M. Nilsson, R. Nyqvist, The Asymptotic Number of Periodic Points of Discrete p-Adic Dynamical Systems, *Труды МИАН*, 2004, том 245, 210–217

ТРУДЫ МАТЕМАТИЧЕСКОГО ИНСТИТУТА ИМ. В.А. СТЕКЛОВА, 2004, т. 245, с. 210–217

УДК 517.94+512.625

The Asymptotic Number of Periodic Points of Discrete p-Adic Dynamical Systems

©2004 г. M. Nilsson[1], R. Nyqvist[2]

Поступило в декабре 2003 г.

Let $A(n,a,y)$ denote a specific weighted average of different zeros of $f^n(x)-x$ for all prime numbers $p \le y$, where $f(x)=x^p+ax \in \mathbb{F}_p[x]$, $a \neq 0$, and f^n denotes the n-fold composition of f by itself. If $a=1$, then $A(n,a,x) \to 0$ as $x \to \infty$, and if $a>1$, then $A(n,a,x) \to 1$ as $x \to \infty$. We also discuss a method for counting the number of linear factors of a polynomial whose zeros are n-periodic points of $f(x) \in \mathbb{Z}[x]$ by using a theorem of Frobenius. Finally, we obtain some results in the monomial case over p-adic numbers by using this method.

1. INTRODUCTION

Over the last ten to fifteen years, the theory of dynamical systems over p-adic numbers or finite fields has grown considerably (see, for instance, Arrowsmith and Vivaldi [2], Batra and Morton [3, 4], Benedetto [5, 6], Khrennikov [10], Khrennikov and Nilsson [11], Lubin [13], Nilsson [16–18], Nyqvist [19], Vivaldi and Hatjispyros [23], and Vivaldi [24]). A discrete dynamical system can be described by iterations of a mapping. The periodic points of such a system give us information about its long-time behavior.

In this paper, we consider discrete polynomial dynamical systems over both finite fields and p-adic numbers. Let $f(x)=x^p+ax \in \mathbb{F}_p[x]$ and let $N(n,p,a)$ denote the number of different zeros of $f^n(x)-x$ in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. In this paper, we prove that the average

$$\frac{1}{\pi(x)} \sum_{p \le x} \frac{1}{p^n} N(n,p,a)$$

approaches 1 as x approaches infinity when $a>1$. If $a=1$, then we conclude that the average approaches zero instead.

We also calculate the average number of periodic points of a dynamical system generated by a polynomial $f(x) \in \mathbb{Z}[x]$ in the finite fields $\mathbb{F}_p$ for all prime numbers p. This is done by counting linear factors of a certain polynomial related to $f(x)$ and using a theorem of Frobenius. This theorem connects the periodic points in $\mathbb{F}_p$ to the Galois group of a polynomial.

For monomial $f(x)$, the average value was computed in Nilsson [17, 16] and Khrennikov and Nilsson [11], using a sort of a probabilistic method. We will obtain the same result in this paper.

2. THE NUMBER OF PERIODIC POINTS

Let $f(x) \in K[x]$, where K is a field, be a monic polynomial of degree greater than 1. By $f^n(x)$, we denote the n-fold composition of $f(x)$ with itself. An element α with the property $f^r(\alpha)=\alpha$ for some positive integer n is called an *n-periodic point*. If n is the smallest such integer, then n is called the *period* of α, or we say that α is a *primitive n-periodic point*.

[1]School of Mathematics and Systems Engineering, Växjö University, SE-351 95 Växjö, Sweden.
E-mail: Marcus.Nilsson@msi.vxu.se

[2]School of Mathematics and Systems Engineering, Växjö University, SE-351 95 Växjö, Sweden.
E-mail: Robert.Nyqvist@msi.vxu.se

Let p be a prime number. In this section, we will study the polynomial

$$f(x) = x^p + ax \in \mathbb{F}_p[x], \tag{1}$$

where $a \neq 0$. Let $N(n,p,a)$ denote the number of different n-periodic points of f in $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. Hence, $N(n,p,a)$ is equal to the number of different zeros of $f^n(x) - x$. Let $\operatorname{ord}_p(a)$ denote the smallest positive integer c such that $a^c \equiv 1 \pmod{p}$.

