LINEAR RECURSION CONGRUENCES
WITH PERIODIC COEFFICIENTS

V. I. Nechaev

The paper deals with the problem of the primitive period of a sequence satisfying a linear recursion congruence, modulo a power of a prime, with periodic coefficients.

1. Let $k$, $n$, and $m$ be natural numbers, $p$ a prime, and $x$ an integer. In this paper we shall consider a recursion congruence of the form

$$
\delta_{x+n} \equiv a_{nx}\delta_{x+n-1} + \cdots + a_{1x}\delta_{x} \pmod{p^k},
$$

whose coefficients are integer-valued functions of $x$ with period $m$ modulo $p^k$, i.e.,

$$
a_{i, x+m} \equiv a_{i, x} \pmod{p^k}, \quad i = 1, \ldots, n,
$$

for all $x \geq 0$, and which, moreover, satisfy for all $x$ the condition

$$(a_{1x}, p) = 1.$$  

We call such a congruence a recursion congruence of type $(n, m)$ modulo $p^k$, while the sequence of integers

$$
\{\delta_x\}_{x \geq 0},
$$

satisfying Congruence (1) is called its solution.

For given $p$ and $k$, with certain constraints on $m$, we shall establish an unimprovable bound on the primitive period modulo $p^k$ of the solution to congruence (1). The transition to an arbitrary modulus can be easily performed ([1], Theorem 4). It is also possible to carry the results over to any Dedekind ring, $R$, on the condition that the factor ring $R/\mathfrak{m}$ with respect to each proper ideal $\mathfrak{m}$ of ring $R$ is finite. The result corresponding to $k = 1$ was elucidated previously [2].

2. In what follows we shall use the term "complex" to denote an ordered collection, while the term "vector" is to be understood as an $n$-dimensional integer-valued column or row vector if nothing to the contrary is said. The symbol $\theta$ denote the $n$-dimensional zero vector. If $a_1, \ldots, a_S$ are vectors, then the symbol $[a_1, \ldots, a_S]$ denotes the matrix whose columns are, respectively, the vectors $a_1, \ldots, a_S$. The elements of the matrices considered here, as well as the coefficients of the polynomials, are assumed to be integers. All the square matrices are of the same order, i.e., $n$. The letter $E$ denotes the unit matrix. By the $C$-matrix of vector $(a_1, \ldots, a_n)$ we understand the square matrix

$$
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
a_1 & a_2 & a_3 & \cdots & a_n
\end{pmatrix}
$$

We assume that the reader knows the definitions and simplest properties of congruences for matrices and vectors. A vector is said to be regular if not all its components are multiples of $p$. A square matrix is called regular if its determinant is not divisible by $p$.

Let 

\[ \{\alpha_1, \ldots, \alpha_s\} \]  \hspace{1cm} (1) 

be some complex of vectors; we shall say that the rank modulo \( p^k \) of complex (1) equals \( r \) \((r \leq s)\) if no vector of any subsystem of \( r \) sequences of vectors of complex (1) is a linear combination (with integer coefficients) modulo \( p^k \) of the remaining vectors of this subsystem. It is clear that the rank modulo \( p^k \) of complex (1) equals \( n \) if and only if, for each \( x \) from 1 to \( s-n+1 \), matrix \([\alpha_1, \ldots, \alpha_{x+n-1}]\) is regular.

The complexes of vectors, \( \{\beta_1, \ldots, \beta_s\} \) and \( \{\gamma_1, \ldots, \gamma_s\} \) will be called equivalent modulo \( p^k \) if

\[ [\alpha_1, \ldots, \alpha_s] \equiv [\beta_1, \ldots, \beta_s] \pmod{p^k}. \]

It is clear that the ranks modulo \( p^k \) of complexes of vectors which are equivalent modulo \( p^k \) are equal.

**Lemma 1.** Let \( \gamma \) be some vector, \( \{\alpha_1, \ldots, \alpha_s\} \) and \( \{\beta_1, \ldots, \beta_t\} \) two complexes of vectors of the same rank, \( n \), modulo \( p^k \). If \( p^k > n \), it is then possible to choose a vector \( \mu \equiv \gamma \pmod{p^k} \) with the condition that the rank of the complex \( \{\alpha_1, \ldots, \alpha_s, \mu, \beta_1, \ldots, \beta_t\} \) modulo \( p^k \) equals \( \min (r+1, n) \).

**Proof.** The set of linear combinations of all subsystems of \( n-1 \) sequences of vectors of the complex \( \{\alpha_s-n+2, \ldots, \alpha_s, \beta_1, \ldots, \beta_{n-1}\} \) contains no more than

\[ n \left( p^{k(n-1)} - 1 \right) + 1 \leq p^n - 2 \]

vectors which are pairwise incongruent modulo \( p^k \). Therefore, we can find a vector \( \mu \) incongruent modulo \( p^k \) to \( \gamma \) and to any such linear combinations. This also proves the lemma.

If \( A \) is a regular matrix, then some of its powers are congruent to \( E \) modulo \( p^k \) (cf., for example, [3], p. 904). The smallest natural \( t \) satisfying \( A^t \equiv E \pmod{p^k} \) is called the period modulo \( p^k \) of matrix \( A \).

**Lemma 2.** Let \( A \equiv E \pmod{p} \), and let \( \beta \) be the largest integer satisfying \( A^\beta \equiv E \pmod{p^\beta} \). If \( p \neq 2 \), or if \( p = 2 \) and \( \beta = 1 \), then the period of matrix \( A \) modulo \( p^k \) equals \( p^k - \beta \).

As a further part of this lemma, let \( \delta \) be the largest integer satisfying \( A^\delta \equiv E \pmod{2^\delta} \), and let \( B \) be the matrix defined by the equation \( A = E + 2B \). If \( p = 2 \) and \( \beta = 1 \), then the period of matrix \( A \) modulo \( 2^k \) equals \( 2^k - 1 \), depending on whether or not \( B = -E \pmod{2^{k-2}} \).

This lemma unifies Theorems 5.3, 6.1, and 6.2 of [3]. From Lemma 2 we immediately obtain

**Lemma 3.** If the period of matrix \( A \) modulo \( p \) equals \( t \), then the period of the same matrix modulo \( p^k \) does not exceed \( t \cdot p^{k-1} \). In particular, this period equals \( t \cdot p^{k-1} \) if

\[ A^t \equiv E \pmod{p^t} \quad \text{for} \quad p \neq 2 \]

or

\[ A^t \equiv \pm E \pmod{p^4} \quad \text{for} \quad p = 2 \]  \hspace{1cm} (2)

**Lemma 4.** If the characteristic polynomial, \( \phi_A (\lambda) \), of matrix \( A \) of period \( t \) modulo \( p^k \) is irreducible modulo \( p \), and if \( \alpha \) is a regular vector, it then follows from the congruence

\[ A^x \alpha \equiv \alpha \pmod{p^k} \]

that \( t \mid n \).

**Proof.** It obviously suffices for us to show that

\[ A^x \equiv E \pmod{p^k}. \]

We obtain this last congruence if we establish that (3) holds for any regular vector. For this we shall show that a consequence of (3) is the existence of a pair of polynomials, \( u(\lambda) \) and \( v(\lambda) \), such that

\[ \lambda^x = 1 + u(\lambda) \varphi_A (\lambda) + p^x v(\lambda). \]  \hspace{1cm} (4)