TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 343, Number 2, June 1994

THE ORDERS OF SOLUTIONS OF THE KUMMER SYSTEM OF CONGRUENCES

LADISLAV SKULA

ABSTRACT. A new method concerning solutions of the Kummer system of congruences (K) (modulo an odd prime l) is developed. This method is based on the notion of the Stickelberger ideal. By means of this method a new proof of Pollaczek's and Morishima's assertion on solutions of (K) of orders 3, 6 and 4 mod l is given. It is also shown that in case there is a solution of $(K) \not\equiv 0, \pm 1 \pmod{l}$, then for the index of irregularity $\mathrm{i}(l)$ of the prime l we have $\mathrm{i}(l) \geq [\sqrt[3]{l/2}]$.

INTRODUCTION

In 1857, Kummer [12] introduced the following system of congruences (in equivalent form) for an odd prime l

$$\text{(K)} \qquad B_{2j}\varphi_{l-2j} \equiv 0 \pmod{l} \qquad (1 \leq j \leq (l-3)/2),$$

where B_{2j} means the *Bernoulli number* ($B_0 = 1$, $B_1 = \frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}, \ldots$) and $\varphi_i(t) = \sum_{v=1}^{l-1}(-1)^{v-1}v^{i-1}t^v$ $(1 \leq i \leq l-1)$ the *Mirimanof polynomial*.

The system (K) will be called the *Kummer system of congruences*.

Kummer showed that if the First Case of Fermat's Last Theorem for the prime l fails and x, y, z are integers not divisible by l with $x^l + y^l + z^l = 0$, then each $t \in G = \{x/y, y/x, x/z, z/x, y/z, z/y\}$ is a solution of (K). It is easy to see then also the congruence $\varphi_{l-1}(t) \equiv 0 \pmod{l}$ is satisfied for each $t \in G$.

In 1917, Pollaczek [17] "proved" that if $t \in G$, then t cannot have order 3 or 6 mod l, and in 1931, Morishima [16] "gave a proof" of the same for order 4. These "proofs" have not been accepted as correct mathematical proofs but Gunderson [10, 1948] corrected them (for detail see [9]).

The aim of this paper is not an analysis of these proofs but rather to propose a new proof (actually for any solution of (K)) using a quite different method. This method allows us to extend these results to other orders mod l of a solution for certain upper bounds of the index of irregularity of l (§§6 and 7).

The basic steps of this method are the following:

Received by the editors October 5, 1990 and, in revised form, August 12, 1991 and April 27, 1992.

1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11B50, 11C20.

Key words and phrases. Kummer system of congruences, the first case of Fermat's Last Theorem, Stickelberger ideal, index of irregularity of a prime.

0002-9947/94 $1.00 + $.25 per page

(1) The Kummer system (K) of congruences is transferred to a new system (S) depending on the *Stickelberger ideal* I^- ((1.7) and (1.8)), as in my paper [20, 1982].

(2) For a solution τ of (S) we introduce a matrix $D_l(\tau)$ which plays the role of the matrix of coefficients of a system of linear equations over the Galois field $\mathbf{Z}/l\mathbf{Z}$ derived from the system (S). The elements of the Stickelberger ideal I^- play here the role of solutions of this system (2.2).

(3) We use the formula giving the number of elements of the Stickelberger ideal $I^-(l)$ (The Stickelberger ideal I^- considered mod l) proved in my paper [22, 1986] (1.1):

$$\operatorname{card} I^-(l) = l^{N-\mathrm{i}(l)}$$

where $N = (l-1)/2$ and $\mathrm{i}(l)$ denotes the index of irregularity of the prime l.

This implies $\mathrm{r}(D_l(\tau)) \leq \mathrm{i}(l)$, where $\mathrm{r}(D_l(\tau))$ means the rank of $D_l(\tau)$ over the Galois field $\mathbf{Z}/l\mathbf{Z}$ (Theorem 2.3).

(4) The core of this method is to give some bounds for $\mathrm{r}(D_l(\tau))$ and $\mathrm{i}(l)$ leading to a contradiction with the above inequality.

For the index of irregularity $\mathrm{i}(l)$ we use a bound (4.9) derived from Carlitz's bound for the first factor of the lth cyclotomic field [4, 1961].

(5) If τ has order 4 mod l (Morishima's case), then

$$\mathrm{r}(D_l(\tau)) = (l-3)/2 - \mathrm{i}_E(l)$$

(5.1), and if τ has order 3 mod l (one of *Pollaczek's* cases), then

$$\mathrm{r}(D_l((\tau)) = (l-3)/2 - \mathrm{i}_D(l)$$

(5.4). Here $\mathrm{i}_E(l)$, $\mathrm{i}_D(l)$ is the index of E-irregularity of l, the index of D-irregularity of l, respectively. E symbolizes the Euler numbers and D the D-numbers defined by Kleboth [11, 1955] by the recursion formula

$$(D+1)^n + (D-1)^n + D^n = 0 \qquad (n \geq 1), \quad D_0 = 1.$$

These general indices of irregularity were introduced by Ernvall [8, 1985], where he also obtained an upper bound for them. For our needs we have had to improve Ernvall's bound, which was done by using the special matrices P and Q in §3 (3.4, Theorem 4.5).

In Pollaczek's other case, τ has order 6 mod l, we use the inequality

$$\mathrm{r}(D_l)(\tau) \geq (l-3)/2 - \mathrm{i}_D(l) - \mu(l)$$

(5.3), where $\mu(l)$ means a special function defined in 4.7 with an upper bound in 4.8.

It seems that the depth of Pollaczek's and Morishima's Theorems consists in the proof of nonvanishing of $\det P$ and $\det Q$ (Theorem 3.3). Here, the theorem $\sum_{a=1}^{f} \chi(a)a \neq 0$ for an odd Dirichlet character χ of conductor f is used.

At the conclusion we give a general theorem (7.6) on the existence of a non-trivial solution of the system (S). In this case we get $\mathrm{i}(l) \geq [\sqrt[3]{l/2}]$.

Note that Eichler [5, 1965] proved: "If the First Case of Fermat's Last Theorem for the prime l $(l > 3)$ fails, then l^r $(r = [\sqrt{l}] - 1)$ divides the first factor h^- of the lth cyclotomic field." It was observed by Brückner [2] (and Oberwolfach Conference 1975), Iwasawa, and Skula [19] ([27, §6.5]) that the statement l^r/h^- can be substituted for $\mathrm{i}(l) \geq [\sqrt{l}] - 1$.

Uehara [25] improved this result a little.

1. Preliminaries

Throughout this paper we will use the following notations:

l	an odd prime
$N = \frac{l-1}{2}$	
r	a primitive root mod l
ind x	index of an integer $x (l \nmid x)$ relative to the primitive root r of l
$\mathbf{Z}$	the ring of integers; the small latin letters will usually denote integers
r_i	the integer $(i \in \mathbf{Z})$, $0 < r_i < l$, $r_i \equiv r^i \pmod{l}$
$\overline{v}$	the integer with $1 \leq \overline{v} \leq l-1$, $v \cdot \overline{v} \equiv 1 \pmod{l}$, where $v \in \mathbf{Z}$, $l \nmid v$
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
$R = \mathbf{Z}[G]$	the group ring of the group G over the ring $\mathbf{Z}$, thus $R = \{\sum_i a_i s^i : a_i \in \mathbf{Z}\}$; for $j \in \mathbf{Z}$ put $a_j = a_i$ $(0 \leq i \leq l-2,\ j \equiv i \pmod{l-1})$
$R^- =$	$\{\alpha = \sum_i a_i s^i \in R : a_i + a_{i+(l-1)/2} = 0$ for each $i \in \mathbf{Z}\}$ $= \{\alpha \in R : (1 + s^{(l-1)/2}) \cdot \alpha = 0\}$, a subring of the ring R
$I =$	$\{\alpha \in R$: there exists $\rho \in R$, $\rho \cdot \sum_i r_{-i} s^i = l\alpha\}$, the Stickelberger ideal of the ring R
$I^- = R^- \cap I$	the Stickelberger ideal of the ring R^-
$f_\alpha(t) =$	$\sum_{\nu=1}^{l-1} a_{\text{ind}\, v} \overline{v} t^v \in \mathbf{Z}[t]$ for $\alpha = \sum_i a_i s^i \in R$
$\mathrm{i}(l) =$	$\mathrm{card}\{1 \leq i \leq (l-3)/2 : l/B_{2i}\}$ the index of irregularity of l
$\mathrm{r}(M)$	the rank of a matrix M, the elements of which are integers, over $\mathbf{Z}/l\mathbf{Z}$
$I^-(l) =$	$\{\sum_i a_i s^i : a_i \in \mathbf{Z}/l\mathbf{Z}$ with the property: there exist $b_i \in a_i$ such that $\sum_i b_i s^i \in I^-\}$, the Stickelberger ideal mod l.

