Journal of Number Theory 135 (2014) 139–150

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

An application of a product formula for the cubic Gauss sum

Hiroshi Ito

Department of Mathematics, Kanagawa University, Hiratsuka, 259-1293, Japan

ARTICLE INFO

Article history:
Received 9 March 2013
Accepted 13 August 2013
Available online 17 October 2013
Communicated by David Goss

MSC:
primary 11L05
secondary 11G05, 11G16

Keywords:
Gauss sums
Elliptic functions

ABSTRACT

A product formula of Matthews [4] for the cubic Gauss sum $\tau_3(\omega)$ as defined in the Introduction will be applied to determine which of the three intervals $(-2\sqrt{p}, -\sqrt{p})$, $(-\sqrt{p}, \sqrt{p})$ and $(\sqrt{p}, 2\sqrt{p})$ contains the cubic Gauss sum $g_3(p) = \sum_{a=0}^{p-1} e^{2\pi i a^3/p}$, where p is a prime number congruent to one modulo 3.

1. Introduction

Let p be a prime number congruent to one modulo 3 and consider the sum

$$g_3(p) = \sum_{a=0}^{p-1} e^{2\pi i a^3/p}.$$

Let $\rho = e^{2\pi i/3}$ and write $p = \omega\bar{\omega}$ with a number ω in $\mathbf{Z}[\rho]$ such that $\omega \equiv 1 \pmod 3$. Set

$$\tau_3(\omega) = \sum_{a=1}^{p-1} \left(\frac{a}{\omega}\right)_3 e^{2\pi i a/p},$$

where the symbol $(\frac{a}{\omega})_3$ denotes the cubic residue symbol in $\mathbf{Q}(\rho)$. We have

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.08.005

$$g_3(p) = \tau_3(\omega) + \overline{\tau_3(\omega)}$$

and

$$\tau_3(\omega)^3 = -p\omega, \quad \left|\tau_3(\omega)\right| = \sqrt{p},$$

cf. Berndt, Evans and Williams [1] for general facts concerning the sums $g_3(p)$ and $\tau_3(\omega)$. Therefore, the sum $g_3(p)$ belongs to the interval $(-2\sqrt{p}, 2\sqrt{p})$ and the problem of determining which cube root of $-p\omega$ coincides to the sum $\tau_3(\omega)$ is equivalent to that of determining which of the three intervals $(-2\sqrt{p}, -\sqrt{p})$, $(-\sqrt{p}, \sqrt{p})$ and $(\sqrt{p}, 2\sqrt{p})$ contains the sum $g_3(p)$. Many people have made efforts to get clear and satisfying knowledge on these questions (cf. [1, Chapter 4]).

Now, for the sum $\tau_3(\omega)$, Matthews [4] has proved a formula conjectured by Cassels [2], according to which $\tau_3(\omega)$ is expressed in terms of a product of division values of the Weierstraß $\wp$-function $\wp(z)$ which satisfies $\wp'^2 = 4\wp^3 - 1$. In this paper, by evaluating this product of division values, we will get a formula for $\tau_3(\omega)$ and obtain a criterion for determining the interval which contains the sum $g_3(p)$.

We shall state the main theorem. Let c and d be the integers such that

$$p = c^2 + cd + d^2, \quad 0 < d < c$$

and let f be the integer satisfying

$$cf \equiv d \pmod{p}, \quad 1 \leqslant f \leqslant p - 1.$$

The integers c, d and f are uniquely determined by these conditions and f gives a primitive cube root of unity modulo p. Define the subset R_p of $\mathbf{Z}$ by

$$R_p = \left\{ \frac{u-2v}{3} + \frac{2u-v}{3} f;\ \begin{array}{l} 0 \leqslant u \leqslant c-1,\ 1 \leqslant v \leqslant c-1, \\ u+v \equiv 0 \pmod{3} \end{array} \right\} \\ \cup \left\{ \frac{c-u-2v}{3} + \frac{2c+u-v}{3} f;\ \begin{array}{l} 0 \leqslant u \leqslant d,\ 1 \leqslant v \leqslant c+d-1, \\ u-v-c \equiv 0 \pmod{3} \end{array} \right\}. \tag{1}$$

