ACTA ARITHMETICA
LXXV.3 (1996)

Kummer type congruences and Stickelberger subideals

by

Takashi Agoh (Chiba) and Ladislav Skula (Brno)

1. Introduction. Let l be an odd prime, B_m the *Bernoulli number* defined by

$$\frac{X}{e^X - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} X^m$$

and $\varphi_k(X)$ the *Mirimanoff polynomial*, i.e.,

$$\varphi_k(X) = \sum_{v=1}^{l-1} v^{k-1} X^v \quad (k \in \mathbb{Z}).$$

In 1857, Kummer [11] considered the following system of congruences in connection with the first case of Fermat's last theorem:

$$\text{(K)} \qquad \begin{cases} \varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ B_{2m}\varphi_{l-2m}(t) \equiv 0 \pmod{l} \quad (1 \le m \le (l-3)/2). \end{cases}$$

This system has many kinds of interesting variations and consequences (see, e.g., Agoh [2, 3], Fueter [7] and Ribenboim [13]). In the papers of Skula [16, 17] the equivalent system to (K) was introduced by means of the Stickelberger ideal in a certain group ring.

We now consider the special system of congruences as follows:

$$\text{(K}(N)\text{)} \qquad \begin{cases} \varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ \frac{1-N^{2m}}{2m} B_{2m}\varphi_{l-2m}(t) \equiv 0 \pmod{l} \quad (1 \le m \le (l-3)/2), \end{cases}$$

where N is a fixed positive integer with $2 \le N \le l-1$.

It is clear that all the solutions of (K) satisfy (K(N)). In addition, we can see that if N is a primitive root mod l, then each solution of (K(N)) is

The first author was supported in part by a grant of the Ministry of Education, Science and Culture of Japan.

Research of the second author was supported by the Grant Agency of the Czech Republic, Number Theory, its Algebraic Aspect and its Relationship to Computer Science, No. 201/93/2122.

also a solution of (K), which implies that the systems (K) and (K(N)) are equivalent in this case.

The main purpose of this paper is to introduce some equivalent systems to (K(N)) and investigate subideals of the Stickelberger ideal relating to these systems.

Section 2 contains general notations which will be needed throughout the whole paper. In Section 3 we shall present a certain polynomial equality (Proposition 3.2), in which all the terms in the system (K(N)) are involved. By making use of this equality we shall derive some systems of congruences equivalent to (K(N)) (Theorems 3.3, 3.4 and Proposition 3.5). In Section 4, we define a special matrix K_N (Definition 4.2) which is related to the modified Dem'yanenko matrix and give an explicit formula (Theorem 4.4) for $\det K_N$ by means of the first factor h^- of the class number of the lth cyclotomic field $\mathbb{Q}(\zeta_l)$ (where $\zeta_l = e^{2\pi i/l}$) over the field $\mathbb{Q}$ of rational numbers. This formula will be proved in Section 5 using Sinnott's Lemma (Lemma 5.4). Proposition 4.5 is used for the determination of the sign of $\det K_N$.

Section 5 deals with a special ideal $\mathcal{B}_N$ which is contained in the Stickelberger ideal $\mathcal{I}$ of the group ring $\mathbb{Z}[G]$, where G is a cyclic group of order $l-1$. First, the group indices $[R' : \mathcal{B}_N]$ and $[\mathcal{I} : \mathcal{B}_N]$ are evaluated by constructing a $\mathbb{Z}$-basis of $\mathcal{B}_N$, where R' is a special subring of $\mathbb{Z}[G]$ (Theorem 5.8). Here, again Sinnott's Lemma plays a central role. Subsequently, we define a special system of congruences by means of $\mathcal{B}_N$ and show in Theorem 5.10 that it is equivalent to the system (V) mentioned in Proposition 3.5.

When $N = 2$, our matrix K_N is related to the matrix H considered by Hazama [8], which is essentially a modified Dem'yanenko matrix $D'(l)$ for $l \geq 5$ from the paper of Folz and Zimmer [6].

We note that in his recent paper ([9], Section 5) Hazama deals with an analogous $(0, 1)$ square matrix whose determinant is connected with the first factor of the class number of the pqth cyclotomic field $\mathbb{Q}(\zeta_{pq})$, where p, q are distinct odd primes.

A generalization of the Dem'yanenko matrix associated with an arbitrary abelian field of odd prime power conductor is introduced by Sands and Schwarz [14].

The ideal $\mathcal{B}_N$ for $N = 2$ was recently investigated by Skula [18]. The corresponding system of congruences with $\mathcal{B}_2$ is equivalent to that of Benneton introduced in [4] (see Skula [18], Theorem 5.3).

