<table>
<thead>
<tr>
<th>Title</th>
<th>ON DEDEKIND SUMS II REMARKS ON HIGHER DIMENSIONAL DEDEKIND SUMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>HIROOKA, EIKO</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1985-11</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/99187">http://hdl.handle.net/2433/99187</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
ON DEDEKIND SUMS II

REMARKS ON HIGHER DIMENSIONAL DEDEKIND SUMS

EIKO HIROOKA

Department of Mathematics,
Kobe University

§1. Classical Dedekind sums

Dedekind uses the symbol $s(a,c)$ for classical Dedekind sums. He originally introduced these sums in connection with the transformation properties, under the modular group, of his $\eta$-function

$$\eta(z) = e^{\pi iz/12} \prod_{n=1}^{\infty} (1-e^{2\pi inz}) \quad (\text{Im} z > 0),$$

namely, for $c > 0$,

$$\log \eta \left( \frac{az+b}{cz+d} \right) = \log \eta(z) + \frac{1}{2} \log \frac{cz+d}{1} + \pi i \left( \frac{a+d}{12c} - s(d,c) \right),$$

where the principal branch is taken for the logarithm.

Let $a, c$ be integers such that $(a,c)=1, c \geq 1$. Then $s(a,c)$ was evaluated by Dedekind and he proved the relation

$$s(a,c) = \frac{1}{c} \sum_{k=1}^{c-1} \left( \frac{k}{c} \right) \left( \frac{ak}{c} \right).$$

Here the symbol $(x)$ is defined by

$$(x) = \begin{cases} x - [x] - 1/2 & \text{if } x \not\in \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}, \end{cases}$$

where $[x]$ denotes the greatest integer function. And these sums are represented by cotangents,
namely
\[ s(a,c) = \frac{1}{4c} \sum_{k=1}^{c-1} \cot \frac{\pi k}{c} \cot \frac{\pi k a}{c}. \]

We focus our attention now on its properties and its connection with other mathematical topics ([5]).

Proposition 1. (Reciprocity Law)
Let \( a, c \) be positive integers, \((a,c)=1\). Then,
\[ s(a,c) + s(c,a) = \frac{1}{4ac}(a^2+c^2+1-3ac). \]

The number of lattice points in a tetrahedron has been related to Dedekind sums by L.J. Mordell ([4]). He proved the following result:

Proposition 2. (Lattice Points)
Let \( a, b, c \) be pairwise coprime, positive integers and let \( N_3(a,b,c) \) be the number of lattice points in the tetrahedron
\[ 0 \leq x < a, 0 \leq y < b, 0 \leq z < c, 0 \leq \frac{x}{a} + \frac{y}{b} + \frac{z}{c} < 1; \]
than
\[ N_3(a,b,c) = -[s(bc,a) + s(ca,b) + s(ab,c)] + \frac{1}{6} abc + \frac{1}{4} (bc+ca+ab) \]
\[ + \frac{1}{4} (a+b+c) + \frac{1}{12} \left( \frac{bc}{a} + \frac{ca}{b} + \frac{ab}{c} \right) + \frac{1}{12abc} - 2. \]

Since the Dedekind sums are rational, we can evaluate its denominators:

Proposition 3. (Evaluation of the Denominators)
\[ 2c(3,c) s(a,c) \] is an integer.

The range of values of \( s(a,c) \) is not fully known. Saie ([5]) proved that \( s(a,c) \) always satisfies one of the following five congruences:
\[ 6cs(a,c) \equiv 0, \pm 1, \pm 3 \pmod{9} \]. So the problem of the
"Missing Values" ([1]) has arisen.

Dedekind sums are connected with the Jacobi symbol:

**Proposition 4.** (Connection with the Jacobi Symbol)

If \( c \) is odd, then

\[
6cs(a,c) \equiv \frac{a+1}{2} - \left( \frac{a}{c} \right) \pmod{4}.
\]

This means that the Dedekind sums become the Jacobi symbol if we have them modulo 4. Hence we can consider that the Dedekind sums explain the Jacobi symbol in detail. We have some other properties, for example, the range of \( s(a,c) \) is dense on the real axis and connected with class numbers of quadratic fields etc. Now we explain about the classical Dedekind sums no more and we come to the higher dimensional Dedekind sums that are one of the extented Dedekind sums.

§2. Higher Dimensional Dedekind Sums

2.1 Let \( p \) be a positive integer and let \( a_1, \ldots, a_n \) be integers prime to \( p \), and \( n \) is even. Then we define

\[
d(p:a_1, \ldots, a_n) = (-1)^{n/2} \prod_{k=1}^{p-1} \cot \frac{ka_1}{p} \ldots \cot \frac{ka_n}{p}.
\]

Remark.

If \( n \) is odd, the sum is clearly equal to zero.

