [2] for characters χ and ψ of $\mathbf{F}_p^*$ of order dividing 12. In particular, if ψ is the normalized character of $\mathbf{F}_q^*$ satisfying $\psi(G) = \zeta_{12}$, then the Jacobi sums $J(\psi^m,\chi^n)$, with m or n relatively prime to 12, may be determined using (10) from the values $J(\psi,\psi^n)$ given below.

For a prime $p \equiv 1 \pmod 3$, write $4p = r_3^2 + 3s_3^2$ with r_3 and s_3 uniquely determined by the conditions $r_3 \equiv 1 \pmod 3$, $s_3 \equiv 0 \pmod 3$ and $3s_3 \equiv (2G^{(p-1)/3} + 1)r_3 \pmod p$. Put $Z = \operatorname{ind}_G 2$ and $T = \operatorname{ind}_G 3$. Then the quantity

$$a_3 + ib_3\sqrt{3} = \zeta_3^{2Z}(r_3 + i\sqrt{3}s_3)/2 \tag{11}$$

satisfies $a_3^2 + 3b_3^2 = p$ with $a_3 \equiv -1 \pmod 3$ and $3b_3 \equiv (2G^{(p-1)/3} + 1)a_3 \pmod p$. Similarly, for a prime $p \equiv 1 \pmod 4$, write $p = a_4^2 + b_4^2$ with a_4 and b_4 uniquely determined by the conditions $a_4 \equiv -(-1)^Z \pmod 4$ and $b_4 \equiv a_4 G^{(p-1)/4} \pmod p$. For a prime $p \equiv 1 \pmod{12}$, set

$$a_{12} + ib_{12} = (-1)^{T/2+Z}(a_4 + ib_4). \tag{12}$$

(Note that 3 is a quadratic residue modulo p here so T is even.) If c_{12} is the unique 4-th root of unity determined by

$$c_{12} = \begin{cases} \pm 1 \text{ with } c_{12} \equiv -a_4 \pmod 3 & \text{if } 3|b_4 \\ \pm i \text{ with } c_{12} \equiv -ib_4 \pmod 3 & \text{if } 3|a_4, \end{cases} \tag{13}$$

then

$$a_{12} + ib_{12} = c_{12}^2(a_4 + ib_4) \tag{14}$$

from (12) and Lemma 3.5.1 in [2].

In terms of the quantities defined above, we have (chiefly [2, p. 116])

Proposition 1 *The values $J(\psi,\psi^n)$ $(0 \le n \le 6)$ are*

$$\begin{aligned}
&J(\psi,\psi^0) = 0\\
&J(\psi,\psi) = c_{12}^2\zeta_6^{-Z}(a_4 + ib_4)\\
&J(\psi,\psi^2) = \bar{c}_{12}\zeta_3^{-Z}(r_3 + i\sqrt{3}s_3)/2\\
&J(\psi,\psi^3) = (-1)^Z\bar{c}_{12}(a_4 + ib_4)\\
&J(\psi,\psi^4) = (r_3 + i\sqrt{3}s_3)/2\\
&J(\psi,\psi^5) = (-1)^{T/2}(a_4 + ib_4)\\
&J(\psi,\psi^6) = c_{12}^2(a_4 + ib_4)
\end{aligned}$$

I am now ready to give the values of the Eisenstein sums $E_r(\chi)$ of order 12, where χ is the (normalized) character of $\mathbf{F}_q^*$ satisfying $\chi(\gamma) = \zeta_{12}$, noting that r is even if $p \not\equiv 1 \pmod{12}$. The results given for $p \equiv 5 \pmod{12}$ agree with the evaluation of the Eisenstein sums of order 12 for $\mathbf{F}_{p^2}$ appearing in [2, p. 433].

Theorem 1 *The Eisenstein sum $E_r(\chi)$ is explicitly given as follows:*

(a) *If $p \equiv 1 \pmod{12}$, say $p = 12k+1$, then $E_r(\chi) = \epsilon p^\alpha \pi^\beta \lambda^\delta$ where $\pi = a_4 + ib_4$ and $\lambda = (r_3 + i\sqrt{3}s_3)/2$, with*

$$\epsilon = \begin{cases} 1 & \text{if } r \equiv 0, 1, 5 \pmod{12} \\ -1 & \text{if } r \equiv 4, 8 \pmod{12} \\ (-1)^k & \text{if } r \equiv 7, 11 \pmod{12} \\ (-1)^k c_{12} & \text{if } r \equiv 3 \pmod{12} \\ -(-1)^{T/2} & \text{if } r \equiv 6 \pmod{12} \\ \bar{c}_{12} & \text{if } r \equiv 9 \pmod{12} \\ -(-1)^{T/2}\zeta_6^{2Z} & \text{if } r \equiv 2 \pmod{12} \\ -(-1)^{T/2}\zeta_6^{4Z} & \text{if } r \equiv 10 \pmod{12}, \end{cases}$$

$$\alpha = [(r-1)/12],$$

$$\beta = \begin{cases} r/2 & \text{if } r \equiv 0 \pmod{2} \\ (r-1)/2 & \text{if } r \equiv 1, 3, 5 \pmod{12} \\ (r+1)/2 & \text{if } r \equiv 7, 9, 11 \pmod{12} \end{cases}$$

and

$$\delta = \begin{cases} r/3 & \text{if } r \equiv 0 \pmod{3} \\ (r-1)/3 & \text{if } r \equiv 1, 4, 7 \pmod{12} \\ (r-2)/3 & \text{if } r \equiv 2 \pmod{12} \\ (r+1)/3 & \text{if } r \equiv 5, 8, 11 \pmod{12} \\ (r+2)/3 & \text{if } r \equiv 10 \pmod{12}. \end{cases}$$

