H. Ito
Nagoya Math. J.
Vol. 118 (1990), 35–43

DEDEKIND SUMS AND QUADRATIC RESIDUE SYMBOLS

HIROSHI ITO

1. In this paper we first prove a simple relation between sums of a certain type and quadratic residue symbols. Then we apply this to Dedekind sums introduced by Sczech [5]. In particular one of his conjectures in [6] will be proved.

2. We will consider congruence relations such as

$$a \equiv b \pmod{2^n}, \quad n \geq 1,$$

where a and b are algebraic (not necessarily integral) numbers. We take this to mean that $a - b = 2^n c$ with a 2-integral algebraic number c. Let K be an algebraic number field of finite degree, $\mathfrak{o}$ its ring of integers, and $\mathfrak{c}$ an integral ideal of K prime to 2. Denote by $N\mathfrak{c}$ the absolute norm of $\mathfrak{c}$. Let f be a map from $\mathfrak{o}/\mathfrak{c} - \{0\}$ to an algebraic number field containing K.

PROPOSITION 1. *If f satisfies the conditions*

$$f(-k) = -f(k), \tag{1}$$

$$f(k) \equiv 1 \pmod 2, \tag{2}$$

then, for every $a \in \mathfrak{o}$ prime to $\mathfrak{c}$,

$$\sum_{\substack{k \in \mathfrak{o}/\mathfrak{c} \\ k \neq 0}} f(ak)f(k) \equiv N\mathfrak{c} + 1 - 2\left(\frac{a}{\mathfrak{c}}\right) \pmod 8 .$$

Here $(a/\mathfrak{c})$ is the quadratic residue symbol of K.

Proof. Let R be a subset of $\mathfrak{o}/\mathfrak{c}$ such that $R \cap (-R) = \varnothing$ and $\mathfrak{o}/\mathfrak{c} = R \cup (-R) \cup \{0\}$. By (1),

$$\begin{aligned} &(f(-ak) - 1)(f(-k) + 1) \\ &= (f(ak) - 1)(f(k) + 1) + 2(f(k) - f(ak)) . \end{aligned}$$

Therefore, from (2),

Received March 22, 1988.
The author was supported by NSF Grant DMS-8601978.

$$(3) \qquad \sum_{\substack{k\in\mathfrak{o}/\mathfrak{c}\\ k\neq 0}} (f(ak)-1)(f(k)+1)$$
$$= 2\sum_{k\in R}\{(f(ak)-1)(f(k)+1)+f(k)-f(ak)\}$$
$$\equiv 2\{\sum_{k\in R} f(k) - \sum_{k\in aR} f(k)\} \qquad (\mathrm{mod}\ 8)\,.$$

Put

$$R_n = R\cap(-1)^n aR\,, \qquad n=0,1\,.$$

Then $R=R_0\cup R_1$ and $aR=R_0\cup(-R_1)$, the unions being disjoint. Therefore, by (1) and (2),

$$2\{\sum_{k\in R} f(k) - \sum_{k\in aR} f(k)\}$$
$$= 4\sum_{k\in R_1} f(k)$$
$$\equiv 4\cdot \sharp R_1 \qquad (\mathrm{mod}\ 8)\,.$$

A generalization of Gauss' lemma (cf. Reichardt [4]) says

$$\sharp R_1 \equiv \frac{1}{2}\left(1-\left(\frac{a}{\mathfrak{c}}\right)\right) \qquad (\mathrm{mod}\ 2)\,.$$

Because (3) is equal to

$$\sum_{\substack{k\in\mathfrak{o}/\mathfrak{c}\\ k\neq 0}} f(ak)f(k) - N\mathfrak{c}+1\,,$$

we have proved the proposition.