Theorem 2.1 (Batra and Morton [3]). *If $\operatorname{ord}_p(a)$ divides n, then $f^n(x) - x$ is a pth power. Also, if $(n,p) = 1$, then $f^n(x) - x = g(x)^p$, where g has distinct zeros. If $\operatorname{ord}_p(a)$ does not divide n, then $f^n(x) - x$ has no multiple factors.*

By the theorem above, it follows that $N(n,p,a) = p^n$ if $\operatorname{ord}_p(a) \nmid n$, that $N(n,p,a) = p^{n-1}$ if $\operatorname{ord}_p(a) \mid n$ and $(n,p) = 1$, and that $N(n,p,a) \leq p^{n-1}$ if $\operatorname{ord}_p(a) \mid n$ and $(n,p) > 1$. Set

$$A(n,a,x) = \frac{1}{\pi(x)} \sum_{p \leq x} \frac{1}{p^n} N(n,p,a),$$

where $\pi(x)$ is the number of primes p less than or equal to x and the sum is taken over all these primes p.

First, let $a = -1$. If n is odd, then $N(n,p,-1) = p^n$ since $\operatorname{ord}_p(-1) = 2$. Therefore, we have

$$A(n,-1,x) = \frac{1}{\pi(x)} \sum_{p \leq x} 1 = \frac{\pi(x)}{\pi(x)} = 1.$$

If n is even, then $N(n,p,-1) \leq p^{n-1}$, and the prime number theorem (see, for instance, Apostol [1]) gives

$$\begin{aligned} A(n,-1,x) &\leq \frac{1}{\pi(x)} \sum_{p \leq x} \frac{1}{p} = \frac{1}{\pi(x)} \left(\log\log x + C + O\left(\frac{1}{\log x}\right)\right) \\ &\sim \frac{\log x}{x} \left(\log\log x + C + O\left(\frac{1}{\log x}\right)\right) \\ &= \frac{1}{x} \log x \cdot \log\log x + C \frac{\log x}{x} + O\left(\frac{1}{x}\right), \end{aligned}$$

where C is the constant

$$1 - \log\log 2 + \int_2^\infty \frac{O(1)}{t \log^2 t}\, dt.$$

Suppose that g and h are real-valued functions that satisfy $h(x) \to B < \infty$ as $x \to \infty$ and $g(x) \sim h(x)$, i.e., $\lim_{x\to\infty} g(x)/h(x) = 1$; then,

$$\lim_{x\to\infty} (g(x) - h(x)) = \lim_{x\to\infty} h(x) \left(\frac{g(x)}{h(x)} - 1 \right) = B \cdot 0 = 0.$$

Hence, it follows that $A(p,-1,x) \to 0$ as $x \to \infty$.

Theorem 2.2. *If $a = 1$, then $A(n,a,x) \to 0$ as $x \to \infty$. If $a > 1$, then $A(n,a,x) \to 1$ as $x \to \infty$.*

Proof. If $a = 1$, then $\operatorname{ord}_p(a) = 1$ and $A(n,1,x) \to 0$ as $x \to \infty$ by the same argument as in the case when $a = -1$ and n is even. Now, suppose that $a > 1$. If p divides a, then $f(x) = x^p$ and

$f^n(x) - x = x^{p^n} - x$, which has no multiple zeros. Hence, $N(n,p,a) = p^n$ in this case. Observe that $\operatorname{ord}_p(a)$ is not defined if p divides a. Therefore,

$$\sum_{p\le x} \frac{1}{p^n} N(n,p,a) = \sum_{\substack{p\mid a\\ p\le x}} 1 + \sum_{\substack{p\le x\\ \operatorname{ord}_p(a)\nmid n}} 1 + \sum_{\substack{p\le x\\ \operatorname{ord}_p(a)\mid n\\ (n,p)=1}} \frac{1}{p} + \sum_{\substack{p\le x\\ \operatorname{ord}_p(a)\mid n\\ (n,p)>1}} O\left(\frac{1}{p}\right). \tag{2}$$

The first and the fourth sums on the right-hand side in (2) are finite. Also, the third sum is finite. To see this, set $c = \operatorname{ord}_p(a)$. We have $a^c > p$, which is equivalent to $\log a^c > \log p$, i.e.,

$$c > \frac{\log p}{\log a} = \log_a p.$$

Hence, for all primes p such that $\log_a p > n$, we have $\operatorname{ord}_p(a) > n$ and, therefore, also $\operatorname{ord}_p(a) \nmid n$. This proves that the third sum on the right-hand side in (2) is also finite. The second sum is then asymptotic to $\pi(x)$, which proves that $A(n,a,x) \to 1$ as $x \to \infty$. $\square$

