Archivum Mathematicum

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

ARCHIVUM MATHEMATICUM (BRNO)
Vol. 21 No. 1 (1985), 23–38

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 $\mathbf{Z}(l)$ (l prime) depending on the certain ideals $\mathfrak{J}(\mathscr{T})$ of the group ring of a cyclic group of order $l-1$ over $\mathbf{Z}(l)$. If $\mathfrak{J}(\mathscr{T})$ is the Stickelberger ideal modulo l, then we get a system of equations in certain sense equivalent to the Kummer's system of equations.

Key words: 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 $\mathbf{Z}(l)$ of congruence classes modulo l is presented by means of the *Stickelberger ideal* $\mathfrak{J}^-(l)$ modulo l and it is shown that an element $\tau \in \mathbf{Z}(l)$, $\tau \neq -1$ is a solution of the system (K) if and only if τ 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* transformated 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 $\geqq 5$
$\mathbf{Z}(l)$	the field of congruence classes modulo l
$0, 1 \in \mathbf{Z}(l)$	the cosets modulo l containing integers 0, 1, thus an integer n can be considered an element of $\mathbf{Z}(l)$
G	a multiplicative cyclic group of order $l - 1$
s	a generator of G, hence $G = \{1 = s^0, s, s^2, \ldots, s^{l-2}\}$
$\sum_i \delta_i = \sum_{i=0}^{l-2} \delta_i$	for suitable symbols δ_i
r	a primitive root modulo l
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 $i \geqq 0$, $r_i r^{-i} \equiv 1 \pmod l$ for integer $i < 0$

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

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

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

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

$\mathfrak{J}_T^-(l) = \{\alpha = \sum_i a_i s^i \in \mathfrak{R}^-(l) : \sum_i a_i r_{iT} = 0\}$ for an integer $0 \leqq T \leqq l - 2$.

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

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

$$F(\alpha) = \sum_{v=1}^{l-1} a_{-\operatorname{ind} v} \bar{v} s^v.$$

Clearly,

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

For $\emptyset \neq M \subseteq \mathfrak{R}(l)$ we denote by $\mathscr{F}(M)$ 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 $\mathbf{Z}(l)[t]/(t^{l-1} - 1)$. This isomorphism is induced by the mapping*

$$\varphi(t) \to \varphi(s)$$

for $\varphi(t) \in \mathbf{Z}(l)[t]$ *and* $\varphi(s) \in \mathfrak{R}(l)$.

1.2. $\mathfrak{R}^-(l) = \mathfrak{R}(l)\left(1 - s^{\frac{l-1}{2}}\right)$,

$$\mathfrak{L} = \mathfrak{R}(l)(1 + s).$$

Proof. The first assertion is obvious.

a) Let $\alpha = \sum_i a_i s^i \in \mathfrak{L}$. Put

$$x_i = a_i - a_{i-1} + a_{i-2} - \dots + (-1)^i a_0 \qquad (0 \leqq i \leqq l - 3),$$
$$x_{l-2} = 0,$$
$$\beta = \sum_i x_i s^i \in \mathfrak{R}(l).$$

Then $\beta(1 + s) = \sum_i x_i s^i + \sum_i x_i s^{i+1} = \sum_i c_i s^i$, where

$$c_i = x_i + x_{i-1} \qquad \text{for } 1 \leqq i \leqq l - 2$$
$$c_0 = x_0 + x_{l-2}.$$

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

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

Then one has $\alpha = \beta(1 + s) = \sum_i b_i s^i + \sum_{i=1}^{l-2} b_{i-1} s^i + b_{l-2}$, hence

$$a_i = b_i + b_{i-1} \qquad \text{for } 1 \leqq i \leqq l - 2$$
$$a_0 = b_0 + b_{l-2}.$$

This follows

$$\sum_{i=0}^{l-2} a_i(i \text{ odd}) = a_1 + a_3 + \dots + a_{l-2} = \sum_i b_i,$$
$$\sum_{i=0}^{l-2} a_i(i \text{ even}) = a_0 + a_2 + \dots + a_{l-3} = \sum_i b_i.$$

Thus $\alpha \in \mathfrak{L}$.

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

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

$$\alpha_u = s^u\left(1 - s^{\frac{l-1}{2}}\right) = s^u - s^{u+\frac{l-1}{2}}.$$

The set $\left\{\alpha_u : 0 \leqq u \leqq \frac{l-3}{2}\right\}$ is a system of group generators of the group $(\mathfrak{R}^-(l), +)$, hence

$$\mathscr{F}(\mathfrak{R}^-(l)) = \mathscr{F}\left(\left\{\alpha_u : 0 \leqq u \leqq \frac{l-3}{2}\right\}\right).$$

Since

$$\mathscr{F}(\alpha_u) = r_u s^{r-u} + r_u s^{l-r-u} \in B,$$

one has $\mathscr{F}(\mathfrak{R}^-(l)) \subseteq \mathfrak{L}$.