Note that, for every odd integer n,

$$n-1\equiv 2(1-(-1)^{(n^2-1)/8})-1+(-1)^{(n-1)/2} \qquad (\mathrm{mod}\ 8)\,.$$

Then the congruence of Proposition 1 can be written as

$$(4) \qquad \sum_{\substack{k\in\mathfrak{o}/\mathfrak{c}\\ k\neq 0}} f(ak)f(k) \equiv 2\left(1-\left(\frac{2a}{\mathfrak{c}}\right)\right)-1+\left(\frac{-1}{\mathfrak{c}}\right) \qquad (\mathrm{mod}\ 8)\,.$$

We also remark that the condition (1) can be replaced by

$$f(-k)\equiv -f(k) \qquad (\mathrm{mod}\ 4)\,.$$

3. EXAMPLE. We apply Proposition 1 with $K=\boldsymbol{Q}$ and $\mathfrak{c}=c\boldsymbol{Z}$, c being an odd integer. Define

$$f_1(k)=2\left(\left(\frac{k}{c}\right)\right), \qquad f_2(k)=i^{-1}\cot\left(\pi\frac{k}{c}\right)$$

for every integer k not divisible by c. Here

$$((x)) = x - [x] - \frac{1}{2}, \qquad x \in \boldsymbol{R} - \boldsymbol{Z}$$

with $[x]$ the greatest integer not exceeding x. It is easy to see that both of f_1 and f_2, viewed as functions on $\boldsymbol{Z}/c\boldsymbol{Z} - \{0\}$, satisfy the conditions for f in Proposition 1. Therefore,

$$\begin{aligned} 4 \sum_{\substack{k \in \boldsymbol{Z}/c\boldsymbol{Z} \\ k \neq 0}} \left(\left(\frac{ak}{c}\right)\right)\left(\left(\frac{k}{c}\right)\right) & \\ &\equiv - \sum_{\substack{k \in \boldsymbol{Z}/c\boldsymbol{Z} \\ k \neq 0}} \cot\left(\pi\frac{ak}{c}\right)\cot\left(\pi\frac{k}{c}\right) \\ &\equiv |c| + 1 - 2\left(\frac{a}{c}\right) \qquad (\mathrm{mod}\ 8)\,. \end{aligned}$$

These congruences are well-known (cf. Rademacher and Grosswald [3]).

4. In the following K denotes an imaginary quadratic field with discriminant D and $\mathfrak{o}$ the ring of integers of K. We fix an embedding of K into $\boldsymbol{C}$. Here we recall some known facts contained in [5]. Let L be a lattice in $\boldsymbol{C}$ such that $\mathfrak{o} = \{m \in \boldsymbol{C};\ mL \subset L\}$ and let, for $z \in \boldsymbol{C}$ and $n \in \boldsymbol{Z}$, $n \geq 0$,

$$E_n(z) = E_n(z, L) = \sum_{\substack{w \in L \\ w+z \neq 0}} (w + z)^{-n}|w + z|^{-s}\Big|_{s=0},$$

where the value at $s = 0$ is to be understood in the sense of analytic continuation. These functions are periodic with respect to L, E_{2n} is even, and E_{2n+1} is odd. They satisfy

$$(5) \qquad \sum_{k \in L/cL} E_n\left(\frac{k}{c} + z\right) = c^n E_n(cz)$$

for every $c \in \mathfrak{o}$, $c \neq 0$. If $\wp(z)$ denotes the Weierstrass $\wp$-function with respect to L, then

$$(6) \qquad \wp(z) = E_2(z) - E_2(0)\,, \qquad z \notin L\,.$$

Let, for $a, c \in \mathfrak{o}$ with $c \neq 0$,

$$D(a, c) = \frac{1}{c} \sum_{k \in L/cL} E_1\left(\frac{ak}{c}\right)E_1\left(\frac{k}{c}\right).$$

Define the map $\Phi = \Phi_L\colon SL(2, \mathfrak{o}) \to \boldsymbol{C}$ by

$$\Phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} E_2(0)I\left(\dfrac{a+d}{c}\right) - D(a, c)\,, & c \neq 0 \\ E_2(0)I\left(\dfrac{b}{d}\right), & c = 0\,, \end{cases}$$

where $I(z) = z - \bar{z}$. Then

$$\Phi(AB) = \Phi(A) + \Phi(B)\,, \qquad A, B \in SL(2, \mathfrak{o})\,,$$

i.e., Φ is a homomorphism. Let g_2 and g_3 be the coefficients of the equation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3\,.$$

