A note on a product formula for the cubic Gauss sum

by

HIROSHI ITO (Yokohama)

1. Introduction. For an odd prime number $p$, denote by $(\frac{\cdot}{p})_2$ the quadratic residue symbol of the rational number field $\mathbb{Q}$ and consider the quadratic Gauss sum

$$\tau_2(p) = \sum_{a=1}^{p-1} \left( \frac{a}{p} \right)_2 e^{2\pi i a/p}.$$ 

As is well-known, the product expression

$$(1.1) \quad \tau_2(p) = \prod_{s=1 \atop s \text{ odd}}^{p-1} \left( 2i \sin \frac{2\pi s}{p} \right)$$

holds, and by evaluating the right-hand side, we see that

$$\tau_2(p) = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod{4}, \\ i\sqrt{p}, & p \equiv 3 \pmod{4}. \end{cases}$$

Let $\rho = e^{2\pi i/3}$ and $\varpi$ be the generator of a prime ideal of degree one in $\mathbb{Q}(\rho)$ which satisfies the congruence $\varpi \equiv 1 \pmod{3}$. Let $p$ be the norm of $\varpi$. Denote by $(\frac{\cdot}{\varpi})_3$ the cubic residue symbol of $\mathbb{Q}(\rho)$ and consider the cubic Gauss sum

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

Matthews [6] has proved a product formula for this Gauss sum:

$$(1.2) \quad \tau_3(\varpi) = p^{1/3} \varpi \alpha(S)^{-1} \prod_{s \in S} \varphi \left( \frac{s\theta}{\varpi} \right).$$ 

Here, $\varphi(z)$ is the Weierstraß $\varphi$-function satisfying $\varphi^2 = 4\varphi^3 - 1$ and we write the period lattice of $\varphi(z)$ as $\mathbb{Z}[\rho]\theta$ ($\theta > 0$). The letter $S$ denotes a

2010 Mathematics Subject Classification: Primary 11L05; Secondary 11G05, 11G16.

Key words and phrases: Gauss sums, elliptic functions.
1/3-representative system modulo $\varpi$, that is, $S$ is a set of $(p-1)/3$ elements of $\mathbb{Z}[\rho]$ such that the numbers
\[ s, \rho s, \rho^2 s \quad (s \in S), \]
together with 0, form a complete representative system modulo $\varpi$. Finally, we let $\alpha(S)$ be the cube root of $-1$ which satisfies the congruence
\[ \alpha(S) \equiv \prod_{s \in S} s \mod \varpi. \]
This is possible by Wilson’s theorem.

The formula (1.2) is an analogue of (1.1) for the cubic Gauss sum $\tau_3(\varpi)$. In (1.1), the evaluation of the product of division values of the trigonometric function leads to the determination of the Gauss sum $\tau_2(p)$. We have a similar product of division values of the elliptic function $\wp(z)$ in (1.2) and hence it will be natural to ask what kind of knowledge we can get by “evaluating” this product. Now, for cubic Gauss sums $\tau_3(\varpi)$, the arguments of the sums $\tau_3(\varpi)$ distribute uniformly, as has been proved by Heath-Brown and Patterson [3] independently of (1.2) (cf. (3.3) in Section 3 for a precise statement). Looking at the formula (1.2) again, we may have the following expectation. Namely, if we assign to every $\varpi$ a 1/3-representative system $S_{\varpi}$ modulo $\varpi$ which consists of lattice points in a plane region with a simple shape, then the value of $\prod_{s \in S_{\varpi}} \wp(s\theta/\varpi)$ will be expressed as a quantity of elementary nature. And then, the uniform distribution of the arguments of $\tau_3(\varpi)$ will be understood as some uniformity of the distribution of $\alpha(S_{\varpi})$.

In this note, the author would like to consider to what extent the above expectation can be fulfilled. The main results are two theorems in the next section. Theorem 1 provides a criterion on the usability of $S_{\varpi}$ for our purpose in terms of the nature of the product $\prod_{s \in S_{\varpi}} \wp(s\theta/\varpi)$. The discussion here is rather formal. We then proceed to take $S_{\varpi}$ satisfying the condition in Theorem 1 as a set of lattice points in a plane region and we try to make the construction of the region as simple as possible. An example of the choice of $S_{\varpi}$ is given in Theorem 2 by the use of a result of McGettrick [7] on division values of elliptic functions. We prove Theorem 1 in Section 3 and Theorem 2 in Section 4.

