Ladislav Skula
Linear transforms supporting circular convolution on residue class rings

Mathematica Slovaca, Vol. 39 (1989), No. 4, 377--390

Persistent URL: http://dml.cz/dmlcz/130500

Math. Slovaca 39, 1989, No. 4, 377—390

LINEAR TRANSFORMS SUPPORTING CIRCULAR CONVOLUTION ON RESIDUE CLASS RINGS

LADISLAV SKULA

0. Introduction

The aim of this paper is to describe all the linear transforms supporting circular convolution on a residue class ring $\mathbf{Z}/m\mathbf{Z}$ for any integer $m \geqq 2$. This question was raised in [4] (5.5). According to the results of [4] (2.9) the investigations of such transforms lead to those of the *matrices supporting circular convolution* — *SCC-matrices* (1.1). It is shown that this general case leads to the case of m being a prime power $m = p^n$.

We describe all the *SCC*-matrices in the residue class ring $\mathbf{Z}/p^n\mathbf{Z}$ in the Main Theorem 1.5 by means of *p-adic integers* discovered by Kurt Hensel at the beginning of this century.

Linear transforms over a commutative ring with an identity element supporting circular convolution are exactly defined in [4] (2.3). The beginning of investigations of these questions is due to R. C. Agarwal and Ch. S. Burrus [1].

The basic property of p-adic integers can be found in [2] or [3].

1. Introductory Paragraph

Throughout the whole paper we shall denote by

N a positive integer

p a prime

n a positive integer

$\mathbf{Z}$ the ring of rational integers

$\mathbf{Z}_p$ the ring of p-adic integers, hence each element $\alpha \in \mathbf{Z}_p$ has the form $\alpha = a_0 + a_1 p + a_2 p^2 + \dots$
whee $0 \leqq a_i \leqq p - 1$ $(i = 0, 1, 2, \dots)$
are rational integers,

Φ_n the canonical homomorphism from the ring $\mathbf{Z}_p$ onto the quotient ring $\mathbf{Z}_p/p^n\mathbf{Z}_p = \mathbf{Z}/p^n\mathbf{Z}$ (canonically), i.e. for $z \in \mathbf{Z}_p$ we have $z \in \Phi_n(z) \in \mathbf{Z}_p/p^n\mathbf{Z}_p$.

If $\mathbf{X} = (x_{ij})$ $(0 \leqq i \leqq K-1, 0 \leqq j \leqq L-1)$ is a matrix over the ring $\mathbf{Z}_p$ of size K/L, we denote by $\Phi_n(\mathbf{X})$ the matrix $(\Phi_n(x_{ij}))$ $(0 \leqq i \leqq K-1,\ 0 \leqq j \leqq L-1)$ over the ring $\mathbf{Z}_p/p^n\mathbf{Z}_p$ of size K/L.

1.1. Let R be a commutative ring with an identity element 1_R different from the zero element 0_R of R. In the paper [4] (2.8) the notion of *matrices supporting circular convolution* was introduced in the following way:

Let $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (c_{ij})$ $(0 \leqq i, j \leqq N-1)$ be square matrices of order N over R $(a_{ij}, b_{ij}, c_{ij} \in R)$. We say that the *matrices* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *support circular convolution* or briefly *they are SSC-matices* if for each $0 \leqq u, v, w \leqq N-1$ the following relation holds:

$$\sum_{k=0}^{N=1} a_{ku} b_{kv} c_{kw} = \begin{cases} 1_R & \text{for } u + v + w \equiv 0 \pmod{N} \\ 0_R & \text{otherwise.} \end{cases}$$

This notion is justified by that of *linear transforms supporting circular convolution* (or *having the circular convolution property*) as explained in [4] (Paragraph 2) and it is connected with the notions of *Circular Convolution* and *Discrete Fourier Transform.*

1.2. For the case R being a (commutative) field the following theorem was derived [4] (3.6):

Theorem. *Let F be a commutative field and* $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (c_{ij})$ $(0 \leqq i, j \leqq N-1)$ *square matrices of order N over F. Then the following statements are equivalent*:

(a) *The matrices* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *support circular convolution.*

(b) *For each* $0 \leqq k \leqq N-1$ *there exist* $a_k, b_k, c_k, g_k \in F$ *such that*

(α) $g_k^N = 1_F$,

(β) $N a_k b_k c_k = 1_F$,

(γ) *the elements* g_k $(0 \leqq k \leqq N-1)$ *are different,*

(δ) $a_{kh} = g_k^h a_k$, $b_{kh} = g_k^h b_k$, $c_{kh} = g_k^h c_k$ *for each* $0 \leqq h \leqq N-1$.

It was also shown in [4] (4.1) that *the Theorem holds even if the field F is replaced by an integral domain D.*

1.3. From the definition of SCC-matrices it follows that the study of SCC-matrices over the direct sum of rings leads to the study of SCC-matrices over single components. Thus *the investigation of SCC-matrices over a residue class ring* $\mathbf{Z}/m\mathbf{Z}$ *(m a rational integer $\geqq 2$) is reduced to the case of m being a prime power.* Our main result gives a description of the SCC-matrices over such a ring by means of p-adic integers.

From the definition of SCC-matrices we immediately obtain.

1.4. Theorem. *Let* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *be SCC-matrices over the ring* $\mathbf{Z}_p$. *Then the matrices* $\Phi_n(\mathbf{A})$, $\Phi_n(\mathbf{B})$, $\Phi_n(\mathbf{C})$ *over the ring* $\mathbf{Z}/p^n\mathbf{Z}$ $(\mathbf{Z}_p/p^n\mathbf{Z}_p)$ *support circular convolution.*

We shall give a proof of the main result of this paper — the converse of 1.4 — in Paragraph 3:

1.5. Main Theorem. *Let $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ be SCC-matrices over the ring $\mathbf{Z}/p^n\mathbf{Z}$. Then there exist SCC-matrices* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *over the ring $\mathbf{Z}_p$ such that* $\mathscr{A} = \Phi_n(\mathbf{A})$, $\mathscr{B} = \Phi_n(\mathbf{B})$, $\mathscr{C} = \Phi_n(\mathbf{C})$.

1.6. Remark. For order $N = 1$ or $N = 2$ of the matrices $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ the proof was given in [4] (5.4).