2. General notation. We list some general notations which will be used throughout this paper:

- $\#S$ — the number of elements of a set S,
- $\mathbb{Z}$ — the ring of rational integers,

- l — an odd prime,
- N — any fixed integer with $2 \le N \le l-1$,
- $\overline{z}$ — the least non-negative residue of $z \in \mathbb{Z}$ modulo l, i.e.,

$$\overline{z} \in \mathbb{Z} \quad \text{with} \quad z \equiv \overline{z} \pmod{l}, \qquad 0 \le \overline{z} \le l-1,$$

- $[x]$ — the greatest integer $\le x$ for a real number x, i.e.,

$$[x] \in \mathbb{Z} \quad \text{with} \quad [x] \le x < [x]+1,$$

- B_m — the mth Bernoulli number in the "*even suffix*" notation, hence

$$B_0 = 1, \quad B_1 = -1/2, \quad B_2 = 1/6, \quad B_3 = 0, \ \ldots,$$

- $S_m(k) = 1^m + 2^m + \ldots + k^m$ $(m, k \in \mathbb{Z},\ m \ge 0,\ k \ge 1)$,
- $\varphi_m(X) = \sum_{v=1}^{l-1} v^{m-1} X^v$ $(m \in \mathbb{Z})$, the Mirimanoff polynomial,
- $q_l(a) = \frac{a^{l-1}-1}{l}$ $(a \in \mathbb{Z},\ l \nmid a)$, the Fermat quotient of l with base a,
- $i(l) = \#\{k \mid B_{2k} \equiv 0 \pmod{l},\ 1 \le k \le (l-3)/2\}$, the irregularity index of l,
- r — a primitive root mod l,
- r_i — the least positive residue of r^i $(i \in \mathbb{Z})$ modulo l, i.e.,

$$r_i \in \mathbb{Z} \quad \text{with} \quad r^i \equiv r_i \pmod{l},\ 1 \le r_i \le l-1,$$

- $\operatorname{ind} x$ — the index of $x \in \mathbb{Z}$, $l \nmid x$, relative to the primitive root r mod l, i.e.,

$$x \equiv r^{\operatorname{ind} x} \pmod{l}, \qquad 0 \le \operatorname{ind} x \le l-2,$$

- $\mathbb{Q}(\zeta_l)$ — the cyclotomic field defined by a primitive lth root of unity $\zeta_l = e^{2\pi i/l}$ over the field $\mathbb{Q}$ of rational numbers,
- h^- — the first factor of the class number of $\mathbb{Q}(\zeta_l)$.

All other notations will be defined as they arise.

3. Some systems equivalent to (K(N))**.** The purpose of this section is to introduce various systems of congruences equivalent to the system (K(N)) by using a certain polynomial equality.

Throughout this section, we denote

$$B_m^{(N)} = \frac{1-N^m}{m} B_m \qquad (m \ge 1),$$

$$S_m(k;N) = S_m(kN) - N^{m+1} S_m(k) \qquad (m \ge 0,\ k \ge 1),$$

$$B(X) = \frac{X}{e^X - 1} \quad \text{(the generating function of Bernoulli numbers)},$$

$$W_N(X) = \frac{e^{(N-2)X} + 2e^{(N-3)X} + \ldots + (N-1)}{e^{(N-1)X} + e^{(N-2)X} + \ldots + 1},$$

$$\alpha_N(l) = \#\{k \mid B_{2k}^{(N)} \equiv 0 \pmod{l},\ 1 \le k \le (l-3)/2\}.$$

If $\eta(N)$ is the number of non-trivial congruences in the system (K(N)), then we obviously have

$$\eta(N) \le \frac{l-1}{2} - \alpha_N(l) \le \frac{l-1}{2} - i(l).$$

Here we note that if N is a primitive root mod l, then $\alpha_N(l) = i(l)$, hence $\eta(N)$ is equal to the number of non-trivial congruences in the system (K).

First we shall show the following functional identity:

Proposition 3.1. *Let m be an integer and k be a positive integer. If t and X are two independent variables, then*

$$\{1 - N + W_N(X)\}\varphi_{m+1}(te^{kNX}) - \varphi_{m+1}(t)W_N(X) = \sum_{v=1}^{l-1}\Big\{\sum_{j=0}^{vkN} e^{jX} - N\sum_{j=0}^{vk} e^{jNX}\Big\}v^m t^v.$$

P r o o f. We let

$$A_{k,m}(t,X) = \{B(X)e^X\}\varphi_{m+1}(te^{kX}) - \varphi_{m+1}(t)B(X),$$

and consider the identity

$$A_{k,m}(t,X) = X\sum_{v=1}^{l-1}\Big\{\sum_{j=0}^{vk} e^{jX}\Big\}v^m t^v \quad \text{(cf. [2], (3.3))}.$$

Since

$$\frac{1}{X}\{B(X)e^X - B(NX)e^{NX}\} = \frac{1}{X}\{(1-N)X + B(X) - B(NX)\} = 1 - N + W_N(X)$$

and

$$W_N(X) = \frac{1}{X}\{B(X) - B(NX)\},$$

it follows that

$$\begin{aligned} &A_{kN,m}(t,X) - A_{k,m}(t,NX)\\ &\quad = \{(B(X)e^X)\varphi_{m+1}(te^{kNX}) - \varphi_{m+1}(t)B(X)\}\\ &\qquad - \{(B(NX)e^{NX})\varphi_{m+1}(te^{kNX}) - \varphi_{m+1}(t)B(NX)\}\\ &\quad = \{B(X)e^X - B(NX)e^{NX}\}\varphi_{m+1}(te^{kNX}) - \varphi_{m+1}(t)\{B(X) - B(NX)\}\\ &\quad = X\{1 - N + W_N(X)\}\varphi_{m+1}(te^{kNX}) - \varphi_{m+1}(t)\{XW_N(X)\}, \end{aligned}$$

which gives the identity indicated in the proposition. ∎

Using this proposition we can deduce a polynomial equality including all the terms in the system (K(N)).

