48. An Arithmetical Application of Elliptic Functions to the Theory of Cubic Residues

By Mutsuo WATABE
Department of Mathematics, Gakushuin University, Tokyo

(Communicated by Kunihiko KODAIRA, M. J. A., Oct. 12, 1977)

In 1845, G. Eisenstein [2] proved the biquadratic reciprocity law in $\boldsymbol{Q}(\sqrt{-1})$ using the Gauss lemniscate function, and in 1921, G. Herglotz [4] proved the quadratic reciprocity law in the same field using the complex multiplication of the Weierstrass elliptic functions. In the same line of ideas, K. Shiratani [7] proved the cubic and biquadratic reciprocity laws in the fields $\boldsymbol{Q}(\sqrt{-3})$ and $\boldsymbol{Q}(\sqrt{-1})$ respectively, and he proved in [8] also a complementary law for the 4-th power residues. We also proved it in [9] using the complex multiplication of another elliptic function than that used in [8]. We used namely the Gauss lemniscate function

$$f(z)=sn(2-2i)\omega z \quad \text{with} \quad \omega=\int_0^1 \frac{1}{\sqrt{1-x^4}}dx.$$

In this paper, we shall prove a complementary law for the cubic residues in $\boldsymbol{Q}(\sqrt{-3})$ using the complex multiplication of a certain elliptic function $f(z\,|\,w_1, w_2)$ defined below. It should be noticed that G. Eisenstein obtained in [1] the complementary laws for the cubic residues in a more general setting with elementary methods, as Gauss did for the biquadratic residues in [3].

§ 1. Let $\mathcal{P}(z\,|\,w_1, w_2)$ be the Weierstrass elliptic function with fundamental periods w_1, w_2, with $\mathrm{Im}\,(w_1/w_2)>0$. We consider the following function:

$$(1)\qquad f(z\,|\,w_1, w_2)=\prod_{j=1}^{4}\left(\mathcal{P}(z\,|\,w_1, w_2)-\mathcal{P}\left(\frac{w_j}{3}\,\middle|\,w_1, w_2\right)\right),$$

where $w_3=w_1+w_2$, $w_4=w_1+2w_2$. Then the following divisor equivalence holds:

$$(2)\qquad f(z\,|\,w_1, w_2)\simeq -8(0)+\sum_{j=1}^{4}\left(\frac{w_j}{3}\right)+\sum_{j=1}^{4}\left(\frac{-w_j}{3}\right).$$

The ring $\mathcal{O}$ of integers of Eisenstein's field $\boldsymbol{Q}(\sqrt{-3})$ has a $\boldsymbol{Z}$-basis $[\rho, 1]$, where $\rho=(-1+\sqrt{-3})/2$. We take $(w_1, w_2)=(\rho, 1)$. Then we have easily the complex multiplication formula:

$$(3)\qquad f(\rho z\,|\,\rho, 1)=\rho f(z\,|\,\rho, 1).$$

For brevity, we write $f(z)=f(z\,|\,\rho, 1)$. We consider the integer ν, μ in $\mathcal{O}$ with $(\nu, \mu)=(\nu, 3)=1$. Because of $(\nu, 3)=1$, we have $\mathcal{O}/(\nu)=\{0, M_\nu, \rho M_\nu, \rho^2 M_\nu\}$, where M_ν is a 1/3-system modulo ν as defined in [6]. Since

$(\nu, \mu)=1$, there exists $\beta' \in M_\nu$ such that $\mu\beta \equiv \zeta_\beta^{(\mu)}\beta' \pmod{\nu}$ for arbitrary $\beta \in M_\nu$, where $\zeta_\beta^{(\mu)}$ is a cubic root of unity. Then, by the Gauss lemma [6], the cubic residue symbol $(\mu/\nu)_3$ can be expressed as follows:

$$\left(\frac{\mu}{\nu}\right)_3 = \prod_{\beta \in M_\nu} \zeta_\beta^{(\mu)}. \tag{4}$$

Then, in virtue of (3), (4), we have

$$\left(\frac{\mu}{\nu}\right)_3 = \prod_{\beta \in M_\nu} \frac{f(\mu(\beta/\nu))}{f(\beta/\nu)}. \tag{5}$$

Another simple consequence of (3), (4) is the following complementary law:

$$\left(\frac{\rho}{\nu}\right)_3 = \rho^{(N\nu-1)/3}$$

for $(\nu, 3)=1$.

