Bull. Korean Math. Soc. **56** (2019), No. 4, pp. 815–827
https://doi.org/10.4134/BKMS.b180043
pISSN: 1015-8634 / eISSN: 2234-3016

ON THE DENOMINATOR OF DEDEKIND SUMS

Stéphane R. Louboutin

Abstract. It is well known that the denominator of the Dedekind sum $s(c,d)$ divides $2\gcd(d,3)d$ and that no smaller denominator independent of c can be expected. In contrast, here we prove that we usually get a smaller denominator in $S(H,d)$, the sum of the $s(c,d)$'s over all the c's in a subgroup H of order $n>1$ in the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$. First, we prove that for $p>3$ a prime, the sum $2S(H,p)$ is a rational integer of the same parity as $(p-1)/2$. We give an application of this result to upper bounds on relative class numbers of imaginary abelian number fields of prime conductor. Finally, we give a general result on the denominator of $S(H,d)$ for non necessarily prime d's. We show that its denominator is a divisor of some explicit divisor of $2d\gcd(d,3)$.

1. Introduction

The *Dedekind sums* are defined by

$$(1)\quad s(c,d) := \frac{1}{4d}\sum_{n=1}^{d-1}\cot\left(\frac{\pi n}{d}\right)\cot\left(\frac{\pi nc}{d}\right) \text{ (for } c\in\mathbb{Z},\ d>1 \text{ and } \gcd(c,d)=1)$$

(see [1, Chapter 3, Exercise 11] or [8, (26)]). Dedekind sums are rational numbers whose denominators divide $2d\gcd(3,d)$:

Proposition 1 (See [8, Theorem 2 page 27])**.** *We have $2d\gcd(3,d)s(c,d)\in\mathbb{Z}$. Hence, $2ps(c,p)\in\mathbb{Z}$ for $p>3$ a prime and $p\nmid c$.*

Since for example, $2d\gcd(3,d)s(1,d)=\frac{(d-1)(d-2)}{6/\gcd(3,d)}$ is a rational integer coprime with d, we cannot expect more in general. Now, for H a subgroup of the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$, $d>1$, we set

$$(2)\qquad S(H,d) := \sum_{c\in H} s(c,d)\in\mathbb{Q}.$$

Theorems 3 and 4 below obtained in [4] led us to suspect that $2S(H,p)$ might always be a rational integer for $p>3$ a prime and $\#H>1$. The first aim

Received January 12, 2018; Revised March 1, 2019; Accepted April 25, 2019.
2010 *Mathematics Subject Classification.* Primary 11F20; Secondary 11M20, 11R29.
Key words and phrases. Dedekind sum, Dirichlet character, mean square value L-functions, relative class number.

of the present paper is to prove that $2S(H,p)$ is indeed a rational integer of known parity for $p>3$ a prime and $\#H>1$ (see Theorem 6). We will then explain that for non-prime d's we still have some cancelation in the denominator $2d\gcd(3,d)$ of $S(H,d)$ (Theorem 10 for the case that d is odd and Theorem 13 for the case that d is even).

It seems that it is the first time someone looks at the denominators of sums of Dedekind sums over elements of subgroups of the multiplicative groups $(\mathbb{Z}/d\mathbb{Z})^*$ (for denominators of Dedekind sums, we refer the reader to [7]). It would be worth to obtain similar results for the higher dimensional Dedekind sums introduced in [11].

2. Dedekind sums, *L*-functions and relative class numbers

Let us first explain our motivation for studying sums of Dedekind sums over elements of a subgroup. We refer the reader to [10] for more background details. Let K be an imaginary abelian number field of prime conductor $p\geq 3$, i.e., let K be an imaginary subfield of a cyclotomic number field $\mathbb{Q}(\zeta_p)$ (Kronecker-Weber's theorem). The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is canonically isomorphic to the multiplicative cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ and $H=\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of odd order n and even index $(p-1)/n=[K:\mathbb{Q}]$. Let X_p^- be the set of the $(p-1)/2$ odd Dirichlet characters mod p. The set

$$X_p^-(H):=\{\chi\in X_p^-;\ \text{and}\ \chi_{/H}=1\}$$

is of cardinal $(p-1)/(2n)$. Let h_K^- be the relative class number of K and w_K be the number of complex roots of unity in K. Hence, $w_K=2$ if $K\neq\mathbb{Q}(\zeta_p)$ and $w_K=2p$ otherwise. Let $L(s,\chi)=\sum_{n\geq 1}\chi(n)n^{-s}$ be the Dirichlet L-functions associated with $\chi\in X_p^-$. Then (see [3, Proposition 1])

$$L(1,\chi)=\frac{\pi}{2p}\sum_{a=1}^{p-1}\chi(a)\cot\left(\frac{\pi a}{p}\right)\qquad(\chi\in X_p^-). \tag{3}$$

Using the arithmetic-geometric mean inequality to obtain (5), plugging (3) in (4) and using the orthogonality relations for characters to obtain (6), we have:

Proposition 2 (See [4, Corollary 3]). *Let $n\geq 1$ be an odd integer. Let $p\equiv 1 \pmod{2n}$ be a prime. Let H_n be the only subgroup of order n of the multiplicative cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Set*

$$S(H_n,p):=\sum_{h\in H_n}s(h,p),$$

$$N(H_n,p):=12S(H_n,p)-p$$

and

$$M(H_n,p):=\frac{2n}{p-1}\sum_{\chi\in X_p^-(H_n)}|L(1,\chi)|^2. \tag{4}$$

Let K be the imaginary subfield of degree $(p-1)/n$ of the cyclotomic number field $\mathbb{Q}(\zeta_p)$. Then

$$h_K^- = w_K\left(\frac{p}{4\pi^2}\right)^{\frac{p-1}{4n}} \prod_{\chi\in X_p^-(H_n)} L(1,\chi) \leq w_K\left(\frac{pM(H_n,p)}{4\pi^2}\right)^{\frac{p-1}{4n}} \tag{5}$$

and we have the mean square value formula

$$M(H_n,p) = \frac{2\pi^2}{p}S(H_n,p) = \frac{\pi^2}{6}\left(1+\frac{N(H_n,p)}{p}\right). \tag{6}$$

2.1. The cases $n = 1$, $n = 3$ and $n = (p-1)/2$

These are the only three cases where explicit formulas for $S(H_n,p)$ are known.

1. Assume that $n = 1$. Then $H_1 = \{1\}$, $X_p^-(H_1) = X_p^-$,

$$S(H_1,p) = s(1,p) = \frac{(p-1)(p-2)}{12p} \tag{7}$$

(e.g. see [3, Lemme (a)], or [8, Lemma 2 page 5] with however an alternative definition of the Dedekind sums), $N(H_1,p) = -3+2/p \leq -1$,

$$M(\{1\},p) := \frac{2}{p-1}\sum_{\chi\in X_p^-}|L(1,\chi)|^2 = \frac{\pi^2}{6}\left(1-\frac{1}{p}\right)\left(1-\frac{2}{p}\right) \leq \frac{\pi^2}{6} \tag{8}$$

(see also [9]) and by (5) (see also [3], [5]):

$$h_{\mathbb{Q}(\zeta_p)}^- \leq 2p\left(\frac{p}{24}\right)^{(p-1)/4}.$$

2. Assume that $n = (p-1)/2$, where $3 < p \equiv 3 \pmod 4$ to assure the oddness of n. Then $H_{(p-1)/2} = \{c^2 : c \in (\mathbb{Z}/p\mathbb{Z})^*\}$ and $X_p^-(H_{(p-1)/2})$ is reduced to the Legendre symbol $\left(\frac{\bullet}{p}\right)$. The class number formula gives $L(1,\left(\frac{\bullet}{p}\right)) = \pi h_{\mathbb{Q}(\sqrt{-p})}/\sqrt{p}$. Hence, $M(H_2,p) = \frac{\pi^2 h_{\mathbb{Q}(\sqrt{-p})}}{p}$ and

$$S(H_2,p) = h_{\mathbb{Q}(\sqrt{-p})}^2/2 \qquad (p\equiv 3 \pmod 4). \tag{9}$$

Notice that in this situation the upper bound (5) is an equality.

3. Assume that $n = 3$. Then $p \equiv 1 \pmod 3$. Surprisingly, we proved in [4] that in that case we have a closed formula:

Theorem 3. *Let $p \equiv 1 \pmod 6$ be a prime. Let H_3 be the subgroup of order 3 of the multiplicative cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Let K be the imaginary subfield of degree $(p-1)/3$ of the cyclotomic number field $\mathbb{Q}(\zeta_p)$. Then $S(H_3,p) = (p-1)/12$ and $N(H_3,p) = -1$. Hence, $M(H_3,p) \leq \pi^2/6$ and $h_K^- \leq 2\,(p/24)^{(p-1)/12}$ (note the misprint in the exponent in* [4, (8)]*).*

4. Since the mean square value of $L(1,\chi)$, $\chi \in X_p^-$, is asymptotic to $\pi^2/6$, by (8), as in the case $n=3$ we might expect to have bounds close to

$$M(H_n,p) \leq \pi^2/6 \text{ and } h_K^- \leq w_K \left(\frac{p}{24}\right)^{\frac{p-1}{4n}}, \tag{10}$$

by (4) and (5), which would follow from $N(H_n,p) \leq 0$, by (5) and (6). However, it is hopeless to expect such a universal mean square upper bound. Indeed, it is likely that there are infinitely many imaginary abelian number fields of a given degree $m = 2n$ and prime conductors p for which

$$M(H_n,p) = \frac{2n}{p-1} \sum_{\chi \in X_p^-(H_n)} |L(1,\chi)|^2 \geq \Big(\prod_{\chi \in X_p^-(H_n)} L(1,\chi)\Big)^{\frac{p-1}{4n}} \gg (\log\log p)^2$$

(see [2] and [6]). Nevertheless, for $n=5$ we do sometimes have (10):

