Ladislav Skula
Systems of equations depending on certain ideals

*Archivum Mathematicum*, Vol. 21 (1985), No. 1, 23--38

Persistent URL: [http://dml.cz/dmlcz/107212](http://dml.cz/dmlcz/107212)

**Terms of use:**

© Masaryk University, 1985

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to
digitized documents strictly for personal use. Each copy of any part of this document must contain
these *Terms of use.*
SYSTEMS OF EQUATIONS DEPENDING ON CERTAIN IDEALS

LADISLAV SKULA, Brno
(Received January 24, 1984)

Abstract. This paper deals with the special system of equations over the Galois field \( \mathbb{Z}(l) \) (\( l \) prime) depending on the certain ideals \( \mathfrak{I}(\mathfrak{P}) \) of the group ring of a cyclic group of order \( l - 1 \) over \( \mathbb{Z}(l) \). If \( \mathfrak{I}(\mathfrak{P}) \) is the Stickelberger ideal modulo \( l \), then we get a system of equations in certain sense equivalent to the Kummer's system of equations.

Keywords: Kummer's system of equations, Stickelberger ideal, the first case of Fermat's last theorem, Mirimanoff polynomials, group ring of a cyclic group over the Galois field.

0. Introduction

The main reason of this paper is the study of the Kummer's system of equations (\( K \)) (Section 6) used for the solution of the first case of Fermat's last theorem ([2], [1], [6]). In this section the system of equations (\( S \)) over the field \( \mathbb{Z}(l) \) of congruence classes modulo \( l \) is presented by means of the Stickelberger ideal \( \mathfrak{I}(\mathfrak{P}) \) modulo \( l \) and it is shown that an element \( x \in \mathbb{Z}(l), x \neq -1 \) is a solution of the system (\( K \)) if and only if \( x \) is a solution of the system (\( S \)) (Theorem 6.6).

This article refers to the paper [8] where the systems of equations (\( M \)) and (\( L \)) are considered. The system (\( M \)) is defined by means of the Mirimanoff polynomials \( \varphi_i(t) \) and Mirimanoff transformed the Kummer's system into the system (\( M \)) ([5]).

The system (\( L \)) is defined by means of the Le Lidec polynomials and Le Lidec showed the relation between these polynomials and the Mirimanoff polynomials ([3], [4]). This implies the relation between the solutions of (\( M \)) and (\( L \)).

The system (\( S \)) considered as a system of congruences) has been introduced in [8], but it was completed by the congruence \( \varphi_{l-1}(t) \equiv 0 \pmod{l} \). Under this assumption the relation between the solutions of (\( S \)) and (\( L \)) was shown here.

In this paper the system of equations of the more general form depending on the ideals of the subring \( \mathfrak{R}^-(l) \) of certain group ring \( \mathfrak{R}(l) \) are studied. A bound for the number of solutions of such system is presented (Theorem 5.5).
The important notion in this field is a special automorphism $F$ of the vector space $\mathfrak{R}(l)$. The ideals of the ring $\mathfrak{R}(l)$ are studied which are generated by the images of the ideals of $\mathfrak{R}^-(l)$ at this automorphism $F$ (Theorem 3.7).

1. Notation and Basic Assertions

In this paper we designate by
- $l$ a prime $\geq 5$
- $\mathbb{Z}(l)$ the field of congruence classes modulo $l$
- $0, 1 \in \mathbb{Z}(l)$ the cosets modulo $l$ containing integers $0, 1$, thus an integer $n$ can be considered an element of $\mathbb{Z}(l)$
- $G$ a multiplicative cyclic group of order $l - 1$
- $s$ a generator of $G$, hence $G = \{1 = s^0, s, s^2, \ldots, s^{l-2}\}$

$$\sum_{i=0}^{l-2} \delta_i = \sum_{i=0}^{l-2} \delta_i$$

$a$ a primitive root modulo $l$

$\text{ind } x$ index of $x$ relative to the primitive root $r$ of $l$

$r_i$ the integer $0 < r_i < l$, $r_i \equiv r^i \pmod{l}$ for integer $i \geq 0$, $r_i r_i^{-1} \equiv 1 \pmod{l}$ for integer $i < 0$

$\mathfrak{R}(l) = \mathbb{Z}(l) [G] = \{\sum_{i} a_i s^i : a_i \in \mathbb{Z}(l)\}$ the group ring of $G$ over $\mathbb{Z}(l)$, here for an integer $j$ we define $a_j = a_i$ where $0 \leq i \leq l - 2$, $i \equiv j \pmod{l - 1}$

$\mathfrak{a}(t) = \sum_{i} a_i t^i \in \mathbb{Z}(l) [t]$ for $\alpha = \sum_{i} a_i s^i \in \mathfrak{R}(l)$

$\mathfrak{R}^-(l) = \left\{ \alpha \in \mathfrak{R}(l) : \alpha = \sum_{i} a_i s^i, a_i + a_{i+\frac{l-1}{2}} = 0 \text{ for } 0 \leq i \leq \frac{l-3}{2} \right\}$

$\mathfrak{F} \mathfrak{L}(l) = \{\alpha = \sum_{i} a_i s^i \in \mathfrak{R}(l) : \sum_{i=0}^{l-2} a_i (i \text{ odd}) = \sum_{i=0}^{l-2} a_i (i \text{ even})\}$

$\mathfrak{F} \mathfrak{R}(l) = \{\alpha = \sum_{i} a_i s^i \in \mathfrak{R}(l) : \sum_{i=0}^{l-2} a_i r_{it} = 0\}$ for an integer $0 \leq T \leq l - 2$.

For an integer $v (l \nmid v)$ we denote by $\mathfrak{F}$ the integer $0 < v < l$, $v \cdot v \equiv 1 \pmod{l}$.

For $\alpha = \sum_{i} a_i s^i \in \mathfrak{R}(l)$ put

$$F(\alpha) = \sum_{v=1}^{l-1} a_{-\text{ind}_v} v^\psi.$$

Clearly,

$F$ is an automorphism of the vector space $(\mathfrak{R}(l), +)$ over $\mathbb{Z}(l)$.

