Canad. Math. Bull. Vol. **44** (1), 2001 pp. 22–26

Gauss Sums of Orders Six and Twelve

Ronald Evans

Abstract. Precise, elegant evaluations are given for Gauss sums of orders six and twelve.

1 Introduction

For an integer $k > 1$ and a prime $p \equiv 1 \pmod{k}$, define the Gauss sum

$$g(k) = \sum_{n=0}^{p-1} \exp(2\pi i n^k/p).$$

In 1805, after four years of effort, Gauss resolved the sign ambiguity in his formula for the quadratic Gauss sum $g(2)$. Much more recently, the ambiguity has been removed in formulas for $g(3)$, $g(4)$, and $g(6)$ (see [2, Ch. 4]). On the other hand, sign ambiguities persist in formulas for $g(8)$, $g(12)$, $g(24)$ [1] and $g(16)$ [3]. Research Problem 6 in [2, p. 496] asks for complete determinations of $g(8)$ and $g(12)$. Both parts of this problem have been open for about twenty years, but it turns out that there is a surprisingly elementary resolution for $g(12)$. The main purpose of this note is to present, in Theorem 2, the complete evaluation of $g(12)$, in terms of the known quantities $g(3)$ and $g(4)$. Additionally, in Theorem 1, we give a new formulation of $g(6)$ (in terms of $g(3)$) which is more elegant than that given previously [1], [2, p. 156]. (The problem of determining $g(8)$ in terms of $g(4)$ is still open and appears to be very difficult.)

This note is best read in conjunction with [2], since heavy use is made of the results and notation in that book.

2 Evaluation of $g(6)$

Let p be a prime $\equiv 1 \pmod{6}$. Define integers a_3, b_3 as in [2, Thm. 3.1.1], so that

$$p = a_3^2 + 3b_3^2, \quad a_3 \equiv -1 \pmod{3}. \tag{1}$$

Note that a_3 is uniquely determined by (1). If $3 \nmid b_3$, specify the sign of b_3 as follows:

$$b_3 \equiv -1 \pmod{3}, \quad \text{if } 3 \nmid b_3. \tag{2}$$

By [2, p. 105], $3 \mid b_3$ if and only if 2 is a cubic residue modulo p. Define (*cf.* [2, p. 105])

$$r_3 = -a_3 - 3b_3, \quad s_3 = a_3 - b_3, \tag{3}$$

Received by the editors November 27, 1998.
AMS subject classification: 11L05, 11T24.

so that

$$4p = r_3^2 + 3s_3^2. \tag{4}$$

By [2, p. 155],

$$g(3)^3 = 3pg(3) + pr_3 \tag{5}$$

and

$$|g(3)| < 2\sqrt{p}. \tag{6}$$

The following theorem gives an unambiguous evaluation of $g(6)$ which is more elegant than that found in [2, Thm. 4.1.4].

Theorem 1 *Let p be a prime $\equiv 1 \pmod 6$, and define r_3 and s_3 as in (3). If 2 is a cubic residue modulo p, then*

$$g(6) = g(3) + i^{(p-1)^2/4}\big(g(3)^2 - p\big) \Big/ \sqrt{p};$$

if 2 is not a cubic residue modulo p, then

$$g(6) = g(3) + i^{(p-1)^2/4}\Big(4p - g(3)^2 + s_3^{-1}\big(2pg(3) + 2pr_3 - r_3g(3)^2\big)\Big) \Big/ (2\sqrt{p}).$$

Proof In view of [2, Thm. 4.1.4 and eq. (3.1.3)], it remains to prove that when 2 is not a cubic residue modulo p,

$$s_3^{-1}\big(2pg(3) + 2pr_3 - r_3g(3)^2\big) = \nu g(3)\big(12p - 3g(3)^2\big)^{1/2}, \tag{7}$$

where $\nu = \operatorname{sgn}\Big(s_3\big(g(3)^2 - p\big)\Big)$. Such a formula, once written down, is not difficult to prove. With the aid of (5), we easily find that the square of the left member of (7) equals the square of the right member. Thus it remains to show that the two expressions $\big(2pg(3)+2pr_3-r_3g(3)^2\big)$ and $\big(g(3)^3-pg(3)\big)$ have the same sign. This follows because the quotient of these expressions is $4 - g(3)^2/p$, which is positive by (6).

3 Evaluation of $g(12)$

Let p be a prime $\equiv 1 \pmod{12}$, and let χ be a multiplicative character modulo p of order 12. Define the Gauss character sum

$$G(\chi) = \sum_{m=0}^{p-1} \chi(m) \exp(2\pi i m/p).$$

Write

$$S = G(\chi) + G(\chi^5) + G(\chi^7) + G(\chi^{11}) \tag{8}$$

and

$$R = G(\chi^3) + G(\chi^9). \tag{9}$$

(Note that R and S do not depend on the choice of χ.) We have

$$R = g(4) - g(2) = g(4) - \sqrt{p}, \tag{10}$$

by [2, pp. 15, 160, 161]. Define integers a, b as in [2, Thm. 3.2.1], so that

$$p = a^2 + b^2, \quad a \equiv -\left(\frac{2}{p}\right) \pmod 4. \tag{11}$$

Note that a is uniquely determined by (11). If $3 \nmid b$, specify the sign of b as follows:

$$b \equiv -1 \pmod 3, \quad \text{if } 3 \nmid b. \tag{12}$$

By [2, p. 161],

$$R^2 = 2\left(\frac{2}{p}\right)(p + a\sqrt{p}) \tag{13}$$

and by [2, p. 166],

$$S^2 = \begin{cases} p^{-1}g(3)^2 \cdot 2(\frac{2}{p})(p + a\sqrt{p}), & \text{if } 3 \nmid a \\ p^{-1}g(3)^2 \cdot 2(\frac{2}{p})(p - a\sqrt{p}), & \text{if } 3 \mid a. \end{cases} \tag{14}$$