Zagier called these sums the higher dimensional Dedekind sums for the first time. Why he was interested in sums of this type? There are two reasons. Firstly the case \( n=2 \) is, up to a factor, the classical Dedekind sums:

\[
d(p:a_1, a_2) = -4ps(a_1a_2^{-1}, p),
\]

3
where $a_2^{-1}$ is an inverse of $a_2 \pmod{p}$. And as I mentioned at §1, the Dedekind sums are connection with other mathematical topics. So the same things may hold about higher dimensional analogues. The second ground for studying this sum is that it arises in topological situations. The first appearance of trigonometric functions in this context was the index theorem of Hirzebruch, which evaluates the signature (a certain invariant of the homology of a differentiable manifold) by means of a formula involving cotangents([3]). In that case, if the dimension of the manifold is four, classical Dedekind sums appear and generally if the dimension of the manifold is $2n$, $d(p:a_1,\ldots,a_n)$ appears. After that we shall pay more attention to the number theoretical part of higher dimensional case.

2.2 Some Properties of the Higher Dimensional Dedekind Sums

**Proposition 5. (Rational Number ([7]))**

\[
d(p:a_1,\ldots,a_n) \text{ is rational:}
\]

\[
d(p:a_1,\ldots,a_n) = 2^n p \sum_{0 < k_i < p \mid k_1 a_1 + \ldots + k_n a_n} (k_1/p) \ldots (k_n/p).
\]

**Proposition 6. (Reciprocity Law ([7]))**

Let $a_0,\ldots,a_n$ be pairwise coprime positive integers.

Then

\[
\sum_{j=0}^{n} \frac{1}{a_j} d(a_j:a_0,\ldots,\hat{a}_j,\ldots,a_n) = 1 - \frac{1}{a_0,\ldots,a_n/a_0,\ldots,a_n}.
\]
where $l_n(a_0,\ldots,a_n)$ is a polynomial defined by the next formula:

$$
\sum_{n=0}^{\infty} l_n(a_0,\ldots,a_n) t^n = \prod_{j=0}^{n} a_j t/\tanh a_j t = \prod_{j=0}^{n} \left( 1 + a_j^2 t^2/3 - a_j^4 t^4/45 + 2a_j^6 t^6/945 - \ldots \right)
$$

Remark.

$l_n(a_0,\ldots,a_n)$ is nearly equal to the Hizebruch L-polynomial.

In Proposition 5, $d(p:a_1,\ldots,a_n)$ is rational; so we can evaluate the denominator:

**Proposition 7.** (Evaluation of the Denominators ([7]))

Let

$$
c(n,p) = \prod_{m : \text{odd prime}} \frac{n}{(m-1)}, \text{ then } m \equiv p^n \mod m
$$

$c(n,p)d(p:a_1,\ldots,a_n)$ is an integer.

And for $n=2,4$ the denominator of $d(p:a_1,\ldots,a_n)$ equals to $c(n,p)$.

We want to add much more about the evaluation of the denominators, but before that let's consider the generalization of the lattice points in the Proposition 2:

**Proposition 8.** (Generalization of the Lattice Points ([8]))

Let $a_1,\ldots,a_n$ (n:odd) be positive integers and $N$ a common multiple of the $a_i$'s. Let

$$
t(a_1,\ldots,a_n) = \text{Cord}(x_1,\ldots,x_n) \mid 0 < x_1 \leq a_1, 0 < \sum_{i=1}^{n} x_i/a_i < 1 \mod 2 \}
$$

$$
- \text{Cord}(x_1,\ldots,x_n) \mid 0 < x_1 < a_1, 1 \leq \sum_{i=1}^{n} x_i/a_i < 2 \mod 2 \}
$$

Then

$$
t(a_1,\ldots,a_n) = \frac{(-1)^{(n-1)/2}}{N} 2^{N-1} \prod_{k=1,k \text{ odd}}^{N} \cot \frac{\pi k}{2N} \cot \frac{\pi k}{2a_1} \cdots \cot \frac{\pi k}{2a_n}
$$
This is a kind of the higher dimensional Dedekind sums, too. And the formula by which we define \( t(a_1, \ldots, a_n) \) is the value found by Brieskorn ([2]) for the signature of the \((2n-3)\)-dimensional manifold defined by

\[
V = \{ (z_1, \ldots, z_n) \in \mathbb{C}^n | z_1^{a_1} + \ldots + z_n^{a_n} = 0, |z_1|^2 + \ldots + |z_n|^2 = 1 \}.
\]

2.3 From now on we shall give some new results for the higher dimensional Dedekind sums.

The first is a result about the evaluation of the denominators. In §1 we saw the congruence which \( s(a, c) \) satisfies. And for \( n=4 \) we have the next congruences:

**Theorem 1.**

Let

\[
d(p, 4) = d(p; a_1, a_2, a_3, a_4).
\]

Then

1) \( d(p, 4) \equiv 0 \pmod{2} \) if \( 3, 5 \mid p \),
2) \( 9d(p, 4) \equiv \pm 2 \pmod{18} \) if \( 3 \mid p, 5 \nmid p \),
3) \( 5d(p, 4) \equiv 0 \pmod{2}, \neq 0 \) if \( 5 \mid p, 3 \nmid p \),
4) \( 45d(p, 4) \equiv \pm 10 \pmod{18} \) if \( 15 \mid p \).