For $\emptyset \neq M \subseteq \mathfrak{R}(l)$ we denote by $\mathfrak{F}(M)$ the ideal of the ring $\mathfrak{R}(l)$ generated by the set $F(M)$.

Obviously,

1.1. The ring $\mathfrak{R}(l)$ is isomorphic to the quotient ring $\mathbb{Z}(l) [t] / (t^{l-1} - 1)$. This isomorphism is induced by the mapping
for \( \varphi(t) \in \mathbb{Z}(l)[t] \) and \( \varphi(s) \in \mathcal{R}(l) \).

1.2. \( \mathcal{R}^{-}(l) = \mathcal{R}(l) \left( 1 - s^{\frac{l-1}{2}} \right) \),
\[ \mathcal{L} = \mathcal{R}(l) (1 + s). \]

Proof. The first assertion is obvious.

a) Let \( \alpha = \sum a_i s^i \in \mathcal{L} \). Put
\[ x_i = a_i - a_{i-1} + a_{i-2} - \ldots + (-1)^i a_0 \quad (0 \leq i \leq l - 3), \]
\[ x_{i-2} = 0, \]
\[ \beta = \sum x_i s^i \in \mathcal{R}(l). \]

Then \( \beta(1 + s) = \sum x_i s^i + \sum x_i s^{i+1} = \sum c_i s^i \), where
\[ c_i = x_i + x_{i-1} \quad \text{for } 1 \leq i \leq l - 2 \]
\[ c_0 = x_0 + x_{l-2}. \]

One has \( c_i = a_i \), hence \( \beta(1 + s) = \alpha. \)

b) Let \( \alpha = \beta(1 + s) \) for a \( \beta = \sum b_i s^i \in \mathcal{R}(l). \)

Then one has \( \alpha = \beta(1 + s) = \sum b_i s^i + \sum_{i=1}^{l-2} b_{i-1} s^i + b_{l-2} \), hence
\[ a_i = b_i + b_{i-1} \quad \text{for } 1 \leq i \leq l - 2 \]
\[ a_0 = b_0 + b_{l-2}. \]

This follows
\[ \sum_{i=0}^{l-2} a_i (i \text{ odd}) = a_1 + a_3 + \ldots + a_{l-2} = \sum b_i, \]
\[ \sum_{i=0}^{l-2} a_i (i \text{ even}) = a_0 + a_2 + \ldots + a_{l-3} = \sum b_i. \]

Thus \( \alpha \in \mathcal{L}. \)

1.3. \( \mathcal{F}(\mathcal{R}^{-}(l)) = \mathcal{L}. \)

Proof. Since \( 1 - s^{\frac{l-1}{2}} \in \mathcal{R}^{-}(l) \) and \( F \left( 1 - s^{\frac{l-1}{2}} \right) = 1 + s \), one has \( \mathcal{L} \subseteq \mathcal{F}(\mathcal{R}^{-}(l)). \) For \( 0 \leq u \leq \frac{l-3}{2} \) put
\[ \alpha_u = s^u \left( 1 - s^{\frac{l-1}{2}} \right) = s^u - s^{u + \frac{l-1}{2}}. \]

The set \( \{ \alpha_u : 0 \leq u \leq \frac{l-3}{2} \} \) is a system of group generators of the group \( (\mathcal{R}^{-}(l), +) \), hence
LADISLAV SKULA

\[ \mathcal{F}(\mathfrak{R}^{-}(l)) = \mathcal{F}\left( \left\{ x_{u} : 0 \leq u \leq \frac{l-3}{2} \right\} \right). \]

Since
\[ \mathcal{F}(x_{u}) = r_{u}s^{r-u} + r_{u}s^{r-\frac{l-3}{2}} \in B, \]
onone has \( \mathcal{F}(\mathfrak{R}^{-}(l)) \subseteq \mathfrak{R}. \)

1.4. If \( 0 \leq T \leq l-3 \) is even, then
\[ \mathcal{F}^{-}(l) = \mathfrak{R}^{-}(l). \]

Proof. For \( \alpha = \sum a_{i}s^{i} \in \mathfrak{R}^{-}(l) \) we have
\[ \sum_{i} a_{i}r_{iT} = \sum_{i=0}^{\frac{l-3}{2}} a_{i}r_{iT} + \sum_{i=0}^{\frac{l-3}{2}} a_{i+1} r_{\frac{i+1}{2}} = 0. \]

2. Ideals of the Ring \( \mathfrak{R}(l) \)

2.1. Proposition. Let \( I \) be a nonzero ideal of the ring \( \mathfrak{R}(l) \) and \( M \) be a set of generators of \( I \). Then
\[ I = (s - a_{1}) \cdots (s - a_{k}) \mathfrak{R}(l), \]
where \( a_{1}, \ldots, a_{k} \) are all distinct nonzero solutions of the following system of equations over \( \mathbb{Z}(l) \):
\[ \alpha(t) = 0 \quad \text{for } \alpha \in M. \]

Proof. I. Let \( g(t) \) be the greatest common divisor of the polynomial \( \alpha(t) (\alpha \in M) \) in \( \mathbb{Z}(l)[t] \) and let \( g_{\alpha}(t) \in \mathbb{Z}(l)[t], g_{\alpha}(t)g(t) = \alpha(t) \) for each \( \alpha \in M. \)

For each \( \beta \in I \) there exist \( b_{\alpha}(t) \in \mathbb{Z}(l)[t] \) such that \( \beta = \sum b_{\alpha}(s) \cdot \alpha(\alpha \in M), \) hence
\[ \beta = g(s) \sum b_{\alpha}(s) g_{\alpha}(s) (\alpha \in M) \in g(s) \cdot \mathfrak{R}(l). \]
Thus
\[ I \subseteq g(s) \mathfrak{R}(l). \]