1.7. The question of SCC-matrices over the residue class ring $\mathbf{Z}/p_n\mathbf{Z}$ is transferred in this way to the question of SCC-matrices over the ring $\mathbf{Z}_p$ of p-adic integers. The existence of these matrices is solved by theorem [4] (5.1):

Theorem. *Ther exist SSC-matrices* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *of order N over the ring $\mathbf{Z}_p$ if and only if N divides $p - 1$.*

The description of these matrices is then given by Theorem 1.2 for the integral domain $D = \mathbf{Z}_p$.

2. The Rank of Special Matrix $\mathfrak{A}$

We shall suppose in this paragraph that

$$N \geqq 2,\ N/p - 1$$

and g will mean a rational integer of order $N \bmod p$.

The congruence $\bmod N$ on $\mathbf{Z}$ will be denoted only by $\equiv$.

The *Galois field* $GF(p) = \mathbf{Z}/p\mathbf{Z}$ will be denoted by P and the rational integers will often be considered as the eements of the field P as well as the number g^{-1}.

In this paragraph a special matrix $\mathfrak{A}$ of size $N^3/3N^2$ over P is defined and it is shown (2.9) that the rank of $\mathfrak{A}$ (over P) is equal to $3N^2 - 2N$.

2.1. Notation. For $u, v, w, t \in \mathbf{Z}$, $u \not\equiv 0$, $v \not\equiv 0$ let $c = c([u, v, w], t) \in P$ be defined in the following way:

a) for $u \not\equiv v$, $u \not\equiv -v$

$$c = \begin{cases} 1 & \text{for } t \equiv w, \\ -1 & \text{for } t \equiv v + w, \\ -1 & \text{for } t \equiv u + w, \\ 1 & \text{for } t \equiv u + v + w, \\ 0 & \text{otherwise,} \end{cases}$$

b) for $u \equiv -v$, $u \not\equiv v$

$$c = \begin{cases} 2 & \text{for } t \equiv w, \\ -1 & \text{for } t \equiv v + w \equiv -u + w, \\ -1 & \text{for } t \equiv u + w, \\ 0 & \text{otherwise,} \end{cases}$$

c) for $u \equiv v$, $u \not\equiv -v$

$$c = \begin{cases} 1 & \text{for } t \equiv w, \\ -2 & \text{for } t \equiv w + u, \\ 1 & \text{for } t \equiv w + 2u, \\ 0 & \text{otherwise,} \end{cases}$$

d) for N even, $u \equiv v \equiv \frac{N}{2}$

$$c = \begin{cases} 2 & \text{for } t \equiv w, \\ -2 & \text{for } t \equiv \frac{N}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

Put for $u, v, \lambda, t \in Z$, $u \not\equiv 0$, $v \not\equiv 0$

$$c^{(\lambda)}([u, v], t) = c([u, v, \lambda - (u + v)], t)$$

and for $0 \leqq \lambda \leqq N - 1$ denote by $\mathfrak{C}(\lambda)$ the matrix

$$\mathfrak{C}(\lambda) = (c^{(\lambda)}([u, v], t))\,(1 \leqq u, v \leqq N - 1, 0 \leqq t \leqq N - 1)$$

of size $(N - 1)^2/N$ *over* P, *where* [u, v] *is an index for the row and* t *means a column index.*

2.2. Lemma. *The rank of the matrix* $\mathfrak{C}(0)$ *(over P) is* $N - 1$.

Proof. I. For $1 \leqq v \leqq N - 1$ let $\boldsymbol{r}_v$ be the row of matrix $\mathfrak{C}(0)$ with index $[N - v, N - 1]$. Put

$$\boldsymbol{s}_1 = \frac{1}{N}(\boldsymbol{r}_1 + \ldots + \boldsymbol{r}_{N-1}),$$

$$\boldsymbol{s}_v = (v - N)\,\boldsymbol{s}_1 + \boldsymbol{r}_{N-1} + \ldots + \boldsymbol{r}_n \qquad \text{for } 2 \leqq v \leqq N - 1$$

and

$$\boldsymbol{s}_v = (s_{v0}, s_{v1}, \ldots, s_{vN-1}) \qquad \text{for } 1 \leqq v \leqq N - 1.$$

Then for $0 \leqq j \leqq N - 1$ and $1 \leqq v \leqq N - 1$ we have

$$s_{vj} = \begin{cases} 1 & \text{for } j = 0, \\ -1 & \text{for } j = v, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that the vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{N-1}$ are linearly independent (over P) and are elements of the vector space generated by the rows of the matrix $\mathfrak{C}(0)$.

II. It is enough to show that each row of the matrix $\mathfrak{C}(0)$ is a linear combination of th vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{N-1}$.

Let $1 \leqq u, v \leqq N - 1$ and consider the row $\boldsymbol{r} = (r_0, r_1, \ldots, r_{N-1})$ with index $[u, v]$ and let $0 \leqq t \leqq N - 1$.

a) Let $u \not\equiv v$, $u \not\equiv -v$. Then

$$r_t = \begin{cases} 1 & \text{for } t \equiv -(u+v), \\ -1 & \text{for } t \equiv -u, \\ -1 & \text{for } t \equiv -v, \\ 1 & \text{for } t \equiv 0, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\boldsymbol{r} = \boldsymbol{s}_{N-u} + \boldsymbol{s}_{N-v} - \boldsymbol{s}_l$, where $1 \leqq l \leqq N-1$, $l \equiv -(u+v)$.

b) Let $u \equiv -v$, $u \not\equiv v$. Then

$$r_t = \begin{cases} 2 & \text{for } t = 0, \\ -1 & \text{for } t \equiv v, \\ -1 & \text{for } t \equiv u, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\boldsymbol{r} = \boldsymbol{s}_u + \boldsymbol{s}_v$.

c) Let $u \equiv v$, $u \not\equiv -v$. Then

$$r_t = \begin{cases} 1 & \text{for } t \equiv -2u, \\ -2 & \text{for } t \equiv -u, \\ 1 & \text{for } t = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\boldsymbol{r} = 2\boldsymbol{s}_{N-u} - \boldsymbol{s}_l$, where $1 \leqq l \leqq N-1$, $l \equiv -2u$.

d) Let N be even and $u = v = \frac{N}{2}$. Then

$$r_t = \begin{cases} 2 & \text{for } t = 0, \\ -2 & \text{for } t = \frac{N}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\boldsymbol{r} = 2\boldsymbol{s}_{\frac{N}{2}}$.

We get from 2.1 immediately:

2.3. Lemma. *We have for $u, v, w, t, x \in \mathbf{Z}$, $u \not\equiv 0$, $v \not\equiv 0$:*
$c([u, v, w + x], t + x) = c([u, v, w], t)$.

