ACTA ARITHMETICA
XCVII.2 (2001)

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

$$\lim_{n\to\infty} \sum_{m\leq n}, \tag{2}$$

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 Nth 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 $\kappa = \max\{m : 2^m \mid (p-1)\}$. 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.

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 $h_p^- \le 2p(p/24)^{(p-1)/4}$, cf. [16], p. 441). Let $a_j = b_j - \lfloor b_j \rfloor$ denote the fractional part of the number b_j. On summing up sufficiently many terms of the series (1) we find the number α_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 α_j quickly reveals the exact value a_j: it is the uniquely determined convergent of α_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 $p = 43$, κ equals 1 and $2h_p^- = 422$, thus $d = 3$ is a suitable choice. Taking the sum (1) over all suitable $m \le 84 \cdot 10^6$, one obtains 0.0616080 as a candidate for α_1. The convergents of this number are 0, 1/16, 4/65, 13/211, 82/1331, ...; 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"

$$s_j = s_j(N) = 2i \sin(2\pi j/N) \tag{3}$$

and the "cotangent numbers"

$$c_j = c_j(N) = i \cot(\pi j/N), \tag{4}$$

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

$$s_j = \zeta_N^j - \zeta_N^{-j}, \qquad c_j = (1 + \zeta_N^j)/(1 - \zeta_N^j),$$

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

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

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

$$s_1 = \sum_{j\in\mathcal{R}} b_j c_j. \tag{5}$$

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

$$b_{N-j} = -b_j, \quad b_{j+mN} = b_j, \quad m \in \mathbb{Z}, \tag{6}$$

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_χ we denote the conductor of a $\chi \in \mathcal{X}^-$ and by χ_f the primitive character (mod f_χ) belonging to χ. Moreover,

$$B_\chi = \sum_{k=1}^{f_\chi} k\chi_f(k)/f_\chi$$

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_χ, $\chi \in \mathcal{X}^-$. In view of this we call

$$w_\chi = \frac{\mu(N/f_\chi)\overline{\chi}_f(N/f_\chi)}{(N/f_\chi)\prod_{p|N}(1-\overline{\chi}_f(p)/p)} \tag{7}$$

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

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

$$b_j = \frac{-2}{\varphi(N)} \sum_{\chi \in \mathcal{X}^-} w_\chi \frac{\overline{\chi}(j)}{B_\chi}. \tag{8}$$

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_χ (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_χ 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_χ. 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_p^-. 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* $2^\kappa b_j = n_j/h_p^-$ *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*

$$n_{g^m} \equiv n_1 \gamma^m \bmod h_p^-$$

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

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

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

This gives the congruence

$$n'_{g^m} \equiv n_1' \gamma^m \bmod h_p^-, \tag{9}$$

$m \in \mathbb{Z}$, 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 γ) 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 γ 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 $(j,N)=1$:

$$\sum_{\chi\in\mathcal{X}^-}\chi(j)=\begin{cases}0 & \text{if } j\not\equiv\pm1 \bmod N,\\ \varphi(N)/2 & \text{if } j\equiv 1 \bmod N,\\ -\varphi(N)/2 & \text{if } j\equiv -1 \bmod N.\end{cases} \tag{10}$$

They can be proved in the usual manner (if $j\not\equiv\pm1 \bmod N$, separate an even character ψ with $\psi(j)\neq 1$).

In what follows we assume that the characters in $\mathcal{X}^-$ are ordered in some (arbitrary but) fixed way: $\mathcal{X}^-=\{\chi_1,\dots,\chi_{\varphi(N)/2}\}$. 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 $X\overline{X}^T$, one obtains

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

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))

$$a_{-j}=-a_j,\qquad a_{j+mN}=a_j,\qquad m\in\mathbb{Z}. \tag{11}$$

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

$$d_\chi=\sum_{j\in\mathcal{R}}\overline{\chi}(j)a_j. \tag{12}$$

Now

$$A=X\Delta\overline{X}^T \tag{13}$$

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

$$a_{jk^*}=\frac{2}{\varphi(N)}\sum_{\chi\in\mathcal{X}^-}\chi(jk^*)d_\chi. \tag{14}$$

