ARCHIVUM MATHEMATICUM (BRNO)
Tomus 32 (1996), 211 – 232

KUMMER TYPE SYSTEM OF CONGRUENCES AND BASES OF STICKELBERGER SUBIDEALS

Takashi Agoh and Kenichi Mori

Abstract. A new Kummer type system of congruences is introduced and some bases of subideals of the Stickelberger ideal in a certain group ring are discussed. Further, we consider special Stickelberger subideals and evaluate the group indices of them in a subring of the group ring.

1. Introduction

Let $l \geq 5$ be an odd prime, $\mathbb{Z}$ the ring of integers, $\mathbb{Z}_l = \mathbb{Z}/l\mathbb{Z}$ the ring of residue classes modulo l, $\mathbb{Q}$ the field of rational numbers and $\mathbb{Q}(\zeta)$ the cyclotomic field over $\mathbb{Q}$ defined by a primitive l-th root of unity $\zeta = e^{2\pi i/l}$. Also let B_m be the m-th Bernoulli number defined by

$$B(x) = \frac{x}{e^x - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} x^m$$

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

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

The following system of congruences was first introduced by Kummer (1857) in connection with the first case of Fermat's last theorem :

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

Many kinds of equivalent systems to (K) are known (see, e.g., Agoh [2, 3] and Granville [7]). In his paper [11] Skula devised a very interesting system of

1991 *Mathematics Subject Classification*: 11D42, 11R54, 11B68, 16S34.
Key words and phrases: Kummer system of congruences, Stickelberger ideal, Mirimanoff polynomial, Bernoulli number, class number of cyclotomic field.
Received March 18, 1996.

congruences (S) equivalent to (K) by means of the Stickelberger ideal in a certain group ring (see Section 2). Here, we emphasize that at present it is unknown whether the system (K) has a non-trivial solution.

Recently, Agoh and Skula [4] considered the following special system $(\mathrm{K}(N))$ of congruences and they investigated equivalent systems and specific connections with Stickelberger subideals :

$$(\mathrm{K}(N)) \qquad \begin{cases} \varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ B_{2m}^{(N)} \varphi_{l-2m}(t) \equiv 0 \pmod{l} \quad \left(1 \leq m \leq \dfrac{l-3}{2}\right), \end{cases}$$

where N is a fixed positive integer with $2 \leq N \leq l-1$ and

$$B_k^{(N)} = \frac{1-N^k}{k} B_k \quad (k \geq 1).$$

The system $(\mathrm{K}(N))$ for the special case where $N = 2$ was first observed by Benneton [5] in 1974 and it was recently investigated by Skula [15] from the viewpoint of Stickelberger subideals.

We present here the further generalized system of congruences

$$(\mathrm{K}(M,N)) \qquad \begin{cases} \varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ B_{2m}^{(M,N)} \varphi_{l-2m}(t) \equiv 0 \pmod{l} \quad \left(1 \leq m \leq \dfrac{l-3}{2}\right), \end{cases}$$

where M and N are fixed positive integers with $2 \leq M, N \leq l-1$ and

$$B_k^{(M,N)} = \frac{(1-M^k)(1-N^k)}{k} B_k \quad (k \geq 1).$$

Obviously, we see that all the solutions of (K) (resp. $(\mathrm{K}(N))$) satisfy $(\mathrm{K}(N))$ (resp. $(\mathrm{K}(M,N))$). In particular, if M and N both are primitive roots mod l, then the above three systems (K), $(\mathrm{K}(N))$ and $(\mathrm{K}(M,N))$ are mutually equivalent, that is, these systems have the solutions in common.

Main purpose of this paper is to study some systems equivalent to $(\mathrm{K}(N))$ and $(\mathrm{K}(M,N))$ and to search bases of Stickelberger subideals relating to these systems in certain group rings.

In Section 2, we define the subideals $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$ of the Stickelberger ideal $\mathfrak{I}(l)$ in the group ring $\mathbb{Z}_l[G]$ of a cyclic group G over $\mathbb{Z}_l$ and obtain bases of these subideals. Further, the Skula type systems of congruences concerned with $(\mathrm{K}(N))$ and $(\mathrm{K}(M,N))$ will be derived. In Section 3 we concentrate on identities in $\mathbb{Z}_l[G]$. Section 4 is appropriated to a search other bases of $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$ applying the identities given in Section 3. In Section 5, we observe the special Stickelberger subideals $\mathfrak{B}_N$ and $\mathfrak{B}_{M,N}$, and evaluate the group indices of them in a certain subring of the group ring $\mathbb{Z}[G]$ of G over $\mathbb{Z}$ in terms of the first factor h^- of the class number of $\mathbb{Q}(\zeta)$. In Section 6, we deal with the Fueter type system of congruences equivalent to $(\mathrm{K}(M,N))$. In the last section, we shall incidentally mention a relationship between the above $\mathfrak{I}_N(l)$ and the ideal $\mathfrak{B}_N$ mod l observed by Skula [16].

2. Skula type system

Throughout this paper we use the following notations:

r : a primitive root mod l,

r_i : the least positive residue of r^i mod l for an integer i,

$\operatorname{ind} x$: the index of $x \in \mathbb{Z}$, $l \nmid x$, relating to the primitive root $r \bmod l$,

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

$R = \mathbb{Z}[G] = \Big\{\sum_{i=0}^{l-2} a_i s^i : a_i \in \mathbb{Z}\Big\}$: the group ring of G over $\mathbb{Z}$,

$R_l = \mathbb{Z}_l[G] = \Big\{\sum_{i=0}^{l-2} a_i s^i : a_i \in \mathbb{Z}_l\Big\}$: the group ring of G over $\mathbb{Z}_l$.

The Stickelberger ideal $\mathfrak{I}$ of R is defined by

$$\mathfrak{I} = \Big\{\alpha \in R : \exists \rho \in R,\ \rho \sum_{i=0}^{l-2} r_{-i} s^i = l\alpha\Big\} \quad \text{(see, e.g., [13], 1.1)}.$$

The canonical mapping ψ from $\mathbb{Z}$ onto $\mathbb{Z}_l$ can be naturally extended to the mapping from R onto R_l in the following way: for an element $\alpha = \sum_{i=0}^{l-2} a_i s^i \in R$ we let $\psi(\alpha) = \sum_{i=0}^{l-2} \psi(a_i) s^i \in R_l$. Then the Stickelberger ideal of R_l is defined by

$$\mathfrak{I}(l) = \{\psi(\alpha) : \alpha \in \mathfrak{I}\}.$$

Further we define the following special elements in R_l (cf., [13], Section 3):

$$\alpha_m = \sum_{i=0}^{l-2} r_{-im} s^i \quad (1 \le m \le l-1).$$

In particular, set

$$\gamma = \alpha_1 = \sum_{i=0}^{l-2} r_{-i} s^i, \quad \delta = \alpha_{l-1} = \sum_{i=0}^{l-2} s^i.$$

One may observe and treat ideals of the rings R and R_l regarding as modules over $\mathbb{Z}$ and $\mathbb{Z}_l$, respectively.