From this the problem of the "Missing Values" arises. But we can't find the algorithm of the \( d(p; a_1, a_2, a_3, a_4) \) yet.

To prove this theorem we need some lemmas.

**Lemma 1.**

For the \( a_1 \)'s we can choose \( a_1 \)'s as

\[
d(p; a_1, a_2, a_3, a_4) = d(p; a_1', a_2', a_3', 1) \quad (p, a_1', a_2', a_3' \text{ are pairwise coprime}).
\]
Proof. Since \((p, a_4) = 1\), \(a_4'\) exists such that \(a_4 a_4' \equiv 1 \pmod{p}\). Hence by the definition \(d(p; a_1, a_2, a_3, a_4) = d(p; a_1 a_4', a_2, a_3, a_4')\). And by Dirichlet's theorem on primes in arithmetic progressions, \(a_1 a_4'\) can be replaced by prime number \(a_1'\) congruent to \(a_1 a_4'\) modulo \(p\). Since the value of \(d(p; a_1, \ldots, a_n)\) only depends on the values of the \(a_1 \pmod{p}\), \(d(p; a_1, a_2, a_3, a_4') = d(p; a_1', a_2, a_3, a_4')\). But they can be chosen as arbitrarily large primes, so in particular they can be made prime to one another and then to \(p\). Therefore we have the result.

**Lemma 2.**

\[ 45d(p; a_1, a_2, a_3, a_4) \equiv 0 \pmod{2} \]

**Proof.** It suffices to prove this lemma for \(d(p; a_1, a_2, a_3, 1)\) \((p, a_1, a_2, a_3\) are pairwise coprime.) by lemma 1. We first assume that \(p\) is odd. By proposition 5,

\[
d(p; a_1, a_2, a_3, 1) = 2^4 p \sum_{0 \leq k_i < p, \text{ } p \mid a_1 k_1 + a_2 k_2 + a_3 k_3 + k_4} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \left( \frac{k_4}{p} \right) \cdot (N: \text{integer})
\]

We fix one of the \((k_1, k_2, k_3)\) \((0 \leq k_i < p)\). For this \((k_1, k_2, k_3)\) only one \(k_4 (0 \leq k_4 < p)\) exists such that \(p \mid a_1 k_1 + a_2 k_2 + a_3 k_3 + k_4\). Therefore

\[
d(p; a_1, a_2, a_3, 1) = 2^4 p \sum_{0 \leq k_i < p, \text{ } p \mid a_1 k_1 + a_2 k_2 + a_3 k_3} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \left( \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \right) \cdot (N: \text{integer})
\]

\[
= -2^4 p \sum_{0 \leq k_1 < p} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \left( \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \right) \cdot (N: \text{integer})
\]
\[= -2^4 \sum_{0 \leq k_1 < p} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} - \frac{1}{2} \sum_{0 \leq k_1 < p} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} - \frac{1}{2} \sum_{0 \leq k_1 < p} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \]

Here we pay attention to
\[\Sigma \left( \frac{k_1}{p} \right) = 0: \]
\[0 \leq k_1 < p \]

for example
\[\Sigma \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) k_1 = \Sigma k_1 \left( \frac{k_1}{p} \right) \Sigma \left( \frac{k_2}{p} \right) \Sigma \left( \frac{k_3}{p} \right) \]
\[= 0. \]

Therefore
\[d(p; a_1, a_2, a_3, l) = 2^4 \sum_{0 \leq k_1 < p} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \]
\[= 2^4 \sum_{0 \leq k_1 < p} \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \]
\[= 16p \left[ \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \right] \left( \frac{k_1}{p} \right) \left( \frac{k_2}{p} \right) \left( \frac{k_3}{p} \right) \]
\[= 16p \left[ \frac{a_1 k_1 + a_2 k_2 + a_3 k_3}{p} \right] \left( \frac{k_1 k_2}{p} \right) \left( \frac{k_3}{p} \right) \]
\[= \frac{1}{4p} \left( k_1 + k_2 + k_3 \right) \left( \frac{1}{8} \right) . \]

45d(p; a_1, a_2, a_3, l) is an integer and since p is odd,
\[45d(p; a_1, a_2, a_3, l) \equiv 45p^2 d(p; a_1, a_2, a_3, l) \equiv 0 \pmod{2}. \]
If $p$ is even, we use the reciprocity law and we find
\[
45a_1a_2a_3d(p;1,a_1,a_2,a_3) + 45pa_3d(a_1:p,1,a_2,a_3)
+ 45pa_1a_3d(a_2;p,1,a_1,a_3) + 45pa_2a_3d(a_3;p,1,a_1,a_2)
= 45pa_1a_2a_3 + p^4 + 1 + a_1^4 + a_2^4 + a_3^4 - 5(p^2 + p^2a_1^2 + \ldots + a_2^2a_3^2)
\]
modulo 2. Since $a_1$'s are odd,
\[
45d(p;1,a_1,a_2,a_3) \equiv 4-5\cdot 6 \equiv 0 \pmod{2}.
\]

Proof of Theorem 1.