3. THE AVERAGE OF LINEAR FACTORS

The results in this and the following sections are also presented in Khrennikov, Nilsson, and Nyqvist [12]. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree greater than 1. Define

$$\Phi_{r,f}(x) = \prod_{d\mid r} \bigl(f^d(x) - x\bigr)^{\mu(r/d)}, \tag{3}$$

where μ is the Möbius function, that is, $\mu(1) = 1$ and $\mu(n) = 0$ if the integer n has a square factor, otherwise $\mu(n) = (-1)^k$, where k is the number of distinct primes in the factorization of n. If $f(x) \in K[x]$, then $\Phi_{r,f}(x) \in K[x]$ for all r and any field K (see Theorem 2.5 in Morton and Patel [15]). In the same article, the following properties of $\Phi_{n,f}$ are shown:

1. If $\operatorname{char} K \nmid r$, then the formula
$$\prod_{d\mid r} \Phi_{d,f}(x)$$
gives a factorization of $f^r(x) - x$ in $K[x]$.
2. If α is a primitive r-periodic point of f, then $\Phi_{r,f}(\alpha) = 0$.
3. If $\operatorname{char} K \nmid r$, α is a primitive m-periodic point of f, where $m < r$, and $\Phi_{r,f}(\alpha) = 0$, then $(x-\alpha)^2 \mid \Phi_{r,f}(x)$.
4. If $\operatorname{char} K \nmid r$ and $(x-\alpha)$ is a multiple factor of $f^m(x) - x$ for $m < r$, then $(x-\alpha) \nmid \Phi_{r,f}(x)$.

Hence, if $\Phi_{r,f}(x)$ is separable over K, i.e., it has no multiple roots, then the zeros of $\Phi_{r,f}(x)$ are all primitive r-periodic points of f. For more information about the properties of $\Phi_{r,f}$, see also Batra and Morton [3, 4] and Vivaldi and Hatjispyros [23].

Let $g(x) \in \mathbb{Z}[x]$ and define $L(g,p)$ to be the number of linear factors of $g(x)$ modulo p, where p is a prime number. Let $\mathcal{P}_m$ be the set of the first m primes and define the average function

$$I(g) = \lim_{m\to\infty} \frac{1}{m} \sum_{p\in\mathcal{P}_m} L(g,p).$$

Let K be a field and $f(x) \in K[x]$. If $\alpha_1, \dots, \alpha_n$ are the zeros of $f(x)$ in some splitting field of f over K, then the *discriminant* $\operatorname{disc}(f)$ of f is defined as $\prod_{i<j}(\alpha_i - \alpha_j)$.

4. CHEBOTAREV'S DENSITY THEOREM

We are going to use the next theorem, by Frobenius, to calculate $I(\Phi_{n,f})$. In Pohst and Zassenhaus [20] and Dummit and Foote [7], this method was described in detail.

Theorem 4.1 (theorem of Frobenius)**.** *Let $f(x) \in \mathbb{Z}[x]$. Assume that f is monic and* $\operatorname{disc} f \neq 0$. *Let G be the Galois group of f over $\mathbb{Q}$. Then, the density of the set of primes for which f has a given decomposition type $n_1, \dots, n_t$ exists and is equal to $1/|G|$ times the number of elements in G with the cycle pattern $(n_1, \dots, n_t)$.*

Chebotarev's density theorem is a generalization of the previous theorem. An interesting article about Chebotarev and these two theorems can be found in Stevenhagen and Lenstra [22].