2. Main results. Throughout this note, we shall denote by $\varpi$ the generator of a prime ideal of degree one in $\mathbb{Q}(\rho)$ satisfying the congruence $\varpi \equiv 1 \mod 3$. We normalize the argument $\arg z$ of a complex number $z$ ($z \neq 0$) by $-\pi \leq \arg z < \pi$. For real numbers $X, \psi_1$ and $\psi_2$ ($X > 0, -\pi \leq \psi_1 < \psi_2 \leq \pi$) and integers $a$ and $\mu$ in $\mathbb{Z}[\rho]$, we put
\[ P(X; \psi_1, \psi_2; a, \mu) = \{ \varpi : N\varpi \leq X, \psi_1 \leq \arg \varpi < \psi_2, \varpi \equiv a \mod \mu \}, \]
where $N\varpi$ denotes the norm of $\varpi$. For a real number $x$, let $[x]$ be the greatest integer not exceeding $x$.

**Theorem 1.** Suppose that we have chosen a $1/3$-representative system $S_\varpi$ modulo $\varpi$ for every $\varpi$ and the following condition is satisfied: there exist an integer $\nu$ in $\mathbb{Z}[\rho]$ and a natural number $K$ such that the cube root $\zeta_\varpi$ of unity determined by the equation

$$
\varpi \prod_{s \in S_\varpi} \varphi \left( \frac{s\theta}{\varpi} \right) = \zeta_\varpi \sqrt[3]{\varpi} \quad (|\arg \sqrt[3]{\varpi}| < \pi/3)
$$

depends only on the class $\varpi \mod \nu$ and the integer $\left[ \frac{K}{\varpi} \arg \varpi \right]$. Then, for every pair of integers $\mu$ and $a$ in $\mathbb{Z}[\rho]$ ($\mu \neq 0$, $\mu \equiv 0 \pmod{3}$), $(a, \mu) = 1$, $a \equiv 1 \pmod{3}$ and every pair of real numbers $\psi_1$ and $\psi_2$ ($-\pi \leq \psi_1 < \psi_2 \leq \pi$), we have, for $j = 0, 1, 2$,

$$
\lim_{X \to \infty} \frac{\# \{ \varpi \in P(X; \psi_1, \psi_2; a, \mu) : \alpha(S_\varpi) = -\rho^j \}}{\# P(X; \psi_1, \psi_2; a, \mu)} = \frac{1}{3}.
$$

In [1, 3], the fact that $\zeta_3^3 = 1$ follows from a formula due to Eisenstein (cf., for example, Cassels [1, (3.4)]). From the proof of Theorem 1, we see that the uniformity (2.2) of the distribution of $\alpha(S_\varpi)$ is equivalent to the uniform distribution of the arguments of $\tau_3(\varpi)$ proved in [3].

We shall next construct $S_\varpi$ satisfying the condition of Theorem 1 as a set of lattice points in a plane region. Put $\lambda = \rho - \rho^2 = \sqrt{3}i$ and

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

The set $D$ is a fundamental domain for $\mathbb{C}/\mathbb{Z}[\rho]$ and is the interior of the regular hexagon with vertices $(-\rho)^j/\lambda$ ($0 \leq j \leq 5$). For each $\varpi$, we take the integer $n$ ($0 \leq n \leq 5$) and the number $\varpi'$ such that

$$\varpi = (-\rho)^n \varpi', \quad |\arg \varpi'| < \pi/6.$$ 

Moreover let $c$, $d$ and $\sigma$ be the integers such that

$$\varpi' = c - d\rho^\sigma \quad (0 < d < c, \ \sigma = \pm 1).$$

For two points $a$ and $b$ in $\mathbb{C}$, we let $\gamma(a, b) = \{ at + b(1 - t) : 0 \leq t \leq 1 \}$. Now put $L = \gamma(\varpi'/\lambda, c/\lambda) \cup \gamma(c/\lambda, -c/\lambda) \cup \gamma(-c/\lambda, -\varpi'/\lambda)$ and let $T_\varpi$ be the set of points of $\varpi D$ lying between $L$ and $-\rho^2 L$. More precisely,

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

Then, setting $S_\varpi = T_\varpi \cap \mathbb{Z}[\rho]$, we get a $1/3$-representative system $S_\varpi$ modulo $\varpi$. We can prove the following theorem by using a result in [7].