1.4. *If* $0 \leqq T \leqq l - 3$ *is even, then*

$$\mathfrak{J}_T^-(l) = \mathfrak{R}^-(l).$$

Proof. For $\alpha = \sum_i a_i s^i \in \mathfrak{R}^-(l)$ we have

$$\sum_i a_i r_{iT} = \sum_{i=0}^{\frac{l-3}{2}} a_i r_{iT} + \sum_{i=0}^{\frac{l-3}{2}} a_{i+\frac{l-1}{2}} r_{\left(i+\frac{l-1}{2}\right)T} = 0.$$

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*

$$I = (s - a_1) \dots (s - a_k) \, \mathfrak{R}(l),$$

where $a_1, \dots, a_k$ *are all distinct nonzero solutions of the following system of equations over* $\mathbf{Z}(l)$:

$$\alpha(t) = 0 \qquad \textit{for } \alpha \in M.^{1)}$$

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

For each $\beta \in I$ there exist $b_\alpha(t) \in \mathbf{Z}(l)[t]$ such that $\beta = \Sigma b_\alpha(s) \,.\, \alpha (\alpha \in M)$, hence

$$\beta = g(s)\, \Sigma b_\alpha(s)\, g_\alpha(s)\, (\alpha \in M) \in g(s) \,.\, \mathfrak{R}(l).$$

Thus

$$I \subseteq g(s)\, \mathfrak{R}(l).$$

Since there exist $h_\alpha(t) \in \mathbf{Z}(l)[t]$ such that $g(t) = \Sigma h_\alpha(t)\, \alpha(t)\, (\alpha \in M)$, one has

$$g(s) = \Sigma h_\alpha(s)\, \alpha (\alpha \in M) \in I.$$

This implies

$$g(s) \,.\, \mathfrak{R}(l) \subseteq I,$$

hence

$$I = g(s) \,.\, \mathfrak{R}(l). \tag{1}$$

II. Let $g(t) = h(t)\,(t - a_1)^{b_1} \dots (t - a_k)^{b_k} \,.\, t^b$, where $a_1, \dots, a_k$ are nonzero mutually different elements from $\mathbf{Z}(l)$, $b_1, \dots, b_k$ 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 $\geqq 2$ over $\mathbf{Z}(l)$ or $h(t) = 1$. (The case $k = 0$ is also considered.)

For each integer x $(1 \leqq x \leqq l - 1)$ there exists an integer y_x such that

$$h(x) \,.\, y_x \,.\, (x - 1)(x - 2) \ldots [x - (x - 1)][x - (x + 1)] \ldots [x - (l - 1)] \equiv \equiv 1 \pmod{l}.$$

Put

$$f(t) = \sum_{x=1}^{l-1} (t - 1)(t - 2) \ldots [t - (x - 1)][t - (x + 1)] \ldots [t - (l - 1)] \,.\, y_x.$$

Then for each integer z $(1 \leqq z \leqq l - 1)$ one has

$$h(z) \,.\, f(z) \equiv 1 \pmod{l},$$

hence

$$h(t) \,.\, f(t) \equiv 1 (t^{l-1} - 1)$$

and according to 1.1

(2) $$h(s) \,.\, f(s) = 1.$$

III. We construct for each integer $0 \leqq a \leqq l - 1$ a polynomial $f_a(t) \in \mathbf{Z}(l)[t]$ 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, $1 \leqq z \leqq l - 1$, $z \neq a$.

Thus

$$f_a(z)(z - a)^2 \equiv (z - a) \pmod{l}$$

for each integer z, $1 \leqq z \leqq l - 1$, 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 $K \subseteq \mathbf{Z}(l)$, $0 \notin K$ put

$$I(K) = \mathfrak{R}(l) \,.\, \Pi(s - a) \, (a \in K)$$
$$(I(\emptyset) = \mathfrak{R}(l)).$$

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. ($\{0\} = I(\mathbf{Z}(l) - \{0\})$.)