In 1986, Skula [22, Consequence 2.2] proved

1.1. **Theorem.**

$$\mathrm{card}\, I^-(l) = l^{N - \mathrm{i}(l)}.$$

1.2. **Definition.** Let $c_0, c_1, \ldots, c_{n-1}$ be complex numbers (n a positive integer). The left circulant matrix $C(c_0, c_1, \ldots, c_{n-1})$ of order n is a square matrix $C = (\gamma_{ij})$ $(0 \leq i, j \leq n-1)$ of order n, where $\gamma_{ij} = c_m$ $(0 \leq i, j, m \leq n-1)$ and $m \equiv i + j \pmod{n}$.

If we use the proof of the König-Rados Theorem [15, 6.1] we get

1.3. **Theorem.** *Let* $C = C(c_0, c_1, \dots, c_{N-1})$ *be a left circulant matrix of order* N *over the ring* $\mathbf{Z}$.

(i) *Let* ν *be the number of integers* k, $0 \le k \le (l-3)/2$, *with the property*

$$\sum_{t=1}^{N} c_{\operatorname{ind} t} t^{2k} \equiv 0 \pmod{l}.$$

Then

$$\mathrm{r}(C) + \nu = N,$$

$$(c_j = c_i \text{ for } i, j \in \mathbf{Z},\ i \equiv j \pmod{N},\ 0 \le i \le N-1.)$$

Further we have

(ii) $\det C = \prod_{\zeta^N=1} (\sum_{t=1}^{N} c_{\operatorname{ind} t} \zeta^t)$.

1.4. **Proposition.** *Let* D *be a square matrix of order* N *over* $\mathbf{Z}$ *with* $\det D \neq 0$. *Then*

$$N - \mathrm{r}(D) \le \frac{\log |\det D|}{\log l}$$

Proof. Let $r_1, \dots, r_h$ be a maximal linearly independent system of rows of the matrix D over $\mathbf{Z}/l\mathbf{Z}$. For $1 \le j \le N-h$ there exist integers $c_i^{(j)}$ $(1 \le i \le h)$ such that

$$r_{h+j} \equiv \sum_{i=1}^{h} c_i^{(j)} r_i \pmod{l},$$

where $r_{h+1}, \dots, r_N$ are the other rows of D. If we subtract from r_{h+j} the linear combination $\sum_{i=1}^{h} c_i^{(j)} r_i$, we get all elements in rows $h+j$ $(1 \le j \le N-h)$ of the matrix D congruent to zero mod l. Hence $\det D = l^{N-h} d$, where $d \in \mathbf{Z}$, $d \neq 0$, and the result follows.

Further we will consider the system of congruences (S) depending on the Stickelberger ideal I^-.

1.7. **Definition.** The following system of congruences will be denoted by (S):

(S) $$f_\alpha(t) \equiv 0 \pmod{l} \quad \text{for each } \alpha \in I^-.$$

The system (S) was introduced in a slightly different form in [20, 1.3]. The following connection of the systems (K) and (S) was shown in [21, 2.6, 2.11].

1.8. **Theorem.** *Let* τ *be an integer,* $\tau \not\equiv -1 \pmod{l}$. *Then* τ *is a solution of the system* (K) *if and only if* $-\tau$ *is a solution of the system* (S).

1.9. *Remark.* (a) Each integer $\tau \equiv -1 \pmod{l}$ is a solution of the system (K), since the Mirimanoff polynomial $\varphi_i(t)$ is divisible by the polynomial $t+1$ $(2 \le i \le l-1)$ in the ring $\mathbf{Z}[t]$.

On the other hand we get from [20, 1.5]:

(b) Any integer $\sigma \equiv 1 \pmod{l}$ is not a solution of the system (S).

(c) Let τ, σ be integers, $\tau \equiv 1 \pmod{l}$, $\sigma \equiv -1 \pmod{l}$. Then τ is a solution of the system (K) and σ is a solution of the system (S).

Proof. For even m, $2 \le m \le l-3$, we have $\varphi_{m+1}(1) = -\sum_{v=1}^{l-1} (-1)^v v^m \equiv 0 \pmod{l}$. The result follows from 1.8.

Further for the Mirimanoff polynomial $\varphi_{l-1}(t)$ the following assertion holds:

(d) We have for an integer $\tau \equiv 1 \pmod{l}$

$$\varphi_{l-1}(\tau) \equiv 0 \pmod{l}$$

if and only if

$$q_l(2) \equiv 0 \pmod{l}.$$

Here, $q_l(2) = (2^{l-1} - 1)/l$ means the Fermat quotient of the prime l with base 2.

Proof. We have

$$\begin{aligned}\varphi_{l-1}(\tau) &\equiv \sum_{v=1}^{l-1}(-1)^{v-1}\overline{v} \pmod{l} \\ &= -\sum_{v-1}^{N}\overline{2v} + \sum_{v=1}^{N}\overline{(l-2v)} \\ &\equiv -\sum_{v=1}^{N}\overline{v} \pmod{l} \equiv 2q_l(2) \pmod{l}\end{aligned}$$

according to Eisenstein's Theorem [6, 1850].

2. The theorem concerning a solution of (S)

2.1. **Definition.** For $1 \leq x, y \leq l-1$ let $\alpha(x, y)$ be the least positive residue of $xy \pmod{l}$, hence $a(x, y) \in \mathbf{Z}$, $1 \leq l-1$ and $a(x, y) \equiv xy \pmod{l}$.

We also have

$$a(x, y) = xy - l[xy/l] = l\langle xy/l\rangle,$$

where $\langle u\rangle$ is the fractional part of a real number u.

For $t \in \mathbf{Z}$ put

$$D(t) = D_l(t) = (t^{a(x,y)} + t^{(l-a(x,y))})_{1\leq x,y\leq N}.$$

$D(t)$ is a square matrix of order N over $\mathbf{Z}$.

In the paper [23, 4.13] a matrix $D_N(t)$ (N means here an integer ≥ 3) was defined which for $N = l$ differs from this matrix $D(t)$ only by multiplication by t^{-1} and a suitable permutation of rows.

2.2. **Proposition.** *Let an integer τ be a solution of the system (S). Then for each $1 \leq y \leq N$ and each $\alpha = \sum_i a_i s^i \in I^-$ we have*

$$\sum_{v=1}^{N} a_{-\operatorname{ind} v}\overline{v}(\tau^{a(v,y)} + \tau^{l-a(v,y)}) \equiv 0 \pmod{l}.$$

Proof. Let $1 \leq y \leq N$ and $a = \sum_i a_i s^i \in I^-$. Then

$$s^{l-1-\operatorname{ind} y}\alpha = \sum_i b_i s^i \in I^- \quad \text{and} \quad b_i = a_{i+\operatorname{ind} y} \qquad (0 \leq i \leq l-2).$$

Thus

$$\begin{aligned}0 &\equiv \sum_{v=1}^{l-1} b_{-\operatorname{ind} v}\overline{v}\tau^v \pmod{l} \\ &= \sum_{v=1}^{l-1} a_{-\operatorname{ind} v\overline{y}}\overline{v}\tau^v,\end{aligned}$$

from which

$$\sum_{v=1}^{l-1} a_{-\operatorname{ind} v\overline{y}}\overline{v}\cdot\tau^{v} \equiv 0 \pmod{l}$$

follows.

