MATH. SCAND. 37 (1975), 61–75

ON THE CYCLOTOMIC INVARIANTS OF IWASAWA

TAUNO METSÄNKYLÄ

1. Introduction.

Let p be a prime and put $q=p$ if $p>2$ and $q=4$ if $p=2$. For each $n \geqq 0$, denote by k_n the cyclotomic field of q_nth roots of unity, where $q_n = m_0 q p^n$ with $m_0 \geqq 1, (m_0, p) = 1$. Let $p^{e(n)}$ denote the highest power of p dividing the class number h_n of k_n.

The union k_∞ of all the fields k_n is a so-called Z_p-extension (or Γ-extension) of k_0. Thus a general theory of Iwasawa [3] gives the following formula, valid for all sufficiently large n:

$$e(n) = \lambda n + \mu p^n + \nu ,$$

where λ, μ, and ν are integers $(\lambda, \mu \geqq 0)$ depending only upon p and m_0. Numerical computations show that $\mu = 0$ whenever $m_0 = 1$ and $p < 30000$ ([6], [7], [9]); no case where $\mu > 0$ is known.

Similarly, if $e^-(n)$ is the exponent of the p-part of h_n^-, the so-called first factor of h_n, we have

$$e^-(n) = \lambda^- n + \mu^- p^n + \nu^- \tag{1.1}$$

for all n large enough, where again the integers $\lambda^- = \lambda^-(q_0)$, $\mu^- = \mu^-(q_0)$, $\nu^- = \nu^-(q_0)$ are invariants of k_∞ $(0 \leqq \lambda^- \leqq \lambda, 0 \leqq \mu^- \leqq \mu)$. In [5] Iwasawa gave a proof for this, based on the theory of p-adic L-functions. He also used this theory to get information on the vanishing of λ^- and μ^- (see [5, pp. 94–96]). It is the purpose of the present paper to continue the investigation of λ^- and μ^- by means of the theory of p-adic L-functions.

After the required preliminary material, presented in sections 2 and 3, we shall give a natural decomposition of λ^- and μ^- in section 4 and derive some estimates for μ^- in section 5. The main contents of the following sections 6–9 consist of certain results related to the vanishing of μ^- (or, more precisely, the components of μ^-), and the last sections 10–11 include an application of these results. This application shows that if $\mu^-(p) > 0$, then there exist Z_p-extensions k_∞ / k_0 with arbitrarily large μ^-.

In the special case where $m_0 = 1$ some of the subsequent results have

Received December 11, 1974.

been known before. However, the new proofs often look simpler and, in any case, may serve as an illustration of the power of the present methods.

2. Some notation and basic results.

The notation presented in this section is adopted from Iwasawa's book [5]. For the proofs of the results in this and the following section, we refer to the same book.

Let Q_p and Z_p denote the field of p-adic numbers and the ring of p-adic integers, respectively, and let Ω_p be a fixed algebraic closure of Q_p. We shall normalize the p-adic valuation $|\cdot|$ on Ω_p by choosing $|p| = p^{-1}$.

Denote by U the unit group of Z_p. For $p > 2$, let V be the subgroup of U consisting of all $(p-1)$st roots of unity, and for $p=2$, let $V = \{\pm 1\}$. Each a in U has the unique decomposition

$$(2.1) \qquad a = \omega(a)\langle a\rangle \,,$$

where $\langle a\rangle \in 1 + q\mathsf{Z}_p$ and $\omega(a)$ is the following element of V:

$$(2.2) \qquad \begin{aligned} \omega(a) &= \lim\nolimits_{n\to\infty} a^{p^n}, \quad \text{if } p > 2, \\ &= (-1)^k \quad \text{for} \quad a \equiv (-1)^k \bmod 4, \quad \text{if } p=2\,. \end{aligned}$$

For $n \geqq 0$, denote by G_n the multiplicative residue class group mod q_n. For a rational integer a relatively prime to q_0, let $\sigma_n(a)$ denote the element of G_n determined by a. Put

$$(2.3) \qquad \Gamma_n = \{\sigma_n(a) \mid a \equiv 1 \bmod q_0\}\,,$$

$$(2.4) \qquad \Delta_n = \{\sigma_n(a) \mid a^{p-1} \equiv \pm 1 \bmod qp^n\}\,.$$

Then $G_n = \Gamma_n \times \Delta_n$ (direct product). Corresponding to this decomposition, write $\sigma_n(a) = \gamma_n(a)\delta_n(a)$ with $\gamma_n(a) \in \Gamma_n$, $\delta_n(a) \in \Delta_n$.

Let K be a finite extension of Q_p in Ω_p. Denote by $\mathfrak{o}$ the ring of p-adic integers in K and by $\Lambda = \mathfrak{o}[[x]]$ the formal power series algebra over $\mathfrak{o}$. For $n \geqq 0$, denote by $R_n = \mathfrak{o}[\Gamma_n]$ the group algebra of Γ_n over $\mathfrak{o}$.

If $m \geqq n \geqq 0$, the natural homomorphism $G_m \to G_n$, defined by $\sigma_m(a) \mapsto \sigma_n(a)$, induces morphisms $\Gamma_m \to \Gamma_n$, $R_m \to R_n$. Let Γ and R denote the inverse limits of Γ_n and R_n with respect to these morphisms. The group Γ can be imbedded in a natural way in the multiplicative group of the $\mathfrak{o}$-algebra R, and there exists a unique $\mathfrak{o}$-algebra isomorphism $\tau\colon \Lambda \to R$ such that $\tau(1+x) = \lim \gamma_n(1+q_0)$.