Here, u and v represent rational integers. As we shall see later, the set R_p consists of $(p-1)/3$ elements and the union $R_p \cup fR_p \cup f^2R_p \cup \{0\}$ gives a complete representative system for $\mathbf{Z}/p\mathbf{Z}$. Hence, by Wilson's theorem, there exists an integer a_p ($a_p = 0, 1, 2$) such that

$$\prod_{r \in R_p} r \equiv -f^{a_p} \pmod{p}.$$

Furthermore, for every pair of classes C and D in $\mathbf{Z}/9\mathbf{Z}$ with $C \not\equiv D \pmod 3$, we define an integer $z(C, D)$ by Table 1 and, by abbreviation, write $z(c, d)$ for $z(c \bmod 9,\ d \bmod 9)$.

Table 1
The values of $z(C,D)$.

$C\backslash D$	0	1	2	3	4	5	6	7	8
0	/	0	1	/	2	0	/	1	2
1	0	/	1	1	/	2	2	/	0
2	0	1	/	0	1	/	0	1	/
3	/	2	1	/	1	0	/	0	2
4	2	/	2	0	/	0	1	/	1
5	0	2	/	0	2	/	0	2	/
6	/	1	1	/	0	0	/	2	2
7	1	/	0	2	/	1	0	/	2
8	0	0	/	0	0	/	0	0	/

Theorem 1. *The interval which contains the sum $g_3(p)$ is determined by the value of a_p as follows. First, in case $(c,d) \equiv (1,0),(1,2),(0,2) \pmod 3$,*

$$\begin{cases} g_3(p) \in (-2\sqrt{p}, -\sqrt{p}\,) & \textit{if } a_p \equiv z(c,d) \pmod 3, \\ g_3(p) \in (-\sqrt{p}, \sqrt{p}\,) & \textit{if } a_p \equiv z(c,d)+1 \pmod 3, \\ g_3(p) \in (\sqrt{p}, 2\sqrt{p}\,) & \textit{if } a_p \equiv z(c,d)-1 \pmod 3. \end{cases}$$

Secondly, in case $(c,d) \equiv (2,0),(2,1),(0,1) \pmod 3$,

$$\begin{cases} g_3(p) \in (-2\sqrt{p}, -\sqrt{p}\,) & \textit{if } a_p \equiv z(c,d) \pmod 3, \\ g_3(p) \in (-\sqrt{p}, \sqrt{p}\,) & \textit{if } a_p \equiv z(c,d)-1 \pmod 3, \\ g_3(p) \in (\sqrt{p}, 2\sqrt{p}\,) & \textit{if } a_p \equiv z(c,d)+1 \pmod 3. \end{cases}$$

Later, we will make a particular choice of ω and construct a set S called "a 1/3-representative system modulo ω" as the set of points of $\mathbf{Z}[\rho]$ contained in the union of two parallelograms considered suitably in the complex plane $\mathbf{C}$. The above subset R_p of $\mathbf{Z}$ is the set obtained from S by replacing ρ by f in each element $x + y\rho$ $(x, y \in \mathbf{Z})$ of S.

Let, for an odd prime number p,

$$g_2(p) = \sum_{a=0}^{p-1} e^{2\pi i a^2/p}.$$

It can be seen without much difficulty that $g_2(p)^2 = (-1)^{(p-1)/2}p$. Gauss has shown that

$$g_2(p) = \prod_{\substack{a=1 \\ a\colon \mathrm{odd}}}^{p-1} \left(2i \sin\frac{2\pi a}{p}\right)$$

and determined which square root of $(-1)^{(p-1)/2}p$ coincides to the sum $g_2(p)$. Cassels made the conjecture mentioned above looking for an analogy of this fact to the sum $\tau_3(\omega)$. Thus, our work here may be viewed as an effort to pursue his intention as far as possible.