If we put $w \equiv v\overline{y} \pmod{l}$, $1 \leq w \leq l-1$, we get

$$\begin{aligned} 0 &\equiv \sum_{w=1}^{l-1} a_{-\operatorname{ind} w}\overline{w}\tau^{a(w,y)} \pmod{l} \\ &= \sum_{w=1}^{N} a_{-\operatorname{ind} w}\overline{w}\tau^{a(w,y)} + \sum_{w=1}^{N} a_{-\operatorname{ind}(l-w)}\overline{(l-w)}\tau^{a(l-w,y)} \\ &\equiv 2\sum_{w=1}^{N} a_{-\operatorname{ind} w}\overline{w}(\tau^{a(w,y)} + \tau^{l-a(w,y)}) \pmod{l}. \end{aligned}$$

The result follows immediately.

2.3. **Theorem.** *Let an integer τ be a solution of the system (S). Then* $\mathrm{r}(D_l(\tau)) \leq \mathrm{i}(l)$.

Proof. Consider the system of linear congruences

$$(*) \qquad \sum_{v=1}^{N} \xi_v(\tau^{a(v,y)} + \tau^{l-a(v,y)}) \equiv 0 \pmod{l} \qquad (1 \leq y \leq N)$$

with unknowns $\xi_1, \ldots, \xi_N$. The number of solutions of the system $(*)$ is equal to l^{ν}, where $\nu = N - \mathrm{r}(D(\tau))$.

According to 2.2 for each $\alpha = \sum_i a_i s^i \in I^-$ the integers $\{a_{-\operatorname{ind} v}\overline{v}\colon 1 \leq v \leq N\}$ form a solution of the system $(*)$.

The we get $l^{N-\mathrm{i}(l)} \leq l^{\nu} = l^{N-\mathrm{r}(D(\tau))}$ from Theorem 1.1 and the result follows.

2.4. **Proposition.** *Let $\tau \in \mathbf{Z}$. We get from the matrix $D(\tau)$ by a suitable permutation of rows and columns the left circulant matrix $C(c_0, c_1, \ldots, c_{N-1})$, where $c_m = \tau^{r_m} + \tau^{l-r_m}$ $(0 \leq m \leq N-1)$.*

Proof. For $0 \leq i \leq N-1$ put

$$\psi(i) = \begin{cases} r_i & \text{for } r_i \leq N, \\ l - r_i & \text{for } r_i > N. \end{cases}$$

Then ψ is a bijection from the set $0, 1, \ldots, N-1$ onto the set $\{1, 2, \ldots, N\}$. Let $D(\tau) = (\delta_{xy})_{1\leq x,y\leq N}$, $C(c_0, c_1, \ldots, c_{N-1}) = (\gamma_{ij})_{0\leq i,j\leq N-1}$ be the left circulant matrix, where $c_m = \tau^{r_m} + \tau^{l-r_m}$ $(0 \leq m \leq N-1)$.

Then $\gamma_{ij} = c_m$, where $m \equiv i + j \pmod{N}$ and $0 \leq m \leq N-1$. Hence

$$\gamma_{ij} = \tau^{r_{i+j}} + \tau^{l-r_{i+j}} = \delta_{\psi(i)\psi(j)}.$$

Then we get from 1.3.

2.5. **Proposition.** *Let $\tau \in Z$ and let n_1, n_2 be the numbers of k's integers $(0 \leq k \leq (1-3)/2)$ with the properties*

$$\sum_{t=1}^{N} (\tau^t + \tau^{l-t})t^{2k}t^{2k} \equiv 0 \pmod{l},$$

$$\sum_{t=1}^{l-1} \tau^t t^{2k} \equiv 0 \pmod{l},$$

respectively.

Then $n_1 = n_2$ *and*

$$\mathrm{r}(D)(\tau)) + n_1 = \mathrm{r}(D(t)) + n_2 = N.$$

Acknowledgment. When discussing the volume of this paper with *Andrew Granville* he drew my attention to the fact that the polynomials $\sum_{t=1}^{l-1} \tau^t t^{2k}$ in the indeterminate τ $(0 \le k \le (l-3)/2)$ are the Mirimanoff polynomials $\varphi_{2k+1}(-\tau)$ and then he suggested another proof of Theorem 2.3 based on noting that $n_2 = \mathrm{card}\{1 \le j \le \frac{l-3}{2} : \varphi_{l-2j}(-\tau) \equiv 0 \pmod{l}\}$. I would like to thank him for his advice and also for his patience by the discussion of this article.

3. Special matrices P and Q

In this section we will assume $l \ge 5$.

3.1. **Notation.** For $1 \le x, y \le N$ put

$$p(x, y) = \begin{cases} 1 & \text{for } a(x, y) < \frac{l}{4} \text{ or } \frac{3l}{4} < a(x, y), \\ 0 & \text{for } \frac{l}{4} < a(x, y) < \frac{3l}{4}, \end{cases}$$

$$q(x, y) = \begin{cases} 1 & \text{for } \frac{l}{6} < a(x, y) < \frac{l}{3} \text{ or } \frac{2}{3}l < a(x, y) < \frac{5l}{6}, \\ 0 & \text{otherwise.} \end{cases}$$

Further put

$$P = (p(x, y))_{1 \le x, y \le N}, \quad Q = (q(x, y))_{1 \le x, y \le N},$$

$$p(x) = \sum_{1 \le t \le [l/4]} x^{\mathrm{ind}\, t}, \quad q(x) = \sum_{[l/6] < t \le [l/3]} x^{\mathrm{ind}\, t}.$$

Then P and Q are square matrices over $\mathbf{Z}$ of order N and $p(x), q(x) \in \mathbf{Z}[x]$.

3.2. **Proposition.** (a) *We get from the matrices* P, Q *by suitable permutations of rows and columns left circulant matrices.*

$$\text{(b)} \qquad \mathrm{r}(P) = N - \mathrm{card}\left\{0 \le k \le N-1 : \sum_{1 \le t \le [l/4]} t^{2k} \equiv 0 \pmod{l}\right\},$$

$$\text{(c)} \qquad \mathrm{r}(Q) = N - \mathrm{card}\left\{\{0 \le k \le N-1 : \sum_{[l/6] < t \le [l/3]} t^{2k} \equiv 0 \pmod{l}\right\},$$

$$\text{(d)} \qquad |\det P| = \left|\prod_{k=0}^{N-1} p(\zeta^{2k})\right|, \quad |\det Q| = \left|\prod_{k=0}^{N-1} q(\zeta^{2k})\right|,$$

where ζ *denotes a primitive* $l-1$*st root of unity.*

Proof. Put (as in the proof of 2.4)

$$\psi(i) = \begin{cases} r_i & \text{for } r_i \le N \\ l - r_i & \text{for } r_i > N \end{cases} \quad (0 \le i \le N-1).$$

Further let $\gamma_{ij} = p(\psi(i), \psi(j))$, $\delta_{ij} = q(\psi(i), \psi(j))$ and $C = (\gamma_{ij})_{0 \le i, j \le N-1}$, $D = (\delta_{ij})_{0 \le i, j \le N-1}$.

Clearly, the matrices C and D are left circulant matrices. Since for $1 \le t \le N$ we have

$$\gamma_{0 \text{ ind } t} = p(1, t) = \begin{cases} 1 & \text{for } t < \frac{l}{4}, \\ 0 & \text{for } t > \frac{l}{4}, \end{cases}$$

and

$$\delta_{0 \text{ ind } t} = q(1, t) = \begin{cases} 1 & \text{for } \frac{l}{6} < t < \frac{l}{3}, \\ 0 & \text{otherwise.} \end{cases}$$

We get assertions (b) and (c) from 1.3.

The polynomials

$$\sum_{j=0}^{N-1} \gamma_{0j} x^j = \sum_{j=0}^{N-1} p(1, \psi(j)) x^j \quad \text{and} \quad \sum_{j=0}^{N-1} \delta_{0j} x^j = \sum_{j=0}^{N-1} q(1, \psi(j)) x^j$$

are the associated polynomials of C, D (respectively), so we obtain assertion (d) (1.3(ii)).

3.3. **Theorem.** $\det P \cdot \det Q \neq 0$.

Proof. Let ξ denote a primitive $l-1$st root of unity. Since $p(1)q(1) \neq 0$, it is to be shown (according to 3.2(d)) $p(\zeta^{2k}) \cdot q(\zeta^{2k}) \neq 0$ for each $1 \le k \le (l-3)/2$. Let $1 \le k \le (l-3)2$.