Denote by f_χ the conductor of a Dirichlet character χ. (In what follows, all characters are assumed to be primitive.) The number f_χ can be written in the form m_0 or m_0qp^e, where m_0 is a natural number prime to p and $e \geqq 0$. The character χ then has a unique decomposition $\chi = \theta\psi$, where $f_\theta = m_0$ or m_0q, f_ψ is a power of p and $\psi(a) = \psi(b)$ whenever $\langle a\rangle \equiv \langle b\rangle$ mod $f_\psi Z_p$. We call θ the first factor of χ.

By $B_n(\chi), n \geqq 0$, we mean generalized Bernoulli numbers defined by

$$\textstyle\sum_{a=1}^{f}\chi(a)te^{at}/(e^{ft}-1) = \sum_{n=0}^{\infty}B_n(\chi)t^n/n! \qquad (f = f_\chi)\,.$$

If χ is the principal character χ^0, then $B_n(\chi)$ is the ordinary Bernoulli number B_n. For odd characters χ we have

$$B_1(\chi) = f^{-1}\textstyle\sum_{a=1}^{f}\chi(a)a \qquad (f = f_\chi)\,. \tag{2.5}$$

3. On p-adic L-functions and cyclotomic invariants.

For a fixed even character χ, consider the p-adic L-function $L_p(s; \chi)$ defined in a certain disk

$$\{s \in \Omega_p \mid |s-1| < r\} \qquad (r > 1)\,,$$

excluding $s = 1$ in the case $\chi = \chi^0$. By a fundamental result of Iwasawa,

$$L_p(s; \chi) = 2f(\chi(1+q_0)^{-1}(1+q_0)^s - 1; \theta)\,, \tag{3.1}$$

where θ is the first factor of χ and $f(x; \theta)$ is a certain power series if $\theta \neq \chi^0$, and a quotient of two power series if $\theta = \chi^0$. (Recall that $q_0 = m_0q$, where m_0 is now determined by χ.)

To define $f(x; \theta)$ for $\theta \neq \chi^0$, choose the field K appearing in the preceding section so that it contains the values of $\theta(a)$ for all a. For $n \geqq 0$, put

$$\xi_n = \xi_n^{\theta} = -(2q_n)^{-1}\sum_{\substack{a=1\\(a,\,q_0)=1}}^{q_n} a\theta(a)\omega^{-1}(a)\gamma_n(a)^{-1}\,. \tag{3.2}$$

Then $\xi_n \in R_n$ and, moreover, there exists a $\xi_\infty{}^{\theta}$ in R such that $\xi_\infty{}^{\theta} = \lim \xi_n$. Now, $f(x; \theta)$ is defined by the condition

$$\tau : f(x; \theta) \mapsto \xi_\infty{}^{\theta}\,, \tag{3.3}$$

where τ is the mapping mentioned in section 2.

The known connection between the generalized Bernoulli numbers and the values of $L_p(s; \chi)$ at $s = 0, -1, -2, \ldots$ implies, by (3.1), the equations

$$\begin{aligned} &2f(\chi(1+q_0)^{-1}(1+q_0)^{1-n} - 1; \theta) \\ &\quad = -(1-\chi_n(p)p^{n-1})B_n(\chi_n)/n \qquad (n \geqq 1)\,, \end{aligned} \tag{3.4}$$

where $\chi_n = \chi\omega^{-n}$ (note that ω, given in (2.2), defines a character with $f_\omega = q$).

Next, let m_0 be fixed and consider h_n^-, the first factor of the class number of the q_nth cyclotomic field. Put

$$(3.5)\qquad A(x) = \prod\nolimits_{\theta\in X} f(x;\,\theta)\,,$$

where

$$X = X(q_0) = \{\theta \mid \theta \neq \chi^0,\quad \theta(-1) = 1,\quad f_\theta \mid q_0\}\,.$$

Then $A(x) \in \mathsf{Z}_p[[x]]$. Starting from the well-known analytic expression of h_n^- and using (2.5) and then (3.4), for $n=1$, Iwasawa [5, pp. 90–95] showed that

$$(3.6)\qquad |h_m^-| = |h_n^-|\,|\prod\nolimits_\zeta A(\zeta-1)| \qquad (\zeta^{p^m} = 1,\ \zeta^{p^n} \neq 1)\,,$$

and if $m_0=1$,

$$(3.7)\qquad |h_n^-| = |\prod\nolimits_\zeta A(\zeta-1)| \qquad (\zeta^{p^n} = 1)\,,$$

whenever $m \geqq n \geqq 0$.

Now the invariants $\lambda^-=\lambda^-(q_0)$ and $\mu^-=\mu^-(q_0)$ are the unique nonnegative integers such that

$$(3.8)\qquad \begin{aligned} A(x) &= p^{\mu^-}\textstyle\sum_{k=0}^{\infty} b_k x^k \qquad (b_k \in \mathsf{Z}_p)\,,\\ b_k &\equiv 0 \bmod p \quad \text{for} \quad 0 \leqq k < \lambda^-\,,\\ b_k &\not\equiv 0 \bmod p \quad \text{for} \quad k = \lambda^-\,, \end{aligned}$$

where, as often in the sequel, $\bmod p$ stands for $\bmod p\mathsf{Z}_p$. (It should be noted that the symbols λ^- and μ^- are denoted by λ and μ in [5].)

In [5] it is proved that the condition

$$(3.9)\qquad \lambda^- = \mu^- = 0$$

is equivalent to $(p, h_1^-/h_0^-)=1$, and if $m_0=1$, this is equivalent to $(p, h_0^-) =1$, i.e. to the fact that p is a regular prime. These results follow easily from (3.6) and (3.7), for (3.9) holds if and only if $|A(\zeta-1)|=1$, where ζ is any root of unity with p-power order.