Using (10) and (13), we can deduce from [2, Thm. 4.4.1] that

$$g(12) = \begin{cases} g(6) + \big(g(4) - \sqrt{p}\big)\big(1 \pm g(3)/\sqrt{p}\big), & \text{if } 3 \nmid a \\ g(6) + g(4) - \sqrt{p} \pm 2bg(3)/\big(g(4) - \sqrt{p}\big), & \text{if } 3 \mid a. \end{cases} \tag{15}$$

In Theorem 2 below, we resolve the sign ambiguity in the formula for $g(12)$.

Theorem 2 *Let p be a prime $\equiv 1 \pmod{12}$, and define a and b as in (11) and (12). Then, with $g(6)$ as given in Theorem 1,*

$$g(12) = \begin{cases} g(6) + \big(g(4) - \sqrt{p}\big)\big(1 + (\frac{-a}{3})g(3)/\sqrt{p}\big), & \text{if } 3 \nmid a \\ g(6) + g(4) - \sqrt{p} + 2(\frac{2}{p})bg(3)/\big(g(4) - \sqrt{p}\big), & \text{if } 3 \mid a. \end{cases} \tag{16}$$

Proof We first need to compute $S^3 \pmod 3$. This can be accomplished by cubing every summand in each of the four Gauss sums appearing in (8). Thus

$$S^3 \equiv \chi^3(3)\{G(\chi^3) + G(\chi^3) + G(\chi^9) + G(\chi^9)\} = 2\chi^3(3)R \pmod 3, \tag{17}$$

where $X \equiv Y \pmod 3$ means that $(X - Y)/3$ is an algebraic integer. Here we used the fact that $\chi^3(3) = \pm 1$ (since 3 is a square $\pmod p$). In fact, a well known result of Gauss (see [2, p. 216, Thm. 7.2.2]) gives

$$\chi^3(3) = \begin{cases} (\frac{2}{p}), & \text{if } 3 \nmid a, \\ -(\frac{2}{p}), & \text{if } 3 \mid a. \end{cases}$$

Hence

$$S^3 \equiv \begin{cases} -(\frac{2}{p})R \pmod 3, & \text{if } 3 \nmid a, \\ (\frac{2}{p})R \pmod 3, & \text{if } 3 \mid a. \end{cases} \tag{18}$$

Case 1 $3 \nmid a$.

By (13) and (14),

$$S = \delta R g(3)/\sqrt{p} \tag{19}$$

for some $\delta = \pm 1$. By [2, p. 166],

$$g(12) = g(6) + R + S. \tag{20}$$

From (10), (19), and (20), we see that it remains to show that $\delta = (\frac{-a}{3})$. Cubing in (19), we have

$$p\sqrt{p}S^3 = \delta R^3 g(3)^3.$$

Thus by (13), (5), and the fact that $p \equiv r_3 \equiv 1 \pmod 3$,

$$\sqrt{p}S^3 \equiv \delta R \cdot 2 \left(\frac{2}{p}\right)(p + a\sqrt{p}) \pmod 3.$$

Thus

$$S^3 \equiv -\delta R \left(\frac{2}{p}\right)(\sqrt{p} + a) \pmod 3. \tag{21}$$

Combining (18) and (21), we obtain

$$0 \equiv R(1 - \delta a - \delta\sqrt{p}) \pmod 3.$$

Multiplying both sides of this congruence by R, and making use of (13), we obtain

$$0 \equiv (p + a\sqrt{p})(1 - \delta a - \delta\sqrt{p}) \pmod 3.$$

Hence,

$$p(1 + \delta a) + (\delta + a)\sqrt{p} \equiv 0 \pmod 3,$$

or equivalently,

$$(\delta + a)(\delta p + \sqrt{p}) \equiv 0 \pmod 3.$$

If $\delta + a$ is not divisible by 3, then 3 divides $(\delta p + \sqrt{p})$ so that $(\delta p + \sqrt{p})/3$ is an algebraic integer, which is not the case. Thus $\delta + a \equiv 0 \pmod 3$. This completes the proof that $\delta = (\frac{-a}{3})$ in the case $3 \nmid a$.

Case 2 $3 \mid a$.

By (13) and (14),

$$S = 2\delta bg(3)/R \tag{22}$$

for some $\delta = \pm 1$. From (22), (20), and (10), we see that it remains to prove that $\delta = (\frac{2}{p})$. Cubing in (22), we have, by (5) and (12),

$$S^3R^3 = 8\delta b^3 g(3)^3 \equiv \delta \pmod 3. \tag{23}$$

Since by (13),

$$R^4 = 4(p + a\sqrt{p})^2 \equiv 4p^2 \equiv 1 \pmod 3,$$

it follows from (18) that

$$S^3R^3 \equiv \left(\frac{2}{p}\right) R^4 \equiv \left(\frac{2}{p}\right) \pmod 3. \tag{24}$$

Combining (23) and (24), we see that $\delta \equiv (\frac{2}{p}) \pmod 3$. This completes the proof that $\delta = (\frac{2}{p})$ in the case $3 \mid a$.

References

[1] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal.* J. Number Theory **11**(1979), 349–398.

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

[3] R. J. Evans, *Bioctic Gauss sums and sixteenth power residue difference sets.* Acta Arith. **38**(1980), 37–46.

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