#A98 INTEGERS 21 (2021)

ON THE EQUALITY OF DEDEKIND SUMS

Kurt Girstmair
Institut für Mathematik, Universität Innsbruck, Innsbruck, Austria
kurt.girstmair@uibk.ac.at

Received: 2/22/21, Accepted: 10/11/21, Published: 10/15/21

Abstract

We show that deciding the equality of two Dedekind sums $S(c, b)$, $S(d, b)$ is equivalent to deciding whether a Dedekind sum defined by b, c, d takes a certain value. By means of this result we construct infinite sequences of pairwise equal Dedekind sums. Moreover, we prove a result that says how many Dedekind sums $S(d, b)$, $1 \le d \le b-1$, may be equal to a given $S(c, b)$ if b is a square-free number.

1. Introduction

Let b be a natural number and c an integer such that $(c, b) = 1$. The classical Dedekind sum $s(c, b)$ is defined by

$$s(c,b) = \sum_{k=1}^{b} ((k/b))((ck/b)). \tag{1}$$

Here

$$((x)) = \begin{cases} x - \lfloor x \rfloor - 1/2 & \text{if } x \in \mathbb{R} \smallsetminus \mathbb{Z}; \\ 0 & \text{if } x \in \mathbb{Z} \end{cases}$$

(see [10, p. 1]).

Dedekind sums first appeared in the theory of modular forms; see [1]. But these sums have also interesting applications in a number of other fields, so in connection with class numbers, lattice point problems, topology, and algebraic geometry (see, for instance, [2, 3, 8, 10, 12, 13]).

In this paper we work with the normalized Dedekind sum

$$S(c, b) = 12s(c, b).$$

The number b is called the *modulus* and c the *argument* of $S(c, b)$.

Our aim is the study of equal values of Dedekind sums belonging to the same modulus b but to different arguments c, d. Two cases of equality can be considered as trivial. First,

$$S(c,b) = S(c',b)$$

if $c \equiv c' \mod b$ (this justifies calling b the modulus of $S(c,b)$). Second, let c^* denote an inverse of $c \mod b$, i.e., an the integer such that $cc^* \equiv 1 \mod b$. Of course, c^* is determined only up to the addition of multiples of b. It is an easy consequence of the definition (1) that

$$S(c,b) = S(c^*,b);$$

see [10, p. 26].

Cases of nontrivial equality, i.e., $S(c,b) = S(d,b)$ and $d \not\equiv c, c^* \mod b$, do not occur frequently. For example, for $b = 3^3 \cdot 11 = 297$, $S(c,b)$ takes 41 distinct positive values, but only five of them give rise to nontrivial equality, namely, $3076/b$, $1712/b$, $1460/b$, $1456/b$, and $1136/b$. If $b = p_1^{m_1} \cdots p_r^{m_r}$, the p_i being distinct primes, then the number of cases of nontrivial equality seems to increase with r and the exponents m_i.

Suppose that the modulus b and two arguments c, d are given, $d \not\equiv c, c^* \mod b$. So far no simple condition is known that is equivalent to $S(c,b) = S(d,b)$. One has only necessary conditions for this equality like

$$(c-d)(cd-1) \equiv 0 \mod b; \tag{2}$$

see [7]. Indeed, the condition (2) is equivalent to $S(c,b) \equiv S(d,b) \mod \mathbb{Z}$; see [6]. This criterion was extended to a condition for $S(c,b) \equiv S(d,b) \mod 8\mathbb{Z}$; see [11]. However, the latter condition is no more quite simple, because it may involve up to two Jacobi symbols that must be evaluated.

In the present paper we prove the following theorem, which is based on an adaption of a result of U. Dieter; see Section 2.

Theorem 1. *Let $c, d \in \mathbb{Z}$, $(c,b) = (d,b) = 1$, $c \not\equiv d \mod b$. Suppose that b, c, d satisfy condition* (2). *Let $t > 0$ be such that $t \equiv c - d \mod b$. Then $S(c,b) = S(d,b)$ if, and only if,*

$$S(1+ct, bt) = \frac{2+t^2}{bt} - 3.$$

If we want to decide whether two Dedekind sums with the same modulus are equal, we may, instead, decide whether a certain Dedekind sum takes a certain value, as the theorem says. We think that the latter task is not simpler in most cases. But, due to this theorem, it seems to be plausible that no simple necessary and sufficient condition for nontrivial equality exists.