PROPOSITION 3.2. *Let m and k be integers with $m \le l-3$ and $k \ge 1$. Then*

$$\frac{1-N}{2}(kN)^{l-2-m}\varphi_{l-1}(t) + \sum_{i=1}^{l-3-m}\binom{l-2-m}{i}(kN)^{l-2-m-i}\{B_{i+1}^{(N)}\varphi_{l-i-1}(t)\} = \sum_{v=1}^{l-1} S_{l-2-m}(vk;N)v^m t^v.$$

P r o o f. For $n \ge 0$ we have

$$\left[\frac{d^n}{dX^n}\varphi_{m+1}(te^{kNX})\right]_{X=0} = (kN)^n\varphi_{m+n+1}(t)$$

and

$$\left[\frac{d^n}{dX^n}W_N(X)\right]_{X=0} = B_{n+1}^{(N)} \quad \text{(cf. [1], Lemma)},$$

which leads to the desired equality using Leibniz's theorem for the functional identity given in Proposition 3.1. ∎

Next, we shall discuss some systems of congruences equivalent to (K(N)).

THEOREM 3.3. *Let τ be an integer. Then τ is a solution of* (K(N)) *if and only if τ is a solution of any one of the following systems of congruences*:

(I) $$\sum_{v=1}^{l-1} S_{l-3}(vk;N)vt^v \equiv 0 \pmod{l} \quad (1 \le k \le l-1),$$

(II) $$\sum_{v=1}^{l-1} S_{l-2}(vk;N)t^v \equiv 0 \pmod{l} \quad (1 \le k \le l-1),$$

(III$_k$) $$\begin{cases} \varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ \displaystyle\sum_{v=1}^{l-1} S_{l-2-m}(vk;N)v^m t^v \equiv 0 \pmod{l} \quad (2 \le m \le l-3; \\ \qquad\qquad k \text{ is any fixed integer with } 1 \le k \le l-1). \end{cases}$$

P r o o f. For a fixed integer N with $2 \le N \le l-1$ we suppose that τ is a solution of (K(N)). Then we see from Proposition 3.2 that τ is a solution of

(1) $$\sum_{v=1}^{l-1} S_{l-2-m}(vk;N)v^m t^v \equiv 0 \pmod{l} \quad (1 \le k \le l-1;\ 0 \le m \le l-3).$$

This shows that the solution τ of (K(N)) satisfies (I), (II) and (III$_k$). Conversely, if τ is a solution of (1) for certain k and m ($1 \le k \le l-1, 0 \le m \le l-3$), then we know from Proposition 3.2 that τ is a solution of the congruence

$$(2)\quad \frac{1-N}{2}(kN)^{l-2-m}\varphi_{l-1}(t) + \sum_{i=1}^{l-3-m}\binom{l-2-m}{i}(kN)^{l-2-m-i}\{B_{i+1}^{(N)}\varphi_{l-i-1}(t)\} \equiv 0 \pmod{l}.$$

For a fixed integer m with $0 \le m \le l-3$, let $D = [a_{ij}]_{1\le i,j\le l-2-m}$ be the square matrix with $a_{ij} = i^j$. Then it is easy to show that $\det D \not\equiv 0 \pmod{l}$, since $\det D$ is of Vandermonde type. Hence if τ is a solution of (I) or (II), then τ is also a solution of (K(N)). On the other hand, for a fixed integer k with $1 \le k \le l-1$, take successively $m = l-3, l-5, \dots, 2$ in (2). Then we can easily infer that τ is a solution of (K(N)). This completes the proof of the theorem. ∎

THEOREM 3.4. *Let τ be an integer. Then τ is a solution of* (K(N)) *if and only if τ is a solution of the system of congruences*

$$(\mathrm{IV})\quad \sum_{v=1}^{l-1} S_{l-1}(vk;N)\frac{1}{v}t^v \equiv kNq_l(N)\varphi_1(t) \pmod{l} \quad (1 \le k \le l-1).$$

Proof. Take $m = -1$ in the equality of Proposition 3.2. By the von Staudt–Clausen theorem $B_{l-1}^{(N)} \equiv -q_l(N) \pmod{l}$, hence we obtain the result by the same arguments as in the proof of Theorem 3.3. ∎

PROPOSITION 3.5. *Let τ be an integer with $\tau \not\equiv 1 \pmod{l}$. Then τ is a solution of* (K(N)) *if and only if τ is a solution of the system of congruences*

$$(\mathrm{V})\quad \sum_{v=1}^{l-1}\left(\left[\frac{kNv}{l}\right] - N\left[\frac{kv}{l}\right]\right)\frac{1}{v}t^v \equiv 0 \pmod{l} \quad (1 \le k \le l-1).$$

Proof. By Fermat's little theorem we have

$$\begin{aligned} S_{l-1}(vk;N) &= S_{l-1}(vkN) - N^l S_{l-1}(vk) \\ &\equiv \left(vkN - \left[\frac{vkN}{l}\right]\right) - N\left(vk - \left[\frac{vk}{l}\right]\right) \\ &\equiv -\left(\left[\frac{vkN}{l}\right] - N\left[\frac{vk}{l}\right]\right) \pmod{l}. \end{aligned}$$

If $\tau \not\equiv 1 \pmod{l}$, then $\varphi_1(\tau) = (\tau^l - \tau)/(\tau - 1) \equiv 0 \pmod{l}$. Hence the result clearly follows from Theorem 3.4. ∎

In Section 5 we will derive a system of congruences equivalent to (V) by

means of a special subideal $\mathcal{B}_N$ of the Stickelberger ideal (see Theorem 5.10 below).