We want to evaluate

$$\left(\frac{1-\rho}{\nu}\right)_3 = \prod_{\beta \in M_\nu} \frac{f((1-\rho)\beta/\nu)}{f(\beta/\nu)}. \tag{6}$$

From the definition (1) of $f(z)$, we have easily

$$\begin{aligned} \frac{f((1-\rho)z \mid \rho, 1)}{f(z \mid \rho, 1)} &= \frac{(1/(1-\rho)^8) f(z \mid \rho/(1-\rho), 1/(1-\rho))}{f(z \mid \rho, 1)} \\ &\simeq -9\left(\frac{4\rho+1}{9}\right) - 9\left(\frac{\rho+2}{9}\right) + \left(\frac{\rho+2}{9}\right) + \left(\frac{2\rho+2}{9}\right) + \left(\frac{4\rho+8}{9}\right) \\ &+ \left(\frac{2\rho+1}{9}\right) + \left(\frac{4\rho+2}{9}\right) + \left(\frac{8\rho+4}{9}\right) + \left(\frac{\rho+8}{9}\right) + \left(\frac{2\rho+7}{9}\right) \\ &+ \left(\frac{\rho+5}{9}\right) + \left(\frac{7\rho+2}{9}\right) + \left(\frac{8\rho+1}{9}\right) + \left(\frac{5\rho+1}{9}\right) + \left(\frac{4\rho+5}{9}\right) \\ &+ \left(\frac{5\rho+4}{9}\right) + \left(\frac{7\rho+5}{9}\right) + \left(\frac{8\rho+7}{9}\right) + \left(\frac{5\rho+7}{9}\right) + \left(\frac{7\rho+8}{9}\right). \end{aligned} \tag{7}$$

Hence $(f((1-\rho)z \mid \rho, 1))/f(z \mid \rho, 1)$ has neither zero point nor pole on the straight line l joining 0 and $1+\rho$ and on the real axis $\boldsymbol{R}$.

We define the function $g(z \mid \rho, 1)$ as follows:

$$g(z \mid \rho, 1) = \frac{f((1-\rho)z \mid \rho, 1)}{f(z \mid \rho, 1)}. \tag{8}$$

For simplicity, we shall write $g(z)$ for $g(z \mid \rho, 1)$. Then, in virtue of (6), (8), we get

$$\left(\frac{1-\rho}{\nu}\right)_3 = \prod_{\beta \in M_\nu} g\left(\frac{\beta}{\nu}\right). \tag{9}$$

§ 2. It seems to be a very difficult problem to determine the value of $((1-\rho)/\nu)_3$ for arbitrary ν in $\mathcal{O}$ by this method. However, we can determine it for $\nu = a \in \boldsymbol{Z}$, $(a, 3)=1$ as follows. In this case, it is easily seen that we may suppose that $\beta \in M_a$ lies in S or on the line joining 0 and $|a|/3$, where S is the interior of the regular hexagon with the vertices:

$$0,\ \frac{|a|}{3},\ \frac{|a|}{3}(2+\rho),\ \frac{2|a|}{3}(1+\rho),\ \frac{|a|}{3}(1+2\rho),\ \frac{|a|}{3}\rho.^{*)}$$

S is symmetric with respect to l, and the function $g(z)$ has the following properties.

1) If $x \in \boldsymbol{R}$, $\rho g(x)$ is real and positive.

In fact,

$$\overline{\rho g(x)} = \bar{\rho}\frac{f((1-\bar{\rho})x\,|\,\bar{\rho},1)}{f(x\,|\,\bar{\rho},1)} = \frac{1}{\rho}\cdot\frac{f(\rho^{-1}(1-\rho)x\,|\,\rho,1)}{f(x\,|\,\rho,1)}$$
$$= \rho\frac{f((1-\rho)x)}{f(x)} = \rho g(x), \qquad \text{in virtue of (3).}$$

Thus we have $\rho g(x) \in \boldsymbol{R}$.

To show that $\rho g(x) > 0$, we have only to prove $\rho g(0) > 0$, because $g(x)$ has neither zero point nor pole on $\boldsymbol{R}$. Now

$$\rho g(0) = \rho\frac{f((1-\rho)z)}{f(z)}\bigg|_{z=0} = \rho\lim_{z\to 0}\frac{z^8 f((1-\rho)z)}{z^8 f(z)}$$
$$= \frac{\rho}{(1-\rho)^8} = \frac{1}{3^4} > 0.$$

2) $\rho g(z)$ takes real positive values on l; i.e., $\rho g((1+\rho)x) \in \boldsymbol{R}$ and $\rho g((1+\rho)x) > 0$ for $x \in \boldsymbol{R}$.

As $\rho g(0) > 0$, it is sufficient to show $\rho g((1+\rho)x) \in \boldsymbol{R}$. Now we have

$$\overline{\rho g((1+\rho)x)} = \bar{\rho}\frac{f((1-\bar{\rho})(1+\bar{\rho})x\,|\,\bar{\rho},1)}{f((1+\bar{\rho})x\,|\,\bar{\rho},1)} = \frac{1}{\rho}\cdot\frac{f(\rho^{-2}(1-\rho^2)x\,|\,\rho,1)}{f(\rho^{-1}(1+\rho)x\,|\,\rho,1)}$$
$$= \rho\frac{f((1-\rho)(1+\rho)x)}{f((1+\rho)x)} = \rho g((1+\rho)x),$$

again in virtue of (3).