Let $K \subseteq \mathfrak{R}(l)$, $L \subseteq \mathfrak{R}(l)$, $0 \notin K \cup L$, $K \neq \emptyset \neq L$ and $I(K) = I(L)$. Then there exists $\alpha \in \mathfrak{R}(l)$ such that

$$\Pi(s - a)\,(a \in K) = \alpha\Pi(s - b)\,(b \in L).$$

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

$$\Pi(t - a)\,(a \in K) = \alpha(t)\,\Pi(t - b)\,(b \in L) + f(t)\,(t^{l-1} - 1).$$

Substituting $t = b \in L$ one obtains or 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 $\alpha \in \mathfrak{R}(l)$ and $f(t) \in \mathbf{Z}(l)\,[t]$ such that

$$1 = \alpha(t)\,\Pi(t - b)\,(b \in L) + f(t)\,(t^{l-1} - 1).$$

Substituting $t = b \in L$ we get $1 = 0$, which is a contradiction.
This completes the proof.

3. The Ideals $\mathfrak{J}(\mathscr{T})$

Further, we denote by $\mathbf{T}$ the set

$$\mathbf{T} = \{1 \leqq T \leqq l - 2,\ T \text{ odd}\}.$$

For $\mathscr{T} \subseteq \mathbf{T}$ put

$$\mathfrak{J}(\mathscr{T}) = \bigcap \mathfrak{J}_T^-(l)\,(T \in \mathscr{T}) = \{\alpha = \sum_i a_i s^i \in \mathfrak{R}^-(l) \colon \sum_{i=0}^{\frac{l-3}{2}} a_i r_{iT} = 0 \text{ for each } T \in \mathscr{T}\}$$

$(\mathfrak{J}(\emptyset) = \mathfrak{R}^-(l))$.

The number of elements of the set $\mathscr{T}$ is denoted by $i_{\mathscr{T}}(l)$, thus $i_{\mathscr{T}}(l) = \operatorname{card} \mathscr{T}$. For $L \in \mathscr{T}$ put

$$\alpha_L = \sum_i r_{-iL} s^i \in \mathfrak{R}^-(l).$$

3.1. Proposition. $\mathfrak{J}(\mathbf{T}) = \{0\}$.

Proof. Let $\alpha = \sum_i a_i s^i \in \mathfrak{J}(\mathbf{T})$. Then $\sum_{i=0}^{\frac{l-3}{2}} a_i r_{iT} = 0$ for each odd T, $1 \leqq T \leqq l - 2$. Since $D = \det(r_{iT})\left(0 \leqq i \leqq \dfrac{l-3}{2},\ 1 \leqq T \leqq l - 2,\ T \text{ odd}\right)$ is the *Vandermonde determinant*, we have $D \not\equiv 0 \pmod{l}$, which implies $a_i = 0$ for each $0 \leqq i \leqq \dfrac{l-3}{2}$, hence $\alpha = 0$.

The Proposition is proved.
For the same reason we get

3.2. Lemma. *The elements α_L ($L \in \mathrm{T}$) are linearly independent over the field* $\mathbf{Z}(l)$.

3.3. Proposition. *Let $\mathscr{T} \subseteq \mathrm{T}$, $\mathscr{T} \neq \mathrm{T}$. Then the system $S = \{\alpha_L : L \in \mathrm{T} - \mathscr{T}\}$ forms a basis of the vector space $\mathfrak{J}(\mathscr{T})$ over the field $\mathbf{Z}(l)$.*

Proof. According to 3.2 the elements from S are linearly independent over $\mathbf{Z}(l)$. Since for $T \in \mathscr{T}$ and $L \in \mathrm{T} - \mathscr{T}$ the integer $T - L$ is even and $l - 1$ does not divide $T - L$, we have $\sum_{i=0}^{\frac{l-3}{2}} r_{-iL} r_{iT} \equiv \sum_{i=0}^{\frac{l-3}{2}} r_{i(T-L)} \equiv 0 \pmod{l}$, thus $S \subseteq \mathfrak{J}(\mathscr{T})$.

The space o solutions of the following system of equations

$$\sum_{i=0}^{\frac{l-3}{2}} a_i r_{iT} = 0 \qquad (T \in \mathscr{T})$$

with unknowns a_i over $\mathbf{Z}(l)$ has dimension $\dfrac{l-1}{2} - i_{\mathscr{T}}(l) = \operatorname{card} S$. Hence S forms a basis of $\mathfrak{J}(\mathscr{T})$ over $\mathbf{Z}(l)$.

3.4. Corollary. card $\mathfrak{J}(\mathscr{T}) = l^{\frac{l-1}{2} - i_{\mathscr{T}}(l)}$ *for each* $\mathscr{T} \subseteq \mathrm{T}$.