In his papers [12, 13] Skula investigated some bases of $\mathfrak{I}(l)$ and proved

Proposition 2.1 ([12, Proposition 3.3], [13, Proposition 5.4]). *Let*

$$C = \{\alpha_m : B_{l-m} \not\equiv 0 \pmod{l},\ 3 \le m \le l-2,\ m \text{ odd}\}.$$

Then the system $C \cup \{\gamma, \delta\}$ forms a basis of $\mathfrak{I}(l)$ as a $\mathbb{Z}_l$-module. Thus

$$\operatorname{rank} \mathfrak{I}(l) = \frac{l+1}{2} - ii(l),$$

where $ii(l)$ is the irregularity index of l, i.e.,

$$ii(l) = \sharp\Big\{k : B_{2k} \equiv 0 \pmod{l},\ 1 \le k \le \frac{l-3}{2}\Big\}.$$

Also he introduced the following polynomial :

Definition 2.2 ([11], 1.3). *For $\alpha = \sum_{i=0}^{l-2} a_i s^i \in R$ (or R_l), define*

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

where $\tilde{v}$ is an integer (or a class of $\mathbb{Z}_l$) such that $v\tilde{v} \equiv 1 \pmod{l}$ $(1 \le \tilde{v} \le l-1)$ (or $\tilde{v}v = 1$ in $\mathbb{Z}_l$) and a_k $(k \in \mathbb{Z})$ is replaced by a_i $(0 \le i \le l-2)$ if $k \equiv i \pmod{l-1}$.

Here, note that if $\alpha = \sum_{i=0}^{l-2} a_i s^i \in R_l$, then a_i may be replaced by any element of the residue class of $\mathbb{Z}_l$ belonging in a_i.

As basic relations between the Skula and Mirimanoff polynomials, we may state (cf., [14], 2.1)

$$\begin{aligned}
&f_{\alpha_m}(t) \equiv \varphi_m(t) \pmod{l} \quad (2 \le m \le l-2),\\
&f_\gamma(t) \equiv \varphi_1(t) \equiv \varphi_l(t) \pmod{l},\\
&f_\delta(t) \equiv \varphi_{l-1}(t) \pmod{l}.
\end{aligned}$$

Using the above polynomial $f_\alpha(t)$ $(\alpha \in R_l)$ Skula considered the system of congruences

$$\text{(S)} \qquad f_\alpha(t) \equiv 0 \pmod{l} \quad (\alpha \in \mathfrak{I}(l))$$

and showed

Proposition 2.3 ([13], Proposition 6.1). *Let τ be an integer with $\tau \not\equiv 1 \pmod{l}$. Then τ is a solution of the system (K) if and only if τ is a solution of the system (S).*

For integers M and N with $2 \le M, N \le l-1$, we set

$$\begin{aligned}
C_X &= \Big\{\alpha_m : B_{l-m}^{(X)} \not\equiv 0 \pmod{l},\ 3 \le m \le l-2,\ m \text{ odd}\Big\} \ (\text{where } X = M, N),\\
C_{M,N} &= \Big\{\alpha_m : B_{l-m}^{(M,N)} \not\equiv 0 \pmod{l},\ 3 \le m \le l-2,\ m \text{ odd}\Big\}.
\end{aligned}$$

It is clear that $C_{M,N} \subseteq C_X \subseteq C$ and $C_M \cap C_N = C_{M,N}$. If the order of X mod l is not equal to 2, then C_X is not the empty set, because $B_2^{(X)} \not\equiv 0 \pmod{l}$. In the following we assume that C_X (for $X = M, N$) and $C_{M,N}$ are not empty.

We denote by $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$ the subideals of $\mathfrak{I}(l)$ generated by the systems $C_N \cup \{\delta\}$ and $C_{M,N} \cup \{\delta\}$, respectively. Thus,

$$\mathfrak{I}_N(l) = \Big\{ \sum_{\alpha_m \in C_N} \sum_{j=0}^{l-2} c_j^{(m)} s^j \alpha_m + c\delta : \ c_j^{(m)},\, c \in \mathbb{Z}_l \Big\} \subseteq \mathfrak{I}(l),$$

$$\mathfrak{I}_{M,N}(l) = \Big\{ \sum_{\alpha_m \in C_{M,N}} \sum_{j=0}^{l-2} c_j^{(m)} s^j \alpha_m + c\delta : \ c_j^{(m)},\, c \in \mathbb{Z}_l \Big\} \subseteq \mathfrak{I}(l).$$

Similarly to Proposition 2.1, we can state

Proposition 2.4. *Let $2 \leq M, N \leq l-1$. Then*

(i) *the system $C_N \cup \{\delta\}$ forms a basis of $\mathfrak{I}_N(l)$,*

(ii) *the system $C_{M,N} \cup \{\delta\}$ forms a basis of $\mathfrak{I}_{M,N}(l)$.*

Thus

$$\operatorname{rank} \mathfrak{I}_N(l) = \frac{l-1}{2} - ii_N(l), \quad \operatorname{rank} \mathfrak{I}_{M,N}(l) = \frac{l-1}{2} - ii_{M,N}(l),$$

where

$$ii_N(l) = \sharp\Big\{ k : B_{2k}^{(N)} \equiv 0 \pmod{l},\ 1 \leq k \leq \frac{l-3}{2} \Big\}$$

and

$$ii_{M,N}(l) = \sharp\Big\{ k : B_{2k}^{(M,N)} \equiv 0 \pmod{l},\ 1 \leq k \leq \frac{l-3}{2} \Big\}.$$

It is clear that $\mathfrak{I}_{M,N}(l) = \mathfrak{I}_M(l) \cap \mathfrak{I}_N(l)$, $ii(l) \leq ii_N(l) \leq ii_{M,N}(l)$ and the numbers of non-trivial congruences in the systems $(\mathrm{K}(N))$ and $(\mathrm{K}(M,N))$ are at most $\operatorname{rank} \mathfrak{I}_N(l)$ and $\operatorname{rank} \mathfrak{I}_{M,N}(l)$, respectively.

In the following discussion we assume that $\mathfrak{I}_M(l), \mathfrak{I}_N(l) \neq \mathfrak{I}_{M,N}(l)$, in other words, $C_M \not\subseteq C_N$ and $C_N \not\subseteq C_M$.

Analogously to the system (S), we now consider the following two systems of congruences:

$$(\mathrm{S}(N)) \qquad f_\alpha(t) \equiv 0 \pmod{l} \quad (\alpha \in \mathfrak{I}_N(l))$$

and

$$(\mathrm{S}(M,N)) \qquad f_{\alpha'}(t) \equiv 0 \pmod{l} \quad (\alpha' \in \mathfrak{I}_{M,N}(l)).$$

For these systems one can obviously assert

Proposition 2.5. (i) *The system $(\mathrm{K}(N))$ is equivalent to the system $(\mathrm{S}(N))$.*

(ii) *The system $(\mathrm{K}(M,N))$ is equivalent to the system $(\mathrm{S}(M,N))$.*

3. Identities in R_l

This section deals with some polynomial identities and we transport them into the group ring R_l in order to discover other bases of the subideals $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$ of $\mathfrak{I}(l)$.

For $m \geq 0$ and $k \geq 1$, designate by

$$\begin{aligned} S_m(k) =& 1^m + 2^m + \cdots + k^m, \\ S_m(k\,;N) =& S_m(kN) - N^{m+1}S_m(k), \\ S_m(k\,;M,N) =& S_m(kMN) - N^{m+1}S_m(kM) - M^{m+1}S_m(kN) + (MN)^{m+1}S_m(k). \end{aligned}$$

The following identity was described in the paper [4] of Agoh and Skula:

Proposition 3.1 ([4], Proposition 3.2). *Let m, k be integers with $m \leq l-3$ and $k \geq 1$. Then*

$$\begin{aligned} &\frac{1-N}{2}(kN)^{l-2-m}\varphi_{l-1}(t) + \sum_{j=2}^{l-2-m}\binom{l-2-m}{j-1}(kN)^{l-1-m-j}\left\{B_j^{(N)}\varphi_{l-j}(t)\right\} \\ &\qquad = \sum_{v=1}^{l-1} S_{l-2-m}(vk\,;N)v^m t^v. \end{aligned}$$