For $t \in \mathbf{Z}$ put

$$\omega(t) = \omega_k(t) = \begin{cases} \zeta^{2k \text{ ind } t} & \text{for } l \nmid t, \\ 0 & \text{for } l/t, \end{cases}$$

$$\chi_1(t) = \begin{cases} 1 & \text{for } t \equiv 1 \pmod 4, \\ -1 & \text{for } t \equiv 3 \pmod 4, \\ 0 & \text{for } 2/t, \end{cases}$$

$$\chi_2(t) = \begin{cases} 1 & \text{for } t \equiv 1 \pmod 3, \\ -1 & \text{for } t \equiv 2 \pmod 3, \\ 0 & \text{for } 3/t, \end{cases}$$

$$\psi_1(t) = \chi_1(t) \cdot \omega(t), \quad \psi_2(t) = \chi_2(t) \cdot \omega(t).$$

Then ω, χ_1, χ_2, ψ_1, ψ_2 are Dirichlet characters with conductors l, $f_1 = 4$, $f_2 = 3$, $f_1 l = 4l$, $f_2 l = 3l$ (respectively), ω is an even character and χ_1, χ_2, ψ_1, ψ_2 are odd.

For $j = 1, 2$ put

$$T_j = \sum_x x \psi_j(x) \qquad (1 \le x \le f_j l).$$

($T_j = f_j l B^1(\psi_j)$, where $B^n(\chi)$ mean the generalized Bernoulli numbers defined at the beginning of §4.)

The following relation is well known (e.g. [27, Theorem 4.9]):

(a) $T_j \neq 0$.

For $i \in \mathbf{Z}$ put

$$\beta(i) = \sum_t \omega(t) \qquad (1 \le t \le l-1, \ t \equiv il \pmod 4),$$

$$\gamma(i) = \sum_t \omega(t) \qquad (1 \le t \le l-1,\ t \equiv il \pmod 6).$$

Since ω is an even character, we have for $i \in \mathbf{Z}$, $\beta(i) = \beta(1-i)$, $\gamma(i) = \gamma(1-i)$ and since

$$\beta(0) + \beta(1) + \beta(2) + \beta(3) = \gamma(0) + \cdots + \gamma(5) = 0,$$

we get

(b)

$$\beta(1) = \beta(0), \quad \beta(2) = \beta(3) = -\beta(0),$$
$$\gamma(1) = \gamma(0), \quad \gamma(5) = \gamma(2), \quad \gamma(4) = \gamma(3) = -\gamma(0) - \gamma(2).$$

We have

$$\begin{aligned} T_1 &= \sum_{x=1}^{l-1}\sum_{y=0}^{3}(x+yl)\chi_1(x+yl)\omega(x) \\ &= \sum_{x=1}^{l-1} x\omega(x)\sum_{y=0}^{3}\chi_1(x+yl) + l\sum_{x=1}^{l-1}\omega(x)\sum_{y=0}^{3} y\chi_1(x+yl) \\ &= l\sum_{x=1}^{l-1}\omega(x)\sum_{y=1}^{3} y\chi_1(x+yl) \\ &= l[\beta(l-1) - \beta(3l-1) + 2\beta(l-2) - 2\beta(3l-2) + 3\beta(l-3) - 3\beta(3l-3)] \\ &= 8l(-1)^{l+1/2}\beta(0). \end{aligned}$$

Hence, according to (a),

(c) $\beta(0) \neq 0$.

Further we have

$$\begin{aligned} T_2 &= \sum_{x=1}^{l-1}\sum_{y=0}^{2}(x+yl)\chi_2(x+yl)\omega(x) \\ &= \sum_{x=1}^{l-1} x\omega(x)\sum_{y=0}^{2}\chi_2(x+yl) + l\sum_{x=1}^{l-1}\omega(x)\sum_{y=0}^{2} y\chi_2(x+yl) \\ &= l\sum_{x=1}^{l-1}\omega(x)\sum_{y=1}^{2} y\chi_2(x+yl) \\ &= l\sum_{y=1}^{2} y[\gamma(l-y) + \gamma(l-y+3) - \gamma(2l-y) - \gamma(2l-y+3)] \\ &= \begin{cases} 6l\gamma(2) & \text{for } l \equiv 1 \pmod 6, \\ -6l\gamma(2) & \text{for } l \equiv 5 \pmod 6. \end{cases} \end{aligned}$$

According to (a) we have

(d) $\gamma(2) \le 0$.

Since

$$\beta(0) = \sum_{1 \le t \le [l/4]} \omega(4t) = \omega(4) \sum_{1 \le t \le [l/4]} \omega(t) = \omega(4)p(\zeta^{2k}),$$

(c) implies $p(\zeta^{2k}) \neq 0$.

Further we have

$$\begin{aligned}\gamma(2) &= \sum_t \omega(t) \quad (1 \le t \le l-1,\ t \equiv 2l \pmod 6)\\ &= \sum_{-[l/3]\le h\le -[l/6]-1} \omega(2l+6h)\\ &= \sum_{-[l/3]\le h\le -[l/6]-1} \omega(6h)\\ &= \omega(6) \sum_{-[l/3]\le h\le -[l/6]-1} \omega(-h)\\ &= \omega(6) \sum_{[l/6]<h\le [l/3]} \omega(h)\\ &= \omega(6) q(\zeta^{2k})\end{aligned}$$

and (d) implies $q(\zeta^{2k}) \neq 0$. This concludes the proof.

3.4. **Proposition.**

$$|\det P| \le \left[\frac{l}{4}\right]^{(l-1)/4}, \quad |\det Q| \le \left[\frac{l+1}{6}\right]^{(l-1)/4}.$$

Proof. We use Hadamard's lemma [4, p. 260]: "Let $D = \det(a_{rs})_{1\le r,s\le n}$ be a real determinant of order n and let a_r $(1 \le r \le n)$ be nonnegative real numbers defined by the formula:

$$\sum_{s=1}^{n} a_{rs}^2 = a_r^2.$$

Then $|D| \le a_1 \cdots a_n$."

According to 3.2(a) the matrices P, Q have the same number of l's in each row, namely $[\frac{l}{4}]$, $[\frac{l+1}{6}]$, respectively. The result follows.

4. The index of χ-irregularity

Let χ be a Dirichlet character of conductor f. The generalized Bernoulli numbers $B^n(\chi)$ (belonging to χ) are defined by

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B^n(\chi) \frac{t^n}{n!}.$$

These generalized Bernoulli numbers were defined by Leopoldt [14] in 1958.

If χ_0 is the principal character, then

$$B^n(\chi_0) = B_n \qquad (n \ge 0,\ n \neq 1), \quad B^1(\chi_0) = \tfrac{1}{2} = -B_1.$$

If χ_1, χ_2 are the characters with conductors 4, 3 respectively, then for $n \ge 1$

$$B^n(\chi_1) = -\tfrac{1}{2} n E_{n-1}, \quad B^n(\chi_2) = -\tfrac{1}{3} n D_{n-1},$$

where E_n are the Euler numbers defined by the recursion formula:

$$(E+1)^n + (E-1)^n = 0 \qquad (n \ge 1), \quad E_0 = 1,$$

and D_n are the D-numbers defined as follows:

$$(D+1)^n + (D-1)^n + D^n = 0 \qquad (n \geq 1), \quad D_0 = 1.$$

In 1979, Ernvall [7, 3.1] defined the χ-irregular pairs, and in 1985 [8] he defined the index of χ-irregularity of l as the number of these χ-irregular pairs. For $\chi = \chi_1$, $\chi = \chi_2$ the χ-irregular pair is called an E-irregular pair, as D-irregular pair, respectively. Such pairs are just the pairs $(l, 2k)$, $1 \leq k \leq \frac{l-3}{2}$, l/E_{2k}, l/D_{2k}, respectively. The number $\mathrm{i}_E(l)$, $\mathrm{i}_D(l)$ of such pairs is called the *index of E-irregularity of* l, the *index of D-irregularity of* l, respectively. According to definition the (ordinary) index of irregularity $\mathrm{i}(l)$ of l is the index of χ_0-irregularity of l and

$$\mathrm{i}_E(l) = \operatorname{card}\left\{1 \leq k \leq \frac{l-3}{2} : l/E_{2k}\right\}, \quad \mathrm{i}_D(l) = \operatorname{card}\left\{1 \leq k \leq \frac{l-3}{2} : l/D_{2k}\right\}.$$

The following theorem is due to Ernvall [7, 4.2, 4.5] but the statement (a) follows immediately from the congruence (20) in Emma Lehmer's paper [13, 1938].

