Dedekind Sums with Equal Values

Yiwang Chen, Nicholas Dunn, Campbell Hewett and Shashwat Silas

Brown University

August 6, 2014
The Dedekind sum $s(a, b)$ for $(a, b) = 1$ is defined by,

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

where $(\cdot)$ denotes the sawtooth function,

$$((x)) = \begin{cases} 
    x - \lfloor x \rfloor - \frac{1}{2} & \text{if } x \notin \mathbb{Z} \\
    0 & \text{if } x \in \mathbb{Z}
\end{cases}$$

We would like to be able to characterize $a_1, a_2$ such that $s(a_1, b) = s(a_2, b)$
Overview

1. Conjectures for when \( b \) is a prime power in \( s(a, b) \)
2. Generating Functions I
3. Generating Functions II
4. On the Number of Inversions
\[ s(a, b) = s(a + kb, b) \text{ for } k \in \mathbb{Z}. \]

\[
\begin{align*}
   s(a + kb, b) &= \sum_{i=1}^{b-1} \left( \left( \frac{i}{b} \right) \left( \frac{(a + kb)i}{b} \right) \right) \\
   &= \sum_{i=1}^{b-1} \left( \left( \frac{i}{b} \right) \left( \frac{ai + kbi}{b} \right) \right) \\
   &= \sum_{i=1}^{b-1} \left( \left( \frac{i}{b} \right) \left( \frac{ai}{b} \right) \right) = s(a, b)
\end{align*}
\]

\[ s(a_1, b) = s(a_2, b) \text{ if } a_1a_2 \equiv 1 \pmod{b}. \]

\[
\begin{align*}
   s(a_1, b) &= \sum_{i=1}^{b-1} \left( \left( \frac{i}{b} \right) \left( \frac{a_1i}{b} \right) \right) \\
   &= \sum_{i=1}^{b-1} \left( \left( \frac{a_2i}{b} \right) \left( \frac{a_2a_1i}{b} \right) \right) = s(a_2, b)
\end{align*}
\]

\[ s(a, b) + s(b, a) = -\frac{1}{4} + \frac{1}{12} \left( \frac{a}{b} + \frac{1}{ab} + \frac{b}{a} \right) \]

Remark: This allows us to compute Dedekind Sums fast.
Here’s a simple graph of what $s(a, 37)$ looks like,
Here’s a graph of many values of $b$ (divided by $b$ on both axes),

This gives a few insights especially relating to the highest/n–th highest values of the function. But doesn’t tell us much about the equality.
Visualization Strategies ($b$ is prime)

But then we came up with another visualization which was somewhat more fruitful for a while,

Each of the axes range up to $b$. 
A Theorem by Jabuka, Robins and Wang

Let $b$ be a positive integer and $a_1, a_2$ any two integers that are relatively prime to $b$. If $s(a_1, b) = s(a_2, b)$, then $b \mid (a_1a_2 - 1)(a_1 - a_2)$.

This is gives us the corollary that when $b$ is prime, $s(a_1, b) = s(a_2, b) \iff a_1 \equiv a_2 \pmod{b}$ or if $a_1a_2 \equiv 1 \pmod{b}$.

So all equal Dedekind Sums can be explained by the previous two one line proofs when $b$ is prime. Let’s take a look at our old picture again.
The red dots correspond to pairs which are inverses mod $b$ and the blue ones obviously correspond to ones that are the same mod $b$. 
What About the $b = p^2$?

We looked at the same kinds of graphs again,

The green dots correspond to pairs which are inverses mod $b$ and the blue ones correspond to ones that are the same mod $b$. And the red dots are the ones which are aren’t in either of those cases.
They look suspiciously well organized, so we were able to guess what lines they lie on.

The lines in each graph are $kp \pm 1$ for $0 < k < p$ and $k \in \mathbb{Z}$. 
This led us to the conjecture:

\[ s(a_1, p^2) = s(a_2, p^2) \] if and only if one of the following is true:

(i) \( a_1 = a_2 \pmod{p^2} \),
(ii) \( a_1 = a_2^{-1} \pmod{p^2} \),
(iii) \( a_1 = a_2 = \pm 1 \pmod{p} \).