Referring to this proposition one can deduce

Proposition 3.2. *With the same notation as in Proposition* 3.1

$$\begin{aligned} &\frac{(1-M)(1-N)}{2}(kMN)^{l-2-m}\varphi_{l-1}(t) \\ &\qquad\qquad + \sum_{j=2}^{l-2-m}\binom{l-2-m}{j-1}(kMN)^{l-1-m-j}\left\{B_j^{(M,N)}\varphi_{l-j}(t)\right\} \\ &\qquad = \sum_{v=1}^{l-1} S_{l-2-m}(vk\,;M,N)v^m t^v. \end{aligned}$$

Proof. For brevity we let

$$\begin{aligned} W_N(x) &= \frac{1}{x}\left\{B(x) - B(Nx)\right\}, \\ W_{M,N}(x) &= W_N(x) - MW_N(Mx), \\ A_{k,m}(t,x) &= \left\{B(x)e^x\right\}\varphi_{m+1}(te^{kx}) - \varphi_{m+1}(t)B(x), \end{aligned}$$

where $B(x)$ is the generating function of Bernoulli numbers defined in the Introduction. Then $A_{k,m}(t,x)$ can be expressed as

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

Here we have

$$\begin{aligned}
&A_{kMN,m}(t,x) - A_{kM,m}(t,Nx) - A_{kN,m}(t,Mx) + A_{k,m}(t,MNx)\\
&= \left\{B(x)e^{x} - B(Nx)e^{Nx} - B(Mx)e^{Mx} + B(MNx)e^{MNx}\right\}\varphi_{m+1}(te^{kMNx})\\
&\qquad - \{B(x) - B(Nx) - B(Mx) + B(MNx)\}\varphi_{m+1}(t)\\
&= x\{(1-M)(1-N) + W_{M,N}(x)\}\varphi_{m+1}(te^{kMNx}) - xW_{M,N}(x)\varphi_{m+1}(t),
\end{aligned}$$

hence

$$\begin{aligned}
&\{(1-M)(1-N) + W_{M,N}(x)\}\varphi_{m+1}(te^{kMNx}) - W_{M,N}(x)\varphi_{m+1}(t)\\
&= \sum_{v=1}^{l-1}\Big\{\sum_{j=0}^{vkMN} e^{jx} - N\sum_{j=0}^{vkM} e^{jNx} - M\sum_{j=0}^{vkN} e^{jMx} + MN\sum_{j=0}^{vk} e^{jMNx}\Big\}v^m t^v.
\end{aligned}$$

Since for $n \geq 0$

$$\begin{aligned}
\left[\frac{d^n}{dx^n}W_{M,N}(x)\right]_{x=0} &= \left[\frac{d^n}{dx^n}\big(W_N(x) - MW_N(Mx)\big)\right]_{x=0}\\
&= B_{n+1}^{(N)} - M^{n+1}B_{n+1}^{(N)}\\
&= B_{n+1}^{(M,N)} \quad \text{(cf., [1], Lemma)}
\end{aligned}$$

and

$$\left[\frac{d^n}{dx^n}\varphi_{m+1}(te^{kMNx})\right]_{x=0} = (kMN)^n\varphi_{m+n+1}(t),$$

we get the identity as required using Leibniz's theorem for the above functional equality. □

For integers m, k with $0 \leq m \leq l-3$ and $1 \leq k \leq l-1$, we prepare the following special elements of R_l :

$$\begin{aligned}
\sigma(m,k) &= \sum_{i=0}^{l-2} b_i(m,k)s^i,\\
\sigma^{(N)}(m,k) &= \sum_{i=0}^{l-2} b_i^{(N)}(m,k)s^i,\\
\sigma^{(M,N)}(m,k) &= \sum_{i=0}^{l-2} b_i^{(M,N)}(m,k)s^i,
\end{aligned}$$

where for each $i = 0, 1, ..., l-2$

$$\begin{aligned}
b_i(m,k) &= r_{-i(m+1)}S_{l-2-m}(r_{-i}k),\\
b_i^{(N)}(m,k) &= r_{-i(m+1)}S_{l-2-m}(r_{-i}k\,;N),\\
b_i^{(M,N)}(m,k) &= r_{-i(m+1)}S_{l-2-m}(r_{-i}k\,;M,N).
\end{aligned}$$

Then we have

$$f_{\sigma(m,k)}(t) \equiv \sum_{v=1}^{l-1} S_{l-2-m}(vk)v^m t^v \pmod{l} \text{ (cf., [14], 2.3)},$$

$$f_{\sigma^{(N)}(m,k)}(t) \equiv \sum_{v=1}^{l-1} S_{l-2-m}(vk\,;N)v^m t^v \pmod{l},$$

$$f_{\sigma^{(M,N)}(m,k)}(t) \equiv \sum_{v=1}^{l-1} S_{l-2-m}(vk\,;M,N)v^m t^v \pmod{l}.$$

Based on the fact that the mapping η from R_l into $\mathbb{Z}_l[t]$ defined by $\eta(\alpha) = f_\alpha(t)$ conserves addition and scalar multiplication, Skula derived the following proposition (in a slightly different form) using the polynomial identity

$$k^{l-1-m}\varphi_l(t) + \frac{l-1-m}{2}k^{l-2-m}\varphi_{l-1}(t) + \sum_{i=2}^{l-2-m}\binom{l-1-m}{i}k^{l-1-m-i}\{B_i\varphi_{l-i}(t)\}$$
$$= (l-1-m)\sum_{v=1}^{l-1} S_{l-2-m}(vk)v^m t^v \text{ (Agoh [2], (3.4))}.$$

Proposition 3.3 ([14], Proposition 2.4). *Let m, k be integers with $0 \le m \le l-3$ and $1 \le k \le l-1$. Then*

$$\frac{1}{l-1-m}k^{l-1-m}\gamma + \frac{1}{2}k^{l-2-m}\delta + \sum_{j=2}^{l-2-m}\binom{l-2-m}{j-1}k^{l-1-m-j}\frac{1}{j}\{B_j\alpha_{l-j}\}$$
$$= \sigma(m,k).$$

By Propositions 2.1 and 3.3 one recognizes that $\sigma(m,k)$ is an element of $\mathfrak{I}(l)$.

Similarly to the above proposition, we may deduce the following proposition from the polynomial identities given in Propositions 3.1 and 3.2.

Proposition 3.4. *With the same notation as in Proposition* 3.3

(i)
$$\frac{1-N}{2}(kN)^{l-2-m}\delta + \sum_{j=2}^{l-2-m}\binom{l-2-m}{j-1}(kN)^{l-1-m-j}\left\{B_j^{(N)}\alpha_{l-j}\right\}$$
$$= \sigma^{(N)}(m,k),$$

(ii)
$$\frac{(1-M)(1-N)}{2}(kMN)^{l-2-m}\delta$$
$$+ \sum_{j=2}^{l-2-m}\binom{l-2-m}{j-1}(kMN)^{l-1-m-j}\left\{B_j^{(M,N)}\alpha_{l-j}\right\}$$
$$= \sigma^{(M,N)}(m,k).$$

By Proposition 2.4 we know that the systems $C_N \cup \{\delta\}$ and $C_{M,N} \cup \{\delta\}$ form bases of $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$, respectively. Therefore, we may state from Proposition 3.4

Proposition 3.5. *Let m, k be as in Proposition 3.3. Then $\sigma^{(N)}(m,k)$ and $\sigma^{(M,N)}(m,k)$ are the elements in the ideals $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$ of R_l, respectively.*

4. Other bases of $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$

In this section we would like to search some other bases of the subideals $\mathfrak{I}_N(l)$ and $\mathfrak{I}_{M,N}(l)$ regarding as $\mathbb{Z}_l$-modules. For this purpose we utilize the identities (i) and (ii) in Proposition 3.4 adopting the same ideas as mentioned in Skula's paper ([14], Sections 3 and 4).