In this paper we present two applications of Theorem 1. The first application is the construction of infinite sequences of pairwise equal Dedekind sums. To this end let $c, d \in \mathbb{Z}$, $c \neq d$, with $(c,b) = (d,b) = 1$. We say that $\{c, d\}$ is a *suitable set* for (the modulus) b if, and only if, $d \not\equiv c, c^* \mod b$ and $S(c,b) = S(d,b) \neq 0$.

Theorem 2. *In the above setting, let $\{c, d\}$ be a suitable set for b. Let $t > 0$ be such that $t \equiv d - c^* \mod b$. Put $b_1 = bt$, $c_1 = 1 + ct$, $d_1 = 1 + dt$. Then $b_1 > b$ and $\{c_1, d_1\}$ is a suitable set for b_1.*

By Theorem 2, we can define an infinite sequence of strictly increasing moduli b_i, $i \geq 0$, together with sets $\{c_i, d_i\}$ suitable for b_i, provided that one suitable set $\{c, d\}$ is known. Indeed, put $b_0 = b$, $c_0 = c$, $d_0 = d$ and $t_0 = t$. Define, recursively, $b_{i+1} = b_i t_i$, $c_{i+1} = 1 + c_i t_i$, $d_{i+1} = 1 + d_i t_i$, $i \geq 0$. Then define $t_{i+1} > 0$ by $t_{i+1} \equiv d_{i+1} - c^*_{i+1} \mod b_{i+1}$ (the inverse is to be understood $\mod b_{i+1}$). In particular, we obtain $d_i \not\equiv c_i, c_i^* \mod b_i$ and

$$S(c_i, b_i) = S(d_i, b_i) \neq 0$$

for all $i \geq 0$.

Example. Put $b = 7 \cdot 11 = 77$, $c = 16$, $d = 60$. Then $d \not\equiv c, c^* \mod b$ and $S(c, b) = S(d, b) = 300/77$. Obviously, the set $\{c, d\}$ is suitable for b. Since $d - c^* \equiv 7 \mod b$ we may take $t = 7$ and form the sequences b_i and $\{c_i, d_i\}$, $i \geq 0$, in the above way, where t_i is chosen in $\{1, \ldots, b_i - 1\}$. We obtain

$$\begin{aligned}
&b_0 = 77, c_0 = 16, d_0 = 60, \\
&b_1 = 539, c_1 = 113, d_1 = 421, \\
&b_2 = 260337, c_2 = 54580, d_2 = 203344, \\
&b_3 = 6412881321, c_3 = 1344469141, d_3 = 5008972753, \\
&b_4 = 36852630635308805163, c_4 = 7726203273338872624, \\
&d_4 = 28784849350658189860.
\end{aligned}$$

One sees that these numbers grow rapidly. The first values of t_i are $t_0 = 7$, $t_1 = 483$, $t_2 = 24633$, $t_3 = 5746657203$.

How can we find suitable sets $\{c, d\}$ to initiate sequences like the above? A partial answer is given by the following theorem, whose proof involves another application of Theorem 1.

Theorem 3. *Let $1 \leq k \leq r$ and $p_1, \ldots, p_k$ be distinct primes, each of which is congruent $\pm 1 \mod 5$. Put $b_0 = p_1 \cdots p_k$ and let $p_{k+1}, \ldots, p_r$ be distinct primes, each of which is congruent $1 \mod b_0$. Let $b = p_1 \cdots p_r$ and $t = p_{k+1} \cdots p_r$. Then*

$$\left| \left\{ c : 1 \leq c \leq b - 1, (c, b) = 1, S(c, b) = \frac{t^2 + 2}{b} - 3 \right\} \right| = 2^k.$$

On observing that $t = 1$ if $k = r$, we have the following corollary.