**Theorem 2.** Let $\zeta_\varpi$ be the cube root of unity determined by (2.1), where the $1/3$-representative system $S_\varpi$ is chosen as explained above. Then $\zeta_\varpi$ depends only on the class $\varpi \mod 9$ and the integer $\left[ (6/\pi) \arg \varpi \right]$. 

Though the construction of $S_\varpi$ becomes simpler if we use the diagonal line $\gamma(\varpi'/\lambda, -\varpi'/\lambda)$ instead of $L$, there seems to be little possibility that the $1/3$-representative system modulo $\varpi$ thus constructed satisfies the condition stated in Theorem 1 (cf. Remark 2 in Section 4).

Combining the above two theorems, we get the uniformity \([2.2]\) of the distribution of $\alpha(S_\varpi)$ for our $S_\varpi$. Here, we would like to call the reader’s attention to a problem of a similar type. Let $p$ be a prime number with $p \equiv 3 \pmod{4}$. Then, by Wilson’s theorem,

$$\left(\frac{p-1}{2}!\right)^2 \equiv -(p-1)! \equiv 1 \pmod{p},$$

and hence,

$$\frac{p-1}{2}! \equiv \pm 1 \pmod{p}.$$ 

One asks if $+1$ and $-1$ occur with the same frequency. As far as the author knows, this problem is open.

3. The distribution of $\alpha(S_\varpi)$. We prove Theorem 1 in this section. Keeping the notation already introduced, we further put

$$P(X; a, \mu) = P(X; -\pi, \pi; a, \mu), \quad P(X) = P(X; 1, 3).$$

By a result of Mitsui [8], we have

$$\lim_{X \to \infty} \frac{\#P(X; \psi_1, \psi_2; a, \mu)}{\#P(X)} = \frac{\psi_2 - \psi_1}{2\pi} \cdot \frac{6}{\#(\mathbb{Z}[\rho]/\mathbb{Z}[\rho]\mu)^{\times}}$$

if $\mu \not= 0, \mu \equiv 0 \pmod{3}$, $(a, \mu) = 1$ and $a \equiv 1 \pmod{3}$. Here, $(\mathbb{Z}[\rho]/\mathbb{Z}[\rho]\mu)^{\times}$ is the reduced residue class group modulo $\mu$. For intervals in $\mathbb{R}$, we use the notation

$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}.$$ 

Note that, since $\tau_3(\varpi)^3 = -p\varpi$, the conditions

$$\arg \tau_3(\varpi) \in \bigcup_{j=1,3,5} \left(\frac{1}{3}[\psi_1, \psi_2] + \frac{\pi}{3}j\right) \pmod{2\pi}$$

and $\arg \varpi \in [\psi_1, \psi_2)$ are equivalent to each other. Here, “$(\text{mod } 2\pi)$” means that we see both sides of “$\in$” as the images of the natural projection $\mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$.

The next lemma is a reformulation of a result in [3] on the distribution of the arguments of the cubic Gauss sums $\tau_3(\varpi)$.

**Lemma 1.** Let $\mu$ and $a$ be integers in $\mathbb{Z}[\rho]$ such that $\mu \not= 0$, $\mu \equiv 0 \pmod{3}$, $(a, \mu) = 1$ and $a \equiv 1 \pmod{3}$. Let $\psi_1$ and $\psi_2$ be real numbers with
\(-\pi \leq \psi_1 < \psi_2 \leq \pi\). Then, for each \(j\) \((j = 1, 3, 5)\), we have

\[
\lim_{X \to \infty} \frac{\#\{ \varpi \in P(X; \psi_1, \psi_2; a, \mu) : \arg \tau_3(\varpi) \in \frac{1}{3}[\psi_1, \psi_2] + \frac{\pi}{3} j \text{ (mod } 2\pi)\}}{\#P(X; \psi_1, \psi_2; a, \mu)} = \frac{1}{3}.
\]

**Proof.** By [3, p. 113], we know that

\[
\lim_{X \to \infty} \frac{\#\{ \varpi \in P(X; a, \mu) : \arg \tau_3(\varpi) \in [\xi_1, \xi_2) \text{ (mod } 2\pi)\}}{\#P(X; a, \mu)} = \frac{\xi_2 - \xi_1}{2\pi}
\]

for every \(\xi_1\) and \(\xi_2\) \((0 \leq \xi_2 - \xi_1 \leq 2\pi)\). By the remark before Lemma 1, the condition “\(\varpi \in P(X; \psi_1, \psi_2; a, \mu)\)” in (3.2) can be replaced by the condition “\(\varpi \in P(X; a, \mu)\)”.