(I) Bases of $\mathfrak{I}_N(l)$. Let m, k be integers with $0 \le m \le l-3,\ 1 \le k \le l-1$ and

$$T = \left\{ j \text{ even} : B_j^{(N)} \not\equiv 0 \pmod{l},\ 2 \le j \le l-3 \right\}.$$

Denoting by

$$a_1^{(N)}(m,k) = \frac{1-N}{2}(kN)^{l-2-m},$$

$$a_j^{(N)}(m,k) = \begin{cases} \binom{l-2-m}{j-1}(kN)^{l-1-m-j} & \text{if } \ 2 \le j \le l-2-m \text{ and } j \in T, \\ 0 & \text{otherwise,} \end{cases}$$

we get from Proposition 3.4-(i)

$$a_1^{(N)}(m,k)\delta + \sum_{\substack{j \in T \\ 2 \le j \le l-2-m}} a_j^{(N)}(m,k) B_j^{(N)} \alpha_{l-j} = \sigma^{(N)}(m,k).$$

Let $\nu = (l-1)/2 - ii_N(l)$. For a subset L of $\{(m,k) \in \mathbb{Z}^2 : 0 \le m \le l-3,\ 1 \le k \le l-1\}$ with $\sharp L = \nu$, define the square matrix of order ν as follows:

$$D(L) = \left[a_j^{(N)}(m,k) \right]_{(m,k) \in L,\, j \in \{1\} \cup T}.$$

Then we obtain from Propositions 2.4 and 3.5

Theorem 4.1. *The system $\left\{\sigma^{(N)}(m,k) : (m,k) \in L\right\}$ forms a basis of $\mathfrak{I}_N(l)$ if and only if the matrix $D(L)$ is non-singular over $\mathbb{Z}_l$.*

Corollary 4.2. *Let K be any subset of $\{1, 2, \cdots, l-1\}$ with $\sharp K = \nu$. Then the following statements are equivalent :*

(i) *the system $\left\{\sigma^{(N)}(0,k) : k \in K\right\}$ forms a basis of $\mathfrak{I}_N(l)$,*
(ii) *the system $\left\{\sigma^{(N)}(1,k) : k \in K\right\}$ forms a basis of $\mathfrak{I}_N(l)$,*
(iii) *the matrix $[\ k^{l-3-j}]_{k \in K,\, j \in \{1\} \cup T}$ is non-singular over $\mathbb{Z}_l$.*

Proof. For the system $\{\sigma^{(N)}(0,k) : k \in K\}$ we calculate the determinant of the corresponding matrix $D(L)$ with $m = 0$. Letting $K = \{k_1, \cdots, k_\nu\}$ one has

$$\det D(L) = \det \left[\begin{array}{c|c} \frac{1-N}{2}(k_1 N)^{l-2} & \cdots \binom{l-2}{j-1}(k_1 N)^{l-1-j} \cdots \\ \vdots & \vdots \\ \frac{1-N}{2}(k_i N)^{l-2} & \cdots \binom{l-2}{j-1}(k_i N)^{l-1-j} \cdots \\ \vdots & \vdots \end{array}\right] (1 \le i \le \nu,\, j \in T)$$
$$= G \cdot \det[\, k^{l-3-j}]_{k \in K,\, j \in \{1\} \cup T},$$

where

$$G = \frac{(1-N)N^{l-2}}{2} \prod_{j \in T} \binom{l-2}{j-1} N^{l-1-j} \prod_{k \in K} k^2 \not\equiv 0 \pmod{l}.$$

Therefore, we know from Theorem 4.1 that (i) and (iii) are equivalent. The rest follows easily by the similar argument to the above. □

Applying Corollary 4.2 we can find some bases of $\mathfrak{I}_N(l)$ as follows :

Corollary 4.3. *Let $K' = \{r_0, r_1, \cdots, r_g\}$, where r is a primitive root mod l and $g = \nu - 1$. Then the systems $\{\sigma^{(N)}(0,k) : k \in K'\}$ and $\{\sigma^{(N)}(1,k) : k \in K'\}$ form bases of $\mathfrak{I}_N(l)$.*

Proof. Consider the square matrix $Y = \left[r_i^{l-3-j} \right]_{0 \le i \le g, j \in \{1\} \cup T}$ of order $\nu = g+1$. Then we obtain

$$\det Y \equiv \det \left[r_{l-3-j}^{i} \right]_{0 \le i \le g,\, j \in \{1\} \cup T} \not\equiv 0 \pmod{l},$$

which leads to the conclusion by virtue of Corollary 4.2. □

Corollary 4.4. *Let k, $1 \le k \le l-1$, be fixed and put*

$$U = \left\{ m \text{ odd} : B_{l-2-m}^{(N)} \not\equiv 0 \pmod{l},\ 1 \le m \le l-4 \right\}.$$

Then the system $\{\sigma^{(N)}(l-3,k)\} \cup \{\sigma^{(N)}(m,k) : m \in U\}$ forms a basis of $\mathfrak{I}_N(l)$.

Proof. Clearly, we see $\sigma^{(N)}(l-3,k) = ((1-N)/2)kN\delta$. Let g be as in Corollary 4.3 and put in order the elements of T and U as follows :

$$T = \{j(v) : 1 \le v \le g\}, \quad \text{where } 2 \le j(1) < j(2) < \cdots < j(g) \le l-3,$$
$$U = \{m(u) : 1 \le u \le g\}, \quad \text{where } 1 \le m(1) < m(2) < \cdots < m(g) \le l-4.$$

For an integer $\theta, 1 \le \theta \le g$, we have $m(\theta) = l-2-j(g-\theta+1)$. The corresponding matrix $D(L)$ with a fixed k, $1 \le k \le l-1$, becomes

$$D(L) = \left[\begin{array}{c|c} \frac{1-N}{2}kN & 0 \ \cdots \ 0 \\ \hline \vdots & \\ c_u & B \\ \vdots & \end{array}\right],$$

where $c_u = ((1-N)/2)(kN)^{l-2-m(u)}$ $(u = 1, 2, ..., g)$ and

$$B = [\, b_{uv}]_{1 \le u,v \le g}, \quad b_{uv} = a^{(N)}_{j(v)}(m(u), k).$$

Here we have $\det D(L) = ((1-N)/2)kN \cdot \det B$. If $v > g-u+1$, then $j(v) > j(g-u+1) = l-2-m(u)$ and $b_{uv} = 0$. Also, if $v = g-u+1$, then $j(v) = j(g-u+1) = l-2-m(u)$ and so

$$\begin{aligned} b_{uv} &= a^{(N)}_{l-2-m(u)}(m(u), k) \\ &= (l-2-m(u))kN \not\equiv 0 \pmod{l}, \end{aligned}$$

which implies $\det B \not\equiv 0 \pmod{l}$ and hence $D(L)$ is non-singular. According to Theorem 4.1 the system indicated in the statement forms a basis of the $\mathbb{Z}_l$-module $\mathfrak{I}_N(l)$. This completes the proof. $\square$

(II) Bases of $\mathfrak{I}_{M,N}(l)$. We shall develop here the same arguments as done in (I). Let m, k be integers with $0 \le m \le l-3$, $1 \le k \le l-1$ and put

$$S = \left\{ j \text{ even} : B^{(M,N)}_j \not\equiv 0 \pmod{l},\ 2 \le j \le l-3 \right\}.$$

We now define

$$a^{(M,N)}_1(m, k) = \frac{(1-M)(1-N)}{2}(kMN)^{l-2-m},$$

$$a^{(M,N)}_j(m, k) = \begin{cases} \dbinom{l-2-m}{j-1}(kMN)^{l-1-m-j} & \text{if } 2 \le j \le l-2-m, j \in S, \\ 0 & \text{otherwise.} \end{cases}$$

From Proposition 3.4-(ii) we obtain the identity

$$a^{(M,N)}_1(m, k)\delta + \sum_{\substack{j \in S \\ 2 \le j \le l-2-m}} a^{(M,N)}_j(m, k) B^{(M,N)}_j \alpha_{l-j} = \sigma^{(M,N)}(m, k).$$

Let $\mu = (l-1)/2 - ii_{M,N}(l)$ and J be any subset of $\{(m, k) \in \mathbb{Z}^2 : 0 \le m \le l-3,\ 1 \le k \le l-1\}$ with $\sharp J = \mu$. Also, define the square matrix of order μ as follows:

$$C(J) = \left[a^{(M,N)}_j(m, k) \right]_{(m,k) \in J,\, j \in \{1\} \cup S}.$$

Then we get from Propositions 2.4 and 3.5

Theorem 4.5. *The system* $\left\{\sigma^{(M,N)}(m,k):(m,k)\in J\right\}$ *forms a basis of* $\mathfrak{I}_{M,N}(l)$ *if and only if the matrix* $C(J)$ *is non-singular over* $\mathbb{Z}_l$.