Theorem 4.2 (Chebotarev's density theorem)**.** *Let $f(x) \in \mathbb{Z}[x]$. Assume that f is monic and* $\operatorname{disc} f \neq 0$. *Let C be a conjugacy class of the Galois group G of f. Then, the set of primes p that do not divide* $\operatorname{disc} f$ *and for which the Frobenius substitution σ_p belongs to C has density $|C|/|G|$.*

Example 4.1. Let $f(x) = x^2$. Then, $\Phi_{3,f}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $\operatorname{disc}(\Phi_{3,f}) = (-1) \cdot 7^5$. Since $\Phi_{3,f}(x)$ is the 7th cyclotomic polynomial, its Galois group is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^*$ (see, for example, Morandi [14]). Factoring $\Phi_{3,f}(x)$ modulo p for the first 4000 primes p, excluding 7, gives

The degree of the factors	$\{6\}$	$\{3,3\}$	$\{2,2,2\}$	$\{1,1,1,1,1,1\}$
Frequency	1345/4000	1329/4000	665/4000	661/4000

Using the left regular representation of the elements in $(\mathbb{Z}/7\mathbb{Z})^*$, we see that the result in the table above is close to the frequency of the cycle decomposition of the elements in $(\mathbb{Z}/7\mathbb{Z})^*$. Since the left regular representation of the elements in a group is an action on the group itself and the identity in $(\mathbb{Z}/7\mathbb{Z})^*$ is the only element that has fixed points under this action, we have $I(\Phi_{3,f}) = 1$.

Example 4.2. Let $f(x) = x^2 - 2$. Then, $\Phi_{3,f}(x) = (x^3 + x^2 - 2x - 1)(x^3 - 3x + 1)$ and $\operatorname{disc}(\Phi_{3,f}) = 3^4 \cdot 7^2$. Factoring $\Phi_{3,f}(x)$ modulo p for the first 4000 primes p, excluding 3 and 7, gives

The degree of the factors	$\{3,3\}$	$\{3,1,1,1\}$	$\{1,1,1,1,1,1\}$
Frequency	1781/4000	1778/4000	441/4000

We can conclude that the Galois group of $\Phi_{3,f}(x)$ is a group of nine elements. Hence, $\operatorname{Gal}(\Phi_{3,f}) = C_3 \times C_3$ since it is the only subgroup of S_6 with nine elements (the second possible group C_9 can be excluded since it contains elements of order 9, whereas S_6 does not). Further, $I(\Phi_{3,f}) = 3 \cdot 4/9 + 6 \cdot 1/9 = 2$.

Example 4.3. Let $f(x) = x^2 + 1$. Then,

$$\Phi_{3,f}(x) = x^6 + x^5 + 4x^4 + 3x^3 + 7x^2 + 4x + 5$$

and $\operatorname{disc}(\Phi_{3,f}) = (-1) \cdot 3^6 \cdot 11^3$. Factoring $\Phi_{3,f}(x)$ modulo p for the first 4000 primes p, excluding 3 and 11, gives

The degree of the factors	$\{6\}$	$\{3,3\}$	$\{3,1,1,1\}$	$\{2,2,2\}$	$\{1,1,1,1,1,1\}$
Frequency	1356/4000	875/4000	879/4000	670/4000	220/4000

Hence, the Galois group $\operatorname{Gal}(\Phi_{3,f})$ contains 18 elements. There are five groups of cardinality 18: C_{18}, $C_6 \times C_3$, D_9, $D_3 \times C_3$, and $D_3 \times^{\vartheta} D_3$.[3] We can directly exclude the two groups C_{18} and D_9

[3]Let G and H be groups with normal subgroups K and N, respectively, such that there is an isomorphism $\vartheta\colon G/K \to H/N$. Then, the *pullback* $G \times^{\vartheta} H$ is the subgroup of $G \times H$ of elements (g,h) that satisfy $\vartheta(gK) = hN$ (see Humphreys [9]). In our case, ϑ is the identity automorphism on the quotient D_3/D_3'.

since they contain elements of order 9 and, therefore, are not subgroups of S_6. The elements in the remaining groups are only of order 1, 2, 3, and 6. But the group $C_6 \times C_3$ contains only one element of order 2, which is at least two elements too few, and the group $D_3 \times^{\vartheta} D_3$ contains no elements of order 6. Hence, $\mathrm{Gal}(\Phi_{3,f}) = D_3 \times C_3$, and $I(\Phi_{3,f}) = 1$.

In the last example, we were lucky since all the groups of cardinality 18 have different numbers of cycle decomposition, and it is therefore easy to find the Galois group of $\Phi_{3,f}$. But it is known that there exist infinitely many examples of nonisomorphic groups of the same cardinality such that they contain the same number of elements of all cycle decompositions. Hence, in the general case, the use of the Frobenius theorem to determine the Galois group of a polynomial is not practical.