2.4. Proposition. *There exist rational integers $1 \leqq u_i, v_i \leqq N-1$ $(1 \leqq i \leqq \leqq N-1)$ such that for each $0 \leqq \lambda \leqq N-1$ the rows of the matrix $\mathfrak{C}(\lambda)$ with indices $[u_i, v_i]$ $(1 \leqq i \leqq N-1)$ form a maximal linearly independent system of rows of the matrix $\mathfrak{C}(\lambda)$ (over P). The pairs $[u_i, v_i]$ are mutually different.*

Proof. The Proposition follows from 2.2, because according to 2.3 we have

$$c^{(\lambda)}([u, v], t) = c^{(0)}([u, v], \tau)$$

for $1 \leqq u, v \leqq N-1, 0 \leqq \lambda, t, \tau \leqq N-1$ and $\tau \equiv t+\lambda$.

2.5. Notation. Put

$$d = d([u, v, w], [k, t]) = c([u, v, w), t) . g^{(u+v+w-t)k} \in P$$

for $u, v, w, k, t \in \mathbf{Z}, u \not\equiv 0, v \not\equiv 0$.

Further let

$$\mathfrak{D} = (d([u, v, w], [k, t]))(1 \leqq u, v \leqq N-1, 0 \leqq w \leqq N-1, 0 \leqq k, t \leqq N-1)$$

be a matrix of size $N(N-1)^2/N^2$ over P, where the triples $[u, v, w]$ denote row indices and the pairs $[k, t]$ column indices.

Then we have:

2.6. Proposition. *There holds*

a) for $u \not\equiv v, u \not\equiv -v$

$$d = \begin{cases} g^{(u+v)k} & \text{for } t \equiv w, \\ -g^{uk} & \text{for } t \equiv v+w, \\ -g^{vk} & \text{for } t \equiv u+w, \\ 1 & \text{for } t \equiv u+v+w, \\ 0 & \text{otherwise,} \end{cases}$$

b) for $u \equiv -v, u \not\equiv v$

$$d = \begin{cases} 2 & \text{for } t \equiv w, \\ -g^{uk} & \text{for } t \equiv v+w \equiv -u+w, \\ -g^{vk} & \text{for } t \equiv u+w, \\ 0 & \text{otherwise,} \end{cases}$$

c) for $u \equiv v, u \not\equiv -v$

$$d = \begin{cases} g^{2uk} & \text{for } t \equiv w, \\ -2g^{uk} & \text{for } t \equiv w+u, \\ 1 & \text{for } t \equiv w+2u, \\ 0 & \text{otherwise,} \end{cases}$$

d) for N even and $u \equiv v \equiv \frac{N}{2}$

$$d = \begin{cases} 2 & \text{for } t \equiv w, \\ -2g^{\frac{N}{2}k} = (-1)^{k+1}2 & \text{for } t \equiv w+\frac{N}{2} \\ 0 & \text{otherwise.} \end{cases}$$

2.7. Proposition. *The rank of the matrix* $\mathfrak{D}$ *(over P) is equal to* $N(N-1)$.

Proof. According to 2.4 there exist mutually different pairs $[u_i, v_i]$

$(1 \leqq i \leqq N-1,\ 1 \leqq u_i,\ v_i \leqq N-1)$ such that for each $0 \leqq \lambda \leqq N-1$ the rows of the matrix $\mathfrak{C}(\lambda)$ with indices $[u_i, v_i]$ form a maximal linearly independent system of rows of $\mathfrak{C}(\lambda)$.

We show that the rows with indices $[u_i, v_i, s]$ $(1 \leqq i \leqq N-1, 0 \leqq s \leqq N-1)$ of the matrix $\mathfrak{D}$ form a maximal linearly independent system of rows of $\mathfrak{D}$.

a) Let $1 \leqq u,\ v \leqq N-1,\ 0 \leqq w \leqq N-1$ and let $0 \leqq \lambda \leqq N-1,\ \lambda \equiv u + v + w$. There exist $c_i \in P$ $(1 \leqq i \leqq N-1)$ such that

$$c^{(\lambda)}([u, v], t) = \sum_{i=1}^{N-1} c_i c^{(\lambda)}([u_i, v_i], t)$$

for each $0 \leqq t \leqq {}_i$. Let $0 \leqq w_i \leqq N-1,\ w_i \equiv \lambda - (u_i + v_i)$ for each $1 \leqq i \leqq N-1$.

We have for each $0 \leqq k,\ t \leqq N-1$:

$$\sum_{i=1}^{N-1} c_i d(u_i, v_i, w_i], [k, t]) = \sum_{i=1}^{N-1} c_i c([u_i, v_i, \lambda - (u_i + v_i)], t) . g^{(\lambda - t)k} =$$

$$= g^{(\lambda - t)k} \sum_{i=1}^{N-1} c_i c^{(\lambda)}([u_i, v_i], t) =$$

$$= g^{(\lambda - t)k} c^{(\lambda)}([u, v], t) =$$

$$= c([u, v, w], t) g^{(u+v+w-t)} = d([u, v, w], [k, t]) .$$

b) Let $x(i, s) \in P$ for $1 \leqq i \leqq N-1,\ 0 \leqq s \leqq N-1$ such that we have for each $0 \leqq k,\ t \leqq N-1$:

$$\sum_{i=1}^{N-1} \sum_{s=0}^{N-1} x(i, s) d([u_i, v_i, s], [k, t]) = 0 .$$

Put $x(i, \sigma) = x(i, s)$ for $\sigma, s \in \mathbf{Z},\ 0 \leqq s \leqq N-1,\ s \equiv \sigma$. Then

$$\sum_{i=1}^{N-1} \sum_{\lambda=0}^{N-1} x(i, \lambda - (u_i + v_i)) c^{(\lambda)}([u_i, v_i], t) g^{(\lambda - t)k} = 0 .$$

Hence

$$\sum_{\lambda=0}^{N-1} g^{\lambda k} \sum_{i=1}^{N-1} x(i, \lambda - (u_i + v_i)) c^{(\lambda)}([u_i, v_i], t) = 0$$

for each $0 \leqq k,\ t \leqq N-1$. Since $\det(g^{\lambda k})(0 \leqq \lambda,\ k \leqq N-1)$ is the Vandermonde, it differs from 0 and we have

$$\sum_{i=1}^{N-1} x(i, \lambda - (u_i + v_i)) c^{(\lambda)}([u_i, v_i], t) = 0$$

for each $0 \leqq \lambda, t \leqq N-1$. According to 2.4 we have

$x(i, \lambda - (u_i + v_i)) = 0$ for each $1 \leqq i \leqq N-1, 0 \leqq \lambda \leqq N-1$.

