ACTA ARITHMETICA
107.1 (2003)

Generalized Dedekind sums, correlation of L-series, and the Galois module of $\cot(\pi/N)\cot(m\pi/N)$

by

Kurt Girstmair (Innsbruck)

Introduction. Let $N \geq 3$ be a natural number and m an integer such that $(m, N) = 1$. The classical Dedekind sum $S(m, N)$ can be defined by

$$S(m,N) = \frac{1}{4N} \sum_{j=1}^{N-1} \cot(j\pi/N)\cot(jm\pi/N), \tag{1}$$

cf. [10, p. 18]. There are many results about the *distribution* of Dedekind sums, cf. [2]. For example, if $|m/N|$ is small, the point $(x, y) = (m/N, S(m, N))$ lies very close to the hyperbola $xy = 1/12$. This fact can be enounced as

$$S(m,N) = \frac{1}{12m} N + m\theta \tag{2}$$

if m is fixed and N tends to infinity, with $|\theta| \leq 1/5$, say (cf. [9]). Formula (2) is a rather immediate consequence of the reciprocity law for Dedekind sums. In this paper we consider a "character analogue" of $S(m, N)$ in the spirit of [1] (and other papers of the same author): Let χ be a Dirichlet character mod N. We put

$$S(m,\chi) = \frac{1}{4N} \sum_{j=1}^{N-1} \chi(j)\cot(j\pi/N)\cot(jm\pi/N). \tag{3}$$

Obviously, $S(m, \chi)$ vanishes if χ is an odd character, so we may assume that χ is *even*. Some simple properties of $S(m, N)$ have immediate analogues in the case of $S(m, \chi)$. For example, if m^* is a multiplicative inverse of m mod N, then

$$S(m^*, N) = S(m, N) \quad \text{and} \quad S(m^*, \chi) = \chi(m) S(m, \chi).$$

We do not know whether a reciprocity law holds for our sums $S(m, \chi)$. However, there is a close analogue of (2), namely,

2000 *Mathematics Subject Classification*: 11F20, 11M20, 11R18.

THEOREM 1. *Let $m \in \mathbb{Z}$ be fixed and N tend to infinity, $(N,m)=1$. Then*

$$S(m,\chi)=\frac{L(2,\chi)}{2\pi^2 m}N+\left(\frac{|m|}{\pi^2}+\frac{1}{4}\right)\theta\log N \tag{4}$$

with $|\theta|\le 1$.

The main term of (4) involves the value of the L-series

$$L(s,\chi)=\sum_{k=1}^{\infty}\frac{\chi(k)}{k^s}$$

at $s=2$. This means that the main term of (2) arises from that of (4) in the most natural way: One has to replace $L(2,\chi)$ by $\zeta(2)=\pi^2/6$. However, our study of $S(m,\chi)$ (and, in particular, our search for an analogue of (2)) was not so much motivated by the extension of classical results about Dedekind sums to character analogues—rather we had in mind two *applications* of Theorem 1. We are going to describe them now.

Let $\mathcal{X}_N$ denote the set of Dirichlet characters mod N. By $\mathcal{X}_N^+$ and $\mathcal{X}_N^-$ we denote the subsets of even and odd characters in $\mathcal{X}_N$, respectively. The values $L(1,\psi)$ of the L-series $L(s,\psi)$ belonging to characters $\psi\in\mathcal{X}_N^-$ form the entries of the vector

$$X=(L(1,\psi))_{\psi\in\mathcal{X}_N^-}.$$

This vector can be considered as a statistical quantity whose distribution deserves some interest. Its most obvious statistical parameter, namely, the *mean value*

$$\frac{2}{\varphi(N)}\sum_{\psi\in\mathcal{X}_N^-}L(1,\psi)=\frac{\pi}{N}\cot(\pi/N), \tag{5}$$

is well known (here $\varphi(N)$ is the Euler function; formula (5) is an easy consequence of (17) and (18) below). Computing the *variance* of X is basically equivalent to the computation of the *quadratic* mean value

$$\frac{2}{\varphi(N)}\sum_{\psi\in\mathcal{X}_N^-}|L(1,\psi)|^2=\frac{\pi^2}{6}\prod_{p|N}(1-1/p^2)-\frac{\pi^2\varphi(N)}{2N^2}, \tag{6}$$

a problem solved in [6], [7]. The asymptotic behaviour of both mean values for $N\to\infty$ is almost obvious, cf. (23), (24). For higher power mean values of X and related concepts the reader may consult [12], [13] and other articles of the same author.

Another natural question in this connection is the statistical behaviour of X under *character translations*. Two kinds of translation are considered here: First, we fix an *even* character $\chi\in\mathcal{X}_N^+$ and replace $\psi\in\mathcal{X}_N^-$ by $\overline{\chi}\psi$ (the complex conjugate character $\overline{\chi}$ has been chosen instead of χ for esthetic reasons only, cf. Theorem 2). This gives rise to the vector

$$X' = (L(1, \overline{\chi}\psi))_{\psi \in \mathcal{X}_N^-}.$$

Since $\overline{\chi}\psi$ also runs through $\mathcal{X}_N^-$, the vector X' is just a permutation of X. Second, we apply a translation to the *arguments* of ψ, i.e., we multiply each argument $k \in \mathbb{Z}$ by a fixed integer m, $(m, N) = 1$. This leads to the functions $\psi(m)\psi$ and the twisted L-series

$$\psi(m)L(1, \psi) = \sum_{k=1}^{\infty} \frac{\psi(mk)}{k},$$

which are the entries of the vector

$$X'' = (\psi(m)L(1, \psi))_{\psi \in \mathcal{X}_N^-}.$$

Let $K(m, \chi) = K(X'', X')$ denote the statistical *correlation coefficient* (for its definition cf. Section 2) of the vectors X'', X'. One of our main results concerns the asymptotic behaviour of $K(m, \chi)$, namely,

Theorem 2. *Let $m \in \mathbb{Z}$, $m \neq \pm 1$, be fixed, N varying but prime to m. Let χ_0 denote the trivial character in $\mathcal{X}_N$. For $\chi \neq \chi_0$ and N tending to infinity, the correlation coefficient $K(m, \chi)$ satisfies*

$$K(m, \chi) = \frac{\chi(m)L(2, \chi)}{m\sqrt{L(2, \chi_0)^2 - L(2, \chi_0)}} + O\left(\frac{\log N}{N}\right). \tag{7}$$

For the (slightly different) cases $m = \pm 1$ or $\chi = \chi_0$ cf. Theorem 4. It is not hard to see that the absolute value of the main term of Theorem 2 is $\geq 1/(2m)$ (cf. the third remark on Theorem 4), whereas the remainder term tends to 0 for large N, of course. The theorem shows that the size of the correlation coefficient is essentially determined by m and $L(2, \chi)$. It also suggests that large values of m automatically entail a small degree of interdependence of X'' and X'. But this is not always true, since the value of the square root in (7) also depends on m and may be small when m is large. In order to obtain an example of this kind one may take a *prime* number $m \geq 100$, say, whereas N is the product of all primes $p < m^2$, $p \neq m$.

