Cyclotomic matrices and a limit formula for $h_p^-$

by

KURT GIRSTMAIR (Innsbruck)

1. Introduction. Let $N \geq 3$ be a natural number (henceforth often called the modulus) and $j$ an integer with $(j, N) = 1$. One of the main objects of this article is the infinite sum

$$b_j(N) = \frac{2\pi}{N} \sum_{\substack{m=1 \\ (m, N) = 1}}^{\infty} \frac{\mu(m)}{m} \sin \frac{2\pi(mj)^*}{N}. \tag{1}$$

Here $\mu$ denotes the Möbius function and $(\cdot)^*$ an inverse mod $N$ of the respective number (i.e., $k^*$ is an integer such that $kk^* \equiv 1 \text{ mod } N$). The series (1) is conditionally convergent and has to be understood in the usual sense of the limit

$$\lim_{n \to \infty} \sum_{m \leq n} \sum_{m=1}^{\infty} \frac{\mu(m)}{m} \sin \frac{2\pi(mj)^*}{N}, \tag{2}$$

an interpretation which applies to several sums below. We fix $N$ for the time being and, therefore, simply write $b_j$ instead of $b_j(N)$. Obviously, $b_j$ depends on the residue class of $j$ mod $N$ only. Let $\zeta_N = e^{2\pi i/N}$, so $\mathbb{Q}(\zeta_N)$ is the $N$th cyclotomic field. The numbers $b_j$ are in $\mathbb{Q}$ and have to do with the relative class number $h_N^-$ of $\mathbb{Q}(\zeta_N)$. This connection is particularly close in the case of a prime number $N = p$. We note

**Theorem 1.** Let $N = p \geq 3$ be a prime and $\kappa = \max\{m : 2^m | (p-1)\}$. Suppose, moreover, that $h_p^-$ is square-free and prime to $p - 1$. Then the rational numbers $2^\kappa b_j$, $(j, N) = 1$, have the exact denominator $h_p^-$, i.e.,

$$2^\kappa b_j = n_j/h_p^-$$

for an integer $n_j$ with $(n_j, h_p^-) = 1$ (in particular, $b_j \neq 0$ if $h_p^- > 1$).

There are 54 primes $p$, $3 \leq p < 300$, with $h_p^- > 1$. For 30 of these, $h_p^-$ is square-free and prime to $p - 1$. Hence Theorem 1 is, at least, not empty. For primes $p$ not falling under the theorem one has to expect that

2000 Mathematics Subject Classification: 11R18, 11R42, 11R29.

[129]
the denominator of \(2^\kappa b_j\) equals \(h_p^-\) up to powers of small primes (cf. Sections 3–5; in particular, Table 2).

In principle, the relative class number \(h_p^-\) (or a very large divisor of it) may be computed by means of formula (1). Indeed, suppose we know, in the setting of Theorem 1, that \(2^\kappa h_p^-\) has at most \(d\) decimal digits (such a \(d\) can be read from estimates like \(h_p^- \leq 2p(p/24)^{(p-1)/4}\), cf. [16], p. 441). Let \(a_j = b_j - [b_j]\) denote the fractional part of the number \(b_j\). On summing up sufficiently many terms of the series (1) we find the number \(\alpha_j, 0 < \alpha_j < 1\), that consists of the first \(2d+1\) digits (after the decimal point) of \(a_j\). But then the continued fraction expansion of \(\alpha_j\) quickly reveals the exact value \(a_j\): it is the uniquely determined convergent of \(\alpha_j\) with the largest denominator \(< 10^d\) (cf. [2]). However, the said series converges rather slowly, so this method cannot be recommended in practice. We give an example: In the case \(p = 43\), \(\kappa\) equals 1 and \(2h_p^- = 422\), thus \(d = 3\) is a suitable choice.

Taking the sum (1) over all suitable \(m \leq 84 \cdot 10^6\), one obtains 0.0616080 as a candidate for \(\alpha_1\). The convergents of this number are 0, 1/16, 4/65, 13/211, 82/1331, \ldots; accordingly, 13/211 should be the correct value of \(a_1\) (which coincides with \(b_1\) here). This is true, although not all of the seven relevant digits of \(a_1 = 0.0616113\ldots\) are identical with those of our candidate; hence it is not astonishing that the same amount of work does not give the correct value of \(a_4\) (= \(b_4\)), say.

Nevertheless, we think that (1) is an interesting series. A large part of this paper is devoted to the investigation of the arithmetical properties of its value \(b_j = b_j(N)\). The key to these properties is an alternative (and even simpler) definition of \(b_j\) by means of certain numbers in the cyclotomic field \(\mathbb{Q}(\zeta_N)\). To this end we consider the “sine numbers”

(3) \[ s_j = s_j(N) = 2i \sin(2\pi j/N) \]

and the “cotangent numbers”

(4) \[ c_j = c_j(N) = i \cot(\pi j/N), \]

which are defined for all integers \(j\) prime to \(N\). Because of

\[ s_j = \zeta_N^j - \zeta_N^{-j}, \quad c_j = (1 + \zeta_N^j)/(1 - \zeta_N^j), \]

both kinds of numbers lie in the field \(\mathbb{Q}(\zeta_N)\), more precisely, in its \(\mathbb{Q}\)-subspace \(\mathbb{Q}(\zeta_N) \cap i\mathbb{R}\). This subspace has dimension \(\varphi(N)/2\) and (as is known but will anew be shown below) the \(\mathbb{Q}\)-basis \((c_j)_{j \in \mathcal{R}}\), where

\[ \mathcal{R} = \{ j \in \mathbb{Z} : 1 \leq j < N/2, \ (j, N) = 1 \}. \]

Accordingly, there are uniquely determined rational numbers \(b_j, j \in \mathcal{R}\), such that

(5) \[ s_1 = \sum_{j\in\mathcal{R}} b_j c_j. \]
Each number $b_j$ of (5) is, in fact, identical with the respective number $b_j(N)$ of (1), $j \in \mathcal{R}$. We extend the definition of the numbers $b_j$ of (5) to all indices $j \in \mathbb{Z}$, $(j, n) = 1$, by means of

\begin{equation}
    b_{N-j} = -b_j, \quad b_{j+mN} = b_j, \quad m \in \mathbb{Z},
\end{equation}

an extension that is consistent with (1). The study of the arithmetical properties of $b_j$ (in particular, its connection with $h_N^-$) requires some additional notations.

Let $\mathcal{X}^-$ be the set of odd Dirichlet characters mod $N$. By $f_\chi$ we denote the conductor of a $\chi \in \mathcal{X}^-$ and by $\chi_f$ the primitive character (mod $f_\chi$) belonging to $\chi$. Moreover,

\begin{equation}
    B_\chi = \sum_{k=1}^{f_\chi} k\chi_f(k)/f_\chi
\end{equation}

denotes the corresponding Bernoulli number of order 1. It turns out that the number $b_j$ is a sort of weighted mean value of the reciprocals of the numbers $B_\chi$, $\chi \in \mathcal{X}^-$. In view of this we call

\begin{equation}
    w_\chi = \frac{\mu(N/f_\chi)\overline{\chi_f(N/f_\chi)}}{(N/f_\chi)\prod_{p|N}(1 - \overline{\chi_f(p)}/p)}
\end{equation}

denotes the weight factor of $\chi \in \mathcal{X}^-$ (the bar denotes the complex conjugate).

\textbf{THEOREM 2.} Let $N \geq 3$, $(j, N) = 1$. Then

\begin{equation}
    b_j = \frac{-2}{\varphi(N)} \sum_{\chi \in \mathcal{X}^-} w_\chi \overline{\chi(j)} B_\chi.
\end{equation}

Theorem 2 is important both for the arithmetic of the numbers $b_j$ and for their actual computation. Together with the well known formula for $h_N^-$ (cf. [20], p. 42), this theorem suggests that the denominator of the rational number $b_j$ is related to the relative class number. In general, however, this denominator also involves divisors of $\varphi(N)$ and numbers coming from the weight factors $w_\chi$ (cf. Table 1). Fortunately, these unwieldy factors are rather harmless in a number of cases: If $N$ is a prime, $w_\chi = 1$ for all $\chi \in \mathcal{X}^-$; if $N$ is a powerful number, $w_\chi$ takes the values 0, 1 only. It was shown in [1] that, in the case of a prime modulus $N = p$, the rational coefficients $b_j$ occurring in equation (5) take the shape (8)—with 1 instead of the factor $w_\chi$. From (7) it is obvious that the generalization to arbitrary moduli $N$ is not straightforward. The aforementioned paper, which was one of our sources of inspiration, also indicates some connections between $b_j$ and $h_N^-$. We shall study these connections more thoroughly in Sections 3–5. Among other things, this study shows that, in the setting of Theorem 1, the numerators $n_j$ of the numbers $2^\kappa b_j$ are by no means random quantities:
Theorem 3. Let the assumptions and notations of Theorem 1 hold: i.e., $h_p^-$ is square-free and prime to $p - 1$ and $2^k b_j = n_j / h_p^-$ for each $j$ with $(j, N) = 1$. Further, let $g \in \mathbb{Z}$ be a primitive root mod $p$. Then there is a number $\gamma \in \mathbb{Z}$, $(\gamma, h_p^-) = 1$, such that

$$n_g^m \equiv n_1 \gamma^m \mod h_p^-$$

for all $m \in \mathbb{Z}$.

It seems that the exponent $\kappa$ of Theorem 1 is not best possible: In all examples known to the author $\kappa$ can be replaced by the number 1; accordingly,

$$2 b_j = n'_j / h_p^- \quad \text{with} \quad n'_j \in \mathbb{Z}, \ (n'_j, h_p^-) = 1.$$

This gives the congruence

$$(9) \quad n'_g^m \equiv n'_1 \gamma^m \mod h_p^-,$$

$m \in \mathbb{Z}$, which is slightly better than that of Theorem 3 from the computational point of view. In quite a number of cases one can compute all numbers $b_j$, $j \in \mathcal{R}$, using nothing but this congruence, if only $b_1$ and $b_g$ (i.e., $n'_1$ and $\gamma$) are known: Indeed, as $p$ tends to infinity, $|B_\chi| \gg p^{1/2}/\log p$ for characters of order $> 2$, whereas $|B_\chi| \geq 1$ for quadratic characters (cf. [15]). Accordingly, $|b_j| \ll p^{-1/2} \log p$ and $|n'_j| < h_p^-/2$ for large values of $p$. If this is true, $n'_g^m$ is the solution of (9) whose absolute value is smallest possible. It seems that this way of finding $n'_j$ applies to all primes $p \geq 47$ that fall under Theorems 1, 3; we have checked this in a number of cases, among them all primes $< 200$. In these cases the order of $\gamma$ in the group $(\mathbb{Z}/h_p^- \mathbb{Z})^\times$ equals $p - 1$, so the numbers $n'_j$, $1 \leq j \leq p - 1$, are all distinct mod $h_p^-$, which implies that the corresponding $b_j$'s must be distinct. From these considerations one gets an impression of the role that arithmetical properties of the $b_j$'s play in their actual computation. We shall discuss this computation in Section 5.