Theorem 4 (See [4, Theorem 5])**.** *Let $p \equiv 1 \pmod{10}$ be a prime of the form $p = a^4+a^3+a^2+a+1$, $a \in \mathbb{Z}$. Let $H_5 = \langle a \rangle$ be the subgroup of order 5 of the multiplicative cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Let K be the imaginary subfield of degree $(p-1)/5$ of the cyclotomic number field $\mathbb{Q}(\zeta_p)$. Then $S(H_5,p) = (a^4+3a^3+5a^2+3a)/12$ and $N(H_5,p) = 2a(a+1)^2-1$. Hence, for $a \leq -2$ we have $M(H_5,p) \leq \pi^2/6$ and $h_K^- \leq 2\,(p/24)^{(p-1)/20}$ (note the misprint in the exponent in* [4, Theorem 5]*).*

2.2. A question

To conclude this introduction, we give an excerpt of the computations we did on the sign of $N(H_n,p)$. According to them one might expect that asymptotically we have $N(H_n,p) \leq 0$ with a positive probability close to 1/2. Consequently we would have $h_K^- \leq 2(p/24)^{m/4}$ with a positive probability close to 1/2 for imaginary abelian number fields K of prime conductors p and degree m. We have no idea how to efficiently tackle this question.

Setting

$$N_1(B) = \#\{p : 3 \leq p \leq B\},$$
$$N_2(B) = \#E(B),$$

where $E(B) = \{(n,p) : n \geq 1 \text{ odd divides } p-1 \text{ and } p \leq B\}$ is the number of imaginary abelian number fields of prime conductors less than or equal to B,

$$N_3(B) = \#\{(n,p) \in E(B) : N(H_n,p) \leq 0\}$$

and $\rho(B) = N_3(B)/N_2(B)$, we computed:

B	$N_1(B)$	$N_2(B)$	$N_3(B)$	$\rho(B)$
10^2	24	60	50	0.83333...
10^3	167	666	507	0.76126...
10^4	1228	6775	4766	0.70346...
10^5	9591	66921	44629	0.66689...
10^6	78497	666728	427013	0.64046...

3. On the denominator of $S(H_n, p)$

Lemma 5. *Let H be a subgroup of the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$, $d > 1$. Set*

$$T(H,d) := \sum_{c\in H_n} c \in \mathbb{Z}/d\mathbb{Z}. \tag{11}$$

(i) *If $-1 \in H$, then $T(H,d) = 0$ in $\mathbb{Z}/d\mathbb{Z}$ and $S(H,d) = 0$ in $\mathbb{Q}$.*
(ii) *If $\#H > 1$, then $T(H,d) \notin (\mathbb{Z}/d\mathbb{Z})^*$, i.e., $\gcd(d, T(H,d)) > 1$.*

In particular, $T(H,p) = 0$ whenever H is a subgroup of order greater than one in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$, $p \geq 3$ a prime.

Proof. For (i), notice that $c \in H \mapsto -c \in H$ is a bijection and that $s(-c,d) = -s(c,d)$. For (ii), notice that for any $1 \neq c_0 \in H$ we have $(1-c_0)T(H,d) = T(H,d) - T(H,d) = 0$ in $\mathbb{Z}/d\mathbb{Z}$ (as $c \in H \mapsto c_0c \in H$ is a bijection). $\square$

Let $p \geq 3$ be a prime integer. Let $H = H_n$ be a subgroup of order $n > 1$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. If $n = \#H$ is even, then $-1 \in H$ and $S(H,p) = 0$ in $\mathbb{Q}$. Hence, we may assume that $n = \#H > 1$ is odd and in his section we prove that $2S(H_n,p)$ is always a rational integer (for $p \equiv 1 \pmod 6$ we already know that $2S(H_3,p) = (p-1)/6 \in \mathbb{Z}$, by Theorem 3):

Theorem 6. *Let $p > 3$ be a prime integer.* (i) *If $p \nmid c$, then $2ps(c,p)$ is a rational integer of the same parity as $(p-1)/2$.* (ii) *Let H be a subgroup of odd order $\#H > 1$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Let $N(H,p)$ be as in Proposition 2. Then $2S(H,p)$ is a rational integer of the same parity as $(p-1)/2$ and $N(H,p) = 12S(H,p) - p$ is an odd rational integer.*

Proof. To begin with, take $1 \neq c_0 \in H_n$. Then $c \in H \longrightarrow c_0c \in H$ being bijective, we have $T(H_n,p) = c_0T(H_n,p)$ and $T(H_n,p) = 0$. We have

$$S := \sum_{m=1}^{p-1} \cot\left(\frac{\pi m}{p}\right) = \sum_{m=1}^{p-1} \cot\left(\frac{\pi(p-m)}{p}\right) = -S$$

and $S = 0$ in $\mathbb{Q}$. Hence,

$$s(c,p) = -\frac{1}{p}\sum_{n=1}^{p-1}\left(\frac{\cot\left(\frac{\pi n}{p}\right) - i}{2i}\,\frac{\cot\left(\frac{\pi nc}{p}\right) - i}{2i} - \frac{1}{4}\right).$$