The key ingredient of Theorem 2 is the asymptotic behaviour of

$$\Lambda(m, \chi) = \sum_{\psi \in \mathcal{X}_N^-} \psi(m)L(1, \psi)L(1, \chi\overline{\psi}). \tag{8}$$

We shall see, however, that $\Lambda(m, \chi)$ equals $S(m, \chi)$ up to a simple factor, so Theorem 1 is exactly the result needed for our purpose.

The *second* application of Theorem 1 concerns certain *Galois modules* in the Nth cyclotomic field $\mathbb{Q}_N$. Let $G = \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ be the Galois group of $\mathbb{Q}_N$ over $\mathbb{Q}$. For a number $a \in \mathbb{Q}_N$ the Galois module of a is the $\mathbb{Q}$-vector space spanned by the conjugates $\varrho(a)$, $\varrho \in G$, of a. Its $\mathbb{Q}$-dimension is called the *Galois rank* of a and denoted by $\mathrm{rk}(a)$. In previous papers cases like $a = i\cot(\pi/N)$ or $a = \cot(\pi/N)^2$ have been studied, cf. [4], [8], [11]. Here we consider

$$a = \cot(\pi/N)\cot(m\pi/N),$$

for a natural number m prime to N. This number a lies in $\mathbb{Q}_N^+$, the maximal real subfield of $\mathbb{Q}_N$. There are good reasons to expect $\mathrm{rk}(a) = \varphi(N)/2$, which is the same as saying that the Galois module of a is $\mathbb{Q}_N^+$ itself (or that the conjugates of a form a *normal basis* of $\mathbb{Q}_N^+$). This is true for $m = 1$, N arbitrary (which is just the aforementioned case $a = \cot(\pi/N)^2$) and for $m = 2$ and $N \geq 6$. Nevertheless, $\mathrm{rk}(a) < \varphi(N)/2$ is possible, cf. Section 4, Corollary 1. It turns out that the generalized Dedekind sums $S(m,\chi)$ determine the Galois module of $a = \cot(\pi/N)\cot(m\pi/N)$ *completely*; in particular,

$$\mathrm{rk}(a) = |\{\chi \in \mathcal{X}_N^+ : S(m,\chi) \neq 0\}|,$$

by (29), (31). Our results show that $S(m,\chi)$, $\chi \in \mathcal{X}_N^+$, cannot vanish if N is *large* relative to m; so $\mathrm{rk}(a) = \varphi(N)/2$ then. The following theorem is a more precise version of this assertion.

Theorem 3. *Let $m \geq 13$ be a natural number with $(m,N) = 1$. If*

$$N \geq 12\, m^2 \log m,$$

then the Galois module of $\cot(\pi/N)\cot(m\pi/N)$ equals $\mathbb{Q}_N^+$.

Section 1 is devoted to the proof of Theorem 1. The proof presented here is not ours but due to the referee—we only worked out the explicit values of the respective constants. This proof has a double advantage: It is much less complicated and gives a considerably better remainder term than our original proof. The quality of the remainder term determines the bound of Theorem 3, so it is important in the present context. We say some words about our original proof at the end of Section 1. Section 2 concerns the asymptotics of the correlation coefficient $K(m,\chi)$ and a similar statistical concept $\widetilde{K}(m,\chi)$. In Section 3 we provide the tools needed for the treatment of the Galois module of $a = \cot(\pi/N)\cot(m\pi/N)$ and prove the above Theorem 3. We also exhibit the respective bounds for the numbers $m \leq 12$, which are not covered by this theorem. The final section is devoted to (exceptional) cases where $\mathrm{rk}(a) < \varphi(N)/2$ (cf. Propositions 1–3). In addition, it contains *lower* bounds for this rank in some cases where N has a special shape but m is arbitrary (cf. Proposition 5 and Corollary 2).

Acknowledgements. The author gratefully acknowledges the important contribution of the anonymous referee to the present paper (as mentioned above) and a number of other helpful comments of his. Further, he would like to thank his Viennese colleagues C. Baxa and W. G. Nowak for their support in connection with the first version of this article.

1. Proof of Theorem 1. Because of $S(-m,\chi)=-S(m,\chi)$ we shall assume $m\ge 1$, $(m,N)=1$, for the time being. Furthermore, we need something more precise than the usual O-notation. Therefore, $\mathcal{L}(f(x))$ denotes a function $g(x)$ such that $|g(x)|\le|f(x)|$ for all arguments under consideration. Our summation indices j,k are natural numbers unless they are specified otherwise.

We start with some auxiliary results. The function $1/x-\cot x$ is strictly increasing in the interval $]0,\pi/2]$. Hence,

$$0\le 1/x-\cot x\le 2/\pi,\quad \cot x=1/x+\mathcal{L}(2/\pi)\quad \text{for all } x\in\,]0,\pi/2]. \tag{9}$$

Further, we note that

$$\sum_{j\le N/2}\frac{1}{j}\le\log N\quad\text{for all } N\ge 10, \tag{10}$$

which is a simple consequence of the fact that the function

$$f(N)=\log N-\sum_{j\le N/2}\frac{1}{j}$$

satisfies $f(N+2)-f(N)\ge\log((N+2)/N)-2/(N+1)>0$ for all $N\ge 9$. Next,

$$\sum_{j\le N/2}|\cot(jm\pi/N)|\le\frac{N}{\pi}\log N\quad\text{for all } N\ge 10. \tag{11}$$

In fact, the left side of (11) is independent of m; because of (9) we obtain

$$0\le\sum_{j\le N/2}\cot(j\pi/N)\le\sum_{j\le N/2}\frac{N}{j\pi},$$

so (11) follows from (10). Finally,

$$\sum_{j\ge x}\frac{1}{j^2}\le\frac{2}{x}\quad\text{for all } x>0. \tag{12}$$

As to the *proof of Theorem 1*, we assume $N\ge 10$ and write

$$\begin{aligned}4NS(m,\chi)&=\sum_{j=1}^{N-1}\chi(j)\cot(j\pi/N)\cot(jm\pi/N)\\&=2\sum_{j\le N/2}\chi(j)\left(\frac{N}{j\pi}+\mathcal{L}(2/\pi)\right)\cot(jm\pi/N),\end{aligned}$$

by (9). So $4NS(m,\chi)$ consists of the parts

$$M=\frac{2N}{\pi}\sum_{j\le N/2}\frac{\chi(j)}{j}\cot(jm\pi/N)$$

and

$$R = \frac{4}{\pi}\,\mathcal{L}\Big(\sum_{j\le N/2}\chi(j)\cot(jm\pi/N)\Big) = \frac{4}{\pi}\,\mathcal{L}\Big(\sum_{j\le N/2}|\cot(jm\pi/N)|\Big).$$