(b) *If $p \equiv 5 \pmod{12}$, say $p = 12k+5$, then*

$$E_r(\chi) = \begin{cases} -(-1)^{k+(r-2)/4}\beta i p^{(r-2)/4}\pi^{r/2} & \text{if } r \equiv 2 \pmod{4} \\ (-1)^{r/4} p^{r/4-1}\pi^{r/2} & \text{if } r \equiv 0 \pmod{4}, \end{cases}$$

where $\beta = \pm 1$ satisfies $\beta \equiv a_4 b_4 \pmod{3}$.

(c) *If $p \equiv 7 \pmod{12}$, say $p = 12k+7$, then*

$$E_r(\chi) = \begin{cases} -(-1)^{r(k+1)/2} p^{(r-2)/3}\lambda^{(r+1)/3} & \text{if } r \equiv 2 \pmod{6} \\ -(-1)^{r(k+1)/2} p^{(r-1)/3}\lambda^{(r-1)/3} & \text{if } r \equiv 4 \pmod{6} \\ (-1)^{r(k+1)/2} p^{r/3-1}\lambda^{r/3} & \text{if } r \equiv 0 \pmod{6}. \end{cases}$$

(d) *If* $p \equiv 11 \pmod{12}$, *say* $p = 12k + 11$, *then* $E_r(\chi) = (-1)^{kr/2} p^{r/2-1}$.

Proof (a) If $p = 12k + 1$ then χ is the lift of the character ψ of $\mathbf{F}_p$ satisfying $\psi(G) = \zeta_{12}$. In addition, $\chi(G) = \zeta_{12}^{1+p+\cdots+p^{r-1}} = \zeta_{12}^r$ so $\chi^* = \psi^r$. Thus, by (5)

$$E_r(\chi) = \begin{cases} G^r(\psi)/p & \text{if } r \equiv 0 \pmod{12} \\ (-1)^{r-1} G^r(\psi)/G(\psi^r) & \text{if } r \not\equiv 0 \pmod{12} \end{cases} \tag{15}$$

since $E_1(\psi) = 1$. From Proposition 1 and (9), one finds

$$G^2(\psi)/G(\psi^2) = J(\psi,\psi) = c_{12}^2 \zeta_6^{-Z} \pi,$$
$$G^3(\psi)/G(\psi^3) = J(\psi,\psi)J(\psi,\psi^2) = (-1)^Z c_{12} \pi\lambda,$$
$$G^4(\psi)/G(\psi^4) = J(\psi,\psi)J(\psi,\psi^2)J(\psi,\psi^3) = \pi^2\lambda,$$
$$G^5(\psi)/G(\psi^5) = J(\psi,\psi)J(\psi,\psi^2)J(\psi,\psi^3)J(\psi,\psi^4) = \pi^2\lambda^2, \quad \text{and}$$
$$G^6(\psi) = (-1)^{T/2}\sqrt{p}\,\pi^3\lambda^2.$$

Then for $r \equiv r' \pmod{12}$ with $0 < r' \le 6$, $E_r(\chi)$ equals

$$(-1)^{r-1} G^{r'}(\psi) G^{r-r'}(\psi)/G(\psi^{r'}) = (-1)^{r-1}(p\pi^6\lambda^4)^{(r-r')/12} G^r(\psi)/G(\psi^r)$$

which yields the desired forms for $E_r(\chi)$ when $r \equiv 1, 2, 3, 4, 5$ or $6 \pmod{12}$. For $r \equiv r' \pmod{12}$ with $6 < r' < 12$, it follows from (2) and (15) that

$$E_r(\chi) = \frac{(-1)^{r-1} G^{r+(12-r')}(\psi)}{G^{12-r'}(\psi) G(\psi^{r'})} = \frac{(-1)^{kr+r-1} G(\psi^{12-r'})}{p G^{12-r'}(\psi)} (p\pi^6\lambda^4)^{(r-r')/12+1}$$

which yields the desired expressions for $E_r(\chi)$ when $r \equiv 7, 8, 9, 10$ and $11 \pmod{12}$. Finally, if $r \equiv 0 \pmod{12}$ then $E_r(\chi) = p^{-1}(p\pi^6\lambda^4)^{r/6} = p^{r/12-1}\pi^{r/2}\lambda^{r/3}$ from (15).