That is, the non–trivial pairs can be given by,

\[
\begin{align*}
    s(kp - 1, p^2) &= \frac{(p - 1)(p + 1)}{6p^2} = \frac{1}{6} - \frac{1}{6p^2}, \\
    s(kp + 1, p^2) &= -\frac{(p - 1)(p + 1)}{6p^2} = -\frac{1}{6} + \frac{1}{6p^2}.
\end{align*}
\]
From $p^n|(a_1 - a_2)(a_1a_2 - 1)$, we know

$$a_1 = a_2 \pmod{p^k} \text{ and } a_1 = a_2^{-1} \pmod{p^{n-k}}$$

for some $k$. 
For $b = p^n$, some nontrivial pairs are given by

\[ s(kp^{n-m} - 1, p^n) = -\frac{p^{2n-2m} - 3p^n + 2}{12p^n} = \frac{1}{4} - \frac{p^{n-2m}}{12} - \frac{1}{6p^n}, \]

and

\[ s(kp^{n-m} + 1, p^n) = \frac{p^{2n-2m} - 3p^n + 2}{12p^n} = -\frac{1}{4} + \frac{p^{n-2m}}{12} + \frac{1}{6p^n} \]

for $1 \leq m \leq n/2$ and $(k, p) = 1$. 
For the $b = pq$ case, there were no clear patterns.
Some roots of the polynomial on the complex plane for various $b$:

Some are on the unit circle, and some are roots of unity.
A plot of sizes of roots (blue dots) for several values of $b$:

They are bounded by

$$e^{-\frac{8 \log \varphi(b)}{b^2-1}} < x < e^{\frac{8 \log \varphi(b)}{b^2-1}}$$
Some factorizations of the polynomial:

<table>
<thead>
<tr>
<th>$b$</th>
<th>$f_b(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$1$</td>
</tr>
<tr>
<td>3</td>
<td>$1 + x$</td>
</tr>
<tr>
<td>4</td>
<td>$(1 + x)(1 - x + x^2)$</td>
</tr>
<tr>
<td>5</td>
<td>$(1 + x)^2(1 - x + x^2)^2$</td>
</tr>
<tr>
<td>6</td>
<td>$(1 + x^2)(1 - x^2 + x^4 - x^6 + x^8)$</td>
</tr>
<tr>
<td>7</td>
<td>$(1 + x)(1 - x + x^2)(1 - x^3 + 3x^6 - x^9 + x^{12})$</td>
</tr>
<tr>
<td>8</td>
<td>$(1 + x)(1 - x + x^2)(1 + x^4)(1 - x^3 + x^6)(1 - x^4 + x^8)$</td>
</tr>
<tr>
<td>9</td>
<td>$1 + 2x^{10} + 2x^{18} + x^{28}$</td>
</tr>
<tr>
<td>10</td>
<td>$(1 + x^2)^2(1 - x^2 + x^4)^2(1 - x^6 + x^{12})^2$</td>
</tr>
<tr>
<td>11</td>
<td>$(1 + x)(1 - x + x^2)(1 - x^3 + x^6 - x^9 + x^{12} + x^{15} + x^{18} - x^{21} + x^{24} + x^{27} + x^{30} - x^{33} + x^{36} - x^{39} + x^{42})$</td>
</tr>
<tr>
<td>12</td>
<td>$(1 + x)(1 - x + x^2)(1 - x^3 + x^6)(1 - x^9 + x^{18})(1 - x^4 + x^8 - x^{12} + x^{16} - x^{20} + x^{24})$</td>
</tr>
<tr>
<td>13</td>
<td>$(1 + x)^2(1 - x + x^2)^2(1 - 2x^3 + 3x^6 - 4x^9 + 5x^{12} - 6x^{15} + 7x^{18} - 6x^{21} + 5x^{24} - 4x^{27} + 5x^{30} - 4x^{33} + 5x^{36} - 6x^{39} + 7x^{42} - 6x^{45} + 5x^{48} - 4x^{51} + 3x^{54} - 2x^{57} + x^{60})$</td>
</tr>
<tr>
<td>14</td>
<td>$(1 + x^2)(1 - x^2 + x^4)(1 - x^6 + x^{12} - x^{18} + x^{24} + x^{30} - x^{36} + x^{42} + x^{48} - x^{54} + x^{60} - x^{66} + x^{72})$</td>
</tr>
</tbody>
</table>
Proposition. \((x + 1)|f_b(x)\) precisely when \(b\) is odd and not a square or when \(4|b\).