R e m a r k 3.6. (a) In 1922, Fueter ([6], (VI)) considered the following system of congruences:

$$\text{(F)} \qquad \sum_{v=1}^{l-1} \left[\frac{av}{l}\right] \frac{1}{v} t^v \equiv 0 \pmod{l} \quad (1 \le a \le l-1).$$

Obviously, each integer $\tau \not\equiv 1 \pmod{l}$ satisfying (F) is also a solution of (V). On the other hand, putting $a = l-1$ we see immediately that no integer $\tau \equiv 1 \pmod{l}$ is a solution of (F).

(b) Clearly, each integer $\tau \equiv 1 \pmod{l}$ is a solution of the Kummer system (K) and hence also of the system (K(N)) for each N ($2 \le N \le l-1$).

Using Theorem 3.4 and the expression for $S_{l-1}(vk; N)$ given in the proof of Proposition 3.5 we get

$$kNq_l(N) \equiv \sum_{v=1}^{l-1} \left(\left[\frac{vkN}{l}\right] - N\left[\frac{vk}{l}\right] \right) \frac{1}{v} \pmod{l}$$

for each integer k ($1 \le k \le l-1$).

This formula can also be derived from Lerch's expression ([12], (8)) for the Fermat quotient as follows:

$$q_l(a) \equiv \sum_{v=1}^{l-1} \left[\frac{va}{l}\right] \frac{1}{va} \pmod{l} \quad (a \in \mathbb{Z},\ l \nmid a).$$

In fact, from the "logarithmic property" of the Fermat quotient it follows that

$$\begin{aligned} kNq_l(N) &\equiv kN\{q_l(kN) - q_l(k)\} \\ &\equiv \sum_{v=1}^{l-1} \left[\frac{vkN}{l}\right] \frac{1}{v} - N \sum_{v=1}^{l-1} \left[\frac{vk}{l}\right] \frac{1}{v} \\ &\equiv \sum_{v=1}^{l-1} \left(\left[\frac{vkN}{l}\right] - N\left[\frac{vk}{l}\right] \right) \frac{1}{v} \pmod{l}. \end{aligned}$$

Thus, we may conclude that each integer $\tau \equiv 1 \pmod{l}$ is a solution of (V) if and only if $q_l(N) \equiv 0 \pmod{l}$.

4. The determinant of K_N. In this section we shall define a special matrix K_N and deduce the formula for its determinant by means of the first factor h^- of the class number of $\mathbb{Q}(\zeta_l)$.

Let f be the order of N mod l. Put

$$\omega(N) = \begin{cases} (N^{f/2}+1)^{(l-1)/f} & \text{if } f \text{ is even,} \\ (N^f-1)^{(l-1)/(2f)} & \text{if } f \text{ is odd.} \end{cases}$$

In [8] Hazama introduced the square matrix $H = [h_{ij}]_{1\le i,j\le (l-1)/2}$ defined by

$$h_{ij} = \begin{cases} 0 & \text{if } \overline{ij} > l/2, \\ 1 & \text{if } \overline{ij} < l/2. \end{cases}$$

This (0, 1) matrix H is regarded as a modified Dem'yanenko matrix $D'(l)$ for $l \ge 5$ considered by Folz and Zimmer ([6]). Hazama evaluated the determinant of H:

THEOREM 4.1.

$$\det H = (-1)^{[(l-1)/4]} \frac{\omega(2)}{l} h^-.$$

We now define a new square matrix K_N of order $(l-1)/2$ as follows:

DEFINITION 4.2.

$$K_N = [k_{ij}]_{1\le i,j\le (l-1)/2}, \qquad k_{ij} = \nu - (N-1)/2,$$

where ν is an integer such that

$$\nu l/N < \overline{ij} < (\nu+1)l/N,$$

hence $\nu = [\overline{ij}N/l]$.

We note that the entries of H are either 0 or 1, however, those of K_2 are either $-1/2$ or $1/2$. Also, the first rows of H and K_2 are, respectively,

$$[1, 1, \ldots, 1] \quad \text{and} \quad \left[-\tfrac{1}{2}, -\tfrac{1}{2}, \ldots, -\tfrac{1}{2}\right].$$

From Theorem 4.1 we deduce

PROPOSITION 4.3.

$$\det K_2 = (-1)^{(l-1)/2+[(l-1)/4]} \frac{\omega(2)}{2l} h^-.$$

P r o o f. We perform the following row operations to the matrix H:

(a) multiply the first row by $-1/2$ and add it to the others,
(b) multiply all rows by -1,
(c) multiply the first row by $-1/2$.