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

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

where σ_k acts on ζ_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_χ is, essentially, the *Gauss sum*

$$\tau(\chi) = \sum_{k=1}^{N} \chi(k)\zeta_N^k.$$

Indeed, on putting

$$\Gamma = \operatorname{diag}(\tau(\overline{\chi}))_{\chi\in\mathcal{X}^-}$$

we obtain the identity that corresponds to (13), namely,

PROPOSITION 2. *The sine matrix S is normal and satisfies*

$$S = X\Gamma\overline{X}^T.$$

The next number a to be considered is the cotangent number $c_1 = i\cot(\pi/N)$ of (4), which gives rise to the the *cotangent matrix*

$$C = (c_{jk^*})_{j,k\in\mathcal{R}}.$$

Its diagonalization leads to the matrix

$$\Lambda = \frac{iN}{\pi}\cdot\operatorname{diag}(L(1,\overline{\chi}))_{\chi\in\mathcal{X}^-}, \tag{15}$$

which involves the L-series

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

This series is absolutely convergent in the half-plane $\operatorname{Re} s > 1$ and converges in the sense of (2) for $\operatorname{Re} s > 0$.

PROPOSITION 3. *The cotangent matrix C is normal*; *in fact*,

$$C = X\Lambda\overline{X}^T.$$

Proof. Compute $(X\Lambda\overline{X}^T)_{j,k}$ using (14), (15) and the formula

$$\sum_{\substack{m\in\mathbb{Z}\\ m\equiv j \bmod N}} \frac{1}{m} = (\pi/N)\,\cot(\pi j/N).$$

This identity follows from the partial fraction decomposition of the cotangent function; the infinite sum has to be understood in the sense of

$$\lim_{n\to\infty}\sum_{|m|\le n}. \tag{16}$$ ∎

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

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

$$\widehat{c}_j = \widehat{c}_j(N) = \frac{-2i\pi}{N\varphi(N)} \sum_{\chi\in\mathcal{X}^-} \frac{\chi(j)}{L(1,\overline{\chi})}, \tag{17}$$

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

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

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

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

$$L(s,\chi)^{-1} = \sum_{m=1}^{\infty} \mu(m)\chi(m)/m^s. \tag{18}$$

This identity is well known for $\operatorname{Re} s > 1$ but maybe not so widely known in the case $\operatorname{Re} s = 1$. One may argue as follows: As we remarked above, $L(s,\chi)$ does not vanish for $\operatorname{Re} s = 1$, 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 $\operatorname{Re} s = 1$ 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*

$$\widehat{c}_j = \frac{-i\pi}{N} \sum_{\substack{m\in\mathbb{Z}\\ m\equiv j \bmod N}} \frac{\mu(|m|)}{m}, \tag{19}$$

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, $j \in \mathcal{R}$, such that (5) holds, i.e.,

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

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

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

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

$$S = CB^T. \tag{20}$$

Indeed, if one applies automorphisms $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ 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

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

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

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

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

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,

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

The entries $\tau(\overline{\chi})$ of the diagonal matrix Γ can be expressed in terms of the corresponding *primitive* Gauss sums: Put

$$\tau(\chi_f) = \sum_{k=1}^{f_\chi} \chi_f(k) e^{2\pi ik/f_\chi}.$$

By [10], p. 427,

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

This identity has the following analogue for L-series:

$$L(1,\chi) = \prod_{p|N}(1-\chi_f(p)/p)\cdot L(1,\chi_f), \tag{22}$$

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

$$L(1,\overline{\chi}_f) = i\pi\tau(\overline{\chi}_f)B_\chi/f_\chi \tag{23}$$

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

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

where w_χ means the weight factor (7). Then (14) yields the identity (8), i.e., Theorem 2. ∎

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_χ of (12) is essentially the same as the χ-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

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

in this case the elements on the diagonal of Λ 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 $\prod_{\chi\in\mathcal{X}^-} B_\chi$, 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

$$\prod_{\substack{l \text{ prime} \\ v_l(c)<0}} l^{-v_l(c)};$$

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^-) 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 $\mathbb{Q}(\chi)$ denote its field of values, $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(j) : j \in \mathbb{Z})$, and

$$\mathcal{N}_\chi : \mathbb{Q}(\chi) \to \mathbb{Q}$$

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

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

By its definition, B_χ is p-integral for all p not dividing f_χ, therefore h_χ 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^- outside of $2N$.

