International Journal of Number Theory
Vol. 11, No. 8 (2015) 2325–2339

DOI: 10.1142/S1793042115501067

Dedekind sums $s(a, b)$ and inversions modulo b

Yiwang Chen

Department of Mathematics
University of Illinois at Urbana-Champaign
57 East Healey Street Apt. 204
Champaign, IL 61820, USA
ychen137@illinois.edu

Nicholas Dunn

Department of Mathematics
North Carolina State University at Raleigh
Raleigh, NC 27695, USA
njdunn2@ncsu.edu

Campbell Hewett* and Shashwat Silas†

Department of Mathematics, Brown University
69 Brown Street, Providence, RI 02912, USA
**campbell_hewett@brown.edu*
†*shashwat_silas@brown.edu*

Received 15 November 2014
Accepted 12 January 2015
Published 28 July 2015

We introduce the inversion polynomial for Dedekind sums $f_b(x) = \sum x^{\mathrm{inv}(a,b)}$ to study the number of $s(a, b)$ which have the same value for a given b. We prove several properties of this polynomial and present some conjectures. We also introduce connections between Kloosterman sums and the inversion polynomial evaluated at particular roots of unity. Finally, we improve on previously known bounds for the second highest value of the Dedekind sum and provide a conjecture for a possible generalization. Lastly, we include a new sufficient condition for the inequality of two Dedekind sums based on the reciprocity formula.

Keywords: Dedekind sum; Dedekind sum reciprocity law; inversion number; inversion polynomial.

Mathematics Subject Classification 2010: 11F20

1. Introduction

1.1. *The Dedekind sum*

Let a and b be relatively prime integers. The *Dedekind sum* $s(a,b)$ is given by

$$s(a,b) = \sum_{i=1}^{b-1} \frac{i}{b}\left(\left(\frac{ai}{b}\right)\right), \tag{1.1}$$

where

$$((x)) = \begin{cases} 0 & x \in \mathbb{Z}, \\ x - \lfloor x \rfloor - \dfrac{1}{2} & x \notin \mathbb{Z} \end{cases} \tag{1.2}$$

is the sawtooth function. Our motivating problem is to classify all a_1 and a_2 such that $s(a_1,b) = s(a_2,b)$ for a fixed b. Partial results are given by the following theorem in [1].

Theorem. *$s(a_1,b) - s(a_2,b) \in \mathbb{Z}$ if and only if $b \mid (a_1 - a_2)(a_1a_2 - 1)$.*

The problem is solved in the case where b is a prime power in [2].

1.2. *The inversion number*

Given a permutation σ of the numbers $\{1,2,\ldots,b\}$, define the *inversion number* of σ as

$$\mathrm{inv}(\sigma) = \#\{(i,j) \mid 1 \le i < j \le b, \sigma(i) > \sigma(j)\}. \tag{1.3}$$

If a is relatively prime to b, then the map $\sigma_a : \{1,2,\ldots,b\} \to \{1,2,\ldots,b\}$ given by $x \mapsto ax \pmod b$ is a permutation of $\{1,2,\ldots,b\}$. In this case define $\mathrm{inv}(a,b) = \mathrm{inv}(\sigma_a)$. The following is a fact due to Zolotarev.

Theorem. *For $(a,b) = 1$,*

$$\mathrm{inv}(a,b) = -3bs(a,b) + \frac{(b-1)(b-2)}{4}. \tag{1.4}$$

From this, one sees that for a given b, $s(a_1,b) = s(a_2,b)$ if and only if $\mathrm{inv}(a_1,b) = \mathrm{inv}(a_2,b)$.

1.3. *The inversion polynomial*

An advantage of the inversion number is that it is always a non-negative integer. Therefore, for a positive integer b, define the *inversion polynomial*

$$f_b(x) = \sum_{\substack{1 \le a \le b \\ (a,b)=1}} x^{\mathrm{inv}(a,b)}. \tag{1.5}$$

We focus most of our attention on exploring this polynomial because it suggests how often Dedekind sums take on certain values. Indeed, if cx^d is a term in $f_b(x)$, then exactly c different values of a have $\mathrm{inv}(a,b) = d$. There are existing bounds

on the number of such a that can take on the same Dedekind sum; as mentioned in [2], if b is square-free, it can be shown that for a given d, the number of a such that $s(a,b) = d$ cannot exceed 2^r, where r is the number of prime factors of b. A complete understanding of the inversion polynomial will give us the number of equal Dedekind sums. In our paper, we have been able to characterize many polynomial factors of f_b. For certain x, we also show that $f_b(x)$ can be written in terms of Kloosterman sums. We also present novel bounds on the smallest values of $\mathrm{inv}(a,b)$ for a given b.

1.4. *Elementary properties of the inversion polynomial*

A list of facts about the inversion polynomial is as follows.

(i) The degree of f_b is $\frac{(b-1)(b-2)}{2}$. The largest value $\mathrm{inv}(a,b)$ can take is

$$\mathrm{inv}(-1,b) = \frac{(b-1)(b-2)}{2} \tag{1.6}$$

because for every pair $1 \le i < j \le b-1$, $\sigma_{-1}(i) > \sigma_{-1}(j)$.