Let, for a prime number p congruent to one modulo 4,

$$g_4(p) = \sum_{a=0}^{p-1} e^{2\pi i a^4/p}.$$

For $g_4(p)$, consideration similar to that in this paper has already been done by Matthews ([5], cf. also [1, Theorem 4.2.4]). We can express $g_4(p)$ as a sum of Gauss sums with characters, relate the biquadratic Gauss sum appearing there to a product of division values of an elliptic function, and evaluate the product of division values. We see then, if $p \equiv 1 \pmod 8$,

$$g_4(p) = \sqrt{p} + E\left(\frac{B}{|A|}\right)(-1)^{(B^2+2B)/8}\sqrt{2p + 2A\sqrt{p}},$$

and if $p \equiv 5 \pmod 8$,

$$g_4(p) = \sqrt{p} + iE\left(\frac{B}{|A|}\right)(-1)^{(B^2+2B)/8}\sqrt{2p - 2A\sqrt{p}}.$$

Here, A and B are integers such that

$$p = A^2 + B^2, \quad A \equiv -1 \pmod 4, \ B > 0$$

and E is the square root of unity which satisfies the congruence

$$E \equiv \frac{B}{A} \cdot \frac{p-1}{2}! \cdot \left(\frac{2}{p}\right) \pmod p.$$

Also, $(\frac{\cdot}{\cdot})$ is the Jacobi symbol. It is remarked in [1, p. 164] that these formulae enable us to compute the value of $g_4(p)$ in time $O(p^{1/2+\epsilon})$ for every $\epsilon > 0$. The author does not know at present whether or not our results here have similar applications.

In the following, we shall prove Theorem 1 in Sections 2 and 3, and give an example in Section 4.

2. Proof of Theorem 1

We return to the notation introduced before Theorem 1. Thus, p is a prime number congruent to one modulo 3. First, we make a special choice of ω. Let

$$\omega' = c - d\rho^{-1}$$

and define the integer n $(0 \leqslant n \leqslant 5)$ and the number ω in $\mathbf{Z}[\rho]$ by

$$\omega = (-\rho)^n\omega' \equiv 1 \pmod 3.$$

We have $f \equiv \rho \pmod{\omega}$. Furthermore, let θ be the smallest positive period of the Weierstraß $\wp$-function $\wp(z)$ satisfying $\wp'^{\,2} = 4\wp^3 - 1$. The period lattice of $\wp(z)$ is $\mathbf{Z}[\rho]\theta$. Let S be a 1/3-representative system modulo ω, namely, S is a set of $(p-1)/3$ elements of $\mathbf{Z}[\rho]$ such that the union $S \cup \rho S \cup \rho^2 S \cup \{0\}$ gives a complete representative system modulo ω. By Wilson's theorem, we can define a cube root $\alpha(S)$ of -1 by the congruence

$$\alpha(S) \equiv \prod_{s \in S} s \pmod{\omega}.$$

Also, since $\wp(\rho z) = \rho\wp(z)$ and $\prod_{a=1}^{p-1} \wp(\frac{a\theta}{\omega}) = \frac{1}{\omega^2}$ (cf. for example, [2]), we may define a cube root $\zeta(S)$ of unity by the identity

$$\omega \prod_{s \in S} \wp\left(\frac{s\theta}{\omega}\right) = \zeta(S)\sqrt[3]{\omega} \quad \left(|\arg \sqrt[3]{\omega}\,| < \frac{\pi}{3}\right).$$

Here, we agree that $-\pi \leqslant \arg z < \pi$ for the argument $\arg z$ of a non-zero number z in $\mathbf{C}$.

Now, by Matthews [4], we have

$$\tau_3(\omega) = p^{1/3}\omega\alpha(S)^{-1} \prod_{s \in S} \wp\left(\frac{s\theta}{\omega}\right)$$

and hence,

$$\tau_3(\omega) = p^{1/3}\alpha(S)^{-1}\zeta(S)\sqrt[3]{\omega}. \tag{2}$$

Theorem 2. *The subset R_p of $\mathbf{Z}$ defined by (1) is a 1/3-representative system modulo ω and we have*

$$\zeta(R_p) = \rho^{z(c,d)},$$

where the integer $z(c,d) = z(c \bmod 9,\ d \bmod 9)$ is defined by Table 1.

A proof of the above theorem will be given in the next section. Let us put $S = R_p$ in the formula (2) for $\tau_3(\omega)$. By the definition of a_p, we see that

$$\alpha(R_p) \equiv \prod_{r \in R_p} r \equiv -f^{a_p} \equiv -\rho^{a_p} \pmod{\omega}$$

and

$$\alpha(R_p) = -\rho^{a_p}.$$

Hence,

$$\tau_3(\omega) = \xi_p p^{1/3}\sqrt[3]{\omega}$$

Table 2
The values of n and $\arg\omega - \arg\omega'$.