1) Let's recall that
\[
\prod_{m \text{ odd prime}} \mathbb{Z}^{[4/(m-1)]}d(p; a_1, a_2, a_3, a_4) \in \mathbb{Z}.
\]

Now $3, 5 \not| p$ and $m | p$, so $m \geq 7$. Hence $[4/(m-1)] = 0$ and
\[
\prod_{m \text{ odd prime}} \mathbb{Z}^{[4/(m-1)]} = 1.
\]

Therefore $d(p; a_1, a_2, a_3, a_4)$ is an integer. We combine this fact with lemma 2, and we have the result.

About 2), 3), 4) it suffices to prove for $d(p; a_1, a_2, a_3, 1)$ ($p, a_1, a_2, a_3$ are pairwise coprime.). Therefore we use the reciprocity law:

(*) \[
45a_1a_2a_3d(p;1,a_1,a_2,a_3) + 45pa_2a_3d(a_1;p,1,a_2,a_3)
+ 45pa_1a_3d(a_2;p,1,a_1,a_3) + 45pa_2a_3d(a_3;p,1,a_1,a_2)
= 45pa_1a_2a_3 + p^4 + 1 + a_1^4 + a_2^4 + a_3^4 - 5(p^2 + p^2a_1^2 + \ldots + a_2^2a_3^2).
\]

2) We first assume that $5 | a_i$ for all $a_i$'s. Since $3 | a_i$ for all
$a_i$'s, $d(a_1:p,1,...) \in \mathbb{Z}$. Hence we consider (*) modulo 45 and we have

$$45a_1a_2a_3d(p:1,a_1,a_2,a_3) \equiv p^4 + 1 + a_1^4 + a_2^4 + a_3^4 - 5(a_1^2 + a_2^2 + a_3^2 + a_1a_2^2 + a_1a_3^2 + a_2a_3^2)$$

$$= 5(a_1 + a_2a_3)^2 + 5(a_2 + a_3a_1)^2 - 5(a_3 + a_1a_2)^2 + p^4 + 1 + a_1^4 + a_2^4 + a_3^4$$

$$\equiv 10a_1a_2a_3 - 10(a_1^2 + a_2^2 + a_3^2 + a_1a_2a_3) \pmod{45}.$$  

Since either $a_1 + a_1a_2a_3 (i \mod{3})$ is a multiple of 3 at the same time,

$$5(a_1 + a_1a_2a_3)^2 \equiv 0 \pmod{45}.$$

Therefore

$$45a_1a_2a_3d(p:1,a_1,a_2,a_3)$$

$$\equiv p^4 + 1 + a_1^4 + a_2^4 + a_3^4 - 10(a_1^2 + a_2^2 + a_3^2 + a_1a_2a_3) \equiv 10a_1a_2a_3$$

$$\equiv p^4 + 1 + a_1^4 + a_2^4 + a_3^4 + 5(a_1^2 - 1)^2 + 5(a_2^2 - 1)^2 + 5(a_3^2 - 1)^2$$

$$+ 10(a_1a_2a_3 - 10(1 + a_1^4 + a_2^4 + a_3^4) \equiv 10a_1a_2a_3 \pmod{45}.$$  

The last congruence is ground in the fact that either $a_1 \equiv 1$ is a multiple of 3. Put

$$X = p^4 - 9(1 + a_1^4 + a_2^4 + a_3^4);$$

then by $3 | p$ we find $9 | X$. Since $p \not| 5$ and $a_1 \not| 5$, $p^4, a_1^4 \equiv 1 \pmod{5}$. Hence $X \equiv 0 \pmod{5}$ and $x \equiv 0 \pmod{45}$. Therefore