(b) If $p = 12k + 5$ then χ is the lift of the character ψ of $\mathbf{F}_{p^2}$ satisfying

$$\psi(\gamma^{1+p^2+\cdots+p^{2r-2}}) = \zeta_{12} \text{ with } \psi(G) = \zeta_{12}^{1+p} = -1 \text{ and } \chi(G) = \zeta_{12}^{(q-1)/(p-1)}$$

so ψ^* is quadratic and $\chi^* = (\psi^*)^{r/2}$. As $l = 2$ in (5) and $G(\psi^*) = \sqrt{p}$,

$$E_r(\chi) = \begin{cases} E_2^{r/2}(\psi) p^{(r-2)/4} & \text{if } r \equiv 2 \pmod 4 \\ E_2^{r/2}(\psi) p^{r/4-1} & \text{if } r \equiv 0 \pmod 4. \end{cases}$$

Since $E_2(\psi) = -(-1)^k i\beta(a_4 + ib_4)$ here from Proposition 1 in [4] (see also [2, p. 433]), where $\beta = \pm 1$ satisfies $\beta \equiv a_4 b_4 \pmod 3$, one finds that $E_r(\chi)$ equals

$$-(-1)^k i^{r/2} \beta p^{(r-2)/4} \pi^{r/2}$$

if $r \equiv 2 \pmod 4$ or $(-1)^{r/4}p^{r/4-1}\pi^{r/2}$ if $r \equiv 0 \pmod 4$. This yields (b) since $i^{r/2} = (-1)^{(r-2)/4}i$ when $r \equiv 2 \pmod 4$.

(c) If $p = 12k + 7$ then χ is the lift of the character ψ of $\mathbf{F}_{p^2}$ satisfying

$$\psi(\gamma^{1+p^2+\cdots+p^{r-2}}) = \zeta_{12} \text{ with } \psi(G) = \zeta_{12}^{1+p} = \zeta_{12}^{8} \text{ and } \chi(G) = \zeta_{12}^{(q-1)/(p-1)} = \zeta_{12}^{4r}$$

so ψ^* is cubic and $\chi^* = (\psi^*)^{r/2}$ in (5). Thus

$$E_r(\chi) = \begin{cases} -(-1)^{r/2}G^{r/2-1}(\psi^*)E_2^{r/2}(\psi) & \text{if } r \equiv 2 \pmod 6 \\ -(-1)^{r/2}G^{r/2+1}(\psi^*)E_2^{r/2}(\psi)/p & \text{if } r \equiv 4 \pmod 6 \\ (-1)^{r/2}G^{r/2}(\psi^*)E_2^{r/2}(\psi)/p & \text{if } r \equiv 0 \pmod 6. \end{cases}$$

Setting $G_3 = G(\psi^{2*})$ and $\hat{G}_3 = G(\psi^*)$, and noting that $G_3^3 = p\lambda$, $\hat{G}_3^3 = p\bar{\lambda}$ and $E_2(\psi) = (-1)^k\lambda$ from [1, p. 391] (see also Proposition 1 in [4] where the sign of b_3 should be '+'), one finds that if $r \equiv 2 \pmod 6$ then

$$\begin{aligned} E_r(\chi) &= -(-1)^{r/2}\hat{G}_3^{r/2-1}\big((-1)^k\lambda\big)^{r/2} = -(-1)^{r(k+1)/2}p^{(r-2)/6}\bar{\lambda}^{(r-2)/6}\lambda^{r/2} \\ &= -(-1)^{r(k+1)/2}p^{(r-2)/3}\lambda^{(r+1)/3}. \end{aligned}$$

Similarly one finds the desired expressions for $E_r(\chi)$ when $r \equiv 0$ and $4 \pmod 6$.

(d) If $p = 12k + 11$ then $E_r(\chi) = (-1)^{kr/2}p^{r/2-1}$ by Theorem 12.1.6 in [2].

3 Gauss Sums Over $\mathbf{F}_q$ of Order Twelve

Before giving the evaluation of the modified Gauss sum $g_r(12)$, some comments about $g_r(e)$ and the classical Gauss sums $G(\psi)$ for ψ of order $e = 2, 3, 4$ and 6 are in order. Assume, for convenience, that ψ is the (normalized) character satisfying $\psi(G) = \zeta_e$. For $e = 2$, $G(\psi) = i^*\sqrt{p}$ where $i^* = 1$ or i according as $p \equiv 1$ or $3 \pmod 4$. Also,

$$\text{(16)} \qquad g_r(2) = \begin{cases} -(-1)^{(p-1)r/4}p^{r/2} & \text{if } r \equiv 0 \pmod 2 \\ i^*(-1)^{(p-1)(r-1)/4}p^{(r-1)/2}\sqrt{p} & \text{if } r \equiv 1 \pmod 2 \end{cases}$$

from Theorem 12.10.2 in [2]. For $e = 3$, the modified Gauss sum $g = g(3)$ satisfies $x^3 - 3px - pr_3 = 0$ with r_3 and s_3 as before. The correct choice of root for $g(3)$ was determined by Matthews [5] and is described in [2]. In terms of $g(3)$, one sees [4, p. 5] that

$$\text{(17)} \qquad G_3 = G(\psi) = \frac{1}{2}\big(g + (g - g')/(i\sqrt{3})\big)$$

and

$$\text{(18)} \qquad \hat{G}_3 = G(\psi^2) = \frac{1}{2}\big(g - (g'' - g')/(i\sqrt{3})\big),$$

https://doi.org/10.4153/CMB-2003-036-9 Published online by Cambridge University Press

where the conjugates g' and g'' of g are given by

$$g' = \left(g^2 - 2p - \frac{1}{2}(s_3 + r_3)g\right) \Big/ s_3 \quad \text{and} \quad g'' = \left(2p - g^2 - \frac{1}{2}(s_3 - r_3)g\right) \Big/ s_3.$$