4. Decomposition of the invariants.

In the following we shall assume that K/Q_p is the extension generated by all numbers $\theta(a)$, where $\theta \in X(q_0)$ and a is an integer. We also fix a prime element π of the local ring $\mathfrak{o}$.

Let $\theta \in X(q_0)$. As $f(x;\,\theta) \in \mathfrak{o}[[x]]$ and $\mathfrak{o}$ is a unique factorization ring, there exist unique nonnegative integers $\lambda_\theta=\lambda_\theta(q_0)$ and $\mu_\theta=\mu_\theta(q_0)$ such that

$$(4.1) \qquad \begin{aligned} f(x;\theta) &= \pi^{\mu_\theta}\textstyle\sum_{k=0}^{\infty}\beta_k x^k \qquad (\beta_k \in \mathfrak{o})\,, \\ \beta_k &\equiv 0 \bmod \mathfrak{p} \quad \text{for} \quad 0 \leqq k < \lambda_\theta\,, \\ \beta_k &\not\equiv 0 \bmod \mathfrak{p} \quad \text{for} \quad k = \lambda_\theta\,, \end{aligned}$$

where $\mathfrak{p} = \pi\mathfrak{o}$ is the maximal ideal of $\mathfrak{o}$.

Lemma 1. *Let e be the ramification index of K/Q_p. Then*

$$\lambda^- = \textstyle\sum_{\theta\in X}\lambda_\theta, \qquad \mu^- = e^{-1}\textstyle\sum_{\theta\in X}\mu_\theta\,.$$

Proof. Set

$$\textstyle\prod_{\theta\in X}\sum_{k=0}^{\infty}\beta_k x^k = \sum_{k=0}^{\infty}\gamma_k x^k \qquad (\gamma_k \in \mathfrak{o})\,.$$

Then

$$\begin{aligned} \gamma_k &\equiv 0 \bmod \mathfrak{p} \quad \text{for} \quad 0 \leqq k < \textstyle\sum\lambda_\theta\,, \\ \gamma_k &\not\equiv 0 \bmod \mathfrak{p} \quad \text{for} \quad k = \textstyle\sum\lambda_\theta\,. \end{aligned}$$

On the other hand, combining (3.5) and (3.8) and using our new notations we see that

$$\pi^m \textstyle\sum_{k=0}^{\infty}\gamma_k x^k = \varepsilon\pi^{e\mu^-}\sum_{k=0}^{\infty} b_k x^k \qquad (m = \sum\mu_\theta)\,,$$

where ε is a unit of $\mathfrak{o}$. Since the congruence $b_k \equiv 0 \bmod p$ is equivalent to $b_k \equiv 0 \bmod \mathfrak{p}$, it follows that the lemma is true.

Remarks. (i) If $m_0 = 1$, then $K = \mathsf{Q}_p$ and so $\mu^- = \sum_{\theta\in X(p)}\mu_\theta$.

(ii) Let us replace k_0, for a moment, by an arbitrary imaginary abelian field k_0', say, having q_0 as conductor. Let k_∞' be the unique Z_p-extension of k_0' contained in k_∞, and let $k_n', n \geqq 1$, be the subfield of k_∞' cyclic of degree p^n over k_0'. Then we have for the first factor of the class number of k_n' a formula similar to (1.1). Now, if θ belongs to a certain subset of X, then the numbers λ_θ and μ_θ (the latter multiplied by a constant) defined above are components of the invariants λ^- and μ^- of k_∞', too. Thus many of the results to be presented in the following can actually be applied to this more general kind of Z_p-extensions.

5. Upper bounds for μ^-.

By using the theory of Z_p-extensions, Iwasawa [4] proved that

$$(5.1) \qquad \mu^- \leqq e^-(0)\,,$$

if $m_0 = 1$. This can be shown simply by the present method, too. Indeed, the formulas (3.7) and (3.8) imply that

$$|h_0^-| = |A(0)| \leqq |p^{\mu^-}|\,.$$

Moreover, it is seen that if $\lambda^- > 0$, then the inequality above (and so that in (5.1)) is strict.

Note in passing that (5.1) implies the estimate $\mu < (p-1)/2$, because $\mu \leqq 2\mu^-$ and $e^-(0) < (p-1)/4$ ([4],[13]).

The following theorem, concerning the general case where $m_0 \geqq 1$, gives a result of the same kind as (5.1).

THEOREM 1. *We have* $(p-1)\mu^- \leqq e^-(1) - e^-(0)$, *the inequality being strict if* $\lambda^- > 0$.

PROOF. By (3.6) and (3.8),

$$|h_1^-/h_0^-| = |\textstyle\prod_\zeta A(\zeta-1)| \qquad (\zeta^p = 1,\, \zeta \neq 1)$$

with

$$|A(\zeta-1)| \leqq |p^{\mu^-}|\,.$$

As $|\zeta - 1| < 1$, the above inequality is strict if $\lambda^- > 0$.

Turning again to the case $m_0 = 1$, we shall prove an extension of the result (5.1).

THEOREM 2. *Let* $m_0 = 1$ *and denote by* t *the number of nonzero components* λ_θ *in the decomposition of* λ^-. *Then*

$$e^-(n) \geqq \mu^- p^n + t(n+1)$$

for all $n \geqq 0$.