(ii) The constant term and the leading coefficient are both 1. If $\mathrm{inv}(a,b) = 0$, then we must have $a = 1$, and if $\mathrm{inv}(a,b) = \frac{(b-1)(b-2)}{2}$, then we must have $a = -1$. Translating this result into Dedekind sums using (1.4), we obtain a simple proof of the known fact

$$-\frac{(b-1)(b-2)}{12b} \le \mathrm{inv}(a,b) \le \frac{(b-1)(b-2)}{12b}. \tag{1.7}$$

(iii) The coefficients are symmetric. This follows from

$$\mathrm{inv}(a,b) + \mathrm{inv}(-a,b) = \frac{(b-1)(b-2)}{2}, \tag{1.8}$$

which is true because for $1 \le i < j \le b-1$, exactly one of $\sigma_a(i) > \sigma_a(j)$ and $\sigma_{-a}(i) > \sigma_{-a}(j)$ holds.

(iv) For b not divisible by three, there is a polynomial g such that $f_b(x) = g(x^3)$. In other words, if b is not divisible by three, $\mathrm{inv}(a,b)$ is divisible by three. To see this, rewrite (1.4) as

$$2\mathrm{inv}(a,b) = 3\left(-2bs(a,b) + \frac{(b-1)(b-2)}{6}\right). \tag{1.9}$$

When three does not divide b, the quantity in the parentheses is an integer, as shown in [4]. Three does not divide two, so three divides $\mathrm{inv}(a,b)$.

2. Overview of Results and Conjectures

2.1. *Factors of the inversion polynomial*

From decomposing the inversion polynomial into its irreducible factors for many b, it appears that $f_b(x)$ is the product of cyclotomic polynomials as well as exactly

one non-cyclotomic irreducible factor. The following is a conjecture (several parts of which are proved) which characterizes most of the cyclotomic factors. Throughout this paper, we use ζ_m to denote a primitive mth root of unity.

Conjecture 2.1. *For $b = ck$, ζ_{2k} and ζ_{6k} are roots of $f_b(x)$ precisely under the following conditions*:

(i) *If $c = 2 \pmod 4$, then ζ_{2k} and ζ_{6k} are roots of $f_b(x)$ precisely when $k = 4 \pmod 8$.*
(ii) *If $c = 0 \pmod 4$, then ζ_{2k} and ζ_{6k} are roots of $f_b(x)$ precisely when $k \neq 2 \pmod 4$ and $8 \nmid k$.*
(iii) *If $c = 3^m n$, $m \geq 1$, and $(n, 6) = 1$, then only ζ_{2k} is a root of $f_b(x)$ precisely when $3n \nmid k$ and c is not a square.*
(iv) *If $(c, 6) = 1$, then ζ_{2k} and ζ_{6k} are roots of $f_b(x)$ precisely when $c \nmid k$ and c is not a square.*

For some b, there do exist other roots ζ_m, where $m \nmid 2b$ and $m \nmid 6b$. Table 1 shows the first several roots ζ_m not accounted for in Conjecture 2.1.

Below we list several particular cases of Conjecture 2.1 whose proofs are known.

Proposition 2.2. *We can completely characterize the integers b for which $x + 1$ divides $f_b(x)$:*

$$f_b(-1) = \begin{cases} 0 & \text{if } b \text{ is an odd non-square or } 4 \mid b, \\ \varphi(b) & \text{if } b \text{ is an odd square or } b = 2 \pmod 4. \end{cases} \tag{2.1}$$

When b is an odd square or $b = 2 \pmod 4$, $\mathrm{inv}(a, b)$ takes only even values.

Table 1. All roots ζ_m not accounted for in Conjecture 2.1 up to $b = 242$.

b	Unexplained roots	b	Unexplained roots
8	ζ_{18}	136	ζ_{18}, ζ_{306}
18	ζ_{16}	138	ζ_{108}
22	ζ_{20}, ζ_{60}	148	ζ_{18}, ζ_{36}
26	ζ_{20}, ζ_{60}	173	ζ_{18}
29	ζ_{18}	186	ζ_{20}
40	ζ_{18}, ζ_{90}	198	ζ_{20}
45	ζ_8, ζ_{40}	200	ζ_{18}
46	ζ_{36}	204	ζ_{54}
56	ζ_{18}	296	ζ_{18}
57	ζ_{54}	317	ζ_{18}
70	ζ_{18}, ζ_{90}	325	ζ_{18}, ζ_{90}
74	ζ_{36}	332	ζ_{72}
80	ζ_{14}, ζ_{42}	345	ζ_{54}
83	ζ_{18}	362	ζ_{36}
114	ζ_{108}	398	ζ_{18}
117	ζ_8	424	ζ_{18}

The next result is not a special case of Conjecture 2.1 but is a classification of more particular roots.

Proposition 2.3. *For b any non-square integer* $1 \pmod 4$, -1 *is a double root of $f_b(x)$. If in addition three does not divide b, then ζ_6 is a double root of $f_b(x)$; that is, $(x^3+1)^2$ divides $f_b(x)$.*

When b is odd, the situation becomes more manageable. Our next result is explained by Conjecture 2.1 and includes one direction of Proposition 2.2 as a special case.