The identities (1), (8) and others follow from the diagonalization of certain cyclotomic matrices, which is the main topic of Section 2. Section 3 deals with possible denominators of the rational numbers $b_j$, whereas Section 4 contains the congruences underlying Theorem 3. Theorem 1 is a synopsis of the material collected in Sections 3 and 4. As we indicated above, this material is needed for the computations of Section 5.

2. Some cyclotomic matrices. Not all of the following results are new; but they have been included in order to present a reasonably smooth and self-contained exposition of the relevant material. For the same reason most of the necessary references have been placed at the end of this section.

Let $N \geq 3$, $\mathcal{R}$ and $\mathcal{X}^-$ be as above. We note the following orthogonality relations, which hold for every $j \in \mathbb{Z}$ with $(j, N) = 1$: 
Limit formula for $h_p^-$

$$
\sum_{\chi \in \mathcal{X}^-} \chi(j) = \begin{cases} 
0 & \text{if } j \not\equiv \pm 1 \mod N, \\
\varphi(N)/2 & \text{if } j \equiv 1 \mod N, \\
-\varphi(N)/2 & \text{if } j \equiv -1 \mod N.
\end{cases}
$$

They can be proved in the usual manner (if $j \not\equiv \pm 1 \mod N$, separate an even character $\psi$ with $\psi(j) \neq 1$).

In what follows we assume that the characters in $\mathcal{X}^-$ are ordered in some (arbitrary but) fixed way: $\mathcal{X}^- = \{\chi_1, \ldots, \chi_{\varphi(N)/2}\}$. This ordering also applies to the columns of the character matrix

$$
X = \sqrt{2/\varphi(N)} \cdot (\chi(j))_{j \in \mathcal{R}, \chi \in \mathcal{X}^-}
$$

(observe that $|\mathcal{R}| = |\mathcal{X}^-| = \varphi(N)/2$). If $A$ is an arbitrary matrix, $A_{j,k}$ (or, possibly, $A_{j,\chi}$) denotes the element of $A$ in the indicated row and column, e.g., $X_{j,\chi} = \sqrt{2/\varphi(N)} \cdot \chi(j)$. On applying (10) to the entries of the matrix $X X^T$, one obtains

**Proposition 1.** The matrix $X$ is unitary, i.e., $X^T = X^{-1}$.

For the time being, let $\{a_j : j \in \mathbb{Z}, (j, N) = 1\}$ be a set of complex numbers with the property (cf. (6))

$$
a_{-j} = -a_j, \quad a_{j+mN} = a_j, \quad m \in \mathbb{Z}.
$$

Then the matrix $A = (a_{jk^*})_{j,k \in \mathcal{R}}$ is normal, i.e., unitarily congruent to a diagonal matrix. More precisely, put $\Delta = \text{diag}(d_{\chi})_{\chi \in \mathcal{X}^-}$ with

$$
d_{\chi} = \sum_{j \in \mathcal{R}} \overline{\chi}(j)a_j.
$$

Now

$$
A = X \Delta X^T
$$

and the element $A_{j,k} = a_{jk^*}$ has the shape

$$
a_{jk^*} = \frac{2}{\varphi(N)} \sum_{\chi \in \mathcal{X}^-} \chi(jk^*)d_{\chi}.
$$

Indeed, (13), (14) immediately follow from (10).

In what follows we are mainly concerned with cyclotomic matrices $A$ that are formed in the following way: Consider the Galois group

$$
\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = \{\sigma_k : k \in \mathbb{Z}, (k, N) = 1\},
$$

where $\sigma_k$ acts on $\zeta_N$ by $\sigma_k(\zeta_N) = \zeta_N^k$. Further, take a number $a \in \mathbb{Q}(\zeta_N) \cap i\mathbb{R}$ and put $a_j = \sigma_j(a)$, $(j, N) = 1$. Because of $\sigma_{-1}(a) = \overline{a} = -a$, these numbers satisfy (11), so $A = (a_{jk^*})_{j,k \in \mathcal{R}}$ is of the above type. It is not hard to see that the matrix $A$ is invertible if, and only if, the family $(a_j)_{j \in \mathcal{R}}$ is $\mathbb{Q}$-linearly independent.
Our first number \( a \) of this kind is the sine number \( s_1 = 2i \sin(2\pi/N) \) of (3), which leads to the sine matrix
\[
S = (s_{jk})_{j,k \in \mathcal{R}}.
\]

One immediately reads from (12) that the corresponding diagonal element \( d_\chi \) is, essentially, the Gauss sum
\[
\tau(\chi) = \sum_{k=1}^{N} \chi(k) \zeta_N^k.
\]

Indeed, on putting
\[
\Gamma = \text{diag}(\tau(\chi))_{\chi \in \chi^-}
\]
we obtain the identity that corresponds to (13), namely,

**PROPOSITION 2.** The sine matrix \( S \) is normal and satisfies
\[
S = X \Gamma X^T.
\]

The next number \( a \) to be considered is the cotangent number \( c_1 = i \cot(\pi/N) \) of (4), which gives rise to the cotangent matrix
\[
C = (c_{jk})_{j,k \in \mathcal{R}}.
\]

Its diagonalization leads to the matrix
\[
(15) \quad \Lambda = \frac{iN}{\pi} \cdot \text{diag}(L(1, \chi))_{\chi \in \chi^-},
\]
which involves the L-series
\[
L(s, \chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}.
\]
This series is absolutely convergent in the half-plane \( \text{Re} \ s > 1 \) and converges in the sense of (2) for \( \text{Re} \ s > 0 \).

**PROPOSITION 3.** The cotangent matrix \( C \) is normal; in fact,
\[
C = X \Lambda X^T.
\]

**Proof.** Compute \((X \Lambda X^T)_{j,k}\) using (14), (15) and the formula
\[
\sum_{m \in \mathbb{Z}} \frac{1}{m} = (\pi/N) \cot(\pi j/N).
\]
This identity follows from the partial fraction decomposition of the cotangent function; the infinite sum has to be understood in the sense of
\[
(16) \quad \lim_{n \to \infty} \sum_{|m| \leq n} \cdot \bullet.
\]

Recall that the L-series \( L(s, \chi) \) does not vanish on the line \( \text{Re} \ s = 1 \) (e.g., [19], p. 254 ff.); in particular, \( L(1, \chi) \neq 0 \). Accordingly, the matrices \( \Lambda \) and
Limit formula for $h_p^-$

C are invertible. From Proposition 3 we obtain a formula for the elements of the inverse cotangent matrix $C^{-1}$. Indeed, put

$$
\hat{c}_j = \hat{c}_j(N) = \frac{-2i\pi}{N\phi(N)} \sum_{\chi \in \chi^{-}} \frac{\chi(j)}{L(1, \chi)},
$$

(17)

where $j \in \mathbb{Z}$ is prime to $N$. The numbers $\hat{c}_j$ will be called the inverse cotangent numbers mod $N$. Using (14) we have

**Proposition 4.** The inverse cotangent matrix has the shape

$$
C^{-1} = (\hat{c}_{jk^*})_{j, k \in \mathbb{R}}.
$$

Our next objective is an infinite series for the number $\hat{c}_j$. To this end we represent the reciprocal of $L(s, \chi)$ by the Dirichlet series

$$
L(s, \chi)^{-1} = \sum_{m=1}^{\infty} \mu(m)\chi(m)/m^s.
$$

(18)

This identity is well known for Re $s > 1$ but maybe not so widely known in the case Re $s = 1$. One may argue as follows: As we remarked above, $L(s, \chi)$ does not vanish for Re $s = 1$, so the function $L(s, \chi)^{-1}$ has an analytic continuation on this line. Then a theorem of D. J. Newman (cf. e.g., [17], p. 66) says that the series (18) converges to $L(s, \chi)^{-1}$ for Re $s = 1$ in the sense of (2). On combining (17), (18) (with $s = 1$) and (10) we have

**Proposition 5.** Let $j \in \mathbb{Z}$ be prime to $N$. Then

$$
\hat{c}_j = \frac{-i\pi}{N} \sum_{m \in \mathbb{Z}} \frac{\mu(|m|)}{m},
$$

(19)

where the sum is meant in the sense of (16).

The numbers $c_j, (j, N) = 1$, are in the $\mathbb{Q}$-vector space $\mathbb{Q}(\zeta_N) \cap i\mathbb{R}$, whose dimension is $\varphi(N)/2$. The matrix $C$ being invertible, these numbers are $\mathbb{Q}$-linearly independent (as we remarked above), so they form a $\mathbb{Q}$-basis of this space. Since $s_1$ is also in $\mathbb{Q}(\zeta_N) \cap i\mathbb{R}$, there are uniquely determined rational numbers $b_j, j \in \mathbb{R}$, such that (5) holds, i.e.,

$$
s_1 = \sum_{j \in \mathbb{R}} b_j c_j.
$$

We extend this definition, in accordance with (6) and (11), to all indices $j \in \mathbb{Z}$ prime to $N$ and form the matrix

$$
B = (b_{jk^*})_{j, k \in \mathbb{R}},
$$

whose entries are rational numbers. Because of (3), this matrix connects the sine matrix with the cotangent matrix:

$$
S = CB^T.
$$

(20)
Indeed, if one applies automorphisms $\sigma_k \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ to the equation (5), one gets more equations of the same type, which are, as a whole, equivalent to the matrix equation (20). Now (20) says $B^T = C^{-1}S$; by Proposition 4 this is the same as

$$b_j = \sum_{k \in \mathcal{R}} \hat{c}_k s_{(kj)^*}, \quad (j, N) = 1. \tag{21}$$

On inserting the series (19) for the numbers $\hat{c}_k$ into this formula we obtain

**Proposition 6.** Let $j \in \mathbb{Z}$ be prime to $N$. Then

$$b_j = \frac{2\pi}{N} \sum_{m=1}^{\infty} \frac{\mu(m)}{m} \sin \frac{2\pi(mj)^*}{N}. \tag{22}$$

In other words, we have shown the limit formula (1) for the numbers $b_j$ defined by (5) but, of course, none of their arithmetical properties. These properties are based on Theorem 2, which we shall prove now:

**Proof of Theorem 2.** From (20) and Propositions 2 and 3 we see that $B$ is a normal matrix, namely,

$$B^T = \Lambda X^{-1} \Gamma X^T.$$

The entries $\tau(\chi)$ of the diagonal matrix $\Gamma$ can be expressed in terms of the corresponding primitive Gauss sums: Put

$$\tau(\chi) = \sum_{k=1}^{f} \chi_f(k) e^{2\pi i k/f}. \tag{23}$$

By [10], p. 427,

$$\tau(\chi) = \mu(N/f) \chi_f(N/f) \tau(\chi_f).$$

This identity has the following analogue for $L$-series:

$$L(1, \chi) = \prod_{p|N} (1 - \chi_f(p)/p) \cdot L(1, \chi_f), \tag{24}$$

which is an immediate consequence of the Euler product representations of $L(s, \chi)$ and $L(s, \chi_f)$. We use these identities (for $\chi$ instead of $\chi$) and the well known evaluation

$$L(1, \chi_f) = i\pi \tau(\chi_f) B_\chi/f,$$

of $L(1, \chi_f)$ in terms of the generalized Bernoulli number of order 1 (cf. [20], p. 37). Altogether, we obtain

$$\Lambda^{-1} \Gamma = \text{diag}(-w_\chi/B_\chi)_{\chi \in \chi^*},$$

where $w_\chi$ means the weight factor (7). Then (14) yields the identity (8), i.e., Theorem 2. \hfill \blacksquare
REMARKS. 1. Of course, formulas (12)–(14) are only variants of known formulas for group determinants (belonging to the group of prime residues mod $N$, cf. [20], p. 71 ff.). Some cyclotomic matrices, together with certain (rather general) character matrices were diagonalized in [4].