5. PERMUTATIONS

Let X be a set and G be a group. An *action* of G on X is a map from $G \times X$ to X, denoted by $(g, x) \mapsto g \cdot x$, such that

(1) $e \cdot x = x$ for all $x \in X$, where e is the identity element in G;

(2) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Theorem 5.1. *Let G and X be as above. For each element g in G, the function $\sigma_g \colon X \to X$ defined as $\sigma_g(x) = g \cdot x$ is a permutation of X, i.e., it is a one-to-one function.*

We will use different notations for the action, depending on G and X. In general, the dot notation above will be used. However, if $X = \{1, 2, \dots, n\}$ and $g \in G$ is a permutation acting on X, then we will write $g(x)$ instead. An action of G on X is called *transitive* if, for each $x_1, x_2 \in X$, there exists an element $g \in G$ such that $g \cdot x_1 = x_2$. Let X be a finite set and G be a group acting on X. Let $x \in X$. The *orbit* of x is the set

$$Gx = \{y \in X \colon\ g \cdot x = y \text{ for some } g \in G\}.$$

The set of orbits forms a partition of X. Let $g \in G$ and define

$$X^{\langle g \rangle} = \{x \in X \colon\ g \cdot x = x\}.$$

Thus, $X^{\langle g \rangle}$ is the set of all elements in X that are *fixed* under g.

Theorem 5.2 (Burnside's lemma)**.** *The number of orbits in X under G is equal to*

$$\frac{1}{|G|} \sum_{g \in G} \bigl|X^{\langle g \rangle}\bigr|.$$

Let $A(n)$ be the number of $g \in G$ that have exactly n fixed points over X and define

$$\mathcal{F}(G, X) = \sum_{n=1}^{|X|} n \, \frac{A(n)}{|G|}.$$

The function $\mathcal{F}$ can be regarded as the average number of fixed points per element in G acting on X.

Example 5.1. Let $X = \{1, 2, 3, 4\}$ and $G = D_4$. Then,

$$\mathcal{F}(D_4, X) = \sum_{n=1}^{4} n \, \frac{A(n)}{8} = 1 \cdot \frac{0}{8} + 2 \cdot \frac{2}{8} + 3 \cdot \frac{0}{8} + 4 \cdot \frac{1}{8} = 1 \tag{4}$$

since the elements in the 4th dihedral group D_4 have the following cycle patterns:

Cycle pattern	(4)	(2, 2)	(2, 1, 1)	(1, 1, 1, 1)
Number	2	3	2	1

Theorem 5.3. *The number of orbits in X under G is equal to $\mathcal{F}(G, X)$.*

Proof. We have that $A(n)$ is the number of sets $X^{\langle g\rangle}$ such that $|X^{\langle g\rangle}| = n$. Hence,

$$\sum_{n=0}^{|X|} nA(n) = \sum_{g\in G} \left|X^{\langle g\rangle}\right|,$$

and the theorem follows from Theorem 5.2. □

Theorem 5.4. *Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, G be the Galois group of f, and X be the set of zeros of f. Then, $I(f) = \mathcal{F}(G, X)$, i.e., $I(f)$ is equal to the number of orbits in X under G.*

Proof. It follows from Theorem 5.3 and the theorem of Frobenius (see Section 4). □

Corollary 5.5. *If $f(x) \in \mathbb{Z}[x]$ is monic and irreducible, then $I(f) = 1$.*

Proof. Let X be the set of roots of $f(x)$. The action of the Galois group $\mathrm{Gal}(f)$, considered as a permutation group, on X is transitive. Therefore, X contains only one orbit under $\mathrm{Gal}(f)$. Hence, $\mathcal{F}(\mathrm{Gal}(f), X) = 1$, and the corollary follows from Theorem 5.4. □

Remark 5.1. We can also say how many times we will get a certain number of linear factors modulo p of $\Phi_{n,f}(x)$. For instance, if $\mathrm{Gal}(\Phi_{n,f}) = D_4$ and $\deg \Phi_{n,f} = 4$, then we cannot get one linear factor, but we get two linear factors one time out of four (see Example 5.1).