Now (11) shows

$$R = \frac{4N}{\pi^2}\,\mathcal{L}(\log N).$$

Whereas R is a less important part of the remainder term, M will split into the *main* term and the *dominant* part of the remainder term of (4). Accordingly, we write $M = M_1 + M_2$ with

$$M_1 = \frac{2N}{\pi}\sum_{j\le N/(2m)}\frac{\chi(j)}{j}\cot(jm\pi/N)$$

and

$$M_2 = \frac{2N}{\pi}\sum_{N/(2m)<j\le N/2}\frac{\chi(j)}{j}\cot(jm\pi/N).$$

The arguments $jm\pi/N$ occurring in M_1 are in the interval $]0,\pi/2]$. Therefore, (9) gives $\cot(jm\pi/N) = N/(jm\pi) + \mathcal{L}(2/\pi)$. Inserting this in M_1 we obtain

$$M_1 = \frac{2N^2}{m\pi^2}\sum_{j\le N/(2m)}\frac{\chi(j)}{j^2} + \frac{4N}{\pi^2}\,\mathcal{L}\Big(\sum_{j\le N/(2m)}\frac{1}{j}\Big). \tag{13}$$

The first sum on the right side of (13) is

$$\sum_{j\le N/(2m)}\frac{\chi(j)}{j^2} = L(2,\chi) + \mathcal{L}\Big(\sum_{j\ge N/(2m)}\frac{1}{j^2}\Big) = L(2,\chi) + \mathcal{L}(4m/N),$$

by (12). The second one is clearly

$$\mathcal{L}\Big(\sum_{j\le N/2}\frac{1}{j}\Big) = \mathcal{L}(\log N) \quad \text{for all } N\ge 10,$$

by (10). We obtain

$$M_1 = \frac{2N^2}{m\pi^2}L(2,\chi) + \mathcal{L}\Big(\frac{8N}{\pi^2}\Big) + \frac{4N}{\pi^2}\,\mathcal{L}(\log N).$$

As concerns M_2, observe that $1/j \le 2m/N$ for all indices j in the range $N/(2m)\le j\le N/2$. Thus,

$$M_2 = \frac{2N}{\pi}\,\mathcal{L}\Big(\sum_{N/(2m)<j\le N/2}\frac{2m}{N}|\cot(jm\pi/N)|\Big) = \frac{4mN}{\pi^2}\,\mathcal{L}(\log N),$$

by (11). Altogether, we have

$$S(m,\chi) = \frac{L(2,\chi)}{2m\pi^2}N + \mathcal{L}\Big(\frac{m+2}{\pi^2}\log N + \frac{2}{\pi^2}\Big) \tag{14}$$

for $N \geq 10$. This proves Theorem 1 and is precise enough for later applications.

Remarks. 1. The case of the trivial character $\chi = \chi_0$ was treated separately in the first version of this paper. Here (and only here) we obtained a slightly better remainder term in (14), namely

$$\mathcal{L}\biggl(\frac{m+2}{3}\log\log N\biggr)$$

for $N \geq 16$. The proof was based on the reciprocity law for ordinary Dedekind sums.

2. In Section 4 we shall see that $S(m,\chi) = 0$ in a number of cases (of course, N must be small relative to m then). This means that the remainder term of (14) must be $\neq 0$ in general; otherwise, the main term would also vanish in the cases mentioned, which is impossible. Two exceptions, however, are worth noticing: If $m = 1$, $\chi \neq \chi_0$, then $S(1,\chi) = L(2,\chi)N/(2\pi^2)$. This result can be found in [4, Theorem 2] already. In the case $m = 2$, the formula

$$\cot(x)\cot(2x) = \cot^2(x)/2 - 1/2 \tag{15}$$

shows that $S(2,\chi) = S(1,\chi)/2$ for each $\chi \neq \chi_0$. For $m \geq 3$, however, the corresponding trigonometric formulas are no longer helpful.

3. The *classical* Dedekind sums can be defined in a purely rational way in terms of the *sawtooth function*

$$((x)) = \begin{cases} x - \lfloor x \rfloor - 1/2 & \text{if } x \notin \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$$

A slight generalization of such a sum is

$$S(m,N;j) = \sum_{k=1}^{N-1} \biggl(\biggl(\frac{k}{N}\biggr)\biggr)\biggl(\biggl(\frac{mk+j}{N}\biggr)\biggr),$$

where $j \in \mathbb{Z}$ is arbitrary (cf., for instance, [5, p. 72]). For $j = 0$ this definition gives $S(m,N) = S(m,N;0)$. The reader may ask how our sums $S(m,\chi)$ are connected with the above "rational" Dedekind sums. In the case of a *primitive* character $\chi \in \mathcal{X}_N^+$ this connection is remarkably simple, namely

$$S(m,\chi) = \frac{\tau(\chi)}{N}\sum_{j=1}^{N-1} \overline{\chi}(j)S(m,N;j). \tag{16}$$

Here $\tau(\chi)$ is the usual Gauss sum

$$\tau(\chi) = \sum_{k=1}^{N-1} \chi(k)e^{2k\pi i/N}.$$

Our original proof of Theorem 1 was based on this identity. As we said above, it was much more complicated, but a considerable part of these complications was due to the case of imprimitive characters, where (16) is less beautiful.

2. The correlation coefficients. The first aim of this section is to show that the sums $\varLambda(m,\chi)$ and $S(m,\chi)$ of (8) and (3) are equal up to a simple factor. The formula

$$L(1,\psi)=\frac{\pi}{2N}\sum_{j=1}^{N-1}\psi(j)\cot(j\pi/N) \tag{17}$$

holds for arbitrary characters $\psi\in\mathcal{X}_N^-$, cf. [6, Proposition 1]. Applied to (8), this formula gives

$$\varLambda(m,\chi)=\frac{\pi^2}{4N^2}\sum_{j=1}^{N-1}\cot(j\pi/N)\sum_{k=1}^{N-1}\chi(k)\cot(k\pi/N)\sum_{\psi\in\mathcal{X}_N^-}\psi(mj)\overline{\psi}(k).$$

The last of these sums can be simplified by means of the orthogonality relation

$$\sum_{\psi\in\mathcal{X}_N^-}\psi(j)=\begin{cases}\varphi(N)/2 & \text{if } j\equiv 1 \bmod N,\\ -\varphi(N)/2 & \text{if } j\equiv -1 \bmod N,\\ 0 & \text{otherwise.}\end{cases} \tag{18}$$

This yields

$$\varLambda(m,\chi)=\frac{\pi^2\varphi(N)\chi(m)}{N}\,S(m,\chi), \tag{19}$$

which is what we desired.

Now we consider the vector space $\mathbb{C}^n$ with the standard (hermitian) inner product $\langle -,-\rangle$ (which is $\mathbb{C}$-linear in the first component) and the corresponding norm $\|-\|$. For a (statistical) vector $X=(X_j)\in\mathbb{C}^n$,

$$Z(X)=\Big(X_j-\frac{1}{n}\sum_j X_j\Big)\in\mathbb{C}^n$$

denotes its *centred version.* Then

$$\frac{1}{n}\|Z(X)\|^2$$

is the *variance* of X. If, moreover, $Y\in\mathbb{C}^n$ is another vector, then

$$\frac{1}{n}\langle Z(X),Z(Y)\rangle$$

is the statistical *covariance* of X and Y. These quantities occur in the *correlation coefficient*

$$K(X,Y)=\frac{\langle Z(X),Z(Y)\rangle}{\|Z(X)\|\cdot\|Z(Y)\|} \tag{20}$$

of X and Y, which is defined if $Z(X)$, $Z(Y)$ are both $\neq 0$. If $|K(X,Y)|$ is close to 1, then $Z(Y)$ is nearly a $\mathbb{C}$-multiple of $Z(X)$, in the opposite case $K(X,Y) \approx 0$, these vectors are almost orthogonal to each other. In the language of statistics one would say that X and Y are *dependent* or *independent* instead. From the viewpoint of euclidean geometry, however, one identifies $\mathbb{C}^n$ with $\mathbb{R}^{2n}$ and calls $\arccos(\operatorname{Re}\{K(X,Y)\})$ the *angle* between $Z(X)$ and $Z(Y)$. In the special situation studied here both vectors X, Y will have real mean values, i.e., $\sum_j X_j$ and $\sum_j Y_j$ are real numbers. This implies

$$\begin{aligned} \|Z(X)\|^2 &= \|X\|^2 - \frac{1}{n}\Big(\sum_j X_j\Big)^2, \\ \langle Z(X), Z(Y)\rangle &= \langle X, Y\rangle - \frac{1}{n}\sum_j X_j \sum_j Y_j; \end{aligned} \tag{21}$$

so these expressions look simpler than those obtained from the mere definition of the variance or covariance.