Then we easily see that $\det H = (-1)^{(l-1)/2} 2 \det K_2$, which leads to the conclusion in view of Theorem 4.1. ∎

The following theorem is a generalization of Theorem 4.1 and hence of Proposition 4.3. In Section 5 we shall give the proof of this theorem using Proposition 5.5.

THEOREM 4.4.

$$\det K_N = (-1)^{(l^2-1)/8}\frac{\omega(N)}{2l}h^-.$$

For the determination of the sign of $\det K_N$ we need the following

PROPOSITION 4.5. *Suppose that a_{uv} are complex numbers satisfying*

$$a_{u+(l-1)/2,v} = a_{u,v+(l-1)/2} = -a_{uv}$$

for all integers u, v. Let $A = [a_{uv}]_{0\le u,v\le (l-3)/2}$ and $D = [d_{xy}]_{1\le x,y\le (l-1)/2}$ with $d_{xy} = a_{\operatorname{ind} x, -\operatorname{ind} y}$. Then

$$\det D = (-1)^{(l-1)(l-3)/8}\det A.$$

P r o o f. I. For integers u and v put

$$c_{uv} = \begin{cases} a_{uv} & \text{if } r_u, r_{-v} < l/2 \text{ or } r_u, r_{-v} > l/2,\\ -a_{uv} & \text{otherwise,}\end{cases}$$

and consider the matrix $C = [c_{uv}]_{0\le u,v\le (l-3)/2}$. Then for $u, v \in \mathbb{Z}$ we have

$$c_{u+(l-1)/2,\,v} = c_{u,\,v+(l-1)/2} = c_{uv},$$

and therefore

$$\det C = (-1)^{(l-3)/2}\det A.$$

II. For an integer w with $0 \le w \le (l-3)/2$ let $\varphi(w) = \operatorname{ind}(w+1)$ or $\varphi(w) = \operatorname{ind}(w+1) - (l-1)/2$ such that $0 \le \varphi(w) \le (l-3)/2$. Also, let $\psi(0) = 0$ and $\psi(w) = (l-1)/2 - w$ for $w \in \mathbb{Z}$, $1 \le w \le (l-3)/2$. Then φ, ψ and $\pi = \psi \circ \varphi$ are permutations of the set $\{0, 1, \dots, (l-3)/2\}$.

Since $d_{xy} = c_{\operatorname{ind} x, -\operatorname{ind} y}$ for $x, y \in \mathbb{Z}$ $(1 \le x, y \le (l-1)/2)$, we get $d_{u+1,\,v+1} = c_{\varphi(u),\,\pi(v)}$ for integers u, v $(0 \le u, v \le (l-3)/2)$, hence

$$\det D = (-1)^{\varepsilon(l)}\det C,$$

where

$$\varepsilon(l) = \begin{cases} (l-3)/4 & \text{when } (l-3)/2 \text{ is even,}\\ (l-5)/4 & \text{when } (l-3)/2 \text{ is odd.}\end{cases}$$

Since

$$\varepsilon(l) + \frac{l-3}{2} \equiv \frac{(l-1)(l-3)}{8} \pmod 2,$$

the result follows. ∎

5. The ideal $\mathcal{B}_N$. In this section we deal with a special ideal $\mathcal{B}_N$ of the group ring $R = \mathbb{Z}[G]$, which is contained in the Stickelberger ideal $\mathcal{I}$ for the lth cyclotomic field $\mathbb{Q}(\zeta_l)$.

We write:

• $G = \{1, s, s^2, \dots, s^{l-2}\}$, a multiplicative cyclic group of order $l-1$ with generator s,

• $R = \mathbb{Z}[G]$, the group ring of G over $\mathbb{Z}$; hence each element of R is of the form $\alpha = \sum_{i=0}^{l-2} a_i s^i$ $(a_i \in \mathbb{Z})$,

• $$R' = \Big\{\alpha = \sum_{i=0}^{l-2} a_i s^i \in R \mid a_j + a_{j+(l-1)/2} = a_k + a_{k+(l-1)/2} \quad \text{for each } j,\, k \in \mathbb{Z} \text{ with } 0 \le j, k \le (l-3)/2\Big\}$$
$$= \Big\{\alpha \in R \mid (1 + s^{(l-1)/2})\alpha \in \mathbb{Z} \cdot \sum_{i=0}^{l-2} s^i\Big\}, \quad \text{a subring of } R,$$

• $\varepsilon_h = s^h(1 - s^{(l-1)/2})$ for $h \in \mathbb{Z}$,

• $\varepsilon = \sum_{i=0}^{(l-3)/2} s^i$,

• $S' = \{\varepsilon_h \mid 0 \le h \le (l-3)/2\} \cup \{\varepsilon\}$, a basis of R' considered as a $\mathbb{Z}$-module,

• $\gamma = \sum_{i=0}^{l-2} r_{-i} s^i \in R'$,

• $\mathcal{I} = \{\alpha \in R \mid \exists \beta \in R \text{ such that } l\alpha = \beta\gamma\} \subseteq R'$, the Stickelberger ideal of R,

• $\gamma_k = \sum_{i=0}^{l-2} \frac{1}{l}(r_{-i}r_k - r_{-i+k})s^i = \sum_{i=0}^{l-2} \left[\frac{r_{-i}r_k}{l}\right] s^i \in R'$ for $k \in \mathbb{Z}$,

• $\delta = \sum_{i=0}^{l-2} s^i$, a special element from R corresponding to the norm of $\mathbb{Q}(\zeta_l)$.