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

$$N_1 = \prod_{v_p(N)=1} p, \qquad N_2 = \prod_{v_p(N)>1} p^{v_p(N)}.$$

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

$$b_j = \frac{-2}{\varphi(N)} \sum_{\chi\in\mathcal{X}'} w_\chi \frac{\overline{\chi}(j)}{B_\chi}. \tag{24}$$

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

$$\widehat{h} = h_N^-/h_{N/p}^- \tag{25}$$

outside of $2p$. The quotient $\widehat{h}$ is a natural number (cf. [16], p. 474).

Besides the norm factors h_χ we also need the norms of the weight factors w_χ, $\chi \in \mathcal{C}$. By virtue of (7), w_χ can be written as

$$w_\chi = \varepsilon / \prod_{\substack{p|N \\ p \nmid f_\chi}} (p - \overline{\chi}_f(p)) \tag{26}$$

with a certain root ε of unity; so we obtain

$$\mathcal{N}_\chi(w_\chi) = \pm 1 / \prod_{\substack{p|N \\ p \nmid f_\chi}} \mathcal{N}_\chi(p - \overline{\chi}_f(p)).$$

The norms in the denominator of this number are certain values of cyclotomic polynomials. Indeed, let Φ_d denote the dth cyclotomic polynomial. For a prime p dividing N, $p \nmid f_\chi$, put

$$d_{\chi,p} = \operatorname{ord}(\chi_f(p)),$$

i.e., the order of the root of unity $\chi_f(p)$. Then

$$\mathcal{N}_\chi(p - \chi_f(p)) = \Phi_{d_{\chi,p}}(p). \tag{27}$$

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

$$\lambda_j = -v_l(b_j) \tag{28}$$

(which is ≤ 0 if l does not occur in the denominator). First suppose $l \nmid N$. Then h_χ / B_χ is l-integral for any character $\chi \in \mathcal{X}'$. In the same way,

$$w_\chi \prod_{\substack{p|N \\ p \nmid f_\chi}} \Phi_{\chi,p}$$

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 λ_j be the exponent defined in* (28). *Then*

$$\lambda_j \le v_l(\varphi(N)/2) + \max\Big\{v_l(h_\chi) + \sum_{\substack{p\mid N\\ p\nmid f_\chi}} v_l(\Phi_{\chi,p}) : \chi \in \mathcal{C}'\Big\}. \tag{29}$$

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 $\chi \in \mathcal{C}'$ and a prime p, $p \mid N$, $p\nmid f_\chi$, 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 ≥ 3, however, this value is easy to find: Here the character χ 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 $\mathrm{ord}(p, q^e)$ denote the order of p mod q^e. Then

$$d_{\chi,p} = \frac{d}{(d, \varphi(q^e)/\mathrm{ord}(p, q^e))},$$

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

$$\lambda_j \le v_l(\varphi(N)/2) + \max\{v_l(h_\chi) : \chi \in \mathcal{C}'\}. \tag{30}$$

This formula shows that it is desirable to have a survey of the values h_χ, $\chi \in \mathcal{C}'$. 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

$$v_l(h') \ (\ge \max\{v_l(h_\chi) : \chi \in \mathcal{C}'\}). \tag{31}$$

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

$$\lambda_j \le v_l(\varphi(N)) + v_l(\widehat{h}).$$

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 $\lambda_j \ge 1$.*

Proof. Using (8) and the orthogonality relation

$$\sum_{(j,N)=1} \chi\overline{\chi'}(j) = \begin{cases} \varphi(N) & \text{if } \chi = \chi', \\ 0 & \text{otherwise,} \end{cases}$$

one verifies

$$\sum_{j\in\mathcal{R}} \chi(j) b_j = -w_\chi / B_\chi \tag{32}$$

for each $\chi \in \mathcal{X}^-$. 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_χ/B_χ is l-integral, so $v_l(\mathcal{N}_\chi(w_\chi)/h_\chi) \geq 0$. But (26) implies $v_l(\mathcal{N}_\chi(w_\chi)) \leq 0$; and since h_χ 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_χ 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 $l = 11$ ($\nmid N$) 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 $h_N^- = 85 \cdot 73$. 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 $4 \cdot 29 \cdot 11489 \cdot h_N^-$. 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 $N \equiv 2 \bmod 4$, 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_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.