2. We could not find Proposition 3 in the literature, although it is implicitly known in the terminology of Leopoldt’s character coordinates: Indeed, the diagonal element $d_{\chi}$ of (12) is essentially the same as the $\chi$-coordinate $y(\chi|a)$ of the corresponding number $a$ (cf. [7]). In the said paper this coordinate was computed for $a = c_1$, the cotangent number. The results of [7] immediately give the diagonalization of other cyclotomic matrices, for instance, the tangent matrix

$$(i \tan(\pi j k^* / N))_{j, k \in \mathbb{R}};$$

in this case the elements on the diagonal of $A$ must be multiplied by certain non-vanishing Euler factors (e.g., by $1 - 2\chi(2)$ if $N$ is odd; ibid., Th. 3).

3. The determinant of the cotangent matrix $C$ can be expressed in terms of the product $\prod_{\chi \in \chi^*} B_{\chi}$, which is essentially the same as $h_N$. This is an immediate consequence of Proposition 3, (22) and (23). In the case $N = p \geq 3$ this connection of $h_N$ with the cotangent determinant was given in [5]. As to the general case, [8] contains an index formula which is equivalent to this determinant formula; the determinant formula itself can be found in [18]. The papers [14], [13] and a number of papers of the author (e.g., [6], [9]) deal with various aspects of cotangent (and related) numbers.

4. The inverse cotangent numbers $\widehat{c}_j(N)$ (in a shape slightly different from the infinite sums (19) and without the normalizing factor $-i\pi / N$) play a role in the work of Hecke on Eisenstein series of higher levels (cf. [12]). We do not go into details of this application here. The arithmetic of the numbers $\widehat{c}_j$ seems to be even more complicated than that of the $b_j$’s.

3. PRIMES IN THE DENOMINATOR OF $b_j(N)$. Let $N \geq 3$ be as above. We also adopt the other notations. In what follows a prime number dividing $N$ is, in general, denoted by $p$, whereas arbitrary primes go by the name of $l$.

For a prime $l$ let $v_l : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ denote the corresponding valuation of $\mathbb{Q}$; this means that $v_l(l^m) = m$ for all $m \in \mathbb{Z}$. For $c, d \in \mathbb{Q}$ and $m \in \mathbb{Z}$ we say $c$ divides $d$ outside of $m$ (c equals $d$ outside of $m$, resp.) if $v_l(c) \leq v_l(d)$ ($v_l(c) = v_l(d)$, resp.) for all primes $l$ not dividing $m$. An algebraic number $a$ will be called $l$-integral if there is an integer $c$ with $v_l(c) = 0$ such that $ac$ is an algebraic integer. The denominator of a rational number $c$ is the natural number defined by
hence the denominator of an integer is 1.

This section is devoted to the study of primes \( l \) that may occur in the denominator of a number \( b_j = b_j(N) \). A survey of these primes is both interesting for its own and useful for the computation of \( b_j \). A look at Theorem 2 shows that it is probably much easier to describe the denominator of \( b_j \) (in terms of primes occurring in \( h_N^{-1} \)) than to predict any primes occurring in the numerator. Some insight into the arithmetic of the numerator will be obtained in the next section (cf. Theorems 3, 5).

For a character \( \chi \in \mathcal{X}^- \) let \( Q(\chi) \) denote its field of values, \( Q(\chi) = Q(\chi(j) : j \in \mathbb{Z}) \), and

\[
\mathcal{N}_\chi : Q(\chi) \rightarrow Q
\]

the corresponding norm (relative to \( Q \)). Two characters \( \chi, \chi' \) are mutually conjugate if, and only if, they generate the same group \( \langle \chi \rangle = \langle \chi' \rangle \). By \( \lbrack \chi \rbrack \) we denote the conjugacy class of \( \chi \in \mathcal{X}^- \). The Bernoulli number \( B_{\chi} \) lies in \( Q(\chi) \). Its norm \( h_{\chi} \) can be written as

\[
h_{\chi} = \mathcal{N}_\chi(B_{\chi}) = \prod_{\chi' \in [\chi]} B_{\chi'}.
\]

By its definition, \( B_{\chi} \) is \( p \)-integral for all \( p \) not dividing \( f_{\chi} \), therefore \( h_{\chi} \) is also \( p \)-integral for these primes. Let \( \mathcal{C} \) denote a system of representatives of the conjugacy classes in \( \mathcal{X}^- \). The relative class number formula ([20], p. 42) shows that the product \( \prod_{\chi \in \mathcal{C}} h_{\chi} \) equals \( h_N^{-1} \) outside of \( 2N \).

Next we pick out those characters \( \chi \in \mathcal{X}^- \) for which the weight factor \( w_\chi \) does not vanish. To this end we write

\[
N_1 = \prod_{v_p(N)=1} p, \quad N_2 = \prod_{v_p(N)>1} p^{v_p(N)}.
\]

Using (7), the reader may convince himself that \( w_\chi \neq 0 \) if, and only if, \( N_2 \mid f_\chi \mid N \). This fact suggests the definitions

\[
\mathcal{X}' = \{ \chi \in \mathcal{X}^- : N_2 \mid f_\chi \mid N \} \quad \text{and} \quad \mathcal{C}' = \mathcal{C} \cap \mathcal{X}'.
\]

The size of \( \mathcal{X}' \) depends on the structure of \( N \): the cases of a square-free modulus \( N \) (where \( \mathcal{X}' = \mathcal{X}^- \)) and of a powerful modulus \( N \) (where \( \mathcal{X}' = \{ \chi \in \mathcal{X}^- : f_\chi = N \} \)) mark the two possible extremes. Now (8) reads

\[
b_j = \frac{-2}{\phi(N)} \sum_{\chi \in \mathcal{X}'} w_\chi \frac{\overline{\chi}(j)}{B_{\chi}}.
\]
Further, we define
\[ h' = \prod_{\chi \in \mathcal{C}'} h_{\chi}. \]
Of course, \( h' \) divides \( h^{-}_{N} \) outside of \( 2N \). If \( N \) is square-free, one even has equality outside of \( 2N \); on the other hand, if \( N = p^{e} \) is a prime power, \( h' \) equals
\[ \hat{h} = h^{-}_{N}/h^{-}_{N/p} \] (25)
outside of \( 2p \). The quotient \( \hat{h} \) is a natural number (cf. [16], p. 474).

Besides the norm factors \( h_{\chi} \) we also need the norms of the weight factors \( w_{\chi}, \chi \in \mathcal{C} \). By virtue of (7), \( w_{\chi} \) can be written as
\[ w_{\chi} = \varepsilon \prod_{p \mid N} (p - \overline{\chi}_{f}(p)) \] (26)
with a certain root \( \varepsilon \) of unity; so we obtain
\[ \mathcal{N}_{\chi}(w_{\chi}) = \pm 1 \prod_{p \mid N} \mathcal{N}_{\chi}(p - \overline{\chi}_{f}(p)). \]
The norms in the denominator of this number are certain values of cyclotomic polynomials. Indeed, let \( \Phi_{d} \) denote the \( d \)th cyclotomic polynomial. For a prime \( p \) dividing \( N \), \( p \nmid f_{\chi} \), put
\[ d_{\chi,p} = \text{ord}(\chi_{f}(p)), \]
i.e., the order of the root of unity \( \chi_{f}(p) \). Then
\[ \mathcal{N}_{\chi}(p - \chi_{f}(p)) = \Phi_{d_{\chi,p}}(p). \] (27)
Henceforth the right side of (27) will simply be written \( \Phi_{\chi,p} \).

Fix a prime number \( l \) for the time being. We investigate the exponent of \( l \) in the denominator of \( b_{j}, j \in \mathbb{Z}, (j, N) = 1 \), namely
\[ \lambda_{j} = -v_{l}(b_{j}) \] (28)
(which is \( \leq 0 \) if \( l \) does not occur in the denominator). First suppose \( l \nmid N \). Then \( h_{\chi}/B_{\chi} \) is \( l \)-integral for any character \( \chi \in \mathcal{X}' \). In the same way,
\[ w_{\chi} \prod_{p \mid N} \Phi_{\chi,p} \]
is \( l \)-integral. In view of (24), these observations yield

**Proposition 7.** Let \( j \in \mathbb{Z} \) be prime to \( N \). For a prime number \( l, l \nmid N \), let \( \lambda_{j} \) be the exponent defined in (28). Then
\( \lambda_j \leq v_l(\varphi(N)/2) + \max \left\{ v_l(h_{\chi}) + \sum_{\substack{p | N \ni f_{\chi} \\
p | N}} v_l(\Phi_{\chi,p}) : \chi \in C' \right\}. \)

Accordingly, \( l \) occurs in the denominator of \( b_j \) only if it belongs to one of the following three types:

(A) \( l \) is a divisor of \( \varphi(N)/2 \);

(B) \( l \) divides \( h' \) (outside of \( N \), to be precise);

(C) there is a character \( \chi \in C' \) and a prime \( p \), \( p | N \), \( p \upharpoonright f_{\chi} \), such that \( l \) divides \( \Phi_{\chi,p} \).

 Remarks. 1. The actual computation of the number \( \Phi_{\chi,p} \) involves the number \( d_{\chi,p} \) (cf. (27)), whose value is not always obvious. In the case \( f_{\chi} = q^e \), \( q \) a prime \( \geq 3 \), however, this value is easy to find: Here the character \( \chi \) has an order of the shape \( d = q^{e-1}m \), where \( m \) divides \( q - 1 \) and \( v_2(m) = v_2(q - 1) \). Let \( \text{ord}(p, q^e) \) denote the order of \( p \) mod \( q^e \). Then

\[
\frac{d}{(d, \varphi(q^e)/\text{ord}(p, q^e))},
\]

which is sufficiently explicit.