Corollary 1. *Let $1 \leq r$ and $p_1, \ldots, p_r$ be distinct primes, each of which is congruent $\pm 1 \mod 5$. Let $b = p_1 \cdots p_r$. Then*

$$\left| \left\{ c : 1 \leq c \leq b - 1, (c, b) = 1, S(c, b) = \frac{3}{b} - 3 \right\} \right| = 2^r.$$

It is easy to see that the common value $(t^2+2)/b-3$ of the Dedekind sums in Theorem 3 cannot vanish; see the end of the proof of Theorem 2 in Section 3.

The proof of Theorem 3 shows how to find the numbers c in question by means of the Chinese remainder theorem; see Section 3. Suppose, for a moment, that b is as in Corollary 1 with $r=3$. Then we have eight numbers c such that $S(c,b)=3/b-3$. These numbers give us 24 suitable sets for the modulus b. Section 3 contains additional examples of suitable sets and a few remarks on the above sequences of suitable sets.

Given b and c, $(c,b)=1$, we consider the number

$$N(c,b)=|\{d : 1\le d\le b-1, (d,b)=1, S(d,b)=S(c,b)\}|. \tag{3}$$

Suppose that b is a square-free number *consisting of r primes*, i.e., $b=p_1\cdots p_r$, the p_i being distinct. It is known that $N(c,b)\le 2^r$; see [6, Theorem 3]. Theorem 3 exhibits the 2-powers 2^k, $1\le k\le r$, as possible values of $N(c,b)$ for this case. At the end of Section 3 we will see that there may be values greater than 1 of $N(c,b)$ different from the aforesaid 2-powers for a number b of this kind.

2. The Criterion

The proof of Theorem 1 is based on the following proposition.

Proposition 1. *Let $c,d\in\mathbb{Z}$, $(c,b)=(d,b)=1$, $c\not\equiv d \mod b$. Let $t>0$ be such that $t\equiv c-d \mod b$. Then*

$$S(1+d^*t,bt)-\left(\frac{t^2+2}{bt}-3\right)=S(d,b)-S(c,b). \tag{4}$$

Of course, the identity (4) may also serve as a criterion for the equality of $S(c,b)$ and $S(d,b)$. It is, however, less simple than Theorem 1 since it involves the inversion of $d \mod b$. This inversion involves more work than checking the condition (2) (as required by Theorem 1).

Proposition 1 can be found, in a rather disguised form, in a paper of U. Dieter; see [4, Satz 4]. In particular, it is not obvious that Dieter's version contains a criterion for the equality of Dedekind sums. Dieter obtained his result as an application of his three-term relation; see [4, Satz 1]. We prefer deriving Proposition 1 directly from this well-known relation since adapting Dieter's Satz 4 would not be simpler.

Proof of Proposition 1. The three-term relation, in its most convenient form for the present purpose, reads as follows; see [5]. Let B and D be natural numbers, A and C integers with $(A,B)=(C,D)=1$. Suppose that

$$Q=AD-BC>0.$$

Let j and k be integers such that

$$-Cj + Dk = 1.$$

Define R by

$$R = Aj - Bk.$$

Then

$$S(A,B) = S(C,D) + S(R,Q) + \frac{B^2 + D^2 + Q^2}{BDQ} - 3. \tag{5}$$

Let b, c, d, and t be as in the proposition. Let $c' \equiv c \mod b$ be such that $c' - d = t$. We put $B = D = b$, $A = c'$, and $C = d$. Then $Q = bt > 0$. Since $-Cj + Dk = -dj + bk = 1$, $j = -d^*$ for an inverse d^* of $d \mod b$ and $k = (1 - dd^*)/b$. We obtain $R = -1 - d^*t$. Since $-S(R,Q) = S(1+d^*t, bt)$ and $(B^2+D^2+Q^2)/(BDQ) = (t^2+2)/(bt)$, the identity (5) gives (4), but with c' instead of c. However, $S(c', b) = S(c, b)$, and the other quantities in the identity (4) depend only of t and b. Hence the equation (4) holds in the above form. □

Lemma 1. *Suppose that b, c, d satisfy the congruence* (2). *Then*

$$c - d \equiv d^* - c^* \mod b.$$

Proof. Indeed, suppose $b = p_1^{m_1} \cdots p_r^{m_r}$, where the p_i are distinct primes. It suffices to show

$$c - d \equiv d^* - c^* \mod p_i^{m_i} \text{ for all } i \in \{1, \dots, r\}.$$