In particular (chiefly, Theorem 12.10.3 in [2]), if $p \equiv 1 \pmod 3$,

(19)
$$g_r(3) = \begin{cases} -(-1)^r p^{r/3} V_{r/3} & \text{if } r \equiv 0 \pmod 3 \\ -(-1)^r p^{(r-1)/3}(gV_{(r-1)/3} + (g'' - g')U_{(r-1)/3})/2 & \text{if } r \equiv 1 \pmod 3 \\ -(-1)^r p^{(r-2)/3}(gV_{(r+1)/3} - (g'' - g')U_{(r+1)/3})/2 & \text{if } r \equiv 2 \pmod 3 \end{cases}$$

whereas if $p \equiv 2 \pmod 3$

$$g_r(3) = -2(-1)^{r/2} p^{r/2} \text{or } 0 \quad \text{as } r \text{ is even or odd.} \tag{20}$$

Here V_n and U_n are Lucas sequences given by

$$V_n = \lambda^n + \bar{\lambda}^n, \quad U_n = \frac{1}{i\sqrt{3}}(\lambda^n - \bar{\lambda}^n) \tag{21}$$

for $n \geq 0$. For later use we introduce the related sequences

$$V_{j,n} = \zeta_6^{-j}\lambda^n + \zeta_6^j\bar{\lambda}^n, U_{j,n} = \frac{1}{i\sqrt{3}}(\zeta_6^{-j}\lambda^n - \zeta_6^j\bar{\lambda}^n) \quad (n \geq 0)$$

for any integer j, noting that $V_{j,n} = V_n$ and $U_{j,n} = U_n$ when $6|j$.

For $e = 6$ one finds from Lemma 4.1.4 in [2] that

$$G(\psi) = \frac{i*}{\sqrt{p}}\zeta_6^{4Z}\lambda\hat{G}_3 \quad \text{and} \quad G(\psi^{-1}) = \frac{i*}{\sqrt{p}}\zeta_6^{2Z}\bar{\lambda}G_3 \tag{22}$$

using the fact that $G_3^2 = \lambda\hat{G}_3$. For χ, the (normalized) character of $\mathbf{F}_q^*$ satisfying $\chi(\gamma) = \zeta_6$, one computes $G_r(\chi) + G_r(\chi^5)$ for $p \equiv 1 \pmod 6$ using (4), (22) and Theorem 12.6.1 in [2].

Proposition 2 *The value of $G_r(\chi) + G_r(\chi^5)$ above is given by*

$$\begin{array}{ll} -(-1)^{kr/2}p^{r/6}(\lambda^{2r/3} + \bar{\lambda}^{2r/3}) & \text{if } r \equiv 0 \pmod 6, \\ (-1)^{k(r-1)/2}p^{(r-1)/6}(\lambda^{(2r-2)/3}G(\psi) + \bar{\lambda}^{(2r-2)/3}G(\psi^5)) & \text{if } r \equiv 1 \pmod 6, \\ -(-1)^{kr/2}p^{(r-2)/6}(\zeta_6^{2Z}\lambda^{(2r-1)/3}G_3 + \zeta_6^{4Z}\bar{\lambda}^{(2r-1)/3}\hat{G}_3) & \text{if } r \equiv 2 \pmod 6, \\ (-1)^{k(r-1)/2}p^{(r-3)/6}i*\sqrt{p}(\lambda^{2r/3} + \bar{\lambda}^{2r/3}) & \text{if } r \equiv 3 \pmod 6, \\ -(-1)^{kr/2}p^{(r-4)/6}(\zeta_6^{4Z}\lambda^{(2r+1)/3}\hat{G}_3 + \zeta_6^{2Z}\bar{\lambda}^{(2r+1)/3}G_3) & \text{if } r \equiv 4 \pmod 6, \\ (-1)^{k(r-1)/2}p^{(r-5)/6}(\lambda^{(2r+2)/3}G(\psi^5) + \bar{\lambda}^{(2r+2)/3}G(\psi)) & \text{if } r \equiv 5 \pmod 6, \end{array}$$

where p has the form $6k + 1$.

https://doi.org/10.4153/CMB-2003-036-9 Published online by Cambridge University Press

In view of (7) the above proposition gives the value for $g_r(6) - g_r(3) - g_r(2)$ which may be conveniently expressed in terms of the sequences $V_{j,n}$ and $U_{j,n}$ using relations (17), (18) and (22). Namely, if $p = 6k + 1$ then depending on the value of r modulo 6, $g_r(6) - g_r(3) - g_r(2)$ equals

(23)
$$\begin{cases} -(-1)^{kr/2} p^{r/6} V_{2r/3} & \text{if } r \equiv 0 \\ \quad (-1)^{(k(r-1)/2} p^{(r-1)/6} \frac{i^*}{2\sqrt{p}} \left(g V_{2Z,(2r+1)/3} - (g'' - g') U_{2Z,(2r+1)/3} \right) & \text{if } r \equiv 1 \\ -(-1)^{kr/2} p^{(r-2)/6} \left(g V_{4Z,(2r-1)/3} + (g'' - g') U_{4Z,(2r-1)/3} \right) / 2 & \text{if } r \equiv 2 \\ \quad (-1)^{k(r-1)/2} p^{(r-3)/6} i^* \sqrt{p} V_{2r/3} & \text{if } r \equiv 3 \\ -(-1)^{kr/2} p^{(r-2)/4} \left(g V_{2Z,(2r+1)/3} - (g'' - g') U_{2Z,(2r+1)/3} \right) / 2 & \text{if } r \equiv 4 \\ \quad (-1)^{k(r-1)/2} p^{(r+1)/6} \frac{i^*}{2\sqrt{p}} \left(g V_{4Z,(2r-1)/3} + (g'' - g') U_{4Z,(2r-1)/3} \right) & \text{if } r \equiv 5. \end{cases}$$

If $p = 6k + 5$ then

$$g_r(6) = \begin{cases} -\left(3(-1)^{kr/2} + 2(-1)^{r/2} \right) p^{r/2} & \text{if } r \text{ is even} \\ (-1)^{k(r-1)/2} p^{(r-1)/2} i^* \sqrt{p} & \text{if } r \text{ is odd.} \end{cases} \tag{24}$$

using Theorem 12.6.1 in [2].