Hence, from (3.1) and (3.3) we see that the left hand side of (3.2) equals

\[
\lim_{X \to \infty} \left[ \frac{\#\{ \varpi \in P(X; a, \mu) : \arg \tau_3(\varpi) \in \frac{1}{3}[\psi_1, \psi_2] + \frac{\pi}{3} j \text{ (mod } 2\pi)\}}{\#P(X; a, \mu)} \right] 
\]

\[
\times \frac{\#P(X; a, \mu)}{\#P(X; \psi_1, \psi_2; a, \mu)} = \frac{1}{3} (\psi_2 - \psi_1) \cdot \frac{2\pi}{\psi_2 - \psi_1} = \frac{1}{3}.
\]

This proves Lemma 1.

Now, suppose that we have assigned to each \(\varpi\) a 1/3-representative system \(S_{\varpi}\) modulo \(\varpi\) and the condition in Theorem 1 is satisfied. Fix a number \(\nu\) of \(\mathbb{Z}[\rho]\) and a positive integer \(K\) appearing in the condition. We may assume without loss of generality that \(\nu \equiv 0 \text{ (mod } 3)\) and \(K \equiv 0 \text{ (mod } 2)\).

Put, for each integer \(J\) \((-K/2 \leq J \leq K/2 - 1)\),

\[
I_J = \left[ \frac{2\pi}{K} J, \frac{2\pi}{K} (J + 1) \right).
\]

**Lemma 2.** Let \(\nu\) and \(K\) be as above and let \(\mu\) and \(a\) be integers in \(\mathbb{Z}[\rho]\) with \(\mu \neq 0\), \(\mu \equiv 0 \text{ (mod } \nu)\), \((a, \mu) = 1\) and \(a \equiv 1 \text{ (mod } 3)\). Then, for every pair of real numbers \(\psi_1\) and \(\psi_2\) \((\psi_1 < \psi_2)\) such that \([\psi_1, \psi_2) \subset I_J\) for some \(J\) \((-K/2 \leq J \leq K/2 - 1)\), we have (2.2) for \(j = 0, 1, 2\).

**Proof.** Let \(\varpi \in P(X; \psi_1, \psi_2; a, \mu)\). Take \(S = S_{\varpi}\) in (1.2) and use (2.1) for the product of division values of \(\varphi(z)\). Then we see that

\[
\tau_3(\varpi) = \alpha(S_{\varpi})^{-1} \zeta_{\varpi} \sqrt[3]{\varpi} \rho^{1/3}.
\]

Note that \(|\sqrt[3]{\varpi}| < \pi/3\) and that \(\zeta_{\varpi}\) does not depend on \(\varpi\) as long as \(\varpi\) belongs to \(P(X; \psi_1, \psi_2; a, \mu)\). Write \(\zeta_{\varpi} = \rho^h\) \((h \in \mathbb{Z})\). If \(\alpha(S_{\varpi}) = -\rho^j\), we
have
\[
\arg \tau_3(\varpi) = \arg \{-\rho^{-j+h} \sqrt{\varpi}\} \\
\equiv \frac{\pi}{3} (3 - 2j + 2h) + \frac{1}{3} \arg \varpi \pmod{2\pi},
\]
and hence
\[
\arg \tau_3(\varpi) \in \frac{1}{3} [\psi_1, \psi_2] + \frac{\pi}{3} (3 - 2j + 2h) \pmod{2\pi}.
\]
Conversely, if \(\arg \tau_3(\varpi)\) belongs to the above interval, then \(\alpha(S_\varpi) = -\rho^j\).

The assertion of Lemma 2 then follows from Lemma 1.