6. THE MONOMIAL CASE

Let n be a positive integer. In this section, we will study the iterations of the monomial function $f(x) = x^n \in F[x]$, where $F = \mathbb{Q}$ or $F = \mathbb{F}_p$ for $p \nmid n^r - 1$. (This guarantees that there exists a primitive $(n^r - 1)$th root of unity in the splitting field of $x^{n^r-1} - 1$.)

Lemma 6.1. *Let $r \geq 2$. The polynomials $\Phi_{r,f}(x)$ over F are the products of cyclotomic polynomials Ψ_d. For $r = 1$, we have*

$$\Phi_{1,f}(x) = f(x) - x = x \prod_{d|n-1} \Psi_d(x).$$

Proof. We know that $f^r(x) - x = \prod_{d|r} \Phi_{d,f}(x)$ and that

$$f^r(x) - x = x \prod_{s|n^r-1} \Psi_s(x),$$

where $\Psi_s(x)$ is the sth cyclotomic polynomial. We will prove that all (linear) factors in a specific $\Psi_s(x)$ are factors in the same $\Phi_{d,f}(x)$. We will do this by showing that all the zeros of $\Psi_s(x)$ have the same primitive period. Let $s_0 \mid (n^r - 1)$, α be a zero of $\Psi_{s_0}(x)$, and d_α be the primitive period of α. If β is another zero of $\Psi_{s_0}(x)$ with primitive period d_β such that $d_\alpha \geq d_\beta$, then we have

$$f^{d_\beta}(x) - x = x \prod_{s|n^{d_\beta}-1} \Psi_s(x).$$

Since $f^{d_\beta}(\beta) - \beta = 0$, we have that $s_0 \mid n^{d_\beta} - 1$ and, therefore, $f^{d_\beta}(\alpha) - \alpha = 0$. But we assumed that α had a primitive period $d_\alpha \geq d_\beta$. Hence, $d_\alpha = d_\beta$. □

Let $g(x) \in F[x]$. By $T(g)$, we mean the number of irreducible factors in $g(x)$ over F. For $f(x) = x^n \in F[x]$, we have

$$T(f^r(x) - x) = \sum_{d|r} T(\Phi_{d,f}(x)), \tag{5}$$

and by the Möbius inversion (see, for example, Dummit and Foote [7]), we get

$$T(\Phi_{r,f}(x)) = \sum_{d|r} \mu(r/d) T(f^d(x) - x). \tag{6}$$

Let m be a positive integer. By $\tau(m)$, we mean the number of positive divisors of m. In the case $F = \mathbb{Q}$, we have

$$T(f^r(x) - x) = T((x^{n^r-1} - 1)x) = \tau(n^r - 1) + 1.$$

We have proved the following theorem.

Theorem 6.2. *The number of irreducible factors of $\Phi_{r,f}(x)$ over $\mathbb{Q}$ is given by*

$$T(\Phi_{r,f}(x)) = \sum_{d|r} \mu(r/d)(\tau(n^d - 1) + 1).$$

Observe that if $r \geq 2$, then we have

$$T(\Phi_{r,f}(x)) = \sum_{d|r} \mu(r/d)\tau(n^d - 1) \tag{7}$$

since $\sum_{d|r} \mu(r/d) = 0$ if $r \geq 2$.

When the Galois group of a polynomial $\Phi_{r,f}(x)$ acts on the set of zeros of $\Phi_{r,f}(x)$, the number of orbits is equal to the number of irreducible factors of $\Phi_{r,f}(x)$.

Theorem 6.3. *For $r \geq 2$, we have*

$$I(\Phi_{r,f}) = \sum_{d|r} \mu(d)\tau(n^{r/d} - 1).$$

We recognize this formula from Khrennikov and Nilsson [11], where it describes the mean value of the number of r-periodic points of $f(x)$ in p-adic fields (see Gouvêa [8] or Schikhof [21] for an introduction to p-adic fields).

Let $n \in \mathbb{Z}^+$ and let $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ such that $f(x) = x^n$. Let $r \in \mathbb{Z}^+$. Let now p be a prime number such that $p \geq 3$ and $p \nmid n^r - 1$. Since $\operatorname{char} \mathbb{Q}_p = 0$, we can repeat the construction of the polynomials $\Phi_{r,f}(x)$. Since the roots of $\Phi_{r,f}$ are roots of unity, we have the same number of roots in $\mathbb{Q}_p$ as in $\mathbb{F}_p$. We have the following theorem.