For $e = 4$ with $p \equiv 1 \pmod 4$, one has (chiefly, from Theorem 4.2.4 in [2])

$$G_4 = G(\psi) = \epsilon(A + iB) \quad \text{and} \tag{25}$$

$$\hat{G}_4 = G(\psi^3) = (-1)^Z \epsilon(A - iB), \tag{26}$$

where $A = \sqrt{p + (-1)^Z a_4 \sqrt{p})/2}$, $B = \frac{(-1)^Z b_4}{|b_4|} \sqrt{(p - (-1)^Z b_4 \sqrt{p})/2}$ and $\epsilon = \pm 1$. The correct choice of sign for ϵ was determined by Matthews [5] and is described in [2, p. 162]. In particular (chiefly Theorem 12.4.1 in [2]), if $p \equiv 1 \pmod 4$

$$g_r(4) - g_r(2) = \begin{cases} -p^{r/4} Q_{r/2} & \text{if } r \equiv 0 \pmod 4 \\ p^{(r-1)/4} (G_4 \pi^{(r-1)/2} + \hat{G}_4 \bar{\pi}^{(r-1)/2}) & \text{if } r \equiv 1 \pmod 4 \\ (-1)^{(p+3)/4} p^{(r-2)/4} Q_{r/2} \sqrt{p} & \text{if } r \equiv 2 \pmod 4 \\ (-1)^Z p^{(r-3)/4} (\hat{G}_4 \pi^{(r+1)/2} + G_4 \bar{\pi}^{(r+1)/2}) & \text{if } r \equiv 3 \pmod 4, \end{cases} \tag{27}$$

whereas if $p \equiv 3 \pmod 4$

$$g_r(4) = \begin{cases} -\left(2(-1)^{(p-3)r/8} + (-1)^{r/2} \right) p^{r/2} & \text{if } r \text{ even} \\ i(-1)^{(r-1)/2} p^{(r-1)/2} \sqrt{p} & \text{if } r \text{ odd.} \end{cases} \tag{28}$$

Here Q_n and P_n are the Lucas sequences given by

$$Q_n = \pi^n + \bar{\pi}^n \text{ and } P_n = -i(\pi^n - \bar{\pi}^n) \quad \text{for } n \geq 0. \tag{29}$$

I am ready to consider the case $e = 12$. For the (normalized) characters χ_j of $\mathbf{F}_q^*$ satisfying $\chi_j(\gamma) = \zeta_{12}^j$, put $R = G_r(\chi_3) + G_r(\chi_9)$ and $S = G_r(\chi_1) + G_r(\chi_5) + G_r(\chi_7) + G_r(\chi_{11})$ so the (modified) Gauss sum

$$g_r(12) = S + R + g_r(6). \tag{30}$$

For $p = 12k+1$ and ψ the (normalized) character of $\mathbf{F}_p^*$ of order 12 satisfying $\psi(G) = \zeta_{12}$, I explicitly evaluate $G(\psi^j)$ next for $\gcd(j, 12) = 1$.

Proposition 3 *For ψ as above with $p = 12k + 1$, one has*

$$G(\psi) = \bar{c}_{12} G_3 \hat{G}_4/\bar{\pi} \qquad G(\psi^7) = c_{12} G_3 G_4/\pi$$

$$G(\psi^5) = \bar{c}_{12} \hat{G}_3 \hat{G}_4/\bar{\pi} \qquad G(\psi^{11}) = c_{12} \hat{G}_3 G_4/\pi$$

where $\pi = a_4 + ib_4$ with G_3 and G_4 as in (17) and (25).

Proof In view of (2) it suffices to verify the expressions for $G(\psi^{11})$ and $G(\psi^5)$. Using (9) and (10),

$$G(\psi^{11}) = \frac{G(\psi^3)G(\psi^8)}{J(\psi^3, \psi^8)} = \frac{G_4 \hat{G}_3}{(-1)^k J(\psi, \psi^3)} = c_{12} G_4 \hat{G}_3/\pi$$

by Proposition 1. Also from (9), $G(\psi)G(\psi^5) = G(\psi^6) J(\psi, \psi^5) = (-1)^{T/2}\pi\sqrt{p}$ so $G(\psi^5) = \frac{(-1)^{T/2}\pi\sqrt{p}\bar{\pi}}{\bar{c}_{12} G_3 \hat{G}_4} = \bar{c}_{12} \hat{G}_3 \hat{G}_4 (-1)^Z \sqrt{p}/(\hat{G}_4^2) = \bar{c}_{12} \hat{G}_3 \hat{G}_4/\bar{\pi}$ by (26).