(c,d) mod 3	$(1,0)$	$(1,2)$	$(2,0)$	$(2,1)$	$(0,1)$	$(0,2)$
n	0	5	3	2	1	4
$\arg\omega - \arg\omega'$	0	$\frac{\pi}{3}$	$-\pi$	$-\frac{2\pi}{3}$	$-\frac{\pi}{3}$	$\frac{2\pi}{3}$

with

$$\xi_p = -\rho^{z(c,d)-a_p}.$$

For the interval containing $g_3(p) = \tau_3(\omega) + \overline{\tau_3(\omega)}$, we have, in case $\arg\omega > 0$,

$$\begin{cases} g_3(p) \in (-2\sqrt{p}, -\sqrt{p}\,) & \text{if } \xi_p = -1, \\ g_3(p) \in (-\sqrt{p}, \sqrt{p}\,) & \text{if } \xi_p = -\rho^{-1}, \\ g_3(p) \in (\sqrt{p}, 2\sqrt{p}\,) & \text{if } \xi_p = -\rho. \end{cases}$$

Also, in case $\arg\omega < 0$, we have

$$\begin{cases} g_3(p) \in (-2\sqrt{p}, -\sqrt{p}\,) & \text{if } \xi_p = -1, \\ g_3(p) \in (-\sqrt{p}, \sqrt{p}\,) & \text{if } \xi_p = -\rho, \\ g_3(p) \in (\sqrt{p}, 2\sqrt{p}\,) & \text{if } \xi_p = -\rho^{-1}. \end{cases}$$

The value of n is determined by the condition

$$(-\rho)^{-n} \equiv \omega' \equiv c - d\rho^{-1} \pmod 3$$

and we can see it is determined by the classes of c and d modulo 3 as in Table 2. Note that $\omega = (-\rho)^n\omega'$ and $0 < \arg\omega' < \pi/6$. Then, we see that

$$\begin{cases} \arg\omega > 0 & \text{if } (c,d) \equiv (1,0),\ (1,2),\ (0,2) \pmod 3, \\ \arg\omega < 0 & \text{if } (c,d) \equiv (2,0),\ (2,1),\ (0,1) \pmod 3. \end{cases}$$

This concludes the proof of Theorem 1. □

We remark here that the value of $\arg\omega - \arg\omega'$ is determined by the value of n as in Table 2.

3. Proof of Theorem 2

Theorem 2 follows from a result of McGettrick [6] concerning division values of elliptic functions if we add some consideration similar to that in [3]. First, we recall the construction of a certain 1/3-representative system S_ω of [3] and quote a result on the determination of $\zeta(S_\omega)$ from [3].

Let $\lambda = \rho - \rho^2 = \sqrt{3}i$ and let

$$D = \{z \in \mathbf{C};\ |z| < |z - \alpha|\ (0 \neq \alpha \in \mathbf{Z}[\rho])\}.$$

The set D is a fundamental domain for $\mathbf{C}/\mathbf{Z}[\rho]$ and is the interior of the regular hexagon with vertices $\frac{(-\rho)^j}{\lambda}$ $(0 \leqslant j \leqslant 5)$. For two numbers a and b in $\mathbf{C}$, we set $\gamma(a,b) = \{at + b(1-t);\ 0 \leqslant t \leqslant 1\}$ and

$$L = \gamma\left(\frac{\omega'}{\lambda}, \frac{c}{\lambda}\right) \cup \gamma\left(\frac{c}{\lambda}, -\frac{c}{\lambda}\right) \cup \gamma\left(-\frac{c}{\lambda}, -\frac{\omega'}{\lambda}\right).$$

Let T_ω be the set of points of ωD lying between L and $-\rho^2 L$. More precisely, we define

$$T_\omega = \left(\bigcup_{0<\psi\leqslant\frac{\pi}{3}} e^{i\psi} \cdot L\right) \cap \omega D - \{0\}.$$

Then, setting

$$S_\omega = T_\omega \cap \mathbf{Z}[\rho],$$

we get a 1/3-representative system S_ω modulo ω. In Fig. 1, we show T_ω in the case of $p = 43$ as the shaded region.