2. Of course, the upper bound (29) looks much simpler in the cases where the weight factors do not occur. E.g., if \( N = p \) is a prime or \( N = N_2 \) is powerful, then

\[
\lambda_j \leq v_l(\varphi(N)/2) + \max\{v_l(h_{\chi}) : \chi \in C'\}. \tag{30}
\]

This formula shows that it is desirable to have a survey of the values \( h_{\chi}, \chi \in C' \). Not every table of \( h_N \) gives this additional information (cf. [20], p. 352 ff.; cf., however, the tables quoted there). In this case one may work with weaker bounds like

\[
v_l(h') (\geq \max\{v_l(h_{\chi}) : \chi \in C'\}). \tag{31}
\]

In the case of a prime power \( N = p^e \geq 3, l \upharpoonright 2p \), (31) gives (cf. (25))

\[
\lambda_j \leq v_l(\varphi(N)) + v_l(h).
\]

3. The right side of (29) often takes the value 1 if the prime \( l \) is large (say \( l > N \)). This is due to the following fact: On the one hand, \( l \) does not belong to both types (B) and (C) in general; on the other hand, \( v_l(h') \) equals 1 in most cases if \( l \) is of type (B), whereas all values \( v_l(\Phi_{\chi,p}) \) are 0 except one, which is equal to 1, if \( l \) is of type (C). The next proposition, however, shows that primes of type (B) or (C) play a role in the denominator of at least one number \( b_j, j \in \mathcal{R} \).

**Proposition 8.** Let \( l \) be a prime not dividing \( N \). If \( l \) belongs to one of the above types (B), (C), then there is an index \( j \in \mathcal{R} \) such that \( \lambda_j \geq 1 \).
Proof. Using (8) and the orthogonality relation
\[ \sum_{(j,N)=1} \overline{\chi(j)} \chi(j) = \begin{cases} \varphi(N) & \text{if } \chi = \chi', \\ 0 & \text{otherwise}, \end{cases} \]
one verifies
\[ \sum_{j \in \mathcal{R}} \chi(j)b_j = -w_{\chi}/B_{\chi} \quad (32) \]
for each \( \chi \in \mathcal{X}^\sim \). Fix \( \chi \in \mathcal{C}' \) and suppose that \( v_l(b_j) \geq 0 \) for all \( j \in \mathcal{R} \). By (32), the number \( w_{\chi}/B_{\chi} \) is \( l \)-integral, so \( v_l(N_{\chi}(w_{\chi})/h_{\chi}) \geq 0 \). But (26) implies \( v_l(N_{\chi}(w_{\chi})) \leq 0 \); and since \( h_{\chi} \) is \( l \)-integral, \( v_l(1/h_{\chi}) \leq 0 \). Therefore, \( l \) cannot be of type (B) or of type (C).

Examples. 1. Take \( l = 2 \), so \( l \nmid N \) means \( N \) is odd. Let \( \chi \in \mathcal{C}' \) be a character with \( f_{\chi} = N \). Then \( h_{\chi} \) is even unless \( N = p^e \) for a Fermat prime \( p \) (cf. [11], pp. 82, 93). Accordingly, the prime 2 must occur in the denominator of some number \( b_j(N) \) whenever \( N \) does not have this particular shape (cf. Tables 1, 2).

2. Let \( N = p = 41 \), \( h_p^- = 121 = 11^2 \), so \( l = 11 \) (\( l \nmid N \)) is of type (B). In fact, \( b_2 = b_3 = 1/22 \), i.e., \( l \) occurs in the denominator of these numbers; however, \( b_1 = b_4 = 0 \).

3. The foregoing example is exceptional in some sense. According to our experience, primes \( l \) occurring in the denominator of one number \( b_j \) show a tendency to occur in the denominators of all \( b_j \)'s (unless they are very small). Consider \( N = 85 = 5 \cdot 17 \). Here \( h_{\sim N} = 85 \cdot 73 \). The primes of type (C) come from two characters \( \chi, \chi' \in \mathcal{C}' \) with respective conductors 5, 17, which produce the numbers \( \Phi_{\chi,17} = \Phi_4(17) = 17^2 + 1 = 2 \cdot 5 \cdot 29 \) and \( \Phi_{\chi',5} = \Phi_{16}(5) = 5^8 + 1 = 2 \cdot 17 \cdot 11489 \). Accordingly, 73, 2, 29 and 11489 must occur in the denominators of some \( b_j \)'s. Indeed, all \( b_j \)'s have the same denominator \( 4 \cdot 29 \cdot 11489 \cdot h_{\sim N} \). Other examples with the same common denominator for all \( b_j \)'s are \( N = 51, 57, 69 \) (cf. Table 1).

Table 1 gives an impression of the primes of type (C). For this purpose, the table contains only moduli \( N \) which are neither primes nor powerful numbers (otherwise type (C) is impossible). We have also ruled out all moduli \( N \equiv 2 \) mod 4, which are not so interesting (cf. Section 5, Proposition 14). With these restrictions, the table covers the range \( 50 \leq N \leq 100 \). The main information is given in the fourth column, namely, the smallest common denominator \( D \) of all numbers \( b_j, (j,N) = 1 \), decomposed into prime factors. The numbers \( \varphi(N) \) and \( h_{\sim N} \) have been included in order to survey the types (A) and (B). Finally, the last column contains the (factorized) value of \( D \cdot b_1 \)—just to give an impression what the numbers \( b_j \) are looking like. The table shows that primes of type (C) may be fairly large.
In view of (24) one expects that primes $l$ of type (A) also occur in the denominators of the numbers $b_j$. This, however, is not true in quite a number of cases. For instance look at $N = 69$, $l = 11$, $N = 87$, $l = 7$, or $N = 99$, $l = 5$, in Table 1. The next proposition gives a partial explanation for this fact: If $N$ is square-free, a prime $l$ of type (A), $l \mid 2N$, cannot occur in the denominator unless it is of type (B) or (C); in the general case the proposition is slightly weaker than this statement.

**Proposition 9.** Let $l$ be a prime, $l \mid 2N$, and let $\lambda_j$, $(j, N) = 1$, be as in (28). Then

$$\lambda_j \leq v_l(h_N^{-}) + \sum_{\chi \in \mathcal{C}} \sum_{p \mid N} v_l(\Phi_{X,p}).$$

**Table 1.** Non-powerful composite moduli $N$

<table>
<thead>
<tr>
<th>$N$</th>
<th>$\varphi(N)$</th>
<th>$h_N^{-}$</th>
<th>$D$</th>
<th>$D \cdot b_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>51</td>
<td>$2^3$</td>
<td>5</td>
<td>$h_N^{-} \cdot 2^2 \cdot 3 \cdot 193$</td>
<td>547</td>
</tr>
<tr>
<td>52</td>
<td>$2^3 \cdot 3$</td>
<td>3</td>
<td>$h_N^{-} \cdot 2^3$</td>
<td>1</td>
</tr>
<tr>
<td>55</td>
<td>$2^3 \cdot 5$</td>
<td>2 \cdot 5</td>
<td>$h_N^{-} \cdot 2 \cdot 71$</td>
<td>-53</td>
</tr>
<tr>
<td>56</td>
<td>$2^3 \cdot 7$</td>
<td>2</td>
<td>$h_N^{-} \cdot 2^4$</td>
<td>1</td>
</tr>
<tr>
<td>57</td>
<td>$2^2 \cdot 3^2$</td>
<td>3^2</td>
<td>$h_N^{-} \cdot 2^3 \cdot 3 \cdot 7 \cdot 37$</td>
<td>-113</td>
</tr>
<tr>
<td>60</td>
<td>$2^4$</td>
<td>1</td>
<td>$2^6$</td>
<td>1</td>
</tr>
<tr>
<td>63</td>
<td>$2^2 \cdot 3^2$</td>
<td>7</td>
<td>$h_N^{-} \cdot 2 \cdot 3 \cdot 19$</td>
<td>17</td>
</tr>
<tr>
<td>65</td>
<td>$2^4 \cdot 3$</td>
<td>$2^6$</td>
<td>$2^3 \cdot 13 \cdot 17$</td>
<td>-3^3</td>
</tr>
<tr>
<td>68</td>
<td>$2^5$</td>
<td>$2^3$</td>
<td>$h_N^{-} \cdot 2^4$</td>
<td>-3</td>
</tr>
<tr>
<td>69</td>
<td>$2^5 \cdot 11$</td>
<td>3 \cdot 23</td>
<td>$h_N^{-} \cdot 2^4 \cdot 3851$</td>
<td>96001</td>
</tr>
<tr>
<td>75</td>
<td>$2^3 \cdot 5$</td>
<td>11</td>
<td>$h_N^{-} \cdot 2 \cdot 5 \cdot 1181$</td>
<td>2339</td>
</tr>
<tr>
<td>76</td>
<td>$2^3 \cdot 3^2$</td>
<td>19</td>
<td>$h_N^{-} \cdot 2^2 \cdot 5$</td>
<td>2 \cdot 3</td>
</tr>
<tr>
<td>77</td>
<td>$2^2 \cdot 3^2$</td>
<td>$19 \cdot 5^2 \cdot 19 \cdot 191$</td>
<td>$-7 \cdot 29 \cdot 229$</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>$2^5$</td>
<td>5</td>
<td>$h_N^{-} \cdot 2^2 \cdot 13$</td>
<td>-2 \cdot 3</td>
</tr>
<tr>
<td>84</td>
<td>$2^3 \cdot 3$</td>
<td>1</td>
<td>$2^6 \cdot 7$</td>
<td>-3 \cdot 5</td>
</tr>
<tr>
<td>85</td>
<td>$2^5 \cdot 5$</td>
<td>$5 \cdot 17 \cdot 73$</td>
<td>$h_N^{-} \cdot 2^2 \cdot 29 \cdot 11489$</td>
<td>3 \cdot 113 \cdot 430543</td>
</tr>
<tr>
<td>87</td>
<td>$2^3 \cdot 7$</td>
<td>$2^9 \cdot 3$</td>
<td>$2^4 \cdot 3 \cdot 5 \cdot 16493$</td>
<td>$-2^2 \cdot 7 \cdot 2971$</td>
</tr>
<tr>
<td>88</td>
<td>$2^3 \cdot 5$</td>
<td>$5 \cdot 11$</td>
<td>$h_N^{-} \cdot 2^2 \cdot 5$</td>
<td>3 \cdot 19</td>
</tr>
<tr>
<td>91</td>
<td>$2^3 \cdot 3^2$</td>
<td>$2^4 \cdot 7 \cdot 13 \cdot 37$</td>
<td>$h_N^{-} \cdot 5^2 \cdot 181$</td>
<td>3 \cdot 2480663</td>
</tr>
<tr>
<td>92</td>
<td>$2^2 \cdot 11$</td>
<td>3 \cdot 87</td>
<td>$h_N^{-} \cdot 2^3$</td>
<td>-13</td>
</tr>
<tr>
<td>93</td>
<td>$2^2 \cdot 3 \cdot 5$</td>
<td>$3^2 \cdot 5 \cdot 151$</td>
<td>$h_N^{-} \cdot 2^3 \cdot 5 \cdot 7 \cdot 61 \cdot 271$</td>
<td>241 \cdot 953 \cdot 1021</td>
</tr>
<tr>
<td>95</td>
<td>$2^3 \cdot 3^2$</td>
<td>$2^2 \cdot 13 \cdot 19 \cdot 109$</td>
<td>$h_N^{-} \cdot 2^3 \cdot 5 \cdot 31 \cdot 829$</td>
<td>3 \cdot 62656691</td>
</tr>
<tr>
<td>96</td>
<td>$2^5$</td>
<td>$3^2$</td>
<td>$2^2 \cdot 3 \cdot 41$</td>
<td>7</td>
</tr>
<tr>
<td>99</td>
<td>$2^2 \cdot 3 \cdot 5$</td>
<td>$3 \cdot 31^2$</td>
<td>$2 \cdot 3 \cdot 31 \cdot 37$</td>
<td>29</td>
</tr>
</tbody>
</table>
In particular, $l$ does not occur in the denominator of any number $b_j(N)$ if $l$ is of type (A) but prime to $h_\overline{N}$ and to all numbers $\Phi_{\chi,p}$ occurring on the right side of (33).