Since \( g(s) \) is a product of linear factors, \( g(s) = \sum h_{\alpha}(s) \alpha(\alpha \in M) \in I. \)

This implies
\[ g(s) \cdot \mathfrak{R}(l) \subseteq I, \]

hence
\[ I = g(s) \cdot \mathfrak{R}(l). \]

II. Let \( g(t) = h(t)(t - a_{1})^{b_{1}} \cdots (t - a_{k})^{b_{k}} \cdot t^{b} \), where \( a_{1}, \ldots, a_{k} \) are nonzero mutually different elements from \( \mathbb{Z}(l) \), \( b_{1}, \ldots, b_{k} \) positive integers, \( b \) non-negative

---

1) If this system has no nonzero solution, then \( I = \mathfrak{R}(l). \)
integer and \( h(t) \) an irreducible polynomial of degree \( \geq 2 \) over \( \mathbb{Z}(l) \) or \( h(t) = 1 \).
(The case \( k = 0 \) is also considered.)

For each integer \( x \) (\( 1 \leq x \leq l - 1 \)) there exists an integer \( y_x \) such that
\[
h(x) \cdot y_x \cdot (x - 1)(x - 2) \ldots [x - (x - 1)] [x - (x + 1)] \ldots [x - (l - 1)] \equiv 1 \pmod{l}.
\]

Put
\[
f(t) = \sum_{x=1}^{l-1} (t - 1)(t - 2) \ldots [t - (x - 1)] [t - (x + 1)] \ldots [t - (l - 1)] \cdot y_x.
\]
Then for each integer \( z \) (\( 1 \leq z \leq l - 1 \)) one has

\[
h(z) \cdot f(z) \equiv 1 \pmod{l},
\]

hence
\[
h(t) \cdot f(t) \equiv 1(t^{l-1} - 1)
\]
and according to 1.1

(2)
\[
h(s) \cdot f(s) = 1.
\]

III. We construct for each integer \( 0 \leq a \leq l - 1 \) a polynomial \( f_a(t) \in \mathbb{Z}(l)[t] \)
in a similar way as the polynomial \( f \) in II such that
\[
f_a(z) (z - a) \equiv 1 \pmod{l}
\]
for each integer \( z \), \( 1 \leq z \leq l - 1 \), \( z \neq a \).

Thus
\[
f_a(z) (z - a)^2 \equiv (z - a) \pmod{l}
\]
for each integer \( z \), \( 1 \leq z \leq l - 1 \), hence
\[
f_a(t) (t - a)^2 \equiv (t - a) (t^{l-1} - 1).
\]

Using 1.1 one obtains

(3)
\[
f_a(s) (s - a)^2 = s - a.
\]

The proof now follows from (1), (2) and (3).

2.2. Definition. For \( K \subseteq \mathbb{Z}(l) \), \( 0 \notin K \) put
\[
I(K) = \mathfrak{R}(l), \quad \Pi(s - a) (a \in K)
\]
\[
I(\emptyset) = \mathfrak{R}(l).
\]

Obviously, \( I(K) \) is an ideal of the ring \( \mathfrak{R}(l) \).

2.3. Proposition. Each ideal \( I \) of the ring \( \mathfrak{R}(l) \) has the form
\[
I = I(K),
\]
where \( K \subseteq \mathfrak{R}(l) \), \( 0 \notin K \).

If \( K \subseteq \mathfrak{R}(l) \), \( L \subseteq \mathfrak{R}(l) \), \( 0 \notin K \cup L \) and \( I(K) = I(L) \), then \( K = L \).

Proof. According to Proposition 2.1 each ideal \( I \) of the ring \( \mathfrak{R}(l) \) has the given form. (\( \{0\} = I(\mathbb{Z}(l) - \{0\}) \)).
Let \( K \subseteq \mathbb{R}(l), L \subseteq \mathbb{R}(l), 0 \neq K \cup L, K \neq \emptyset \neq L \) and \( I(K) = I(L) \).

Then there exists \( \alpha \in \mathbb{R}(l) \) such that

\[
\Pi(s - a) (a \in K) = \alpha \Pi(s - b) (b \in L).
\]

According to Proposition 1.1 there exists a polynomial \( f(t) \in \mathbb{Z}(l) [t] \) such that

\[
\Pi(t - a) (a \in K) = \alpha(t) \Pi(t - b) (b \in L) + f(t)(t^l - 1).
\]

Substituting \( t = b \in L \) one obtains for each \( b \in L \)

\[
\Pi(b - a) (a \in K) = 0,
\]

hence \( b \in K \) and then \( L \subseteq K \). Substituting \( t = a \in K \) we get \( K \subseteq L \).

If \( K = \emptyset \) and \( L \neq \emptyset \), then there exist \( \alpha \in \mathbb{R}(l) \) and \( f(t) \in \mathbb{Z}(l) [t] \) such that

\[
1 = \alpha(t) \Pi(t - b) (b \in L) + f(t)(t^l - 1).
\]

Substituting \( t = b \in L \) we get \( 1 = 0 \), which is a contradiction.

This completes the proof.

3. The Ideals \( \mathcal{J}(\mathcal{F}) \)

Further, we denote by \( T \) the set

\[
T = \{1 \leq T \leq l - 2, \text{T odd}\}.
\]

For \( \mathcal{F} \subseteq T \) put

\[
\mathcal{J}(\mathcal{F}) = \bigcap_{T \in \mathcal{F}} \mathcal{J}_T(l) = \{\alpha = \sum_{i=0}^{l-3} a_i r_{iT} \in \mathbb{R}^-(l) : \sum_{i=0}^{l-3} a_i r_{iT} = 0 \text{ for each } T \in \mathcal{F}\},
\]

(\( \mathcal{J}(\emptyset) = \mathbb{R}^-(l) \)).

The number of elements of the set \( \mathcal{F} \) is denoted by \( i_{\mathcal{F}}(l) \), thus \( i_{\mathcal{F}}(l) = \text{card } \mathcal{F} \).