If both g_2 and g_3 belong to the field $F = \boldsymbol{Q}(j)$ of the j-invariant $j = 12^3 g_2^3/(g_2^3 - 27g_3^2)$ of L, then the values of $\sqrt{D}^{-1}\Phi$ are contained in F (see also [2]). If g_2 and g_3 are both integral, then the values of 2Φ are integral. Assume $D < -4$. Then $E_2(0) \neq 0$. Since $\Phi_{\lambda L} = \lambda^{-2}\Phi_L$ and

$$(7) \qquad \Phi\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} = \sqrt{D}\,E_2(0) \qquad \text{if} \quad b = \begin{cases} (1 + \sqrt{D})/2, & D \equiv 1 \pmod 4 \\ \sqrt{D}/2, & D \equiv 0 \pmod 4). \end{cases}$$

the values of $\sqrt{D}^{-1}E_2(0)^{-1}\Phi$ depend only on the equivalence class of L and belong to F. In general they are not integral, as is seen from the numerical example for the case $D = -23$ in [6].

5. To apply Proposition 1 to $D(a, c)$, we prepare some congruences for division values of E_1 and E_2. For the rest of the paper we assume

$$D \equiv 1 \pmod 8)\,.$$

Let ψ be a 4-division point of $\boldsymbol{C}/L$ such that

$$2\mathfrak{o} = \{m \in \mathfrak{o};\ 2m\psi = 0\}\,.$$

Put

$$t = \frac{12\wp(2\psi)}{\wp(\psi) - \wp(2\psi)}$$

and

$$T(z) = \frac{\wp(\psi) - \wp(2\psi)}{\wp(z) - \wp(2\psi)}\,.$$

Because 2 splits in K the choice of 2ψ is unique and t is determined by

L up to the sign. We use the following known facts concerning t and $T(z)$ (Fueter [1]).

LEMMA 1. *Both t and $T(\alpha)$ are algebraic integers prime to 2 if $\alpha \notin L$ and $n\alpha \in L$ with an odd integer n.*

LEMMA 2. (i) *If $\alpha \notin L$ and $n\alpha \in L$ with an odd integer n, then $\wp(2\psi)^{-1}\wp(\alpha)$ is algebraic and*

$$\wp(2\psi)^{-1}\wp(\alpha) \equiv 1 \qquad (\bmod 4)\,.$$

(ii) *$\wp(2\psi)^{-1}E_2(0)$ is algebraic and*

$$\wp(2\psi)^{-1}E_2(0) \equiv -1 \qquad (\bmod 4)\,.$$

Proof. (i) follows from Lemma 1 and

$$\frac{\wp(\alpha)}{\wp(2\psi)} - 1 = \frac{12}{tT(\alpha)}\,.$$

Let $\mu \in \mathfrak{o}$ with $\mu \equiv \sqrt{D}$ (mod 8). We see from (5) and (6) that

$$(\mu^2 - |\mu|^2)E_2(0) = \sum_{k \in L/\mu L - \{0\}} \wp\left(\frac{k}{\mu}\right),$$

hence

$$\frac{1}{2}(\mu^2 - |\mu|^2)E_2(0) = \sum_{\substack{k \in L/\mu L - \{0\} \\ k \bmod \pm 1}} \wp\left(\frac{k}{\mu}\right).$$

Devide both sides by $\wp(2\psi)$ and use (i). The asserted congruence of (ii) follows from

$$\frac{1}{2}(\mu^2 - |\mu|^2) \equiv 1 \qquad (\bmod 4)\,,$$

$$\frac{1}{2}(|\mu|^2 - 1) \equiv -1 \qquad (\bmod 4)\,.$$

LEMMA 3. *Let α be a point of $\mathbf{C}/L$ of finite, odd order > 1. Then $E_2(0)^{-1/2}E_1(\alpha)$ is algebraic and*

$$E_2(0)^{-1/2}E_1(\alpha) \equiv 1 \qquad (\bmod 2)\,.$$

Proof. Denote by n the order of α. By Lemma 2,

$$E_2(0)^{-1}\wp(k\alpha) \equiv -1 \qquad (\bmod 4)\,,$$

for $1 \leq k \leq n-1$. Note that $a \equiv 1 \pmod 2$ if and only if $a^2 \equiv 1 \pmod 4$. Then the assertions follow from the following identities (cf. [5], [6]):

$$nE_1(\alpha) = \sum_{k=1}^{n-2} (E_1(k\alpha) + E_1(\alpha) - E_1((k+1)\alpha)),$$
$$(E_1(k\alpha) + E_1(\alpha) - E_1((k+1)\alpha))^2 = \wp(k\alpha) + \wp(\alpha) + \wp((k+1)\alpha).$$