Corollary 4.6. *Let* H *be any subset of* $\{1,2,\cdots,l-1\}$ *with* $\sharp H=\mu$. *Then the following statements are equivalent :*

(i) *the system* $\left\{\sigma^{(M,N)}(0,k):k\in H\right\}$ *forms a basis of* $\mathfrak{I}_{M,N}(l)$,
(ii) *the system* $\left\{\sigma^{(M,N)}(1,k):k\in H\right\}$ *forms a basis of* $\mathfrak{I}_{M,N}(l)$,
(iii) *the matrix* $[\ k^{l-3-j}]_{k\in H,\,j\in\{1\}\cup S}$ *is non-singular over* $\mathbb{Z}_l$.

Corollary 4.7. *Let* $H'=\{r_0,r_1,\cdots,r_q\}$, *where* r *is a primitive root mod* l *and* $q=\mu-1$. *Then the systems* $\{\sigma^{(M,N)}(0,k):k\in H'\}$ *and* $\{\sigma^{(M,N)}(1,k):k\in H'\}$ *form bases of* $\mathfrak{I}_{M,N}(l)$.

The proofs of the above corollaries can be performed by similar methods to those of Corollaries 4.2 and 4.3.

Corollary 4.8. *Let* k, $1\le k\le l-1$, *be fixed and*

$$W=\left\{m\ odd:B^{(M,N)}_{l-2-m}\not\equiv 0\pmod{l},\ 1\le m\le l-4\right\}.$$

Then the system $\{\sigma^{(M,N)}(l-3,k)\}\cup\{\sigma^{(M,N)}(m,k):m\in W\}$ *forms a basis of* $\mathfrak{I}_{M,N}(l)$.

Proof. We obviously see $\sigma^{(M,N)}(l-3,k)=((1-M)(1-N)/2)kMN\delta$. Let q be an integer defined above and put in order the elements of S and W as follows :

$$S=\{j(v):1\le v\le q\},\quad \text{where}\ \ 2\le j(1)<j(2)<\cdots<j(q)\le l-3,$$
$$W=\{m(u):1\le u\le q\},\ \text{where}\ \ 1\le m(1)<m(2)<\cdots<m(q)\le l-4.$$

Here, we have $m(\varepsilon)=l-2-j(q-\varepsilon+1)$ for an integer ε, $1\le\varepsilon\le q$. The matrix $C(J)$ for a fixed k is equivalent to

$$C(J)=\left[\begin{array}{c|c} \frac{(1-M)(1-N)}{2}kMN & 0\ \cdots\ 0 \\ \hline \vdots & \\ d_u & E \\ \vdots & \end{array}\right],$$

where $d_u=((1-M)(1-N)/2)(kMN)^{l-2-m(u)}$ $(u=1,2,...,q)$ and

$$E=[\,e_{uv}]_{1\le u,v\le q},\quad e_{uv}=a^{(M,N)}_{j(v)}(m(u),k).$$

Hence, it follows that $\det C(J) = ((1-M)(1-N)/2)kMN \cdot \det E$. If $v > q-u+1$, then $j(v) > j(q-u+1) = l-2-m(u)$ and $e_{uv} = 0$. If $v = q-u+1$, then $j(v) = j(q-u+1) = l-2-m(u)$ and so we have

$$\begin{aligned} e_{uv} &= a^{(M,N)}_{l-2-m(u)}(m(u), k) \\ &= (l-2-m(u))kMN \not\equiv 0 \pmod{l}. \end{aligned}$$

Consequently, we may say that $\det E \not\equiv 0 \pmod{l}$ and so $C(J)$ is non-singular. By Theorem 4.5, it can be concluded that the system indicated in the statement forms a basis of the $\mathbb{Z}_l$-module $\mathfrak{I}_{M,N}(l)$. This completes the proof. □

5. Special ideals $\mathfrak{B}_N$ and $\mathfrak{B}_{M,N}$

In this section we will consider special subideals $\mathfrak{B}_N$ and $\mathfrak{B}_{M,N}$ of the Stickelberger ideal $\mathfrak{I}$ in the group ring R and evaluate the group index $[\mathfrak{B}_N : \mathfrak{B}_{M,N}]$. In addition, by making use of the result ([4], Theorem 5.8) by Agoh and Skula relating to the first factor h^- of the class number of $\mathbb{Q}(\zeta)$ we deduce a formula for $\left[R^{'} : \mathfrak{B}_{M,N}\right]$, where $R^{'}$ is a special subring of R defined below.

Let $R^{'}$ be the subring of R defined by

$$R^{'} = \Big\{\alpha = \sum_{i=0}^{l-2} a_i s^i \in R :\ a_j + a_{j+(l-1)/2} = a_k + a_{k+(l-1)/2},\ 0 \le j, k \le \frac{l-3}{2}\Big\}.$$

The following theorem follows from Iwasawa's class number formula ([8]):

Theorem 5.1.

$$\left[R^{'} : \mathfrak{I}\right] = h^-.$$

We should supplement here that in his profound papers [9, 10] Sinnott extended the above formula to more wider class of cyclotomic fields by means of Stickelberger ideals.

We now put for an integer k

$$\gamma_k = \sum_{i=0}^{l-2} \frac{1}{l}(r_{-i} r_k - r_{-i+k}) s^i = \sum_{i=0}^{l-2} \left[\frac{r_k r_{-i}}{l}\right] s^i.$$

By choosing an appropriate integer n such that $N = r_n$ let

$$\beta = \gamma_n = \sum_{i=0}^{l-2} \left[\frac{N r_{-i}}{l}\right] s^i \quad (2 \le N \le l-1),$$

where $[x]$ is the greatest integer $\le x$.

Then, we extract from the paper [4] of Agoh and Skula the following

Proposition 5.2 ([4], Proposition 5.2). *For an integer* j

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

and

$$s^j\beta + s^{j+\frac{l-1}{2}}\beta = (N-1)\delta.$$

Definition 5.3 ([4], Definition 5.3). *Denote by* $\mathfrak{B}_N$ *the ideal of* R *generated by the elements* β *and* δ*, thus*

$$\mathfrak{B}_N = \left\{\sum_{j=0}^{l-2} b_j s^j\beta + b\delta : b_j, b \in \mathbb{Z}\right\} \subseteq \mathfrak{I}.$$

Let X be an integer with $2 \le X \le l-1$, $f = f_X$ be the order of X mod l and put

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

Theorem 5.4 ([4], Theorem 5.8). *Let* $2 \le N \le l-1$*. Then the system*

$$\left\{s^j\beta : 0 \le j \le \frac{l-3}{2}\right\} \cup \{\delta\}$$

forms a basis of $\mathfrak{B}_N$ *as a* $\mathbb{Z}$*-module and*

$$\left[R' : \mathfrak{B}_N\right] = \frac{\omega(N)}{l}h^-, \quad [\mathfrak{I} : \mathfrak{B}_N] = \frac{\omega(N)}{l}.$$

Referring to Proposition 5.2 and Theorem 5.4 we will describe analogous results for a special ideal $\mathfrak{B}_{M,N}$ of R defined below (Definition 5.6).