2.8. Notation. For $u, v, w, k, t \in \mathbf{Z}$ and $\omega \in \{x, y, z\}$ (x, y, z are any different symbols) we define an element from P:

$$a([u, v, w], [\omega, k, t]) = \begin{cases} 0 & \text{for } \omega = x,\ t \not\equiv u, \\ g^{(v+w)k} & \text{for } \omega = x,\ t \equiv u, \\ 0 & \text{for } \omega = y,\ t \not\equiv v, \\ g^{(u+w)k} & \text{for } \omega = y,\ t \equiv v, \\ 0 & \text{for } \omega = z,\ t \not\equiv w, \\ g^{(u+v)k} & \text{for } \omega = z,\ t \equiv w. \end{cases}$$

Further let

$$\mathfrak{A} = (a([u, v, w], [\omega, k, t])) \ (0 \leqq u, v, w \leqq N-1,\ \omega \in \{x, y, z\},\ 0 \leqq k, t \leqq N-1)$$

be the matrix of size $N^3/3N^2$ over the field P, where $[u, v, w]$ ar indices for rows and $[\omega, k, t]$ are indices for columns.

2.9. Theorem. *The rank of the matrix* $\mathfrak{A}$ *(over* P*) is equal to* $3N^2 - 2N$.

Proof. Let $0 \leqq u, w \leqq N-1$, $1 \leqq v \leqq N-1$, $0 \leqq \alpha \leqq N-1$, $\alpha \equiv w + w$. We subtract from the row of $\mathfrak{A}$ with index $[u, v, w]$ the row with index $[u, 0, \alpha]$. In this matrix we subtract from the row with index $[u, v, w]$ the row with index $[0, v, \beta]$, where $1 \leqq u, v \leqq N-1$, $0 \leqq w \leqq N-1$, $0 \leqq \beta \leqq N-1$ and $\beta \equiv \equiv u + w$.

Then we get the matrix $\mathfrak{B} = (b([u, v, w], [\omega, k, t])$ $(0 \leqq u, v, w \leqq N-1$, $\omega \in \{x, y, z\}$, $0 \leqq k, t \leqq N-1)$. Let $\boldsymbol{T} = [x, k, t]$, $0 \leqq k, t \leqq N-1$ and let $0 \leqq \leqq u, v, w \leqq N-1$. We have

$$b([u, 0, w], \boldsymbol{T}) = a([u, 0, w], \boldsymbol{T}) = \begin{cases} g^{wk} & \text{for } t = u, \\ 0 & \text{for } t \neq u. \end{cases}$$

For $v \neq 0$, $u = 0$ we have

$$b((0, v, w], \boldsymbol{T}) = a([0, v, w], \boldsymbol{T}) - a([0, 0, v + w], \boldsymbol{T}) = 0.$$

For $v \neq 0$, $u \neq 0$ we have

$$b([u, v, w], \boldsymbol{T}) = a([u, v, w], \boldsymbol{T}) - a([u, 0, v + w], \boldsymbol{T}) - - a([0, v, u + w], \boldsymbol{T}) + a([0, 0, u + v + w], \boldsymbol{T}) = 0.$$

Hence we obtain for $0 \leqq u, v, w \leqq N-1$, $0 \leqq k, t \leqq N-1$

$$(*) \qquad b([u, v, w], [x, k, t]) = \begin{cases} g^{wk} & \text{for } t = u,\ v = 0, \\ 0 & \text{otherwise}. \end{cases}$$

Let $\boldsymbol{T} = [y, k, t]$, $0 \leqq k, t \leqq N-1$, $0 \leqq u, v, w \leqq N-1$, $v \neq 0$.Then

$$b([0, v, w], \boldsymbol{T}) = a([0, v, w], \boldsymbol{T}) - a([0, 0, v+w], \boldsymbol{T}) =$$

$$= \begin{cases} -g^{(v+w)k} & \text{for } t = 0, \\ g^{wk} & \text{for } t = v, \\ 0 & \text{otherwise.} \end{cases}$$

For $u \neq 0$ we get

$$b([u, v, w], \boldsymbol{T}) = a([u, v, w], \boldsymbol{T}) - a([u, 0, v+w], \boldsymbol{T}) -$$

$$- a([0, v, u+w], \boldsymbol{T}) + a([0, 0, u+v+w], \boldsymbol{T}) = 0,$$

so for $0 \leqq u, v, w \leqq N-1$, $v \neq 0$ and $0 \leqq k, t \leqq N-1$ there holds

$$(**) \qquad b([u, v, w], [y, k, t]) = \begin{cases} -g^{(v+w)k} & \text{for } u = 0,\ t = 0, \\ g^{wk} & \text{for } u = 0,\ t = v, \\ 0 & \text{otherwise.} \end{cases}$$

For $1 \leqq u, v \leqq N-1$, $0 \leqq w \leqq N-1$, $0 \leqq k, t \leqq N-1$, $\boldsymbol{T} = [z, k, t]$ we get

$$b([u, v, w], \boldsymbol{T}) = a([u, v, w], \boldsymbol{T}) - a([u, 0, v+w], \boldsymbol{T}) -$$

$$- a([0, v, u+w], \boldsymbol{T}) + a([0, 0, u+v+w], \boldsymbol{T}) =$$

$$= \begin{cases} g^{(u+v)k} & \text{for } t = w,\ u \not\equiv -v, \\ g^{(u+v)k} + 1 = 2 & \text{for } t = w,\ u \equiv -v, \\ -g^{uk} & \text{for } t \equiv v + w,\ u \not\equiv v, \\ -g^{uk} - g^{uk} = -2g^{uk} & \text{for } t \equiv v + w,\ u = v, \\ -g^{vk} & \text{for } t \equiv v + w,\ u \neq v, \\ 1 & \text{for } t \equiv u + v + w,\ u \not\equiv -v, \\ 0 & \text{otherwise.} \end{cases}$$

Then we obtain according to 2.6 for $1 \leqq u, v \leqq N-1$, $0 \leqq w \leqq N-1$, $0 \leqq k$, $t \leqq N-1$.