For \( L \in \mathcal{F} \) put

\[
\alpha_L = \sum_{i=0}^{l-3} r_{iT} s_i \in \mathbb{R}^-(l).
\]

3.1. Proposition. \( \mathcal{J}(T) = \{0\} \).

Proof. Let \( \alpha = \sum_{i=0}^{l-3} a_i r_{iT} \in \mathcal{J}(T) \). Then \( \sum_{i=0}^{l-3} a_i r_{iT} = 0 \) for each odd \( T, 1 \leq T \leq l - 2 \). Since \( D = \det (r_{iT}) \left( 0 \leq i \leq \frac{l-3}{2}, 1 \leq T \leq l - 2, \text{T odd} \right) \) is the Vandermonde determinant, we have \( D \neq 0 \) (mod \( l \)), which implies \( a_i = 0 \) for each \( 0 \leq i \leq \frac{l-3}{2} \), hence \( \alpha = 0 \).

The Proposition is proved.

For the same reason we get
3.2. Lemma. The elements \( \alpha_L \) \((L \in T)\) are linearly independent over the field \( \mathbb{Z}(l) \).

3.3. Proposition. Let \( \mathcal{I} \subseteq T \), \( \mathcal{I} \neq T \). Then the system \( S = \{ \alpha_L : L \in T - \mathcal{I} \} \) forms a basis of the vector space \( \mathcal{I}(\mathcal{I}) \) over the field \( \mathbb{Z}(l) \).

Proof. According to 3.2 the elements from \( S \) are linearly independent over \( \mathbb{Z}(l) \). Since for \( T \in \mathcal{I} \) and \( L \in T - \mathcal{I} \) the integer \( T - L \) is even and \( l - 1 \) does not divide \( T - L \), we have \( \sum_{i=0}^{l-3} r_{iT} = 0 \) (mod \( l \)), thus \( S \subseteq \mathcal{I}(\mathcal{I}) \).

The space of solutions of the following system of equations

\[
\sum_{i=0}^{l-3} a_i r_{iT} = 0 \quad (T \in \mathcal{I})
\]

with unknowns \( a_i \) over \( \mathbb{Z}(l) \) has dimension \( \frac{l - 1}{2} - i_\mathcal{I}(l) = \text{card } S \). Hence \( S \) forms a basis of \( \mathcal{I}(\mathcal{I}) \) over \( \mathbb{Z}(l) \).

3.4. Corollary. \( \text{card } \mathcal{I}(\mathcal{I}) = l^{\frac{l-1}{2}} \) for each \( \mathcal{I} \subseteq T \).

3.5. Corollary. The ideal \( \mathcal{I}(\mathcal{I}) \) of the ring \( \mathcal{R}(l) \) is generated by elements \( F(\alpha_L) \) \((L \in T - \mathcal{I})\).

3.6. Proposition. For each \( L \in T \)

\[
F(\alpha_L) = \sum_{v=1}^{l-1} v^{L-1} s^v = \sum_v v^{L-1} s^v.
\]

Proof. Let \( 1 \leq v \leq l - 1 \), \( i = - \text{ind } v \), \( a_i = r_{-1L} \). Then \( v = r_{-i} \) and \( a_{-\text{ind } v} = r_{-1L} \equiv r_{-i(L-1)} \equiv v^{L-1} \) (mod \( l \)). Hence \( F(\alpha_L) = \sum_{v=1}^{l-1} v^{L-1} s^v = \sum_v v^{L-1} s^v \).

3.7. Theorem. Let \( \mathcal{I} \subseteq T \). Then

\[
\mathcal{I}(\mathcal{I}) = (s - a_1) \ldots (s - a_k) \mathcal{R}(l),
\]

where \( a_1, \ldots, a_k \) are all distinct solutions of the following system of equations over \( \mathbb{Z}(l) \): \( \sum_v v^{L-1} t^v = 0 \) \((L \in T - \mathcal{I})\).

Proof. The theorem follows from 3.5, 3.6 and 2.1 for \( \mathcal{I} \neq T \). If \( \mathcal{I} = T \), we understand under a solution of the given system each element from \( \mathbb{Z}(l) \). According to 3.1 \( \mathcal{I}(\mathcal{I}) = \{0\} = \mathcal{R}(l) \Pi(s - a) \) \((a \in \mathbb{Z}(l))\). The theorem is proved.

3.8. Remark. The coset \(-1\) is a solution of \( \sum_v v^{L-1} t^v = 0 \) for each \( L \in T \), hence by 3.7 \( \mathcal{I}(\mathcal{I}) \subseteq (s + 1) \mathcal{R}(l) = \mathcal{I} \) for each \( \mathcal{I} \subseteq T \), which is in accordance with 1.3.

\(^1\) \( 0^{l-1} = 1 \) by definition.
From 2.3 and from the relation \( R^{-}(l) = \left( \frac{l-1}{s^2} - 1 \right) R(l) \) we get

**3.9. Proposition.** Each ideal \( I^{-} \) of the ring \( R^{-}(l) \) is of the form \( I^{-} = \mathcal{I}(\mathcal{T}) = R^{-}(l) \Pi(s - r_T) \) \((T \in \mathcal{T})\), where \( \mathcal{T} \subseteq \mathcal{T} \).

**4. Some Special Cases**

**4.1. Definition.** For \( 2 \leq i \leq l - 1 \) the polynomials

\[
\phi_i(t) = \sum_{v=1}^{l-1} (-1)^{v-1} v^{i-1} t^v
\]

are called the *Mirimanoff polynomials* and

\[
\phi_i(t) \equiv (t + 1)^{l-i} P_i(t) \pmod{l},
\]

where \( P_i(t) \) are certain polynomials over the ring of integers divisible by \( t - t^2 \) for each odd \( i \).