$$45a_1a_2a_3d(p:1,a_1,a_2,a_3) \equiv 10a_1a_2a_3 \pmod{45}.$$
By \((a_1 a_2 a_3, 45) = 1\) we have
\[
45d(p; l, a_1, a_2, a_3) \equiv \mp 10 \pmod{45}.
\]
We combine this with lemma 2 and we have
\[
9d(p; l, a_1, a_2, a_3) \equiv \pm 2 \pmod{18}.
\]
If \(5 | a_1\), we may assume \(5 | a_1\). And we consider (*) modulo 45 so
\[
45a_1 a_2 a_3 d(p; l, a_1, a_2, a_3) + 45pa_2 a_3 d(a_1; p, l, a_2, a_3)
\]
\[
\equiv p^4 + 1 + a_1^4 + a_2^4 + a_3^4 - 5(a_1^2 + a_2^2 + \ldots + a_2^2 a_3^2) \pmod{45}.
\]
We multiply 5 in the both sides and we notice that
\[
225pa_2 a_3 d(a_1; p, l, a_2, a_3) \equiv 0 \pmod{45}.
\]
Then
\[
225a_1 a_2 a_3 d(p; l, a_1, a_2, a_3)
\]
\[
\equiv 5(p^4 + 1 + a_1^4 + a_2^4 + a_3^4) - 25(a_1^2 + \ldots + a_2^2 a_3^2) \pmod{45}.
\]
By using the same way we have
\[
225a_1 a_2 a_3 d(p; l, a_1, a_2, a_3)
\]
\[
\equiv 25(a_1 + a_2 a_3)^2 + 25(a_2 + a_1 a_3)^2 - 25(a_3 + a_1 a_2)^2 + 5(1 + a_1^4 + a_2^4 + a_3^4)
\]
\[
\mp 50a_1 a_2 a_3 - 50(a_1^2 + a_2^2 + a_2 a_3^2 + a_2^2 a_3^2)
\]
\[
\equiv 5(1 + a_1^4 + a_2^4 + a_3^4) \mp 50a_1 a_2 a_3 + 25(a_1^2 - 1)^2 + 25(a_2^2 - 1)^2
\]
\[
+ 25(a_2^2 - a_3^2)^2 + 25(a_1^2 - a_3^2)^2 - 50(1 + a_1^4 + a_2^4 + a_3^4)
\]
\[
\equiv - 45(1 + a_1^4 + a_2^4 + a_3^4) \mp 50a_1 a_2 a_3
\]
\[
\equiv \mp 50a_1 a_2 a_3 \pmod{45}.
\]
And by \((a_2 a_3, 45) = 1\)
\[
225a_1 d(p; l, a_1, a_2, a_3) \equiv \mp 50a_1 \pmod{45}.
\]
Hence
\[45a_1d(p:1, a_1, a_2, a_3) \equiv 10a_1 \pmod{9}\]
and by \((5a_1, 9)=1\), we have
\[9d(p:1, a_1, a_2, a_3) \equiv 2 \pmod{9}.
By lemma 2 we have also
\[9d(p:1, a_1, a_2, a_3) \equiv 2 \pmod{18}.
3) Since \(3 \nmid p\) and \(5 \nmid p\), \(5d(p:1, a_1, a_2, a_3)\) is an integer. By using the lemma 2 we have
\[5d(p:1, a_1, a_2, a_3) \equiv 0 \pmod{2}.
4) Since \(3, 5 \nmid a_1\)'s, \(d(a_i:p,1,\ldots) \in \mathbb{Z}\).
Hence
\[45a_1a_2a_3d(p:1, a_1, a_2, a_3) \equiv 1 + a_1^4 + a_2^4 + a_3^4 - 5(a_1^2 + \ldots + a_2^2a_3^2) \pmod{9}.
By using the same way of 1), we have
\[45a_1a_2a_3d(p:1, a_1, a_2, a_3) \equiv -9(1 + a_1^4 + a_2^2 + a_3^4) + 10a_1a_2a_3 \equiv 3a_1a_2a_3 \pmod{9}.
And by \((a_1a_2a_3, 9)=1\)
\[45d(p:1, a_1, a_2, a_3) \equiv 1 \pmod{9}.
By lemma 2 we have
\[45d(p:1, a_1, a_2, a_3) \equiv 10 \pmod{18}.
Q.E.D.

Higher dimensional Dedekind sums are connected with n's Jacobi symbols:
Theorem 2.

Put
\[ \mu_{n/2} = \prod_{m: \text{odd prime}} m^{[n/(m-1)]}. \]

If \( p \) is odd, then
\[ \mu_{n/2} d(p:a_1, \ldots, a_n) \equiv \mu_{n/2} (p-1) - 2n + 2\left\{ \frac{a_1}{p} + \ldots + \frac{a_n}{p} \right\} \pmod{8}. \]

**Proof.** We first show the theorem for the type \( d(p:b_1, \ldots, b_{n-1}, 1) \).

By the definition,
\[ d(p:b_1, \ldots, b_{n-1}, 1) = 2^n \sum_{k_i \leq p} \frac{k_1}{p} \ldots \frac{k_{n-1}}{p}. \]

And we use the same way in the proof of lemma 2, then
\[ d(p:b_1, \ldots, b_{n-1}, 1) = 2^n \sum_{0 \leq k_i < p} [\frac{b_1 k_1 + \ldots + b_{n-1} k_{n-1}}{p}] \frac{k_1}{p} \ldots \frac{k_{n-1}}{p}. \]

where \( A \) is an integer and
\[ \mu_{n/2} A \equiv 0 \pmod{8}. \]

Therefore
\[ \mu_{n/2} d(p:b_1, \ldots, b_{n-1}, 1) \equiv 4 \sum_{k_1=1}^{p-1} \frac{b_1 k_1 + \ldots + b_{n-1} k_{n-1}}{p} \pmod{8}. \]

First we calculate \( \sum k_1 \frac{b_1 k_1 + \ldots + b_{n-1} k_{n-1}}{p} \) modulo 2.
\[
\sum_{k_{n-1}=1}^{p-1} b_{\frac{k_{n-1}+...+b_{n-1}k_{n-1}}{p}} = \sum_{k_{n-1}=0}^{p-1} b_{\frac{k_{n-1}+...+b_{n-1}k_{n-1}}{p}} - \sum_{k_{n-1}=0}^{p-1} \frac{b_{\frac{k_{n-1}+...+b_{n-1}k_{n-1}}{p}}}{p} - \frac{b_{\frac{k_{n-2}k_{n-2}}{p}}}{p},
\]

where \{ \} denotes the fractional part and

\[
\sum_{k_{n-1}=0}^{p-1} b_{\frac{k_{n-1}+...+b_{n-1}k_{n-1}}{p}} = \frac{p-1}{2}.
\]