PROOF. Now the coefficients b_k in (3.8) satisfy

(5.2) $$|b_k| \leqq |p^{t-k}| \qquad (0 \leqq k < t)\,.$$

Hence we get first

(5.3) $$|A(0)| = |p^{\mu^-} b_0| \leqq |p^{\mu^- + t}|\,,$$

so that $e^-(0) \geqq \mu^- + t$. Secondly, let $m \geqq 1$ and let ζ be a primitive p^mth root of unity. Then $|\zeta - 1| = |p^z|$ with $z = (p-1)^{-1} p^{1-m}$, which together with (5.2) implies

$$|A(\zeta - 1)| \leqq |p^{\mu^- + tz}|\,.$$

Substituting this and (5.3) into (3.7) we obtain the asserted inequality.

6. The first and second coefficient of $f(x;\theta)$.

Throughout this section we shall suppose that $m_0 = 1$ and $p > 3$. Then

(6.1) $$X = X(p) = \{\omega^{m+1} \mid m = 1,3,\ldots,p-4\}\,.$$

For a fixed character ω^{m+1} in X, we put

$$f(x;\, \omega^{m+1}) = a_0+a_1x+a_2x^2+\dots \qquad (a_k \in \mathbf{Z}_p)$$

and investigate the divisibility of a_0 and a_1 by p.

LEMMA 2. *The coefficient a_0 is divisible by p if and only if $B_{m+1}\equiv 0$ $\operatorname{mod} p$, i.e. $(p,m+1)$ is an irregular pair.*

PROOF. Apply (3.4) for $\chi=\omega^{m+1}$ and $n=1$, and then (2.5) to get

$$a_0 = f(0;\, \omega^{m+1}) = -\tfrac{1}{2}B_1(\omega^m) = -(2p)^{-1}\textstyle\sum_{a=1}^{p-1}\omega^m(a)a.$$

By (2.2), $\omega(a)\equiv a^p \operatorname{mod} p^2$. Furthermore, it follows from a well-known summation formula (see, e.g. [1, p. 384]) that

$$\textstyle\sum_{a=1}^{p-1} a^{2k} = pB_{2k} \operatorname{mod} p^2 \quad (k \geqq 1,\ (p,2k+1) = 1)\,. \tag{6.2}$$

Hence we infer that $a_0\equiv -\tfrac{1}{2}B_{mp+1} \operatorname{mod} p$. But since $mp+1\equiv m+1\not\equiv 0$ $\operatorname{mod} p-1$, Kummer's congruence modulo p [1, p. 385] shows that the condition $B_{mp+1}\equiv 0 \operatorname{mod} p$ is equivalent to $B_{m+1}\equiv 0 \operatorname{mod} p$.

LEMMA 3. *If $m>1$, the coefficient a_1 is divisible by p if and only if $B_{mp^2+1}\equiv \tfrac{1}{2}B_{(m-1)p^2+2} \operatorname{mod} p^2$.*

PROOF. Because the Bernoulli numbers with odd indices >1 vanish, it is easy to see that (6.2) holds even mod p^3 provided that $k\geqq 2$ and $p-1$ does not divide $2k-2$. Thus a slight modification of the preceding argument yields, for $m>1$,

$$f(0;\, \omega^{m+1}) \equiv -\tfrac{1}{2}B_{mp^2+1} \operatorname{mod} p^2\,. \tag{6.3}$$

Imitating the proof of (2.5), presented in [5, p. 14], one can show that

$$B_2(\chi) = f^{-1}\textstyle\sum_{a=1}^{f} \chi(a)a^2-\sum_{a=1}^{f} \chi(a)a = f^{-1}\sum_{a=1}^{f} \chi(a)a^2 \qquad (f = f_\chi) \tag{6.4}$$

for even nonprincipal characters χ. Let $c=-p(1+p)^{-1}$. We apply (3.4) for $n=2$ and then (6.4) obtaining

$$2f(c;\, \omega^{m+1}) = -\tfrac{1}{2}B_2(\omega^{m-1}) \equiv -\tfrac{1}{2}B_{(m-1)p^2+2} \operatorname{mod} p^2\,, \tag{6.5}$$

when $m>1$. Now, as $p|c$, a necessary and sufficient condition for $p|a_1$ is

$$a_1c+a_2c^2+\dots \equiv 0 \operatorname{mod} p^2$$

or

$$f(0;\omega^{m+1}) \equiv f(c;\, \omega^{m+1}) \operatorname{mod} p^2\,.$$

Comparing this with (6.3) and (6.5) we see that the lemma is proved.

Lemma 4. *For natural numbers i, put*

$$A_n^{2i} = B_{2i+n(p-1)}/(2i+n(p-1)) \qquad (n \geqq 0).$$

Then $a_0 \equiv a_1 \equiv 0 \bmod p$ if and only if

$$B_{m+1} \equiv 0 \bmod p, \quad A_0^{m+1} \equiv A_1^{m+1} \bmod p^2. \tag{6.6}$$

Proof. For a fixed irregular pair $(p, m+1)$, set $A_n = A_n^{m+1}$. Note that $m > 1$ because $B_2 \not\equiv 0 \bmod p$. By Kummer's congruences modulo p and modulo p^2 (see, e.g. [8]),

$$A_n \equiv 0 \bmod p \qquad (n \geqq 0),$$

$$A_n - 2A_{n+1} + A_{n+2} \equiv 0 \bmod p^2 \qquad (n \geqq 0). \tag{6.7}$$

These imply easily

$$A_n \equiv A_{n+kp} \bmod p^2 \qquad (n \geqq 0, k \geqq 0). \tag{6.8}$$

Now we find that lemma 4 is obtained by combining lemmas 2 and 3. Indeed, the congruence of lemma 3 can be written in the form

$$A_{(p+1)m} \equiv A_{(p+1)(m-1)} \bmod p^2,$$

and by (6.8) and (6.7) this is equivalent to $A_0 \equiv A_1 \bmod p^2$.

