On the Number of Equivalence Classes of Attracting Dynamical Systems

Per-Anders Svensson
School of Mathematics and Systems Engineering
Växjö University
SE-351 95 Växjö, Sweden
Per-Anders.Svensson@vxu.se

Robert Nyqvist
Department of Mathematics and Science
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden
Robert.Nyqvist@bth.se

Abstract

We study discrete dynamical systems of the kind $h(x) = x + g(x)$, where $g(x)$ is a monic irreducible polynomial with coefficients in the ring of integers of a $\mathfrak{p}$-adic field K. The dynamical systems of this kind, having attracting fixed points, can in a natural way be divided into equivalence classes, and we investigate whether something can be said about the number of those equivalence classes, for a certain degree of the polynomial $g(x)$.

1 Introduction

The interest of discrete dynamical systems in fields provided with a non-archimedean valuation has been increasing in the last couple of decades, see e.g. Arrowsmith and Vivaldi [2], Benedetto [3], Khrennikov [5, 6], Khrennikov and Nilsson [7, 8], Lubin [11], Nyqvist [12], and Svensson [14]. Among the applications one can find for instance cryptography (generating pseudorandom sequences to be used for stream ciphers), see e.g. Anashin [1].

In this paper we will study a special class of discrete dynamical systems defined over a $\mathfrak{p}$-adic field K. The class consist of polynomials of the kind

$$h(x) = x + g(x),$$

where $g(x)$ is a monic irreducible polynomial, whose coefficients belong to the ring of integers in K. In Svensson [14], necessary and sufficient conditions have been studied, for the fixed points of such a dynamical system to be attracting. Some generalizations of these results have been made in Khrennikov and Svensson [9], of which this paper can be contemplated as a continuation.

2 Prerequisites and Notation

Let K be a $\mathfrak{p}$-adic field. By this, we will mean that $\operatorname{char} K = 0$, that K is complete with respect to a non-trivial discrete valuation defined on K, and that the residue class field of K is finite. We let $\mathfrak{O}_K$ denote the ring of integers in K, and $\mathfrak{P}_K$ the unique maximal ideal in $\mathfrak{O}_K$. The residue class field $\mathfrak{O}_K/\mathfrak{P}_K$ of K (which, as mentioned, is finite by definition) will be denoted by $K_\mathfrak{p}$. If $\operatorname{char} K_\mathfrak{p} = p$, then the field $K_\mathfrak{p}$ is isomorphic to $\mathbb{F}_q$, the finite field of q elements, where $q = p^m$ for some $m \in \mathbb{Z}^+$. If u is any element in $\mathfrak{O}_K$, we write $\bar{u}$ for its canonical image in $K_\mathfrak{p}$. In the same manner, $\bar{f}(x)$ denotes the canonical image in $K_\mathfrak{p}[x]$ of a polynomial $f(x) \in \mathfrak{O}_K[x]$.

Any $\mathfrak{p}$-adic field is isomorphic to some finite extension of the p-adic number field $\mathbb{Q}_p$, see Cassels [4]. In the special case when $K = \mathbb{Q}_p$, one usually writes $\mathbb{Z}_p$ and $p\mathbb{Z}_p$ for $\mathfrak{O}_K$ and $\mathfrak{P}_K$, respectively. Here, the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to the finite field $\mathbb{F}_p$ of p elements.

By a *discrete dynamical system* (or dynamical system, for short) h on L, we will mean a mapping $L \ni \beta \mapsto h(\beta) \in L$, where $h(x)$ is a polynomial in $K[x]$. Given a dynamical system h on L and an element α in L, we define a sequence $(\alpha_j)_{j=0}^{\infty}$ of elements in L recursively by

$$\begin{cases} \alpha_0 = \alpha \\ \alpha_j = h(\alpha_{j-1}), \quad j = 1, 2, \ldots. \end{cases}$$

We will write $h^j(\alpha) = \alpha_j$ for every j, where we interpret h^j as the composition of h with itself j times.

3 Attracting Fixed Points

Let K be a $\mathfrak{p}$-adic field and $g(x) \in \mathfrak{O}_K[x]$ a monic polynomial that is irreducible over K. We study the dynamical system

$$h(x) = x + g(x) \tag{3.1}$$

over an extension L of K that contains (at least one of) the fixed points of $h(x)$, i.e. elements $\alpha \in L$ having the property $h(\alpha) = \alpha$. These fixed points are exactly the zeros of $g(x)$ in L.

Even though the polynomial $g(x)$ is claimed to be irreducible over K, its canonical image $\bar{g}(x) \in K_\mathfrak{p}[x]$ is of course not necessarily irreducible over $K_\mathfrak{p}$. However, if this happens to be the case, we will say that $g(x)$ is *inertial*.