$$(***) \qquad b([u, v, w], [z, k, t]) = d([u, v, w], [k, t]).$$

If we delete from the matrix $\mathfrak{B}$ the rows with indices $[u, 0, w]$ $(0 \leqq u, w \leqq N-1)$ and $[0, v, w]$ $(0 \leqq v, w \leqq N-1, v \neq 0)$ and the columns with indices $[x, k, t]$ and $[y, k, t]$ $(0 \leqq k, t \leqq N-1)$, we get according to $(***)$ the matri $\mathfrak{D}$. If we denote by $r(\mathfrak{A})$, $r(\mathfrak{B})$, $r(\mathfrak{D})$ the ranks of matrices $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{D}$, then we get according to $(*)$, $(**)$ and 2.7 th equality:

$$r(\mathfrak{A}) = r(\mathfrak{B}) = r(\mathfrak{D}) + N^2 + N(N-1) = 3N^2 - 2N.$$

2.10. Remark. a) We can also define the matrix $\mathfrak{A}$ for $N = 1$. Then

$$\mathfrak{A} = (1, 1, 1)$$

and the rank of $\mathfrak{A}$ is 1, so Theorem 2.9 is valid also in the case of $N = 1$.

b) As a colleague of mine Mr. R. Kučera told me, it is aslso possible to use here the following function δ defined for $z \in \mathbf{Z}$:

$$\delta(z) = \begin{cases} 0 & \text{for } z \not\equiv 0 \\ 1 & \text{for } z \equiv 0 . \end{cases}$$

Then for $u, v, w, k, t \in \mathbf{Z}$, and $\omega \in \{x, y, z\}$ we have

$$c = c([u, v, w], t) = \delta(w - t) - \delta(w + v - t) - \delta(w + u - t) + \\ + \delta(w + u + v - t)$$

(for $u \not\equiv 0$, $v \not\equiv 0$) and

$$a([u, v, w], [\omega, k, t]) = \begin{cases} \delta(u - t)\, g^{(v+w)k} & \text{for } \omega = x \\ \delta(v - t)\, g^{(u+w)k} & \text{for } \omega = y \\ \delta(w - t)\, g^{(u+v)k} & \text{for } \omega = z . \end{cases}$$

Thus function δ can be used in 2.2, 2.5 and 2.9.

3. Proof of the Main Theorem

3.1. Definition. Let $\mathbf{X} = (x_{ij})$, $\mathbf{Y} = (y_{ij})$ $(0 \leqq i \leqq K - 1, 0 \leqq j \leqq L - 1)$ be matrices of size K/L over the ring $\mathbf{Z}_p$ of p-adic integers and let m be a positive integer. Put $\mathbf{X} \equiv \mathbf{Y} \pmod{m}$ if $x_{ij} \equiv y_{ij} \pmod{m}$ for each $0 \leqq i \leqq K - 1, 0 \leqq j \leqq L - 1$. In the opposite case $\mathbf{X} \not\equiv \mathbf{Y} \pmod{m}$. If $\mathbf{T} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$, $\mathbf{T}' = (\mathbf{X}', \mathbf{Y}', \mathbf{Z}')$ are triples of matrices over $\mathbf{Z}_p$, put $\mathbf{T} \equiv \mathbf{T}' \pmod{m}$ in the case of $\mathbf{X} \equiv \mathbf{X}' \pmod{m}$, $\mathbf{Y} \equiv \mathbf{Y}' \pmod{m}$, $\mathbf{Z} \equiv \mathbf{Z}' \pmod{m}$. Otherwise put $\mathbf{T} \not\equiv \mathbf{T}' \pmod{m}$.

3.2. Lemma. *Let $\mathbf{T} = (\alpha, \beta, \gamma)$ be a matrix of size $1/3$ ver $\mathbf{Z}_p$ such that $N\alpha\beta\gamma = 1$. Then there exist matrices $\mathbf{T}_1, \mathbf{T}_2, \ldots, \mathbf{T}_{p^2}$ of size $1/3$ over $\mathbf{Z}_p$ with the following properties:*

1° $\mathbf{T}_i \equiv \mathbf{T} \pmod{p^n}$ *for each* $1 \leqq i \leqq p^2$,

2° $\mathbf{T}_i \not\equiv \mathbf{T}_j \pmod{p^{n+1}}$ *for each* $1 \leqq i, j \leqq p^2$, $i \neq j$,

3° *if* $\mathbf{T}' = (\alpha', \beta', \gamma')$ *is a matrix of size* $1/3$ *over* $\mathbf{Z}_p$ *such that* $N\alpha'\beta'\gamma' = 1$ *and* $\mathbf{T}' \equiv \mathbf{T} \pmod{p^n}$, *then there exists* $1 \leqq i \leqq p^2$ *such that* $\mathbf{T}' \equiv \mathbf{T}_i \pmod{p^{n+1}}$,

4° *for* $1 \leqq i \leqq p^2$, $\mathbf{T}_i = (\alpha_i, \beta_i, \gamma_i)$ *we have* $N\alpha_i\beta_i\gamma_i) = 1$.

Proof. For the integers $0 \leqq x, y \leqq p - 1$ put $\bar{\alpha} = \alpha + xp^n$, $\bar{\beta} = \beta + yp^n$. Since $N\alpha\beta\gamma = 1$ and $\bar{\alpha}$, $\bar{\beta}$ are units in $\mathbf{Z}_p$, there exists $z \in \mathbf{Z}_p$ such that $1 - N\bar{\alpha}\bar{\beta}\gamma = Nzp^n\bar{\alpha}\bar{\beta}$. Put $\bar{\gamma} = \gamma + zp^n$. Then $N\bar{\alpha}\bar{\beta}\bar{\gamma} = 1$. The matrix $(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ is denoted by $\mathbf{T}(x, y)$. The number of these matrices is equal to p^2 and obviously they have properties 1°, 2° and 4°.

Let $\mathbf{T}' = (\alpha', \beta', \gamma')$ be a matrix of size 1/3 over $\mathbf{Z}_p$ such that $N\alpha'\beta'\gamma' = 1$ and $\mathbf{T}' \equiv \mathbf{T}(\operatorname{mod} p^n)$. Then there exist $\xi, \eta, \zeta \in \mathbf{Z}_p$ such that $\alpha' = \alpha + \xi p^n$, $\beta' = B + \eta np^n$, $\gamma' = \gamma + \zeta p^n$. Let $x, y \in \mathbf{Z}$, $0 \leqq x, y \leqq p-1$ with the property $x \equiv \xi(\operatorname{mod} p)$ and $y \equiv \eta(\operatorname{mod} p)$. We have for the matrix $\mathbf{T}(x, y) = (\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ obviously $\bar{\alpha} \equiv \alpha'(\operatorname{mod} p^{n+1})$ and $\bar{\beta} \equiv \beta'(\operatorname{mod} p^{n+1})$. Hence $N\bar{\alpha}\bar{\beta}\gamma' \equiv 1$ $(\operatorname{mod} p^{n+1})$ and $N\gamma' \equiv \bar{\alpha}^{-1} . \bar{\beta}^{-1} = N\bar{\gamma}(\operatorname{mod} p^{n+1})$, thus $\bar{\gamma} \equiv \gamma'(\operatorname{mod} p^{n+1})$. It follows immediately $\mathbf{T}(x,y) \equiv \mathbf{T}'(\operatorname{mod} p^{n+1})$. The Lemma is proved.