Remarks. (i) As a first consequence of lemma 4 we state that if $\mu^-(p) > 0$ then there is an odd index $m, 1 \leqq m \leqq p-4$, such that the conditions (6.6) are fulfilled. This result was proved also by Iwasawa (see [2, p. 782]), who started from the congruences appearing below in lemma 6 and derived an infinite sequence of congruences (of which only these two were explicitly given), all being necessary conditions for $\mu^-(p) > 0$.

(ii) If $(p, m+1)$ is an irregular pair for which

$$A_0^{m+1} \not\equiv A_1^{m+1} \bmod p^2, \tag{6.9}$$

then lemmas 2 and 4 imply that $\mu_\theta = 0$ and $\lambda_\theta = 1$ for $\theta = \omega^{m+1}$. By using a computer, Johnson [8], [9], [10] showed that (6.9) holds for every irregular pair with $p < 30000$ and concluded that $\mu^-(p) = 0$ for these p. By the above result these computations allow us to draw a further conclusion, namely that $\lambda^-(p)$ then equals the index of irregularity of p, i.e. the number of irregular pairs $(p, m+1)$. We remark that the latter result was verified in [9] by another computational method, due to Iwasawa and Sims [6].

(iii) Looking at the proofs of lemmas 3 and 4 we see that $p^2|a_0, p|a_1$ implies $A_n{}^{m+1} \equiv 0 \bmod p^2$ for all $n \geqq 0$. Again, it was shown by Johnson [8], [9] that $A_0{}^{m+1} \not\equiv 0 \bmod p^2$ for $p < 30000$.

7. A general criterion for μ^- to vanish.

Let us consider the groups $\Gamma_n, n \geqq 0$, given in (2.3). Denote by g_{nk} $(k = 0, \ldots, p^n - 1)$ the elements of Γ_n in some fixed arrangement. Then the elements $\xi_n = \xi_n{}^\theta$ of the group algebra $R_n = \mathfrak{o}[\Gamma_n]$, defined in (3.2), may be written in the form

$$\xi_n = \sum_{k=0}^{p^n-1} S_{nk} g_{nk}$$

with

$$S_{nk} = S_{nk}(\theta) = -(2q_n)^{-1} \sum\nolimits^{(k)} a\theta(a)\omega^{-1}(a) \in \mathfrak{o} , \tag{7.1}$$

where $\sum^{(k)}$ denotes summation extended over the values of a satisfying

$$1 \leqq a < q_n, \quad (a, q_0) = 1, \quad \gamma_n(a)^{-1} = g_{nk} . \tag{7.2}$$

LEMMA 5. *Let $\theta \in X(q_0)$. A necessary and sufficient condition for $\mu_\theta > 0$ is that*

$$S_{nk}(\theta) \equiv 0 \bmod \mathfrak{p} \qquad (k = 0, \ldots, p^n - 1) \tag{7.3}$$

for all $n \geqq 0$.

PROOF. The definition (3.3) of $f(x; \theta)$ together with (4.1) shows that $\mu_\theta > 0$ if and only if $\xi_\infty^\theta \equiv 0 \bmod \pi R$. Since $\xi_\infty{}^\theta = \lim \xi_n{}^\theta$, it is immediately seen that this congruence is equivalent to

$$\xi_n{}^\theta \equiv 0 \bmod \pi R_n \qquad (n = 0, 1, \ldots) ,$$

and the lemma follows.

REMARKS. (i) Choose a $\theta \in X(q_0)$ so that the conductors of θ and $\theta\omega^{-1}$ are equal to q_0. Then $(\theta\omega^{-1})(p) = 0$, and arguing in the same way as in the proof of lemma 2 we get

$$f(0; \theta) = -\tfrac{1}{2} B_1(\theta\omega^{-1}) = -(2q_0)^{-1} \sum_{a=1}^{q_0} a(\theta\omega^{-1})(a) = S_{00}(\theta) .$$

Thus the first congruence in lemma 5, $S_{00}(\theta) \equiv 0 \bmod \mathfrak{p}$, holds in this case if and only if at least one of the two numbers λ_θ and μ_θ does not vanish. In particular, if $m_0 = 1$ and $p > 3$, then $S_{00}(\omega^{m+1}) \equiv 0 \bmod p$ is again equivalent to the fact that $(p, m+1)$ is an irregular pair.

(ii) We know that $\xi_{n+1} \mapsto \xi_n$ under the $\mathfrak{o}$-algebra homomorphism $R_{n+1} \to R_n$, defined by $\sigma_{n+1}(a) \mapsto \sigma_n(a) (n \geqq 0)$. Therefore

$$S_{nk} = \sum\nolimits_h S_{n+1,h} ,$$

the sum being extended over those indices h for which $g_{n+1,h} \mapsto g_{nk}$. Specially,

$$S_{00} = \sum_{k=0}^{p^n-1} S_{nk} \qquad (n \geqq 0) .$$

It follows also that if the congruences (7.3) hold for some $n_0 \geqq 1$, then they hold for every n less than n_0.

8. An equivalent form of the criterion in the special case.

We shall again suppose that $m_0 = 1$ and $p > 3$ and give another formulation for lemma 5.