3.5. Corollary. *The ideal $\mathscr{F}(\mathfrak{J}(\mathscr{T}))$ of the ring $\mathfrak{R}(l)$ is generated by elements $F(\alpha_L)$ ($L \in \mathrm{T} - \mathscr{T}$).*

3.6. Proposition. *For each $L \in \mathrm{T}$*

$$F(\alpha_L) = \sum_{\nu=1}^{l-1} \nu^{L-1} s^\nu = \sum_{\nu} \nu^{L-1} s^\nu.^{1)}$$

Proof. Let $1 \leqq \nu \leqq l - 1$, $i = -\operatorname{ind} \nu$, $a_i = r_{-iL}$. Then $\nu = r_{-i}$ and $a_{-\operatorname{ind} v} v = r_{-iL} r_i \equiv r_{-i(L-1)} \equiv \nu^{L-1} \pmod{l}$. 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 $\mathscr{T} \subseteq \mathrm{T}$. Then*

$$\mathscr{F}(\mathfrak{J}(\mathscr{T})) = (s - a_1) \dots (s - a_k)\, \mathfrak{R}(l),$$

where $a_1, \dots, a_k$ are all distinct solutions of the following system of equations over $\mathbf{Z}(l)$:

$$\sum_\nu \nu^{L-1} t^\nu = 0 \qquad (L \in T - \mathscr{T}).$$

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

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

---

1) $0^{L-1} = 1$ by definition.

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

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

4. Some Special Cases

4.1. Definition. For $2 \leqq i \leqq l - 1$ the polynomials

$$\varphi_i(t) = \sum_{\nu=1}^{l-1} (-1)^{\nu-1} \nu^{i-1} t^\nu$$

are called the *Mirimanoff polynomials* and

$$\varphi_i(t) \equiv (t + 1)^{l-i} P_i(t) \pmod{l},$$

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

$$\begin{aligned} P_3(t) &= t - t^2, \\ P_5(t) &= (t - t^2)\,.\,u(t), \\ P_7(t) &= (t - t^2)\,.\,v(t), \\ P_9(t) &= (t - t^2)\,.\,w(t), \end{aligned}$$

where

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

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

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

4.2. Proposition. (*a*) *For $l \geqq 5$ there does not exist any integer τ such that*

$$\begin{aligned} u(\tau) &\equiv 0 \pmod{l}, \\ v(\tau) &\equiv 0 \pmod{l}. \end{aligned}$$

(*b*) *For $l \geqq 7$ there does not exist any integer τ such that*

$$\begin{aligned} u(\tau) &\equiv 0 \pmod{l}, \\ w(\tau) &\equiv 0 \pmod{l}. \end{aligned}$$

(*c*) *For $l \geqq 7$ there does not exist any integer τ such that*

$$\begin{aligned} v(\tau) &\equiv 0 \pmod{l}, \\ w(\tau) &\equiv 0 \pmod{l}. \end{aligned}$$

Proof. Put

$$\begin{aligned}
\alpha &= \alpha(t) = t^2 - 46t + 1,\\
\beta &= \beta(t) = t^4 - 236t^3 + 1{,}686t^2 + 5{,}524t + 57{,}601,\\
\gamma &= \gamma(t) = 138t^3 - 33{,}283t^2 + 938{,}188t + 312{,}977,\\
\delta &= \delta(t) = 138t - 7{,}063
\end{aligned}$$

and

$$\begin{aligned}
a &= a(t) = t^2,\\
b &= b(t) = 99t - 10,\\
c &= c(t) = 231{,}329t^2 - 52{,}406t + 889 = 7.33{,}047t^2 - 52{,}406t + 7.127.
\end{aligned}$$

Then we get by calculation

(1) $v = u\alpha - 216a,$

(2) $w = u\beta + 5{,}760b,$

(3) $\gamma v - \delta w = 360c.$

Assume that $l \geqq 7$ and τ is an integer such that

$$v(\tau) \equiv 0 \pmod{l},$$
$$w(\tau) \equiv 0 \pmod{l}.$$

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

Obviously $l \nmid \tau$ and there exists an integer $\varkappa$ such that

$$\tau \,.\, \varkappa \equiv 1 \pmod{l}.$$

Then $\tau \not\equiv \varkappa \pmod{l}$ and

$$v(\varkappa) \equiv 0 \pmod{l},$$
$$w(\varkappa) \equiv 0 \pmod{l}$$

and according to (3)

$$c(\tau) \equiv 0 \pmod{l},$$
$$c(\varkappa) \equiv 0 \pmod{l}.$$

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 $62\varkappa + 45 \equiv \pmod{l}$. This follows $\tau \equiv \varkappa \pmod{l}$, therefore $\tau \equiv \pm 1 \pmod{l}$, which is a contradiction.