In the remainder of this section n equals $\varphi(N)/2$, $N \geq 3$. We identify the set

$$\mathbb{C}^{\mathcal{X}_N^-} = \{(x_\psi)_{\psi\in\mathcal{X}_N^-} : x_\psi \in \mathbb{C}\}$$

with $\mathbb{C}^n$ and consider the vector

$$X = (L(1,\psi))_{\psi\in\mathcal{X}_N^-} \in \mathbb{C}^n$$

of the Introduction. Recall the relevant modifications of X, namely,

$$X' = (L(1,\overline{\chi}\psi))_{\psi\in\mathcal{X}_N^-}, \qquad X'' = (\psi(m)L(1,\psi))_{\psi\in\mathcal{X}_N^-},$$

with $\chi \in \mathcal{X}_N^+$ and $m \in \mathbb{Z}$, $(m,N) = 1$. The correlation coefficient

$$K(m,\chi) = K(X'', X')$$

is defined by (20). At this point we mention that the correlation remains the same if X remains unchanged, say $X' = X$, whereas the second vector X'' undergoes *both* kinds of character translations: In fact, for

$$X''' = (\chi\psi(m)L(1,\chi\psi))_{\psi\in\mathcal{X}_N^-}$$

we have $K(m,\chi) = K(X''', X)$. Because of $K(-m,\chi) = -K(m,\chi)$ it suffices to consider *natural* numbers m.

Our *proof of Theorem 2* is based on the formulas (21). So it requires, first of all, the knowledge of the asymptotic behaviour of the mean values of X'' and X' when m is *fixed* and N tends to infinity. To this end we use

$$\sum_{\psi\in\mathcal{X}_N^-} \psi(m)L(1,\psi) = \frac{\varphi(N)\pi}{2N}\cot(m^*\pi/N); \tag{22}$$

here m^* is, as above, an inverse of m mod N. Like (5), this follows from (17) by means of the orthogonality relation (18). In the case of an *arbitrary* m, (22) supplies the mean value of X''; the case $m = 1$ gives the mean value of X'. The asymptotics of the right hand side of (22) can be read from

$$\frac{\pi}{N}\cot(m^*\pi/N) = \begin{cases} 1 + O(1/N) & \text{if } m = 1, \\ O(1/N) & \text{if } m > 1. \end{cases} \tag{23}$$

The case $m = 1$ of (23) is an immediate consequence of (9). In the case $m > 1$, we have $mm^* = 1 + kN$, $k \in \mathbb{Z}$, $k \neq 0$, and may suppose $|m^*| \leq N/2$. Accordingly, $1/2 \geq |m^*/N| = |k/m + 1/(Nm)| \geq 1/m - 1/(3m)$, so (9) gives $\cot(m^*\pi/N) = \mathcal{L}(3m/(2\pi)) = O(1)$.

The next entries of (21) are the variances or, in our terminology,

$$\|X''\|^2 = \|X'\|^2 = \sum_{\psi\in\mathcal{X}_N^-} |L(1,\psi)|^2.$$

As above, let χ_0 denote the trivial character mod N. Then $L(2,\chi_0) = \prod_{p|N}(1 - 1/p^2)\zeta(2)$; hence (6) yields

$$\sum_{\psi\in\mathcal{X}_N^-} |L(1,\psi)|^2 = \frac{\varphi(N)}{2}\,(L(2,\chi_0) + O(1/N)). \tag{24}$$

From (21)–(24) we obtain

$$\|Z(X')\|^2 = \frac{\varphi(N)}{2}\,(L(2,\chi_0) - 1 + O(1/N)).$$

This equals $\|Z(X'')\|^2$ in the case $m = 1$. For $m > 1$, (23) implies

$$\|Z(X'')\|^2 = \frac{\varphi(N)}{2}\,(L(2,\chi_0) + O(1/N))$$

instead. Altogether, the asymptotics of the denominator of $K(X'', X')$ is clear now, cf. (20). The numerator, in turn, involves

$$\langle X'', X'\rangle = \sum_{\psi\in\mathcal{X}_N^-} \psi(m)L(1,\psi)L(1,\chi\overline{\psi}) = \Lambda(m,\chi),$$

cf. (8). In view of (19), this is basically the same as $S(m,\chi)$, whose behaviour is described by Theorem 1. It is not hard to put these facts together and to prove Theorem 2 and its analogues for $m = \pm 1$ or $\chi = \chi_0$. One should, however, recall that the remainder term of $S(m,\chi)$ vanishes in the case $\chi \neq \chi_0$, $m = \pm 1$, cf. the second remark at the end of Section 1. We have, indeed,

Theorem 4. *Let $m \in \mathbb{Z}$, $m \neq 0$, be fixed, N varying but prime to m, further $\chi \in \mathcal{X}_N^+$. If N tends to infinity, then*

$$K(m,\chi)=H(m,\chi)+O\left(\frac{\log N}{N}\right),$$

where the main term $H(m,\chi)$ and sharper versions of the error term look as follows:

(a) *Let $m\neq\pm1$. Then*

$$H(m,\chi)=\frac{\chi(m)L(2,\chi)}{m\sqrt{L(2,\chi_0)^2-L(2,\chi_0)}},$$

χ_0 denoting the trivial character mod N. In the case $\chi=\chi_0$, the error term is $O(N^{-1}\log\log N)$.

(b) *Let $m=\pm1$. Then*

$$H(m,\chi)=m\,\frac{L(2,\chi)-1}{L(2,\chi_0)-1}.$$

The error term is $O(1/N)$ for $\chi\neq\chi_0$, and $=0$ otherwise.

Remarks. 1. The better error term in the case $m\neq\pm1$, $\chi=\chi_0$, is a consequence of the first remark at the end of Section 1 (whose proof was part of the first version of this article).