As we have seen in [3, p. 19], we can calculate the cube root $\zeta(S_\omega)$ of unity utilizing a result of McGettrick [6] and get that

$$\begin{aligned}\frac{1}{2\pi}\arg\zeta(S_\omega) \equiv{}& \frac{p}{3\pi}\left(\arg\omega - \arg\omega'\right) + \frac{1}{9}(p-1)\\ &+ \frac{1}{3}\left(\frac{1}{3}cd - q - k - \frac{2}{3}l\right) \pmod 1.\end{aligned} \tag{3}$$

Here, we let

$$q = \begin{cases} [\frac{d}{3}] & \text{if } c + 2d \equiv 1 \pmod 3,\\ [\frac{d+1}{3}] & \text{if } c + 2d \equiv -1 \pmod 3,\end{cases}$$

$$k = \left[\frac{c-1}{3}\right]$$

with $[x]$ denoting the greatest integer not exceeding x. Also, we put

$$l = \begin{cases} 1 & \text{if } c \equiv 0 \pmod 3,\\ 0 & \text{if } c \equiv 1, 2 \pmod 3.\end{cases}$$

Note that the class on the right-hand side of (3) depends only on the classes of c and d modulo 9, cf. the remark on $\arg\omega - \arg\omega'$ made in the last paragraph of the previous section.

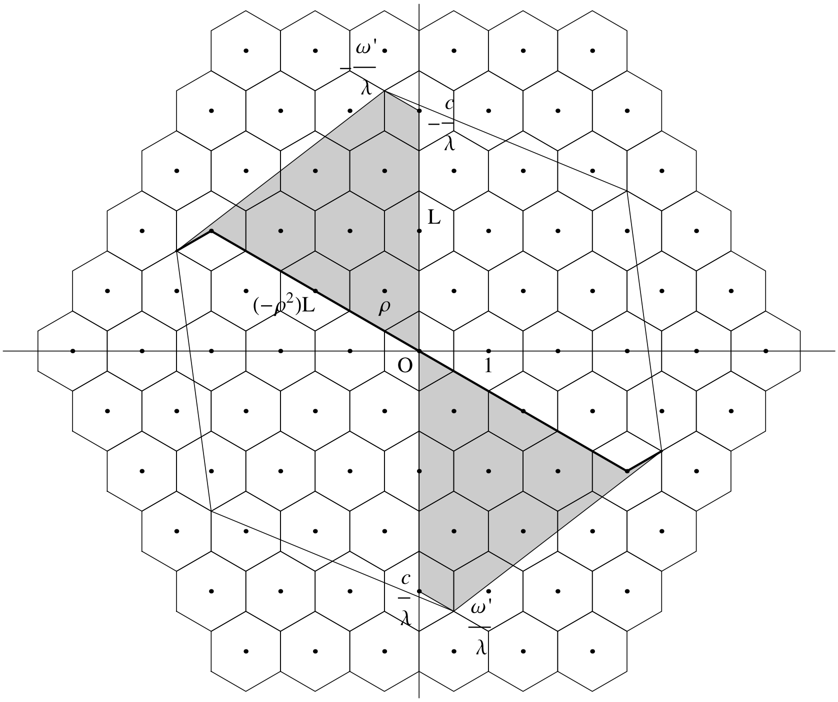

Fig. 1. T_ω in the case of $p = 43$ ($c = 6$, $d = 1$, $\omega = 1 - 6\rho$).

Next, we shall modify the set S_ω and relate it to the set R_p defined by (1). We can express T_ω as the following disjoint union:

$$T_\omega = T_\omega^{(1)} \cup T_\omega^{(2)} \cup \left(-T_\omega^{(1)}\right) \cup \left(-T_\omega^{(2)}\right).$$

Here, we let

$$T_\omega^{(1)} = \left\{-\frac{c}{\lambda}x + \frac{\rho^2 c}{\lambda}y;\ 0 \leqslant x,\ 0 < y,\ x + y < 1\right\},$$
$$T_\omega^{(2)} = \left\{-\frac{c}{\lambda} + \frac{\rho^2 d}{\lambda}x - \frac{\rho(c+d)}{\lambda}y;\ 0 \leqslant x,\ 0 < y,\ x + y < 1\right\}.$$

Note that

$$-\frac{\omega'}{\lambda} = -\frac{c}{\lambda} + \frac{\rho^2 d}{\lambda} \cdot 1 - \frac{\rho(c+d)}{\lambda} \cdot 0,$$
$$\frac{\rho^2\omega'}{\lambda} = -\frac{c}{\lambda} + \frac{\rho^2 d}{\lambda} \cdot 0 - \frac{\rho(c+d)}{\lambda} \cdot 1.$$