**Proof.** By (21), $b_j = \sum_{k \in \mathcal{R}} \hat{c}_k s_{(kj)}^*$. The numbers $s_{(kj)}^*$ occurring in this identity are algebraic integers. Hence it suffices to show that each inverse cotangent number $\hat{c}_k$, $k \in \mathcal{R}$, can be written as

$$\hat{c}_k = \frac{\alpha_k}{(2N)^r \cdot h_\overline{N} \cdot \prod_{\chi,p} \Phi_{\chi,p}}$$

for some algebraic integer $\alpha_k$ (the product runs over all characters $\chi$ and primes $p$ occurring on the right side of (33)). Since $\hat{c}_k$ is an entry of the inverse of the cotangent matrix $C = (c_{mn^*})_{m,n \in \mathcal{R}}$, the number $\det C \cdot \hat{c}_k$ is a polynomial in the $c_m$’s with integral coefficients. The identity $c_m = (1 + \zeta_N^m)/(1 - \zeta_N^m)$ shows that $N \cdot c_m$ is an algebraic integer. Finally, $\det C$ equals $h_\overline{N} \cdot \prod_{\chi,p} \Phi_{\chi,p}$ outside of $2N$—this follows from Theorem 4.3 of [18] but can also be deduced from Proposition 3 and formulas (22), (23) above. 

Under certain conditions the bound (29) for the exponent $\lambda_j$ can be refined, as the next proposition shows. We shall use the notation $[c]$ for the integer part of a real number $c$. Further, it is clear that the maximum $m$ occurring in this proposition can be replaced by larger numbers that are easier to obtain (cf. (31)).

**Proposition 10.** Let $p \geq 3$ be a prime number, $N = p^e$ and $\kappa = v_2(p - 1)$. Let $l \geq 3$, $l \neq p$, be another prime and

$$m = \max\{v_l(h_\chi) : \chi \in \mathcal{C}'\}.$$

Then the numbers $\lambda_j$, $(j, N) = 1$, of (28) satisfy

$$\lambda_j \leq v_l(\varphi(N)) + \lceil m/\text{ord}(l, 2^\kappa p^{e-1}) \rceil. \tag{34}$$

**Proof.** Let $\chi \in \mathcal{X}'$ be arbitrary, $d = \text{ord}(\chi)$, and consider a prime ideal $l$ of $\mathbb{Q}(\chi)$ lying above $l$. By $v_l$ we denote the corresponding valuation of $\mathbb{Q}(\chi)$ and by $f_l$ the residue class degree of $l$ in $\mathbb{Q}(\chi)$. First note that

$$f_l \geq \text{ord}(l, 2^\kappa p^{e-1}).$$

In order to see this, observe that $v_2(d) = \kappa$ and $v_p(d) = e - 1$ ($\chi$ is odd and $f_\chi = N$). Since $\mathbb{Q}(\chi)$ is the $d$th cyclotomic field, $f_l$ is the order of $l$ modulo $d/l^{v_l(d)}$, which is clearly $\geq \text{ord}(l, 2^\kappa p^{e-1})$. Now $h_\chi = N_\chi(B_\chi)$, so

$$v_l(h_\chi) \geq v_l(B_\chi) \cdot f_l.$$

This gives $v_l(B_\chi) \leq n$ for $n = \lceil m/\text{ord}(l, 2^\kappa p^{e-1}) \rceil$ and shows that $l^n/B_\chi$ is $l$-integral. 

Proposition 10 remains valid—with some minor changes—in the case $N = 2^c$ and $l \geq 3$. Without loss of generality one may assume $N \geq 8$, the
only relevant value for \( N = 4 \) being \( b_1 = 2 \). Then \( \mathcal{C}' \) consists of a unique character \( \chi \) of order \( N/4 \); so \( m \) boils down to \( m = v_l(h') = v_l(\hat{h}) \), and \( 2^\kappa \) must be replaced by \( N/4 \). Finally, (34) reads
\[
\lambda_j \leq \lfloor m / \text{ord}(l, N/4) \rfloor.
\]
We shall illustrate the meaning of last two propositions with the following examples.

**Examples.** 1. As above, consider \( N = p = 41 \), \( h' = 11^2 \), \( l = 11 \), so \( v_l(h') = 2 \). Hence Proposition 9 gives \( \lambda_j \leq 2 \), an estimate which is not sharp. On the other hand, replace the number \( m \) of Proposition 10 by the (possibly larger) value \( v_l(h') = 2 \) and observe that \( \text{ord}(11, 2^\kappa) = 2 \); then (34) gives \( \lambda_j \leq 1 \), which is sharp since \( \lambda_2 = \lambda_3 = 1 \).

2. Put \( N = p = 71 \) and \( l = 7 \), so \( v_l(h') = 2 \) (cf. Table 2). Here \( \kappa = 1 \) and, accordingly, \( \text{ord}(l, 2^\kappa) = 1 \), which means that Proposition 10 does not really improve the estimate (30). However, there are two characters \( \chi \in \mathcal{C}' \) (of respective orders 2 and 14) such that \( v_l(h_\chi) = 1 \), so \( m = 1 \). Therefore, (30) gives the sharp bound \( \lambda_j \leq 2 \). On the other hand, Proposition 9 yields the same bound.

We turn to the case \( l \mid 2N \). The treatment of primes \( l \) of this kind leads to quite a number of subcases, even if \( N = p^\kappa \); the whole reasoning resembles that of [11], Chapter III. In view of this, we confine ourselves to the following proposition, which is not best possible and whose proof is omitted:

**Proposition 11.** Let \( N = p^\kappa \geq 3 \) be a prime power and \( \hat{h} = h_N h_{N/p}^{-1} \) as in (25). For \( l \in \{2, p\} \) and any \( j \), \( (j, N) = 1 \),
\[
\lambda_j \leq v_l(\varphi(N)) + v_l(\hat{h}).
\]

Without going into details we note that Iwasawa theory (cf. [20], p. 127 ff.) yields, for a fixed prime \( l = p \geq 3 \) and all sufficiently large moduli \( N = p^\kappa \), the bound \( \lambda_j \leq \kappa \). We conclude this section with an immediate (but more comprehensive) consequence of the foregoing propositions.

**Theorem 4.** Let \( N = p^\kappa \geq 3 \) be a prime power and \( \kappa = v_2(p - 1) \) (so \( \kappa = 0 \) for \( p = 2 \)). Suppose that \( h_N^- \) and \( \varphi(N) \) are relatively prime. Then the denominator of \( 2^\kappa p^{\kappa-1}b_j \) is a divisor of \( \hat{h} = h_N^- / h_{N/p}^- \).

**4. A congruence for the numbers \( b_j(N) \).** The main goal of this section is a congruence for the numbers \( b_j = b_j(N) \) in the case of a prime power \( N = p^\kappa \). This congruence shows that certain (large) primes \( l \) of the above type (B) actually occur in the denominators of all numbers \( b_j, (j, N) = 1 \). Moreover, it shows that the numerator of \( b_j \) is subject to strong restrictions such as Theorem 3, restrictions which are both of theoretical interest and useful for the practical computation of the numbers \( b_j \). If \( N \) is a composite
number, the congruence holds for the “weight-factor-free” part of \( b_j(N) \), which we introduce now. Let \( N \geq 3 \) be arbitrary and put
\[
\tilde{\mathcal{X}} = \{ \chi \in \mathcal{X}^- : f_\chi = N \}, \quad \tilde{\mathcal{C}} = \tilde{\mathcal{X}} \cap \mathcal{C}, \quad \tilde{h} = \prod_{\chi \in \tilde{\mathcal{C}}} h_\chi.
\]
If one restricts the sum on the right side of (24) to characters \( \chi \in \tilde{\mathcal{X}} \), one obtains
\[
\tilde{b}_j = \tilde{b}_j(N) = \frac{-2}{\varphi(N)} \sum_{\chi \in \tilde{\mathcal{X}}} \chi(j); \tag{35}
\]
indeed, \( w_\chi = 1 \) whenever \( f_\chi = N \) (cf. (7)). Of course, \( \tilde{b}_j = b_j \) if \( N \) is a prime or a powerful number (e.g., a prime power \( N = p^e \)). In Section 5 we shall see how \( \tilde{b}_j \) can be used for computing the numbers \( b_j \) in the non-powerful composite case.

In most examples known to the author the square of a large prime divisor \( l \) of \( h_N^- \) does not divide \( h_N^- \); so one expects \( v_l(h_N^-) = 1 \) for these primes. Keeping this in mind we make the following assumption for the time being:
\[
v_l(h) = 1 \quad \text{and}, \quad l \nmid N \cdot \varphi(N) \quad (\text{thus}, \quad l \geq 2 \text{ because of } N \geq 3).
\]
Since \( v_l(h_\chi) \geq 0 \) for all \( \chi \in \tilde{\mathcal{C}} \), there is exactly one character in \( \tilde{\mathcal{C}} \), say \( \psi \), with \( v_l(h_\psi) = 1 \), whereas \( v_l(h_{\psi'}) = 0 \) for all \( \psi' \in \tilde{\mathcal{C}}, \psi' \neq \psi \). If \( \psi' \) is of this kind, \( 1/B_\chi \) is \( l \)-integral for each \( \chi \in [\psi'] \): In fact, we have seen above that \( h_{\psi''}/B_\chi \) is \( l \)-integral; however, since \( v_l(h_{\psi''}) = 0 \) this means that \( 1/B_\chi \) itself is \( l \)-integral. Consequently,
\[
\tilde{b}_j = \tilde{b}_j(N) = \frac{-2}{\varphi(N)} \sum_{\chi \in [\psi]} \chi(j)^{-1} B_\chi + a_j \tag{36}
\]
for an \( l \)-integral number \( a_j \). Let \( d \) denote the order of \( \psi \). Recall that \( v_l(h_\psi) \) must be a multiple of the residue class degree \( f_l \) of \( l \) in \( \mathbb{Q}(\psi) \); therefore, \( f_l = 1 \), because we know \( v_l(h_\psi) = 1 \). Moreover, our assumption \( l \nmid \varphi(N) \) implies that \( l \) is unramified in \( \mathbb{Q}(\psi) \). Together with \( f_l = 1 \) this observation yields \( l \equiv 1 \mod d \).