Proposition 2.4. *If $b = ck$, where b is odd, c is not square, and $(c,k) = 1$, then ζ_{2k} is a root $f_b(x)$. If b is not divisible by three, then ζ_{6k} is also a root of $f_b(x)$.*

For certain b, f_b takes values in terms of Kloosterman sums when evaluated on roots of unity. Here we define the Kloosterman sum

$$K(a,b,m) = \sum_{\substack{1\le x\le m\\(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^{-1})}, \tag{2.2}$$

where x^{-1} is the inverse of x modulo m.

Proposition 2.5. *Write $b = ck$. If $c = 0 \pmod 4$, we have*

$$f_b(e^{2\pi i/2k}) = \frac{1}{2} e^{\frac{2\pi i}{4k}} K\left(\frac{b}{4k}, \frac{b}{4k}, 2b\right). \tag{2.3}$$

So, (ii) *in Conjecture* 2.1 *now says that if $4k \mid b$, then $K(b/4k, b/4k, 2b) = 0$ precisely when $k \neq 2 \pmod 4$ and $8 \nmid k$.*

If k is even and $c = 2 \pmod 4$, we have

$$f_b(e^{2\pi i/2k}) = \frac{1}{4} i e^{\frac{2\pi i}{4k}} K\left(\frac{b}{2k}, \frac{b}{2k}(1-b), 4b\right). \tag{2.4}$$

Case (i) *in Conjecture* 2.1 *says k must be even, so it now becomes the statement that if k is even and $2k \mid b$ but $4k \nmid b$, then $K(b/2k, b(1-b)/2k, 4b) = 0$ precisely when $k = 4 \pmod 8$.*

2.2. *Smallest values of inversion number*

For a given b, we know that the smallest value of inversion number occurs at $\mathrm{inv}(1,b)$ and the largest at $\mathrm{inv}(-1,b)$. Here we prove a bound on the second smallest and second largest values, which improves on bounds given in [5, Sec. 6].

Proposition 2.6. *If $2 \le a \le b-2$, then*

$$\frac{b^2-1}{8} \le \mathrm{inv}(a,b) \le \frac{3b^2-12b+9}{8}. \tag{2.5}$$

If b is odd, then

$$\operatorname{inv}(2,b)=\frac{b^2-1}{8} \quad \textit{and} \quad \operatorname{inv}(-2,b)=\frac{3b^2-12b+9}{8}. \tag{2.6}$$

Translating this result into Dedekind sums using (1.4)*, we get*

$$-\frac{(b-1)(b-5)}{24b}\le s(a,b)\le\frac{(b-1)(b-5)}{24b}, \tag{2.7}$$

where

$$s(2,b)=\frac{(b-1)(b-5)}{24b} \quad \textit{and} \quad s(-2,b)=-\frac{(b-1)(b-5)}{24b}. \tag{2.8}$$

The above proposition is part of a larger conjecture about the six smallest values of inversion number.

Conjecture 2.7. *Let $I_n(b)$ be the nth smallest value of* $\operatorname{inv}(a,b)$ *for fixed b and $1\le n\le 6$. Then*

$$I_n(b)\ge\frac{(n-1)(b+1)(b+1-n)}{4n}, \tag{2.9}$$

with equality occurring with

$$\operatorname{inv}(n,b)=\frac{(n-1)(b+1)(b+1-n)}{4n} \tag{2.10}$$

when $b\equiv -1 \pmod{n}$.

We suspect that this conjecture can be proved in a manner similar to the proof of Proposition 2.6 given below.

The following result is a novel condition on a_1 and a_2 such that $s(a_1,b)\neq s(a_2,b)$.

Proposition 2.8. *Suppose we have $1\le a_1,a_2\le b-1$ such that $b\equiv r \pmod{a_1}$, $b\equiv r \pmod{a_2}$, $a_1\equiv a_2 \pmod{r}$, and* $\operatorname{inv}(a_1,b)=\operatorname{inv}(a_2,b)$*. Then $a_1=a_2$.*

In other words, if $b\equiv r \pmod{a_1}$, $b\equiv r \pmod{a_2}$, $a_1\equiv a_2 \pmod{r}$, and $a_1\neq a_2$, then $s(a_1,b)\neq s(a_2,b)$. Note that we do not require $r\le a_1,a_2$.

3. Proofs of Propositions

Many of the proofs rely on the following well-known theorem, known as the reciprocity formula for Dedekind sums.