Now, put

$$\begin{aligned}T'_\omega &= T_\omega^{(1)} \cup \rho^2\bigl(-T_\omega^{(1)}\bigr) \cup T_\omega^{(2)} \cup \bigl(-T_\omega^{(2)} + \rho\omega'\bigr),\\ S'_\omega &= T'_\omega \cap \mathbf{Z}[\rho].\end{aligned}$$

Then, S'_ω is also a 1/3-representative system modulo ω and T'_ω is the union of two parallelograms

$$T_\omega^{(1)} \cup \rho^2\bigl(-T_\omega^{(1)}\bigr) = \left\{-\frac{c}{\lambda}x - \frac{\rho c}{\lambda}y;\ 0 \leqslant x < 1,\ 0 < y < 1\right\}$$

and

$$T_\omega^{(2)} \cup \bigl(-T_\omega^{(2)} + \rho\omega'\bigr) = \left\{-\frac{c}{\lambda} + \frac{\rho^2 d}{\lambda}x - \frac{\rho(c+d)}{\lambda}y;\ 0 \leqslant x \leqslant 1,\ 0 < y < 1\right\}.$$

Lemma 1. *Let $S_\omega^{(1)} = T_\omega^{(1)} \cap \mathbf{Z}[\rho]$ and define the integer k' by*

$$k' = \begin{cases} -\frac{c}{3} & \text{if } c \equiv 0 \pmod 3,\\ \frac{c-1}{3} & \text{if } c \equiv 1 \pmod 3,\\ 0 & \text{if } c \equiv 2 \pmod 3.\end{cases}$$

Then, we have

$$2 \cdot \bigl|S_\omega^{(1)}\bigr| \equiv k' \pmod 3.$$

We shall prove the lemma later. Since $\wp(\rho z) = \rho\wp(z)$, we have

$$\begin{aligned}\zeta\bigl(S'_\omega\bigr)\sqrt[3]{\omega} = \omega \prod_{s \in S'_\omega} \wp\left(\frac{s\theta}{\omega}\right) &= \rho^{2|S_\omega^{(1)}|} \cdot \omega \prod_{s \in S_\omega} \wp\left(\frac{s\theta}{\omega}\right)\\ &= \rho^{k'} \cdot \zeta(S_\omega)\sqrt[3]{\omega}\end{aligned}$$

and

$$\zeta\bigl(S'_\omega\bigr) = \rho^{k'}\zeta(S_\omega).$$

Therefore, by (3),

$$\begin{aligned}\frac{1}{2\pi}\arg\zeta\bigl(S'_\omega\bigr) &\equiv \frac{k'}{3} + \frac{1}{2\pi}\arg\zeta(S_\omega)\\ &\equiv \frac{p}{3\pi}\bigl(\arg\omega - \arg\omega'\bigr) + \frac{1}{9}(p-1)\\ &\quad + \frac{1}{9}\bigl(cd - 3q - 3k + 3k' - 2l\bigr) \pmod 1.\end{aligned}$$

Because the class k' mod 3 is determined by the class c mod 9, we see that the class $\frac{1}{2\pi}\arg\zeta(S'_\omega)$ mod 1 is determined by the classes of c and d modulo 9. By calculation, we observe that

$$\frac{1}{2\pi}\arg\zeta\bigl(S'_\omega\bigr)\equiv\frac{1}{3}z(c,d)\ (\mathrm{mod}\ 1)$$

and

$$\zeta\bigl(S'_\omega\bigr)=\rho^{z(c,d)}$$

with the integer $z(c,d)$ defined by Table 1.