Hence

\[
\sum_{k_{n-1}=1}^{p-1} b_{\frac{k_{n-1}+...+b_{n-1}k_{n-1}}{p}} = \sum_{k_{n-1}=1}^{p-1} b_{\frac{k_{n-1}+...+b_{n-1}k_{n-1}}{p}} - \frac{(p-1)(b_{n-1} - 1)}{2}.
\]

And by noticing that \( p \) is odd,

\[
\sum_{k_{n-2}=1}^{p-1} b_{\frac{k_{n-2}+...+b_{n-2}k_{n-2}}{p}} = \sum_{k_{n-2}=1}^{p-1} b_{\frac{k_{n-2}+...+b_{n-2}k_{n-2}}{p}} - \frac{b_{n-2}p(p-1)}{2} - \frac{(p-1)(b_{n-2} - 1)}{2} + \frac{b_{\frac{k_{n-1}+...+b_{n-3}k_{n-3}}{p}}}{p} \pmod{2}
\]

\[
\sum_{k_{n-3}=1}^{b_{n-3}p(p-1)} b_{\frac{k_{n-3}+...+b_{n-3}k_{n-3}}{p}} = \sum_{k_{n-3}=1}^{b_{n-3}p(p-1)} b_{\frac{k_{n-3}+...+b_{n-3}k_{n-3}}{p}} - \frac{n-1}{2} + \sum_{k_{n-3}=1}^{b_{n-3}p(p-1)} b_{\frac{k_{n-3}+...+b_{n-3}k_{n-3}}{p}} \pmod{2}.
\]

We repeat this operation and we notice that \( n \) is even. So
\[ \sum_{k_1, \ldots, k_{n-1}} \frac{b_1 k_1 + \ldots + b_{n-1} k_{n-1}}{p} \equiv \]
\[ \frac{b_2 p(p-1) - b_1 k_1}{2} - \frac{(p-1)(b_2-1)}{2} + \left[ \frac{b_1 k_1}{p} \right] \]
\[ \equiv - b_1 k_1 + \frac{p-1}{2} + \left[ \frac{-b_1}{2} \right] \pmod{2}. \]
\[ \sum_{k_1, \ldots, k_{n-1}} \frac{b_1 k_1 + \ldots + b_{n-1} k_{n-1}}{p} \equiv \]
\[ - \frac{b_1 p(p-1)(2p-1)}{6} + \frac{p(p-1)^2}{4} + \sum_{k_1} \frac{b_1 k_1}{p} \pmod{2}. \]

Here
\[ \sum_{k_1=1}^{n-1} \frac{b_1 k_1}{p} \equiv \sum_{k_1=1}^{n-1} \frac{b_1 k_1}{p} \equiv \left( \frac{p-1}{2} \right) \left( \frac{b_1}{p} - 1 \right) \pmod{2}, \]
hence
\[ 2b_1 p(p-1)(2p-1) \equiv 2b_1 p(p-1)(2p-1) + p(p-1)^2 + 4(p-1)(b_1 - 1) + 4\left( \frac{b_1}{p} - 1 \right) \pmod{8}. \]

Since in the first term \( p \) or \( p-1 \) or \( 2p-1 \equiv 0 \pmod{3} \) and \( (3,4)=1, \)
\[ \frac{p(p-1)(2p-1)}{3} \equiv n-1 \pmod{4}. \]

Thus
\[ 4 \sum_{k_1} \frac{b_1 k_1 + \ldots + b_{n-1} k_{n-1}}{p} \equiv \]
\[ -2b_1 (p-1) + 2(p-1) + 2(b_1 - 1)(p-1) + 2\left( \frac{b_1}{p} - 1 \right) \]
\[ \equiv 2(p-1)(-b_1 + b_1 - 1) + 2\left( \frac{b_1}{p} - 1 \right) \]
\[ \equiv 2\left( \frac{b_1}{p} - 1 \right) \pmod{8}. \]
Therefore
\[ \Sigma (k_1 + \cdots + k_{n-1}) \frac{b_1 k_1 \cdots + b_{n-1} k_{n-1}}{p} \]
\[ \equiv 2 \left( \frac{b_1}{p} \right) + \cdots + \left( \frac{b_{n-1}}{p} \right) - (n-1) \pmod{8}. \]