Assume now that $\alpha \in L$ is an attracting fixed point of h, meaning that there is a neighborhood $V \subseteq L$ of α such that

$$\lim_{j\to\infty} h^j(\beta) = \alpha$$

for every $\beta \in V$. The following theorem (see Svensson [14]) gives a necessary and sufficient condition for a fixed point of the dynamical system (3.1) to be attracting.

Theorem 3.1. *Suppose $g(x) \in \mathfrak{O}_K[x]$ is monic and irreducible over K. Then a fixed point of $h(x) = x + g(x)$ is attracting, if and only if $g(x)$ is inertial and if there exists a non-constant polynomial $\psi(x) \in K_\mathfrak{p}[x]$ such that*

$$\bar{g}(x) = \psi(x^p) - x,$$

where $p = \operatorname{char} K_\mathfrak{p}$.

With Theorem 3.1 in mind, we obtain in a natural manner a partition of all dynamical systems into disjoint equivalence classes, in the following way. We say that two polynomials in $\mathfrak{O}_K[x]$ are $K_\mathfrak{p}[x]$-*equivalent*, if they have the same canonical images in $K_\mathfrak{p}[x]$. Let $N(m,p)$ denote the number of equivalence classes that can be represented by an inertial polynomial, having a canonical image of the kind $\psi(x^p) - x$ in $K_\mathfrak{p}[x]$, for some $\psi(x) \in K_\mathfrak{p}[x]$ of degree m. In other words, $N(m,p)$ is simply the cardinality of the subset

$$\mathcal{I}(m,p) = \{\psi(x) \,:\, \psi(x) \text{ is monic, } \deg\psi(x) = m,\ \psi(x^p) - x \text{ is irreducible}\}$$

of the polynomial ring $K_\mathfrak{p}[x]$.

	m							
p	2	3	4	5	6	7	8	9
2	1	2	0	4	6	12	16	32
3	3	0	0	36	72	0	0	1,404
5	0	20	0	380	0	4,540	0	87,160
7	7	0	0	896	5,593	0	0	1,273,944
11	11	0	0	6,534	54,780	0	0	?

Table 3.1: $N(m, p)$ for some small values of m and p

Example 3.2. In Table 3.1 we list $N(m, p)$ for some small values of m and p, in the case when $K = \mathbb{Q}_p$.[1] We see for instance that $N(2, 2) = 1$. This is due to $\psi(x) = x^2 + 1$ being the only quadratic polynomial in $\mathbb{F}_2[x]$ such that $\psi(x^2) - x$ is irreducible over $\mathbb{F}_2$. On the other hand, for $K = \mathbb{Q}_3$ we obtain $N(2, 3) = 3$, since $\psi(x)$ can be chosen as any of the polynomials $x^2 + 2$, $x^2 + x + 1$, and $x^2 + 2x + 2$ in $\mathbb{F}_3[x]$.

As we can see from the table, $N(9, 11)$ is unknown. This number is however nonzero (since $\psi(x) = x^9 + x^2 + 4x + 1$ is an example of a polynomial such that $\psi(x^{11}) - x \in \mathbb{F}_{11}[x]$ is irreducible), and by the next theorem—which is a generalization of a theorem in Svensson [14]—we also know that it has to be a multiple of 11. ◊

Theorem 3.3. *Let K be a $\mathfrak{p}$-adic field, and define $N(m, p)$ as above. If $m \neq 1$ and $p \nmid m$, then $p \mid N(m, p)$.*

Proof. Let G be the set of all elements $a \in K_{\mathfrak{p}}$, such that $a^p = a$. Then $(G, +)$ is a cyclic group of order p, generated by the unity 1 of $K_{\mathfrak{p}}$. Put

$$K_{\mathfrak{p}}^{(m)}[x] = \{\psi(x) \in K_{\mathfrak{p}}[x] : \psi(x) \text{ is monic, } \deg \psi(x) = m\},$$

where $m \geq 2$, and define an action

$$G \times K_{\mathfrak{p}}^{(m)}[x] \ni (b, \psi(x)) \mapsto b.\psi(x) \in K_{\mathfrak{p}}^{(m)}[x]$$

of G on $K_{\mathfrak{p}}^{(m)}[x]$ by

$$b.\psi(x) = \psi(x + b) - b$$

for each $b \in G$. Let $G_{\psi(x)}$ denote the stabilizer of a given polynomial $\psi(x)$ in $K_{\mathfrak{p}}^{(m)}[x]$. Suppose $G_{\psi(x)} \neq \{0\}$. Then $G_{\psi(x)} = G$, whence

$$\psi(x + 1) = \psi(x) + 1. \tag{3.2}$$

[1] These figures are results of computer calculations.