4.1. **Theorem.** *Let* $1 \leq k \leq \frac{l-3}{2}$.

(a) *A pair* $(l, 2k)$ *is E-irregular if and only if*

$$\sum_{1 \leq t \leq [l/4]} t^{2k} \equiv 0 \pmod{l}.$$

(b) *A pair* $(l, 2k)$ *is D-irregular if and only if*

$$\sum_{1 \leq t \leq [l/3]} t^{2k} \equiv 0 \pmod{l}.$$

For $1 \leq k \leq \frac{l-3}{2}$ *use the notations*

$$a(k) = \sum_{1 \leq t \leq [l/6]} t^{2k}, \quad b(k) = \sum_{[l/6] < t \leq [l/3]} t^{2k},$$

$$c(k) = \sum_{[l/3] < t \leq [l/2]} t^{2k}.$$

Then $a(k) + b(k) + c(k) \equiv 0 \pmod{l}$ and according to [6, §4.3] we have

4.2. **Lemma.**

$$2^{2k} a(k) \equiv (2^{2k} + 1)(a(k) + b(k)) \pmod{l}.$$

This lemma and 4.1(b) prove the following result:

4.3. **Proposition.** *Let* $1 \leq k \leq \frac{l-3}{2}$. *Then the following assertions are equivalent*:

(a) $(l, 2k)$ *is a D-irregular pair,*

(b) $b(k) \equiv 0 \pmod{l}$,

(c) $a(k) \equiv b(k) \equiv c(k) \equiv 0 \pmod{l}$,

(d) $a(k) + b(k) \equiv 2c(k) \pmod{l}$.

Similarly

4.4. **Proposition.** *The following assertions are equivalent for* $1 \leq k \leq \frac{l-3}{2}$:
(a) $a(k) \equiv c(k) \pmod{l}$,
(b) $b(k) \equiv 0 \pmod{l}$ *or* $2^{2k+1} + l \equiv 0 \pmod{l}$.

4.5. **Theorem.**

$$\mathrm{i}_E(l) < \frac{1}{4}\left(1 - \frac{\log 4}{\log l}\right) \quad \text{for } l \geq 5,$$

$$\mathrm{i}_D(l) < \frac{1}{4}\left(1 - \frac{\log 6}{\log l}\right) \quad \text{for } l \geq 7,$$

$$\mathrm{i}_E(3) = \mathrm{i}_D(3) = \mathrm{i}_D(5) = 0.$$

Proof. According to 3.2(b), (c), Theorem 4.1(a) and 4.3 we have for $l \geq 5$ and for the defined matrices P, Q

$$\mathrm{r}(P) = N - \mathrm{i}_E(l), \quad \mathrm{r}(Q) = N - \mathrm{i}_D(l).$$

We get from 1.4, 3.3 and 3.4

$$\mathrm{i}_E(l) < \frac{l}{4}\left(1 - \frac{\log 4}{\log l}\right),$$

$$\mathrm{i}_D(l) < \frac{l}{4}\left(1 - \frac{\log 6}{\log l}\right) \quad \text{for } l \equiv 1 \pmod{6},$$

$$\mathrm{i}_D(l) < \frac{l-1}{4}\left(\frac{\log(l+1)}{\log l} - \frac{\log 6}{\log l}\right) \quad \text{for } l \equiv 5 \pmod{6}.$$

By means of the table of D-irregular pairs [7] we conclude the proof.

4.6. *Remark.* We get from results of Ernvall's paper [8, Theorem] for $\mathrm{i}_E(l)$, $\mathrm{i}_D(l)$ the upper bounds

$$\frac{l-1}{4} + \frac{l-1}{2}\frac{(\log\log l + M)}{\log l},$$

where M is a constant dependent only on the sequences of Euler or D-numbers. This bound is larger than that in Theorem 4.5.

4.7. **Notation.** Put

$$\mu(l) = \mathrm{card}\left\{1 \leq k \leq \frac{l-3}{2} : 2^{2k+1} + 1 \equiv 0 \pmod{l}\right\}.$$

4.8. **Proposition.**

$$\mu(l) < \frac{l \log 2}{2 \log l}.$$

Proof. For an integer x, $3 \leq x \leq l-2$, we have $2^x + 1 \equiv 0 \pmod{l}$ if and only if $x \operatorname{ind} 2 \equiv (l-1)/2 \pmod{l-1}$. Let $\delta = \gcd(l-1, \operatorname{ind} 2)$ and let $l-1 = \delta \cdot \lambda$, $\operatorname{ind} 2 = \delta \cdot \rho$. Then the congruence $x \operatorname{ind} 2 \equiv (l-1)/2 \pmod{l-1}$ is soluble if and only if $2/\lambda$. In this case it has δ solutions and $2^{\lambda/2} + 1 \equiv 0 \pmod{l}$. Since $\mu(l) = 0$ for a Fermat prime, we can assume $2^{\lambda/2} > l$, hence

$$\mu(l) \leq \delta = \frac{l-1}{\lambda} < \frac{l \log 2}{2 \log l}.$$

We get from Carlitz's bound for the first factor of the lth cyclotomic field [4, 1961]:

4.9. **Theorem.**

$$\mathrm{i}(l) < \frac{l}{4}\left(1 - \frac{1+\log 4}{\log l}\right) + \frac{1}{2}.$$

Proof. According to (26) in [4] we have for the first factor h^- of the lth cyclomic field

$$h^- \leq \begin{cases} (m-1)! & \text{for } l = 4m+1, \\ (m-1)!m^{1/2} & \text{for } l = 4m+3. \end{cases}$$

Then $m = [\frac{l}{4}]$ and

$$\log h^- \leq \sum_{t=2}^{m-1} \log t + \frac{1}{2}\log m < \int_2^m \log t\, dt + \frac{1}{2}\log\frac{l}{4} < \frac{l}{4}(\log l - \log 4 - 1) + \frac{1}{2}\log l.$$

The result follows by noting that $l^{\mathrm{i}(l)} \leq h^-$. we get from 4.5, 4.8 and 4.9

4.10. **Theorem.** *For $l \geq 5$ we have*

$$\mathrm{i}(l) + \mathrm{i}_E(l) < \frac{l-3}{2}, \quad \mathrm{i}(l) + \mathrm{i}_D(l) + \mu(l) < \frac{l-3}{2}.$$

5. Solutions of order 3, 4 and 6 of (S)

5.1. **Proposition.** *Let τ be an integer with order* 4 mod l *(i.e. integer τ belongs to exponent* 4 *with respect to modulo l). Then*

$$\mathrm{r}(D_l(\tau)) = \frac{l-3}{2} - \mathrm{i}_E(l).$$

Proof. We have $l \equiv 1 \pmod 4$, $\tau^2 \equiv -1 \pmod l$, $\tau^3 \equiv -\tau \pmod l$ and $\tau^4 \equiv 1 \pmod l$. According to 2.5 $\mathrm{r}(D_l(\tau)) = N - n_1$, where n_1 means the number of integers k, $0 \leq k \leq (l-3)/2$ such that

$$\sum_{t=1}^{N} (\tau^t + \tau^{l-t})t^{2k} \equiv 0 \pmod l.$$

For $t \in \mathbf{Z}$ put

$$\varepsilon(t) = \begin{cases} 1 & \text{for } t \equiv 0 \text{ or } t \equiv 1 \pmod 4, \\ -1 & \text{for } t \equiv 2 \text{ or } t \equiv 3 \pmod 4. \end{cases}$$

Then

$$\sum_{t=1}^{N} (\tau^t + \tau^{l-t})t^{2k} \equiv (1+\tau)\sum_{t=1}^{N} \varepsilon(t)t^{2k} \pmod l.$$

Since $\sum_{t=1}^{N} \varepsilon(t) = 0$ and $\sum_{t=1}^{N} t^{2k} \equiv 0 \pmod l$ for $1 \leq k \leq (l-3)/2$, the number $n_1 - 1$ equals the number of integers k $(1 \leq k \leq (l-3)/2)$ with

$$\sum_{t=1}^{N} t^{2k}(t \equiv 0 \text{ or } t \equiv 1 \pmod 4) \equiv 0 \pmod l.$$

Since

$$\sum_{t=1}^{N} t^{2k}(t \equiv 0 \text{ or } t \equiv 1 \pmod 4)$$
$$\equiv \sum_{t=1}^{N} t^{2k}(t \equiv 0 \pmod 4) + \sum_{t=1}^{N}(l-t)^{2k}(t \equiv 1 \pmod 4) \pmod l$$
$$= 4^{2k} \sum_{1 \le t \le [l/4]} t^{2k},$$

we get the proposition from Theorem 4.1.