Set $\pi_p = 1 - \zeta_p$. Then $\frac{\cot(m\pi/p)-i}{2i} = \frac{1}{\zeta_p^m - 1} = -\pi_p^{-1}u_m$ for $p \nmid m$, where $u_m := (1-\zeta_p)/(1-\zeta_p^m) \in \mathbb{Z}[\zeta_p]$ is in fact a unit of $\mathbb{Z}[\zeta_p]$, by [10, Lemma 1.3]. We obtain

$$2ps(c,p) = -2\pi_p^{-2}w_{p,c} + \frac{p-1}{2}, \text{ where } w_{p,c} := \sum_{n=1}^{p-1} u_nu_{cn} \in \mathbb{Z}[\zeta_p]. \tag{12}$$

Now, in the quotient ring $\mathbb{Z}[\zeta_p]/\pi_p^3\mathbb{Z}[\zeta_p]$ we have

$$u_m = \frac{\pi_p}{1-(1-\pi_p)^m} = \frac{1}{m}\left(1+\frac{m-1}{2}\pi_p + \frac{m^2-1}{12}\pi_p^2\right) \qquad (\text{ if } p\nmid m).$$

Therefore, for $p \nmid c$ we have

$$w_{p,c} = \sum_{n=1}^{p-1}\frac{1}{cn^2}\left(1+\frac{(c+1)n-2}{2}\pi_p + \frac{(c^2+3c+1)n^2-3(c+1)n+1}{12}\pi_p^2\right).$$

Moreover, since π_p^3 divides π_p^{p-1} and π_p^{p-1} divides $p=\prod_{k=1}^{p-1}(1-\zeta_p^k)$ and since in $\mathbb{Z}/p\mathbb{Z}$ we have

$$\sum_{n=1}^{p-1} 1 = p-1 = -1, \quad \sum_{n=1}^{p-1}\frac{1}{n} = \sum_{n=1}^{p-1} n = \frac{p(p-1)}{2} = 0$$

and

$$\sum_{n=1}^{p-1}\frac{1}{n^2} = \sum_{n=1}^{p-1} n^2 = \frac{p(p-1)(2p-1)}{6} = 0,$$

we deduce that

$$w_{p,c} = -\frac{c^2+3c+1}{12c}\pi_p^2 \qquad (\text{in } \mathbb{Z}[\zeta_p]/\pi_p^3\mathbb{Z}[\zeta_p]). \tag{13}$$

Hence, π_p^2 divides $w_{p,c}$ in $\mathbb{Z}[\zeta_p]$, i.e., $w_{p,c} = \pi_p^2 W_{p,c}$ with $W_{p,c} \in \mathbb{Z}[\zeta_p]$. By (12), we have $W_{p,c} = \frac{p-1}{4} - ps(c,p) \in \mathbb{Q}\cap\mathbb{Z}[\zeta_p] = \mathbb{Z}$, $2ps(c,p) = -2W_{p,c} + \frac{p-1}{2} \in \mathbb{Z}$ and $2ps(c,p) \equiv \frac{p-1}{2} \pmod 2$. The proof of the first point is complete.

Moreover,

$$W_{p,c} = -\frac{c^2+3c+1}{12c} \qquad (\text{in } \mathbb{Z}[\zeta_p]/\pi_p\mathbb{Z}[\zeta_p]),$$

by (13), and $T(H,p) = \sum_{c\in H} c = \sum_{c\in H} 1/c = 0$ in $\mathbb{Z}/p\mathbb{Z}$.

Hence, in $\mathbb{Z}[\zeta_p]/\pi_p\mathbb{Z}[\zeta_p]$ we have

$$2ps(c,p) = -2W_{p,c} + \frac{p-1}{2} = \frac{c^2+1}{6c}$$

and

$$2pS(H,p) = \sum_{c\in H} 2ps(c,p) = \sum_{c\in H}\frac{c^2+1}{6c} = 0.$$

Hence, $2pS(H,p) \in \mathbb{Q}\cap\pi_p\mathbb{Z}[\zeta_p] = p\mathbb{Z}$, $2S(H,p) \in \mathbb{Z}$ and using point (i) we have

$$2S(H,p) \equiv 2pS(H,p) \equiv \sum_{c\in H} 2ps(c,p) \equiv \sum_{c\in H}\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod 2.$$

The proof of the second point is complete. $\square$

4. On the denominator of $S(H_n, d)$

Throughout the paper, we set

$$\delta = \gcd(3, d).$$

Now, what can we say about the denominator of $S(H_n, d)$ for H_n a subgroup of order $n > 1$ of the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$ if we do not assume anymore that d is prime? A key ingredient of the proof of Theorem 6 is that $T(H_n, p) = 0$. This does not necessarily hold true in general.

For example, there are 4 subgroups of order 3 in $(\mathbb{Z}/91\mathbb{Z})^*$ and we respectively have:

(i) $S(\{1, 9, 81\}, 91) = 15/2$ and $T(\{1, 9, 81\}, 91) = 0$,
(ii) $S(\{1, 16, 74\}, 91) = 15/2$ and $T(\{1, 16, 74\}, 91) = 0$,
(iii) $S(\{1, 22, 29\}, 91) = 97/14$ and $T(\{1, 22, 29\}, 91) = 52 = 4 \cdot 13$, and
(iv) $S(\{1, 53, 79\}, 91) = 171/26$ and $T(\{1, 53, 79\}, 91) = 42 = 6 \cdot 7$.