First a notation. If an element x in Z_p has the p-adic representation

$$x = \sum_{k=0}^{\infty} x_k p^k \qquad (0 \leqq x_k < p) ,$$

then we set for each $n \geqq 0$

$$s_n(x) = \sum_{k=0}^{n} x_k p^k .$$

LEMMA 6. *Let $\theta = \omega^{m+1}$, where m is odd, $1 \leqq m \leqq p-4$. A necessary and sufficient condition for $\mu_\theta > 0$ is that*

$$(8.1) \qquad \sum_{v \in V} s_n(uv) v^m \equiv 0 \bmod p^{n+2}$$

for all $n \geqq 0$ and all units $u \in 1 + p\mathsf{Z}_p$.

PROOF. Using (2.1) we may write any rational integer a prime to p in the form $a = \omega(a)\langle a \rangle$, where $\omega(a) \in V$ and $\langle a \rangle \in 1 + p\mathsf{Z}_p$. Let a run through the values mentioned in (7.2). Since $\gamma_n(a) = \gamma_n(b)$ if and only if $\langle a \rangle \equiv \langle b \rangle \bmod p^{n+1}$, we conclude that $\omega(a)$ then runs through V and the value of $\langle a \rangle$ mod p^{n+1} is a constant depending on k. Now we have $a = s_n(a) = s_n(uv)$, where u is any p-adic number satisfying $u \equiv \langle a \rangle$ mod p^{n+1} and $v = v(a) = \omega(a)$. It follows that

$$-2p^{n+1} S_{nk}(\omega^{m+1}) = \sum^{(k)} a\omega^m(a) = \sum_{v \in V} s_n(uv) v^m .$$

Moreover, $u \in 1 + p\mathsf{Z}_p$.

It remains to show that for every u in $1 + p\mathsf{Z}_p$ there exists a rational integer a prime to p such that $u \equiv \langle a \rangle \bmod p^{n+1}$. But this is easy: take $a = s_n(u)$.

The following lemma is a supplement to lemma 6.

LEMMA 7. *Let $n \geqq 0$ be fixed. If* (8.1) *holds for all units $u \in 1 + p\mathsf{Z}_p$, then it holds for all $u \in U$.*

PROOF. For an arbitrary $u \in U$, let $u \equiv u_0 \bmod p (0 < u_0 < p)$ and put $w = \omega(u_0) \in V$. Then $w \equiv u_0 \bmod p$ and so $uw^{-1} \in 1 + p\mathbf{Z}_p$. Accordingly,

$$(8.2) \qquad \textstyle\sum_{v \in V} s_n(uw^{-1}v)v^m \equiv 0 \bmod p^{n+2} .$$

We obtain the congruence (8.1) for u on multiplying (8.2) by w^{-m} and noting that with v also $w^{-1}v$ runs through V.

REMARKS. (i) By using the theory of $\mathbf{Z}_p$-extensions, Iwasawa [2] proved the criterion of lemma 6 in the form, where u is an arbitrary p-adic unit. Johnson [11] proved lemma 7 in the special case where $n = 0$.

(ii) Remark (i) in the preceding section shows that the condition (8.1) for $n = 0$ (and $u = 1$, say) is equivalent to the fact that $(p, m+1)$ is an irregular pair. Johnson [7], [9] showed by computation that there exist no irregular pairs such that $p < 30000$ and (8.1) holds for $n = 1$ with the units 1 and $1 + p$ simultaneously. This proves again that $\mu^-(p) = 0$ for these values of p (cf. remark (ii) in section 6).

9. Another equivalent form.

We shall continue to discuss the case where $m_0 = 1$ and $p = 2s + 1 > 3$.

Let r be a primitive root $\bmod p^{n+1}$ for all $n \geqq 0$. Denote by $r_n(i)$ the least positive residue of $r^i \bmod p^{n+1}$. Moreover, let α be a primitive $(p-1)$st root of unity such that

$$\omega(a) = \alpha^i \quad \text{for} \quad a \equiv r^i \bmod p .$$

LEMMA 8. *Let* $\theta = \omega^{m+1}$ *(m odd, $1 \leqq m \leqq p-4$). A necessary and sufficient condition for* $\mu_\theta > 0$ *is that*

$$(9.1) \qquad \textstyle\sum_{i=0}^{p-2} r_n(ip^n + k)\alpha^{mi} \equiv 0 \bmod p^{n+2} \qquad (k = 0, \ldots, p^n - 1)$$

or, equivalently,

$$(9.2) \quad \textstyle\sum_{i=0}^{s-1} r_n(ip^n + k)\alpha^{mi} \equiv p^{n+1}(1 - \alpha^m)^{-1} \bmod p^{n+2} \qquad (k = 0, \ldots, p^n - 1)$$

for all $n \geqq 0$.

PROOF. We may write the group Δ_n, defined in (2.4), in the form

$$\Delta_n = \{\sigma_n(a) \mid a = r_n(ip^n), i = 0, \ldots, p-2\} .$$

After a suitable rearrangement of the elements g_{nk} of Γ_n we thus get

$$-2p^{n+1}S_{nk} = \textstyle\sum^{(k)} a\omega^m(a) = \sum_{i=0}^{p-2} r_n(ip^n + k)\alpha^{m(i+k)} .$$

Hence (7.3) is in this case equivalent to (9.1).

By using the equations $\alpha^{ms} = -1$ and

$$r_n((i+s)p^n+k) = p^{n+1} - r_n(ip^n+k)$$

we can express the left hand side of (9.1) in the form

$$\begin{aligned} &\textstyle\sum_{i=0}^{s-1} [2r_n(ip^n+k)\alpha^{mi} - p^{n+1}\alpha^{mi}] \\ &= 2\textstyle\sum_{i=0}^{s-1} r_n(ip^n+k)\alpha^{mi} - 2p^{n+1}(1-\alpha^m)^{-1} \,. \end{aligned}$$

Thus the proof of the lemma is complete.