Then Theorems 2.3 and 4.10 give the following:

5.2. **Theorem** ("Morishima's" case). *Any integer* τ *with order* 4 mod l *is no solution of the system* (S).

5.3. **Proposition.** *Let* τ *be an integer with order* 6 mod l. *Then*

$$\mathrm{r}(D_l(\tau)) \ge \frac{l-3}{2} - \mathrm{i}_D(l) - \mu(l).$$

Proof. We have $l \equiv 1 \pmod 6$, $\tau^2 \equiv \tau - 1 \pmod l$, $\tau^3 \equiv -1 \pmod l$, $\tau^4 \equiv -\tau \pmod l$, $\tau^5 \equiv 1 - \tau \pmod l$ and $\tau^6 \equiv 1 \pmod l$. For $t \in \mathbf{Z}$ put

$$\varepsilon(t) = \begin{cases} 1 & \text{for } t \equiv 0 \text{ or } t \equiv 1 \pmod 6, \\ 0 & \text{for } t \equiv 2 \text{ or } t \equiv 5 \pmod 6, \\ -1 & \text{for } t \equiv 3 \text{ or } t \equiv 4 \pmod 6. \end{cases}$$

Then for an integer k, $0 \le k \le (l-3)/2$, we have

$$\sum_{t=1}^{N}(\tau^t + \tau^{l-t})t^{2k} \equiv (1+\tau)\sum_{t=1}^{N}\varepsilon(\tau)t^{2k} \pmod l.$$

Since $\sum_{t=1}^{N}\varepsilon(t) = 0$, $\mathrm{r}(D(\tau)) = N - n_1$ according to 2.5, where $n_1 - 1$ is the number of k's, $1 \le k \le (l-3)/2$, with the property

$$\sum_{t=1}^{N}\varepsilon(t)t^{2k} \equiv 0 \pmod l.$$

The following holds:

$$\sum_{t=1}^{N} t^{2k}(t \equiv 0 \text{ or } t \equiv 1 \pmod 6) \equiv \sum_{t=1}^{N} t^{2k}(t \equiv 0 \pmod 6)$$
$$+ \sum_{t=1}^{N}(l-t)^{2k}(t \equiv 1 \pmod 6) \pmod l$$
$$= \sum_{t}(6t)^{2k}\ (1 \le t \le (l-1)/6) = 6^{2k}a(k)$$

(definition of $a(k)$ and $c(k)$ behind 4.1),

$$\begin{aligned}
&\sum_{t=1}^{N} t^{2k}(t \equiv 3 \text{ or } t \equiv 4 \pmod 6) \\
&\quad \equiv \sum_{t=1}^{N} t^{2k}(t \equiv 3 \pmod 6) + \sum_{t=1}^{N}(l-t)^{2k}(t \equiv 4 \pmod 6) \pmod l \\
&\quad = \sum_{t=1}^{l-1} t^{2k}(t \equiv 3) \pmod 6) \\
&\quad \equiv \sum_{t}(6t + 3 \cdot 6(l-1)/6)^{2k}(1 \le t \le (l-1)/6) \\
&\quad \equiv 6^{2k} \sum_{t}(l - t - N)^{2k}(1 \le t \le (l-1)/6) \pmod l = 6^{2k} c(k).
\end{aligned}$$

Therefore $n_1 - 1$ equals the number of k's, $1 \le k \le (l-3)/2$, with the property $a(k) \equiv c(k) \pmod l$.

Using 4.3 and 4.4 we get $n_1 - 1 \le \mathrm{i}_D(l) + \mu(l)$, and we are done.

5.4. **Proposition.** *Let τ be an integer with order 3 mod l. Then*

$$\mathrm{r}(D_l(\tau)) = \frac{l-3}{2} - \mathrm{i}_D(l).$$

Proof. Let $l \equiv 1 \pmod 6$ and put for $t \in \mathbf{Z}$.

$$\varepsilon(t) = \begin{cases} 1 & \text{for } t \equiv 0 \text{ or } t \equiv 1 \pmod 3, \\ -2 & \text{for } t \equiv 2 \pmod 3. \end{cases}$$

Since $\tau^2 \equiv -(1+\tau) \pmod l$ and $\tau^3 \equiv 1 \pmod l$, we have for an integer k, $0 \le k \le (l-3)/2$,

$$\sum_{t=1}^{N}(\tau^t + \tau^{1-t} t^{2k} \equiv (1+\tau) \sum_{t=1}^{N} \varepsilon(t) t^{2k} \pmod l.$$

Similarly as in the proof of 5.3 $\mathrm{r}(D(\tau)) = N - n_1$, where n_1 is the number of k's, $1 \le k \le (l-3)/2$ such that

$$\sum_{t=1}^{N} \varepsilon(t) t^{2k} \equiv 0 \pmod l.$$

We have for $1 \le k \le (l-3)/2$

$$\sum_{t=1}^{N} t^{2k}(t \equiv 0 \text{ or } t \equiv 1 \pmod 3) = \sum_{t=1}^{N} t^{2k}(t \equiv 0 \pmod 3)$$
$$+ \sum_{t=1}^{N} t^{2k}(t \equiv 1 \pmod 3) \equiv \sum_{t=1}^{N} t^{2k}(t \equiv 0 \pmod 3)$$
$$+ \sum_{t=1}^{N} (l-t)^{2k}(t \equiv 1 \pmod 3) \pmod l$$
$$= \sum_{t=1}^{l-1} t^{2k}(t \equiv 0 \pmod 3) = 3^{2k}(a(k) + b(k)),$$

$$\sum_{t=1}^{N} t^{2k}(t \equiv 2 \pmod 3)$$
$$\equiv \sum_{t} (3t + 3(l-1)/3)^{2k} \quad \left(1 \le t \le \frac{l-1}{6}\right) \pmod l$$
$$= 3^{2k} c(k).$$

The result follows immediately from 4.3.

Theorems 2.3, 4.10 and Propositions 5.3, 5.4 give the following result:

5.5. **Theorem** ("Pollaczek's" case). *Any integer* τ *with order* 3 *or* 6 mod l *is no solution of the system* (S).

6. Solutions of (S) with "small" orders

6.1. Let n, k, τ be integers, $n \ge 5$, $k \ge 1$, and let order of τ mod l equals n. Assume that there exist subsets $X_1, \dots, X_k, Y_1, \dots, Y_k$ of $\{1, 2, \dots, N\}$ with the following properties:

(a) the sets X_i, Y_j form complete sets of residues modulo n $(1 \le i, j \le k)$,
(b) for $2 \le j \le k$ the following holds: $x \in X_j$, $y \in Y_j \Rightarrow l < xy < 2l$,
(c) for $1 \le j < i \le k$ we have $x \in X_i$, $y \in Y_j \Rightarrow xy < l$,
(d) $x \in X_1$, $y \in Y_1 \cup \cdots \cup Y_k \Rightarrow xy < l$.

Note that then the collections of sets $\{X_1, X_2, \dots, X_k\}$ and $\{Y_1, Y_2, \dots, Y_k\}$ are pairwise disjoint.

6.1.1. **Proposition.** *The columns* $\mathbf{c}_y$ $(y \in Y_1 \cup \cdots \cup Y_k)$ *of the matrix* $D_l(\tau)$ *are linearly independent over the Galois field* $\mathbf{Z}/l\mathbf{Z}$.