The elements γ_k $(k \in \mathbb{Z})$ of R were used in Fueter's paper ([7], Section 8) to derive a special system of congruences (see Remark 3.6(a)). The elements γ_k, γ and δ belong to the Stickelberger ideal $\mathcal{I}$ of R and satisfy, for each $k \in \mathbb{Z}$,

$$\gamma_k + \gamma_{k+(l-1)/2} = \gamma - \delta.$$

Since $\gamma_{(l-1)/2} = \gamma - \delta$, we get the following theorem from the result by Skula ([17], Theorem 2.7):

THEOREM 5.1. *The system*

$$\{\gamma_k \mid 1 \le k \le (l-1)/2\} \cup \{\delta\}$$

forms a basis of the Stickelberger ideal $\mathcal{I}$ considered as a $\mathbb{Z}$-module.

For a fixed integer N with $2 \le N \le l-1$, we let $N = r_n$ $(1 \le n \le l-2)$ and put for simplicity

$$\beta = \gamma_n = \sum_{i=0}^{l-2} \left[\frac{Nr_{-i}}{l}\right] s^i.$$

Then it is easy to show the following

PROPOSITION 5.2. *Let j be an integer. Then*

$$s^j\beta = \sum_{i=0}^{l-2} \left[\frac{Nr_{-i+j}}{l}\right] s^i \quad \textit{and} \quad s^j\beta + s^{j+(l-1)/2}\beta = (N-1)\delta.$$

DEFINITION 5.3. Denote by $\mathcal{B}_N$ the ideal of R generated by β and δ, thus

$$\mathcal{B}_N = \Big\{ \sum_{j=0}^{l-2} b_j s^j\beta + b\delta \,\Big|\, b_j, b \in \mathbb{Z} \Big\} \subseteq \mathcal{I}.$$

We see from Proposition 5.2 that the elements of the system $\{s^j\beta \mid 0 \le j \le (l-3)/2\} \cup \{\delta\}$ are generators of the $\mathbb{Z}$-module $\mathcal{B}_N$.

For an element ξ of the group ring $\mathbb{Q}[G]$ of the cyclic group G over the rational number field $\mathbb{Q}$, there exist rational numbers x_{hk} $(0 \le h, k \le (l-3)/2)$ such that

$$\varepsilon_h\xi = \sum_{k=0}^{(l-3)/2} x_{hk}\varepsilon_k \quad \text{for each } h \text{ with } 0 \le h \le (l-3)/2.$$

Define

$$M(\xi) = [x_{hk}]_{0\le h,\, k\le (l-3)/2}, \qquad D(\xi) = \det M(\xi).$$

Note that $M(\xi)$ is a skew circulant matrix (cf. [5], 3.2.1).

For the proof of Proposition 5.5 stated below, we formulate Sinnott's Lemma ([15], Lemma 1.2(b)) as follows:

LEMMA 5.4. *Let $\xi = \sum_{i=0}^{l-2} x_i s^i \in \mathbb{Q}[G]$ $(x_i \in \mathbb{Q})$ and let X^- be the set of all odd characters of G. Then*

$$D(\xi) = \prod_{\chi\in X^-} \sum_{i=0}^{l-2} x_i\chi(s)^i.$$

(This lemma can also be proved directly by using a skew circulant matrix. See Davis [5], 3.2.1, Proposition 6.)

PROPOSITION 5.5.

$$D(\beta) = (-1)^{(l-1)/2} 2^{(l-3)/2} \frac{\omega(N)}{l} h^-.$$

P r o o f. For a real number θ, we write $\langle\theta\rangle$ for the fractional part of θ (i.e., $\langle\theta\rangle = \theta - [\theta]$). Let $B_{1,\chi}$ denote the generalized first Bernoulli number for an odd character χ of G, hence

$$B_{1,\chi} = \frac{1}{l} \sum_{a=1}^{l-1} \chi(a)a.$$

Then it is well known that h^- can be expressed as

$$h^- = 2l \prod_{\chi\in X^-}\Big(-\frac{1}{2}B_{1,\chi}\Big).$$

Also, we easily see that

$$\sum_{a=1}^{l-1}\Big\langle\frac{Na}{l}\Big\rangle\overline{\chi}(a) = \frac{\chi(N)}{l}\sum_{a=1}^{l-1}\overline{\chi}(a)a$$

and

$$\prod_{\chi\in X^-}(N-\chi(N)) = \omega(N),$$

where $\overline{\chi}$ is the conjugate character of χ. By Lemma 5.4, we obtain

$$\begin{aligned}
D(\beta) &= \prod_{\chi\in X^-}\sum_{i=0}^{l-2}\Big[\frac{Nr_{-i}}{l}\Big]\chi(s)^i = \prod_{\chi\in X^-}\sum_{a=1}^{l-1}\Big[\frac{Na}{l}\Big]\overline{\chi}(a)\\
&= \prod_{\chi\in X^-}\sum_{a=1}^{l-1}\Big(\frac{Na}{l}-\Big\langle\frac{Na}{l}\Big\rangle\Big)\overline{\chi}(a)\\
&= \prod_{\chi\in X^-}(N-\chi(N))\cdot\prod_{\chi\in X^-}\frac{1}{l}\sum_{a=1}^{l-1}\chi(a)a\\
&= \omega(N)(-2)^{(l-1)/2}\prod_{\chi\in X^-}\Big(-\frac{1}{2}B_{1,\chi}\Big) = (-1)^{(l-1)/2}2^{(l-3)/2}\frac{\omega(N)}{l}h^-,
\end{aligned}$$

as desired. ∎

Now we are able to evaluate $\det K_N$:

Proof of Theorem 4.4. For integers u, v put

$$a_{uv} = \Big[\frac{Nr_{-u+v}}{l}\Big] - \frac{N-1}{2}.$$

Then $a_{u+(l-1)/2,v} = a_{u,v+(l-1)/2} = -a_{uv}$. By Proposition 5.2, it follows that for each integer h $(0 \le h \le (l-3)/2)$,

$$\begin{aligned}
\varepsilon_h\beta &= s^h\beta - s^{h+(l-1)/2}\beta = 2s^h\beta - (N-1)\delta\\
&= 2\sum_{k=0}^{(l-3)/2}\Big(\Big[\frac{Nr_{-k+h}}{l}\Big]s^k + \Big[\frac{Nr_{-k+h+(l-1)/2}}{l}\Big]s^{k+(l-1)/2}\Big)\\
&\quad + (N-1)\sum_{k=0}^{(l-3)/2}\varepsilon_k - 2(N-1)\varepsilon
\end{aligned}$$

$$= 2\sum_{k=0}^{(l-3)/2}\left[\frac{Nr_{-k+h}}{l}\right]\varepsilon_k + 2(N-1)\sum_{k=0}^{(l-3)/2} s^{k+(l-1)/2}$$
$$+ (N-1)\sum_{k=0}^{(l-3)/2}\varepsilon_k - 2(N-1)\varepsilon$$
$$= \sum_{k=0}^{(l-3)/2}\left(2\left[\frac{Nr_{-k+h}}{l}\right] - (N-1)\right)\varepsilon_k = 2\sum_{k=0}^{(l-3)/2} a_{kh}\varepsilon_k.$$

Since the entries k_{xy} $(1 \le x, y \le (l-1)/2)$ of K_N satisfy $k_{xy} = a_{-\operatorname{ind} y, \operatorname{ind} x}$, from Propositions 4.5 and 5.5 we get

$$\det K_N = (-1)^{(l-1)(l-3)/8}\det[a_{uv}]^T_{0\le u,v\le(l-3)/2}$$
$$= (-1)^{(l-1)(l-3)/8+(l-1)/2}\frac{\omega(N)}{2l}h^- = (-1)^{(l^2-1)/8}\frac{\omega(N)}{2l}h^-,$$

which completes the proof of Theorem 4.4. ∎

PROPOSITION 5.6. *Let $\xi \in R'$ and let M be the transition matrix from the basis S' of R' to the elements $s^j\xi$ $(0 \le j \le (l-3)/2)$ and δ. Then*

$$\det M = 2^{-(l-3)/2}D(\xi).$$

P r o o f. Assume that $\xi = \sum_{i=0}^{l-2} x_i s^i$, where $x_i \in \mathbb{Z}$ and $x_i + x_{i+(l-1)/2} = c \in \mathbb{Z}$ for each integer i $(0 \le i \le (l-1)/2)$. Let $M(\xi) = [x_{hk}]_{0\le h,k\le(l-3)/2}$ be the matrix defined above. Then for each $h \in \mathbb{Z}$ $(0 \le h \le (l-3)/2)$ we have

$$\varepsilon_h\xi = s^h\xi - s^{h+(l-1)/2}\xi = 2s^h\xi - c\delta.$$

Since

$$\delta = \sum_{i=0}^{l-2} s^i = -\sum_{k=0}^{(l-3)/2}\varepsilon_k + 2\varepsilon,$$

it follows that

$$s^h\xi = \frac{1}{2}(\varepsilon_h\xi + c\delta) = \frac{1}{2}\sum_{k=0}^{(l-3)/2}(x_{hk} - c)\varepsilon_k + c\varepsilon.$$

If J is the square matrix of order $(l-1)/2$ whose entries are all ones, then

$$M = \left[\begin{array}{ccc|c} & & & c \\ & \frac{1}{2}M(\xi) - \frac{c}{2}J & & \vdots \\ & & & c \\ \hline -1 & \dots & -1 & 2 \end{array}\right].$$

Multiply the last column of M by $1/2$ and add it to the others. Using Proposition 5.5 we obtain

$$\det M = 2^{-(l-3)/2} D(\xi),$$

which completes the proof. ∎

The next theorem follows from the Iwasawa class number formula ([10]) and was generalized by Sinnott ([15]).

THEOREM 5.7.

$$[R' : \mathcal{I}] = h^-.$$

Here, $[A : B]$ means the index of B in A in case of A being a commutative group and B a subgroup of A.