Theorem 3.1. *For $(a,b)=1$,*

$$s(a,b)+s(b,a)=\frac{1}{12}\left(\frac{a}{b}+\frac{1}{ab}+\frac{b}{a}\right)-\frac{1}{4}. \tag{3.1}$$

In terms of inversion number, (1.4) *and* (3.1) *become*

$$a\operatorname{inv}(a,b)+b\operatorname{inv}(b,a)=\frac{(a-1)(b-1)(a+b-1)}{4}. \tag{3.2}$$

Proof of Proposition 2.2. First take the case where b is odd. Then we use Zolotarev's theorem

$$(-1)^{\mathrm{inv}(a,b)} = \left(\frac{a}{b}\right), \tag{3.3}$$

where $(\frac{a}{b})$ is the Jacobi symbol, to compute

$$f_b(-1) = \sum_{(a,b)=1} (-1)^{\mathrm{inv}(a,b)} = \sum_{(a,b)=1} \left(\frac{a}{b}\right) = \begin{cases} 0 & \text{if } b \text{ is not a square,} \\ \varphi(b) & \text{if } b \text{ is a square.} \end{cases} \tag{3.4}$$

Now take the case where b is even. If $4 \mid b$, then from

$$\mathrm{inv}(a,b) + \mathrm{inv}(-a,b) = \frac{(b-1)(b-2)}{2} = 1 \pmod 2, \tag{3.5}$$

we know that one of $\mathrm{inv}(a,b)$ and $\mathrm{inv}(-a,b)$ is even and the other is odd. It follows that

$$f_b(-1) = \sum_{(a,b)=1} (-1)^{\mathrm{inv}(a,b)} = 0. \tag{3.6}$$

If $b = 2 \pmod 4$, then from reducing (3.2) modulo 2,

$$\begin{aligned} \mathrm{inv}(a,b) &= \frac{1}{4} a^{-1}(a-1)(b-1)(a+b-1) \\ &= \left(\frac{a-1}{2}\right)\left(\frac{a-1}{2} + \frac{b}{2}\right) \\ &= \left(\frac{a-1}{2}\right)\left(\frac{a-1}{2} + 1\right) = 0 \pmod 2. \end{aligned} \tag{3.7}$$

It follows that $f_b(-1) = \varphi(b)$. □

Proof of Proposition 2.3. First we show that -1 is a root of $f_b'(x)$. Then we show that when b is not divisible by three, $e^{\pi i/3}$ is a root of both $f_b(x)$ and $f_b'(x)$. First compute

$$\mathrm{inv}(-a,b)\left(\frac{-a}{b}\right) = \left(\frac{(b-1)(b-2)}{2} - \mathrm{inv}(a,b)\right)\left(\frac{a}{b}\right), \tag{3.8}$$

because of (1.8) and $(\frac{-1}{b}) = 1$. In other words,

$$\mathrm{inv}(-a,b)\left(\frac{-a}{b}\right) + \mathrm{inv}(a,b)\left(\frac{a}{b}\right) = \frac{(b-1)(b-2)}{2}\left(\frac{a}{b}\right). \tag{3.9}$$

Write

$$\begin{aligned} x f_b'(x) &= \sum_{(a,b)=1} \mathrm{inv}(a,b) x^{\mathrm{inv}(a,b)} \\ &= \frac{1}{2}\left(\sum_{(a,b)=1} \mathrm{inv}(a,b) x^{\mathrm{inv}(a,b)} + \sum_{(a,b)=1} \mathrm{inv}(-a,b) x^{\mathrm{inv}(-a,b)}\right) \end{aligned} \tag{3.10}$$

so that

$$-2f_b'(-1) = \sum_{(a,b)=1} \mathrm{inv}(a,b)\left(\frac{a}{b}\right) + \sum_{(a,b)=1} \mathrm{inv}(-a,b)\left(\frac{-a}{b}\right)$$
$$= \frac{(b-1)(b-2)}{2} \sum_{(a,b)=1} \left(\frac{a}{b}\right) = 0. \tag{3.11}$$

Now assume b is not divisible by three. Then, by (iv) in Sec. 1.4,

$$f_b(e^{\pi i/3}) = \sum_{(a,b)=1} (e^{\pi i/3})^{\mathrm{inv}(a,b)} = \sum_{(a,b)=1} (e^{\pi i})^{\mathrm{inv}(a,b)/3}$$
$$= \sum_{(a,b)=1} (-1)^{\mathrm{inv}(a,b)/3} = \sum_{(a,b)=1} ((-1)^3)^{\mathrm{inv}(a,b)/3} = 0. \tag{3.12}$$

Using the same reasoning, we see that $f_b'(e^{\pi i/3}) = 0$. □

Proof of Proposition 2.4. Reduce (3.2) modulo k to get

$$4a\,\mathrm{inv}(a,b) = -(a-1)^2 \pmod{k}. \tag{3.13}$$

Then, because b is odd, we have from Zolotarev's theorem

$$\mathrm{inv}(a,b) = \frac{1}{2}\left(\left(\frac{a}{b}\right) - 1\right) \pmod 2 \tag{3.14}$$

and by the Chinese remainder theorem,

$$\mathrm{inv}(a,b) = -(4a)^{-1}(a-1)^2(k+1) + \frac{1}{2}\left(\left(\frac{a}{b}\right) - 1\right)k \pmod{2k}. \tag{3.15}$$