Table 1. Non-powerful composite moduli N

N	$\varphi(N)$	h_N^-	D	$D \cdot b_1$
51	2^5	5	$h_N^- \cdot 2^2 \cdot 3 \cdot 193$	547
52	$2^3 \cdot 3$	3	$h_N^- \cdot 2^2 \cdot 3$	1
55	$2^3 \cdot 5$	$2 \cdot 5$	$h_N^- \cdot 2 \cdot 71$	-53
56	$2^3 \cdot 3$	2	$h_N^- \cdot 2^4$	1
57	$2^2 \cdot 3^2$	3^2	$h_N^- \cdot 2^3 \cdot 3 \cdot 7 \cdot 37$	-113
60	2^4	1	2^6	1
63	$2^2 \cdot 3^2$	7	$h_N^- \cdot 2 \cdot 3 \cdot 19$	17
65	$2^4 \cdot 3$	2^6	$2^3 \cdot 13 \cdot 17$	-3^3
68	2^5	2^3	$h_N^- \cdot 2^4$	-3
69	$2^2 \cdot 11$	$3 \cdot 23$	$h_N^- \cdot 2^4 \cdot 3851$	96001
75	$2^3 \cdot 5$	11	$h_N^- \cdot 2 \cdot 5 \cdot 1181$	2339
76	$2^3 \cdot 3^2$	19	$h_N^- \cdot 2^2 \cdot 5$	$2 \cdot 3$
77	$2^2 \cdot 3 \cdot 5$	$2^8 \cdot 5$	$2^4 \cdot 5^2 \cdot 19 \cdot 191$	$-7 \cdot 29 \cdot 229$
80	2^5	5	$h_N^- \cdot 2^2 \cdot 13$	$-2 \cdot 3$
84	$2^3 \cdot 3$	1	$2^6 \cdot 7$	$-3 \cdot 5$
85	2^6	$5 \cdot 17 \cdot 73$	$h_N^- \cdot 2^2 \cdot 29 \cdot 11489$	$3 \cdot 113 \cdot 430543$
87	$2^3 \cdot 7$	$2^9 \cdot 3$	$2^4 \cdot 3 \cdot 5 \cdot 16493$	$-2^2 \cdot 7 \cdot 2971$
88	$2^3 \cdot 5$	$5 \cdot 11$	$h_N^- \cdot 2^2 \cdot 5$	$3 \cdot 19$
91	$2^3 \cdot 3^2$	$2^4 \cdot 7 \cdot 13 \cdot 37$	$h_N^- \cdot 5^2 \cdot 181$	$3 \cdot 2480663$
92	$2^2 \cdot 11$	$3 \cdot 87$	$h_N^- \cdot 2^3$	-13
93	$2^2 \cdot 3 \cdot 5$	$3^2 \cdot 5 \cdot 151$	$h_N^- \cdot 2^3 \cdot 5 \cdot 7 \cdot 61 \cdot 271$	$241 \cdot 953 \cdot 1021$
95	$2^3 \cdot 3^2$	$2^2 \cdot 13 \cdot 19 \cdot 109$	$h_N^- \cdot 2^3 \cdot 5 \cdot 31 \cdot 829$	$3 \cdot 62656691$
96	2^5	3^2	$2^2 \cdot 3 \cdot 41$	7
99	$2^2 \cdot 3 \cdot 5$	$3 \cdot 31^2$	$2 \cdot 3 \cdot 31 \cdot 37$	29

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), $l \nmid 2N$, 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, $l \nmid 2N$, and let λ_j, $(j, N) = 1$, be as in* (28). *Then*

$$\lambda_j \le v_l(h_N^-) + \sum_{\chi \in \mathcal{C}} \sum_{\substack{p \mid N \\ p \nmid f_\chi}} v_l(\Phi_{\chi,p}). \tag{33}$$

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_N^- and to all numbers $\Phi_{\chi,p}$ occurring on the right side of* (33).