Especially for \( i = 3, 5, 7, 9 \) we have

\[
\begin{align*}
P_3(t) &= t - t^2, \\
P_5(t) &= (t - t^2) \cdot u(t), \\
P_7(t) &= (t - t^2) \cdot v(t), \\
P_9(t) &= (t - t^2) \cdot w(t),
\end{align*}
\]

where

\[
\begin{align*}
u &= u(t) = t^2 - 10t + 1, \\
v &= v(t) = t^4 - 56t^3 + 246t^2 - 56t + 1, \\
w &= w(t) = t^6 - 246t^5 + 4,047t^4 - 11,572t^3 + 4,047t^2 - 246t + 1.
\end{align*}
\]

(S. [1] Nr. 41 and 42.)

For these polynomials \( u, v, w \) the following assertion holds:

**4.2. Proposition.** (a) For \( l \geq 5 \) there does not exist any integer \( \tau \) such that

\[
\begin{align*}
u(\tau) &\equiv 0 \pmod{l}, \\
v(\tau) &\equiv 0 \pmod{l}.
\end{align*}
\]

(b) For \( l \geq 7 \) there does not exist any integer \( \tau \) such that

\[
\begin{align*}
u(\tau) &\equiv 0 \pmod{l}, \\
w(\tau) &\equiv 0 \pmod{l}.
\end{align*}
\]

(c) For \( l \geq 7 \) there does not exist any integer \( \tau \) such that

\[
\begin{align*}
v(\tau) &\equiv 0 \pmod{l}, \\
w(\tau) &\equiv 0 \pmod{l}.
\end{align*}
\]
Proof. Put
\[ a = a(t) = t^2 - 46t + 1, \]
\[ \beta = \beta(t) = t^4 - 236t^3 + 1,686t^2 + 5,524t + 57,601, \]
\[ \gamma = \gamma(t) = 138t^3 - 33,283t^2 + 938,188t + 312,977, \]
\[ \delta = \delta(t) = 138t - 7,063 \]
and
\[ a = a(t) = t^2, \]
\[ b = b(t) = 99t - 10, \]
\[ c = c(t) = 231,329t^2 - 52,406t + 889 = 7.33,047t^2 - 52,406t + 7.127. \]

Then we get by calculation
\[ (1) \quad v = u\alpha - 216\alpha, \]
\[ (2) \quad w = u\beta + 5,760b, \]
\[ (3) \quad \gamma v - \delta w = 360c. \]

Assume that \( l \geq 7 \) and \( \tau \) is an integer such that
\[ v(\tau) \equiv 0 \pmod{l}, \]
\[ w(\tau) \equiv 0 \pmod{l}. \]

If \( \tau \equiv 1 \pmod{l} \), then \( 0 \equiv v(1) = 136 = 2^3 \cdot 17 \pmod{l} \) and \( 0 \equiv w(1) = -3,968 = 2^7 \cdot 31 \pmod{l} \). If \( \tau \equiv -1 \pmod{l} \), then \( 0 \equiv v(-1) = 360 = 2^3 \cdot 3^2 \cdot 5 \pmod{l} \). Thus \( \tau \equiv \pm 1 \pmod{l} \).

Obviously \( l \nmid \tau \) and there exists an integer \( x \) such that
\[ \tau \cdot x \equiv 1 \pmod{l}. \]

Then \( \tau \equiv x \pmod{l} \) and
\[ v(\tau) \equiv 0 \pmod{l}, \]
\[ w(\tau) \equiv 0 \pmod{l} \]
and according to (3)
\[ c(\tau) \equiv 0 \pmod{l}, \]
\[ c(\tau) \equiv 0 \pmod{l}. \]

If \( l = 7 \), then \( c(t) \equiv 3t \pmod{l} \), hence \( \tau \equiv 0 \pmod{l} \), which is a contradiction.

If \( l = 127 \), then \( c(t) \equiv t(62t + 45) \pmod{l} \), hence \( 62\tau + 45 \equiv 0 \pmod{l} \) and \( 62x + 45 \equiv (mod l) \). This follows \( \tau \equiv x \pmod{l} \), therefore \( \tau \equiv \pm 1 \pmod{l} \), which is a contradiction.

If \( l/33,047 \), we obtain a contradiction in a similar way.

Let \( l \geq 11 \) and \( l \nmid 127,33,047 \). Then \( c(t) \equiv 7.33,047(t - \tau) (t - x) \pmod{l} \), which implies
\[ 7.33,047 \equiv 7.127 \pmod{l}, \]
hence \( l/2^3 \cdot 5.823 \), thus \( l = 823 \). Then

\[
c(t) = 66t^2 + 266t + 66 \pmod{l},
\]

\[
eq 2 \cdot (33t^2 + 133t + 33).
\]

The discriminant of \( c(t) \) is congruent to 165 = 3\cdot5\cdot11 \pmod{823} and we have

for the Legendre symbol \( \left( \frac{165}{823} \right) \):

\[
\left( \frac{165}{823} \right) = \left( \frac{3}{823} \right) \left( \frac{5}{823} \right) \left( \frac{11}{823} \right) = \left( \frac{823}{3} \right) \left( \frac{823}{5} \right) \left( \frac{823}{11} \right) = \left( \frac{1}{3} \right) \left( \frac{3}{5} \right) \left( \frac{9}{11} \right) = -1.
\]

This completes the proof of (c).

Using (1) and (2) we can prove (a) and (b).

The proposition is proved.

For \( L \in T, L \neq 1 \) we have

\[
\sum_v v^{L-1} \tau^v \equiv 1 \pmod{l} = -\varphi_L(-t) - t^{L-1} + 1 = -(1 - t)^{L-1} P_L(-1) - t^{L-1} + 1 = t(1 - t)^{L-1}(1 + t) y_L(t) - t^{L-1} + 1,
\]

where \( y_L(t) \) is the polynomial \( \frac{-P_L(-t)}{t(1 + t)} \) over the ring of integers. Therefore

**4.3. Proposition.** Let \( L \in T, L \neq 1 \) and let \( \tau \) be an integer. Then

\[
\sum_v v^{L-1} \tau^v \equiv 0 \pmod{l},
\]

if and only if \( \tau \equiv \pm 1 \pmod{l} \) or

\[
y_L(\tau) \equiv 0 \pmod{l}.
\]

Now we give the form of the ideal \( \mathcal{I}(\mathcal{I}) \) for \( i_{\mathcal{I}}(l) = 0, 1, 2 \).