3.3. Proposition. *Let $\mathbf{T}$ be a triple of SCC-matrices of order N over $\mathbf{Z}_p$. Then there exist p^{2N} triples $\{\mathbf{T}_i : 1 \leqq i \leqq p^{2N}\}$ of SCC-matrices of order N over $\mathbf{Z}_p$ with the following properties*:

1° $\mathbf{T}_i \equiv \mathbf{T}(\operatorname{mod} p^n)$ *for each* $1 \leqq i \leqq p^{2N}$,

2° $\mathbf{T}_i \not\equiv \mathbf{T}_j(\operatorname{mod} p^{n+1})$ *for each* $1 \leqq i, j \leqq p^{2N}$, $i \neq j$,

3° *if* $\mathbf{T}'$ *is a triple of SCC-matrices of order N over $\mathbf{Z}_p$ such that* $\mathbf{T}' \equiv \mathbf{T}(\operatorname{mod} p^n)$, *then there exists* $1 \leqq i \leqq p^{2N}$ *with the property* $\mathbf{T}' \equiv \mathbf{T}_i$ $(\operatorname{mod} p^{n+1})$.

Proof. Suppose $\mathbf{T} = (\mathbf{A}, \mathbf{B}, \mathbf{C})$, $\mathbf{A} = (a_{kh})$, $\mathbf{B} = (b_{kh})$, $\mathbf{C} = (c_{kh})$ $(0 \leqq k, h \leqq N-1)$ is a triple of *SCC*-matrices of order N over $\mathbf{Z}_p$. According to 1.2 (for integral domain $\mathbf{Z}_p$) there exist $\alpha_k, \beta_k, \gamma_k, \varrho_k \in \mathbf{Z}_p$ for each $0 \leqq k \leqq N-1$ such that $N\alpha_k\beta_k\gamma_k = 1$, $\{\varrho_0, \varrho_1, \ldots, \varrho_{N-1}\}$ is the N-element set of all the Nth roots of unity in $\mathbf{Z}_p$ and

$$a_{kh} = \varrho_k^h\alpha_k\,, \; b_{kh} = \varrho_k^h\beta_k\,, \; c_{kh} = \varrho_k^h\gamma_k$$

$(0 \leqq k, h \leqq N-1)$. For $0 \leqq k \leqq N-1$ and the matrix $\mathbf{T}^{(k)} = (\alpha_k, \beta_k, \gamma_k)$ let $\mathbf{T}_i^{(k)} = (\alpha_{ki}, \beta_{ki}, \gamma_{ki})$ be matrices of size 1/3 over $\mathbf{Z}_p$ $(1 \leqq i \leqq p^2)$ with the properties from 3.2. For a mapping ϕ from the set $\{0, 1, \ldots, N-1\}$ into the set $\{1, 2, \ldots, p^2\}$ put

$$\mathbf{A}_\phi = (\varrho_k^h\alpha_{k\phi(k)})\,, \; \mathbf{B}_\phi = (\varrho_k^h\beta_{k\phi(k)})\,, \; \mathbf{C}_\phi = (\varrho_k^h\gamma_{k\phi(k)}) \qquad (0 \leqq k, h \leqq N-1)\,.$$

According to 1.2 the triple $\mathbf{T}_\phi = (\mathbf{A}_\phi, \mathbf{B}_\phi, \mathbf{C}_\phi)$ forms *SCC*-matrices of order N over $\mathbf{Z}_p$. Clearly, $\mathbf{T}_\phi \equiv \mathbf{T}(\operatorname{mod} p^n)$.

Let ϕ, ψ be different mappings from $\{0, 1, \ldots, N-1\}$ into $\{1, 2, \ldots, p^2\}$. Then there exists $0 \leqq k \leqq N-1$ such that $\phi(k) \neq \psi(k)$. Hence $\mathbf{T}_{\phi(k)}^{(k)} \not\equiv \mathbf{T}_{\phi(k)}^{(k)}$ $(\operatorname{mod} p^{n+1})$, which follows $\mathbf{T}_\phi \not\equiv \mathbf{T}_\psi(\operatorname{mod} p^{n+1})$.

Let $\mathbf{T}' = (\mathbf{A}', \mathbf{B}', \mathbf{C}')$ be a triple of *SCC*-matrices of order N over $\mathbf{Z}_p$ with the property $\mathbf{T}' \equiv \mathbf{T}(\operatorname{mod} p^n)$. According to 1.2 we have $\mathbf{A}' = (a'_{kh})$, $\mathbf{B}' = (b'_{kh})$, $\mathbf{C}' = (c'_{kh})$ and

$$a'_{kh} = \sigma_k^h\alpha'_k,\; b'_{kh} = \sigma_k^h\beta'_k,\; c'_{kh} = \sigma_k^h\gamma'_h \qquad (0 \leqq k, h \leqq N-1)\,,$$

where $\{\sigma_0, \sigma_1, \ldots, \sigma_{N-1}\} = \{\varrho_0, \varrho_1, \ldots, \varrho_{N-1}\}$, $\alpha'_k, \beta'_k, \gamma'_k \in \mathbf{Z}_p$ and $N\alpha'_k\beta'_k\gamma'_k = 1$ for each $0 \leqq k \leqq N-1$. Further

$$a'_{kh} \equiv a_{kh} (\bmod p^n), \; b'_{kh} \equiv b_{kh} (\bmod p^n), \; c'_{kh} \equiv c_{kh} (\bmod p^n)$$

$(0 \leqq k, h \leqq N-1)$. For $h = 0$ we obtain $(\alpha'_k, \beta'_k, \gamma'_k) \equiv (\alpha_k, \beta_k, \gamma_k) \; (\bmod p^n)$. Hence there exists a mapping ϕ from $\{0, 1, \ldots, N-1\}$ into $(1, 2, \ldots, p^2\}$ such that $(\alpha'_k, \beta'_k, \gamma'_k) \equiv (\alpha_{k\phi(k)}, \beta_{k\phi(k)}, \gamma_{k\phi(k)}) \; (\bmod p^{n+1})$.

