UDC 511.176 DOI 10.17223/20710410/31/5

ON THE PERIOD LENGTH OF VECTOR SEQUENCES GENERATED BY POLYNOMIALS MODULO PRIME POWERS

N. G. Parvatov

National Research Tomsk State University, Tomsk, Russia

We give an upper bound on the period length for vector sequences defined recursively by systems of multivariate polynomials with coefficients in the ring of integers modulo a prime power.

Keywords: *recurrence sequences, vector sequences, period length, polynomial functions, polynomial permutations, finite rings.*

Introduction

Let n and m be positive integers, p be a prime number, and $f_1, \dots, f_n$ be polynomials in n variables with integer coefficients. Consider a recurrence sequence

$$f^0(x) + p^m\mathbb{Z}^n,\ f^1(x) + p^m\mathbb{Z}^n,\ f^2(x) + p^m\mathbb{Z}^n, \dots,$$

where $x \in \mathbb{Z}^n$, $f(x) = (f_1(x), \dots, f_n(x))$, $f^0(x) = x$, and $f^k(x) = f(f^{k-1}(x))$ for all positive k. Denote it by $s(f, m, x)$. The sequence $s(f, m, x)$ is said to be *purely periodic* if there exists a positive integer d such that $f^d(x) \equiv x \bmod p^m\mathbb{Z}^n$. In this case, the smallest d is called *the period* of $s(f, m, x)$ and is denoted by $\tau(f, m, x)$.

Further, the function on $\mathbb{Z}^n/p^m\mathbb{Z}^n$ induced by f is denoted by $[f]_m$. Clearly, this function is a permutation iff the sequence $s(f, m, x)$ is purely periodic for all $x \in \mathbb{Z}^n$.

Permutations induced by polynomials modulo prime powers are considered in [1 – 3]. They are characterized in [1]. Transitive polynomial permutations are described in [1, 2]. The cycle structure of permutations induced by univariate polynomials over Galois rings is investigated in [3]. In this paper, we extend this result to polynomials in several variables over the ring of integers modulo p^m. Namely, we derive an upper bound on the period length $\tau(f, m, x)$ under the condition that the sequence $s(f, m, y)$ is purely periodic for each $y \in x + p\mathbb{Z}^n$.

This paper is organized as follows. In section 1, we formulate Theorem 1. This theorem gives an upper bound on the value of $\tau(f, m, x)$. In section 2, we prove auxiliary Lemmas 1 and 2. In section 3, we prove the theorem.

1. Main results

We begin with some notation. Let $\mathbb{M}_n$ be the ring of $(n \times n)$-matrices over $\mathbb{Z}$ with the identity matrix E. For a matrix A, let $\det(A)$ denote its determinant. If $\det(A) \not\equiv 0 \bmod p\mathbb{Z}$, then there exists a positive integer k such that $A^k \equiv E \bmod p\mathbb{M}_n$. The smallest integer with this property is denoted by $\mathrm{ord}_p(A)$. By definition, put

$$J_f(x) = \begin{pmatrix} \dfrac{d\,f_1}{dx_1}(x) & \cdots & \dfrac{d\,f_n}{dx_1}(x) \\ \vdots & & \vdots \\ \dfrac{d\,f_1}{dx_n}(x) & \cdots & \dfrac{d\,f_n}{dx_n}(x) \end{pmatrix}$$

and $J_f^\tau(x) = J_f(f^0(x)) \cdots J_f(f^{\tau-1}(x))$ for a positive integer τ. The matrix $J_f(x)$ is called *the Jacobi matrix* and the determinant $\det(J_f(x))$ is called *the Jacobian* of the function f at the point x.

The aim of this paper is to prove the following result.

Theorem 1. Let x be a tuple in $\mathbb{Z}^n$ and m be a positive integer such that $m > 1$. Suppose the sequence $s(f, 1, x)$ is purely periodic and $\tau_1 = \tau(f, 1, x)$; then the following statements hold.