We now prove Theorem 1. Suppose that the conditions on \(\mu, a, \psi_1\) and \(\psi_2\) are weakened from the conditions in Lemma 2 to those of Theorem 1. We must show that (2.2) still holds. Now, take an integer \(\mu' \neq 0\) in \(\mathbb{Z}[\rho]\) which is divisible by both \(\mu\) and \(\nu\). Then we have a decomposition
\[
P(X; \psi_1, \psi_2; a, \mu) = \bigcup_{a', \psi_1', \psi_2'} P(X; \psi_1', \psi_2'; a', \mu') \cup \{\text{a finite number of } \varpi\text{'s}\},
\]
where the union on the right hand side is disjoint and the numbers \(a', \psi_1'\) and \(\psi_2'\) satisfy the condition that \((a', \mu') = 1, a' \equiv 1 \pmod{3}\) and \([\psi_1', \psi_2'] \subset I_J\) for some \(J\). From Lemma 2 we see that, for each \(j = 0, 1, 2\),
\[
\lim_{X \to \infty} \frac{\#\{\varpi \in P(X; \psi_1, \psi_2; a, \mu) : \alpha(S_\varpi) = -\rho^j\}}{\#P(X; \psi_1, \psi_2; a, \mu)} = \frac{1}{3} \sum_{a', \psi_1', \psi_2'} \lim_{X \to \infty} \frac{\#P(X; \psi_1', \psi_2'; a', \mu')}{\#P(X; \psi_1, \psi_2; a, \mu)} = \frac{1}{3}.
\]
This proves Theorem 1.

Tracing the above argument backward, we may deduce (3.3) for every \(\mu, a, \xi_1\) and \(\xi_2\) with \(\mu \neq 0, \mu \equiv 0 \pmod{3}\), \((a, \mu) = 1, a \equiv 1 \pmod{3}\) and \(0 \leq \xi_2 - \xi_1 \leq 2\pi\) from the assumption that (2.2) holds for every \(\mu, a, \psi_1, \psi_2\) and \(j\) with \(\mu \neq 0, \mu \equiv 0 \pmod{3}\), \((a, \mu) = 1, a \equiv 1 \pmod{3}\), \(-\pi \leq \psi_1 < \psi_2 \leq \pi\) and \(j = 0, 1, 2\). In this sense, (2.2) is equivalent to the uniform distribution of the arguments of the cubic Gauss sums \(\tau_3(\varpi)\).

4. The product of division values of \(\wp(z)\). In this section, we prove Theorem 2 using a result of McGettrick [7]. First, we recall his result. Let,
as before, \( \varpi \) be the generator of a prime ideal of degree one in \( \mathbb{Z}[\rho] \) with \( \varpi \equiv 1 \pmod{3} \) and put \( J = \left\lfloor (6/\pi) \arg \varpi \right\rfloor \) \((-6 \leq J \leq 5)\). We have
\[
\frac{\pi}{6} J \leq \arg \varpi < \frac{\pi}{6} (J + 1).
\]
Take the integers \( n, \sigma, c, d \) and the number \( \varpi' \) in \( \mathbb{Z}[\rho] \) satisfying (2.3) and (2.4). Set \( \varphi' = \arg \varpi' \). Note that the condition \( \varphi' > 0 \) is equivalent to the condition \( \sigma = -1 \) and further to the condition \( J \equiv 0 \pmod{2} \).

Let \( \wp(z) \) be the Weierstraß \( \wp \)-function associated to the lattice \( \mathbb{Z}[\rho] \varpi \), that is,
\[
\wp(z) = 1 + \sum_{0 \neq w \in \mathbb{Z}[\rho] \varpi} \frac{1}{(z-w)^2} - \frac{1}{w^2}.
\]
Then
\[
(4.1) \quad \wp(z) = \theta^2 \varpi^{-2} \wp\left(\frac{z\theta}{\varpi}\right).
\]

Following [7], we define a function \( \log \wp(z) \) on \( \mathbb{C} - (1/\lambda)\mathbb{Z}[\rho] \varpi \) as follows. Recall the path \( L \) defined in Section 2 and consider the following domain:
\[
\{ z \in \mathbb{C} : z \text{ is not congruent to a point of } L \text{ modulo } \mathbb{Z}[\rho] \varpi \}.
\]
First, we define \( \log \wp(z) \) on this domain to be the branch of the logarithm of \( \wp(z) \) which is determined by the condition that
\[
\lim_{\varepsilon \to +0} \text{Im}(\log \wp(\varepsilon)) = 0.
\]
The function \( \log \wp(z) \) is a single-valued regular function with period \( \mathbb{Z}[\rho] \varpi \). Next, for a point \( z \) on \( L \) different from 0 or \( \pm \varpi'/\lambda \), we let
\[
(4.2) \quad \log \wp(z) = \begin{cases} \lim_{\varepsilon \to +0} \log \wp(z + \varepsilon), & \text{Im } z > 0, \\ \lim_{\varepsilon \to +0} \log \wp(z - \varepsilon), & \text{Im } z < 0. \end{cases}
\]
Furthermore, if a point \( z' \) is congruent modulo \( \mathbb{Z}[\rho] \varpi \) to such a point \( z \), we set \( \log \wp(z') = \log \wp(z) \). Thus we get a function \( \log \wp(z) \) on \( \mathbb{C} - (1/\lambda)\mathbb{Z}[\rho] \varpi \) which is periodic with respect to \( \mathbb{Z}[\rho] \varpi \). The following is the main theorem of [7].