Theorem 6.4. *The number of linear factors in $\Phi_{r,f}(x)$ when we factorize over $\mathbb{Q}_p$ is the same as the number of linear factors when we factorize $\Phi_{r,f}(x)$ over $\mathbb{F}_p$ for $p \nmid \operatorname{disc}(\Phi_{r,f}(x))$, $p \nmid n^r - 1$, and $p \geq 3$.*

Therefore, we can also use Theorem 6.3 when we factorize over $\mathbb{Q}_p$. This is the same result as in Khrennikov and Nilsson [11]. See also Nilsson [17] for a more probabilistic view of the number of periodic points in p-adic fields.

REFERENCES

1. *Apostol T.M.* Introduction to analytic number theory. New York: Springer, 1976.
2. *Arrowsmith D.K., Vivaldi F.* Geometry of p-adic Siegel discs // Physica D. 1994. V. 71. P. 222–236.
3. *Batra A., Morton P.* Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. I // Rocky Mount. J. Math. 1994. V. 24, N 2. P. 453–481.
4. *Batra A., Morton P.* Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. II // Rocky Mount. J. Math. 1994. V. 24, N 3. P. 905–932.

5. *Benedetto R.L.* p-Adic dynamics and Sullivan's no wandering domains theorem // Compos. Math. 2000. V. 122. P. 281–298.
6. *Benedetto R.* Hyperbolic maps of p-adic dynamics // Ergod. Theory and Dyn. Syst. 2001. V. 21. P. 1–11.
7. *Dummit D.S., Foote R.M.* Abstract algebra. 2nd ed. Upper Saddle River (NJ): Prentice Hall, 1999.
8. *Gouvêa F.Q.* p-Adic numbers: An introduction. 2nd ed. Berlin etc.: Springer, 1997.
9. *Humphreys J.F.* A course in group theory. Oxford: Oxford Univ. Press, 1996.
10. *Khrennikov A.Yu.* Non-Archimedean analysis: Quantum paradoxes, dynamical systems and biological models. Dordrecht: Kluwer, 1997.
11. *Khrennikov A., Nilsson M.* On the number of cycles of p-adic dynamical systems // J. Number Theory. 2001. V. 90, N 2. P. 255–264.
12. *Khrennikov A., Nilsson M., Nyqvist R.* The asymptotic number of periodic points of discrete polynomial p-adic dynamical system // Ultrametric functional analysis: Proc. Seventh Intern. Conf. on p-Adic Analysis. Providence (RI): Amer. Math. Soc., 2003. P. 159–166. (Contemp. Math.; V. 319).
13. *Lubin J.* Non-Archimedean dynamical systems // Compos. Math. 1994. V. 94. P. 321–346.
14. *Morandi P.* Field and Galois theory. New York: Springer, 1996.
15. *Morton P., Patel P.* The Galois theory of periodic points of polynomial maps // Proc. London Math. Soc. 1994. V. 68. P. 224–263.
16. *Nilsson M.* Cycles of monomial and perturbated monomial p-adic dynamical systems // Ann. Math. B. Pascal. 2000. V. 7, N 1. P. 37–63.
17. *Nilsson M.* Cycles of monomial p-adic dynamical systems: Licentiate thesis. Växjö: School Math. and Syst. Eng., Växjö Univ., 2001.
18. *Nilsson M.* Periodic points of monomials in the field of p-adic numbers: Rept. MSI 02020. Växjö: Växjö Univ., Mar. 2002.
19. *Nyqvist R.* Linear factors of discrete dynamical systems: Rept. MSI 02029. Växjö: Växjö Univ., Apr. 2002.
20. *Pohst M., Zassenhaus H.* Algorithmic algebraic number theory. Cambridge: Cambridge Univ. Press, 1989.
21. *Schikhof W.H.* Ultrametric calculus: An introduction to p-adic analysis. Cambridge: Cambridge Univ. Press, 1984.
22. *Stevenhagen P., Lenstra H.W. Jr.* Chebotarev and his density theorem // Math. Intell. 1996. V. 18, N 2. P. 26–37.
23. *Vivaldi F., Hatjispyros S.* Galois theory of periodic orbits of rational maps // Nonlinearity. 1992. V. 5. P. 961–978.
24. *Vivaldi F.* Dynamics over irreducible polynomials // Nonlinearity. 1992. V. 5. P. 941–960.