1) If the sequence $s(f, m, y)$ is purely periodic for every $y \in x + p\mathbb{Z}^n$, then
$$\det(J_f^{\tau_1}(x)) \not\equiv 0 \bmod p\mathbb{Z}.$$
2) If $\det(J_f^{\tau_1}(x)) \not\equiv 0 \bmod p\mathbb{Z}$ and $y \in x + p\mathbb{Z}^n$, then the sequence $s(f, m, y)$ is purely periodic and the following relation holds:
$$\tau(f, m, y) \,|\, \tau_1 \cdot p^{m-1} \cdot \operatorname{ord}_p(J_f^{\tau_1}(x)).$$
3) If $\det(J_f^{\tau_1}(x)) \not\equiv 0 \bmod p\mathbb{Z}$ and $\det(J_f^{\tau_1}(x) - E) \not\equiv 0 \bmod p\mathbb{Z}$, then, for every $y \in x + p\mathbb{Z}^n$, the following relation holds:
$$\tau(f, m, y) \,|\, \tau_1 \cdot p^{m-2} \cdot \operatorname{ord}_p(J_f^{\tau_1}(x)).$$

We will prove Theorem 1 in section 3.

Remark 1. We have $\operatorname{ord}_p(A) \leqslant p^n - 1$ for each $A \in \mathbb{M}_n$ such that $\det(A) \not\equiv 0 \bmod p\mathbb{Z}$. Indeed, $\operatorname{ord}_p(A)$ is equal to the period of the sequence of nonzero polynomials
$$x^0 \bmod m_A(x),\ x^1 \bmod m_A(x),\ x^2 \bmod m_A(x),\ \ldots$$
from the ring $\mathbb{Z}/p\mathbb{Z}[x]$, where $m_A(x)$ is the minimal polynomial of the matrix A over the field $\mathbb{Z}/p\mathbb{Z}$. Since $\deg m_A \leqslant n$, there are less than p^n distinct polynomials here.)

Thus, we obtain
$$\tau(f, m, y) \leqslant \tau_1 \cdot p^k(p^n - 1) \leqslant p^n \cdot p^k(p^n - 1),$$
where $k = m - 1$ in conditions of statement 2 and $k = m - 2$ in conditions of statement 3 in Theorem 1.

Remark 2. Let f be given by $f(z) = z \cdot A$ for all $z \in \mathbb{Z}^n$, where $A \in \mathbb{M}_n$ and $\det(A) \not\equiv 0 \bmod p\mathbb{Z}$. In this case, $s(f, m, x)$ is the congruential sequence
$$x + p^m\mathbb{Z}^n,\ x \cdot A + p^m\mathbb{Z}^n,\ x \cdot A^2 + p^m\mathbb{Z}^n,\ \ldots$$
In conditions of statement 2, we have $\tau_1 \,|\, \operatorname{ord}_p(A)$ and $J_f^{\tau_1}(x) = A^{\tau_1}$. Hence,
$$\tau(f, m, y) \leqslant \tau_1 \cdot p^{m-1} \cdot \operatorname{ord}_p(A^{\tau_1}) = p^{m-1} \cdot \operatorname{ord}_p(A) \leqslant p^{m-1}(p^n - 1).$$
In [4], this bound is proved and congruential sequences of period $p^{m-1}(p^n - 1)$ are constructed.

Remark 3. Let $\exp_p(\mathbb{M}_n)$ denote the exponent of the multiplicative group of the ring $\mathbb{M}_n/p\mathbb{M}_n$. Suppose that $[f]_m$ is a permutation of order $\tau(f, m)$. Then we have
$$\tau(f, m) \,|\, \tau(f, 1) \cdot p^k \cdot \exp_p(\mathbb{M}_n),$$
where $k = m - 1$ in conditions of statement 2 and $k = m - 2$ in conditions of statement 3. The value of $\exp_p(\mathbb{M}_n)$ is determined in [5, 6].

To prove Theorem 1, we need two auxiliary lemmas.

2. Two Lemmas

We use the notation $U(J,k) = E + J + \ldots + J^{k-1}$.