**Theorem 3** (McGettrick [7]). We have
\[
\sum_{0 \neq a \in \mathbb{Z}[\rho]/\mathbb{Z}[\rho] \varpi} \text{Im}(\log \wp(a)) = -2p\varphi' + \text{sgn } \varphi' \cdot \frac{2}{3} \pi cd - 2\pi q - 2\pi k - \frac{4}{3} \pi l.
\]
Here, \( q, k \) and \( l \) are integers defined as follows:
\[
q = \#\{b \in \gamma(\varpi'/\lambda, c/\lambda) \cap \mathbb{Z}[\rho] : b \neq \varpi'/\lambda, c/\lambda\},
\]
\[
k = \#\{b \in \gamma(c/\lambda, 0) \cap \mathbb{Z}[\rho] : b \neq c/\lambda, 0\},
\]
\[
l = \begin{cases} 
 1 & \text{if } c \equiv 0 \pmod{3} \text{ and } \varphi' > 0, \\
 2 & \text{if } c \equiv 0 \pmod{3} \text{ and } \varphi' < 0, \\
 0 & \text{if } c \equiv 1, 2 \pmod{3}.
\end{cases}
\]

Note that the points \( A_2, B, B' \) and \( A_5 \) in \( \mathbb{T} \) coincide with our points 
\(-\varpi'/\lambda, -c/\lambda, c/\lambda \) and \( \varpi'/\lambda \) respectively.

Since \( \varphi_*(\rho z) = \rho^{-2} \varphi_*(z) \), there exists an integer \( g(z) \) such that
\[
(4.3) \quad \log \varphi_*(\rho z) = \log \varphi_*(z) - \frac{4}{3} \pi i + 2\pi i g(z)
\]
for every point \( z \) of \( \mathbb{C} - (1/\lambda)\mathbb{Z}[\rho]\varpi \). Clearly, \( g(z) \) is periodic with respect to \( \mathbb{Z}[\rho]\varpi \). We prepare a lemma concerning \( g(z) \).

**Lemma 3.** For every point \( z \) in \( T_{\varpi} \), we have
\[
g(z) = 0, \quad g(\rho z) = 1, \quad g(\rho^2 z) = 1.
\]

**Proof.** Since \( \log \varphi_*(\rho z) \) is continuous on the domain
\[
\{z \in \mathbb{C} : z \text{ is not congruent to a point of } \rho^{-1} L \text{ modulo } \mathbb{Z}[\rho]\varpi\},
\]
the function \( g(z) \) is continuous on the set
\[
\{z \in \mathbb{C} : z \text{ is not congruent to a point of } L \cup \rho^{-1} L \text{ modulo } \mathbb{Z}[\rho]\varpi\},
\]
and hence it is constant on every connected component of this set. Note also that the values of \( g(z) \) on the boundary of each connected component are determined from (4.2). Then, we see that \( g(z), g(\rho z) \) and \( g(\rho^2 z) \) are constant and \( g(\rho z) = g(\rho^2 z) \) on \( T_{\varpi} \). Put \( g(z) = b_0 \) and \( g(\rho z) = g(\rho^2 z) = b_1 \) (\( z \in T_{\varpi} \)).