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

$$\widehat{c}_k = \frac{\alpha_k}{(2N)^r \cdot h_N^- \cdot \prod_{\chi,p} \Phi_{\chi,p}}$$

for some algebraic integer α_k (the product runs over all characters χ and primes p occurring on the right side of (33)). Since $\widehat{c}_k$ is an entry of the inverse of the cotangent matrix $C = (c_{mn^*})_{m,n\in\mathcal{R}}$, the number $\det C \cdot \widehat{c}_k$ 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 $h_N^- \cdot \prod_{\chi,p} \Phi_{\chi,p}$ 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 λ_j can be refined, as the next proposition shows. We shall use the notation $\lfloor c \rfloor$ 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 λ_j, $(j,N) = 1$, of (28) *satisfy*

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

Proof. Let $\chi \in \mathcal{X}'$ be arbitrary, $d = \mathrm{ord}(\chi)$, and consider a prime ideal $\mathfrak{l}$ of $\mathbb{Q}(\chi)$ lying above l. By $v_\mathfrak{l}$ 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

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

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

$$v_l(h_\chi) \geq v_\mathfrak{l}(B_\chi) \cdot f_l.$$

This gives $v_\mathfrak{l}(B_\chi) \leq n$ for $n = \lfloor m/\mathrm{ord}(l, 2^\kappa p^{e-1}) \rfloor$ and shows that l^n/B_χ is l-integral. ∎

Proposition 10 remains valid—with some minor changes—in the case $N = 2^e$ 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 χ of order $N/4$; so m boils down to $m = v_l(h') = v_l(\widehat{h})$, and 2^κ must be replaced by $N/4$. Finally, (34) reads

$$\lambda_j \le \lfloor m/\mathrm{ord}(l, N/4) \rfloor.$$

We shall illustrate the meaning of last two propositions with the following

EXAMPLES. 1. As above, consider $N = p = 41$, $h_p^- = 11^2$, $l = 11$, so $v_l(h') = 2$. Hence Proposition 9 gives $\lambda_j \le 2$, 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 $\mathrm{ord}(11, 2^\kappa) = 2$; then (34) gives $\lambda_j \le 1$, 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, $\mathrm{ord}(l, 2^\kappa) = 1$, 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 $v_7(h_\chi) = 1$, so $m = 1$. Therefore, (30) gives the sharp bound $\lambda_j \le 2$. 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 $N = p^e$; 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 $N = p^e \ge 3$ be a prime power and $\widehat{h} = h_N^-/h_{N/p}^-$ as in* (25). *For $l \in \{2, p\}$ and any j, $(j, N) = 1$,*

$$\lambda_j \le v_l(\varphi(N)) + v_l(\widehat{h}).$$

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

THEOREM 4. *Let $N = p^e \ge 3$ 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 $2^\kappa p^{e-1} b_j$ is a divisor of $\widehat{h} = h_N^-/h_{N/p}^-$.*

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* $N = p^e$. 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

$$\widetilde{\mathcal{X}} = \{\chi \in \mathcal{X}^- : f_\chi = N\}, \quad \widetilde{\mathcal{C}} = \widetilde{\mathcal{X}} \cap \mathcal{C}, \quad \widetilde{h} = \prod_{\chi \in \widetilde{\mathcal{C}}} h_\chi.$$

If one restricts the sum on the right side of (24) to characters $\chi \in \widetilde{\mathcal{X}}$, one obtains

$$\widetilde{b}_j = \widetilde{b}_j(N) = \frac{-2}{\varphi(N)} \sum_{\chi \in \widetilde{\mathcal{X}}} \frac{\overline{\chi}(j)}{B_\chi}; \tag{35}$$

indeed, $w_\chi = 1$ whenever $f_\chi = N$ (cf. (7)). Of course, $\widetilde{b}_j = b_j$ if N is a prime or a powerful number (e.g., a prime power $N = p^e$). In Section 5 we shall see how $\widetilde{b}_j$ 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: $v_l(\widetilde{h}) = 1$ and, in addition, $l \nmid N \cdot \varphi(N)$ (thus, $l \geq 2$ because of $N \geq 3$). Since $v_l(h_\chi) \geq 0$ for all $\chi \in \widetilde{\mathcal{C}}$, there is exactly one character in $\widetilde{\mathcal{C}}$, say ψ, with $v_l(h_\psi) = 1$, whereas $v_l(h_{\psi'}) = 0$ for all $\psi' \in \widetilde{\mathcal{C}}$, $\psi' \neq \psi$. If ψ' 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,

$$\widetilde{b}_j = \frac{-2}{\varphi(N)} \sum_{\chi \in [\psi]} \frac{\chi(j)^{-1}}{B_\chi} + a_j \tag{36}$$

for an l-integral number a_j. Let d denote the order of ψ. 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 $l \equiv 1 \bmod d$.