But by plugging

$$\psi(x) = x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0$$

into (3.2) and then identifying the coefficients, we obtain especially

$$a_{m-1} = a_{m-1} + m,$$

which is impossible since $p \nmid m$. Hence if $p \nmid m$, then the length of any orbit in $K_{\mathfrak{p}}^{(m)}[x]$ under the action of G equals p, especially those who contain a polynomial $\psi(x)$ such that $\psi(x^p) - x$ is irreducible over $K_{\mathfrak{p}}$. This proves the theorem, since if $f(x) = \psi(x^p) - x$ is irreducible, then

$$b.\psi(x^p) - x = \psi(x^p + b) - b - x = \psi((x + b)^p) - (x + b) = f(x + b)$$

is also irreducible. □

Remark 1. We must exclude the case when $m = 1$, since it is easily shown that $N(1, p) = p - 1$ for all p, if $K_{\mathfrak{p}} = \mathbb{F}_p$.

Remark 2. Computer calculations (for the case $K_{\mathfrak{p}} = \mathbb{F}_p$) indicate that $p \,|\, N(m, p)$ is valid most of the time, even though $p \,|\, m$. The only known counterexample is when $m = p = 2$, see Example 3.2.

4 Estimations and Plots

Let us assume that $K = \mathbb{Q}_p$, from now on. In Khrennikov and Svensson [9], a question about the asymptotic behavior of $N(m, p)$ is raised, namely what one can say about

$$\frac{1}{\pi(n)} \sum N(m, p),$$

where the sum is taken over all primes p such that $p \leq n$, and $\pi(n)$ denotes the number of primes not exceeding n.

We recall (from e.g. Lidl and Niederreiter [10, Theorem 3.25]) that the number $I_q(n)$ of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ is

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

where μ denotes the Möbius function. Thus, if pm is a large number, we can do the approximation

$$I_p(pm) \approx \frac{p^{pm-1}}{m},$$

i.e. there are about p^{pm-1}/m monic irreducible polynomials of degree pm in $\mathbb{F}_p[x]$. If one randomly picks a monic polynomial of degree pm, not having $0 \in \mathbb{F}_p$ as a zero, the probability for it to be irreducible is

$$\frac{p^{pm-1}/m}{p^{pm-1}(p-1)} = \frac{1}{m(p-1)}.$$

In $\mathbb{F}_p[x]$, there are $p^{m-1}(p-1)$ monic polynomials such that $f(x) = \psi(x^p) - x$ for some polynomial $\psi(x) \in \mathbb{F}_p[x]$ of degree m, where $\psi(0) \neq 0$. Thus a rough estimation would be

$$N(m,p) \approx \frac{p^{m-1}(p-1)}{m(p-1)} = \frac{p^{m-1}}{m},$$

when mp is large. Thereby

$$\frac{1}{\pi(n)} \sum_{p \leq n} N(m,p) \approx \frac{1}{m\,\pi(n)} \sum_{p \leq n} p^{m-1}. \tag{4.1}$$

By Nyqvist [12, Theorem 4.19],

$$\frac{1}{\pi(n)} \sum_{p \leq n} p^{m-1} \sim \frac{n^{m-1}}{m},$$

which together with (4.1) yields

$$\frac{1}{\pi(n)} \sum_{p \leq n} N(m,p) \sim \frac{n^{m-1}}{m^2}.$$

Thus, for a fixed degree m of $\psi(x)$,

$$\frac{1}{\pi(n)} \sum_{p \leq n} N(m,p) = O(n^{m-1}). \tag{4.2}$$

Of course, the above reasoning has to be taken with a pinch of salt, since the polynomials $\psi(x^p) - x$ are not picked randomly—in some cases, the irreducible polynomials avoid those kind of polynomials. For instance, $N(4,p) = 0$ for all primes p (see Example 5.5 below). On the other hand, no p is known such that $N(m,p) = 0$, if $m \equiv 1 \pmod 4$, see the remark at the end of this paper.