Now, if \( z \) is a point in \( \mathbb{C} - (1/\lambda)\mathbb{Z}[\rho]\varpi \), we see, by (4.3),
\[
0 = \log \varphi_*(\rho^3 z) - \log \varphi_*(z)
= (\log \varphi_*(\rho^3 z) - \log \varphi_*(\rho^2 z)) + (\log \varphi_*(\rho^2 z) - \log \varphi_*(\rho z))
+ (\log \varphi_*(\rho z) - \log \varphi_*(z))
= -4\pi i + 2\pi i (g(\rho^2 z) + g(\rho z) + g(z)).
\]
Hence,
\[
g(z) + g(\rho z) + g(\rho^2 z) = 2
\]
and \( b_0 + 2b_1 = 2 \). If a point \( z \) near to the origin moves around the origin counter-clockwise, the value of \( \log \varphi_*(z) \) increases by \( 2\pi i \) when \( z \) crosses \( L \), and the value of \( \log \varphi_*(\rho z) \) increases by \( 2\pi i \) when \( z \) crosses \( \rho^{-1} L \). Therefore, if \( z \) is in the interior of \( T_{\varpi} \) and near to the origin, (4.3) yields
\[
g(\rho z) = g(z) + 1
\]
and hence \( b_1 = b_0 + 1 \). It follows that \( b_0 = 0 \) and \( b_1 = 1 \). This proves Lemma 3.

Let us now prove Theorem 2. Let \( \zeta_\varpi \) be defined by (2.1). From (4.1) we have

\[
\prod_{s \in S_\varpi} \varphi_*(s) = \theta^{2(p-1)/3} \zeta_\varpi \sqrt{\varpi}^{-2p},
\]

and hence, setting

\[
Y = \sum_{s \in S_\varpi} \text{Im}(\log \varphi_*(s)),
\]

we see from \( \arg \sqrt{\varpi} = \frac{1}{3} \arg \varpi \) that

\[
\arg \zeta_\varpi \equiv Y + 2p \cdot \frac{3}{3} \arg \varpi \pmod{2\pi}.
\]

We also deduce, by the periodicity of \( \log \varphi_*(z) \) with respect to \( \mathbb{Z}[\rho] \varpi \) and by Lemma 3, that

\[
\sum_{0 \neq a \in \mathbb{Z}[\rho]/\mathbb{Z}[\rho] \varpi} \text{Im}(\log \varphi_*(a)) = \sum_{j=0}^{2} \sum_{s \in S_\varpi} \text{Im}(\log \varphi_*(\rho^j s)) = 3Y - 2\pi \cdot \frac{p - 1}{3}.
\]

Therefore, the value of \( Y \) can be determined from Theorem 3 and we see that

\[
\arg \zeta_\varpi \equiv \frac{2p}{3} \arg \varpi + \frac{2\pi}{9} (p - 1)
\]

\[
+ \frac{1}{3} \left( -2p\varphi' + \text{sgn} \varphi' \cdot \frac{2}{3} \pi cd - 2\pi q - 2\pi k - \frac{4}{3} \pi l \right)
\]

\[
\equiv \frac{2p}{3} (\arg \varpi - \varphi') + \frac{2\pi}{9} (p - 1)
\]

\[
+ \frac{1}{3} \left( \text{sgn} \varphi' \cdot \frac{2}{3} \pi cd - 2\pi q - 2\pi k - \frac{4}{3} \pi l \right) \pmod{2\pi}.
\]

Now it suffices to show that each factor appearing above depends only on the class \( \varpi \mod 9 \) and the integer \( J \).

First, by (2.3), \( \arg \varpi - \varphi' = \arg \varpi - \arg \varphi' \) is determined by \( n \), and \( n \) is clearly determined by \( J \). Next, since \( p = \varpi \varpi' \), \( p \mod 9 \) is determined by \( \varpi \mod 9 \). Moreover, since

\[
c - d\rho^\sigma = (-\rho)^{-n} \varpi
\]

from (2.3) and (2.4), the classes \( c \mod 9 \) and \( d \mod 9 \) are determined by the class \( \varpi \mod 9 \) and the integers \( \sigma \) and \( n \), and hence by \( \varpi \mod 9 \) and \( J \) (cf. the remark in the first paragraph of this section). Thus, \( \text{sgn} \varphi' \cdot (2\pi/9) cd \mod 2\pi \).
is determined by $\varpi \mod 9$ and $J$. Now, we see that $l$ is also determined by $\varpi \mod 9$ and $J$, from the definition in Theorem 3. Finally, by Corollary to Theorem 3.1 in [7],

$$q = \begin{cases} 
\left\lfloor \frac{d}{3} \right\rfloor & \text{if } c + 2d \equiv 1 \pmod{3}, \\
\left\lfloor \frac{(d+1)}{3} \right\rfloor & \text{if } c + 2d \equiv -1 \pmod{3},
\end{cases}$$

and

$$k = \left\lfloor \frac{(c-1)}{3} \right\rfloor.$$

Therefore, the classes $q \mod 3$ and $k \mod 3$ are determined by the classes $c \mod 9$ and $d \mod 9$, and hence by the class $\varpi \mod 9$ and the integer $J$. This completes the proof of Theorem 2.