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 $\overline{\mathbb{Q}}_l$ 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 ψ, however, are $(l-1)$th roots of unity (because of $d \,|\, (l-1)$), 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_χ. 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 χ'. Altogether, we obtain

PROPOSITION 12. *Let $N \geq 3$ and l be a prime, $l \nmid N \cdot \varphi(N)$. Suppose that $v_l(\widetilde{h}) = 1$. Then there is exactly one $\psi \in \widetilde{\mathcal{C}}$ 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 χ,*

$$\widetilde{b}_j \equiv \frac{-2\chi(j)^{-1}}{\varphi(N)B_\chi} \bmod \mathbb{Z}_l \tag{37}$$

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

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

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

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 $\operatorname{ord}(\chi^{-1}) = \operatorname{ord}(\psi) = d$, the range of $\chi(j)^{-1}$ coincides with the set of dth roots of unity in $\mathbb{Z}_l$, whose cardinality is d. However, any two distinct dth 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 *Teichmüller* character, which is defined by $\omega(j) \equiv j \bmod p\mathbb{Z}_p$. Then $\widetilde{\mathcal{X}} = \mathcal{X}^- = \{\omega^k : 1 \leq k \leq p-2,\ k \text{ odd}\}$. By [20], p. 61,

$$\pm 2^{(p-3)/2} h_p^- = p \prod_{\substack{1 \leq k \leq p-1 \\ k \text{ odd}}} B_{\omega^k}.$$

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):

$$b_j \equiv \frac{-2 \cdot \omega^{-k}(j)}{(p-1)B_{\omega^k}} \bmod \mathbb{Z}_p. \tag{38}$$

In particular, $v_p(b_j) = -1$.

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

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

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 ≥ 2.

For practical purposes it is useful to transform the congruences (37), (38) into congruences of *integers*, i.e., instead of working with $\mathbb{Q}_l/\mathbb{Z}_l$ one works with the ring $\mathbb{Z}/l\mathbb{Z}$. We discuss this transformation in the case $N = p^e$, $p \ge 3$, where $\widetilde{b}_j = b_j$ for all j, $(j, N) = 1$ and $\widetilde{h} = h'$. Our discussion will also show how to *find* the l-character χ in practice. In accordance with Proposition 12, we assume $l \nmid p(p-1)$ and $v_l(\widetilde{h}) = v_l(\widehat{h}) = 1$ (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

$$b \equiv a/c \bmod m;$$

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

$$lb_j \equiv a/c \bmod l,$$

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

Suppose we have taken our prime l with $v_l(\widehat{h}) = 1$ 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 χ *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 $d = p^{e-1}s$, $s \mid (p-1)$, $v_2(s) = v_2(p-1)$, 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

$$\operatorname{ord}(w, l) = d.$$

Then the congruence

$$\psi(g) \equiv w \bmod l\mathbb{Z}_l \tag{39}$$

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

$$\psi(g) \equiv w^{l^{m-1}} \bmod l^m\mathbb{Z}_l, \qquad m \ge 1, \tag{40}$$

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

write B_χ in the form

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

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

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

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

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

Since χ 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

$$B_\chi/l \equiv c \bmod l\mathbb{Z}_l.$$

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

$$lb_{g^m} \equiv \frac{-2w^{-mk}}{\varphi(N)c} \bmod l, \tag{43}$$

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

Example. Consider $N = p = 53$, for which $h_p^- = 4889$ 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 χ is given by $\chi(g) \equiv 3637 \bmod l\mathbb{Z}_l$ and the above number c satisfies $c \equiv 1674 \bmod l$. This gives the following congruences for the integers $2lb_j$ when j runs through the powers of g mod p : $2lb_1 \equiv 82$, $2lb_2 \equiv 5$, $2lb_4 \equiv -1371$, $2lb_8 \equiv 453$, $\ldots \bmod l$. 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, $1 \le j \le p - 1$, 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 $N = p = l \ge 3$ and suppose $v_p(h_p^-) = 1$ (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,