Now we show that $e^{2\pi i/(2k)}$ is a root of $f_b(x)$ and $e^{2\pi i/(6k)}$ is a root as well if b is not divisible by 3. Compute

$$f_b(e^{2\pi i/(2k)}) = \sum_{(a,b)=1} e^{2\pi i\,\mathrm{inv}(a,b)\frac{1}{2k}}$$
$$= \sum_{(a,b)=1} e^{\pi i\frac{1}{k}(-(4a)^{-1}(a-1)^2(k+1)+\frac{1}{2}((\frac{a}{b})-1)k)}$$
$$= \sum_{(a,b)=1} e^{\pi i\frac{1}{k}(-(4a)^{-1}(a-1)^2(k+1))}(-1)^{\frac{1}{2}((\frac{a}{b})-1)}$$
$$= \sum_{(a,b)=1} e^{\pi i\frac{1}{k}(-(4a)^{-1}(a-1)^2(k+1))}\left(\frac{a}{b}\right). \tag{3.16}$$

Now, write $a = qk + r$ for q and r such that $(r,k) = 1$ and $(qk + r, c) = 1$. This is a valid parametrization of the values of a because $(c,k) = 1$. The above equation

becomes

$$
\begin{aligned}
&= \sum_{(r,k)=1} \sum_{(qk+r,c)=1} e^{\pi i \frac{1}{k}(-(4(qk+r))^{-1}(qk+r-1)^2(k+1))} \left(\frac{qk+r}{ck}\right) \\
&= \sum_{(r,k)=1} \sum_{(qk+r,c)=1} e^{\pi i \frac{1}{k}(-(4r)^{-1}(qk+r-1)^2(k+1))} \left(\frac{qk+r}{c}\right)\left(\frac{r}{k}\right) \\
&= \sum_{(r,k)=1} e^{\pi i \frac{1}{k}(-(4r)^{-1}(r-1)^2(k+1))} \left(\frac{r}{k}\right) \\
&\quad \times \sum_{(qk+r,c)=1} e^{\pi i \frac{1}{k}(-(4r)^{-1}(q^2k^2+2qk(r-1))(k+1))} \left(\frac{qk+r}{c}\right) \\
&= \sum_{(r,k)=1} e^{\pi i \frac{1}{k}(-(4r)^{-1}(r-1)^2(k+1))} \left(\frac{r}{k}\right) \\
&\quad \times \sum_{(qk+r,c)=1} e^{\pi i(-(4r)^{-1}(q^2k+2q(r-1))(k+1))} \left(\frac{qk+r}{c}\right) \\
&= \sum_{(r,k)=1} e^{\pi i \frac{1}{k}(-(4r)^{-1}(r-1)^2(k+1))} \left(\frac{r}{k}\right) \\
&\quad \times \sum_{(qk+r,c)=1} e^{\pi i(-(4r)^{-1}q^2k(k+1))} \left(\frac{qk+r}{c}\right). \qquad (3.17)
\end{aligned}
$$

Then, $k(k+1)$ is always even, so this is

$$
= \sum_{(r,k)=1} e^{\pi i \frac{1}{k}(-(4r)^{-1}(r-1)^2(k+1))} \left(\frac{r}{k}\right) \sum_{(qk+r,c)=1} \left(\frac{qk+r}{c}\right) = 0 \qquad (3.18)
$$

because c is not a square. If b is not divisible by three, then $e^{2\pi i/(6k)}$ is a root for the same reason as in the proof of Proposition 2.3. □

Proof of Proposition 2.5. If $c = 0 \pmod 4$, then $4k \mid b$. Then we know

$$
\operatorname{inv}(a,b) = -a^{-1}\left(\frac{a-1}{2}\right)^2 \pmod{2k} \qquad (3.19)
$$

by reducing (3.2) modulo $2k$. Here we denote a^{-1} as the inverse of a modulo $4b$. Then,

$$
\begin{aligned}
f_b(e^{2\pi i/2k}) &= \sum_{(a,b)=1} e^{\frac{2\pi i}{2k}(-a^{-1}(\frac{a-1}{2})^2)} \\
&= \sum_{(a,b)=1} e^{\frac{2\pi i}{8k}(-a^{-1}(a^2-2a+1))}
\end{aligned}
$$

$$= e^{\frac{2\pi i}{4k}} \sum_{(a,b)=1} e^{\frac{2\pi i}{8k}(a+a^{-1})}$$
$$= e^{\frac{\pi i}{4k}} \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+a^{-1})}. \tag{3.20}$$

Because $c = 0 \pmod 4$, we have $(a+b)^{-1} = a^{-1} + b \pmod{2b}$. To see this,

$$(a+b)(a^{-1}+b) = 1 + (a+a^{-1})b + b^2 = 1 \pmod{2b} \tag{3.21}$$

because a and a^{-1} are both odd and b is even:

$$\begin{aligned} K\left(\frac{c}{4}, \frac{c}{4}, 2b\right) &= \sum_{(a,2b)=1} e^{\frac{2\pi i}{8b}c(a+a^{-1})} \\ &= \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+a^{-1})} + \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c((a+b)+(a+b)^{-1})} \\ &= \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+a^{-1})} + e^{\frac{2\pi i}{4}c} \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+a^{-1})} \\ &= 2 \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+a^{-1})}. \end{aligned} \tag{3.22}$$

Hence, (3.20) is

$$f_b(e^{2\pi i/2k}) = \frac{1}{2} e^{\frac{2\pi i}{4k}} K\left(\frac{b}{4k}, \frac{b}{4k}, 2b\right). \tag{3.23}$$