We fix i for the time being. So we write $p = p_i$, $m = m_i$. The congruence (2) implies

$$(c - d)(cd - 1) \equiv 0 \mod p^m.$$

If we multiply this congruence by c^*, we obtain

$$(1 - c^*d)(d - c^*) \equiv 0 \mod p^m.$$

Accordingly, $1 - c^*d \equiv 0 \mod p^j$, $d - c^* \equiv 0 \mod p^k$, where the nonnegative integers j, k are such that $j + k \geq m$. Since $c^* \equiv d \mod p^k$, we have $c \equiv d^* \mod p^k$. If we write $c = d^* + up^k$, $1 - c^*d = vp^j$, $u, v \in \mathbb{Z}$, we obtain

$$c(1 - c^*d) = d^*(1 - c^*d) + uvp^{j+k}$$

and $c - d \equiv d^* - c^* \mod p^{j+k}$. □

Proof of Theorem 1. Let $t > 0$, $t \equiv c - d \mod b$. Because b, c, d satisfy the condition (2), Lemma 1 yields $t \equiv d^* - c^* \mod b$. We replace, in the setting of Proposition 1, the number c by d^* and d by c^*. This gives

$$S(1 + ct, bt) - \left(\frac{t^2 + 2}{bt} - 3\right) = S(c^*, b) - S(d^*, b) = S(c, b) - S(d, b),$$

whence the assertion follows. □

3. Suitable Sets

Proof of Theorem 2. Let $t > 0$ be as in Theorem 2, i.e., $t \equiv c - d^* \mod b$. Since $S(c, b) = S(d^*, b)$, the numbers c and d^* satisfy the condition (2), and Theorem 1 gives

$$S(1 + ct, bt) = \frac{t^2 + 2}{bt} - 3. \tag{6}$$

By Lemma 1, we also have $t \equiv d - c^* \mod b$. Since $S(d, b) = S(c^*, b)$, Theorem 1 yields

$$S(1 + dt, bt) = \frac{t^2 + 2}{bt} - 3.$$

Accordingly, $S(c_1, b_1) = S(d_1, b_1)$ for $b_1 = bt$, $c_1 = 1 + ct$, and $d_1 = 1 + dt$.

It remains to be shown that $d_1 \not\equiv c_1, c_1^* \mod b_1$, $t > 1$, and $S(c_1, b_1) \neq 0$.

First we check $d_1 \not\equiv c_1 \mod b_1$. Since $d - c \not\equiv 0 \mod b$, we have $(d - c)t \not\equiv 0 \mod bt$. However,

$$d_1 - c_1 \equiv (d - c)t \mod bt,$$

whence the assertion follows.

We also have to exclude that d_1 is an inverse of $c_1 \mod b_1$. From

$$(1 + ct)(1 + dt) \equiv 1 \mod bt$$

we obtain

$$cdt^2 + (c + d)t \equiv 0 \mod bt \text{ and } cdt + c + d \equiv 0 \mod b.$$

If we use $t \equiv c - d^* \mod b$ in the last congruence, we obtain $c^2d + d \equiv 0 \mod b$, and so $c^2 \equiv -1 \mod b$. But this implies $S(c, b) = 0$ (see [9, Satz 1]), which we excluded.

Now we show $(t, b) > 1$. The congruences $c - d^* \equiv t \mod b$ and $d - c^* \equiv t \mod b$ imply $cd - 1 \equiv td \mod b$ and $cd - 1 \equiv tc \mod b$. In particular, $td \equiv tc \mod b$. Thus, if $(t, b) = 1$, we have $c \equiv d \mod b$, which we excluded. In particular, $t = 1$ is impossible.