If $l/33{,}047$, we obtain a contradiction in a similar way.

Let $l \geqq 11$ and $l \dagger 127.33{,}047$. Then $c(t) \equiv 7.33{,}047(t - \tau)(t - \varkappa) \pmod{l}$, which implies

$$7.33{,}047 \equiv 7.127 \pmod{l},$$

hence $l/2^3 \,.\, 5.823$, thus $l = 823$. Then

$$c(t) \equiv 66t^2 + 266t + 66 \pmod{l},$$
$$= 2\,.\,(33t^2 + 133t + 33).$$

The discriminant of $c(t)$ is congruent to $165 = 3.5.11$ modulo 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 $L \in \mathrm{T}$, $L \neq 1$ we have

$$\sum_{v} v^{L-1} t^{v} \equiv \sum_{v=1}^{l-1} v^{L-1} t^{v} - t^{l-1} + 1 \pmod{l} = -\varphi_L(-t) - t^{l-1} + 1 =$$
$$= -(1 - t)^{l-L} P_L(-1) - t^{l-1} + 1 = t(1 - t)^{l-L}(1 + t)\, y_L(t) - t^{l-1} + 1,$$

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

4.3. Proposition. *Let $L \in \mathrm{T}$, $L \neq 1$ and let τ 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 $\mathscr{F}(\mathfrak{J}(\mathscr{T}))$ for $i_{\mathscr{T}}(l) = 0, 1, 2$.

For $i_{\mathscr{T}}(l) = 0$ one has

$$\mathscr{F}(\mathfrak{J}(\mathscr{T})) = (1 + s)\, \mathfrak{R}(l) = \mathfrak{L},$$

since $\mathscr{T} = \emptyset$ and $\mathscr{F}(\mathfrak{J}(\mathscr{T})) = \mathscr{F}(\mathfrak{R}^{-}(l)) = \mathfrak{L} = (1 + s)\, \mathfrak{R}(l)$ according to 1.3 and 1.2.

For $i_{\mathscr{T}}(l) = 1$ we get

4.4. Theorem. *If $\mathscr{T} = \{1\}$, then*

$$\mathscr{F}(\mathfrak{J}(\mathscr{T})) = \mathscr{F}(\mathfrak{J}_1^{-}(l)) = (s + 1)(s - 1)\, \mathfrak{R}(l).$$

If $\mathscr{T} = \{T\}$, where $T \in T - \{1\}$ we have

$$\mathscr{F}(\mathfrak{J}(\mathscr{T})) = \mathscr{F}(\mathfrak{J}_{\mathscr{T}}^{-}(l)) = (s + 1)\, \mathfrak{R}(l) \qquad \textit{for } l \geqq 7$$

and

$$\mathcal{F}(\mathfrak{J}(\mathcal{T})) = \mathcal{F}(\mathfrak{J}_3^-(5)) = (s + 1)(s + 2)(s + 3)\,\mathfrak{R}(l) \qquad \textit{for } l = 5.$$

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

Since $y_5(t) = u(-t)$ and $y_7(t) = v(-t)$, the congruence $y_5(t) \equiv 0 \pmod 7$ 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 $l \geqq 11$ by 4.2. This completes the proof according to 3.7 and 4.3.

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

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

(*a*) $l = 5 \Rightarrow \mathcal{F}(\mathfrak{J}(\mathcal{T})) = \{0\}$,

(*b*) $l \geqq 7, 1 \in \mathcal{T} \Rightarrow \mathcal{F}(\mathfrak{J}(\mathcal{T})) = (s + 1)(s - 1)\,\mathfrak{R}(l)$,

(*c*) $l = 7, 1 \notin \mathcal{T} (\mathcal{T} = \{3, 5\}) \Rightarrow \mathcal{F}(\mathfrak{J}(\mathcal{T})) = (s + 1)(s + 2)(s + 3)(s + 4)\,.$ $.\,(s + 5)\,\mathfrak{R}(7)$,

(*d*) $l \geqq 11, 1 \notin \mathcal{T} \Rightarrow \mathcal{F}(\mathfrak{J}(\mathcal{T})) = (s + 1)\,\mathfrak{R}(l)$.