6. From [6] and [7], we know that there is a homomorphism χ: $SL(2, \mathfrak{o}) \to \boldsymbol{Z}/8\boldsymbol{Z}$ which is uniquely characterized by

$$\chi\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = 0$$

and

$$\chi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2\varepsilon + 2\left(1 - \left(\frac{2a}{c}\right)\right) + \operatorname{tr}\left(\frac{(a+d)c}{\sqrt{D}}\right) \qquad \bmod 8$$

for $c \equiv 1 \pmod 2$. Here,

$$\varepsilon = \begin{cases} 0, & c \equiv \pm 1 \pmod 4 \\ 1, & c \equiv \sqrt{D} \pmod 4 \\ -1, & c \equiv -\sqrt{D} \pmod 4 \end{cases}$$

and we agree that $(0/\pm 1) = 1$. This homomorphism χ describes the eighth roots of unity which occur in the transformation formula of a certain theta series. We note here that χ depends on the choice of the square root $\sqrt{D}$ of D; if we change $\sqrt{D}$ to $-\sqrt{D}$, then χ changes to $-\chi$.

THEOREM 1. *For every* $A \in SL(2, \mathfrak{o})$,

$$\sqrt{D}^{-1} E_2(0)^{-1} \Phi(A) \equiv \chi(A) \pmod 8.$$

Remark. Although $\chi(A)$ is a class of $\boldsymbol{Z}/8\boldsymbol{Z}$ the above congruence obviously makes sense if we consider $\chi(A)$ as a representative in $\boldsymbol{Z}$ of the class.

Proof. It suffices to prove the above under the assumption $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $c \equiv 1 \pmod 2$. Let α be a primitive c-division point of $\boldsymbol{C}/L$. By Lemma 3 we can apply Proposition 1 with $\mathfrak{c} = c\mathfrak{o}$ and

$$f(k) = E_2(0)^{-1/2} E_1(k\alpha).$$

We get, by (4),

$$cE_2(0)^{-1}D(a, c) \equiv 2\left(1 - \left(\frac{2a}{c}\right)\right) - 1 + \left(\frac{-1}{c}\right) \qquad (\mathrm{mod}\ 8)\,.$$

Because 2 splits in K, $c^2 \equiv 1 \pmod 8$. Therefore

$$\sqrt{D}^{-1} I\left(\frac{a+d}{c}\right) \equiv \mathrm{tr}\left(\frac{(a+d)c}{\sqrt{D}}\right) \qquad (\mathrm{mod}\ 8)\,.$$

Hence,

$$\begin{aligned}&\sqrt{D}^{-1} E_2(0)^{-1} \Phi(A)\\ &\quad \equiv \mathrm{tr}\left(\frac{(a+d)c}{\sqrt{D}}\right) - 2\left(1 - \left(\frac{2a}{c}\right)\right) + \frac{1}{c\sqrt{D}}\left(1 - \left(\frac{-1}{c}\right)\right) \qquad (\mathrm{mod}\ 8)\,.\end{aligned}$$

The value $(-1/c)$ is 1 if $\varepsilon = 0$ and -1 if $\varepsilon \neq 0$. Moreover $c\sqrt{D} \equiv \varepsilon \pmod 4$ if $\varepsilon \neq 0$. This completes the proof.

7. By Lemma 1 and Lemma 2, (ii), the number $12\sqrt{D}\,E_2(0)\,(\wp(\psi) - \wp(2\psi))^{-1}$ is algebraic and prime to 2. Hence we obtain from Theorem 1 the congruence in the next theorem.