For the situation at hand, one finds an elegant expression for S in terms of $R = g_r(4) - g_r(2)$, $g_r(3)$ and $g_r(2)$.

Proposition 4 *For ψ as in Proposition 3 with $p = 12k + 1$, one has*

$$S = \begin{cases} c_{12}^r g_r(3) R/g_r(2) & \text{if } r \text{ even or } 3|b_4 \\ \omega g_r(3) P_r/R = \frac{(-1)^k \omega g_r(3) P_r}{g_r(2)\left(Q_r + 2g_r(2)\right)} & \text{if } r \text{ odd and } 3|a_4, \end{cases}$$

where $\omega = \pm 1$ satisfies $\omega \equiv (-1)^{(r+1)/2+k} b_4 \pmod 3$.

Proof For $r \equiv 0 \pmod{12}$, one finds $S = -p(E_r(\chi_1) + E_r(\chi_5) + E_r(\chi_7) + E_r(\chi_{11})) = -p^{r/12}(\pi^{r/2}\lambda^{r/3} + \pi^{r/2}\bar{\lambda}^{r/3} + \bar{\pi}^{r/2}\lambda^{r/3} + \bar{\pi}^{r/2}\bar{\lambda}^{r/3}) = -p^{r/3}(\lambda^{r/3} + \bar{\lambda}^{r/3})(\pi^{r/2} + \bar{\pi}^{r/2})/p^{r/4}$ or

$$p^{r/4} S = -g_r(3) Q_{r/2} \tag{31}$$

from Theorem 1 and (19).

For $r \not\equiv 0 \pmod{12}$, one finds

$$S = E_r(\chi_1)G(\psi^r) + E_r(\chi_5)G(\psi^{5r}) + E_r(\chi_7)G(\psi^{7r}) + E_r(\chi_{11})G(\psi^{11r})$$

with $G(\psi^j)$ given in Proposition 3, (17) or (22). In each case one finds a factorization for S. To illustrate for odd r, consider the case $r \equiv 1 \pmod{12}$. Then

$$\begin{aligned} S &= p^{(r-1)/12}(\bar{c}_{12}\pi^{(r-1)/2}\lambda^{(r-1)/3} G_3 \hat{G}_4/\bar{\pi} + \bar{c}_{12}\pi^{(r-1)/2}\bar{\lambda}^{(r-1)/3}\hat{G}_3\hat{G}_4/\bar{\pi} \\ &\quad + c_{12}\bar{\pi}^{(r-1)/2}\lambda^{(r-1)/3} G_3 G_4/\pi + c_{12}\bar{\pi}^{(r-1)/2}\bar{\lambda}^{(r-1)/3}\hat{G}_3 G_4/\pi) \\ &= p^{(r-13)/12}(\bar{c}_{12}\pi^{(r+1)/2)}\lambda^{(r-1)/3} G_3\hat{G}_4 + \bar{c}_{12}\pi^{(r+1)/2}\bar{\lambda}^{(r-1)/3}\hat{G}_3\hat{G}_4 \\ &\quad + c_{12}\bar{\lambda}^{(r+1)/2}\lambda^{(r-1)/3} G_3 G_4 + c_{12}\bar{\pi}^{(r+1)/2}\bar{\lambda}^{(r-1)/3}\hat{G}_3 G_4) \\ &= p^{(r-1)/3}(\lambda^{(r-1)/3} G_3 + \bar{\lambda}^{(r-1)/3}\hat{G}_3) \cdot (\bar{c}_{12}\pi^{(r+1)/2}\hat{G}_4 + c_{12}\bar{\pi}^{(r+1)/2} G_4)/p^{(r+3)/4} \end{aligned}$$

or

$$p^{(r+3)/4}S = g_r(3)(\bar{c}_{12}\pi^{(r+1)/2}\hat{G}_4 + c_{12}\bar{\pi}^{(r+1)/2}G_4). \tag{32}$$

The formula (32) is seen to hold for any $r \equiv 1 \pmod 4$. Similarly, for $r \equiv 3 \pmod 4$ one finds

$$p^{(r+1)/4}S = g_r(3)(-1)^k(c_{12}\pi^{(r-1)/2}G_4 + \bar{c}_{12}\bar{\pi}^{(r-1)/2}\hat{G}_4). \tag{33}$$

For $r \equiv 4$ or $8 \pmod{12}$, formula (31) is found to hold. Finally, for $r \equiv 2 \pmod 4$ one finds that

$$p^{(r-2)/4}\sqrt{p}S = (-1)^{T/2}g_r(3)Q_{r/2}. \tag{34}$$

To illustrate formula (34) when $r \equiv 2 \pmod{12}$, one finds

$$\begin{aligned}
S &= -(-1)^{T/2}p^{(r-2)/12}\big(\zeta_6^{2Z}\pi^{r/2}\lambda^{(r-2)/3}G(\psi^2) + \zeta_6^{4Z}\pi^{r/2}\bar{\lambda}^{(r-2)/3}G(\psi^{10}) \\
&\qquad + \zeta_6^{2Z}\bar{\pi}^{r/2}\lambda^{(r-2)/3}G(\psi^2) + \zeta_6^{4Z}\bar{\pi}^{r/2}\bar{\lambda}^{(r-2)/3}G(\psi^{10})\big) \\
&= -(-1)^{T/2}p^{(r-2)/12}(\zeta_6^{2Z}\lambda^{(r-2)/3}G_6 + \zeta_6^{4Z}\bar{\lambda}^{(r-2)/3}\hat{G}_6)(\pi^{r/2} + \bar{\pi}^{r/2}) \\
&= -(-1)^{T/2}p^{(r-14)/12}\sqrt{p}(\lambda^{(r+1)/3}\hat{G}_3 + \bar{\lambda}^{(r+1)/3}G_3)Q_{r/2}
\end{aligned}$$

or $= (-1)^{T/2}g_r(3)Q_{r/2}/(p^{(r-2)/4}\sqrt{p})$ from (17)–(19) and (22).