Proof.

If \(b\) is odd, then \((-1)^{\text{inv}(a,b)} = \left(\frac{a}{b}\right)\). Hence,

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

When \(b\) is even, it turns out

\[
(-1)^{\text{inv}(a,b)} = \begin{cases} (-1)^{\frac{a-1}{2}} & \text{if } b = 0 \pmod{4} \\ 1 & \text{if } b = 2 \pmod{4} \end{cases}
\]

from which it follows that

\[
f_b(-1) = \begin{cases} 0 & \text{if } b = 0 \pmod{4} \\ \varphi(b) & \text{if } b = 2 \pmod{4} \end{cases}
\]
Other facts:

1. If $b$ is odd, not a square, and not divisible by 3, then $(x^3 + 1) | f_b(x)$.

2. If $b$ is not a square and is 1 (mod 4), then $(x + 1)^2 | f_b(x)$. If $b$ is also not divisible by 3, then $(x^3 + 1)^2 | f_b(x)$.

3. If $b = ck$ is odd, $c$ is not a square, and $(c, k) = 1$, then $f_b(\zeta_{2k}) = 0$. If $b$ is also not divisible by 3, then $f_b(\zeta_{6k}) = 0$. 
Conjecture. For $b = ck$, $\zeta_{2k}$ and $\zeta_{6k}$ are roots of $f_b(x)$ precisely under the following conditions:

(i) If $c = 2 \pmod{4}$, then $\zeta_{2k}$ and $\zeta_{6k}$ are roots of $f_b(x)$ precisely when $k = 4 \pmod{8}$.

(ii) If $c = 0 \pmod{4}$, then $\zeta_{2k}$ and $\zeta_{6k}$ 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 $\zeta_{2k}$ is a root of $f_b(x)$ precisely when $3n \nmid k$ and $c$ is not a square.

(iv) If $(c, 6) = 1$, then $\zeta_{2k}$ and $\zeta_{6k}$ are roots of $f_b(x)$ precisely when $c \nmid k$ and $c$ is not a square.
In trying to understand this conjecture, we discovered that the polynomial takes values of Kloosterman sums:

\[ K_m(x, y) = \sum_{(a,m)=1} e^{\frac{2\pi i}{m}(xa+ya^{-1})} \]

If \( 4k \mid b \), then

\[ f_b \left( e^{\frac{\pi i}{k}} \right) = \frac{1}{2} e^{\frac{\pi i}{2k}} K_{2b} \left( \frac{b}{4k}, \frac{b}{4k} \right) \]

If \( 2k \mid b \) but \( 4k \nmid b \), then

\[ f_b \left( e^{\frac{\pi i}{k}} \right) = \frac{1}{4} i e^{\frac{\pi i}{2k}} K_{4b} \left( \frac{b}{2k}, \frac{b}{2k}(1 - b) \right) \]
The conjecture seems to cover all cases when $\zeta_{2k}$ or $\zeta_{6k}$ is a root for $k \mid b$. There are rarer cases when $k \nmid b$ which are more mysterious.