THEOREM 2. *For every $A \in SL(2, \mathfrak{o})$,*

$$\frac{12}{\wp(\psi) - \wp(2\psi)}\Phi(A) \equiv \frac{12\sqrt{D}\,E_2(0)}{\wp(\psi) - \wp(2\psi)}\chi(A) \qquad (\mathrm{mod}\ 8)\,. \tag{8}$$

The left hand side and the coefficient of χ are of the form $\sqrt{-1} \times$ (an integer of F).

Proof. Because of (7) it suffices to prove the second assertion for the left hand side of (8). First we see the integrality. Put

$$\gamma = \wp(\psi) - \wp(2\psi)\,, \qquad \delta = \wp(2\psi)$$

and

$$T_1(z) = \gamma^{-1/2}\frac{d}{dz}T(z)\,.$$

Then,

$$T_1^2 = T(4T^2 + tT + 4)\,,$$

cf. [1]. From this follows that

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

with

$$(9)\qquad \begin{aligned} g_2 &= 12\delta^2 - 4\gamma^2 = 12^{-1}\gamma^2 t^2 - 4\gamma^2\,, \\ g_3 &= 4\gamma^2\delta - 8\delta^3 = 3^{-1}\gamma^3 t - 6^{-3}\gamma^3 t^3\,. \end{aligned}$$

Recall that the numbers we are interested in do not change when we replace the pair (L, ψ) by $(\lambda L, \lambda\psi)$. Taking $\lambda = \sqrt{6\gamma^{-1}}$, we may assume $\gamma = 6$. Then

$$(10)\qquad g_2 = 3t^2 - 144\,, \qquad g_3 = (72 - t^2)t$$

and the left hand side of (8) becomes $2\Phi(A)$. Since g_2 and g_3 are integral, it is also integral. To prove that it is of the form $\sqrt{-1}\mu$ $(\mu \in F)$, it suffices to show that g_2, $|D|^{1/2}g_3 \in F$ for the values of g_2 and g_3 given in (10). This condition is equivalent to $|D|^{1/2}t \in F$. We may assume $L = \bar{L}$. It is known (cf. [1]) that t^2 belongs to the Hilbert class field $F(\sqrt{D})$ of K and that t generates over K the ray class field modulo 4 of K, which is $F(\sqrt{D}, \sqrt{-1})$ in our case. It follows that $t \in F(|D|^{1/2})$, $t^2 \in F$ and $t \notin F$. Hence $|D|^{1/2}t \in F$. This concludes the proof.

If our lattice L satisfies

$$(11)\qquad (\wp(\psi) - \wp(2\psi))^2 = 144|D|\,,$$

then

$$\frac{1}{\sqrt{D}}\Phi(A) \equiv E_2(0)\chi(A) \qquad (\mathrm{mod}\ 8)$$

and $\sqrt{D}^{-1}\Phi(A)$ and $E_2(0)$ are integers of F. Furthermore, $E_2(0)$ is prime to 2. It can be seen that the lattices considered in [6], § 5 satisfy (11). Hence we have proved Conjecture 1 of Sczech [6]. The condition (11) is independent of the choice of ψ.

References

[1] R. Fueter, Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen I, II, Teubner, Leipzig-Berlin, 1924, 1927.

[2] H. Ito, On a property of elliptic Dedekind sums, J. Number Theory, **27** (1987), 17–21.

[3] H. Rademacher and E. Grosswald, Dedekind sums, Carus Mathematical Monographs, No. 16, Mathematical Assoc. America, Washington D. C., 1972.

[4] H. Reichardt, Eine Bemerkung zur Theorie des Jacobischen Symbols, Math. Nachr., **19** (1958), 171–175.

[5] R. Sczech, Dedekindsummen mit elliptischen Funktionen, Invent. Math., **76** (1984), 523–551.

[6] ——, Dedekind sums and power residue symbols, Compositio Math., **59** (1986), 89–112.
[7] ——, Theta functions on the hyperbolic three space, Kokyuroku RIMS, Kyoto Univ., No. **603** (1987), pp. 9–20.

The Institute for Advanced Study
Princeton, NJ 08540
USA

and

Nagoya University
Chikusa-ku, Nagoya, 464
Japan

Current address:
Department of Mathematics
College of Arts and Sciences
University of Tokyo
Tokyo 153, Japan