Remark. If the congruences (9.1) and (9.2) hold for the values $0,\ldots,p^n-1$ of k (with a fixed n), then they hold for any integral value, say h, of k. One can verify this easily by writing

$$h \equiv i_0p^n + k_0 \bmod p^n(p-1) \qquad (0 \leqq i_0 \leqq p-2,\ 0 \leqq k_0 \leqq p^n-1)$$

and applying (9.1) for $k=k_0$.

10. The case where m_0 is a prime.

We shall apply preceding results to obtain information on the relationship between $\mu^-(p)$ and $\mu^-(lp)$, where $p=2s+1$ and $l=2t+1$ are primes $>3, l \neq p$. To this end, we shall let $q_n = lp^{n+1}$ and deal with the numbers $S_{nk}(\theta)$, where $\theta \in X(lp)$.

Let g be a primitive root mod l. For $n \geqq 0$, denote by $c_n(i,j)$ the rational integer satisfying

$$0 < c_n(i,j) < q_n, \quad \begin{aligned} c_n(i,j) &\equiv r^i \bmod p^{n+1} \,, \\ &\equiv g^j \bmod l \,. \end{aligned}$$

Let β be a primitive $(l-1)$st root of unity, so that the condition

$$\psi(a) = \beta^j \quad \text{for} \quad a \equiv g^j \bmod l$$

defines a generating character ψ of the character group modulo l. Then the characters

$$(10.1) \qquad \omega^{m+1}\psi^u, \quad m = 1,3,\ldots,p-4; \quad u = 0,2,\ldots,l-3 \,,$$

belong to the set $X(lp)$.

Lemma 9. *Let $n \geqq 0$ and let θ be any character given in* (10.1). *Then*

$$S_{nk}(\theta) = S_{nk}(\omega^{m+1}\psi^u) = -(2q_n)^{-1} \textstyle\sum_{i=0}^{p-2} \sum_{j=0}^{l-2} c_n(ip^n+k,j)\alpha^{m(i+k)}\beta^{uj}$$

$(k=0,\ldots,p^n-1)$, *provided the elements g_{nk} of Γ_n are suitably ordered.*

Proof. Use the same argument as in the proof of lemma 8, observing that now

$$\Delta_n = \{\sigma_n(a) \mid a = c_n(ip^n,j);\quad i = 0,\dots,p-2;\quad j = 0,\dots,l-2\}.$$

The following lemma, whose proof is quite computational, gives a connection between the cases where $m_0=l$ and $m_0=1$. Here we shall use some ideas from [12].

Lemma 10. *Let the assumptions of lemma 9 be satisfied. If, in addition,* $l\equiv 1 \bmod p$ *and* u *is restricted to the set* $\{\varkappa(l-1)/p \mid \varkappa=1,\dots,p-1\}$, *then*

$$S_{nk}(\omega^{m+1}\psi^u) \equiv -p^{-n-1}\textstyle\sum_{i=0}^{s-1}[r_n(ip^n+k)-r_n(ip^n+k-d_n)]\alpha^{m(i+k)} \bmod \mathfrak{p}$$

$(k=0,\dots,p^n-1)$, *where* d_n *is defined by*

$$l \equiv r_n(d_n) \bmod p^{n+1}\,. \tag{10.2}$$

Proof. For simplicity we shall here omit subscripts and set $r(i)=r_n(i), c(i,j)=c_n(i,j)$. Moreover, put $i'=ip^n+k$.

We apply first the equations $\alpha^{ms}=-1$ and $\beta^{ut}=1$ and write the double sum appearing in lemma 9 in the form

$$\begin{aligned}\textstyle\sum_{i=0}^{s-1}\sum_{j=0}^{t-1}&[c(i',j)-c(i'+sp^n,j)+c(i',j+t)-c(i'+sp^n,j+t)]\alpha^{m(i+k)}\beta^{uj}\\ &= 2\textstyle\sum_{i=0}^{s-1}\sum_{j=0}^{t-1}[c(i',j)+c(i',j+t)-q_n]\alpha^{m(i+k)}\beta^{uj}\,.\end{aligned}$$

Next we use the fact that β^u satisfies also the equation $x^{t-1}+x^{t-2}+\dots+1=0$. Then we arrive at

$$S_{nk}(\theta) = -q_n{}^{-1}\textstyle\sum_{i=0}^{s-1}\sum_{j=0}^{t-2}C(i,j)\alpha^{m(i+k)}\beta^{uj}\,,$$

where

$$C(i,j) = c(i',j)+c(i',j+t)-c(i',t-1)-c(i',2t-1) \equiv 0 \bmod q_n\,.$$

Observe now that β^u is a root of unity whose order is p. Therefore $\beta^u\equiv 1 \bmod \mathfrak{p}$ and so

$$S_{nk}(\theta) \equiv -q_n{}^{-1}\textstyle\sum_{i=0}^{s-1}C_i\alpha^{m(i+k)} \bmod \mathfrak{p} \tag{10.3}$$

with

$$C_i = \textstyle\sum_{j=0}^{l-2}c(i',j)-t[c(i',t-1)+c(i',2t-1)] \quad (i = 0,\dots,s-1). \tag{10.4}$$

The definition of $d=d_n$ implies that $lr(i'-d)\equiv r(i') \bmod p^{n+1}$. Hence we can deduce that

$$\textstyle\sum_{j=0}^{l-2}c(i',j) = \sum_{a=0}^{l-1}[r(i')+ap^{n+1}]-lr(i'-d) = ltp^{n+1}+l[r(i')-r(i'-d)]\,.$$