Lemma 1. Let l, k, τ, τ_1 be positive integers and x, y, z, w be tuples in $\mathbb{Z}^n$ such that $x \equiv y \bmod p\mathbb{Z}^n$. Suppose the sequence $s(f,1,x)$ is purely periodic and $\tau(f,1,x) \mid \tau_1$. Then the following statements hold.

1) $f^k(y + p^l z) \equiv f^k(y) + p^l z \cdot J_f^k(x) \bmod p^{l+1}\mathbb{Z}^n$.
2) If $f^\tau(y) = y + p^l w$ and $\tau_1 \mid \tau$, then

$$f^{k\tau}(y + p^l z) \equiv y + p^l w \cdot U(J_f^{\tau_1}(x)^\sigma, k) + p^l z \cdot J_f^{\tau_1}(x)^{k\sigma} \bmod p^{l+1}\mathbb{Z}^n,$$

where $\sigma = \tau/\tau_1$.

Proof. It is well known (see, for example, [1]) that

$$f(y + p^l z) \equiv f(y) + p^l z \cdot J_f(y) \bmod p^{l+1}\mathbb{Z}^n.$$

Using this formula, we get

$$\begin{gathered} f^2(y + p^l z) \equiv f(f(y) + p^l z \cdot J_f(y)) \equiv f^2(y) + p^l z \cdot J_f(y) \cdot J_f(f(y)) \equiv \\ \equiv f^2(y) + p^l z \cdot J_f^2(y) \bmod p^{l+1}\mathbb{Z}^n; \\ f^3(y + p^l z) \equiv f(f^2(y) + p^l z \cdot J_f^2(y)) \equiv f^3(y) + p^l z \cdot J_f^2(y) \cdot J_f(f^2(y)) \equiv \\ \equiv f^3(y) + p^l z \cdot J_f^3(y) \bmod p^{l+1}\mathbb{Z}^n; \\ \ldots \\ f^k(y + p^l z) \equiv f^k(y) + p^l z \cdot J_f^k(y) \bmod p^{l+1}\mathbb{Z}^n. \end{gathered}$$

Here, take $J_f^k(x)$ in place of $J_f^k(y)$. We claim that this replacing is correct. Indeed, since

$$x \equiv y,\ f(x) \equiv f(y),\ \ldots,\ f^{k-1}(x) \equiv f^{k-1}(y) \bmod p\mathbb{Z}^n,$$

we have

$$J_f(x) \equiv J_f(y),\ J_f(f(x)) \equiv J_f(f(y)),\ \ldots,\ J_f(f^{k-1}(x)) \equiv J_f(f^{k-1}(y)) \bmod p\mathbb{M}_n.$$

Hence, $J_f^k(y) \equiv J_f^k(x) \bmod p\mathbb{M}_n$ and $p^l z \cdot J_f^k(y) \equiv p^l z \cdot J_f^k(x) \bmod p^{l+1}\mathbb{Z}^n$. This proves the statement 1. Let us prove the statement 2. Note that the sequence

$$J_f(x) \bmod p\mathbb{M}_n,\quad J_f(f(x)) \bmod p\mathbb{M}_n,\quad J_f(f^2(x)) \bmod p\mathbb{M}_n,\quad \ldots$$

is purely periodic and its period divides τ_1. Hence, $J_f^\tau(x) \equiv J_f^{\tau_1}(x)^\sigma \bmod p\mathbb{Z}^n$. Using the statement 1, we get

$$\begin{gathered} f^\tau(y + p^l z) \equiv f^\tau(y) + p^l z \cdot J_f^{\tau_1}(x)^\sigma \equiv y + p^l w + p^l z \cdot J_f^{\tau_1}(x)^\sigma \equiv \\ \equiv y + p^l w \cdot U(J_f^{\tau_1}(x)^\sigma, 1) + p^l z \cdot J_f^{\tau_1}(x)^\sigma \bmod p^{l+1}\mathbb{Z}^n. \end{gathered}$$