3) If z and $z' \in \boldsymbol{C}$ are symmetric with respect to l, then $g(z') = \overline{\rho g(z)}$.

In fact,

$$\overline{\rho g(z)} = \rho\frac{f((1-\bar{\rho})\bar{z}\,|\,\bar{\rho},1)}{f(\bar{z}\,|\,\bar{\rho},1)} = \frac{f(\rho^2(1-\rho)\bar{z}\,|\,\rho,1)}{f(\bar{z}\,|\,\rho,1)}$$
$$= \rho^2\frac{f((1-\rho)\rho\bar{z})}{f(\bar{z})} = \frac{f((1-\rho)\rho\bar{z})}{\rho f(\bar{z})}$$
$$= \frac{f((1-\rho)\rho\bar{z})}{f(\rho\bar{z})} = \frac{f((1-\rho)z')}{f(z')} = g(z').$$

Now, we shall compute $((1-\rho)/a)_3$ according to (9). As this value is on the unit circle, we have only to take into account the argument of $g(\beta/a)$.

The number of the β's on the line joining 0 and $|a|/3$ is $[|a|/3]$. The argument of $g(\beta/a)$ for these β's is the same as that of $1/\rho$, in virtue of 1) above. There are $[2|a|/3]$ β's on the line joining 0 and $2|a|(1+\rho)/3$, and 2) says that $g(\beta/a)$ for these β's have again the same argument as $1/\rho$.

The total number of β's in M_a is $(Na-1)/3=(a^2-1)/3$ and there remain $(a^2-1)/3-[|a|/3]-[2|a|/3]$ β's in S which are not on l, i.e., $\{(a^2-1)/3-[|a|/3]-[2|a|/3]\}/2$ pairs of β's, lying symmetrically with respect to l. The argument of $g(z)g(z')$ is the same as that of $\rho=1/\rho^2$ in virtue of 3).

Thus we have

$$\left(\frac{1-\rho}{a}\right)_3=\prod_{\beta\in M_a} g\left(\frac{\beta}{a}\right)$$
$$=\left(\frac{1}{\rho}\right)^{[|a|/3]}\left(\frac{1}{\rho}\right)^{[2|a|/3]}\left(\frac{1}{\rho^2}\right)^{\{(a^2-1)/3-[|a|/3]-[2|a|/3]\}/2}$$
$$=\left(\frac{1}{\rho}\right)^{(a^2-1)/3}$$
$$=\begin{cases}\rho^{(a-1)/3} & \text{for } a\equiv 1 \pmod 3,\\ \rho^{2(a+1)/3} & \text{for } a\equiv 2 \pmod 3.\end{cases}$$

Acknowledgment. The author owes remark *) to Professor Hideo Wada, whereas his original choice of M_a was more complicated.

References

[1] G. Eisenstein: Nachtrag zum kubischen Reciprocitätssatz für dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. Kriterien des kubischen Charakters der Zahl 3 und ihrer Teiler. J. für reine u. angew. Math., **28**, 28–35 (1844).
[2] ——: Applications de l'algèbre à l'arithmétique. J. für reine u. angew. Math., **29**, 177–184 (1845).
[3] C. F. Gauss: Theoria residuorum biquadraticorum. II. Göttinger Abh., **7** (1832).
[4] G. Herglotz: Über das quadratische Reziprozitätsgesetz in imaginären quadratischen Zahlkörpern. Leipziger Berichte Math. Phys. Klasse, **73**, 303–310 (1921).
[5] T. Kubota: Some arithmetical applications of an elliptic function. J. für reine u. angew. Math., **214/215**, 141–145 (1964).
[6] H. Reichardt: Eine Bemerkung zur Theorie des Jacobischen Symbols. Math. Nachr., **19**, 171–175 (1958).
[7] K. Shiratani: Die Diskriminante der Weierstraßschen elliptischen Funktionen und das Reziprozitätsgesetz in besonderen imaginärquadratischen Zahlkörpern. Abh. Math. Sem. Univ. Hamburg, **31**, 51–61 (1967).
[8] ——: Über eine Anwendung elliptischer Funktionen auf das biquadratische Reziprozitätsgesetz. J. für reine u. angew. Math., **268/269**, 203–209 (1974).
[9] M. Watabe: An arithmetical application of elliptic functions to the theory of biquadratic residues (to appear in Abh. Math. Sem. Univ. Hamburg).