For \( i_{\mathcal{I}}(l) = 0 \) one has

\[
\mathcal{I}(\mathcal{I}) = (1 + s) R(l) = \mathcal{L},
\]

since \( \mathcal{I} = \emptyset \) and \( \mathcal{I}(\mathcal{I}) = \mathcal{I}(\mathcal{R}^{-}(l)) = \mathcal{L} = (1 + s) R(l) \) according to 1.3 and 1.2.

For \( i_{\mathcal{I}}(l) = 1 \) we get

**4.4. Theorem.** If \( \mathcal{I} = \{1\} \), then

\[
\mathcal{I}(\mathcal{I}) = \mathcal{I}(\mathcal{I}_{\mathcal{I}}(l)) = (s + 1) (s - 1) R(l).
\]

If \( \mathcal{I} = \{T\}, \) where \( T \in T - \{1\} \) we have

\[
\mathcal{I}(\mathcal{I}) = \mathcal{I}(\mathcal{I}_{\mathcal{T}}(l)) = (s + 1) R(l) \quad \text{for } l \geq 7
\]
and
\[ \mathcal{F}(\mathcal{I}(\mathcal{F})) = \mathcal{F}(\mathcal{I}_{3}(5)) = (s + 1)(s + 2)(s + 3) \mathcal{R}(l) \quad \text{for } l = 5. \]

**Proof.** For \( \mathcal{I} = \{1\} \) the proposition follows from 3.7 and 4.3 according to \( y_3(t) = 1 \).

Since \( y_3(t) = u(-t) \) and \( y_5(t) = v(-t) \), the congruence \( y_3(t) \equiv 0 \pmod{7} \) has no solution and the congruences \( y_5(t) \equiv 0 \pmod{l} \), \( y_7(t) \equiv 0 \pmod{l} \) has also no solution for \( l \geq 11 \) by 4.2. This completes the proof according to 3.7 and 4.3.

For \( i_{\mathcal{F}}(l) = 2 \) we obtain in a similar way from 3.7, 4.3 and 4.2:

4.5. **Theorem.** Let \( \mathcal{F} \subseteq T \) and \( i_{\mathcal{F}}(l) = 2 \). Then it holds

(a) \( l = 5 \Rightarrow \mathcal{F}(\mathcal{I}(\mathcal{F})) = \{0\} \),

(b) \( l \geq 7, 1 \in \mathcal{F} \Rightarrow \mathcal{F}(\mathcal{I}(\mathcal{F})) = (s + 1)(s - 1) \mathcal{R}(l) \),

(c) \( l = 7, 1 \notin \mathcal{F}(\mathcal{I} = \{3, 5\}) \Rightarrow \mathcal{F}(\mathcal{I}(\mathcal{F})) = (s + 1)(s + 2)(s + 3)(s + 4) \).

5. Special System of Equations Depending on \( \mathcal{I}(\mathcal{F}) \)

5.1. **Definition.** For \( \alpha = \sum a_i s^i \in \mathcal{R}(l) \) put

\[ f_\alpha(t) = \sum_{v=1}^{L-1} a_{-\text{ind}} v t^v \in \mathcal{Z}(l) \{t\}. \]

5.2. **Theorem.** For \( \mathcal{F} \subseteq T \) the system of equations (over the field \( \mathcal{Z}(l) \))

(1) \( f_\alpha(t) = 0, \alpha \in \mathcal{I}(\mathcal{F}) \)

is equivalent to the system of equations (over \( \mathcal{Z}(l) \))

(2) \( \sum_{v=1}^{L-1} v^{L-1} t^v = 0, L \in T - \mathcal{F}. \)

**Proof.** Let \( I \) be the ideal of the ring \( \mathcal{R}(l) \) generated by the set \( \{f_\alpha(s) : \alpha \in \mathcal{I}(\mathcal{F})\} \). Then \( I = \mathcal{F}(\mathcal{I}(\mathcal{F})) \) and according to 2.1

\[ I = (s - a_1) \ldots (s - a_k) \mathcal{R}(l), \]

where \( a_1, \ldots, a_k \) are all distinct nonzero solutions of the system (1). Then the theorem follows from 3.7 and 2.3.

5.3. **Definition.** Put

\[ \mathcal{R}^*(l) = \{ \alpha = \sum a_i s^i \in \mathcal{R}(l) : a_0 = a_1, a_1 = a_{i-1} (2 \leq i \leq \frac{l-1}{2}) \}. \]

1) It means that \( \tau \in \mathcal{Z}(l) \) is a solution of (1) if and only if it is a solution of (2). If \( \mathcal{F} = T \) then each \( \tau \in \mathcal{Z}(l) \) is a solution of (1) and (2) by definition.
5.4. Proposition. Let \(1 \leq n \leq l - 2\), \(m = \left\lfloor \frac{1}{2} (l - n - 1) \right\rfloor\) and \(\beta = (s - b_1) \cdot \ldots \cdot (s - b_n)\), where \(b_1, \ldots, b_n\) are distinct nonzero elements from \(\mathbb{Z}(l)\). Then

\[
\text{card } [\mathfrak{A}(l) \cdot \beta \cap \mathfrak{A}^*(l)] \leq \begin{cases} 
\binom{l}{m} & \text{for } n \text{ even,} \\
\binom{l}{m+1} & \text{for } n \text{ odd.}
\end{cases}
\]