Finally, every point of $T_\omega^{(1)}\cup\rho^2(-T_\omega^{(1)})$ is of the form

$$-\frac{u}{\lambda}-\frac{\rho v}{\lambda}=\frac{u-2v}{3}+\frac{2u-v}{3}\rho\quad(0\leqslant u<c,\ 0<v<c)$$

and this belongs to $\mathbf{Z}[\rho]$ if and only if

$$u,v\in\mathbf{Z},\quad u+v\equiv 0\ (\mathrm{mod}\ 3).$$

Also, every point of $T_\omega^{(2)}\cup(-T_\omega^{(2)}+\rho\omega')$ is of the form

$$-\frac{c}{\lambda}+\frac{\rho^2u}{\lambda}-\frac{\rho v}{\lambda}=\frac{c-u-2v}{3}+\frac{2c+u-v}{3}\rho$$
$$(0\leqslant u\leqslant d,\ 0<v<c+d)$$

and this belongs to $\mathbf{Z}[\rho]$ if and only if

$$u,v\in\mathbf{Z},\quad u-v-c\equiv 0\ (\mathrm{mod}\ 3).$$

Since, $\rho\equiv f\ (\mathrm{mod}\ \omega)$, we see that there is a one-to-one correspondence modulo ω between the sets S'_ω and R_p. Therefore, R_p is a 1/3-representative system modulo ω and we have that

$$\zeta(R_p)=\zeta\bigl(S'_\omega\bigr)=\rho^{z(c,d)}.$$

This proves Theorem 2. □

Proof of Lemma 1. The number $2|S_\omega^{(1)}|$ is equal to the number of points of $\mathbf{Z}[\rho]$ in $T_\omega^{(1)}\cup\rho^2(-T_\omega^{(1)})$ and, by what we have mentioned above, this number is equal to the number of elements of the set

$$\bigl\{(u,v)\in\mathbf{Z}^2;\ 0\leqslant u\leqslant c-1,\ 1\leqslant v\leqslant c-1,\ u+v\equiv 0\ (\mathrm{mod}\ 3)\bigr\}.$$

We can calculate the number of elements of this set and we get, writing $c = 3c_1 + c_2$ ($c_1, c_2 \in \mathbf{Z}$, $0 \leqslant c_2 \leqslant 2$),

$$2 \cdot \left|S_\omega^{(1)}\right| = \begin{cases} 3c_1^2 - c_1 & \text{if } c_2 = 0, \\ 3c_1^2 + c_1 & \text{if } c_2 = 1, \\ 3c_1^2 + 3c_1 & \text{if } c_2 = 2. \end{cases}$$

This proves Lemma 1. □

4. An example

We describe an example of determination of the interval containing $g_3(p)$ by the use of Theorem 1. Let $p = 43$. We have

$$c = 6, \qquad d = 1, \qquad f = 36$$

and, from Table 1,

$$z(c, d) = z(6, 1) = 1.$$

Also,

$$\begin{aligned} R_{43} = {} & \left\{ \frac{u - 2v}{3} + \frac{2u - v}{3} \cdot 36;\ \begin{array}{l} 0 \leqslant u \leqslant 5,\ 1 \leqslant v \leqslant 5, \\ u + v \equiv 0 \pmod 3 \end{array} \right\} \\ & \cup \left\{ \frac{6 - u - 2v}{3} + \frac{12 + u - v}{3} \cdot 36;\ \begin{array}{l} 0 \leqslant u \leqslant 1,\ 1 \leqslant v \leqslant 6, \\ u - v \equiv 0 \pmod 3 \end{array} \right\} \\ = {} & \{-38, -1, -39, 36, -2, 35, 72, 34, 109, 71\} \\ & \cup \{108, 70, 145, 107\} \end{aligned}$$

and we have

$$\prod_{r \in R_{43}} r \equiv 37 \equiv -f^2 \pmod{43}.$$

It follows that

$$a_{43} = 2 \equiv z(c, d) + 1 \pmod 3$$

and we see from Theorem 1 that

$$g_3(43) \in (\sqrt{43}, 2\sqrt{43}).$$

References

[1] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley–Interscience, New York, 1998.
[2] J.W.S. Cassels, On Kummer sums, Proc. Lond. Math. Soc. (3) 21 (1970) 19–27.
[3] H. Ito, A note on a product formula for the cubic Gauss sum, Acta Arith. 152 (2012) 11–21.
[4] C.R. Matthews, Gauss sums and elliptic functions: I. The Kummer sum, Invent. Math. 52 (1979) 163–185.
[5] C.R. Matthews, Gauss sums and elliptic functions: II. The Quartic sum, Invent. Math. 54 (1979) 23–52.
[6] A.D. McGettrick, A result in the theory of Weierstrass elliptic functions, Proc. Lond. Math. Soc. (3) 25 (1972) 41–54.