**Remark 1.** In (c) of Corollary to Theorem 3.1 in [7], the conditions “$\varphi' > 0$” and “$\varphi' < 0$” should be exchanged. Note also that the relations

$$u = c + d, \quad v = \begin{cases} 
d & \text{if } \varphi' > 0, \\
c & \text{if } \varphi' < 0
\end{cases}$$

hold between the integers $u, v$ in [7] and our $c, d$, and therefore we have

$$\text{sgn}(u - 2v) = \text{sgn} \varphi'.$$

**Remark 2.** Here we add some remarks on whether we can simplify the construction of our $1/3$-representative system $S_{\varpi}$ modulo $\varpi$. The set $S_{\varpi}$ we use in Theorem 2 is defined as $S_{\varpi} = T_{\varpi} \cap \mathbb{Z} \rho$, where $T_{\varpi}$ is defined by (2.5) using the path $L$ connecting the points $\varpi'/\lambda$, $c/\lambda$, $-c/\lambda$ and $-\varpi'/\lambda$. Let $R_{\varpi}$ be the $1/3$-representative system modulo $\varpi$ constructed in the same way using the segment $\gamma(0, c/\lambda, -\varpi'/\lambda)$ instead of $L$. Then we see that

$$\frac{\prod_{r \in R_{\varpi}} \varphi(r \theta / \varpi)}{\prod_{s \in S_{\varpi}} \varphi(s \theta / \varpi)} = \begin{cases} 
\rho^N & \text{if } \varphi' > 0, \\
\rho^{-(N+M)} & \text{if } \varphi' < 0.
\end{cases}$$

Here, $N$ is the number of points in $\mathbb{Z} \rho$ which lie in the interior of the triangle with vertices $(0, 0), (c/\lambda, \varpi'/\lambda)$, and $M$ denotes the number of points in $\mathbb{Z} \rho$ which lie on the path $\gamma(0, c/\lambda) \cup \gamma(c/\lambda, \varpi'/\lambda)$ and are different from $0$ or $\varpi'/\lambda$.

Since

$$M = \begin{cases} 
q + k + 1 & \text{if } c \equiv 0 \pmod{3}, \\
q + k & \text{if } c \equiv 1, 2 \pmod{3},
\end{cases}$$

where $q$ and $k$ are as in Theorem 3, the class $M \mod 3$ is a simple quantity determined by the class $\varpi \mod 9$ and the integer $J$. However, the class $N \mod 3$ does not seem to be of simple nature. We may, for example, recall the following fact. Let $p$ and $q$ be distinct odd prime numbers and let $n$ be the number of points of $\mathbb{Z}^2$ inside the triangle with vertices $(0, 0), (p/2, 0)$
and \((p/2, q/2)\). Then, for the quadratic residue symbol \(\left(\frac{q}{p}\right)\), we have
\[
\left(\frac{q}{p}\right) = (-1)^n
\]
(cf. Hua [4, p. 40], for example). As \(N\) is the number of lattice points in a triangle some of whose vertices are non-trivial 3-division points, the class \(N \mod 3\) will share some properties with \(n \mod 2\), though it may not be related directly to power residue symbols. Thus the author supposes \(N \mod 3\) is not of very simple nature and does not expect the 1/3-representative system \(R_\wp\) to satisfy the condition described in Theorem 1.

Remark 3. In [2], Habicht considers various modifications of the parallelogram with vertices 0, \(\wp/\lambda\), \(-\rho^2\wp/\lambda\) and \(-\rho\wp\) in order to give a proof of the cubic reciprocity law in \(\mathbb{Q}(\rho)\). Similar modifications are utilized by Kubota [5] in more general situations. Although their treatments are more complicated than our construction of \(T_\wp\) in (2.5), they will be helpful for understanding the point of it and for considering 1/3-representative systems modulo \(\wp\) with the condition in Theorem 1 which are different from our \(S_\wp\) in Theorem 2.

References


Hiroshi Ito
Department of Mathematics
Kanagawa University
Yokohama, Japan 221-8686
E-mail: itouh023@kanagawa-u.ac.jp

Received on 20.9.2010
and in revised form on 4.3.2011