In the same manner, we can see that

$$\begin{gathered} f^{2\tau}(y + p^l z) \equiv y + p^l w \cdot U(J_f^{\tau_1}(x)^\sigma, 2) + p^l z \cdot J_f^{\tau_1}(x)^{2\sigma} \bmod p^{l+1}\mathbb{Z}^n, \\ f^{3\tau}(y + p^l z) \equiv y + p^l w \cdot U(J_f^{\tau_1}(x)^\sigma, 3) + p^l z \cdot J_f^{\tau_1}(x)^{3\sigma} \bmod p^{l+1}\mathbb{Z}^n, \\ \ldots \\ f^{k\tau}(y + p^l z) \equiv y + p^l w \cdot U(J_f^{\tau_1}(x)^\sigma, k) + p^l z \cdot J_f^{\tau_1}(x)^{k\sigma} \bmod p^{l+1}\mathbb{Z}^n. \end{gathered}$$

This completes the proof. ■

Lemma 2. Let r be a positive integer. Suppose $J \in \mathbb{M}_n$ and $\det(J) \not\equiv 0 \bmod p\mathbb{Z}$. Then the following statements hold.

1) $U(J, p \cdot \mathrm{ord}_p(J) \cdot r) \equiv 0 \bmod p\mathbb{M}_n$.
2) If $\det(J - E) \not\equiv 0 \bmod p\mathbb{Z}$, then $U(J, \mathrm{ord}_p(J) \cdot r) \equiv 0 \bmod p\mathbb{M}_n$.

Proof. Clearly, if $i \equiv j \bmod \mathrm{ord}_p(J)$, then $J^i \equiv J^j \bmod p\mathbb{M}_n$. Hence,

$$U(J, p \cdot \mathrm{ord}_p(J) \cdot r) \equiv p \cdot r \cdot U(J, \mathrm{ord}_p(J)) \equiv 0 \bmod p\mathbb{M}_n$$

and statement 1 holds. Further, for every positive integer k we have

$$(J - E)U(J, k) = J^k - E.$$

For $k = \mathrm{ord}_p(J) \cdot r$, this gives

$$(J - E)U(J, \mathrm{ord}_p(J) \cdot r) \equiv 0 \bmod p\mathbb{M}_n.$$

If $\det(J - E) \not\equiv 0 \bmod p\mathbb{Z}$, then the matrix $J - E$ is invertible modulo $p\mathbb{M}_n$. In this case, $U(J, \mathrm{ord}_p(J) \cdot r) \equiv 0 \bmod p\mathbb{M}_n$. ■

3. Proof of Theorem 1

Suppose that, for every $y \in x + p\mathbb{Z}^n$, the sequence $s(f, m, y)$ is purely periodic; then the sequence $s(f, 2, y)$ is purely periodic too. We may choose a positive integer k such that the relation $\tau(f, 2, y) \mid k\tau_1$ holds for each $y \in x + p\mathbb{Z}^n$. This means that

$$f^{k\tau_1}(x + pz) \equiv x + pz \bmod p^2\mathbb{Z}^n$$

for all $z \in \mathbb{Z}^n$. At the same time, by statement 2 of Lemma 1, we have

$$f^{k\tau_1}(x + pz) \equiv x + pw \cdot U(J_f^{\tau_1}(x), k) + pz \cdot J_f^{\tau_1}(x)^k \bmod p^2\mathbb{Z}^n,$$

where $pw = f^{\tau_1}(x) - x$. If we take $z = 0$, we have $pw \cdot U(J_f^{\tau_1}(x), k) \equiv 0 \bmod p^2\mathbb{Z}^n$ and

$$f^{k\tau_1}(x + pz) \equiv x + pz \cdot J_f^{\tau_1}(x)^k \equiv x + pz \bmod p^2\mathbb{Z}^n$$

for all $z \in \mathbb{Z}^n$. This implies that

$$pz \cdot J_f^{\tau_1}(x)^k \equiv pz \bmod p^2\mathbb{Z}^n \text{ and } z \cdot J_f^{\tau_1}(x)^k \equiv z \bmod p\mathbb{Z}^n$$

for all z. Hence, $J_f^{\tau_1}(x)^k \equiv E \bmod p\mathbb{M}_n$ and $(\det(J_f^{\tau_1}(x)))^k \equiv 1 \bmod p\mathbb{Z}$. Thus, $\det(J_f^{\tau_1}(x)) \not\equiv \not\equiv 0 \bmod p\mathbb{Z}$. We have proved the first statement of Theorem 1.