Now assume k is even. If $c = 2 \pmod 4$, then, using the same procedure, we start with

$$\mathrm{inv}(a,b) = -a^{-1}\left(\frac{a-1}{2}\right)^2 - a^{-1}\left(\frac{a-1}{2}\right)\frac{b}{2} \pmod{2k}, \tag{3.24}$$

which is again (3.2) reduced modulo $2k$. So then the analogous form of (3.20) is

$$\begin{aligned} f_b(e^{2\pi i/2k}) &= \sum_{(a,b)=1} e^{\frac{2\pi i}{2k}(-a^{-1}(\frac{a-1}{2})^2 - a^{-1}(\frac{a-1}{2})\frac{b}{2})} \\ &= \sum_{(a,b)=1} e^{-\frac{2\pi i}{8k}a^{-1}(a^2-2a+1+ab-b)} \\ &= \sum_{(a,b)=1} e^{-\frac{2\pi i}{8k}(a-2+a^{-1}+b-ba^{-1})} \\ &= e^{\frac{2\pi i}{8k}(2-b)} \sum_{(a,b)=1} e^{\frac{2\pi i}{8k}(a+(1-b)a^{-1})} \\ &= ie^{\frac{2\pi i}{4k}} \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+(1-b)a^{-1})}. \end{aligned} \tag{3.25}$$

Following the steps we did before, we see that $(a+jb)^{-1} = a^{-1} - jb \pmod{4b}$. To see this,

$$\begin{aligned}(a+jb)(a^{-1}-jb) &= 1-(a-a^{-1})jb - j^2b^2 \\ &= 1 - a^{-1}(a^2-1)jb - j^2b^2 = 1 \pmod{4b} \end{aligned} \tag{3.26}$$

because a^2-1 and b are both divisible by four. Then,

$$\begin{aligned} K\left(\frac{c}{2}, \frac{c}{2}(1-b), 4b\right) &= \sum_{(a,4b)=1} e^{\frac{2\pi i}{8b}c(a+(1-b)a^{-1})} \\ &= \sum_{j=0}^{3} \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c((a+jb)+(1-b)(a+jb)^{-1})} \\ &= \sum_{j=0}^{3} \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c((a+jb)+(1-b)(a^{-1}-jb))} \\ &= \sum_{j=0}^{3} \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+(1-b)a^{-1}+jb^2)} \\ &= 4 \sum_{(a,b)=1} e^{\frac{2\pi i}{8b}c(a+(1-b)a^{-1})}. \end{aligned} \tag{3.27}$$

So (3.25) becomes

$$f_b(e^{2\pi i/2k}) = \frac{1}{4} i e^{\frac{2\pi i}{4k}} K\left(\frac{b}{2k}, \frac{b}{2k}(1-b), 4b\right). \tag{3.28}$$

□

Proof of Proposition 2.6. Because the polynomial is symmetric, it is enough to show the first inequality. We proceed by induction on b. This can be easily verified for small values of b. Now, suppose the statement is true up to $b-1$. First take the case $b \neq \pm 1 \pmod{a}$. Then from

$$\mathrm{inv}(a,b) = \frac{(a-1)(b-1)(a+b-1)}{4a} - \frac{b}{a}\mathrm{inv}(b,a), \tag{3.29}$$

we get

$$\begin{aligned} \mathrm{inv}(a,b) &\geq \frac{(a-1)(b-1)(a+b-1)}{4a} - \frac{b}{a}\left(\frac{3a^2-12a+9}{8}\right) \\ &= -\frac{1}{8}(b+2)a + \frac{1}{4}(b^2+3b+2) - \frac{1}{8}(2b^2+5b+2)\frac{1}{a} =: F(a). \end{aligned} \tag{3.30}$$

We may compute the minimum value $F(a)$ takes on the interval $3 \leq a \leq b-2$ (note that if $b \neq \pm 1 \pmod{a}$, then $a \neq 2$). Its derivative is

$$\frac{d}{da}F(a) = -\frac{1}{8}(b+2) + \frac{1}{8}(2b^2+5b+2)\frac{1}{a^2}. \tag{3.31}$$

This has a zero at $a = \sqrt{2b+1}$, which is inside the interval, but it is a maximum because the second derivative is negative:

$$\frac{d^2}{da^2}F(a) = -\frac{1}{4}(2b^2+5b+2)\frac{1}{a^3}. \tag{3.32}$$

So, we check the end points

$$F(3) = \frac{b^2+b-2}{6} = \frac{b^2+4b-5}{24} + \frac{b^2-1}{8} \tag{3.33}$$

and

$$F(b-2) = \frac{b^3+2b^2-9b-18}{8b-16} = \frac{b^2-2b+5}{2b-4} + \frac{b^2-1}{8}. \tag{3.34}$$

The fraction $(b^2+4b-5)/24$ is positive for $b > 1$, so $F(3) > (b^2-1)/8$. The fraction $(b^2-2b+5)/(2b-4)$ is always positive as well. To see this, note that the largest root of b^2-2b+5 is $1+\sqrt{6} \approx 3.449$, so for $b \geq 4$, the numerator and denominator are both positive. This tells us that for $b \geq 4$, $F(b-2) > (b^2-1)/8$.