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

which gives the desired congruence of $B_{\omega^k}/p \bmod p\mathbb{Z}_p$, $1 \le k \le p-4$, 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 $N = p^e \ge 3$ be a prime power (so $\widehat{h} = h_N^-/h_{N/p}^-$ as usual). Put $\kappa = v_2(p-1)$. Suppose that h_N^- is square-free and prime to $\varphi(N)$. Then for all j, $(j,N) = 1$,*

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

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

$$n_{g^m} \equiv n_1 \gamma^m \bmod \widehat{h}$$

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

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

5. Computation of the numbers $b_j(N)$. As above, let $N \ge 3$ and $\mathcal{R} = \{j : 1 \le j \le N/2,\ (j,N) = 1\}$. In this section we discuss the actual computation of the numbers $b_j = b_j(N)$, $j \in \mathcal{R}$, in the range $N \le 250$. The author has computed these numbers for all $N \le 100$ and for some other moduli (among them all primes $p \le 200$, 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 $d = 2^\kappa h_p^-$ 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 $B^T = (b_{jk^*})_{k,j\in\mathcal{R}}$ fulfils $B^T = C^{-1}S$. 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 99×99-matrix, $d = 2h_p^-$ 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_χ 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, $1 \le k < p/2$); 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,

$$b_1 = -1412925450453852175182668183372274 37/h_p^-.$$

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, $l \nmid (p-1)$, $v_l(h_p^-) = 1$, 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 $n_j \bmod d'$. Suppose, in addition, we know an approximate value β_j of b_j such that

$$|b_j - \beta_j| < d'/(2d). \tag{44}$$

Then b_j is also known: Determine an integer k, $k \equiv n_j \bmod d'$, such that

$$|k - d\beta_j| \le d'/2.$$

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 $p \ge 47$ 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 $b_j = \widetilde{b}_j$. We have performed computations of this kind up to $N = 3^5 = 243$, where $\widehat{h} = 6252002011 \cdot 922099242709 = h_{243}^-/h_{81}^-$. Table 2 covers the numbers N under consideration for $N \le 100$—only the (simple) cases when $h_N^- = 1$ have been omitted for reasons of space; thus, it covers all primes $23 \le p \le 97$ 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

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

We now consider the case where b_j differs from $\widetilde{b}_j$, 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 $\widetilde{b}_j$, 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 $b_j(N)$, $\widetilde{b}_j(N)$ instead of b_j, $\widetilde{b}_j$. This distinction will also be necessary for the weight factors $w_\chi = w_\chi(N)$.

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

$$x = \frac{-2}{\varphi(N)} \sum_{\substack{\chi \in \mathcal{X}' \\ f_\chi \mid N_0}} w_\chi(N) \frac{\overline{\chi}(j)}{B_\chi}, \qquad y = \frac{-2}{\varphi(N)} \sum_{\substack{\chi \in \mathcal{X}' \\ l \mid f_\chi}} w_\chi(N) \frac{\overline{\chi}(j)}{B_\chi}$$

(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:

$$w_\chi(N) = \frac{-\overline{\chi}_f(l)}{l - \overline{\chi}_f(l)} w_\chi(N_0). \tag{45}$$

If η is an rth root of unity, one has the polynomial identity

$$(Z^r - 1)/(Z - \eta) = \sum_{k=1}^{r} \eta^{k-1} Z^{r-k}.$$

In our situation η equals $\chi_f(l)$ and $r = \operatorname{ord}(l, N_0)$, so

$$\frac{\overline{\chi}_f(l)}{l - \overline{\chi}_f(l)} = \frac{1}{l^r - 1} \sum_{k=1}^{r} \overline{\chi}_f(l^k) l^{r-k}.$$

This identity, together with (45), gives

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

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 $N \equiv 2 \bmod 4$. Since there is no character χ with $2 \mid f_\chi$ but $4 \nmid f_\chi$, the number y vanishes and we obtain

Proposition 14. *Let $N \geq 3$, $N \equiv 2 \bmod 4$. Put $r = \operatorname{ord}(2, N/2)$. Then*

$$b_j(N) = \frac{-1}{2^r - 1} \sum_{k=1}^{r} 2^{r-k} b_{j2^k}(N/2)$$

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 $N \equiv 2 \bmod 4$. 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 $N \not\equiv 2 \bmod 4$.