2. Because of the Cauchy–Schwarz inequality, $|H(m,\chi)|$ is expected to be ≤ 1 for large values of N. In case (b) of Theorem 4 this is obviously true for *all* values of N. In case (a) it suffices to show

$$\frac{L(2,\chi_0)}{m\sqrt{L(2,\chi_0)^2-L(2,\chi_0)}}\leq 1,$$

which is equivalent to $L(2,\chi_0)\geq m^2/(m^2-1)$. Since m and N are coprime,

$$L(2,\chi_0)=\sum_{\substack{k=1\\(k,N)=1}}^{\infty}\frac{1}{k^2}\geq\sum_{j=0}^{\infty}\frac{1}{m^{2j}}=\frac{m^2}{m^2-1}.$$

3. Let $m\neq\pm1$. From

$$\frac{\pi^2}{15}=\frac{\zeta(4)}{\zeta(2)}=\prod_p\frac{1}{1+1/p^2}\leq|L(2,\chi)|\leq\zeta(2)=\frac{\pi^2}{6}\tag{25}$$

one sees that for all possible values of N,

$$|H(m,\chi)|\geq C/m\quad\text{with}\quad C=\frac{2\pi}{5\sqrt{\pi^2-6}}\approx 0.638817.$$

Accordingly, there is always some (statistical) dependence between X'' and X' if m is small and N large.

Next we introduce another modification of the vector X, namely,

$$\widetilde{X}=(\overline{\psi}(m)L(1,\psi))_{\psi\in\mathcal{X}_N^-},$$

which differs from X'' inasmuch as the character value $\psi(m)$ is replaced by $\overline{\psi}(m)$. Clearly $\widetilde{X} = X''$ if $m = \pm1$. In the case $m \neq \pm1$, however, the correlation coefficient

$$\widetilde{K}(m,\chi) = K(\widetilde{X}, X')$$

is fairly different from $K(m,\chi)$. There are two reasons for this fact: First, the factor $\chi(m)$ disappears from the main term $H(m,\chi)$, since

$$\sum_{\psi\in\mathcal{X}_N^-} \overline{\psi}(m)L(1,\psi)L(1,\chi\overline{\psi}) = \overline{\chi}(m)\Lambda(m,\chi),$$

cf. (8). Second, the asymptotic behaviour of the mean value of $\widetilde{X}$ is different; indeed,

$$\frac{2}{\varphi(N)}\sum_{\psi\in\mathcal{X}_N^-} \overline{\psi}(m)L(1,\psi) = \frac{\pi}{N}\cot\left(\frac{m\pi}{N}\right) = 1/m + O(1/N),$$

cf. (22), (9). In the end we have

Theorem 5. *In the setting of Theorem* 4, *let m be different from* ±1. *Then*

$$\widetilde{K}(m,\chi) = \frac{L(2,\chi)-1}{m\sqrt{L(2,\chi_0)^2-(1+1/m^2)L(2,\chi_0)+1/m^2}} + O\left(\frac{\log N}{N}\right).$$

In the case $\chi=\chi_0$, the error term can be replaced by $O(N^{-1}\log\log N)$.

Remark. The expression under the square root in Theorem 5 is at least $(L(2,\chi_0)-1)^2$. This implies that the main term of $|\widetilde{K}(m,\chi)|$ is always $\le 1/m$.

3. The Galois module of $\cot(\pi/N)\cot(m\pi/N)$ **in the main case.** Put $\zeta_N = e^{2\pi i/N}$. Then $\mathbb{Q}_N = \mathbb{Q}(\zeta_N)$ is the Nth cyclotomic field. The Galois group $G = \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ consists of the automorphisms ϱ_k, $(k,N)=1$, defined by $\zeta_N \mapsto \zeta_N^k$. Let

$$\mathbb{Q}[G] = \bigoplus_{\varrho\in G}\mathbb{Q}\varrho$$

denote the *rational group ring* over G, which acts on the field $\mathbb{Q}_N$ in the usual way. For a number $a\in\mathbb{Q}_N$,

$$\mathbb{Q}[G]a = \sum_{\varrho\in G}\mathbb{Q}\varrho(a)$$

is the *Galois module* of a. This module can be described completely in terms of eigenvalues of the matrix $(\varrho_{jk^*}(a))_{j,k}$; here $1\le j,k\le N$, $(j,N)=$

$(k, N) = 1$, and $kk^* \equiv 1 \bmod N$. The eigenvalues mentioned have the shape

$$y(a\,|\,\chi) = \sum_{\substack{k\le N\\(k,N)=1}} \chi(k)\varrho_k(a), \qquad \chi \in \mathcal{X}_N. \tag{26}$$

We do not discuss all details of this description; they have been given, e.g., in [4]. Some important facts, however, will be highlighted in the next two paragraphs.

Fix a character $\chi \in \mathcal{X}_N$ for the time being and let $d = \operatorname{ord}(\chi)$ denote its order. We say $\chi' \in \mathcal{X}_N$ is *conjugate* to χ if χ and χ' generate the same subgroup of $\mathcal{X}_N$; in this case we write $\chi' \sim \chi$. Clearly $\chi' \sim \chi$ implies $d = \operatorname{ord}(\chi')$. First suppose $y(a\,|\,\chi) = 0$. Then the same holds for each $\chi' \sim \chi$. So we have a system of $\varphi(d)$ relations of the form

$$y(a\,|\,\chi') = 0, \qquad \chi' \sim \chi, \tag{27}$$

among the conjugates $\varrho_k(a)$ of a. By (26), however, the coefficients of these relations are character values, hence they are *not rational* in general. But one can transform this system into an equivalent system of relations

$$\sum_{\substack{k\le N\\(k,N)=1}} c_{j,k}\varrho_k(a) = 0, \qquad j = 0, 1, \ldots, \varphi(d) - 1, \tag{28}$$

with all coefficients $c_{j,k} \in \mathbb{Q}$. To this end one chooses an integer g such that $\operatorname{ord}(\chi(g)) = d$. For each j and each k as in (28), let $d_{j,k}$ denote the *order* of the root of unity $\chi(g^j k)$. Then the integers

$$c_{j,k} = \mu(d_{j,k})\varphi(d)/\varphi(d_{j,k})$$

have the desired property (here $\mu(-)$ is the Möbius function).

The *proof* of this assertion uses the Vandermonde matrix $(\chi'(g^j))_{j,\chi'}$, whose subscripts run through $j = 0, 1, \ldots, \varphi(d) - 1$ and all $\chi' \sim \chi$; further, it is based on the fact that $\sum_{\chi'\sim\chi} \chi'(g^j k)$ is a rational integer, namely, the number $c_{j,k}$ just displayed.