Proof. I. Put \(M = \mathfrak{A}(l) \cdot \beta \cap \mathfrak{A}^*(l)\) and \(M' = \{\beta \cdot \alpha : \alpha \in \mathfrak{A}(l), \beta \cdot \alpha \in \mathfrak{A}^*(l), \alpha = \sum_{i=0}^{l-2-n} a_i s^i\}\). Obviously, \(M' \subseteq M\). Let \(\omega \in M\). Then there exists \(\alpha = \sum_i a_i s^i \in \mathfrak{A}(l)\) such that \(\omega = \beta \cdot \alpha \in \mathfrak{A}^*(l)\). Put

\[
f(t) = (t - b_{n+1}) (t - b_{n+2}) \ldots (t - b_{l-1}),
\]

where \(\{b_1, b_2, \ldots, b_{l-1}\} = \mathbb{Z}(l) - \{0\}\). Let \(q(t), r(t) \in \mathbb{Z}(l)[t]\), \(\deg r < \deg f = l - 1 - n\) and

\[
\alpha(t) = f(t) q(t) + r(t).
\]

Then

\[
\beta \cdot \alpha = \beta \cdot f(s) \cdot q(s) + \beta \cdot r(s).
\]

Since \(\beta \cdot f(s) = 0\), one has \(\beta \cdot \alpha = \beta \cdot r(s) \in M'\). Thus \(M = M'\).

II. Let \(\alpha_1 = \sum_{i=0}^{I-2-n} a_i^{(1)} s^i \in \mathfrak{A}(l), \alpha_2 = \sum_{i=0}^{I-2-n} a_i^{(2)} s^i \in \mathfrak{A}(l)\) and \(\beta \cdot \alpha_1 = \beta \cdot \alpha_2\). Then \(\alpha_1 = \alpha_2\).

According to 1.1

\[
\beta(t) \alpha_1(t) = \beta(t) \alpha_2(t) + g(t) (t^{l-1} - 1),
\]

where \(g(t) \in \mathbb{Z}(l)[t]\). Since \(\deg \beta(t) \alpha_1(t), \deg \beta(t) \alpha_2(t) \leq l - 2\), one obtains \(g(t) = 0\) and \(\alpha_1(t) = \alpha_2(t)\), thus \(\alpha_1 = \alpha_2\).

From I we get then

\[
\text{card } M = \text{card } \{\alpha = \sum_{i=0}^{I-2-n} a_i s^i \in \mathfrak{A}(l) : \beta \cdot \alpha \in \mathfrak{A}^*(l)\}.
\]

III. We have \(\beta = \beta_0 + \beta_1 s + \ldots + \beta_{n-1} s^{n-1} + \beta_n s^n\), where \(\beta_0, \ldots, \beta_{n-1}, \beta_n \in \mathbb{Z}(l), \beta_0 \neq 0, \beta_n = 1\). For \(\alpha = \sum_{i=0}^{I-2-n} x_i s^i \in \mathfrak{A}(l)\) we have \(\beta \cdot \alpha = \sum_i c_i s^i\) and

\[
\begin{align*}
&c_{i-2} = x_{i-2} - n \beta_n, \\
&c_{i-3} = x_{i-2} - n \beta_{n-1} + x_{i-3} - n \beta_n, \\
&\quad \vdots \\
&c_1 = \sum x_j \beta_{i-j} (\max \{0, i - n\} \leq j \leq \min \{l - 2 - n, i\}), \\
&c_0 = x_0 \beta_0.
\end{align*}
\]
The system
\[(4) \quad c_0 - c_1 = 0, \quad c_i - c_{i-1} = 0, \quad (2 \leq i \leq \frac{l-1}{2})\]
forms a system of \(\frac{l-1}{2}\) linear equations with unknowns \(x_0, x_1, \ldots, x_{l-2-n}\).

Assume \(m \geq 2\) and assume that for \(2 \leq k \leq m - 1\) we expressed the unknowns \(x_1, x_{l-2-n}, x_{l-3-n}, \ldots, x_{l-k-n}\) by means of the unknowns \(x_0, x_2, x_3, \ldots, x_k\) from the equations
\[c_0 - c_1 = 0, \quad c_i - c_{i-1} = 0, \quad (2 \leq i \leq k)\]

The unknowns \(x_0, x_1, \ldots, x_k, x_{k+1}\) occur in the expression \(c_{k+1}\) and the unknowns \(x_{l-2-n}, x_{l-3-n}, \ldots, x_{l-k-n}, x_{l-k-1-n}\) occur in the expression \(c_{l-k-1}\). The unknown \(x_{l-k-1-n}\) has the coefficient \(\beta_n = 1\).

Hence the unknowns \(x_1, x_{l-2-n}, x_{l-3-n}, \ldots, x_{l-m-n}\) are expressed by means of \(x_0, x_2, x_3, \ldots, x_m\) from the equations
\[c_0 - c_1 = 0, \quad c_i - c_{i-1} = 0, \quad (2 \leq i \leq m)\]

Thus the system (4) cannot have more than \(l - 1 - n - m\) free unknowns and
\[l - 1 - n - m = \begin{cases} m & \text{for } n \text{ even}, \\ m + 1 & \text{for } n \text{ odd}. \end{cases}\]

This gives the result for \(m \geq 2\). The case \(0 \leq m \leq 1\) is easy to show.

5.5. Theorem. Let \(T \subseteq T\). Then for the number \(n_T(l)\) of solutions of the system (1) different from \(-1\) it holds
\[n_T(l) \leq \begin{cases} 2i_T(l) & \text{for } 1 \notin \mathcal{T}, \\ 2i_T(l) - 1 & \text{for } 1 \in \mathcal{T}. \end{cases}\]

Proof. Obviously, if \(\tau\) is a solution of (2), then \(\tau^{-1}\) is also a solution of (2). Further \(-1\) is always a solution of (2) and 1 is a solution of (2) if and only if \(1 \notin \mathcal{T}\). Thus \(n = n_T(l) + 1\) is the number of solutions of (1) and \(n_T(l)\) is even if and only if \(1 \notin \mathcal{T}\).