Next we go over to the \( l \)-adic number field \( \mathbb{Q}_l \) (i.e., the \( l \)-adic completion of \( \mathbb{Q} \)). The valuation \( v_l \) of \( \mathbb{Q} \) extends to this field in the usual way. Consider the algebraic closure \( \overline{\mathbb{Q}_l} \) of \( \mathbb{Q}_l \). Since \( \overline{\mathbb{Q}} \) contains the algebraic closure \( \overline{\mathbb{Q}} \) of \( \mathbb{Q} \), we may assume \( \overline{\mathbb{Q}_l} \) contains \( \mathbb{Q}(\psi) \). The values \( \neq 0 \) of \( \psi \), however, are \((l-1)\)th roots of unity (because of \( d \mid (l-1) \)), which lie in the field \( \mathbb{Q}_l \) already. So this field contains the values \( \chi(j), (j,N) = 1, \) of all characters \( \chi \in [\psi] \) and the corresponding Bernoulli numbers \( B_\chi \). Hence the number \( a_j \) on the right side of (36) is an \( l \)-integral algebraic number lying in \( \mathbb{Q}_l \); in particular, \( a_j \) lies in the ring \( \mathbb{Z}_l = \{ a \in \mathbb{Q}_l : v_l(a) \geq 0 \} \) of \( l \)-adic integers. From \( h_\psi = \prod_{\chi \in [\psi]} B_\chi \) and \( v_l(B_\chi) \geq 0, \chi \in [\psi] \), we conclude that there
must be exactly one character \( \chi \in [\psi] \) with \( v_l(B_\chi) = 1 \), whereas \( v_l(B_{\chi'}) = 0 \) for all \( \chi' \in [\psi], \chi' \neq \chi \). Therefore, \( 1/B_{\chi'} \) is in \( \mathbb{Z}_l \) for these characters \( \chi' \).

Altogether, we obtain

\textbf{Proposition 12.} Let \( N \geq 3 \) and \( l \) be a prime, \( l \nmid N \cdot \varphi(N) \). Suppose that \( v_l(h) = 1 \). Then there is exactly one \( \psi \in \overline{C} \) such that \( l \mid h_\psi \). The order \( d \) of this character divides \( l - 1 \), which means that the numbers \( \chi(j)^{-1}/B_\chi \), \( \chi \in [\psi] \), can be considered as numbers in \( \mathbb{Q}_l \). There is a uniquely determined \( \chi \in [\psi] \) with \( v_l(B_\chi) = 1 \); and for this specific \( \chi \),

\[
(37) \quad \tilde{b}_j \equiv \frac{-2\chi(j)^{-1}}{\varphi(N)B_\chi} \mod \mathbb{Z}_l
\]

for all \( j, (j, N) = 1 \). In particular, \( v_l(\tilde{b}_j) = -1 \).

In what follows the uniquely determined character \( \chi \) of Proposition 12 will be called the \( l \)-character. The following corollary to this proposition often implies that the numbers \( b_j, 1 \leq j \leq \bar{N}, (j, N) = 1 \), are all distinct:

\textbf{Proposition 13.} In the setting of Proposition 12, let \( d \) be the order of \( \psi \). The numbers \( \tilde{b}_j, (j, N) = 1 \), belong to exactly \( d \) different residue classes \( \mod \mathbb{Z}_l \).

\textbf{Proof.} Let \( \chi \in [\psi] \) be the \( l \)-character. What we have to prove is equivalent to the following statement: The character values \( \chi(j)^{-1}, (j, N) = 1 \), belong to exactly \( d \) different residue classes \( \mod l\mathbb{Z}_l \). Since \( \text{ord}(\chi^{-1}) = \text{ord}(\psi) = d \), the range of \( \chi(j)^{-1} \) coincides with the set of \( d \)-th roots of unity in \( \mathbb{Z}_l \), whose cardinality is \( d \). However, any two distinct \( d \)-th roots of unity in \( \mathbb{Z}_l \) remain distinct \( \mod l\mathbb{Z}_l \). ✷

Proposition 12 can be extended to certain prime divisors \( l \) of \( N \), but we confine ourselves to the most important case \( N = p = l \geq 3 \). Since \( \mathbb{Q}_p \) contains all \( (p-1) \)-th roots of unity in \( \overline{\mathbb{Q}} \), all characters \( \chi \in \mathcal{X}^- \) have values in \( \mathbb{Z}_p \). Let \( \omega \in \mathcal{X}^- \) denote the \textit{Teichmuller} character, which is defined by \( \omega(j) \equiv j \mod p\mathbb{Z}_p \). Then \( \tilde{\mathcal{X}} = \mathcal{X}^- = \{ \omega^k : 1 \leq k \leq p-2, k \text{ odd} \} \). By [20], p. 61,

\[
\pm 2^{p-3}/2h_p^- = p \prod_{1 \leq k \leq p-1 \atop k \text{ odd}} B_{\omega^k}.
\]

We note that \( v_p(B_{\omega^k}) \geq 0 \) for all relevant exponents \( k < p - 2 \), whereas \( v_p(p \cdot B_{\omega^{p-2}}) = 0 \) (ibid.). Therefore, if \( v_p(h_p^-) = 1 \), then there is a unique (odd) exponent \( k, 1 \leq k \leq p - 4 \), with \( v_p(B_{\omega^k}) = 1 \). The arguments used above now yield, for this specific \( k \), the following analogue of (37):

\[
(38) \quad b_j \equiv \frac{-2 \cdot \omega^{-k}(j)}{(p - 1)B_{\omega^k}} \mod \mathbb{Z}_p.
\]

In particular, \( v_p(b_j) = -1 \).
Remark. The congruence (38) can easily be extended to the case when \( v_p(B_{\omega^k}) \leq 1 \) for all odd exponents \( k, 1 \leq k \leq p-4 \). According to [3], this is true for all irregular primes \( p < 4 \cdot 10^6 \). Here we have

\[
b_j \equiv \frac{-2}{p-1} \sum_k \omega^{-k}(j)/B_{\omega^k} \mod \mathbb{Z}_p,
\]

the sum being taken over those (few) \( k \) with \( v_p(B_{\omega^k}) = 1 \). However, we cannot (easily) deduce \( v_p(b_j) = -1 \) from this congruence as soon as the index of irregularity of \( p \) is \( \geq 2 \).

For practical purposes it is useful to transform the congruences (37), (38) into congruences of integers, i.e., instead of working with \( \mathbb{Q}/\mathbb{Z} \) one works with the ring \( \mathbb{Z}/l\mathbb{Z} \). We discuss this transformation in the case \( N = p^e, p \geq 3 \), where \( \tilde{b}_j = b_j \) for all \( j \), \( (j, N) = 1 \) and \( \tilde{h} = h' \). Our discussion will also show how to find the \( l \)-character \( \chi \) in practice. In accordance with Proposition 12, we assume \( l \nmid p(p-1) \) and \( v_l(\tilde{h}) = v_l(h) = 1 \) (cf. (25)). We adopt the usual conventions for congruences: for instance, if \( a, b, c \) and \( m \) are integers with \( (c, m) = 1 \), we sometimes write

\[
 b \equiv a/c \mod m;
\]

so \( 1/c \) stands for the inverse of \( c \mod m \) here. Our goal is a congruence of the shape

\[
lb_j \equiv a/c \mod l,
\]

the integers \( a, c \) on the right side being both prime to \( l \).

Suppose we have taken our prime \( l \) with \( v_l(\tilde{h}) = 1 \) from a table of relative class numbers. It does not mean much extra work if we do not know the order \( d \) of the \( l \)-character \( \chi \) a priori. In fact, since the group \( (\mathbb{Z}/N\mathbb{Z})^\times \) of prime residues mod \( N \) is cyclic for our \( N \), there is exactly one conjugacy class \( [\psi] \) for every possible order \( d \). These orders are given by \( d = p^{s-1}s, s \mid (p-1), v_2(s) = v_2(p-1), \) and they fulfil \( d \mid (l-1) \). We start with \( s = p-1 \). Let \( g \) denote a primitive root mod \( N \) and \( w \in \mathbb{Z} \setminus l\mathbb{Z} \) an integer with

\[
 \text{ord}(w, l) = d.
\]

Then the congruence

\[
(39) \quad \psi(g) \equiv w \mod l\mathbb{Z}_l
\]

determines an \((l\text{-adic})\) Dirichlet character \( \psi : \mathbb{Z} \rightarrow \mathbb{Z}_l \) of order \( d \). This \( \psi \) can also be characterized by the infinite system

\[
(40) \quad \psi(g) \equiv w^{m-1} \mod l^m \mathbb{Z}_l, \quad m \geq 1,
\]

of congruences. The characters \( \chi \in [\psi] \) have the shape \( \chi = \psi^k, 1 \leq k \leq d, (k, d) = 1 \). For an integer \( m \), let \( (m)_N \) denote the uniquely determined number in \( \{0, 1, \ldots, N-1\} \) which is \( \equiv m \mod N \). We use this notation to
write $B_\chi$ in the form

$$B_\chi = \frac{1}{N} \varphi(N)^{-1} \sum_{m=0}^{\varphi(N)} (g^m)_N \chi(g^m)$$

(observe that $f_\chi = N$ for each $\chi \in [\psi]$). Together with (39) and the notation $\chi = \psi^k$, this identity gives

$$B_\chi \equiv \frac{1}{N} \varphi(N)^{-1} \sum_{m=0}^{\varphi(N)} (g^m)_N w^{mk} \mod l\mathbb{Z}_l. \quad (41)$$

Accordingly, one has to check whether the sum on the right side of this congruence is divisible by $l$ for some $k$ in the above range. If this is never the case, we must try another possible order $d$. Otherwise, we have found the $l$-character $\chi = \psi^k$. Because of (40), we also have the stronger congruence

$$B_\chi \equiv \frac{1}{N} \varphi(N)^{-1} \sum_{m=0}^{\varphi(N)} (g^m)_N w^{lmk} \mod l^2\mathbb{Z}_l. \quad (42)$$

Since $\chi$ is the $l$-character, the sum on the right side of (42) is divisible by $l$ but not by $l^2$. On dividing both sides of (42) by $l$ we obtain an integer $c$, $l \nmid c$, such that

$$B_\chi / l \equiv c \mod l\mathbb{Z}_l. \quad (43)$$

The knowledge of $c$ is the main point. In fact, (37) now yields

$$lb_{g^m} \equiv \frac{-2w^{-mk}}{\varphi(N)c} \mod l,$$

for $m = 0, 1, \ldots, \varphi(N) - 1$.