The characters corresponding to *nonvanishing* eigenvalues $y(a\,|\,\chi) \neq 0$, on the other hand, determine the structure of the $\mathbb{Q}[G]$-module $\mathbb{Q}[G]a$, cf. [4]. Each class of conjugate characters of this kind gives rise to a certain *simple* submodule of $\mathbb{Q}[G]a$; and in this way one obtains the *complete decomposition* of $\mathbb{Q}[G]a$ into simple components. One also knows the idempotent elements that generate the corresponding simple ideals of $\mathbb{Q}[G]$. Moreover, the *Galois rank* $\operatorname{rk}(a)$ of a, i.e., the $\mathbb{Q}$-dimension of $\mathbb{Q}[G]a$, is given by the formula

$$\operatorname{rk}(a) = |\{\chi \in \mathcal{X}_N : y(a\,|\,\chi) \neq 0\}|.$$

We consider the case when a lies in $\mathbb{Q}_N^+ = \mathbb{Q}_N \cap \mathbb{R}$. Because of $\varrho_{-k}(a) = \varrho_k(a)$ for all k, $y(a\,|\,\chi) = 0$ for all *odd* characters $\chi \in \mathcal{X}_N$. Therefore, the

Galois module structure of $\mathbb{Q}[G]a$ is determined by the set

$$\{\chi \in \mathcal{X}_N^+ : y(a \,|\, \chi) = 0\}.$$

If this set is empty, then $\mathrm{rk}(a) = \varphi(N)/2$, i.e., $\mathbb{Q}[G]a = \mathbb{Q}_N^+$. Otherwise, this set describes the nontrivial rational relations (28) among the conjugates of a; further,

$$\mathrm{rk}(a) = \varphi(N)/2 - |\{\chi \in \mathcal{X}_N^+ : y(a \,|\, \chi) = 0\}|. \tag{29}$$

In what follows we concentrate on the particular number

$$a = \cot(\pi/N)\cot(m\pi/N),$$

with $m \in \mathbb{Z}$ prime to N, as usual. The notation

$$a(j,k) = \cot(j\pi/N)\cot(k\pi/N)$$

$(j,k \in \mathbb{Z}$ prime to $N)$ will be useful. Because of

$$i\cot(k\pi/N) = (1+\zeta_N^k)/(1-\zeta_N^k), \qquad (k,N) = 1,$$

$a(1,m)$ lies in $\mathbb{Q}_N^+$, indeed, and its conjugates are the numbers

$$a(k,mk) = \varrho_k(a(1,m)), \qquad (k,N) = 1. \tag{30}$$

Together with (3) and (26), this gives the fundamental identity

$$y(a(1,m) \,|\, \chi) = 4NS(m,\chi). \tag{31}$$

One has to decide, thus, which of the generalized Dedekind sums $S(m,\chi)$, $\chi \in \mathcal{X}_N^+$, vanish. It is clear that we may restrict ourselves to *positive* numbers m.

We start with the case $m = 1$, which is known (cf. [8], [11]). At the end of Section 1 we remarked that

$$S(1,\chi) = \frac{L(2,\chi)N}{2\pi^2} \neq 0$$

for each $\chi \in \mathcal{X}_N^+$, $\chi \neq \chi_0$. Moreover, (6) in connection with (19) gives

$$\begin{aligned} S(1,\chi_0) &= \frac{NL(2,\chi_0)}{2\pi^2} - \frac{\varphi(N)}{4N} \\ &= \frac{1}{4}\prod_{p|N}\left(1-\frac{1}{p}\right)\left(\frac{N}{3}\prod_{p|N}\left(1+\frac{1}{p}\right)-1\right), \end{aligned} \tag{32}$$

which cannot vanish for $N \geq 3$. Altogether, $\mathrm{rk}(a(1,1)) = \varphi(N)/2$ for all $N \geq 3$.

In the case $m = 2$, $N \geq 3$, the aforementioned remark yields $y(a(1,2) \,|\, \chi) \neq 0$ whenever $\chi \neq \chi_0$, whereas $y(a(1,2) \,|\, \chi_0) = 0$ only for $N = 5$ (use (15) and (32)). So $\mathrm{rk}(a(1,2)) = \varphi(N)/2$ for all $N \geq 6$. The next theorem shows that the statement "$\mathrm{rk}(a(1,m)) = \varphi(N)/2$" (the so-called "main case") holds whenever N is large relative to m:

Theorem 6. *Let $N \geq 10$ and m be natural numbers with $(m, N) = 1$. If*

$$\frac{N}{\log N} > \frac{30}{\pi^2}\left(m^2 + 2m + \frac{2m}{\log N}\right) \tag{33}$$

then $\mathrm{rk}(a(1,m)) = \varphi(N)/2$.

Proof. If $\mathrm{rk}(a(1,m)) < \varphi(N)/2$, then $S(m,\chi) = 0$ for some character $\chi \in \mathcal{X}_N^+$, by (31). So (14) entails

$$\frac{|L(2,\chi)|N}{2m} \leq (m+2)\log N + 2.$$

Because of $|L(2,\chi)| \geq \pi^2/15$ (cf. (25)), this requires that $N/\log N$ does not exceed the right side of (33). ■

Theorem 3 is a slightly weaker but more handsome version of Theorem 6. For its *proof* suppose that (33) does *not* hold. We evaluate the constants of (33) numerically and assume $m \geq 13$ and $N \geq 5000$. This yields

$$\frac{N}{\log N} < 3.04\left(1 + \frac{2}{13} + \frac{2}{13\log 5000}\right)m^2 < Cm^2$$

for $C = 3.57$. Put $\beta = 3.34$, further $x = \beta C m^2 \log m$. Thus, $\beta C < 12$ and

$$\log x \leq 2\log m + \log\log m + \log 12 \leq \left(2.37 + \frac{\log 12}{\log 13}\right)\log m \leq \beta \log m;$$

here we have used $\log\log m \leq 0.37\log m$, which is, indeed, true for all m under consideration. Accordingly, $x/\log x \geq Cm^2$. By the monotonicity of the function $N/\log N$, $N/\log N < Cm^2$ cannot hold for $N \geq x = 11.9238m^2\log m$. Theorem 3 follows since the conditions $m \geq 13$ and $N \geq 12\,m^2\log m$ automatically imply $N \geq 5000$.

The cases $m = 1, 2$ have been treated above. So the only cases not covered by Theorem 3 concern the numbers $m \in \{3, 4, \ldots, 12\}$. Here (33) shows that $\mathrm{rk}(a(1,m)) = \varphi(N)/2$ as soon as $N \geq C_m$, where the value of C_m can be read from the following list of pairs (m, C_m): $(3, 275)$, $(4, 474)$, $(5, 733)$, $(6, 1052)$, $(7, 1435)$, $(8, 1883)$, $(9, 2397)$, $(10, 2979)$, $(11, 3630)$, $(12, 4352)$.

Remark. The data collected by the author suggests that a bound like $N \geq 2m^2$ might be sufficient for $\mathrm{rk}(a(1,m)) = \varphi(N)/2$ in the case of *prime* numbers N (at least). In fact, the largest exceptions we know have the shape $N = m^2 + 3m + 1$ (cf. the next section).

4. The Galois module of $\cot(\pi/N)\cot(m\pi/N)$: special results.

We adopt the notations of the foregoing section but also consider *negative* values m. As above, m^* denotes a multiplicative inverse of m mod N. In addition, one should recall that $a(j,k)$ (j, k prime to N) depends on the *residue classes* of j and k mod N only.

In the first part of this section we consider pairs (m, N) for which the above "main case" does not hold, so $\mathrm{rk}(a(1,m)) < \varphi(N)/2$. We start with a sort of equivalence for the pairs (m, N) that helps keeping the final list small. Because of

$$a(1,-m) = -a(1,m)$$

the Galois modules of $a(1,m)$ and $a(1,-m)$ are the same. Moreover, $a(1,m^*)$ is *conjugate* to $a(1,m)$, since

$$\varrho_m(a(1,m^*)) = a(m,mm^*) = a(m,1) = a(1,m),$$

cf. (30). So the Galois modules of $a(1,m)$ and $a(1,m^*)$ are also identic. Hence it is justified to say that two pairs (m', N) and (m'', N) are *trivially equivalent* if m' and m'' are congruent mod N to one of the numbers m, $-m$, m^*, $-m^*$.