5. Special System of Equations Depending on $\mathfrak{J}(\mathcal{T})$

5.1. Definition. For $\alpha = \sum_i a_i s^i \in \mathfrak{R}(l)$ put

$$f_\alpha(t) = \sum_{v=1}^{l-1} a_{-\mathrm{ind}_v \bar{v}}\, t^v \in \mathrm{Z}(l)\,[t].$$

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

(1) $f_\alpha(t) = 0, \alpha \in \mathfrak{J}(\mathcal{T})$

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

(2) $\sum_{v=1}^{l-1} v^{L-1} t^v = 0, L \in \mathrm{T} - \mathcal{T}$.[1])

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

$$I = (s - a_1) \dots (s - a_k)\,\mathfrak{R}(l),$$

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

5.3. Definition. Put

$$\mathfrak{R}^*(l) = \left\{\alpha = \sum_i a_i s^i \in \mathfrak{R}(l) : a_0 = a_1,\ a_i = a_{l-i}\left(2 \leqq i \leqq \frac{l-1}{2}\right)\right\}.$$

---

[1]) It means that $\tau \in \mathrm{Z}(l)$ is a solution of (1) if and only if it is a solution of (2). If $\mathcal{T} = \mathrm{T}$ then each $\tau \in \mathrm{Z}(l)$ is a solution of (1) and (2) by definition.

5.4. Proposition. *Let* $1 \leqq n \leqq l - 2$, $m = \left[\frac{1}{2}(l - n - 1)\right]$ *and* $\beta = (s - b_1) \,.\, (s - b_2) \dots (s - b_n)$, *where* $b_1, \dots, b_n$ *are distinct nonzero elements from* $\mathrm{Z}(l)$. *Then*

$$\operatorname{card}\left[\mathfrak{R}(l) \,.\, \beta \cap \mathfrak{R}^*(l)\right] \leqq \begin{cases} l^m & \text{for } n \text{ even,} \\ l^{m+1} \,. & \text{for } n \text{ odd.} \end{cases}$$

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

$$f(t) = (t - b_{n+1})(t - b_{n+2}) \dots (t - b_{l-1}),$$

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

$$\alpha(t) = f(t)\, q(t) + r(t).$$

Then

$$\beta \,.\, \alpha = \beta \,.\, f(s) \,.\, q(s) + \beta \,.\, r(s).$$

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

II. Let $\alpha_1 = \sum_{i=0}^{l-2-n} a_i^{(1)} s^i \in \mathfrak{R}(l)$, $\alpha_2 = \sum_{i=0}^{l-2-n} a_i^{(2)} s^i \in \mathfrak{R}(l)$ and $\beta \,.\, \alpha_1 = \beta \,.\, \alpha_2$. 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 $g(t) \in \mathrm{Z}(l)[t]$. Since $\deg \beta(t)\, \alpha_1(t)$, $\deg \beta(t)\, \alpha_2(t) \leqq l - 2$, one obtains $g(t) = 0$ and $\alpha_1(t) = \alpha_2(t)$, thus $\alpha_1 = \alpha_2$.

From I we get then

$$\operatorname{card} M = \operatorname{card}\{\alpha = \sum_{i=0}^{l-2-n} a_i s^i \in \mathfrak{R}(l) : \beta \,.\, \alpha \in \mathfrak{R}^*(l)\}.$$

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

$$\begin{aligned}
&c_{l-2} = x_{l-2-n}\beta_n, \\
&c_{l-3} = x_{l-2-n}\beta_{n-1} + x_{l-3-n}\beta_n, \\
&\vdots \\
(3)\quad &c_i = \Sigma x_j \beta_{i-j} \ (\max\{0, i - n\} \leqq j \leqq \min\{l - 2 - n, i\}), \\
&\vdots \\
&c_1 = x_1\beta_0 + x_0\beta_1, \\
&c_0 = x_0\beta_0.
\end{aligned}$$

The system

(4) $\quad c_0 - c_1 = 0,$

$$c_i - c_{l-i} = 0, \qquad \left(2 \leqq i \leqq \frac{l-1}{2}\right)$$

forms a system of $\frac{l-1}{2}$ linear equations with unknowns $x_0, x_1, \ldots, x_{l-2-n}$.

Assume $m \geqq 2$ and assume that for $2 \leqq k \leqq m - 1$ 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

$$\begin{aligned} c_0 - c_1 &= 0, \\ c_i - c_{l-i} &= 0, \qquad (2 \leqq i \leqq k). \end{aligned}$$

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

$$\begin{aligned} c_0 - c_1 &= 0, \\ c_i - c_{l-i} &= 0, \qquad (2 \leqq i \leqq m). \end{aligned}$$

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 $m \geqq 2$. The case $0 \leqq m \leqq 1$ is easy to show.