Assume $\det(J_f^{\tau_1}(x)) \not\equiv 0 \bmod p\mathbb{Z}$ and $y \in x + p\mathbb{Z}^n$. Let

$$\tau_l = \begin{cases} \tau_1 \cdot p^{l-1} \cdot \mathrm{ord}_p(J_f^{\tau_1}(x)), & \text{if } \det(J_f^{\tau_1}(x) - E) \equiv 0 \bmod p\mathbb{Z}, \\ \tau_1 \cdot p^{l-2} \cdot \mathrm{ord}_p(J_f^{\tau_1}(x)), & \text{if } \det(J_f^{\tau_1}(x) - E) \not\equiv 0 \bmod p\mathbb{Z} \end{cases}$$

for all $l \geqslant 2$. Suppose inductively that the following relation holds:

$$f^{\tau_l}(y) \equiv y \bmod p^l\mathbb{Z}^n,$$

where $l \geqslant 1$. Then using Lemma 1, we obtain

$$f^{\tau_{l+1}}(y) \equiv y + pw \cdot U(J_f^{\tau_1}(x)^\sigma, k) \bmod p^{l+1}\mathbb{Z}^n,$$

where $pw = f^{\tau_l}(y) - y$, $\sigma = \tau_l/\tau_1$, and $k = \tau_{l+1}/\tau_l$. For $l = 1$, we have $\sigma = 1$ and

$$k = \begin{cases} p \cdot \mathrm{ord}_p(J_f^{\tau_1}(x)), & \text{for } \det(J_f^{\tau_1}(x) - E) \equiv 0 \bmod p\mathbb{Z}, \\ 1 \cdot \mathrm{ord}_p(J_f^{\tau_1}(x)), & \text{for } \det(J_f^{\tau_1}(x) - E) \not\equiv 0 \bmod p\mathbb{Z}. \end{cases}$$

For $l \geqslant 2$, we have $\mathrm{ord}_p(J_f^{\tau_1}(x)) \mid \sigma$ and $p \mid k$.

Using Lemma 2, we get $U(J_f^{\tau_1}(x)^{\sigma}, k) \equiv 0 \bmod p\mathbb{M}_n$ and $f^{\tau_{l+1}}(y) \equiv y \bmod p^l\mathbb{Z}^n$ for all $l \geqslant 1$. Thus, for every $l \geqslant 1$, the sequence $s(f, l, y)$ is purely periodic and $\tau(f, l, y) \mid \tau_l$. We take $l = m$ to complete the proof. ■

REFERENCES

1. *Anashin V. S.* Uniformly distributed sequences of p-adic integers. Discrete Math. Appl., 2002, vol. 12, no. 6, pp. 527–590.
2. *Larin M. V.* Transitive polynomial transformations of residue class rings. Discrete Math. Appl., 2002, vol. 12, no. 2, pp. 127–140.
3. *Ermilov D. M. and Kozlitin O. A.* Cyclic structure of a polynomial generator over the Galois ring. Mathematical Aspects of Cryptography, 2013, vol. 4, no. 1, pp. 27–57. (in Russian)
4. *Eichenauer-Herrmann J., Grothe H., and Lehn J.* On the period length of pseudo random vector sequences generated by matrix generators. Matematics of Computation, 1989, vol. 52, no. 185, pp. 145–148.
5. *Marshall I. B.* On the extension of Fermat's theorem to matrices of order n. Proc. Edinburgh Math. Soc., 1939–1941, vol. 5, pp. 85–91.
6. *Niven I.* Fermat's theorem for matrices. Duke Math. J., 1948, vol. 15, pp. 823–826.