Now take the case where $b = 1 \pmod{a}$. Then $\operatorname{inv}(b,a) = \operatorname{inv}(1,a) = 0$, so

$$\begin{aligned}\operatorname{inv}(a,b) &= \frac{(a-1)(b-1)(a+b-1)}{4a} \\ &= \frac{1}{4}(b-1)a + \frac{1}{4}(b^2-3b+2) - \frac{1}{4}(b^2-2b+1)\frac{1}{a} =: G(a).\end{aligned} \tag{3.35}$$

Note that $G(a)$ is increasing for $b \geq 2$ because its derivative is positive:

$$\frac{d}{da}G(a) = \frac{1}{4}(b-1) + \frac{1}{4}(b-1)^2\frac{1}{a^2}. \tag{3.36}$$

So,

$$\operatorname{inv}(a,b) \geq G(2) = \frac{b^2-1}{8}. \tag{3.37}$$

For the last case, $b = -1 \pmod{a}$, we have $\operatorname{inv}(b,a) = \operatorname{inv}(-1,a) = (a-1)(a-2)/2$, so

$$\begin{aligned}\operatorname{inv}(a,b) &= \frac{(a-1)(b-1)(a+b-1)}{4a} - \frac{b}{a}\frac{(a-1)(a-2)}{2} \\ &= -\frac{1}{4}(b+1)a + \frac{1}{4}(b^2+3b+2) - \frac{1}{4}(b^2+2b+1)\frac{1}{a} =: H(a).\end{aligned} \tag{3.38}$$

As in the case of $F(a)$, we can compute the minimum value it takes in the interval $2 \leq a \leq b-2$. Compute the derivative

$$\frac{d}{da}H(a) = -\frac{1}{4}(b+1) + \frac{1}{4}(b+1)^2\frac{1}{a^2}. \tag{3.39}$$

This has a zero at $a = \sqrt{b+1}$, which is inside the interval for $b \geq 2$, but it is a maximum because the second derivative is negative:

$$\frac{d^2}{da^2}H(a) = -\frac{1}{2}(b+1)^2\frac{1}{a^3}. \tag{3.40}$$

So, we check the end points

$$H(2) = \frac{b^2-1}{8}. \tag{3.41}$$

The other end point actually does get smaller than $(b^2-1)/8$, but if $b \equiv -1 \pmod{a}$, then $a \le (b+1)/2$. Thus, we only need to look at the end point

$$H\left(\frac{b+1}{2}\right) = \frac{b^2-1}{8}. \tag{3.42}$$

Therefore, in all cases, $\operatorname{inv}(a,b)$ gets no lower than $(b^2-1)/8$. □

Proof of Proposition 2.8. One can show by induction on n and using (3.2) that if we have the following sequence

$$r_{-1} = b, \quad r_0 = a, \quad r_1, r_2, r_3, \ldots, r_n, r_{n+1} = 1 \tag{3.43}$$

where $r_{j+2} = r_j \pmod{r_{j+1}}$ for all $-1 \le j \le n-1$, then

$$\begin{aligned}\operatorname{inv}(a,b) = {} & \frac{a-1}{4a}b^2 \\ & + \left(\frac{(a-1)(a-2)}{4a} + \frac{1}{4}\sum_{j=1}^{n}\frac{(-1)^j}{r_j r_{j-1}}(r_j-1)(r_{j-1}-1)(r_j+r_{j-1}-1)\right) \\ & \times b - \frac{(a-1)^2}{4a}.\end{aligned} \tag{3.44}$$

From this, if $\operatorname{inv}(a_1,b) = \operatorname{inv}(a_2,b)$,

$$\begin{aligned}0 = {} & \left(\frac{a_1-1}{4a_1} - \frac{a_2-1}{4a_2}\right)b^2 \\ & + \left(\frac{(a_1-1)(a_1-2)}{4a_1} - \frac{(a_2-1)(a_2-2)}{4a_2} - \frac{(a_1-1)(r-1)(a_1+r-1)}{4a_1 r}\right. \\ & \left. + \frac{(a_2-1)(r-1)(a_2+r-1)}{4a_2 r}\right)b - \left(\frac{(a_1-1)^2}{4a_1} - \frac{(a_2-1)^2}{4a_2}\right) \\ = {} & -\frac{1}{4a_1} - \frac{a_1}{4} + \frac{1}{4a_2} + \frac{a_2}{4} - \frac{b^2}{4a_1} + \frac{b^2}{4a_2} + \frac{b}{4a_1 r} \\ & + \frac{a_1 b}{4r} - \frac{b}{4a_2 r} - \frac{a_2 b}{4r} + \frac{br}{4a_1} - \frac{br}{4a_2} \\ = {} & \frac{1}{a_1}\left(-\frac{1}{4} + \frac{b}{4r}\right)(a_1-a_2)\left(a_1 - \frac{1}{a_2} + \frac{br}{a_2}\right).\end{aligned} \tag{3.45}$$

This means that $a_1 = a_2$ or $a_1 = (1-br)/a_2$. The second one is impossible if $1 \le a_1, a_2 \le b-1$, so $a_1 = a_2$. □

4. Directions for Further Research

As mentioned above, understanding all of the factors of f_b will tell us the number of equal Dedekind sums. In this effort, it would be of great interest to discover a more general version of Conjecture 2.1 which covers the cyclotomic roots not classified in our paper. It would also be necessary to understand the large non-cyclotomic irreducible factor of the inversion polynomial. From analyzing the roots of f_b for many b, some patterns are apparent. For example, all roots which are not on the unit circle belong to the large non-cyclotomic irreducible factor; however, this factor does contain roots on the unit circle as well. Figure 1 shows plots of the roots of f_b for $b = 11$, 14, and 21.