If $S(c_1, b_1) = 0$, then $t^2 + 2 - 3bt = 0$, by (6). Therefore, $t \mid 2$, and so $t = 2$, since $t = 1$ is excluded. If $t = 2$, we have $6 - 6b = 0$, which implies $b = 1$. But in this case a suitable set $\{c, d\}$ does not exist. □

Remark 1. Recall the definition of the sequences b_i, $\{c_i, d_i\}$, $i \geq 0$, of Section 1. The congruence $t_{i+1} \equiv d_{i+1} - c_{i+1}^* \mod b_{i+1}$ implies $t_{i+1} \equiv d_{i+1} - c_{i+1}^* \mod t_i$. Since $c_{i+1} \equiv d_{i+1} \equiv 1 \mod t_i$, this gives $t_{i+1} \equiv 0 \mod t_i$ for all $i \geq 0$. So the numbers t_i form an ascending chain $t_0 \mid t_1 \mid t_2 \cdots$ of divisors.

Remark 2. If we are looking for a suitable set in order to start with a sequence of this type, we will be successful, as it seems, if we restrict our search to square-free numbers $b \geq 70$ consisting of exactly two primes ≥ 5. We present a small table of such numbers b together with suitable sets $\{c, d\}$. In all cases the Dedekind sum belonging to the suitable set is positive.

b	77	85	91	95	115	119	133	143
c	9	7	5	33	18	31	54	8
d	16	22	31	52	78	45	73	73

Remark 3. Suppose that we restrict t_i to the range $1 \leq t_i \leq b_i$ in the above sequence. It would be interesting to understand the limiting behaviour of the sequence $S(c_i, b_i)$, which, by (6), is equivalent to the behaviour of t_i/b_i.

Remark 4. Note that every set $\{c, d\}$ suitable for b defines three additional suitable sets, namely, $\{c, d^*\}$, $\{c^*, d\}$, and $\{c^*, d^*\}$. Each of these four sets defines an appropriate number t. Even if we restrict t to the range $1 \leq t \leq b$, we obtain, as a rule, four possibilities for $\{c, d\}$ and t. Of course, one may use these possibilities for the construction of $\{c_i, d_i\}$ and t_i in each step $i \geq 0$. In this way one obtains, instead of an infinite sequence, an infinite cascade of pairwise equal Dedekind sums.

Proof of Theorem 3. In the setting of this theorem, let $i \in \{1, \ldots, k\}$. Since 5 is a quadratic residue $\bmod p_i$, there is an integer α_i such that $\alpha_i^2 \equiv 5 \mod p_i$. Define $c \in \{1, \ldots, b\}$ by

$$c \equiv (3 + \alpha_i)/2 \mod p_i,\ i = 1, \ldots, k, \text{ and } c \equiv 1 \mod p_i,\ i = k+1, \ldots, r$$

(here 1/2 stands for an inverse of 2 mod p_i). Let $d \in \{1, \ldots, b\}$ be a solution of the congruence (2). This means that

$$(c - d)(cd - 1) \equiv 0 \mod p_i,$$

for all $i \in \{1, \ldots, r\}$. If $i \in \{k+1, \ldots, r\}$, this congruence is equivalent to $(1 - d)(1 - d) \equiv 0 \mod p_i$, i.e., $d \equiv 1 \equiv c \mod p_i$. If $i \in \{1, \ldots, k\}$, d must satisfy one of the congruences

$$d \equiv (3 + \alpha_i)/2 \mod p_i \text{ or } d \equiv (3 - \alpha_i)/2 \mod p_i,$$

since $(3 - \alpha_i)/2$ is an inverse of $(3 + \alpha_i)/2 \mod p_i$. Altogether, d can be defined by the congruences

$$d \equiv (3 + (-1)^{j_i}\alpha_i)/2 \mod p_i, i = 1, \ldots, k, \text{ and } d \equiv 1 \mod p_i, i = k+1, \ldots, r,$$

where $j_i \in \{0, 1\}$ may be arbitrary for each $i \in \{1, \ldots, k\}$. Accordingly, we have exactly 2^r distinct numbers $d \in \{1, \ldots, b-1\}$ such that the congruence (2) holds.

Observe that $(c,b)=1$ since an inverse c^* of $c \mod b$ is given by $c^* \equiv (3-\alpha_i)/2 \mod p_1$, $i=1,\ldots,k$, and $c^* \equiv 1 \mod p_i$, $i=k+1,\ldots,r$. Because the condition (2) is equivalent to $S(c,b)-S(d,b)\in\mathbb{Z}$, there are exactly 2^k integers $d\in\{1,\ldots,b-1\}$ such that $S(c,b)-S(d,b)\in\mathbb{Z}$.