Theorem 10 will clarify the appearance of these various denominators. Notice that Theorem 10 asserts that for d odd and $n > 1$, the denominator of $S(H_n, d)$ is always smaller than $2d\delta$. Instead of using (1), throughout this section we will use an equivalent definition (15) of the Dedekind sums.

Lemma 7. *For $d \geq 1$, $c \in \mathbb{Z}$ with $\gcd(c, d) = 1$, we have*

$$2d\delta s(c,d) = \frac{(d-1)(2d-1)}{3/\delta}c - \delta\frac{d(d-1)}{2} - 2\delta\sum_{n=1}^{d-1} n\left[\frac{nc}{d}\right]. \tag{14}$$

Hence (compare with [8, Theorem 2 page 27]), the rational number $2d\delta s(c, d)$ is a rational integer of known parity, namely

$$2d\delta s(c,d) \equiv \begin{cases} (d-1)/2 \pmod 2 & \text{if } d \text{ is odd,} \\ d/2 - 1 \pmod 2 & \text{if } d \text{ is even.} \end{cases}$$

Proof. For $x \in \mathbb{R}$ we write $x = [x] + \{x\}$ with $[x] \in \mathbb{Z}$ and $0 \leq \{x\} < 1$. By d-periodicity of both sides of (14), we may assume that $1 \leq c \leq d-1$. According to [1, Chapter 3, (31) and Exercice 11] or [8, (1) page 1] and since $\left[\frac{n}{d}\right] = 0$ for $1 \leq n \leq d-1$, we have

$$\begin{aligned} s(c,d) &= \sum_{n=1}^{d-1}\left(\frac{n}{d} - \left[\frac{n}{d}\right] - \frac{1}{2}\right)\left(\frac{nc}{d} - \left[\frac{nc}{d}\right] - \frac{1}{2}\right) \\ &= \sum_{n=1}^{d-1}\left\{\frac{n^2c}{d^2} - \frac{n(c+1)}{2d} + \frac{1}{4} + \frac{1}{2}\left[\frac{nc}{d}\right] - \frac{n}{d}\left[\frac{nc}{d}\right]\right\}. \end{aligned} \tag{15}$$

Using $\sum_{n=1}^{d-1}\left\{\frac{nc}{d}\right\} = \sum_{n=1}^{d-1}\left\{\frac{n}{d}\right\} = \sum_{n=1}^{d-1}\frac{n}{d}$ for $\gcd(c, d) = 1$, we obtain

$$\sum_{n=1}^{d-1}\left[\frac{nc}{d}\right] = \sum_{n=1}^{d-1}\left(\frac{nc}{d} - \left\{\frac{nc}{d}\right\}\right) = \sum_{n=1}^{d-1}\frac{n(c-1)}{d} = \frac{(d-1)(c-1)}{2}. \tag{16}$$

The desired first result follows. Since (14) clearly yields

$$2d\delta s(c,d) \equiv (d-1)c + \frac{d(d-1)}{2} \pmod 2,$$

the second assertion follows by noticing that if d is even, then c is odd. □

Lemma 8. *For $d \geq 1$, set $\delta = \gcd(3,d)$. For $c \in \mathbb{Z}$ and $\gcd(c,d) = 1$, let c^* be such that where $cc^* \equiv 1 \pmod d$ and set*

$$G(c,d) := \frac{(d-1)(2d-1)}{3/\delta}c - c^*\frac{(d-1)(2d-1)(c^2-1)}{6/\delta} - \delta\frac{d(d-1)}{2} - c^*\delta d\frac{(d-1)(c-1)}{2},$$

a rational integer (since c is odd whenever d is even, the four fractions that appear in this formula are all in $\mathbb{Z}$). Then $2d\delta s(c,d) \equiv G(c,d) \pmod{2\delta d}$.

Proof. By (14), we have

$$(17)\quad 2d\delta s(c,d) \equiv \frac{(d-1)(2d-1)}{3/\delta}c - \delta\frac{d(d-1)}{2} - 2\delta c^* \sum_{n=1}^{d-1} nc\left[\frac{nc}{d}\right] \pmod{2\delta d}.$$

Since $2x[x] = x^2 - \{x\}^2 + [x]^2$ and

$$\sum_{n=1}^{d-1}\left\{\frac{nc}{d}\right\}^2 = \sum_{n=1}^{d-1}\left\{\frac{n}{d}\right\}^2 = \sum_{n=1}^{d-1}\frac{n^2}{d^2} \qquad (\gcd(c,d)=1),$$

we have

$$2\sum_{n=1}^{d-1}\frac{nc}{d}\left[\frac{nc}{d}\right] = \sum_{n=1}^{d-1}\frac{n^2(c^2-1)}{d^2} + \sum_{n=1}^{d-1}\left[\frac{nc}{d}\right]^2 = \frac{(d-1)(2d-1)(c^2-1)}{6d} + \sum_{n=1}^{d-1}\left[\frac{nc}{d}\right]^2.$$