Let \(-1, a_1, \ldots, a_{n-1}\) be the set of solutions of (1) and put \(\beta = (s + 1)(s + a_1) \ldots (s + a_{n-1})\). According to 3.7
\[\mathcal{F}(\mathcal{I}(\mathcal{T})) = \beta \cdot \mathcal{R}(l)\]
and obviously
\[\mathcal{F}(\mathcal{I}(\mathcal{T})) \subseteq \mathcal{F}(\mathcal{I}(\mathcal{T})) \cap \mathcal{R}(l).\]
From 3.4 we get
\[ \text{card } \mathcal{F}(\mathcal{I}(\mathcal{I})) = \text{card } \mathcal{I}(\mathcal{I}) = l^{\frac{l-1}{2} - i_{\mathcal{I}(\mathcal{I})}}, \]
hence according to 5.4
\[ \frac{l-1}{2} - i_{\mathcal{I}(\mathcal{I})} \leq \text{card } [\mathcal{R}(l) \cdot \beta \cap \mathcal{R}(l)] \leq \binom{l}{m+1} \text{ for } n \text{ even}, \]
\[ \frac{l-1}{2} - i_{\mathcal{I}(\mathcal{I})} + 1 \leq \text{card } [\mathcal{R}(l) \cdot \beta \cap \mathcal{R}(l)] \leq \binom{l}{m} \text{ for } n \text{ odd}, \]
where
\[ m = \left[ \frac{1}{2} (l - n - 1) \right] = \begin{cases} \frac{l-3}{2} - \frac{n_{\mathcal{I}(\mathcal{I})}}{2} & \text{for } 1 \not\in \mathcal{I}, \\ \frac{l-1}{2} - \frac{n_{\mathcal{I}(\mathcal{I})} + 1}{2} & \text{for } 1 \in \mathcal{I}. \end{cases} \]
Hence for 1 \not\in \mathcal{I}
\[ \frac{l-1}{2} - i_{\mathcal{I}(\mathcal{I})} \leq m + 1 = \frac{l-1}{2} - \frac{n_{\mathcal{I}(\mathcal{I})}}{2} \]
and
\[ n_{\mathcal{I}(\mathcal{I})} \leq 2i_{\mathcal{I}(\mathcal{I})}. \]
For 1 \in \mathcal{I} we have
\[ \frac{l-1}{2} - i_{\mathcal{I}(\mathcal{I})} \leq m = \frac{l-1}{2} - \frac{n_{\mathcal{I}(\mathcal{I})} + 1}{2}, \]
therefore
\[ n_{\mathcal{I}(\mathcal{I})} \leq 2i_{\mathcal{I}(\mathcal{I})} - 1. \]
The theorem is proved.

6. System of Equations Depending on the Stickelberger Ideal

6.1. Notation. The Stickelberger ideal \( \mathfrak{I} \) in the group ring \( \mathfrak{R} = \{ \sum a_i t^i : a_i \) \text{ } l\text{-adic integer}\} \) of the group \( G \) over the ring of \( l\text{-adic integers} \) is the ideal
\[ \mathfrak{I} = \{ x \in \mathfrak{R} : \exists q \in \mathfrak{R}, \sum r_i t^i = lx \} \]
of the ring \( \mathfrak{R} \).
\[ \text{Put } \mathfrak{R}^- = \{ \sum a_i t^i \in \mathfrak{R} : a_i + a_{i+1} + \cdots + a_{i+\frac{l-3}{2}} = 0 \text{ for } 0 \leq i \leq \frac{l-3}{2} \} \text{ and } \mathfrak{I}^- = \mathfrak{I} \cap \mathfrak{R}^- \text{. The Stickelberger ideal } \mathfrak{I}^-(l) \text{ modulo } l \text{ is defined as follows} \]
\[ \mathfrak{I}^-(l) = \{ \sum a_i t^i \in \mathfrak{R}^- : \exists b_i \in a_i, \Sigma b_i t^i \in \mathfrak{I}^- \} \]
(the \( l\text{-adic integers } b_i \) are considered the elements of the cosets \( a_i \)).

For the sequence of the Bernoulli numbers \( B_n \) we use the "even-index" notation, thus

36
For an odd integer $T$, $1 \leq T \leq l - 4$ such that $B_{T+1} \equiv 0 \pmod{l}$ let $h(T)$ be the positive integer such that

$$B_{h(T) - 1 + T} \equiv 0 \pmod{l^{h(T)}}$$

and for integer $X > h(T)$

$$B_{lX - 1 + T} \not\equiv 0 \pmod{l^X}.$$

If $B_{T+1} \not\equiv 0 \pmod{l}$, we put $h(T) = 0$.

For an integer $T$, $0 \leq T < l - 1$ and a positive integer $m$ put

$$\mathfrak{F}_{Tm} = \{\sum a_i T^{i} \in \mathfrak{A} : \sum a_i T^{i} \equiv 0 \pmod{m}\}$$

and

$$\mathfrak{F}_{T0} = \mathfrak{A}.$$
6.6. Theorem. The element $\tau \in \mathbb{Z}(l)$, $\tau \neq -1$, is a solution of the system (K) if and only if $-\tau$ is a solution of the system (S).

Proof. Let $\tau \in \mathbb{Z}(l)$, $\tau \neq -1$. Obviously, $\tau$ is a solution of (K) if and only if $\tau$ is a solution (over $\mathbb{Z}(l)$) of the system

\begin{equation}
\varphi_i(t) B_{1-i} = 0 \quad (3 \leq i \leq l-2, \text{ odd})
\end{equation}

and $\tau$ is a solution of (1) if and only if $\tau$ is a solution of the system

\begin{equation}
\varphi_i(t) = 0 \quad (3 \leq i \leq l-2, \text{ odd, } i \notin \mathcal{U}).
\end{equation}

Further, $\tau$ is a solution of (2) if and only if $-\tau$ is a solution of the system

\begin{equation}
\sum_{v=1}^{l-1} v^{L-1} t^v = 0, \quad L \in T - \mathcal{U}.
\end{equation}

Then we obtain the theorem from 5.2 and 6.4.

REFERENCES


L. Skula
Department of Mathematics
Faculty of Science, J. E. Purkyně University
Jandčkovo ná n. 2a, 662 95 Brno
Czechoslovakia