5.5. Theorem. *Let $\mathscr{T} \subseteq$ T. Then for the number $n_{\mathscr{T}}(l)$ of solutions of the system* (1) *different from -1 it holds*

$$n_{\mathscr{T}}(l) \leqq \begin{cases} 2i_{\mathscr{T}}(l) & \text{for } 1 \notin \mathscr{T}, \\ 2i_{\mathscr{T}}(l) - 1 & \text{for } 1 \in \mathscr{T}. \end{cases}$$

Proof. Obviously, if τ is a solution of (2), then τ^{-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 $1 \notin \mathscr{T}$. Thus $n = n_{\mathscr{T}}(l) + 1$ is the number of solutions of (1) and $n_{\mathscr{T}}(l)$ is even if and only if $1 \notin \mathscr{T}$.

Let $-1, a_1, \ldots, a_{n-1}$ be the set of solutions of (1) and put $\beta = (s + 1)(s + a_1) \ldots \ldots (s + a_{n-1})$. According to 3.7

$$\mathscr{F}(\mathfrak{J}(\mathscr{T})) = \beta \,.\, \mathfrak{R}(l)$$

and obviously

$$\mathscr{F}(\mathfrak{J}(\mathscr{T})) \subseteq \mathscr{F}(\mathfrak{J}(\mathscr{T})) \cap \mathfrak{R}^*(l).$$

From 3.4 we get

$$\operatorname{card} \mathscr{F}(\mathfrak{J}(\mathscr{T})) = \operatorname{card} \mathfrak{J}(\mathscr{T}) = l^{\frac{l-1}{2} - i_{\mathscr{T}}(l)},$$

hence according to 5.4

$$l^{\frac{l-1}{2} - i_{\mathscr{T}}(l)} \leqq \operatorname{card} [\mathfrak{R}(l) \,.\, \beta \cap \mathfrak{R}^*(l)] \leqq \begin{cases} l^m & \text{for } n \text{ even}, \\ l^{m+1} & \text{for } n \text{ odd}, \end{cases}$$

where

$$m = \left[\frac{1}{2}(l - n - 1)\right] = \begin{cases} \dfrac{l-3}{2} - \dfrac{n_{\mathscr{T}}(l)}{2} & \text{for } 1 \notin \mathscr{T}, \\ \dfrac{l-1}{2} - \dfrac{n_{\mathscr{T}}(l)+1}{2} & \text{for } 1 \in \mathscr{T}. \end{cases}$$

Hence for $1 \notin \mathscr{T}$

$$\frac{l-1}{2} - i_{\mathscr{T}}(l) \leqq m + 1 = \frac{l-1}{2} - \frac{n_{\mathscr{T}}(l)}{2}$$

and

$$n_{\mathscr{T}}(l) \leqq 2 i_{\mathscr{T}}(l).$$

For $1 \in \mathscr{T}$ we have

$$\frac{l-1}{2} - i_{\mathscr{T}}(l) \leqq m = \frac{l-1}{2} - \frac{n_{\mathscr{T}}(l)+1}{2},$$

therefore

$$n_{\mathscr{T}}(l) \leqq 2 i_{\mathscr{T}}(l) - 1.$$

The theorem is proved.

6. System of Equations Depending on the Stickelberger Ideal

6.1. Notation. The *Stickelberger ideal* $\overline{\mathfrak{J}}$ in the group ring $\overline{\mathfrak{R}} = \{\sum_i a_i s^i : a_i$ *l*-adic integer$\}$ of the group G over the ring of *l*-adic integers is the ideal

$$\overline{\mathfrak{J}} = \{\alpha \in \overline{\mathfrak{R}} : \exists\, \varrho \in \overline{\mathfrak{R}}, \varrho \,.\, \sum_i r_{-i} s^i = l\alpha\}$$

of the ring $\overline{\mathfrak{R}}$.

Put $\overline{\mathfrak{R}}^- = \left\{\sum_i a_i s^i \in \overline{\mathfrak{R}} : a_i + a_{i+\frac{l-1}{2}} = 0 \text{ for } 0 \leqq \leqq i \leqq \dfrac{l-3}{2}\right\}$ and $\overline{\mathfrak{J}}^- = \overline{\mathfrak{J}} \cap \overline{\mathfrak{R}}^-$. The *Stickelberger ideal* $\mathfrak{J}^-(l)$ *modulo* l is defined as follows

$$\mathfrak{J}^-(l) = \{\sum_i a_i s^i \in \mathfrak{R}^-(l) \colon \exists b_i \in a_i, \Sigma b_i s^i \in \overline{\mathfrak{J}}^-\}$$