Therefore, using $\left[\frac{nc}{d}\right]^2 \equiv \left[\frac{nc}{d}\right] \pmod 2$ and (16), we obtain

$$2\delta\sum_{n=1}^{d-1} nc\left[\frac{nc}{d}\right] \equiv \frac{(d-1)(2d-1)(c^2-1)}{6/\delta} + \delta d\frac{(d-1)(c-1)}{2} \pmod{2\delta d}.$$

Using (17), the desired result follows. □

By Lemma 7, if $d \equiv 1, 2 \pmod 4$, then $d\delta s(c,d)$ is a rational integer whose parity we now determine:

Lemma 9. (i) *If $d \equiv 1 \pmod 4$, then $d\delta s(c,d)$ is a rational integer of the same parity as $(d-1)/4$.* (ii) *If $d \equiv 2 \pmod 4$, then $d\delta s(c,d)$ is a rational integer of the same parity as $(d-2)/4$.*

Proof. Let us prove point (i).

We have $\frac{(d-1)(2d-1)}{3/\delta}c \in 4\mathbb{Z}$ and the three others terms in $G(c,d)$ are even. Hence $G(c,d)$ is even. Since if n is even and a is odd, then $an \equiv n \pmod 4$, we have

$$G(c,d) \equiv \frac{3}{\delta}G(c,d) \equiv \frac{d-1}{2}\big(-(2d-1)c^*(c^2-1) - 3d - 3dc^*(c-1)\big)$$
$$\equiv \frac{d-1}{2}\big(-c^*(c^2-1) - 1 - c^*(c-1)\big) \equiv \frac{d-1}{2} \pmod 4,$$

since $-c^*(c^2-1) - 1 - c^*(c-1) = -c^*(c^2+c-2) - 1$ is odd.

Let us prove point (ii).

Since c is odd, we have $c^2 - 1 \equiv 0 \pmod 8$ and $\frac{(d-1)(2d-1)(c^2-1)}{6/\delta} \in 4\mathbb{Z}$. Hence,

$$G(c,d) \equiv \delta c - 0 - \delta\frac{d}{2} - \delta\frac{d}{2}c^*(c-1) \equiv \delta c(1 - d/2) \equiv d/2 - 1 \pmod 4,$$

using $d \equiv 2 \pmod 4$ and $c^*(c-1) \equiv c - 1 \pmod 4$ (as c and c^* are odd). □

Using Lemma 8 we will obtain Theorem 10 (which implies Theorem 6).

Using Lemmas 8 and 9 we will obtain Theorem 13 and obtain in Corollary 14 the same result for $S(H_n, 2p)$ than the one obtained for $S(H_n, p)$ in Theorem 6 or Corollary 11.

4.1. The case that d is odd

Theorem 10. *Assume that $d > 1$ is odd. Set $\delta = \gcd(3,d)$. Let H_n be a subgroup of order n of the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$. Let $T(H_n,d)$ be as in (11). Then $\gcd(d, T(H_n,d)) > 1$ and*

$$2\delta\frac{d}{\gcd(d, T(H_n,d))}S(H_n,d)$$

is a rational integer of the same parity as $n\frac{d-1}{2}$ and

$$2\delta S(H_n,d) \in \mathbb{Z} \Leftrightarrow d \mid T(H_n,d).$$

In contrast, $2\delta s(c,d) \in \mathbb{Z} \Leftrightarrow c^2 \equiv -1 \pmod d$, in which case $s(c,d) = 0$.

Proof. For the first assertion, see point (ii) of Lemma 5.

Noticing that $D_6 := \frac{(d-1)(2d-1)}{6/\delta} \in \mathbb{Z}$, that the third and fourth terms of $G(c,d)$ in Lemma 8 are in $d\mathbb{Z}$ and that $2c - c^*(c^2-1) \equiv c + c^* \pmod d$, we obtain (in $\mathbb{Z}$)

$$2d\delta s(c,d) \equiv G(c,d) \equiv D_6(c + c^*) \pmod d$$

and

$$2d\delta S(H_n,d) \equiv 2D_6 T(H_n,d) \pmod d.$$

Therefore, $2d\delta S(H_n,d)$ is indeed in $\gcd(d, T(H_n,d))\mathbb{Z}$. Since $\gcd(2D_6, d) = 1$, the rational number $2\delta S(H_n,d)$ is in $\mathbb{Z}$ if and only if d divides $T(H_n,d)$, as asserted, and the rational number $2\delta s(c,d)$ is in $\mathbb{Z}$ if and only if $c + c^* \equiv 0$

(mod d), i.e., if and only if $c^2 \equiv -1 \pmod{d}$, as asserted. In that case, the change of variable $n \mapsto c^*n$ in (1) gives $s(c,d) = s(c^*,d) = -s(c,d)$ and $s(c,d) = 0$, as asserted.

