V. I. Nechaev

1963

Abstract

Full Text

V. I. Nechaev

THE GROUP OF NONSINGULAR MATRICES OVER A FINITE FIELD AND RECURRENT SEQUENCES

(Presented by Academician I. M. Vinogradov on 5 IV 1963)

Let p be prime; let k, n, and q be natural numbers; let K be a field of algebraic numbers of finite degree over the field of rational numbers; let ρ be a prime ideal of the field K; let $a_1(x), \dots, a_n(x)$ be functions periodic modulo ρ, taking, for all natural values of the argument x, integral values of the field K, and let q be the least natural number with the condition that, for all natural x, the congruences

$$a_i(x+q) \equiv a_i(x) \pmod{\rho}, \qquad i = 1, \dots, n.$$

hold.

By a **recurrent function over the field K modulo ρ of order n** we shall mean a recurrent function $\psi(x)$, defined for natural values of the argument x, of the form

$$\psi(x) = a_1(x)\psi(x-n) + \cdots + a_n(x)\psi(x-1), \tag{1}$$

if:

A. $a_1(x) \not\equiv 0 \pmod{\rho}$ for all natural x.

B. The initial values $\psi(1), \dots, \psi(n)$ of the function $\psi(x)$ are algebraic integers of the field K, not all divisible by ρ.

For $q = 1$ the function $\psi(x)$ will be called a **recurrent function with constant coefficients**.

For each natural x, denote by δ_x the residue class modulo ρ of the algebraic integers of the field K with representative $\psi(x)$. Then the sequence

$$\delta_1, \delta_2, \dots, \delta_x, \dots \tag{2}$$

will be called a **recurrent sequence over the field K modulo ρ of order n**.

The class of recurrent functions with constant coefficients over the field of rational numbers, of order n, modulo a prime p, was considered earlier. It is easy to show that the sequence (2) for any function of this class is periodic and that its period is $\leqslant p^n - 1$. D. H. Lehmer [1] showed that in the indicated class there exists a function with maximal period $\tau = p^n - 1$. In the present note the analogous assertion is proved for recurrent functions with nonconstant coefficients over an arbitrary field of algebraic numbers. V. I. Nechaev and L. L. Stepanova considered recurrent functions with constant coefficients over an arbitrary field K. The idea of considering recurrent functions over the field of rational numbers with polynomial coefficients belongs to A. M. Polosuev. A. O. Gelfond proposed considering recurrent functions with arbitrary periodic coefficients.

Let, further, $P = GF(p^k)$ be the finite field of p^k elements; $V_n(P)$ the n-dimensional vector space over the field P; G the group of nonsingular matrices of order n over the field P.

Lemma 1. The group G is finite and its order is

$$\prod_{i=0}^{n-1} (p^{kn} - p^{ki}) .$$

Lemma 2. If the characteristic polynomial $\varphi(x)$ of a matrix B of the group G is irreducible over the field P, then the order of the matrix B (in the group-theoretic–

(in the above sense) is equal to the order of the multiplicative group generated by the roots of the polynomial $\varphi(x)$.

Lemma 3. The order of any element of the group G does not exceed $p^{kn} - 1$.

Lemma 4. Let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$ be two systems of vectors of the space $V_n(P)$, linearly independent over the field P, and let $p^k > n$. Then for any natural number s and any set of elements $c_1, \dots, c_s$ of the field P, one can find in the space $V_n(P)$ such vectors $\gamma_1, \dots, \gamma_s$ that:

a) for each i $(i = 1, \dots, s)$ the last coordinate of the vector γ is different from c_i;

b) any n adjacent vectors of the sequence

$$\alpha_1, \dots, \alpha_n, \gamma_1, \dots, \gamma_s, \beta_1, \dots, \beta_n$$

are linearly independent over the field P.

Let $N(\rho)$ be the norm of the ideal ρ, equal to p^k. It is known that the residue-class ring of the integers of the field K modulo ρ is a finite field of order p^k, and since all finite fields of the same order are isomorphic, this field may be identified with the field P.

Let Δ_x be the n-dimensional vector of the space $V_n(P)$ of the form

$$\Delta_x = (\delta_x, \delta_{x+1}, \dots, \delta_{x+n-1}).$$

Consider the sequence

$$\Delta_1, \Delta_2, \dots, \Delta_x, \dots \tag{3}$$

It is easy to see that if $x-y \pmod q$ and $\Delta_x = \Delta_y$, then $\Delta_{x+1} = \Delta_{y+1}$. Further, if $x \equiv y \pmod q$, then $a_i(x) \equiv a_i(y) \pmod \rho$. Therefore the vector-function $(a_1(x), \dots, a_n(x))$ can be specified by a rectangular matrix A of the form

$$A = \begin{pmatrix} a_{10}a_{20} \dots \dots a_{n0} \\ a_{11}a_{21} \dots \dots a_{n1} \\ \dots\dots\dots\dots\dots \\ a_{1,q-1}a_{2,q-1} \dots a_{n,q-1} \end{pmatrix},$$

whose element a_{ir} $(1 \le i \le n,\ 0 \le r \le q-1)$ is the homomorphic image of the element $a_i(qx+r)$ under the homomorphic mapping of the field K onto the field P.