Next we calculate \[ \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-1} k_{n-1}}{p} \right) \pmod{4}. \]

\[ \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-1} k_{n-1}}{p} \right) = b_1 k_1 + \cdots + b_{n-2} k_{n-2} + \frac{(p-1)(b_{n-1}-1)}{2} \]

\[ - \left( \frac{b_1 k_1 + \cdots + b_{n-2} k_{n-2}}{p} \right) \]

\[ \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-1} k_{n-1}}{p} \right) = (p-1)(b_1 k_1 + \cdots + b_{n-3} k_{n-3}) \]

\[ + \frac{b_{n-2} p (p-1)}{2} - \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-2} k_{n-2}}{p} \right). \]

\[ \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-1} k_{n-1}}{p} \right) \equiv \frac{b_1 k_1 + \cdots + b_{n-3} k_{n-3}}{2} + \frac{b_{n-2} p (p-1)^2}{2} - \frac{b_{n-3} p (p-1)^2}{2} \]

\[ + \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-3} k_{n-3}}{p} \right) \pmod{4}. \]

We repeat this operation and we obtain

\[ \Sigma \left( \frac{b_1 k_1 + \cdots + b_{n-1} k_{n-1}}{p} \right) \equiv \frac{b_1 p (p-1)^2}{2} + \frac{b_{2} p (p-1)^2}{2} - \frac{(p-1)^2 (b_2 - 1)}{2} \]

\[ - \frac{b_1 p (p-1)}{2} - \Sigma \left( \frac{b_1 k_1}{p} \right) \]

\[ \equiv \frac{b_1 p (p-1)(p-2)}{2} - \frac{(p-1)^2 (b_2 (p-1) + 1)}{2} + \Sigma \left( \frac{b_1 k_1}{p} \right) \]

\[ \equiv \frac{(p-1)^2}{2} + \frac{b_1 p (p-1)(p-2)}{2} + \frac{(p-1)(b_1 - 1)}{2} \pmod{4}. \]
\[2p^\mu_{n/2} \left[ \frac{b_1^k \cdots + b_{n-1}^{k-1}}{p} \right] \equiv p^{\mu_{n/2}} ((p-1)^2 + b_1 p (p-1)(p-2) + (p-1)(b_1 - 1)\right) \\
\equiv p^{\mu_{n/2}} [2(1-p) + 3b_1 (p-1) + (p-1)(b_1 - 1)] \\
\equiv p^{\mu_{n/2}} (p-1) (-2 + 3b_1 + b_1 - 1) \\
\equiv p^{\mu_{n/2}} (p-1) (4b_1 - 3) \\
\equiv -3p^{\mu_{n/2}} p (p-1) \\
\equiv 3p^{\mu_{n/2}} (p-1) \pmod{8}.
\]

Therefore
\[u^{\mu_{n/2}} d(p;b_1, \ldots, b_{n-1}, 1) \equiv 2\left(\frac{b_1}{p} + \cdots + \frac{b_{n-1}}{p} - (n-1)\right) + 5u^{\mu_{n/2}} (p-1) \\
\equiv u^{\mu_{n/2}} (p-1) + 2\left(\frac{b_1}{p} + \cdots + \frac{b_{n-1}}{p} - (n-1)\right) \pmod{8}.
\]

By the way
\[d(p;a_1, a_2, \ldots, a_n) = d(p;a_1 x, \ldots, a_{n-1} x, 1) \quad (a_n x \equiv 1 \pmod{p}).
\]

Hence
\[u^{\mu_{n/2}} d(p;a_1, \ldots, a_n) = u^{\mu_{n/2}} d(p;a_1 x, \ldots, a_{n-1} x, 1) \\
\equiv u^{\mu_{n/2}} (p-1) + 2\left(\frac{a_1 x}{p} + \cdots + \frac{a_{n-1} x}{p} - (n-1)\right) \\
\equiv u^{\mu_{n/2}} (p-1) + 2\left(\frac{x}{p}\right)\left(\frac{a_1}{p} + \cdots + \frac{a_{n-1}}{p}\right) - 2(n-1) \pmod{8}.
\]

And since \(a_n x \equiv 1 \pmod{p}\), \(\frac{x}{p} = \frac{a_n}{p}\).

By using this fact we obtain that
\[u^{\mu_{n/2}} d(p;a_1, \ldots, a_n) \equiv u^{\mu_{n/2}} (p-1) + 2\left(\frac{a_n}{p}\right)\left(\frac{a_1}{p} + \cdots + \frac{a_{n-1}}{p}\right) - 2(n-1) \\
\equiv u^{\mu_{n/2}} (p-1) + 2\left(\frac{-n}{p}\right)\left(\frac{a_1}{p} + \cdots + \frac{a_{n-1}}{p}\right) - 2n \pmod{8}.
\]
We have the last congruence by noticing that
\[
\left(\frac{a_1}{p}\right)^* + \ldots + \left(\frac{a_n}{p}\right)^*
\]
is always even. 

Q.E.D.

We use this theorem in the reciprocity law and we obtain the next corollarys:

**Corollary 1.**

Let \(a_0, \ldots, a_n\) be odd and pairwise coprime. Then

\[
2 \sum_{i < j} \left\{ a_i \left(\frac{a_j}{a_i}\right) + a_j \left(\frac{a_i}{a_j}\right) \right\} = -n^{\mu_n/2} + (\mu_{n/2} + 2n)(a_0^* + \ldots + a_n^*) - \mu_{n/2}a_0 \ldots a_n \pmod{8}.
\]

This formula is very beautiful but I don't know what it means. To prove this we need the next lemma:

**Lemma 3.**

\(J_n\) is defined as the coefficient of \(t^n\) in the power series expansion of \(\frac{t}{\tanh t}\)\(^{n+1}\), where \(n\) is even. Then \(J_n = 1\). This lemma has been shown ([3]).