For integers M, N with $2 \le M, N \le l-2$, choosing integers m, n with $M = r_m$ and $N = r_n$ we set

$$\begin{aligned}\beta' =& \gamma_{m+n} + \left[\frac{MN}{l}\right]\gamma - N\gamma_m - M\gamma_n\\ =& \sum_{i=0}^{l-2}\left(\left[\frac{MNr_{-i}}{l}\right] - N\left[\frac{Mr_{-i}}{l}\right] - M\left[\frac{Nr_{-i}}{l}\right]\right)s^i.\end{aligned}$$

Then, we may describe

Proposition 5.5. *For an integer* j

$$s^j\beta' = \sum_{i=0}^{l-2}\left(\left[\frac{MNr_{-i+j}}{l}\right] - N\left[\frac{Mr_{-i+j}}{l}\right] - M\left[\frac{Nr_{-i+j}}{l}\right]\right)s^i$$

and

$$s^j\beta' + s^{j+\frac{l-1}{2}}\beta' = -(M-1)(N-1)\delta.$$

Proof. The expression of $s^j\beta'$ is obvious. Since for a positive integer a prime to l

$$\left[\frac{ar_{-i+j+(l-1)/2}}{l}\right] = \left[\frac{a(l-r_{-i+j})}{l}\right] = a-1-\left[\frac{ar_{-i+j}}{l}\right],$$

we have

$$\begin{aligned} s^{j+\frac{l-1}{2}}\beta' &= \sum_{i=0}^{l-2}\left(\left[\frac{MNr_{-i+j+(l-1)/2}}{l}\right] - N\left[\frac{Mr_{-i+j+(l-1)/2}}{l}\right]\right. \\ &\quad \left. -M\left[\frac{Nr_{-i+j+(l-1)/2}}{l}\right]\right)s^i \\ &= \sum_{i=0}^{l-2}\left\{\left((MN-1)-\left[\frac{MNr_{-i+j}}{l}\right]\right) - N\left((M-1)-\left[\frac{Mr_{-i+j}}{l}\right]\right)\right. \\ &\quad \left. -M\left((N-1)-\left[\frac{Nr_{-i+j}}{l}\right]\right)\right\}s^i \\ &= -(M-1)(N-1)\delta - s^j\beta', \end{aligned}$$

which implies the result. □

We now define a special ideal $\mathfrak{B}_{M,N}$ of R depending on M and N as follows:

Definition 5.6. *Denote by $\mathfrak{B}_{M,N}$ the ideal of R generated by the elements β' and δ, thus*

$$\mathfrak{B}_{M,N} = \left\{\sum_{j=0}^{l-2} b'_j s^j\beta' + b'\delta : b'_j, b' \in \mathbb{Z}\right\} \subseteq \mathfrak{I}.$$

By Proposition 5.5 we know that the elements of $\left\{s^j\beta' : 0 \le j \le (l-3)/2\right\} \cup \{\delta\}$ are generators of the $\mathbb{Z}$-module $\mathfrak{B}_{M,N}$. Here, we can prove

Theorem 5.7. *The system*

$$\left\{s^j\beta' : 0 \le j \le \frac{l-3}{2}\right\} \cup \{\delta\}$$

forms a basis of $\mathfrak{B}_{M,N}$ and

$$[\mathfrak{B}_N : \mathfrak{B}_{M,N}] = \omega(M).$$

Proof. We have

$$
\begin{aligned}
\beta' &= \sum_{i=0}^{l-2} \left(\left[\frac{MNr_{-i}}{l} \right] - N \left[\frac{Mr_{-i}}{l} \right] - M \left[\frac{Nr_{-i}}{l} \right] \right) s^i \\
&= \sum_{i=0}^{l-2} \left(\left[\frac{MNr_{-i}}{l} \right] - N \left[\frac{Mr_{-i}}{l} \right] \right) s^i - M \sum_{i=0}^{l-2} \left[\frac{Nr_{-i}}{l} \right] s^i \\
&= \sum_{i=0}^{l-2} \left[\frac{N\overline{Mr_{-i}}}{l} \right] s^i - M \sum_{i=0}^{l-2} \left[\frac{Nr_{-i}}{l} \right] s^i,
\end{aligned}
$$

where $\overline{a}$ is the least non-negative residue of an integer a modulo l. In particular, putting $M = r_m$ with an appropriate integer m

$$
\begin{aligned}
\beta' &= \sum_{i=0}^{l-2} \left[\frac{Nr_{-i+m}}{l} \right] s^i - M \sum_{i=0}^{l-2} \left[\frac{Nr_{-i}}{l} \right] s^i \\
&= s^m \beta - M\beta \in \mathfrak{B}_N,
\end{aligned}
$$

which implies that $\mathfrak{B}_{M,N}$ is a subideal of $\mathfrak{B}_N$. According to Proposition 5.2 we present the transition matrix A from the elements $s^i\beta$ $(0 \le j \le (l-3)/2)$ and δ which form a basis of $\mathfrak{B}_N$ to the elements $s^i\beta'$ $(0 \le j \le (l-3)/2)$ and δ :

$$A = [a_{uv}]_{0 \le u,v \le (l-1)/2},$$

where

$$
a_{uv} = \begin{cases}
-M & \text{if } u = v,\ 0 \le u, v \le (l-3)/2, \\
1 & \text{if } u = v - m,\ 0 \le u \le (l-3)/2 - m \text{ and } u = v = (l-1)/2, \\
-1 & \text{if } u = v + (l-1)/2 - m,\ (l-1)/2 - m \le u \le (l-3)/2, \\
N-1 & \text{if } (l-1)/2 - m \le u \le (l-3)/2,\ v = (l-1)/2, \\
0 & \text{otherwise.}
\end{cases}
$$

Thus,

$$
A = \begin{array}{cc}
\begin{array}{cc} \overbrace{\qquad\qquad}^{m} & \overbrace{\qquad\qquad}^{\frac{l-1}{2}-m} \end{array} & \\
\left[\begin{array}{ccc|ccc|c}
-M & & & 1 & & & 0 \\
 & \ddots & & & \ddots & & \vdots \\
 & & & & & 1 & 0 \\ \hline
-1 & & & & & & N-1 \\
 & \ddots & & & \ddots & & \vdots \\
 & & -1 & & & -M & N-1 \\ \hline
0 & & \cdots & & & 0 & 1
\end{array}\right] &
\begin{array}{l}
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \frac{l-1}{2}-m \\
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} m \\
\\
\end{array}
\end{array}
$$

Let g be the order of M mod l and set $e = (l-1)/g$. We especially choose the primitive root r mod l such that $M = r_e$ and calculate $\det A$ according to the following procedures :

(i) If g is even, we first multiply the last row of A by $-(N-1)$ and add it to the rows with indices $(l-1)/2-e, \cdots, (l-3)/2$. Next, we divide all the columns of A except for the last column into $g/2$ blocks and perform column operations. Then we exchange the index v $(0 \leq v \leq (l-3)/2)$ of the column for the index $x+ye$ $(0 \leq x \leq e-1, 0 \leq y \leq g/2-1)$ and perform the following column operations for each x :

(a) multiply the column with index $x+ye$ by M and add it to the column with index $x+(y-1)e$, beginning at the column with index $x+(g/2-1)e$,

(b) multiply the column with index x by $-\left(1+M^{g/2}\right)^{-1}$,

(c) multiply the column with index x by $M^{g/2-y}$ and add it to the column with index $x+ye$ $(1 \leq y \leq g/2-1)$,

(d) interchange the columns with indices $x+ye$ and $x+(y+1)e$ $(0 \leq y \leq g/2-2)$.