Finally, by Lemma 7, we have (in $\mathbb{Z}$)

$$2d\delta S(H_n,d) = \sum_{c\in H_n} 2d\delta s(c,d) \equiv n\frac{d-1}{2} \pmod{2}.$$

Using the oddness of $\gcd(d, T(H_n,d))$ we obtain

$$2\delta\frac{d}{\gcd(d,T(H_n,d))}S(H_n,d) \equiv n\frac{d-1}{2} \pmod{2},$$

as asserted. □

Corollary 11. *If H_n is a subgroup of order $n > 1$ of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$, $p > 3$, then $S(H_n,p) = 0$ if n is even, whereas $2S(H_n,p)$ is a rational integer of the same parity as $(p-1)/2$ if n is odd.*

4.2. The case that d is even

We cannot expect Theorem 10 to hold true for d even. For example, for $n = 3$, $d = 14$ and $H_3 = \{1, 9, 11\}$, we have $2\delta S(H_3,d) = 2S(H_3,14) = 1 \in \mathbb{Z}$ but $d = 14$ does not divide $T(H_3,14) = 7$.

If d is even, recalling that c^* is such that $cc^* \equiv 1 \pmod{d}$, we set

$$T'(H_n,d) := \sum_{c\in H_n}\left(c - c^*\frac{c^2-1}{2} - \frac{d}{2}\right) \in \mathbb{Z}/d\mathbb{Z} \tag{18}$$

(if d is even, then c^* and c are odd and $(c^2-1)/2 \in 2\mathbb{Z}$. Moreover, the application c (odd) $\mapsto \frac{c^2-1}{2}$ modulo d is d-periodic. Hence, $T'(H_n,d)$ is well defined).

Lemma 12. *Let H_n be a subgroup of order $n > 1$ of the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$.*

(i) *If d is even, then $T(H_n,d) \equiv n \pmod{2}$, $T'(H_n,d) = T(H_n,d)$ or $T(H_n,d) + \frac{d}{2}$.*

(ii) *If $d \equiv 2 \pmod{4}$ or $d \equiv 4 \pmod{8}$, then $T'(H_n,d) = T(H_n,d) + n\frac{d}{2}$ in $\mathbb{Z}/d\mathbb{Z}$.*

(iii) *Assume that $d = 2p$, where $p \geq 3$ is prime. Then there exists at most one subgroup H_n of a given order n in the cyclic group $(\mathbb{Z}/2p\mathbb{Z})^*$. If n is even, then $-1 \in H_n$ and $S(H_n,d) = 0$ (Lemma 5). If n is odd, then $T(H_n,2p) = p$ and $T'(H_n,2p) = 0$.*

Proof. Any $c \in H_n$ being odd, the first assertion of (i) follows. Since $2c - c^*(c^2-1) \equiv c + c^* \pmod{d}$, we have $2T_n'(H_n,d) \equiv \sum_{c\in H_n}(c+c^*) \equiv 2T(H_n,d) \pmod{d}$ and the second assertion of (i) follows.

For (ii), it suffices to prove that $S := \sum_{c\in H_n} c^*\frac{c^2-1}{2} = 0$ in $\mathbb{Z}/d\mathbb{Z}$. Clearly, $2S = T(H_n,d) - T(H_n,d) = 0$. Hence $S = 0$ or $S = \frac{d}{2}$. Since clearly $S = [4s]_d$

in $\mathbb{Z}/d\mathbb{Z}$ for some $s \in \mathbb{Z}$, if we had $S = d/2$, then we would have $4s \equiv \frac{d}{2} \pmod{d}$ and the contradictions $4s \equiv 1 \pmod{2}$ for $d \equiv 2 \pmod{4}$ and $4s \equiv 2 \pmod{4}$ for $d \equiv 4 \pmod{8}$.

Notice, for example, that if $n = 2$, $d = 8$ and $H_2 = \{1, 9\}$, then $0 = T'(H_2, 8) \neq T(H_2, 8) + n\frac{d}{2} = 4$ in $\mathbb{Z}/8\mathbb{Z}$.

For (iii), we have $T(H_n, 2p) \equiv n \equiv 1 \pmod{2}$, by point (i), and $T(H_n, 2p) \in \{0, 2, p\}$, by point (ii) of Lemma 5. Hence, $T(H_n, 2p) = p$ and point (ii) gives $T'(H_n, 2p) = T(H_n, 2p) + p = 0$. □

Theorem 13. *Assume that $d > 1$ is even. Set $\delta = \gcd(3, d)$. Let H_n be a subgroup of order n of the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^*$. Let $T'(H_n, d)$ be as in* (18). *Then*

$$2\delta \frac{d}{\gcd(d, T'(H_n, d))} S(H_n, d) \in \mathbb{Z}$$

and

$$2\delta S(H_n, d) \in \mathbb{Z} \Leftrightarrow d \mid T'(H_n, d).$$

In contrast, $2\delta s(c, d) \in \mathbb{Z} \Leftrightarrow c^2 \equiv -1 \pmod{d}$, in which case $s(c, d) = 0$.

Moreover, if $d \equiv 2 \pmod{4}$, then

$$2\delta \frac{d}{\gcd(d, T'(H_n, d))} S(H_n, d)$$

is a rational integer of the same parity as $n\frac{d-2}{4}$.

Proof. We set

$$D_3 := \frac{(d-1)(2d-1)}{3/\delta} \in \mathbb{Z}.$$

Notice that $\gcd(D_3, d) = 1$.