(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 $\chi \in \mathcal{X}'$, the condition $l \mid f_\chi$ is equivalent to $f_\chi = N$.

Accordingly, the summand y equals $\widetilde{b}_j(N)$ and

$$b_j(N) = \widetilde{b}_j(N) - \frac{1}{(l-1)(l^r-1)} \sum_{k=1}^{r} l^{r-k} b_{jl^k}(N/l) \tag{46}$$

with $r = \operatorname{ord}(l, N_0)$.

(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 $\widetilde{b}_j(N)$, whereas the other one can be treated like the above sum x, the roles of l and p being interchanged. Altogether, we obtain, with $r = \operatorname{ord}(l, p)$ and $s = \operatorname{ord}(p, l)$,

$$\begin{aligned} b_j(N) = \widetilde{b}_j(N) &- \frac{1}{(l-1)(l^r-1)} \sum_{k=1}^{r} l^{r-k} b_{jl^k}(p) \\ &- \frac{1}{(p-1)(p^s-1)} \sum_{k=1}^{s} p^{s-k} b_{jp^k}(l). \end{aligned} \tag{47}$$

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 $\widetilde{b}_j(N)$ 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 $\widetilde{b}_j(N)$. 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 $\widetilde{d} = 2h_N^-/3 = 4530$ is a possible common denominator of the numbers $\widetilde{b}_j(N)$. By means of the said numerical approximation or by the suitable congruence mod 151, we find

$$\widetilde{b}_1(N) = -32/\widetilde{d}, \quad \widetilde{b}_2(N) = -46/\widetilde{d}, \quad \ldots, \quad \widetilde{b}_7(N) = -23/\widetilde{d}, \quad \ldots$$

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 $\widetilde{b}_j(N)$.

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

[1] R. Ayoub, *On a theorem of Iwasawa*, J. Number Theory 7 (1975), 108–120.

[2] L. Blum, M. Blum and M. Shub, *A simple unpredictable pseudorandom number generator*, SIAM J. Comput. 15 (1986), 364–383.

[3] J. Buhler, R. Crandall, R. Ernvall and T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. 61 (1993), 151–153.

[4] L. Carlitz, *Some cyclotomic matrices*, Acta Arith. 5 (1959), 293–308.

[5] L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. 6 (1955), 265–269.

[6] K. Girstmair, *Ein v. Staudt–Clausenscher Satz für periodische Bernoullizahlen*, Monatsh. Math. 104 (1987), 109–118.

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

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

[9] —, *On the factorization of the relative class number in terms of Frobenius divisions*, Monatsh. Math. 116 (1993), 231–236.

[10] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer, Berlin, 1950.

[11] —, *Über die Klassenzahl abelscher Zahlkörper* (reprint of the first edition), Springer, Berlin, 1985.

[12] E. Hecke, *Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik*, Abh. Math. Sem. Univ. Hamburg 5 (1927), 199–204 (= Mathematische Werke, Göttingen, 1959, 461–486).

[13] M. Ishibashi, $\mathbb{Q}$*-linear relations of special values of the Estermann zeta function*, Acta Arith. 86 (1998), 239–244.

[14] G. Lettl, *Stickelberger elements and cotangent numbers*, Exposition. Math. 10 (1992), 171–182.

[15] T. Metsänkylä, *Estimations for L-functions and the class numbers of certain imaginary cyclic fields*, Ann. Univ. Turku. Ser. I 140 (1970), 1–10.

[16] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer and Polish Scientific Publishers, Berlin and Warszawa, 1990.

[17] D. J. Newman, *Analytic Number Theory*, Springer, 1998.

[18] T. Shimada, *Cyclotomic unit and its Fermat quotient*, Abh. Math. Sem. Univ. Hamburg 67 (1997), 239–254.

[19] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, Cambridge, 1995.

[20] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

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

Received on 17.1.2000 (3740)