From now on we identify $\mathcal{X}_N$ with the *character group* of the Galois group G, i.e., we put

$$\chi(\varrho_k) = \chi(k)$$

for each $\chi \in \mathcal{X}_N$ and each automorphism ϱ_k. In the case of the trivial character $\chi = \chi_0$ this gives $\chi_0(\varrho_k) = 1$ for each ϱ_k. The following criterion supplies, in a sense, *all* pairs (m, N) with $\mathrm{rk}(a(1,m)) < \varphi(N)/2$ known to the author, and, in fact, all *existing* pairs with $m \le 30$, N a prime. Recall that each system $y(a(1,m)\,|\,\chi) = 0$ of vanishing eigenvalues (χ running through a certain conjugacy class in $\mathcal{X}_N^+$) means that the maximal Galois rank $\varphi(N)/2$ decreases by the number $\varphi(\mathrm{ord}(\chi))$ and gives rise to the same number of independent relations, cf. (27)–(29).

Proposition 1. *Let H be a subgroup of the Galois group G and $a \in \mathbb{Q}_N$ such that the trace*

$$T(a) = \sum_{\varrho \in H} \varrho(a)$$

is rational. Then $y(a\,|\,\chi) = 0$ for each character $\chi \neq \chi_0$ which is trivial on H (i.e., $\chi(\varrho) = 1$ whenever $\varrho \in H$). If $T(a) = 0$, this is also true for $\chi = \chi_0$.

Proof. By (26),

$$y(a\,|\,\chi) = \sum_{\varrho \in G} \chi(\varrho)\varrho(a).$$

Let $\mathcal{R} \subseteq G$ be a complete system of representatives of G/H. Thus,

$$y(a\,|\,\chi) = \sum_{\sigma \in \mathcal{R}} \sum_{\varrho \in H} \chi(\sigma\varrho)\sigma\varrho(a).$$

Let χ be trivial on H and $T(a) \in \mathbb{Q}$. Then $\chi(\sigma\varrho) = \chi(\sigma)$ and

$$y(a \mid \chi) = \sum_{\sigma\in\mathcal{R}} \chi(\sigma)\sigma(T(a)) = T(a) \sum_{\sigma\in\mathcal{R}} \chi(\sigma).$$

So $T(a) = 0$ implies $y(a \mid \chi) = 0$. If, on the other hand, $\chi \neq \chi_0$, the character sum on the right hand side vanishes, since χ can be considered as a nontrivial character of G/H. ■

Our first application of Proposition 1 is

PROPOSITION 2. *Let $N \geq 3$ and $m \in \mathbb{Z}$ be such that $m^2 \equiv -1 \bmod N$. If $\chi \in \mathcal{X}_N^+$ is a character with $\chi(m) = 1$, then*

$$y(a(1,m) \mid \chi) = 0.$$

Proof. The subgroup $H = \langle \varrho_m \rangle$ of G has order 4 and

$$T(a(1,m)) = a(1,m) + a(m,m^2) + a(m^2,m^3) + a(m^3,m^4) = 0,$$

since $a(m,m^2) = a(m,-1) = -a(1,m)$ and, in the same way, $a(m^3,m^4) = a(m^3,-m^2) = -a(m^2,m^3)$. ■

We briefly consider the case of a prime number $N = p$. There is a natural number m such that $m^2 \equiv -1 \bmod p$ if, and only if, $p \equiv 1 \bmod 4$. For such a pair (m,p) the set $\{\chi \in \mathcal{X}_p^+ : \chi(m) = 1\}$ is a subgroup of index 2 in $\mathcal{X}_p^+$. Hence (29) and Proposition 2 give

COROLLARY 1. *If $N = p$ is a prime $\equiv 1 \bmod 4$ and $m^2 \equiv -1 \bmod p$, then $\mathrm{rk}(a(1,m)) \leq (p-1)/4$.*

The next application of Proposition 1 gives a less obvious result:

PROPOSITION 3. *Let $N \geq 3$ and $m \in \mathbb{Z}$ be such that $m^2 + m + 1 \equiv 0 \bmod N$. If $\chi \in \mathcal{X}_N^+$, $\chi \neq \chi_0$, is a character with $\chi(m) = 1$, then*

$$y(a(1,m) \mid \chi) = 0.$$

Proof. Let x, y, z be real numbers such that none of them is of the form $n\pi$ but $x + y + z = n\pi$ for some integer n (e.g., the angles of a triangle have this property). Then

$$\cot(x)\cot(y) + \cot(y)\cot(z) + \cot(z)\cot(x) = 1. \tag{34}$$

This can easily be verified by means of the addition theorem

$$\cot(x+y) = (\cot(x)\cot(y) - 1)/(\cot(x) + \cot(y)).$$

Because of $m^2 + m + 1 \equiv 0 \bmod N$, m is prime to N and $m^3 \equiv 1 \bmod N$. Note that a character χ with the properties in question exists only if $N > 3$, so $H = \langle \varrho_m \rangle$ is a group of order 3. The numbers $x = \pi/N$, $y = m\pi/N$ and $z = m^2\pi/N$ are such that (34) holds. Accordingly,

$$T(a(1,m)) = a(1,m) + a(m,m^2) + a(m^2,1) = 1,$$

and Proposition 1 gives the result. ■

In the situation of Proposition 3, we have $m+1 \equiv -m^2 \equiv -m^* \bmod N$. The pairs (m,N) and $(m+1,N)$ are, thus, trivially equivalent in the above sense. The number of characters χ in question amounts to $\varphi(N)/6-1$, which means $\mathrm{rk}(a(1,m)) = \mathrm{rk}(a(1,m+1)) \le \varphi(N)/3+1$.

The criterion contained in Proposition 1 is not hard to check in any particular case—but the settings of Propositions 2 and 3 are the only ones for which the author *a priori* knows that it applies. Are there other examples (m,N) such that the generalized Dedekind sum $S(m,\chi)$ vanishes for some $\chi \in \mathcal{X}_N^+$? This is, in fact, true. We enclose a list of pairs of this kind with prime moduli $N = p$. They have been found by means of the following search procedure: Let m and the prime p be given, p below some bound like $12m^2 \log m$, cf. Theorem 3. Each conjugacy class of even characters χ is completely determined by its order d—and these orders are just the divisors of $\varphi(p)/2 = (p-1)/2$. Looking for some χ with $\mathrm{ord}(\chi) = d$ such that $S(m,\chi) = 0$ we use, first, one of the relations (28), say for $j = 1$. In other words, if

$$\Big|\sum_{k=1}^{p-1} c_{1,k}a(k,km)\Big| < 0.001, \tag{35}$$

then the character χ corresponding to d is a candidate for $S(m,\chi) = 0$. A precision of 24 decimal digits produced only candidates such that the left side of (35) was $< 10^{-16}$; this suggests that $S(m,\chi)$ *really* vanishes. We know two different possibilities how to check this by means of computer calculations but confine ourselves to sketching *one* here: By (16), $S(m,\chi) = 0$ if, and only if,

$$\sum_{k=1}^{p-1} \chi(k)S(m,p;k) = 0.$$

As in the case of (27) and (28), we transform this equation into an equivalent system of linear equations with integral coefficients, namely,

$$\sum_{k=1}^{p-1} c_{j,k}S(m,p;k) = 0, \qquad j = 0,1,\ldots,\varphi(d)-1, \tag{36}$$

the coefficients $c_{j,k}$ being those of (28). It is not hard to verify that $4pS(m,p;k)$ is in $\mathbb{Z}$ whenever $p > 3$. Hence $4p$ times the left side of (36) is always a rational integer, so it is easy to decide whether it is zero or not. All candidates found by our search passed this test and a number of other criteria like computing the left side of (35) with higher precision.