Then it is seen that $\det A = (-1)^{(l-1)/2}\left(1+M^{g/2}\right)^{e}$.

(ii) If g is odd (and so e is even), we multiply the last row of the matrix A by $-(N-1)$ and add it to the rows with indices $(l-1)/2-e, \cdots, (l-3)/2$. Next, we divide all the columns of A except for the last column into g blocks and perform column operations. Then we exchange the index v $(0 \leq v \leq (l-3)/2)$ of the column for the index $x+y\cdot(e/2)$ $(0 \leq x \leq e/2-1, 0 \leq y \leq g-1)$ and perform the following column operations for each x :

(a) multiply the column with index $x+y\cdot(e/)2$ by M and add it to the column with index $x+(y-2)\cdot(e/2)$, beginning at the column with index $x+(g-1)\cdot(e/2)$,

(b) interchange the columns with indices x and $x+e/2$ and multiply the column with index $x+e/2$ by -1,

(c) multiply the column with index $x+e/2$ by $M^{(g-1)/2}$ and add it to the column with index x,

(d) multiply the column with index x by $(M^g-1)^{-1}$,

(e) multiply the column with index x by $-M^{(g+1)/2}$ and add it to the column with index $x+e/2$,

(f) multiply the column with index x by $M^{(g+1)/2-y/2}$ and add it to the column with index $x+y\cdot(e/2)$ $(2 \leq y \leq g-1$ and y even),

(g) multiply the column with index $x+e/2$ by $M^{(g-1)/2-(y-1)/2}$ and add it to the column with index $x+y\cdot(e/2)$ $(3 \leq y \leq g-2$ and y odd),

(h) interchange the columns with indices $x+y\cdot(e/2)$ and $x+(y+2)\cdot(e/2)$ $(0 \leq y \leq g-3)$.

Then we see $\det A = (-1)^{(l-1)/2}(1-M^g)^{e/2}$.

Summarizing (i) and (ii) we may state that

$$\det A = (-1)^{(l-1)/2}\omega(M),$$

which completes the proof of the theorem. □

Combining Theorems 5.4 and 5.7 we can finally derive the following formulas:

Theorem 5.8.

$$\left[R' : \mathfrak{B}_{M,N}\right] = \frac{\omega(M)\omega(N)}{l} h^{-} \quad \textit{and} \quad [\mathfrak{I} : \mathfrak{B}_{M,N}] = \frac{\omega(M)\omega(N)}{l}.$$

6. Fueter type system

It is well-known that if $\tau \not\equiv 1 \pmod{l}$ is a solution of the system (K), then τ is also a solution of the following system of congruences considered by Fueter [6] in 1922 :

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

The Fueter type system corresponding to (K(N)) was observed by Agoh and Skula and they proved

Proposition 6.1 ([4], Proposition 3.5). *Let τ be an integer $\not\equiv 1 \pmod{l}$. Then τ is a solution of* (K(N)) *if and only if τ is a solution of the sysyem*

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

Further, the equivalent system to (F(N)) was given by means of the Skula polynomial.

Theorem 6.2 ([4], Theorem 5.10). *The system* (F(N)) *is equivalent to the system*

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

Referring to these results we will study the Fueter type system of congruences equivalent to (K(M,N)).

First, we shall prove

Proposition 6.3. *The system* (K(M,N)) *is equivalent to the system*

$$\text{(F}(M,N)\text{)} \quad \sum_{v=1}^{l-1} \left(\left[\frac{MNvk}{l}\right] - N \left[\frac{Mvk}{l}\right] - M \left[\frac{Nvk}{l}\right] + MN \left[\frac{vk}{l}\right] \right) \frac{1}{v} t^v$$
$$\equiv 0 \pmod{l} \ (1 \le k \le l-1).$$

Proof. Recall the polynomial identity given in Proposition 3.2 and take $m{=}-1$. For a positive integer a prime to l, we have $S_{l-1}(a) \equiv a - [a/l] \pmod{l}$ by Fermat's little theorem, and so

$$\begin{aligned} S_{l-1}(a; M, N) &= S_{l-1}(aMN) - N^l S_{l-1}(aM) - M^l S_{l-1}(aN) + (MN)^l S_{l-1}(a) \\ &\equiv - \left[\frac{aMN}{l}\right] + N \left[\frac{aM}{l}\right] + M \left[\frac{aN}{l}\right] - MN \left[\frac{a}{l}\right] \pmod{l}. \end{aligned}$$

Therefore,

$$\begin{aligned}
&\frac{(1-M)(1-N)}{2}\varphi_{l-1}(t)+\sum_{i=1}^{l-2}\binom{l-1}{i}(kMN)^{l-1-i}\left\{B_{i+1}^{(M,N)}\varphi_{l-i-1}(t)\right\}\\
&\qquad\equiv-\sum_{v=1}^{l-1}\left(\left[\frac{vkMN}{l}\right]-N\left[\frac{vkM}{l}\right]-M\left[\frac{vkN}{l}\right]+MN\left[\frac{vk}{l}\right]\right)\frac{1}{v}t^{v}\pmod{l}.
\end{aligned}$$

Here we see $\det[(kMN)^j]_{1\le k\le l-1,\,0\le j\le l-2}\not\equiv 0 \pmod{l}$, so the result follows. □

Note that $\tau\equiv 1 \pmod{l}$ is a solution of the both systems $(\mathrm{K}(M,N))$ and $(\mathrm{F}(M,N))$. In fact, one has $\varphi_i(1)=S_{i-1}(l-1)\equiv 0 \pmod{l}$ for $i=2,3,\cdots,l-1$ and $B_{l-1}^{(M,N)}\equiv(M^{l-1}-1)q_l(N)\equiv 0 \pmod{l}$ by the von Staudt-Clausen theorem and Fermat's little theorem, where $q_l(N)=(N^{l-1}-1)/l$ is the Fermat quotient of l with base N, $l\nmid N$. So we can confirm the statement by observing the congruence in the above proof.

Finally, we would like to translate Proposition 6.3 by using the Skula polynomial depending on the ideal $\mathfrak{B}_{M,N}$ of R.

Theorem 6.4. *The system* $(\mathrm{F}(M,N))$ *is equivalent to the system*

$$f_\alpha(t)\equiv 0 \pmod{l}\quad(\alpha\in\mathfrak{B}_{M,N}).$$

Proof. Let k and ρ be integers satisfying $r_\rho=k$, $1\le k\le l-1$, $0\le\rho\le l-2$. Putting $\alpha=s^\rho\beta'$ we get from Proposition 5.5

$$\alpha=\sum_{i=0}^{l-2}\left(\left[\frac{MNr_{-i+\rho}}{l}\right]-N\left[\frac{Mr_{-i+\rho}}{l}\right]-M\left[\frac{Nr_{-i+\rho}}{l}\right]\right)s^{i}.$$

Since for a positive integer a prime to l

$$\left[\frac{ar_{\mathrm{ind}\,v+\rho}}{l}\right]=\left[\frac{a\overline{vk}}{l}\right]=\left[\frac{avk}{l}\right]-a\left[\frac{vk}{l}\right]\quad(1\le v\le l-1),$$

it follows that

$$\begin{aligned}
f_\alpha(t)&=\sum_{v=1}^{l-1}\left(\left[\frac{MNr_{\mathrm{ind}\,v+\rho}}{l}\right]-N\left[\frac{Mr_{\mathrm{ind}\,v+\rho}}{l}\right]-M\left[\frac{Nr_{\mathrm{ind}\,v+\rho}}{l}\right]\right)\frac{1}{v}t^{v}\\
&=\sum_{v=1}^{l-1}\left(\left[\frac{MNvk}{l}\right]-MN\left[\frac{vk}{l}\right]\right)\frac{1}{v}t^{\nu}-N\sum_{v=1}^{l-1}\left(\left[\frac{Mvk}{l}\right]-M\left[\frac{vk}{l}\right]\right)\frac{1}{v}t^{v}\\
&\qquad-M\sum_{v=1}^{l-1}\left(\left[\frac{Nvk}{l}\right]-N\left[\frac{vk}{l}\right]\right)\frac{1}{v}t^{v}\\
&=\sum_{v=1}^{l-1}\left(\left[\frac{MNvk}{l}\right]-N\left[\frac{Mvk}{l}\right]-M\left[\frac{Nvk}{l}\right]+MN\left[\frac{vk}{l}\right]\right)\frac{1}{v}t^{v}.
\end{aligned}$$