Proof. Let $Y = Y_1 \cup \cdots \cup Y_k$ and let $a_y \in \mathbf{Z}$ for each $y \in Y$ such that

$$\sum_{y} a_y \mathbf{c}_y (y \in Y) \equiv 0 \pmod l.$$

Then we have for each $1 \le x \le N$

$$\sum_{y} a_y \tau^{a(x,y)} (y \in Y) + \tau \sum_{y} a_y \overline{\tau}^{a(x,y)} (y \in Y) \equiv 0 \pmod l.$$

Denote by f the bijection from Y onto Y defined by

$$y \equiv Y_j \ (1 \le j \le k) \Rightarrow f(y) \in Y_j, \quad f(y) \equiv -y \pmod{n}.$$

(This mapping is well defined because the sets Y_j are complete sets of residues (mod n) and they are pairwise disjoint.)

Since for each $x \in X_1$ and $y \in Y$, $a(x, y) = xy$ and $(n-1)xy \equiv xf(y) \pmod{n}$, we have

$$\begin{aligned} 0 &\equiv \sum_y a_y \tau^{xy} (y \in Y) + \tau \sum_y a_y \tau^{xf(y)} (y \in Y) \pmod{l} \\ &= \sum_y \tau^{xy} (a_y + \tau a_{f(y)}) (y \in Y) \\ &\equiv \sum_{t=0}^{n-1} \tau^{xt} \sum_y (a_y + \tau a_{f(y)}) (y \in Y, \ y \equiv t \pmod{n}) \pmod{l}, \end{aligned}$$

thus for each $0 \le t \le n-1$

$$\sum_y (a_y + \tau a_{f(y)}) (y \in Y, \ y \equiv t \pmod{n}) \equiv 0 \pmod{l}. \tag{1}$$

Let $k = 1$. Then $a_y + \tau a_{f(y)} \equiv 0 \pmod{l}$ for each $y \in Y$. For $0 \le i \le n-1$ put $b(i) = a_y$, where $y \equiv Y$, $i \equiv y \pmod{n}$.

Then

$$b(0)(1 + \tau) \equiv 0 \pmod{l},$$

hence $b(0) \equiv 0 \pmod{l}$.

For $1 \le i \le n-1$ we have $b(i) \equiv -\tau b(n-i) \pmod{l}$, therefore also $b(n-i) \equiv -\tau b(i) \pmod{l}$.

It follows $b(i) \equiv \tau^2 b(i) \pmod{l}$, hence $b(i) \equiv 0 \pmod{l}$, which shows that $a_y \equiv 0 \pmod{l}$ for each $y \in Y$.

Let $k > 1$. For $0 \le t \le n-1$ put

$$b_t = \sum_y (a_y + \tau a_{f(y)}) (y \in Y - Y_k, \ y \equiv t) \pmod{n})$$

$$c_t = a_y, \quad d_t = \tau a_{f(y)}, \quad \text{where } y \in Y_k, \ y \equiv t \pmod{n}.$$

According to (1) we have for each $0 \le t \le n-1$:

$$c_t + b_t + d_t \equiv 0 \pmod{l}. \tag{2}$$

Let $x \in X_k$. Then

$$\begin{aligned} 0 &\equiv \sum_y a_y \tau^{xy} (y \in Y - Y_k) + \sum_y a_y \tau^{xy-1} (y \in Y_k) \\ &\quad + \tau \sum_y a_{f(y)} \tau^{xy} (y \in Y - Y_k) + \tau \sum_y a_{f(y)} \tau^{xy+1} (y \in Y_k) \pmod{l} \\ &= \sum_{t=0}^{n-1} \tau^{xt-1} \left[\sum_y \tau (a_y + \tau a_{f(y)}) \ (y \in Y - Y_k, \ y \equiv t \pmod{n}) \right. \\ &\qquad \left. + \sum_y (a_y + \tau^3 a_{f(y)}) (y \in Y_k, \ y \equiv t \pmod{n}) \right], \end{aligned}$$

thus we have for each $0 \leq t \leq n-1$

$$c_t + \tau b_t + \tau^2 d_t \equiv 0 \pmod{l}. \tag{3}$$

Congruences (2) and (3) imply

$$c_t \equiv \tau d_t \pmod{l} \quad \text{for each } 0 \leq t \leq n-1.$$

Since $d_0 = \tau c_0 \equiv \tau^2 d_0 \pmod{l}$, we have $c_0 \equiv d_0 \equiv 0 \pmod{l}$.

For $l \leq t \leq n-1$ the following holds

$$d_t = \tau c_{n-t} \equiv \tau^2 d_{n-t} \pmod{l} = \tau^3 c_t \equiv \tau^4 d_t \pmod{l},$$

thus $c_t \equiv d_t \equiv 0 \pmod{l}$.

It follows $a_y \equiv 0 \pmod{l}$ for each $y \in X_k$. Using mathematical induction for k we obtain the proposition.

6.2. **Proposition.** *Let*

$$5 \leq n < \sqrt{l/2}, \quad k = [-1/2n + \sqrt{n^2 + 4ln}/2n^2] + 1.$$

Then there are subsets $X_1, \ldots, X_k, Y_1, \ldots, Y_k$ *of* $\{1, 2, \ldots, N\}$ *with the properties* (a)–(d) *from* 6.1.

Proof. Put $\overline{X}_1 = X_1 = Y_1 = \{1, 2, \ldots, n\}$. If $k = 1$, then X_1, Y_1 possess the given properties. Assume $k > 1$.

For $1 \leq h < -1/2n + \sqrt{n^2 + 4ln}/2n^2$ put

$$\overline{X}_{h+1} = \{x \in \mathbf{Z}\colon l/(hn+1) < x < l/hn\},$$
$$Y_{h+1} = \{y \in \mathbf{Z}\colon hn + 1 \leq y < (h+1)n\}.$$

It is only a technical matter to prove that the sets $\overline{X}_1, \ldots, \overline{X}_k, Y_1, \ldots, Y_k$ fulfil the conditions (b)–(d) from 6.1. Since $\operatorname{card} \overline{X}_i \geq n$, the proposition follows.

6.3. **Proposition.** *Let* $5 \leq n < \sqrt{l/2}$ *and let* τ *be an integer of order* $n \bmod l$. *Then* $\mathrm{r}(D_l(\tau)) \geq [\sqrt{1/n}]$.

Proof. According to 6.1.1 and 6.2 we have $\mathrm{r}(D_l(\tau)) \geq kn$, where $k = [-1/2n + \sqrt{n^2 + 4ln}/2n^2] + 1$.

The result follows by noting that $kn > \sqrt{l/n} - 1$.

Using Proposition 6.3 and Theorem 2.3 we get

6.4. **Theorem.** *Let* $5 \leq n < \sqrt{l/2}$ *and let* τ *be a solution of the system* (S) *of order* $n \bmod l$. *Then* $\mathrm{i}(l) \geq [\sqrt{l/n}]$.

7. Solutions of (S) with "large" orders and conclusion

7.1. **Proposition.** *Let* $1 \leq m < \sqrt{l/2}$ *and let* τ *be an integer of order* $\bmod l$ *greater than* $2m$. *Then* $\mathrm{r}(D_l(\tau)) \geq m$.

Proof. We show that the first m columns $\mathbf{c}_1, \ldots, \mathbf{c}_m$ of the matrix $D_l(\tau)$ are linearly independent over the Galois field $\mathbf{Z}/l\mathbf{Z}$.

Let $a_y \in \mathbf{Z}$ $(1 \leq y \leq m)$ such that

$$\sum_{y=1}^{m} a_y \mathbf{c}_y \equiv 0 \pmod{l}.$$

Then for each x $(1 \leq x \leq 2m)$ we have

$$\sum_{y=1}^{m} a_y \tau^{xy} + \sum_{y=1}^{m} a_y \tau \overline{\tau}^{xy} \equiv 0 \pmod{l}$$

which is a system of $2m$ linear congruences with $2m$ unknowns a_y, $a_y\tau$ $(1 \leq y \leq m)$ with the Vandermonde determinant (multiplied by factors τ^y, $\overline{\tau}^y$)

$$d = \det(\tau^{xy} | \overline{\tau}^{xy}) \qquad (1 \leq x \leq 2m,\ 1 \leq y \leq m).$$

Since order of $\tau \bmod l$ is greater than $2m$, $d \not\equiv 0 \pmod{l}$, hence $a_y \equiv 0 \pmod{l}$ for each $1 \leq y \leq m$, and we are done.