Comparing the expressions (31)–(34) just derived with (16), (19) and (27) for $g_r(2)$, $g_r(3)$ and R, one readily obtains the desired formula for S in case r is even or $3|b_4$ in view of the fact $c_{12}^2 = (-1)^{T/2+k}$.

It remains to establish the formula for S when r is odd and $3|a_4$, in which case $c_{12} = \pm i$ satisfies $c_{12} \equiv -ib_4 \pmod 3$ from (13). For $r \equiv 1 \pmod 4$,

$$\begin{aligned}
&\bar{c}_{12}\pi^{(r+1)/2}\hat{G}_4 + c_{12}\bar{\pi}^{(r+1)/2}G_4 \\
&\qquad = p^{(r-1)/4}\bar{c}_{12}(\pi^{(r+1)/2}\hat{G}_4 - \bar{\pi}^{(r+1)/2}G_4)(\pi^{(r-1)/2}G_4 + \bar{\pi}^{(r-1)/2}\hat{G}_4)/R \\
&\qquad = p^{(r-1)/4}\bar{c}_{12}\big(\pi^r\hat{G}_4G_4 - \bar{\pi}^rG_4\hat{G}_4 + p^{(r-1)/2}(\pi\hat{G}_4^2 - \bar{\pi}G_4^2)\big)\big/R \\
&\qquad = p^{(r+3)/4}\bar{c}_{12}(-1)^Z(\pi^r - \bar{\pi}^r)/R \\
&\qquad = (-1)^Zi\bar{c}_{12}p^{(r+3)/4}P_r/R
\end{aligned}$$

from (27) with $(-1)^Zi\bar{c}_{12} \equiv -(-1)^kb_4 \pmod 3$. This yields the desired form for S when $r \equiv 1 \pmod 4$ and its alternatives since R^2 equals

$$\begin{aligned}
p^{(r-1)/2}(\pi^{(r-1)/2}G_4 + \bar{\pi}^{(r-1)/2}\hat{G}_4)^2 &= p^{(r-1)/2}(\pi^{r-1}G_4^2 + 2p^{(r-1)/2}G_4\hat{G}_4 + \bar{\pi}^{r-1}\hat{G}_4^2) \\
&= (-1)^kp^{(r-1)/2}(\pi^r\sqrt{p} + 2p^{(r+1)/2} + \bar{\pi}^r\sqrt{p}) \\
&= (-1)^kg_r(2)\big(Q_r + 2g_r(2)\big)
\end{aligned}$$

from (25)–(27). For $r \equiv 3 \pmod 4$,

$$\begin{aligned}(-1)^k(c_{12}\pi^{(r-1)/2}G_4 + \bar{c}_{12}\bar{\pi}^{(r-1)/2}\hat{G}_4) \\ &= p^{(r-3)/4}c_{12}(\pi^{(r-1)/2}G_4 - \bar{\pi}^{(r-1)/2}\hat{G}_4)(\pi^{(r+1)/2}\hat{G}_4 + \bar{\pi}^{(r+1)/2}G_4)/R \\ &= p^{(r-3)/4}c_{12}\big(\pi^r G_4\hat{G}_4 - \bar{\pi}^r G_4\hat{G}_4 + p^{(r-1)/2}(\bar{\pi}G_4^2 - \pi\hat{G}_4^2)\big) \\ &= (-1)^k p^{(r+1)/4}c_{12}(\pi^r - \bar{\pi}^r)/R = (-1)^k i c_{12} p^{(r+1)/4} P_r/R\end{aligned}$$

again from (25)–(27), with $(-1)^k i c_{12} \equiv (-1)^k b_4 \pmod 3$. This yields the desired form for S when $r \equiv 3 \pmod 4$ and its alternative since

$$R^2 = (-1)^k g_r(2)\big(Q_r + 2g_r(2)\big)$$

in this case, too.

I completely determine $g_r(12)$ next without any sign ambiguities.

Theorem 2 *The value $g_r(12)$ is explicitly given by*

(i) *If $p = 12k + 1$ then*

$$g_r(12) = \begin{cases} g_r(6) + R\big(1 + c_{12}^r g_r(3)/g_r(2)\big) & \text{if } r \text{ even or } 3|b_4 \\ g_r(6) + R\big(1 + \dfrac{(-1)^k \omega g_r(3)P_r}{g_r(2)(Q_r + 2g_r(2))}\big) & \text{if } r \text{ odd and } 3|a_4. \end{cases}$$

(ii) *If $p = 12k + 5$ then*

$$g_r(12) = \begin{cases} -5p^{r/2} - p^{r/4}Q_{r/2}\big(2(-1)^{r/4} + 1\big) & \text{if } 4|r \\ -p^{r/2} + (-1)^k p^{(r-2)/4}\sqrt{p}\big(Q_{r/2} + (-1)^{(r-2)/4}2\beta P_{r/2}\big) & \text{if } 2||r \\ g_r(4) & \text{if } r \text{ odd.} \end{cases}$$