Applying Propositions 5.5, 5.6 and Theorem 5.7 we obtain

THEOREM 5.8. (a) *For the transition matrix M from the basis S' of R' to the elements $s^j\beta$ $(0 \le j \le (l-3)/2)$ and δ we have*

$$\det M = (-1)^{(l-1)/2} \frac{\omega(N)}{l} h^-.$$

(b) *The system*

$$\{s^j\beta \mid 0 \le j \le (l-3)/2\} \cup \{\delta\}$$

forms a basis of $\mathcal{B}_N$ considered as a $\mathbb{Z}$-module.

(c) $$[R' : \mathcal{B}_N] = \frac{\omega(N)}{l} h^- \quad \text{and} \quad [\mathcal{I} : \mathcal{B}_N] = \frac{\omega(N)}{l}.$$

Lastly, we shall derive a system equivalent to (V) mentioned in Proposition 3.5 by means of the elements $\alpha \in \mathcal{B}_N$.

DEFINITION 5.9 (cf. [16], 1.3). For the element $\alpha = \sum_{i=0}^{l-2} a_i s^i$ of R, we define the polynomial $f_\alpha(t)$ as follows:

$$f_\alpha(t) = \sum_{v=1}^{l-1} a_{-\operatorname{ind} v} \frac{1}{v} t^v,$$

where a_j $(j \in \mathbb{Z})$ is equal to a_i $(0 \le i \le l-2)$ whenever $j \equiv i \pmod{l-1}$.

THEOREM 5.10. *The system* (V) *of Proposition* 3.5 *is equivalent to the system*

$$f_\alpha(t) \equiv 0 \pmod{l} \qquad (\alpha \in \mathcal{B}_N).$$

Proof. Let k and ϱ be integers with $1 \le k \le l-1$, $0 \le \varrho \le l-2$ and $r_\varrho = k$. According to Proposition 5.2 we let

$$\alpha = s^\varrho \beta = \sum_{i=0}^{l-2} \left[\frac{N r_{-i+\varrho}}{l} \right] s^i.$$

Then it follows that

$$f_\alpha(t) = \sum_{v=1}^{l-1} \left[\frac{Nr_{\operatorname{ind} v+\varrho}}{l}\right]\frac{1}{v}t^v = \sum_{v=1}^{l-1}\left[\frac{N\overline{vk}}{l}\right]\frac{1}{v}t^v$$
$$= \sum_{v=1}^{l-1}\left(\left[\frac{vkN}{l}\right] - N\left[\frac{vk}{l}\right]\right)\frac{1}{v}t^v.$$

Since $\varphi_{l-1}(t) \equiv f_\delta(t) \pmod{l}$, the theorem follows. ∎

Acknowledgments. We would like to express many thanks to the referee for his valuable comments and especially for his calling our attention to Sinnott's Lemma (Lemma 5.4).

References

[1] T. Agoh, *On the criteria of Wieferich and Mirimanoff*, C. R. Math. Rep. Acad. Sci. Canada 8 (1986), 49–52.
[2] —, *On the Kummer–Mirimanoff congruences*, Acta Arith. 55 (1990), 141–156.
[3] —, *Some variations and consequences of the Kummer–Mirimanoff congruences*, ibid. 62 (1992), 73–96.
[4] G. Benneton, *Sur le dernier théorème de Fermat*, Ann. Sci. Univ. Besançon Math. 3 (1974), 15pp.
[5] P. J. Davis, *Circulant Matrices*, Wiley, New York, 1979.
[6] H. G. Folz and H. G. Zimmer, *What is the rank of the Demjanenko matrix*?, J. Symbolic Comput. 4 (1987), 53–67.
[7] R. Fueter, *Kummers Kriterium zum letzten Theorem von Fermat*, Math. Ann. 85 (1922), 11–20.
[8] F. Hazama, *Demjanenko matrix, class number, and Hodge group*, J. Number Theory 34 (1990), 174–177.
[9] —, *Hodge cycles on the Jacobian variety of the Catalan curve*, preprint, 1994.
[10] K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. 76 (1962), 171–179.
[11] E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Abhandl. Königl. Akad. Wiss. Berlin 1857, 41–74; Collected Papers, Vol. I, 639–692.
[12] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $\frac{a^{p-1}-1}{p} = q(a)$, Math. Ann. 60 (1905), 471–490.
[13] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979.
[14] J. W. Sands and W. Schwarz, *A Demjanenko matrix for abelian fields of prime power conductor*, J. Number Theory 52 (1995), 85–97.
[15] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.
[16] L. Skula, *A remark on Mirimanoff polynomials*, Comment. Math. Univ. St. Paul. (Tokyo) 31 (1982), 89–97.
[17] —, *Some bases of the Stickelberger ideal*, Math. Slovaca 43 (1993), 541–571.

[18] L. Skula, *On a special ideal contained in the Stickelberger ideal*, J. Number Theory, to appear.

Department of Mathematics
Science University of Tokyo
Noda, Chiba 278, Japan
E-mail: agoh@ma.noda.sut.ac.jp

Department of Mathematics
Faculty of Science
Masaryk University
662 95 Brno, Czech Republic
E-mail: skula@math.muni.cz

Received on 5.5.1995
and in revised form on 31.10.1995 (2788)