**Proof of the Corollary 1.**

Since \(a_i^*\)'s are odd, \(a_i^2 \equiv 1 \pmod{8}\). Hence

\[
\mu_{n/2} a_0^* \ldots a_n^* \equiv \mu_{n/2} J_n \equiv \mu_{n/2} \pmod{8}.
\]

We multiply \(a_0^2 \ldots a_n^2 \equiv 1 \pmod{8}\) in the both sides of the reciprocity law:

\[
18
\]
\[ \sum_{j=0}^{n} a_j d(a_j: a_0, \ldots, \hat{a}_j, \ldots, a_n) \equiv 1 - a_0 \cdots a_{n-1} (a_0, \ldots, a_n) \pmod{8}. \]

\[ u^{n/2} \sum_{j=0}^{n} a_j d(a_j: a_0, \ldots, \hat{a}_j, \ldots, a_n) \equiv u^{n/2} - a_0 \cdots a_{n-1} u^{n/2} (a_0, \ldots, a_n) \]

\[ (*2) \equiv u^{n/2} - u^{n/2} a_0 \cdots a_n \pmod{8}. \]

Here we use the theorem 2:

the left side \[ \equiv \sum_{j=0}^{n} [a_j u^{n/2} (a_j - 1) - 2a_j n + 2a_j \left( a_j - (\frac{a_j}{a_j}) \right) + \cdots + (\frac{n}{a_j})] \]

\[ (n+1) u^{n/2} - (\mu n/2 + 2n)(a_0^+ \cdots + a_n^+) + 2 \sum_{i<j} a_i (a_j^+ - a_j) (\frac{a_j}{a_i}) \pmod{8}. \]

We substitute this for \((**2)\) and then

\[ 2 \sum_{i<j} a_i (a_j^+ - a_j) (\frac{a_j}{a_i}) \equiv -n u^{n/2} + (\mu n/2 + 2n)(a_0^+ \cdots + a_n) \]

\[ - u^{n/2} a_0 \cdots a_n \pmod{8}. \]

Q.E.D.

Corollary 2.

Let \(a, b\) be odd and \((a, b) = 1\). Then

\[ a \left( \frac{b}{a} \right) + b \left( \frac{a}{b} \right) \equiv \frac{3}{2}(a+1)(b+1) \pmod{4}. \]

This is the quadratic reciprocity law. First we assume that \(a, b \equiv -1 \pmod{4}\). Then the right side of the corollary is zero modulo 4,

namely

\[ a \left( \frac{b}{a} \right) + b \left( \frac{a}{b} \right) \equiv 0 \pmod{4}. \]

\[ (b/a) + (a/b) \equiv 0 \pmod{4}. \]

Since \( (b/a) = \pm 1 \),

\[ (b/a) + (a/b) = 0. \]

We use the same way in the remainder part and then we obtain the
result.

Proof of the Corollary 2.

The case \( n=2 \) we use the theorem 2. Since \( \mu_1 = \prod_{m: \text{odd prime}} m^{2/(m-1)} \),

\[
3d(a:b,1) \equiv 3\left(a-1\right) - 4 + 2\left(\frac{b}{a}\right) + \left(\frac{1}{a}\right)
\]

\[
\equiv 3(a+1) + 2\left(\frac{b}{a}\right) \pmod{8}.
\]

Similarly

\[
3d(b:a,1) \equiv 3(b+1) + 2\left(\frac{a}{b}\right) \pmod{8}.
\]

We substitute these formulas for the new reciprocity law (***) in the proof of the cor.1)and then

\[
a(3(a+1) + 2\left(\frac{b}{a}\right)) + b(3(b+1) + 2\left(\frac{a}{b}\right)) \equiv 3 - 3ab \pmod{8}.
\]

Since \( a \) and \( b \) are odd, \( a^2 \equiv b^2 \equiv 1 \pmod{8} \).

Hence

\[
3(a+1) + 2a\left(\frac{b}{a}\right) + 3(b+1) + 2b\left(\frac{a}{b}\right) \equiv 3 - 3ab \pmod{8}.
\]

\[
2\left(a\left(\frac{b}{a}\right) + b\left(\frac{a}{b}\right)\right) \equiv -3(a+b+1+ab)
\]

\[
\equiv -3(a+1)(b+1)
\]

\[
\equiv 3(a+1)(b+1) \pmod{8}.
\]

\[
a\left(\frac{b}{a}\right) + b\left(\frac{a}{b}\right) \equiv \frac{3}{2}(a+1)(b+1) \pmod{4}.
\]

Q.E.D.

As previously stated we can't find the algorithm yet. After this to do first of all is to find the algorithm.
References