This proposition and Theorem 2.3 imply

7.2. **Theorem.** *Let* $1 \leq m < \sqrt{l/2}$ *and let* τ *be a solution of the system* (S) *of order* mod l *greater than* $2m$. *Then* $\mathrm{i}(l) \geq m$.

7.3. **Corollary.** *Let there exist a solution of the system* (S) *of order* $l-1 \bmod l$ *and* $l \geq 5$. *Then* $\mathrm{i}(l) \geq [\sqrt{l/2}]$.

7.4. **Corollary.** *Let there exist a solution of the system* (S) *of order* mod l *greater than* $\sqrt{l/2}$. *Then* $\mathrm{i}(l) \geq [\sqrt{l/8}]$.

7.5. *Remark.* If τ is a solution of the system (S) with $\tau \not\equiv 0 \pmod{l}$ and $\tau \not\equiv -1 \pmod{l}$, then $\mathrm{i}(l) \geq 2$, hence $l \geq 157$.

Proof. According to Theorems 5.3 and 5.5 we have for the order n of $\tau \bmod l$, $n \geq 5$ and $n \neq 6$, hence $l \geq 11$. According to 6.4 and 7.4 we have

$$\mathrm{i}(l) \geq \min\left\{\left[\sqrt{l/8}\right],\ \left[\sqrt[4]{2l}\right]\right\} \geq 1$$

and therefore $\mathrm{i}(l) \geq 2$ for $l \geq 32$.

The result follows from the tables of irregular primes [1, Table 9].

7.6. **Theorem.** *If there exists a solution* τ *of the system* (S), $\tau \not\equiv 0 \pmod{l}$, $\tau \not\equiv -1 \pmod{l}$, *then* $\mathrm{i}(l) \geq [\sqrt[3]{l/2}]$.

Proof. We can assume according to 5.3 and 5.5 that $n \geq 5$, where n is order of $\tau \bmod l$. Further, according to 7.5 assume $l \geq 157$.

It follows from 7.4 $\mathrm{i}(l) \geq [\sqrt{l/8}] \geq [\sqrt[3]{l/2}]$ for $n > \sqrt{l/2}$.

If $n < \sqrt[3]{4l}$, then $n < \sqrt{l/2}$ and according to 6.4 $\mathrm{i}(l) \geq [\sqrt{l/n}] \geq [\sqrt[3]{l/2}]$.

If $\sqrt[3]{4l} < n < \sqrt{l/2}$ put $m = [(n-1)/2]$. Then we get from 7.2

$$\mathrm{i}(l) \geq [(n-1)/2] \geq \frac{n}{2} - 1 > \sqrt[3]{l/2} - 1,$$

hence $\mathrm{i}(l) \geq [\sqrt[3]{l/2}]$.

7.7. *Remark.* Under assumptions of 7.6 we have $l > 150{,}000$ and $\mathrm{i}(l) \geq 42$.

Proof. By the statement in Remark 7.5, $l \geq 157$, so according to Theorem 7.6, $\mathrm{i}(l) \geq 4$. Using again the tables of irregular primes (e.g. [1, Table 9]) we get $l > 432$, therefore by Theorem 7.6, $\mathrm{i}(l) \geq 6$.

Since, according to the latest tables for the index of irregularity by Tanner and Wagstaff [24, 1987] and Wagstaff [26, 1978], $\mathrm{i}(l) \leq 5$ for $l < 150{,}000$, Theorem 7.6 concludes the proof.

Using quite recently made out tables of the index of irregularities by Buhler, Crendall and Sompolski [3, 1991] ($\max \mathrm{i}(l) = 6$ for $l < 10^6$) we get

$$l > 10^6 \quad \text{and} \quad \mathrm{i}(l) \geq 62.$$

7.8. *Remark.* By Washington [27, Chapter 6, §6.5] probability arguments indicate $\mathrm{i}(l) = O(\log l / \log\log l)$. Therefore we can conclude (1.8, 1.9(a), (c) and 7.6) that besides $\tau \equiv 0 \pmod{l}$ and $\tau \equiv \pm 1 \pmod{l}$ the Kummer system of congruences has with great probability no solution.

References

1. Z. J. Borevich and J. R. Shafarevich, *Number theory*, Academic Press, London and New York, 1966.
2. H. Brückner, *Explizites Reciprozitätsgesetz und Anwendungen*, Vorlesungen Fachbereich Math. Univ. Essen, Heft 2, 1979, 83 pp..
3. J. Buhler, R. Crendall, and B. Sompolski, *Irregular primes to one million*, Math. Comp. **59** (1992), 717–722.
4. L. Carlitz, *A generalization of Maillet's determinant and a bound for the first factor of the class number*, Proc. Amer. Math. Soc. **12** (1961), 256–261.
5. M. Eichler, *Eine Bemerkung zur Fermatschen Vermutung*, Acta Arith. **11** (1965), 129–131, 261.
6. G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden*, Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königl. Akademie der Wissenschaften zu Berlin, 1850, pp. 36–452 (p. 41). Math. Werke, Gotthold Eisenstein, Band II, Chelsea, New York, 2nd ed., 1989, pp. 705–711 (p. 710).
7. R. Ernvall, *Generalized Bernoulli numbers, generalized irregular primes, and class number*, Ann. Univ. Turku Ser. A Math. **178** (1979), 72 pp.
8. ———, *An upper bound for the index of χ-irregularity*, Mathematika **32** (1985), 39–44.
9. A. Granville and M. B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714, 591, 416, 091, 389, Trans. Amer. Math. Soc. **306** (1988), 329–359.
10. N. G. Gunderson, *Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent*, Thesis, Cornell Univ., 1948.
11. H. Kleboth, *Untersuchung über Klassenzahl und Reziprozitätsgesetz im Körper der 6l-ten Einheitswurzeln und die Diophantische Gleichung $x^{2l} + 3^l y^{2l} = z^{2l}$ für eine Primzahl l grösser als* 3, Dissertation, Universität Zürich, 1955, 37 pp.
12. E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten comlexen Zahlen, für den Fall, dass die Klassenanzahl durch λ theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Math. Abhandl. Königl. Akad. Wiss. zu Berlin, 1857, pp. 41–74. (Collected Papers, I, 639–692).
13. E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **39** (1938), 350–360.
14. H. W. Leopoldt, *Eine Verallgemeinerung der Bernoullischen Zahlen*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 131–140.
15. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, London, 1983.
16. T. Morishima, *Über die Fermatsche Quotienten*, Japan J. Math. **8** (1931), 159–173.
17. F. Pollaczek, *Über den grossen Fermat'schen Satz*, Sitzungsber. Akad. Wiss. Wien Abt. IIa **126** (1917), 45–59.
18. P. Ribenboim, 13 *lectures on Fermat's Last Theorem*, Springer-Verlag, New York, Heidelberg, and Berlin, 1979.
19. L. Skula, *Non-possiblity to prove infinity of regular primes from some theorems*, J. Reine Angew. Math. **291** (1977), 162–181.

20. ———, *A remark on Mirimanoff polynomials*, Comment. Math. Univ. St. Paul. **31** (1982), 89–97.

21. ———, *On the Kummer's system of congruences*, Comment. Math. Univ. St. Paul. **35** (1986), 137–163.

22. ———, *A note on the index of irregularity*, J. Number Theory **22** (1986), 125–138.

23. ———, *Fermat's last theorem and the Fermat quotients*, Comment. Math. Univ. St. Paul **41** (1992), 35–54.

24. J. W. Tanner and S. S. Wagstaff, *New congruences for the Bernoulli numbers*, Math. Comp. **48** (1987), 341–350.

25. T. Uehara, *Fermat's conjecture and Bernoulli numbers*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **6** (1978), 9–14.

26. S. S Wagstaff, *The irregular primes to* $125,000$, Math. Comp. **32** (1978), 583–591.

27. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, Heidelberg, and Berlin, 1982.

Department of Mathematics, Faculty of Science, Masaryk University, Janáčkovo nám. 2a, 662 95 Brno, Czech Republic