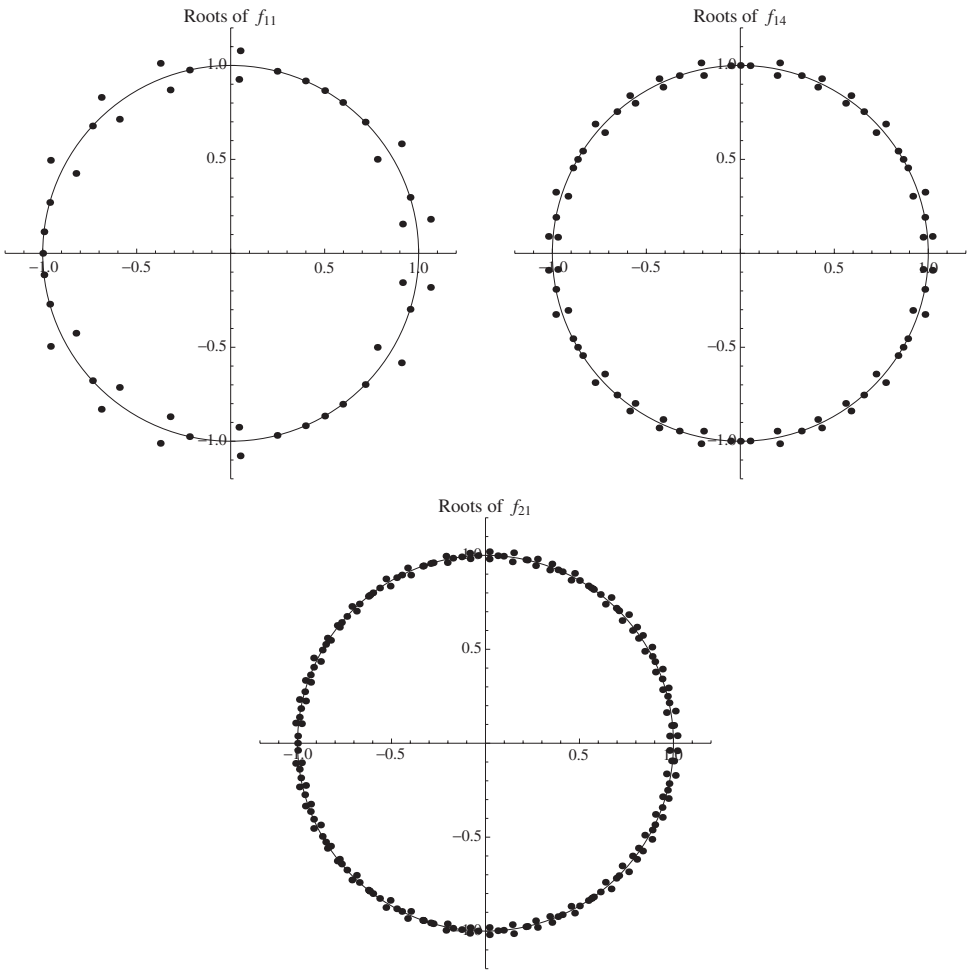

Fig. 1. The roots of f_{11}, f_{14}, and f_{21} respectively, plotted on the complex plane.

One can show, using Proposition 2.6 and Rouche's theorem that if x is a root of f_b, then

$$e^{-\frac{8\log\varphi(b)}{b^2-1}} < |x| < e^{\frac{8\log\varphi(b)}{b^2-1}}. \tag{4.1}$$

By analyzing the roots of the f_b, it may be possible to arrive at bounds for the coefficients.

Acknowledgments

We would like the thank Professor Sinai Robins for his invaluable advice and guidance through this project. He introduced us to the Dedekind sums problem through his previous work, [3]. We also appreciate advice and gracious help of Le Quang Nhat and Emmanuel Tsukerman. This project was funded by ICERM, the Brown UTRA program and the Brown University Department of Mathematics. We are very grateful for their trust and support.

References

[1] K. Girstmair, A criterion for the equality of Dedekind sums, *Int. J. Number Theory* **10**(3) (2014) 565–568.
[2] ———, On Dedekind sums with equal values, preprint (2014); arxiv:1404.4428.
[3] S. Jabuka, S. Robins and X. Wang, When are two Dedekind sums equal?, *Int. J. Number Theory* **7**(8) (2011) 2197–2202.
[4] H. Rademacher, *Dedekind Sums*, The Carus Mathematical Monographs, No. 16 (Mathematical Association of America, 1972).
[5] E. Tsukerman, Fourier–Dedekind sums and an extension of Rademacher reciprocity, *Ramanujan J.* **37** (2015) 421–460.