Recall that $t=p_{k+1}\cdots p_r$. We have to show that $S(c,b)=S(d,b)=(t^2+2)/b-3$ for all these integers d. Given such an integer d, we define $m\in\{1,\ldots,b_0\}$ by $m\equiv d-1 \mod p_i$, $i=1,\ldots,k$. In other words, $m\equiv(1+(-1)^{j_i}\alpha_i)/2 \mod p_i$ for these numbers i. Then m is invertible mod b_0, an inverse m^* being defined by $m^*\equiv((-1)^{j_i}\alpha_i-1)/2 \mod p_i$ for these i. In particular, $m-m^*\equiv 1 \mod b_0$. Now $t\equiv 1\equiv m-m^* \mod b_0$. Since $S(m,b_0)=S(m^*,b_0)$, Theorem 1 can be applied to b_0, m, and m^*. It gives

$$S(1+mt,b_0t)=\frac{t^2+2}{b_0t}-3.$$

Here $1+mt\equiv 1+m\equiv d \mod p_i$, $i=1,\ldots,k$, and $1+mt\equiv 1\equiv d \mod p_i$, $i=k+1,\ldots,r$, because $p_i\,|\,t$ for these i. In other words, $1+mt\equiv d \mod b$, and so $S(d,b)=(t^2+2)/b-3$. In particular, $S(c,b)$ also takes this value, since this case corresponds to $j_1=\cdots=j_k=0$. □

Remark 5. Let b be a square-free number consisting of r primes. For an integer c with $(c,d)=1$ let $N(c,b)$ be defined as in (3). Let $r=3$. Hence $N(c,b)\le 8$, as we said at the end of Section 1. Theorem 3 says that 2, 4, and 8 are possible values greater than 1 of $N(c,b)$. It is not difficult to see that, for a square-free number b, $N(c,b)$ either equals 1 or is even. Therefore, the only possible value greater than 1 not in this list is $N(c,b)=6$. In the case $b=455=5\cdot 7\cdot 13$ we find $N(c,b)=6$ for $c=32$. On the other hand, there are no integers c with $N(c,b)=8$ in this case.

References

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

[2] M. Atiyah, The logarithm of the Dedekind η-function, *Math. Ann.* **278** (1987), 335–380.

[3] S. Boyer, D. Lines, Surgery formulae for Casson's invariant and extensions to homology lens spaces. *J. Reine Angew. Math.* **405** (1990), 181–220.

[4] U. Dieter, Beziehungen zwischen Dedekindschen Summen, *Abh. Math. Sem. Univ. Hamburg* **21** (1957), 109–125.

[5] K. Girstmair, Dedekind sums with predictable signs, *Acta Arith.* **83** (1998), 283–292.

[6] K. Girstmair, A criterion for the equality of Dedekind sums mod $\mathbb{Z}$, *Int. J. Number Theory* **10** (2014), 565–568.

[7] S. Jabuka, S. Robins, X. Wang, When are two Dedekind sums equal? *Int. J. Number Theory* **7** (2011), 2197–2202.

[8] C. Meyer, *Die Berechnung der Klassenzahl Abelscher Körper über Quadratischen Zahlkörpern*, Akademie-Verlag, Berlin, 1957.

[9] H. Rademacher, Zur Theorie der Dedekindschen Summen, *Math. Z.* **63** (1956), 445–463.

[10] H. Rademacher, E. Grosswald, *Dedekind Sums*, Mathematical Association of America, 1972.

[11] E. Tsukerman, Equality of Dedekind sums modulo $8\mathbb{Z}$, *Acta Arith.* **170** (2015), 67–72.

[12] G. Urzúa, Arrangements of curves and algebraic surfaces, *J. Algebraic Geom.* **19** (2010), 335–365.

[13] G. Urzúa and J. I. Yáñez, Characterization of Kollár surfaces, *Algebra Number Theory* **12** (2018), 1073–1105.