Note on a Cubic Character Sum

KENNETH S. WILLIAMS (Ottawa, Ontario, Canada)

Abstract

A short evaluation is given of a cubic character sum considered by Rajwade [5].

Let \( w = (-1 + \sqrt{-3})/2 \) and let \( p \) be a rational prime \( \equiv 1 \pmod{3} \). In the unique factorization domain \( \mathbb{Z}[w] \), \( p \) has the factorization \( p = \pi \bar{\pi} \), where \( \pi, \bar{\pi} \) are primes. By taking a suitable associate of \( \pi \) we can assume that \( \pi, \bar{\pi} \) are primary, that is \( \pi, \bar{\pi} \equiv -1 \pmod{3} \). Rajwade [5] has recently evaluated the character sum \( \sum_{x=0}^{p-1} (x^3 + a/p) \), where \((\cdot/p)\) is the Legendre symbol and \( a \not\equiv 0 \pmod{p} \). He proved, (slightly different notation)

\[
\sum_{x=0}^{p-1} \left( \frac{x^3 + a}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{4a}{\pi} \right)_3 \pi + \left( \frac{4a}{\bar{\pi}} \right)_3 \bar{\pi},
\]

where \((\cdot/\pi)_3\) is the cubic residue character \( \pmod{\pi} \), so that

\[
\left( \frac{y}{\pi} \right)_3 = \left( \frac{y}{\pi} \right)^2 = \left( \frac{y}{\pi} \right).
\]

His proof covers more than three pages. It is the purpose of this note to give the following four-line proof (each step is justified below):

\[
\sum_{x=0}^{p-1} \left( \frac{x^3 + a}{p} \right) = \sum_{y=0}^{p-1} \left( \frac{y+a}{p} \right) \left\{ 1 + \left( \frac{y}{\pi} \right)_3 + \left( \frac{y}{\bar{\pi}} \right)_3 \right\}
\]

\[
= \left( \frac{a}{p} \right) \sum_{y=0}^{p-1} \left\{ 1 + \left( \frac{a(y+a)}{p} \right) \right\} \left\{ \left( \frac{y}{\pi} \right)_3 + \left( \frac{y}{\bar{\pi}} \right)_3 \right\}
\]

\[
= \left( \frac{a}{p} \right) \sum_{z=0}^{p-1} \left\{ \left( \frac{4az(z+1)}{\pi} \right)_3 + \left( \frac{4az(z+1)}{\bar{\pi}} \right)_3 \right\}
\]

\[
= \left( \frac{a}{p} \right) \left\{ \left( \frac{4a}{\pi} \right)_3 \pi + \left( \frac{4a}{\bar{\pi}} \right)_3 \bar{\pi} \right\}.
\]

AMS Primary Subject Classification: 10G05. Secondary Subject Classification: 12C20. Research supported by National Research Council of Canada, Grant A-7233.

Received June 8, 1973
(2) follows from (1) as
\[
\sum_{y=0}^{p-1} \left( \frac{y+a}{p} \right) = \sum_{y=0}^{p-1} \left( \frac{y}{p} \right) = \sum_{y=0}^{p-1} \left( \frac{y}{\pi} \right) = 0;
\]

(3) follows from (2) as the number of solutions \( z \) of \( 4az(z+1) \equiv y \pmod{p} \) is \( 1 + (a(y+a)/p) \); (4) follows from (3) as the Jacobi sum
\[
J = \sum_{y=0}^{p-1} \left( \frac{y(y+1)}{\pi} \right) \equiv \pi
\]
(see [2] Lemma 1, p. 116). Only the last of these is non-trivial (but well-known) and for completeness we indicate a proof.

We set \( G_k(a) = \sum_{y=0}^{p-1} (t/\pi)^k \exp(2\pi i at/p) \) \( (k = 1, 2) \), so that \( G_k(a) = (a/\pi)^2 G_k \), where \( G_k = G_k(1) \). Squaring \( G_1 \) a standard argument shows that \( G_2 = JG_2 \). Evaluating \( \sum_{a=1}^{p-1} G_k(a) \overline{G_k(a)} \) in two ways we obtain \( (p-1) G_k \overline{G_k} = (p-1) \), so that \( G_k \overline{G_k} = p \), giving \( J = \pi \). Note that \( J \in \mathbb{Z} \). Now as \( \sum_{y=0}^{p-1} y^n \equiv 0 \pmod{p} \), if \( n \equiv 0 \pmod{p-1} \), we have
\[
J \equiv \sum_{y=0}^{p-1} y^{p-1/3} (y+1)^{p-1/3} \equiv 0 \pmod{\pi},
\]
so that \( \pi \mid J \), giving \( J = \pm w^r \pi \), \( 0 \leq r \leq 2 \). Finally as
\[
1 + 2 \left( \frac{z}{\pi} \right) \equiv 0 \pmod{\sqrt{-3}},
\]
for any integer \( z \), we have
\[
\sum_{y=0}^{p-1} \left( 1 + 2 \left( \frac{y}{\pi} \right) \right) \left( 1 + 2 \left( \frac{y+1}{\pi} \right) \right) \equiv 0 \pmod{(\sqrt{-3})^2},
\]
so that
\[
p + 4J \equiv 0 \pmod{3}, J \equiv -p \equiv -1 \pmod{3},
\]
proving \( J = \pi \) as required.

It is perhaps worth noting that Rajwade's result includes results of von Schrutka [6], Whiteman [7], Lehmer [3] (Theorem 6), and that it also contains the case \( a = -1 \)
treated by Hasse [1]. In order to verify this it is convenient to appeal to the following consequence of the law of cubic reciprocity:

\[
\left( \frac{2}{\pi} \right)_3 \equiv \pi \pmod{2}
\]

(see [2] (p. 120)).

We also remark that the method of this paper can be used to give a similar evaluation of the sum

\[
\sum_{x=0}^{p-1} \left( \frac{x(x^2 + a)}{p} \right) \equiv \sum_{x=0}^{p-1} \left( \frac{x^4 + a}{p} \right) - \sum_{x=0}^{p-1} \left( \frac{x^2 + a}{p} \right) = \sum_{x=0}^{p-1} \left( \frac{x^4 + a}{p} \right) + 1,
\]

for primes \( p \equiv 1 \pmod{4} \), in a few lines. The recent evaluation by Morlaye [4] takes (unnecessarily) eight pages.

REFERENCES


Carleton University