Consider the matrices

$$A_r = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ a_{1r} & a_{2r} & a_{3r} & \dots & a_{nr} \end{pmatrix}, \quad r = 0, 1, \dots, q-1. \tag{4}$$

We put

$$B_0 = A_{q-1} \dots A_1 A_0, \quad B_1 = A_0 B_0 A_0^{-1}, \dots, \quad B_{q-1} = A_{q-2} B_{q-2} A_{q-2}^{-1}.$$

The matrices $B_0, B_1, \dots, B_{q-1}$ are nonsingular, similar, of the same order, and have one and the same characteristic polynomial $\varphi(x)$. We shall call this polynomial the **characteristic polynomial of the recurrent function** $\psi(x)$. For every natural x we have

$$\delta_{qx-n+1} = \delta_{qx-n+1},$$
$$\dots\dots\dots\dots\dots\dots\dots$$
$$\delta_{qx-1} = \delta_{qx-1},$$
$$\delta_{qx} = a_{10}\delta_{qx-n} + \dots + a_{n0}\delta_{qx-1}.$$

Hence we find

$$\Delta_{qx-n+1} = A_0 \Delta_{qx-n}.$$

In this equality the matrix A_0 plays the role of a linear operator applied to the vector Δ_{qx-n}. Continuing this reasoning, we obtain

$$\Delta_{q(x+1)-n} = B_0 \Delta_{qx-n}.$$

Therefore, for any integer t we have

$$\Delta_{q(x+t)-n} = B_0^t \Delta_{qx-n}.$$

If t is the order of the matrix B_0, then

$$\Delta_{q(x+t)-n} = \Delta_{qx-n}.$$

Thus the sequence (3), and hence also (2), is periodic, and its period (the least one), being a divisor of the number qt, by Lemma 3 does not exceed

$$q(p^{kn} - 1).$$

Choosing as the initial values of the function $\psi(x)$ different sets of integers of the field K, we shall obtain various recurrent functions satisfying equation (1). All such functions we shall call **solutions of equation (1)**. It is easy to see that there exists only a finite set of solutions $\psi^{(1)}(x), \dots, \psi^{(s)}(x)$ of equation (1) with the condition that the periods of the recurrent sequences corresponding to these solutions cannot be obtained from one another by a cyclic permutation of the symbols $\delta_x^{(i)}$. By τ_i we shall denote the length of the period of the recurrent sequence (2) corresponding to the function $\psi^{(i)}(x)$.

We shall assume that the characteristic polynomial $\varphi(x)$ of the function $\psi(x)$ is irreducible over the field P. Denote by t the order of the multiplicative group generated by the roots of the polynomial $\varphi(x)$, and by τ the period (i.e. the length of the period) of the sequence (2) corresponding to some solution $\psi(x)$ of equation (1). By Lemma 2, qt is divisible by τ. But since

$$\Delta_{q(x+\tau)-n} = B_0^\tau \Delta_{qx-n} \quad \text{and} \quad \Delta_{q(x+\tau)-n} = \Delta_{qx-n},$$

it follows that 1 is an eigenvalue of the matrix B_0^τ, which is possible only if τ is divisible by t. Therefore $\tau = dt$, where d is a natural divisor of q. For $q = 1$ this implies the existence of a recurrent function with constant coefficients and maximal period (for $t = p^{kn} - 1 = \tau$).

Lemma 5. *If the characteristic polynomial $\varphi(x)$ of the function $\psi(x)$ is irreducible over the field P, the number of distinct prime ideal divisors of the number q is less than $N(\rho)$, and q is relatively prime to $N^n(\rho) - 1$, then the greatest of the numbers $\tau_1, \dots, \tau_s$ is divisible by each of the others.*

Lemma 6. *Let c be a proper (i.e. not equal to q) natural divisor of the number q, and let h_c be a natural number satisfying the congruence*

$$qh_c \equiv c \pmod{c \cdot (N^n(\rho) - 1)}.$$

If the characteristic polynomial of the matrix B_0 from the group G is irreducible over the field P, $N(\rho) > n$, and the difference between q and the greatest proper divisor of q is not less than n, then the matrix B_0 can be decomposed into a

product of matrices of the form (4): $B_0 = A_{q-1} \cdots A_1 A_0$ *in such a way that, for any proper divisor* c *of the number* q*, the condition* $A_{c-1} \cdots A_0 \neq B_c^{h_c}$ *is fulfilled.*

From this it is easy to obtain the theorem:

Theorem. *Let* $m_1, \ldots, m_v$ *be all proper divisors of the number* n*, and let* t *be a natural divisor of the number* $N^n(\rho) - 1$ *which divides none of the numbers* $N^{m_1}(\rho) - 1, \ldots, N^{m_v}(\rho) - 1$*. If* q *satisfies the conditions of Lemmas 5 and 6 and* $N(\rho) > n$*, then there exists a recurrent sequence over the field* K *modulo* ρ *of order* n *with period (the least one!), equal to* qt*.*

It follows from this theorem that, for ρ and q satisfying the conditions of the theorem, there exists a recurrent sequence over the field K modulo ρ of order n, the length of whose period is equal to $q(N^n(\rho) - 1)$.

Received
3 IV 1963

CITED LITERATURE

1. D. Rees, *J. Lond. Math. Soc.*, **213**, No. 83, 169 (1946).

Note: Figure translations are in progress. See original paper for figures.