Our list is supposed to be *exhaustive* in the following sense: Each possible pair (p,m) with $m \le 30$ and $\mathrm{rk}(a(1,m)) < \varphi(p)/2$ is trivially equivalent (as defined above) either to one of the types covered by Propositions 2, 3 or to a pair from our list. For $m = 30$, Theorem 6 yields 30293 as the largest upper bound for p one has to deal with.

Additional pairs (m, p) with $\mathrm{rk}(a(1, m)) < \varphi(p)/2$

m	p	d	m	p	d
4	29	2	20	461	$2, 5, 10$
7	53	2	21	101	2
8	89	2	21	109	2
9	61	2	25	317	2
11	53	2	26	151	3
12	181	2	27	349	2
13	101	2	27	397	2
15	109	2	27	811	3
15	137	2	28	97	3
16	173	2	30	113	2
19	163	3	30	137	2
20	163	3	30	991	5

Since p and $d = \mathrm{ord}(\chi)$ are known, we also know the possible groups H of Proposition 1. Computing the respective traces shows that *all* pairs of the list are of the type described by this proposition—but the group H is always considerably large, in contrast with the situations of Propositions 2 and 3. This has to do with the fact that d is small. Moreover, (29) implies that

$$\mathrm{rk}(a(1, m)) = \varphi(p)/2 - \sum_{d} \varphi(d)$$

is close to $\varphi(p)/2$ for these examples.

In the final part of this paper we consider some cases where $y(a(1, m) \,|\, \chi)$ cannot vanish. We start with a prime number $N = p$ and the trivial character $\chi = \chi_0$. By (1), $y(a(1, m) \,|\, \chi_0) = 4pS(m, p)$. It is known that the ordinary Dedekind sum $S(m, p)$ vanishes if, and only if, $m^2 \equiv -1 \bmod p$, cf. [9]. So we have a (rather weak) partial converse of Proposition 2:

PROPOSITION 4. *Let $N = p \geq 3$ be a prime number and $m \in \mathbb{Z}$, $p \nmid m$, be such that $m^2 \not\equiv -1 \bmod p$. Then $y(a(1, m) \,|\, \chi_0) \neq 0$.*

Next let χ be a *primitive* character mod N. We sketch a result that was proved in detail in the first version of this paper. By means of a reduction formula for Dedekind sums ([5], p. 79) one can show that the sum on the right side of (16) equals $m^* B_{2,\overline{\chi}}/2$ plus an algebraic integer. Here $B_{2,\overline{\chi}}$ is the generalized Bernoulli number belonging to the complex conjugate of χ, cf. [3]. The reference mentioned also says when $B_{2,\overline{\chi}}/2$ is *not* an algebraic integer: The number N must be an odd prime power $N = p^r$, $r \geq 1$, and χ must be of the shape $\chi = \chi_1^2$ for a generator χ_1 of the (cyclic) group $\mathcal{X}_N$. For such a number N a character χ of this type is, conversely, even and primitive. The denominator of $B_{2,\overline{\chi}}/2$ contains a prime ideal lying above p then. This means that $m^*B_{2,\overline{\chi}}/2$ cannot be integral either. Hence we have, in view of (31),

Proposition 5. *Let $p \geq 3$ be a prime, $N = p^r$, $r \geq 1$, and m not divisible by p. Let χ_1 be a generator of the cyclic group $\mathcal{X}_N$ and $\chi = \chi_1^2$. The number $y(a(1,m)\,|\,\chi)/\tau(\chi)$ is not an algebraic integer and, thus, $\neq 0$. Accordingly, $\mathrm{rk}(a(1,m)) \geq \varphi(\varphi(N)/2)$.*

In the setting of Proposition 5, $\mathrm{ord}(\chi) = \varphi(N)/2$ is the largest order an even character can take, which is reflected by the fact that $\mathrm{rk}(a(1,m))$ cannot be much smaller than its largest possible value $\varphi(N)/2$. If $N = p$ is a prime of the shape $2q + 1$, $q \geq 3$ another prime, then $\varphi(\varphi(p)/2) = q - 1$. Moreover, we have $p \equiv 3 \bmod 4$, so $m^2 \not\equiv -1 \bmod p$ for all m not divisible by p. Accordingly, Propositions 4 and 5 give

Corollary 2. *Let $q \geq 3$ and $p = 2q + 1$ be prime numbers, further $m \in \mathbb{Z}$ not divisible by p. For $N = p$, $\mathrm{rk}(a(1,m)) = \varphi(N)/2$.*

References

[1] B. C. Berndt, *Character transformation formulae similar to those for the Dedekind eta-function*, in: Analytic Number Theory, Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 9–30.

[2] R. W. Bruggeman, *On the distribution of Dedekind sums*, in: Contemp. Math. 166, Amer. Math. Soc., 1994, 197–210.

[3] L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. 202 (1959), 174–182.

[4] K. Girstmair, *Character coordinates and annihilators of cyclotomic numbers*, Manuscripta Math. 59 (1987), 375–389.

[5] D. Knuth, *The Art of Computer Programming*, vol. 2, Addison-Wesley, 1969.

[6] S. Louboutin, *Quelques formules exactes pour des moyennes de fonctions L de Dirichlet*, Canad. Math. Bull. 36 (1993), 190–196.

[7] —, *Corrections à: Quelques formules exactes pour des moyennes de fonctions L de Dirichlet*, ibid. 37 (1994), 89.

[8] T. Okada, *On an extension of a theorem of Chowla*, Acta Arith. 38 (1981), 341–345.

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

[10] H. Rademacher and E. Grosswald, *Dedekind Sums*, Carus Math. Monogr. 16, Math. Assoc. America, 1972.

[11] K. Wang, *On a theorem of Chowla*, J. Number Theory 15 (1982), 1–4.

[12] W. Zhang, *On the mean values of Dedekind sums*, J. Théor. Nombres Bordeaux 8 (1996), 429–442.

[13] W. Zhang, Y. Yi and X. He, *On the 2k-th power mean of Dirichlet L-functions with the weight of general Kloosterman sums*, J. Number Theory 84 (2000), 199–213.

Institut für Mathematik
Universität Innsbruck
Technikerstr. 25/7
A-6020 Innsbruck, Austria
E-mail: Kurt.Girstmair@uibk.ac.at

Received on 16.7.2001
and in revised form on 1.8.2002 (4077)