On the other hand, noticing that $[a(l-1)/l] = a - 1 - [a/l]$ for $a > 0$, $l \nmid a$, we have

$$\begin{aligned}
&\sum_{v=1}^{l-1}\left(\left[\frac{MNv}{l}\right] - N\left[\frac{Mv}{l}\right] - M\left[\frac{Nv}{l}\right] + MN\left[\frac{v}{l}\right]\right)\frac{1}{v}t^v \\
&+\sum_{v=1}^{l-1}\left(\left[\frac{MNv(l-1)}{l}\right] - N\left[\frac{Mv(l-1)}{l}\right]\right. \\
&\qquad\qquad\left. -M\left[\frac{Nv(l-1)}{l}\right] + MN\left[\frac{v(l-1)}{l}\right]\right)\frac{1}{v}t^v \\
&= -(M-1)(N-1)\sum_{v=1}^{l-1}\frac{1}{v}t^v \equiv -(M-1)(N-1)f_\delta(t) \pmod{l},
\end{aligned}$$

where $l \nmid (M-1)(N-1)$. This completes the proof of the theorem. $\square$

Consequently, we can say that the system $(\mathrm{K}(M, N))$ is equivalent to the system mentioned in Theorem 6.4.

7. Addendum

Let $\mathfrak{B}_N$ be the ideal of R given in Definition 5.3 and $\mathfrak{B}_N(l)$ be the ideal of R_l defined by

$$\mathfrak{B}_N(l) = \left\{\sum_{i=0}^{l-2} a_i s^i \in R_l : \exists\, b_i \in a_i \text{ such that } \sum_{i=0}^{l-2} b_i s^i \in \mathfrak{B}_N\right\}.$$

Most recently, Skula ([16], Section 4) investigated basic properties of $\mathfrak{B}_N(l)$ and inclusion relation of these ideals for various integers N (see also [15], Section 4). In a personal communication of him to one of the authors of this paper the exact relationship between the ideal $\mathfrak{I}_N(l)$ treated in Section 2 and the above $\mathfrak{B}_N(l)$ has been shown.

Proposition 7.1. *Let N be an integer with $2 \le N \le l-1$ and γ $(= \alpha_1)$ be the element of R_l defined in Section 2. Then*

$$\begin{aligned}
\mathfrak{I}_N(l) &= \mathfrak{B}_N(l) \quad \text{if } q_l(N) \equiv 0 \pmod{l}, \\
\mathfrak{I}_N(l) \oplus \gamma R_l &= \mathfrak{B}_N(l) \quad \text{if } q_l(N) \not\equiv 0 \pmod{l}.
\end{aligned}$$

Proof. We shall follow to the proof communicated by Skula. Let ν_l be the l-adic value and $h(k)$ $(k \ge 1)$ be the integer defined as follows : for an integer m, $1 \le m \le l-2$, if $B_{l-m} \not\equiv 0 \pmod{l}$, then put $h(l-1-m) = 0$. Also, if $B_{l-m} \equiv 0 \pmod{l}$, then we provide that $h(l-1-m)$ is the largest positive integer c such that $B_{l^{c-1}(l-1-m)+1} \equiv 0 \pmod{l^c}$. Using these notations we define (cf., [16], Section 4)

$$\mu(m) = \begin{cases} \nu_l(N^f - 1) - 1 & \text{if } m = 1, \\ h(l-1-m) + \nu_l(N^f - 1) & \text{if } f \mid m-1 \text{ and } m \neq 1, \\ h(l-1-m) & \text{if } f \nmid m-1 \end{cases}$$

for a fixed integer N, where f is the order of N mod l. Then the system

$$\{\alpha_m : \mu(m) = 0,\ 1 \leq m \leq l-2,\ m \text{ odd}\} \cup \{\delta\}$$

forms a basis of the $\mathbb{Z}_l$-module $\mathfrak{B}_N(l)$ (cf., [15, Theorem 4.7-(c)] for the case $N = 2$). We also see that the system

$$\begin{aligned} &\left\{\alpha_m : B_{l-m}^{(N)} \not\equiv 0 \pmod{l},\ 3 \leq m \leq l-2,\ m \text{ odd}\right\} \cup \{\delta\} \\ &= \{\alpha_m : \mu(m) = 0,\ 3 \leq m \leq l-2,\ m \text{ odd}\} \cup \{\delta\} \end{aligned}$$

forms a basis of the $\mathbb{Z}_l$-module $\mathfrak{I}_N(l)$. Here, we have $\mu(1) = 0 \Leftrightarrow q_l(N) \not\equiv 0 \pmod{l} \Leftrightarrow \alpha_1 \in \mathfrak{B}_N(l)$, which implies the result. $\square$

Acknowledgment. The authors are deeply grateful to Professor Ladislav Skula for his careful reading of the paper and many useful comments.

References

[1] Agoh, T., *On the criteria of Wieferich and Mirimanoff*, C.R. Math. Rep. Acad. Sci. Canada **8**(1989), 49-52.
[2] Agoh, T., *On the Kummer-Mirimanoff congruences*, Acta Arith. **55**(1990), 141-156.
[3] Agoh, T., *Some variations and consequences of the Kummer-Mirimanoff congruences*, Acta Arith. **62**(1992), 73-96.
[4] Agoh, T. and Skula, L., *Kummer type congruences and Stickelberger subideals*, Acta Arith. **75** (1996), 235-250.
[5] Benneton, G., *Sur le dernier théorème de Fermat*, Ann. Sci. Univ. Besançon Math. **3**(1974), 15 pp.
[6] Fueter, R., *Kummers Kriterium zum letzten Theorem von Fermat*, Math. Ann. **85**(1922), 11-20.
[7] Granville, A., *Diophantine equations with varying exponents* (*with special reference to Fermat's last theorem*), Ph.D. thesis, Queen's University, 1987.
[8] Iwasawa, K., *A class number formula for cyclotomic field*, Ann. of Math. **76**(1962), 171-179.
[9] Sinnott, W., *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. **108**(1978), 107-134.
[10] Sinnott, W., *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62**(1980), 181-234.
[11] Skula, L., *A remark on Mirimanoff polynomials*, Comment. Math. Univ. St. Paul. **31**(1982), 89-97.
[12] Skula, L., *Systems of equations depending on certain ideals*, Arch. Math. (Brno) **21**(1985), 23-38.
[13] Skula, L., *Some bases of the Stickelberger ideal*, Math. Slovaca **43**(1993), 541-571.
[14] Skula, L., *Agoh's bases of the Stickelberger ideal*, Math. Slovaca **44**(1994), 663-670.

[15] Skula, L., *On a special ideal contained in the Stickelberger ideal*, J. of Number Theory, **58** (1996), 173-195.
[16] Skula, L., *Inclusion among special Stickelberger subideals*, to appear in the Proceedings of the 12-th Czecho-Slovak Number Theory Conference (1995).

T. Agoh and K. Mori
Department of Mathematics
Science University of Tokyo
Noda, Chiba 278
Japan

E-mail address: agoh@ma.noda.sut.ac.jp