(iii) *If $p = 12k + 7$ then*

$$g_r(12) = \begin{cases} g_r(6) + 2(-1)^{r(k+1)/2}\big(g_r(3) - p^{r/2}\big) & \text{if } r \text{ even} \\ g_r(6) & \text{if } r \text{ odd.} \end{cases}$$

(iv) *If $p = 12k + 11$ then $g_r(12) = -\big(6(-1)^{kr/2} + 5(-1)^{r/2}\big)\, p^{r/2}$ or $g_r(2)$ according as r is even or odd.*

Proof From (30) one knows that $g_r(12) = g_r(6) + R + S$ and from [2, p. 421] that

(35) $$g_r(12) = g_r(d), \quad \text{where } d = \gcd(12, p - 1).$$

Thus statement (i) follows immediately from Proposition 4, and for $p \not\equiv 1 \pmod{12}$ results (ii)–(iv) hold when r is odd due to (35). It remains to verify (ii)–(iv) when r is even.

If $p = 12k + 5$ then $\chi^*(G) = \zeta_{12}^{(q-1)/(p-1)} = \zeta_{12}^{3r}$. For $r \equiv 0 \pmod 4$,

$$S = -p\big(E_r(\chi_1) + E_r(\chi_5) + E_r(\chi_7) + E_r(\chi_{11})\big) = -2(-1)^{r/4} p^{r/2}(\pi^{r/2} + \bar{\pi}^{r/2})$$
$$= -2(-1)^{r/4} p^{r/2} Q_{r/2}$$

from Theorem 1, $R = -p^{r/4} Q_{r/2}$ from (27) and $g_r(6) = -5p^{r/2}$ from (24). Whereas for $r \equiv 2 \pmod 4$, $R = (-1)^k p^{(r-2)/4} Q_{r/2}\sqrt{p}$ from (27),

$$\begin{aligned} S &= \sqrt{p}\big(E_r(\chi_1) + E_r(\chi_5) + E_r(\chi_7) + E_r(\chi_{11})\big) \\ &= -2(-1)^{k+(r-2)/4} \beta p^{(r-2)/4} \sqrt{p}(i\pi^{r/2} - i\bar{\pi}^{r/2}) \\ &= 2(-1)^{k+(r-2)/4} \beta P_r p^{(r-2)/4} \sqrt{p} \end{aligned}$$

from Theorem 1 and $g_r(6) = -p^{r/2}$ from (24). In either case, the expression for $g_r(12)$ in (ii) follows.

If $p = 12k + 7$ then $\chi^*(G) = \zeta_{12}^{4r}$ and one finds from Theorem 1 that

$$S = \begin{cases} -2(-1)^{r(k+1)/2} p^{(r-2)/3}(\lambda^{(r+1)/3}\hat{G}_3 + \bar{\lambda}^{(r+1)/3} G_3) & \text{if } r \equiv 2 \pmod 6 \\ -2(-1)^{r(k+1)/2} p^{(r-1)/3}(\lambda^{(r-1)/3} G_3 + \bar{\lambda}^{(r-1)/3}\hat{G}_3) & \text{if } r \equiv 4 \pmod 6 \\ -2(-1)^{r(k+1)/2} p^{r/3}(\lambda^{r/3} + \bar{\lambda}^{r/3}) & \text{if } r \equiv 0 \pmod 6 \end{cases}$$

or equivalently that

$$S = 2(-1)^{r(k+1)/2} g_r(3) \tag{36}$$

from (19) when r is even. Also $R = g_r(4) - g_r(2) = 2(-1)^{r(k+1)/2} p^{r/2}$ from (16) and (28). This yields the expression for $g_r(12)$ in (iii).

If $p = 12k + 11$ then $S = -4(-1)^{kr/2} p^{r/2}$, $R = -2(-1)^{kr/2} p^{r/2}$ from Theorem 1, (16) and (28), and $g_r(6) = -5(-1)^{r/2} p^{r/2}$ from (24). Thus $g_r(12) = -\big(6(-1)^{kr/2} + 5(-1)^{r/2}\big) p^{r/2}$ in (iv) when r is even.

The proof of the theorem is now complete.

References

[1] B. Berndt and R. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer*. Illinois J. Math. (3) **23**(1979), 374–437.

[2] B. Berndt, R. Evans and K. S. Williams, *Gauss and Jacobi Sums*. Wiley, New York, (1997).

[3] R. Evans, *Gauss sums of orders six and twelve*. to appear.

[4] S. Gurak, *Period polynomials for* $\mathbf{F}_{p^2}$ *of fixed small degree*. In: Finite Fields and Applications, (eds., D. Jungnickel and H. Niederreiter), Springer, 2000, 196-207.

[5] C. R. Matthews, *Gauss sums and elliptic functions I, II*. Invent. Math. **52**(1979), 163–185; **54**(1979), 23–52.

[6] K. S. Williams, K. Hardy and B. K. Spearman, *Explicit evaluation of certain Eisenstein sums*. In: Number Theory, (ed., R. A. Mollin), de Gruyter, Berlin, 1990, 553–626.

Department of Mathematics
University of San Diego
San Diego, California 92110
USA

https://doi.org/10.4153/CMB-2003-036-9 Published online by Cambridge University Press