For $h = 1$ we get $\sigma_k \equiv \varrho_k \; (\bmod p^n)$, hence $\sigma_k = \varrho_k$ for each $0 \leqq k \leqq N-1$. It follows that $\mathbf{T}' \equiv \mathbf{T}_\phi \; (\bmod p^{n+1})$ and the Proposition is proved.

3.4. Notation. Let $\mathbf{T} = (\mathbf{A}, \mathbf{B}, \mathbf{C})$, $\mathbf{T}' = (\mathbf{A}', \mathbf{B}', \mathbf{C}')$ be triples of square matrices of order N over $\mathbf{Z}_p$, $\mathbf{A} = (a_{kt})$, $\mathbf{B} = (b_{kt})$, $\mathbf{C} = (c_{kt})$, $\mathbf{A}' = (a'_{kt})$, $\mathbf{B}' = (b'_{kt})$, $\mathbf{C}' = (c'_{kt})$ $(0 \leqq k, t \leqq N-1)$. If $\mathbf{T}' \equiv \mathbf{T} \; (\bmod p^n)$, then there exists $x_{kt}, y_{kt}, z_{kt} \in \mathbf{Z}_p$ such that

$$a'_{kt} = a_{kt} + x_{kt} p^n,$$
$$b'_{kt} = b_{kt} + y_{kt} p^n$$
$$c'_{kt} = c_{kt} + z_{kt} p^n$$

$0 \leqq k, t \leqq N-1)$. Put

$$\sigma(\mathbf{T}, \mathbf{T}') = (x_{00}, x_{01}, \ldots, x_{0N-1}, \ldots, x_{N-1N-1}, y_{00}, \ldots, z_{N-1N-1}).$$

Then $\sigma(\mathbf{T}, \mathbf{T}')$ is a matrix of size $1/3N^2$ (a vector of dimension $3N^2$ over $\mathbf{Z}_p$. Further we shall consider the following system $\mathscr{S}(\mathbf{T})$ of N^3 linear congruences $\bmod p$ with $3N^2$ unknowns X_{kt}, Y_{kt}, Z_{kt} $(0 \leqq k, t \leqq N-1)$.

$$\mathscr{S}(\mathbf{T}): \sum_{k=0}^{N-1} (X_{ku} b_{kv} c_{kw} + Y_{kv} a_{ku} c_{kw} + Z_{kw} a_{ku} b_{kv}) \equiv 0 \; (\bmod p)$$

$$(0 \leqq u, v, w \leqq N-1).$$

3.5. Proposition. *Let* $\mathbf{T}$ *be a triple of SCC-matrices of order N over* $\mathbf{Z}_p$. *Then the rank of the matrix of the system* $\mathscr{S}(\mathbf{T})$ $(\bmod p)$ *equals* $3N^2 - 2N$, *so the number of solutions* $(\bmod p)$ *of the system* $\mathscr{S}(\mathbf{T}) \bmod p)$ *is* p^{2N}.

Proof. The Proposition follows immediately from the form of the p-adic integers a_{kt}, b_{kt}, c_{kt} defined by 1.2 and from Theorem 2.9.

3.6. Definition. A triple $\mathbf{T}' = (\mathbf{A}', \mathbf{B}', \mathbf{C}')$ of square matrices of order N over $\mathbf{Z}_p$ is said to be a *triple of SCC-matrices* $\bmod p^{n+1}$ if $\phi_{n+1}(\mathbf{A}')$, $\phi_{n+1}(\mathbf{B}')$, $\phi_{n+1}(\mathbf{C}')$ are *SCC*-matrices over the ring $\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p$.

3.7. Proposition. *Let* $\mathbf{T}, \mathbf{T}'$ *be triples of square matrices or order N over* $\mathbf{Z}_p$, $\mathbf{T}$ *be a triple of SCC-matrices (in* $\mathbf{Z}_p$*) and* $\mathbf{T} \equiv \mathbf{T}'$ $(\bmod p^n)$. *Then* $\mathbf{T}'$ *is a triple of SCC-matrices* $\bmod p^{n+1}$ *if and only if the vector* $\sigma(\mathbf{T}, \mathbf{T}')$ *is a solution of the system* $\mathscr{S}(\mathbf{T})$.

Proof. Let $\mathbf{A} = (a_{kt})$, $\mathbf{B} = (b_{kt})$, $\mathbf{C} = (c_{kt})$, $\mathbf{A}' = (a'_{kt})$, $\mathbf{B}' = (b'_{kt})$, $\mathbf{C}' = (c'_{kt})$,

$$a'_{kt} = a_{kt} + x_{kt} p^n,$$

$$b'_{kt} = b_{kt} + y_{kt}p^n,$$

$$c'_{kt} = c_{kt} + z_{kt}p^n,$$

$x_{kt}, y_{kt}, z_{kt} \in \mathbf{Z}_p$ and $0 \leqq k,\ t \leqq N-1$. Then for $0 \leqq u,\ v,\ w \leqq N-1$ we have

$$\sum_{k=0}^{N-1} a'_{ku} b'_{kv} c'_{kw} \equiv \sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} +$$

$$+ p^n \left[\sum_{k=0}^{N-1} (x_{ku} b_{kv} c_{kw} + y_{kv} a_{ku} c_{kw} + z_{kw} a_{ku} b_{kv}) \right] (\operatorname{mod} p^{n+1}).$$

The result follows.

Similarly we can prove:

3.8. Proposition. *Let* $\mathbf{T}, \mathbf{T}', \mathbf{T}''$ *be tripes of square matrices of order* N *over* $\mathbf{Z}_p$ *and let* $\mathbf{T}' \equiv \mathbf{T}\ (\operatorname{mod} p_n)$, $\mathbf{T}'' \equiv \mathbf{T}\ (\operatorname{mod} p_n)$. *Then* $\mathbf{T}' \equiv \mathbf{T}''\ (\operatorname{mod} p^{n+1})$ *if and only if* $\sigma(\mathbf{T}, \mathbf{T}') \equiv \sigma(\mathbf{T}, \mathbf{T}'')\ (\operatorname{mod} p)$.