<table>
<thead>
<tr>
<th>$b$</th>
<th>Unexplained roots</th>
<th>$b$</th>
<th>Unexplained roots</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>$\zeta_{18}$</td>
<td>117</td>
<td>$\zeta_{8}$</td>
</tr>
<tr>
<td>18</td>
<td>$\zeta_{16}$</td>
<td>136</td>
<td>$\zeta_{18}$, $\zeta_{306}$</td>
</tr>
<tr>
<td>22</td>
<td>$\zeta_{20}$, $\zeta_{60}$</td>
<td>138</td>
<td>$\zeta_{108}$</td>
</tr>
<tr>
<td>26</td>
<td>$\zeta_{20}$, $\zeta_{60}$</td>
<td>148</td>
<td>$\zeta_{18}$, $\zeta_{36}$</td>
</tr>
<tr>
<td>29</td>
<td>$\zeta_{18}$</td>
<td>173</td>
<td>$\zeta_{18}$</td>
</tr>
<tr>
<td>40</td>
<td>$\zeta_{18}$, $\zeta_{90}$</td>
<td>186</td>
<td>$\zeta_{20}$</td>
</tr>
<tr>
<td>45</td>
<td>$\zeta_{8}$, $\zeta_{40}$</td>
<td>198</td>
<td>$\zeta_{20}$</td>
</tr>
<tr>
<td>46</td>
<td>$\zeta_{36}$</td>
<td>200</td>
<td>$\zeta_{18}$</td>
</tr>
<tr>
<td>56</td>
<td>$\zeta_{18}$</td>
<td>204</td>
<td>$\zeta_{54}$</td>
</tr>
<tr>
<td>57</td>
<td>$\zeta_{54}$</td>
<td>296</td>
<td>$\zeta_{18}$</td>
</tr>
<tr>
<td>70</td>
<td>$\zeta_{18}$, $\zeta_{90}$</td>
<td>317</td>
<td>$\zeta_{18}$</td>
</tr>
<tr>
<td>74</td>
<td>$\zeta_{36}$</td>
<td>325</td>
<td>$\zeta_{18}$, $\zeta_{90}$</td>
</tr>
<tr>
<td>80</td>
<td>$\zeta_{14}$, $\zeta_{42}$</td>
<td>332</td>
<td>$\zeta_{72}$</td>
</tr>
<tr>
<td>83</td>
<td>$\zeta_{18}$</td>
<td>345</td>
<td>$\zeta_{54}$</td>
</tr>
<tr>
<td>114</td>
<td>$\zeta_{108}$</td>
<td>362</td>
<td>$\zeta_{36}$</td>
</tr>
<tr>
<td>117</td>
<td>$\zeta_{8}$</td>
<td>398</td>
<td>$\zeta_{18}$</td>
</tr>
</tbody>
</table>
If we have the following sequence

\[ r_{-1} = b, \ r_0 = a, \ r_1, \ r_2, \ r_2, \ldots, \ r_n, \ r_{n+1} = 1 \]

where \( r_{j+2} \) is \( r_j \) reduced modulo \( r_{j+1} \) for all \(-1 \leq j \leq n - 1\), then

\[
\text{inv}(a, b) = \frac{a - 1}{4a} b^2 + \left( \frac{(a - 1)(a - 2)}{4a} + \frac{1}{4} \sum_{j=1}^{n} \frac{(-1)^j}{r_j r_{j-1}} (r_j - 1)(r_{j-1} - 1)(r_j + r_{j-1} - 1) \right) b - \frac{(a - 1)^2}{4a}
\]

This means that every \( \text{inv} \) value lies on a parabola in \( b \).
Proposition. If $2 \leq a \leq b - 2$, then

$$\frac{b^2 - 1}{8} \leq \text{inv}(a, b) \leq \frac{3b^2 - 12b + 9}{8}.$$

Proof. The proof is by induction on $b$. There are three cases:

1. If $b \neq \pm 1 \pmod{a}$, then use the induction hypothesis:

$$\text{inv}(a, b) \geq -\frac{1}{8}(b + 2)a + \frac{1}{4}(b^2 + 3b + 2) - \frac{1}{8}(2b^2 + 5b + 2)\frac{1}{a}.$$

2. If $b = 1 \pmod{a}$, then by reciprocity,

$$\text{inv}(a, b) = \frac{1}{4}(b - 1)a + \frac{1}{4}(b^2 - 3b + 2) - \frac{1}{4}(b^2 - 2b + 1)\frac{1}{a}.$$

3. If $b = -1 \pmod{a}$, then again by reciprocity,

$$\text{inv}(a, b) = -\frac{1}{4}(b + 1)a + \frac{1}{4}(b^2 + 3b + 2) - \frac{1}{4}(b^2 + 2b + 1)\frac{1}{a}.$$
More generally, it appears that \( \text{inv}(k, b) \) is the \( k \)th smallest value of \( \text{inv}(a, b) \) for \( 1 \leq k \leq 6 \).

More specifically, the \( k \)th smallest value occurs with the remainder sequence

\[
b, \ k, \ k - 1, \ 1
\]

The longer the remainder sequence \( b, a, ..., 1 \), the closer \( \text{inv}(a, b) \) is to \( \frac{(b-1)(b-2)}{4} \).
Values of $\text{inv}(a,b)$ vs. Length of remainder sequence for $b=100000$
Questions?