**Example.** Consider $N = p = 53$, for which $h_p^p = 4889$ is a prime. Put $l = h_p$. Here $d = 52 = p - 1$ works. If one chooses $g = 2$ as a primitive root mod $p$, the $l$-character $\chi$ is given by $\chi(g) \equiv 3637 \mod l\mathbb{Z}_l$ and the above number $c$ satisfies $c \equiv 1674 \mod l$. This gives the following congruences for the integers $2lb_j$ when $j$ runs through the powers of $g$ mod $p$: $2lb_1 \equiv 82$, $2lb_2 \equiv 5$, $2lb_4 \equiv -1371$, $2lb_8 \equiv 453$, $\ldots \mod l$. These congruences suffice for the actual computation of $b_j$, as one may guess from their numerical values $b_1 = 41/l$, $b_2 = 5/(2l)$, $b_4 = -1371/(2l)$, $\ldots$. Because of $d = p - 1$, the numbers $b_j$, $1 \leq j \leq p - 1$, run through $p - 1$ distinct residue classes mod $\mathbb{Z}_l$, which requires that they are all distinct.

In the case of the congruence (38) one can proceed in a similar way: Let $N = p = l \geq 3$ and suppose $v_p(h_p^p) = 1$ (so the prime $p$ is irregular with index of irregularity = 1). There are two new features here: Because of $p \mid N$, the congruences (41) and (42) must be replaced by “higher” congruences, namely, the respective congruences mod $p^2$ and $p^3$. On the other hand, $w
can be chosen equal to $g$. Accordingly,

$$pB_{\omega^k} = \sum_{m=0}^{p-2} (g^m)p^2m \mod p^3\mathbb{Z}_p,$$

which gives the desired congruence of $B_{\omega^k}/p \mod p\mathbb{Z}_p$, $1 \leq k \leq p-4$, $k$ odd. Further, one may profit from the fact that irregular primes have been investigated extensively. For example, the crucial exponent $k$ (in the sense of (38)) is contained in tables like [20], p. 350. In this way one finds $k = 31, 43, 57$ in the respective cases $p = 37, 59, 67$.

We are now in a position to prove Theorems 1 and 3 of the introduction. They are contained in

**Theorem 5.** Let $N = p^e \geq 3$ be a prime power (so $\hat{h} = h_N^*/h_{N/p}^*$ as usual). Put $\kappa = v_2(p-1)$. Suppose that $h_N^*$ is square-free and prime to $\varphi(N)$. Then for all $j$, $(j, N) = 1$,

$$2^\kappa p^{e-1}b_j = n_j\hat{h}$$

with $n_j \in \mathbb{Z}$, $(n_j, \hat{h}) = 1$. Let $g$ denote a primitive root mod $N$ if $p \geq 3$ and take $g = 5$ for $p = 2$. Then there is a number $\gamma \in \mathbb{Z}$, $(\gamma, \hat{h}) = 1$, such that

$$n_\gamma g^m \equiv n_1\gamma^m \mod \hat{h}$$

for all $m \in \mathbb{Z}$.

**Proof.** By Theorem 4, $2^\kappa p^{e-1}b_j = n_j\hat{h}$ for some integer $n_j$. Let $l$ be a prime, $l \mid \hat{h}$, so $v_l(\hat{h}) = 1$. First suppose $l = p$. Since $\hat{h}$ is an odd number if $p = 2$ (cf. [11], p. 101), $l = p$ must be $\geq 3$. Now $(\hat{h}, \varphi(N)) = 1$ implies $e = 1$, i.e., $N = p = 1$. By the above, we have $v_p(b_j) = -1$, so $p \nmid n_j$. If $l \neq p$, the same condition $(\hat{h}, \varphi(N)) = 1$ shows $l \nmid \varphi(N)$ and Proposition 12 yields $l \nmid n_j$. Altogether, we have $(n_j, \hat{h}) = 1$. With the aid of the Chinese Remainder Theorem, the congruences of type (43) for the various primes $l$ dividing $\hat{h}$ can be rephrased as a unique congruence mod $\hat{h}$ of the desired shape.

5. **Computation of the numbers** $b_j(N)$. As above, let $N \geq 3$ and $\mathcal{R} = \{j : 1 \leq j \leq N/2, (j, N) = 1\}$. In this section we discuss the actual computation of the numbers $b_j = b_j(N)$, $j \in \mathcal{R}$, in the range $N \leq 250$. The author has computed these numbers for all $N \leq 100$ and for some other moduli (among them all primes $p \leq 200$, and some prime powers like $N = 125 = 5^3$, $N = 243 = 3^5$). A look at Table 2 shows that the numerators and denominators of the $b_j$’s may be rather large even for these small values of $N$. All of our computations were performed on a personal computer with the assistance of the *Ubasic* package.
Fix $N$ for the time being. Because of the results of Section 3, we may assume that we know a common multiple $d$ of the denominators of the $b_j$’s that is not much larger than the denominators themselves. For instance, if $N = p$ is a prime, Theorem 4 says that $d = 2^s h_p$ is possible, so we only need a table for $h_N$ such as ([20], p. 352 ff.). Now the computation of $b_j$ can be considered as a problem in numerical linear algebra. Indeed, by (20), the matrix $B^T = (b_{jk^*})_{k,j \in \mathcal{R}}$ fulfills $B^T = C^{-1} S$. Therefore, the numerical inversion of the cotangent matrix $C$ yields approximate values for the elements in the first row of $B^T$, i.e., for the numbers $b_j$, $j \in \mathcal{R}$. But then we also know approximations of the numerators

$$n_j = d \cdot b_j,$$

which are integers and can be found in this way, provided that the approximation is good enough.

We consider the case $N = p = 199$. Here $C$ is a $99 \times 99$-matrix, $d = 2 h_p$ has 38 decimal digits and the numerators $n_j$ are of the same order of magnitude. These mere facts show that the memory capacity required is quite big; consequently, this method comes up against limiting factors quickly. In what follows we present better strategies, as we think.

Let us look at the prime number case $N = p$ first. As a rule, we have computed the corresponding numbers $n_j = d \cdot b_j$ in two different ways, namely, by

- numerical approximations that are based on (8),
- the congruences (37), (38).

In the case $N = p$, formula (8) takes the simplified shape (35). According to our experience this formula is fairly harmless from the numerical point of view and does not require complicated operations with complex numbers. For instance, the real parts of the Bernoulli numbers $B_\chi$ can be written, with the notations used in (41), as

$$\frac{1}{p} \sum_{m=0}^{p-2} (g^m)_p \cos \frac{2\pi km}{p-1}$$

($k$ odd, $1 \leq k < p/2$); replacing the cosine by sine yields the corresponding imaginary parts. The storage space required is proportional to $p$ (instead of $p^2$ in the case of the aforementioned numerical inversion of $C$). In most cases we used floating point numbers with 48 digits after the decimal point (*Ubasic*, however, uses more digits for internal computations). In the above case $p = 199$ this yields the integers $n_j$ with an error $< 10^{-7}$ within seconds. For instance,

$$b_1 = -141292545045385217518266818337227437/h_p.$$
This approximation also gives the number
\[ h_p^- = 81 \cdot 19 \cdot 727 \cdot 25645093 \cdot 207293548177 \cdot 3168190412839 \]
with a sufficient degree of precision (so one can dispense with using a table as long as \( p \) remains in the range under consideration).

We checked the correctness of our computations by means of equation (20), which was multiplied by \( d \) for this purpose. In the case \( p = 199 \) the use of 96 digits after the decimal point (in the above sense) shows that this equation holds with an error \( < 10^{-55} \).

The congruences (37), (38), combined with a rather coarse approximation of the numbers \( b_j \) (if any), form a second tool for the computation of \( b_j \). In our situation this tool serves to show that the corresponding floating point computations are correct. We think, however, that the proper value of this instrument lies in its use with considerably larger moduli \( p \), where sufficiently precise numerical approximations are no longer available.

Let \( d' \) be the product of all primes \( l, l \mid (p - 1), v_l(h^-_p) = 1 \), so \( d' \) divides our aforementioned \( d \). Computing the right side of the congruence (43) for each \( l, l \mid d' \) (to be precise: of the analogous congruence in the case \( l = p \)), is rather inexpensive in every respect; and the Chinese Remainder Theorem quickly supplies the congruence class of \( n_j \) mod \( d' \). Suppose, in addition, we know an approximate value \( \beta_j \) of \( b_j \) such that
\[(44) \quad |b_j - \beta_j| < d'/2d.\]
Then \( b_j \) is also known: Determine an integer \( k, k \equiv n_j \mod d' \), such that
\[ |k - d\beta_j| \leq d'/2. \]
One easily checks that \( k \) must be equal to \( n_j \). The precision required by (44) is quite low in general, since the quotient \( d/d' \) is small. In the above example of \( p = 199 \) we have \( d'/2d = 1/324 \). Since the numbers \( b_j \) are all \( < 1 \) here, such a low precision approximation is even possible on the basis of some thousand terms of the slowly converging series (1)—if one wants to use an approximation that is independent of (8). The corresponding entries of Table 2 have also been found by this alternative method. It seems that no approximation whatsoever is needed for primes \( p \geq 47 \) that fall under Theorem 1 (cf. our comment on Theorem 3).

With the necessary adaptations the above methods can be used for higher powers of primes, more generally, for powerful numbers \( N \), since in all of these cases \( b_j = \beta_j \). We have performed computations of this kind up to \( N = 3^5 = 243 \), where \( \hat{h} = 6252002011 \cdot 922099242709 = h_{243}^-/h^-_{81} \). Table 2 covers the numbers \( N \) under consideration for \( N \leq 100 \)—only the (simple) cases when \( h^-_N = 1 \) have been omitted for reasons of space; thus, it covers all primes \( 23 \leq p \leq 97 \) and the moduli \( N = 49, 64, 72, 81 \) and 100. If \( N \) is a
prime power, the table renders the values \( b_1 \) and \( b_g \) for a primitive root \( g \) mod \( N \), with the exception of \( N = 64 \), where \( g = 5 \) instead. This information, eventually combined with a coarse approximation of the remaining numbers \( b_j \), suffices for their actual computation in the spirit of Theorem 5. As in Table 1, \( D \) is the least common multiple of the denominators of the numbers \( b_j \), \( j \in \mathcal{R} \). Except the moduli \( N = 29, 41, 72 \), the number \( h_N^- \) divides the denominator of each \( b_j \), \( j \in \mathcal{R} \).