Since c is odd, $c^2 - 1$ is even, D_3 is odd, the fourth term of $G(c, d)$ in Lemma 8 is in $d\mathbb{Z}$ and its third term is equal to $d/2$ modulo d. Hence (in $\mathbb{Z}$), we have

$$2d\delta s(c, d) \equiv D_3(c - c^* \frac{c^2 - 1}{2}) - \frac{d}{2} \equiv D_3(c - c^* \frac{c^2 - 1}{2} - \frac{d}{2}) \pmod{d}$$

and

$$2d\delta S(H_n, d) = \sum_{c \in H_n} 2d\delta s(c, d) \equiv D_3 T'(H_n, d) \pmod{d}.$$

Therefore, $2d\delta S(H_n, d)$ is indeed in $\gcd(d, T'(H_n, d))\mathbb{Z}$. Since $\gcd(D_3, d) = 1$, the rational number $2\delta S(H_n, d)$ is in $\mathbb{Z}$ if and only if d divides $T'(H_n, d)$, as asserted, and if the rational number $2\delta s(c, d)$ is in $\mathbb{Z}$, then d divides $2c - c^*(c^2 - 1) - d$, hence divides $c + c^*$ and we obtain $c^2 \equiv -1 \pmod{d}$. Conversely, if $c^2 \equiv -1 \pmod{d}$, then as in the proof of Theorem 10 we have $s(c, d) = 0$ and hence $2\delta s(c, d) \in \mathbb{Z}$.

Finally, assume that $d \equiv 2 \pmod{4}$. Then $T'(H_n, d) \equiv 0 \pmod{2}$, by (18). Hence, $\gcd(d, T'(H_n, d)) = 2\gcd(d/2, T'(H_n, d))$. The oddness of $\gcd(d/2,$

$T'(H_n, d))$ gives

$$2\frac{d}{\gcd(d, T'(H_n, d))}\delta S(H_n, d) = \frac{d}{\gcd(d/2, T'(H_n, d))}\delta S(H_n, d)$$
$$\equiv d\delta S(H_n, d) \pmod 2.$$

By Lemma 9 we have $d\delta s(c, d) \in \mathbb{Z}$, $d\delta S(H_n, d) \in \mathbb{Z}$ and

$$d\delta S(H_n, d) \equiv n\frac{d-2}{4} \pmod 2.$$

The last assertion follows. □

Corollary 14. *If H_n is a subgroup of order $n > 1$ of the multiplicative group $(\mathbb{Z}/2p\mathbb{Z})^*$, $p > 3$, then $S(H_n, 2p) = 0$ if n is even, whereas $2S(H_n, 2p)$ is a rational integer of the same parity as $(p-1)/2$ if n is odd.*

Proof. The last assertion follows from $T'(H_n, 2p) = 0$, n odd (Lemma 12). □

References

[1] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Springer-Verlag, New York, 1976.

[2] P. J. Cho and H. H. Kim, *Dihedral and cyclic extensions with large class numbers*, J. Théor. Nombres Bordeaux **24** (2012), no. 3, 583–603.

[3] S. Louboutin, *Quelques formules exactes pour des moyennes de fonctions L de Dirichlet*, Canad. Math. Bull. **36** (1993), no. 2, 190–196. https://doi.org/10.4153/CMB-1993-028-8

[4] ———, *Dedekind sums, mean square value of L-functions at $s = 1$ and upper bounds on relative class numbers*, Bull. Pol. Acad. Sci. Math. **64** (2016), no. 2-3, 165–174. https://doi.org/10.4064/ba8092-12-2016

[5] T. Metsänkylä, *Class numbers and μ-invariants of cyclotomic fields*, Proc. Amer. Math. Soc. **43** (1974), 299–300. https://doi.org/10.2307/2038882

[6] H. L. Montgomery and P. J. Weinberger, *Real quadratic fields with large class number*, Math. Ann. **225** (1977), no. 2, 173–176. https://doi.org/10.1007/BF01351721

[7] L. Pinzur, *Denominators of Dedekind sums*, J. Number Theory **9** (1977), no. 3, 361–369. https://doi.org/10.1016/0022-314X(77)90071-3

[8] H. Rademacher and E. Grosswald, *Dedekind Sums*, The Mathematical Association of America, Washington, DC, 1972.

[9] H. Walum, *An exact formula for an average of L-series*, Illinois J. Math. **26** (1982), no. 1, 1–3. http://projecteuclid.org/euclid.ijm/1256046895

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, second edition, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997. https://doi.org/10.1007/978-1-4612-1934-7

[11] D. Zagier, *Higher dimensional Dedekind sums*, Math. Ann. **202** (1973), 149–172. https://doi.org/10.1007/BF01351173

Stéphane R. Louboutin
Aix Marseille Université
CNRS, Centrale Marseille, I2M
Marseille, France
Postal address: Institut de Mathématiques de Marseille
Aix Marseille Université
163 Avenue de Luminy, Case 907
13288 Marseille Cedex 9, France
Email address: stephane.louboutin@univ-amu.fr