3.9. Remark. We obtain from 3.3, 3.7 and 3.8 that the system $\mathscr{S}(\mathbf{T})$ for each triple $\mathbf{T}$ of *SCC*-matrices of order N over $\mathbf{Z}_p$ has at least p^{2N} solutions. Then the following inequality holds for the rank r of the matrix of $\mathscr{S}(\mathbf{T})$: $r \leqq 3N^2 - 2N$. But for the rank $\mathrm{r}(\mathfrak{A})$, $\mathrm{r}(\mathfrak{D})$ of the matrices $\mathfrak{A}$, $\mathfrak{D}$ defined in Paragrph 2 there holds $r = \mathrm{r}(\mathfrak{A}) = \mathrm{r}(\mathfrak{D}) + N^2 + N(N-1)$ (s. proof of 2.9), hence $\mathrm{r}(\mathfrak{D}) \leqq N^2 - - N$. It means it is enough to prove only the inequality $N^2 - N \leqq \mathrm{r}(\mathfrak{D})$ in 2.7.

3.10. Theorem. *Let* $\mathbf{T}, \mathbf{T}'$ *be triples of square matrices of order* N *over* $\mathbf{Z}_p$, $\mathbf{T}$ *be a triple of SCC-matrices (in* $\mathbf{Z}_p$*) and* $\mathbf{T}' \equiv \mathbf{T}\ (\operatorname{mod} p^n)$. *If* $\mathbf{T}'$ *is a triple of SCC-matrices* $\operatorname{mod} p^{n+1}$, *then there exists a triple* $\mathbf{T}^*$ *of SCC-matrices of order* N *over* $\mathbf{Z}_p$ *such that*

$$\mathbf{T}' \equiv \mathbf{T}^*\ (\operatorname{mod} p^{n+1}).$$

Proof. We obtain the Theorem directly from 3.3, 3.5, 3.7 and 3.8.

3.11. Proof of Main Theorem 1.5.

We shall prove this Theorem by mathematical induction with regard to n.

I. Suppose $n = 1$ and let $\mathscr{A} = (A_{kt})$, $\mathscr{B} = (B_{kt})$, $\mathscr{C} = (C_{kt})$ $(0 \leqq k,\ t \leqq N-1)$ be *SCC*-matrices over the ring $P = \mathbf{Z}/p\mathbf{Z}$. According to 1.2 there exist a_k, b_k, c_k, $g_k \in \mathbf{Z}$ such that $g_k^N \equiv 1\ (\operatorname{mod} p)$, $Na_k b_k c_k \equiv 1\ (\operatorname{mod} p)$ $(0 \leqq k \leqq N-1)$, the rational integers $g_0, g_1, \ldots, g_{N-1}$ are incongruent $\operatorname{mod} p$ and $g_a^t a_k \in A_{kt}$, $g_k^t b_k \in B_{kt}$, $g_k^t c_k \in C_{kt}$ for each $0 \leqq k,\ t \leqq N-1$.

There exist p-adic integers $\varrho_0, \varrho_1, \ldots, \varrho_{N-1}$ such that $\varrho_k^N = 1$ and $\varrho_k \equiv g_k\ (\operatorname{mod} p)$. Then $\{\varrho_0, \varrho_1, \ldots, \varrho_{N-1}\}$ is the set of all the Nth roots of unity in $\mathbf{Z}_p$. Put $\alpha_k = a_k$, $\beta_k = b_k$ for $0 \leqq k \leqq N-1$. Since α_k, β_k, N are units in $\mathbf{Z}_p$, there exist $\gamma_k \in \mathbf{Z}_p$ such that $N\alpha_k\beta_k\gamma_k = 1$. Then $\gamma_k \equiv c_k \pmod p$ and the matrices $\mathbf{A} = (\varrho_k^t \alpha_k)$, $\mathbf{B} = (\varrho_k^t \beta_k)$, $\mathbf{C} = (\varrho_k^t \gamma_k)$ $(0 \leqq k,\ t \leqq N-1)$ have the requiered properties according to 1.2.

II. Let the Main Theorem hold for $n \geqq 1$. Let $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ be SCC-matrices of order N over the ring $\mathbf{Z}/p^{n+1}\mathbf{Z} = \mathbf{Z}_p/p^{n+1}\mathbf{Z}_p$ (canonically). There exist matrices $\mathbf{A}'$, $\mathbf{B}'$, $\mathbf{C}'$ over the ring $\mathbf{Z}_p$ such that $\phi_{n+1}(\mathbf{A}') = \mathscr{A}$, $\phi_{n+1}(\mathbf{B}') = \mathscr{B}$, $\phi_{n+1}(\mathbf{C}') = \mathscr{C}$. The triple $\mathbf{T}' = (\mathbf{A}', \mathbf{B}', \mathbf{C}')$ is a triple of SCC-matrices $\bmod p^{n+1}$.

By the induction assumption there exists a triple $\mathbf{T}$ of SCC-matrices over the ring $\mathbf{Z}_p$ such that $\mathbf{T} \equiv \mathbf{T}' \pmod{p^n}$. According to Theorem 3.10 there exists a triple $\mathbf{T}^*$ of SCC-matrices of order N over $\mathbf{Z}_p$ such that $\mathbf{T}' \equiv \mathbf{T}^* \pmod{p^{n+1}}$.

The Main Theorem is proved.

REFERENCES

[1] AGARWAL, R. C.—BURRUS, CH. S.: Fast convolution using Fermat number transform with applications to digital filtering. IEEE Transaction on Acoustics, Speech, and Signal Processing, vol. ASSP-22, no. 2, April 1974, 87—97.

[2] BOREVICH, Z. I.—SHAFAREVICH, I. R.: Number Theory. Transl. by N. Greenleaf, New York. Academic Press, 1966.

[3] KOCH, H.—PIEPER, H.: Zahlentheorie. VEB Deutscher Verlag der Wissenschaften, Berlin 1976 (German)

[4] SKULA, L.: Linear transforms and convolution. Math. Slovaca, 37, 1987, No. 1, 9—30.

Received Juni 3, 1987

Katedra matematiky PF UJEP
Janáčkovo nám. 2a
662 95 Brno

ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ СО СВОЙСТВОМ КОНВОПЮЦИИ

В КОЛЬЦЕ КЛАССОВ ВЫЧЕТОВ

Ladislav Skula

Резюме

Описаны все линейные преобразования со свойством конволюции в кольце класов вычетов $\mathbf{Z}/p^n\mathbf{Z}$, где p — простое и n — целое положительные числа. Задача сводится к отысканию всех линейных преобразований со свойством конволюции в кольце целых p-адических чисел. Матрицы соответствующих друг другу линейных преобразований «конгруентны» по $\bmod p^n$.