**Table 2. Primes and powerful moduli \( N \)**

<table>
<thead>
<tr>
<th>( N )</th>
<th>( h_N^- )</th>
<th>( D )</th>
<th>( g )</th>
<th>( D \cdot b_1 )</th>
<th>( D \cdot b_g )</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>3</td>
<td>( 2 \cdot h_N^- )</td>
<td>5</td>
<td>1</td>
<td>−1</td>
</tr>
<tr>
<td>29</td>
<td>( 2^3 )</td>
<td>( h_N^-/2 )</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>( 3^2 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>3</td>
<td>1</td>
<td>−4</td>
</tr>
<tr>
<td>37</td>
<td>37</td>
<td>( 2 \cdot h_N^- )</td>
<td>2</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>41</td>
<td>( 11^2 )</td>
<td>( 2 \cdot h_N^-/11 )</td>
<td>6</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>43</td>
<td>211</td>
<td>( 2 \cdot h_N^- )</td>
<td>3</td>
<td>26</td>
<td>1</td>
</tr>
<tr>
<td>47</td>
<td>5 \cdot 139</td>
<td>( 2 \cdot h_N^- )</td>
<td>5</td>
<td>1</td>
<td>234</td>
</tr>
<tr>
<td>49</td>
<td>43</td>
<td>( 2 \cdot 7 \cdot h_N^- )</td>
<td>3</td>
<td>5</td>
<td>−34</td>
</tr>
<tr>
<td>53</td>
<td>4889</td>
<td>( 2 \cdot h_N^- )</td>
<td>2</td>
<td>82</td>
<td>5</td>
</tr>
<tr>
<td>59</td>
<td>( 3 \cdot 59 \cdot 233 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>2</td>
<td>−875</td>
<td>−7912</td>
</tr>
<tr>
<td>61</td>
<td>( 41 \cdot 1861 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>2</td>
<td>9119</td>
<td>14230</td>
</tr>
<tr>
<td>64</td>
<td>17</td>
<td>( 4 \cdot h_N^- )</td>
<td>5</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>67</td>
<td>67 \cdot 12739</td>
<td>( 2 \cdot h_N^- )</td>
<td>2</td>
<td>29954</td>
<td>11270</td>
</tr>
<tr>
<td>71</td>
<td>( 7^2 \cdot 79241 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>7</td>
<td>114456</td>
<td>−267280</td>
</tr>
<tr>
<td>72</td>
<td>3</td>
<td>( 4 \cdot h_N^- )</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>( 89 \cdot 134353 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>5</td>
<td>998459</td>
<td>−1854465</td>
</tr>
<tr>
<td>79</td>
<td>( 5 \cdot 53 \cdot 377911 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>3</td>
<td>555804</td>
<td>1105246</td>
</tr>
<tr>
<td>81</td>
<td>2593</td>
<td>( 2 \cdot 3 \cdot h_N^- )</td>
<td>2</td>
<td>740</td>
<td>346</td>
</tr>
<tr>
<td>83</td>
<td>( 3 \cdot 279405653 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>2</td>
<td>33610568</td>
<td>−132703937</td>
</tr>
<tr>
<td>89</td>
<td>( 113 \cdot 118401449 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>3</td>
<td>31926605</td>
<td>−132578957</td>
</tr>
<tr>
<td>97</td>
<td>( 577 \cdot 3457 \cdot 206209 )</td>
<td>( 2 \cdot h_N^- )</td>
<td>5</td>
<td>1674823000</td>
<td>54039729138</td>
</tr>
<tr>
<td>100</td>
<td>( 5 \cdot 11 )</td>
<td>( 4 \cdot h_N^- )</td>
<td>7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We now consider the case where \( b_j \) differs from \( \tilde{b}_j \), which is the same as saying that there are non-trivial weight factors. In principle, the numbers \( b_j \) can also be obtained by approximating the right side of (8). Instead, we have used a sort of “step-by-step separation of prime divisors of \( N \)”. This separation is interesting for its own (cf. Proposition 14 below) and allows us to work with the numbers \( \tilde{b}_j \), whose structure is simpler than that of \( b_j \), and the corresponding congruences (37). Since the modulus \( N \) is no more fixed
in what follows, we write $b_j(N), \tilde{b}_j(N)$ instead of $b_j, \tilde{b}_j$. This distinction will also be necessary for the weight factors $w_\chi = w_\chi(N)$.

Let $l$ be a prime, $l \mid N, l^2 \mid N$. We put $N_0 = N/l$, hence $l \nmid N_0$, and write $b_j(N) = x + y$, with

$$x = \frac{-2}{\varphi(N)} \sum_{\chi \in \mathcal{A}, f_\chi | N_0} w_\chi(N) \overline{\chi(j)} B_\chi, \quad y = \frac{-2}{\varphi(N)} \sum_{\chi \in \mathcal{A}, l \nmid f_\chi} w_\chi(N) \overline{\chi(j)} B_\chi$$

(cf. (24)). Next we express the summand $x$ in terms of the numbers $b_k(N_0)$. To this end we write the weight factor $w_\chi(N)$ as follows:

$$w_\chi(N) = \frac{-\overline{\chi_f}(l)}{l - \overline{\chi_f}(l)} w_\chi(N_0).$$

(45)

If $\eta$ is an $r$th root of unity, one has the polynomial identity

$$(Z^r - 1)/(Z - \eta) = \sum_{k=1}^r \eta^{k-1} Z^{r-k}.$$\n
In our situation $\eta$ equals $\chi_f(l)$ and $r = \text{ord}(l, N_0)$, so

$$\frac{\overline{\chi_f}(l)}{l - \overline{\chi_f}(l)} = \frac{1}{l^r - 1} \sum_{k=1}^r \overline{\chi_f(l^k)} l^{r-k}.$$\n
This identity, together with (45), gives

$$x = \frac{-1}{(l - 1)(l^r - 1)} \sum_{k=1}^r l^{r-k} b_{j, l^k}(N_0).$$

The other summand $y$ can be treated more or less in the same way; but we confine ourselves to the following special cases (a), (b), (c), which are the only ones needed for computations with $N \leq 100$ and suffice as an illustration of this technique.

(a) Let $N_0$ be odd, so $N \equiv 2 \mod 4$. Since there is no character $\chi$ with $2 \nmid f_\chi$ but $4 \nmid f_\chi$, the number $y$ vanishes and we obtain

PROPOSITION 14. Let $N \geq 3, N \equiv 2 \mod 4$. Put $r = \text{ord}(2, N/2)$. Then

$$b_j(N) = \frac{-1}{2^r - 1} \sum_{k=1}^r 2^{r-k} b_{j, 2^k}(N/2)$$

for all $j$ with $(j, N) = 1$.

The proposition shows that $b_j(N)$ is an explicit rational linear combination of the numbers $b_k(N/2)$ if $N \equiv 2 \mod 4$. Hence the computation of $b_j(N)$ does not require much extra work if the numbers $b_k(N/2)$ are known. In this way the problem of computing the numbers $b_j(N)$ is reduced to moduli $N \not\equiv 2 \mod 4$.

(b) Let $N_0$ be powerful, for instance, $N_0 = p^e$ with $p \neq l$ and $e \geq 2$. Because $N_0 \mid f_\chi$ for all $\chi \in \mathcal{A}'$, the condition $l \mid f_\chi$ is equivalent to $f_\chi = N$. 


Accordingly, the summand \( y \) equals \( \tilde{b}_j(N) \) and
\[
(46) \quad b_j(N) = \tilde{b}_j(N) - \frac{1}{(l-1)(l^r-1)} \sum_{k=1}^{r} l^{r-k} b_{jk^k}(N/l)
\]
with \( r = \text{ord}(l, N_0) \).

(c) Let \( N_0 = p \) be a prime number, \( p \neq l \). Here \( l \mid f_\chi \) either means \( f_\chi = l \) or \( f_\chi = N \). These cases lead to two new expressions whose sum is equal to \( y \): The first expression is identical with \( \tilde{b}_j(N) \), whereas the other one can be treated like the above sum \( x \), the roles of \( l \) and \( p \) being interchanged. Altogether, we obtain, with \( r = \text{ord}(l, p) \) and \( s = \text{ord}(p, l) \),
\[
(47) \quad b_j(N) = \tilde{b}_j(N) - \frac{1}{(l-1)(l^r-1)} \sum_{k=1}^{r} l^{r-k} b_{jk^k}(p) - \frac{1}{(p-1)(p^s-1)} \sum_{k=1}^{s} p^{s-k} b_{jp^k}(l).
\]

It is rather obvious how to find the number \( b_j(N) \) in the cases (b), (c): Suppose we have already computed all numbers \( b_k(N/l) \) (and, in case (c), also all \( b_k(l) \)'s). Then we compute \( \tilde{b}_j(N) \) by means of approximation, eventually combined with congruences of type (37)—note that it is not difficult, in general, to find a suitable multiple of the denominator of \( \tilde{b}_j(N) \). Now the right sides of (46), (47) are known, which means that we know the exact value of \( b_j(N) \).

**Example.** Consider \( N = 93 = 3 \cdot 31 \). Here \( h_N^- = 6795 = 3^2 \cdot 5 \cdot 151 \) and \( \tilde{d} = 2h_N^-/3 = 4530 \) is a possible common denominator of the numbers \( \tilde{b}_j(N) \). By means of the said numerical approximation or by the suitable congruence mod 151, we find
\[
\tilde{b}_1(N) = -32/\tilde{d}, \quad \tilde{b}_2(N) = -46/\tilde{d}, \quad \ldots, \quad \tilde{b}_7(N) = -23/\tilde{d}, \quad \ldots
\]
Together with (47), these numbers yield the values \( b_j(N) = n_j/D \) with \( D \) as in Table 1. This table shows that the numerators and the denominators of \( b_j(N) \) are much larger than the corresponding items for \( \tilde{b}_j(N) \).

We conclude this paper with a conjecture: There are only finitely many moduli \( N \geq 3 \) such that \( b_j(N) = 0 \) for at least one \( j \), \( (j, N) = 1 \). Without going into details we give a (possibly exhaustive) list of numbers \( N \) of this kind: \( N = 9, 11, 13, 14, 17, 19, 20, 24, 27, 29, 32, 41, 72 \); for \( N = 29 \), e.g., the indices \( j \in \mathcal{R} \) such that \( b_j(29) = 0 \) are \( j = 1, 2, 3, 5, 7, 12 \).

**Acknowledgements.** The author thanks Wolfgang Müller (Graz) for his valuable hints concerning the convergence of the series representing \( 1/L(1, \chi) \).
References

[8] —, An index formula for the relative class number of an abelian number field, J. Number Theory 32 (1989), 100–110.

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

Received on 17.1.2000