Furthermore, the sum $c(i',t-1)+c(i',2t-1)$, being divisible by l and congruent to $2r(i') \bmod p^{n+1}$, must be of the form $2lr(i'-d)+N_ilp^{n+1}$, where N_i is an integer. Substituting these results into (10.4) and noting that $t \equiv 0 \bmod p$ we get

$$C_i \equiv l[r(i') - r(i'-d)] - 2ltr(i'-d) \bmod p^{n+2} .$$

From this and (10.3) it is seen that one has only to show that

$$\sum_{i=0}^{s-1} r(i'-d)\alpha^{mi} \equiv 0 \bmod p^{n+1} . \tag{10.5}$$

To prove (10.5), observe that the congruence $\omega(a) \equiv a \bmod p$ yields

$$\alpha^h = r^h \bmod p; \qquad \alpha^h = \alpha^{hp^n} \equiv r^{hp^n} \bmod p^{n+1}$$

for any integer h. Thus we obtain

$$\sum_{i=0}^{s-1} r^{ip^n}\alpha^{mi} \equiv \sum_{i=0}^{s-1} r^{(m+1)ip^n} \equiv 0 \bmod p^{n+1} ,$$

and the desired congruence follows.

Remark. If $l \equiv 1 \bmod p^{n+1}$, lemma 10 enables us to conclude that

$$S_{nk}(\theta) \equiv 0 \bmod \mathfrak{p} \qquad (k = 0,\ldots,p^n - 1)$$

for the characters θ in question. Consequently, the situation in this case seems quite different from the case where $m_0 = 1$: when l is suitably chosen the congruences of lemma 5 are satisfied for $0 \leqq n \leqq N$ with an arbitrarily large N (cf. remark (ii) in section 8).

11. Relationship between $\mu^-(p)$ and $\mu^-(lp)$.

We shall prove the following

Theorem 3. *Let p and l be primes, $l \equiv 1 \bmod p$. If $\mu_\theta(p) > 0$ for some $\theta \in X(p)$, then there is a character φ in $X(lp)$ with $f_\varphi = lp$ such that $\mu_\varphi(lp) > 0$.*

Proof. The assumption $\mu_\theta(p) > 0$ implies that p is irregular and so, in particular, $p > 3$ and $l > 3$. Let $\theta = \omega^{m+1}$. Using the preceding notations we may then state, by lemma 8 and the remark at the end of section 9, that

$$\sum_{i=0}^{s-1} r_n(ip^n + h)\alpha^{mi} \equiv p^{n+1}(1-\alpha^m)^{-1} \bmod p^{n+2} \tag{11.1}$$

for all $n \geqq 0$ and all integers h.

Denote the left hand side of (11.1) by $T_n(h)$. It follows from lemma 10 that if $\varphi = \omega^{m+1}\psi^u$ with certain values of u, then

$$S_{nk}(\varphi) \equiv -p^{-n-1}(T_n(k) - T_n(k-d_n))\alpha^{mk} \bmod \mathfrak{p}$$

for all $n \geqq 0$ and all $k, 0 \leqq k \leqq p^n - 1$. Comparing this with (11.1) we infer that

$$S_{nk}(\varphi) \equiv 0 \bmod \mathfrak{p}$$

(for these n and k) and accordingly, by lemma 5, $\mu_\varphi(lp) > 0$. As $f_\varphi = lp$, the theorem is proved.

COROLLARY. *Let $\mu^-(p) > 0$. If m_0 is divisible by N different primes $\equiv 1 \bmod p$, then $\mu^-(m_0 p) > N$.*

PROOF. Obviously, it suffices to prove that $\mu^-(lp) > 1$ when $l \equiv 1 \bmod p$. But this is an immediate consequence of the above theorem, because lemma 1 gives us the estimate

$$\mu^-(lp) \geqq \mu^-(p) + e^{-1} \textstyle\sum_{f\theta = lp} \mu_\theta(lp) .$$

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York and London, 1966.
2. K. Iwasawa, *On some invariants of cyclotomic fields*, Amer. J. Math. 80 (1958), 773–783. *Erratum*, ibid. 81 (1959), 280.
3. K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), 183–226.
4. K. Iwasawa, *On the μ-invariants of cyclotomic fields*, Acta Arith. 21 (1972), 99–101.
5. K. Iwasawa, *Lectures on p-adic L-functions*, (Annals of Mathematics Studies 74), Princeton University Press, Princeton, 1972.
6. K. Iwasawa and C. Sims, *Computation of invariants in the theory of cyclotomic fields*, J. Math. Soc. Japan 18 (1966), 86–96.
7. W. Johnson, *On the vanishing of the Iwasawa invariant μ_p for $p < 8000$*, Math. Comp. 27 (1973), 387–396.
8. W. Johnson, *Irregular prime divisors of the Bernoulli numbers*, Math. Comp. 28 (1974), 653–657.
9. W. Johnson, *The irregular primes to 30000 and related tables*, Copy deposited in the UMT File, June 1974.
10. W. Johnson, *Irregular primes and cyclotomic invaiiants*, Math. Comp. 29 (1975), 113–120.
11. W. Johnson, *p-Adic proofs of congruences for the Bernoulli numbers*, J. Number Theory 7 (1975), 251–265.
12. T. Metsänkylä, *Über den ersten Faktor der Klassenzahl des Kreiskörpers*, Ann. Acad. Sci. Fenn., Ser. A I 416 (1967), 48 pp.
13. T. Metsänkylä, *Class numbers and μ-invariants of cyclotomic fields*, Proc. Amer. Math. Soc. 43 (1974), 299–300.

UNIVERSITY OF TURKU, FINLAND