(the *l*-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

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30}, \dots$$

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

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

and for integer $X > h(T)$

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

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

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

$$\overline{\mathfrak{J}}^-_{Tm} = \{\sum_i a_i s^i \in \overline{\mathfrak{R}}^- : \sum_i a_i r^{iTl^{m-1}} \equiv 0 \pmod{l^m}\}$$

and

$$\overline{\mathfrak{J}}^-_{T0} = \overline{\mathfrak{R}}^-.$$

In the paper [7] (Theorem 4.5) it was shown

6.2. $\cap \overline{\mathfrak{J}}^-_{Tm(T)}(3 \leqq T \leqq l-2,\ T\ \mathit{odd}) = \overline{\mathfrak{J}}^-$,
where

$$m(T) = \begin{cases} h(l-1-T) & \text{for } B_{l-T} \equiv 0 \pmod{l}. \\ 0 & \text{otherwise.} \end{cases}$$

let $\mathscr{U} = \{3 \leqq T \leqq l-2 : T \text{ odd and } B_{l-T} \equiv 0 \pmod{l}\} \subseteq \mathrm{T}$. The integer $i_*(l)$ is called the *index of irregularity of the prime* l and is denoted by $i(l)$.

It was shown in the paper [9]:

6.3. card $\overline{\mathfrak{J}}^-(l) = l^{\frac{l-1}{2}-i(l)}$.

From 6.2, 6.3 and 3.4 we can derive

6.4. Proposition. $\mathfrak{J}^-(l) = \mathfrak{J}(\mathscr{U}) = \cap \overline{\mathfrak{J}}^-_T(l)\ (T \in \mathscr{U})$.

We denote by (S) *the following system of equations* (*over* $\mathbf{Z}(l)$) *depending on the Stickelberger ideal:*

$$(S) \qquad f_\alpha(t) = 0, \qquad \alpha \in \mathfrak{J}(\mathscr{U}) = \overline{\mathfrak{J}}^-(l).$$

We get from 5.5

6.5. Theorem. *For the number* $n = n_*(l)$ *of solutions* (*in the field* $\mathbf{Z}(l)$) *of the system* (S) *different from* -1 *it holds*

$$n \leqq 2_i(l).$$

We obtained this inequality in the paper [8] (Theorem 3.5) in another way.

Kummer ([2], s. also [1] or [6]) used in the considerations on *the first case of Fermat's last theorem* the system of congruences transformated to the following system of equations (over $\mathbf{Z}(l)$):

$$(K) \qquad P_{l-2i}(t)\,B_{2i} = 0, \qquad \left(1 \leqq i \leqq \frac{l-3}{2}\right).$$

6.6. Theorem. *The element $\tau \in \mathbf{Z}(l)$, $\tau \neq -1$, is a solution of the system (K) if and only if $-\tau$ is a solution of the system (S).*

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

(1) $\varphi_i(t)\, B_{l-i} = 0$ $(3 \leqq i \leqq l-2,\ i$ odd)

and τ is a solution of (1) if and only if τ is a solution of the system

(2) $\varphi_i(t) = 0$ $(3 \leqq i \leqq l-2,\ i$ odd, $i \notin \mathcal{U})$.

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

$$(3) \qquad \sum_{v=1}^{l-1} v^{L-1} t^v = 0, \qquad L \in \mathbf{T} - \mathcal{U}.$$

Then we obtain the theorem from 5.2 and 6.4.

REFERENCES

[1] P. Bachmann, *Das Fermatproblem in seiner bisherigen Entwicklung*, Walter de Gruyter, Berlin und Leipzig, 1919.

[2] E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichnung $\alpha^\lambda = 1$ gebildeten complexen Zahlen für den Fall, dass die Classenzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermatschen Lehrsatzes*, Abhandl., Königl. Akad. Wiss., Berlin, 1857, 41–74.

[3] P. Le Lidec, *Sur une forme nouvelle des congruences de Kummer-Mirimanoff*, C. R. Acad. Sc. Paris, **265** (1967), Série A, 89–90.

[4] P. Le Lidec, *Nouvelle forme des congruences de Kummer-Mirimanoff pour le premier cas du théorème de Fermat*, Bull. Soc. Math. France, **97** (1969), 321–328.

[5] M. Mirimanoff, *L'équation indéterminèe $z^l + y^l + z^l = 0$ et le critérium de Kummer*, J. Reine Angew. Math., **128** (1905), 45–68.

[6] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York–Heidelberg–Berlin, 1979.

[7] L. Skula, *On certain ideals of the group ring* $\mathbf{Z}[G]$, Archivum Mathematicum (Brno), **XV** (1979), 53–66.

[8] L. Skula, *A remark on Mirimanoff polynomials*, Comentarii Mathematici Universitatis Sancti Pauli (Tokyo), vol. **31**, no. 1 (1982), 89–97.

[9] L. Skula, *A note on index of irregularity*, to appear.

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