In Figure 4.1 on the next page we see a plot of the function

$$n \mapsto \frac{1}{\pi(n)} \sum_{p \leq n} N(2,p)$$

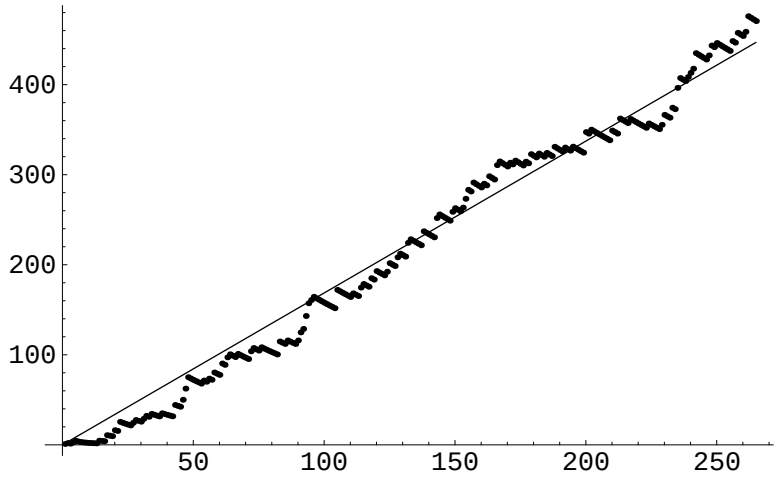

Figure 4.1: Plot of $n \mapsto \pi(n)^{-1} \sum_{p \leq n} N(2, p)$, along with a fitting line

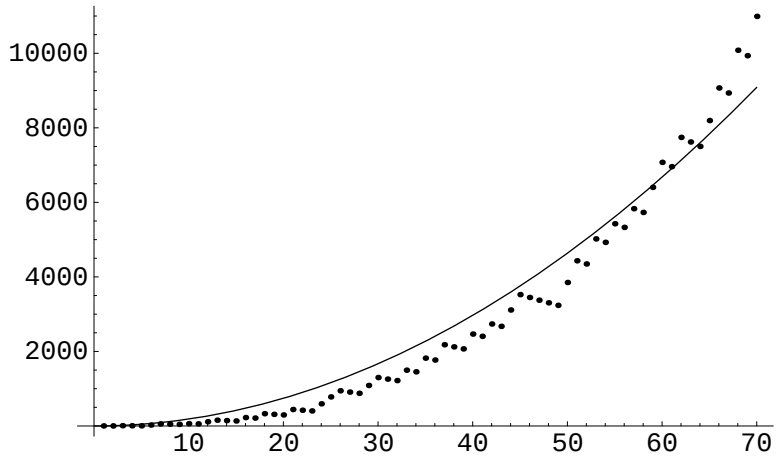

Figure 4.2: Plot of $n \mapsto \pi(n)^{-1} \sum_{p \leq n} N(3, p)$, along with a fitting curve

for the 265 first primes (i.e. $p \leq 1697$). The straight line in figure is of the form $y = kx$, where k is calculated by the method of least squares. It turns out that $k \approx 1.68646$.

Figure 4.2 on the preceding page displays, on the other hand, the plot of

$$n \mapsto \frac{1}{\pi(n)} \sum_{p \leq n} N(3, p).$$

Due to the time complexity, the calculations here only rely on the 70 first primes (i.e. $p \leq 349$). The fitting curve is the least squares fit of the form $y = kx^2$. Here $k \approx 1.85425$.

The empirical investigations above should be compared to (4.2). However, we would like to point out that the amount of data behind these calculations is too small to make any general conclusions about the fitting line/curve.

5 Calculations

To calculate $N(m, p)$ for a given m and p, we could simply use brute force, and examine for all monic $\psi(x) \in \mathbb{F}_p[x]$ of degree m, whether $f(x) = \psi(x^p) - x$ is irreducible or not. But then the time complexity will increase rapidly, the larger m or p gets, so we need to reduce the calculations somewhat. The simplest restriction we can do is to assume that the constant term of $\psi(x)$ is non-zero, since otherwise $f(x)$ would have x as a factor. To reduce the calculations a little bit more, we can use the following result.

Lemma 5.1. *Let $\psi(x) \in \mathbb{F}_p[x]$ be monic of degree m. For every $b \in \mathbb{F}_p$, let $\psi_b(x) = \psi(x + b) - b$. Then there is exactly one $b \in \mathbb{F}_p$ such that the coefficient of x^{m-1} of $\psi_b(x)$ equals 0, provided that $p \nmid m$.*

Proof. The coefficient of x^{m-1} of $\psi_b(x)$ equals $mb + a_{m-1}$. Since $p \nmid m$, the equation $mb + a_{m-1} = 0$ has exactly one solution for b in $\mathbb{F}_p$. □

Note that $\psi_b(x)$ in the lemma above is the result obtained when the element b of the group $(\mathbb{F}_p, +)$ acts on $\psi(x)$ as described in the proof of Theorem 3.3. Due to this, if $\psi(x) \in \mathbb{F}_p[x]$ is monic of degree m and $\psi(x^p) - x$ is irreducible, then each one of the p polynomials in the same orbit has the same property. Therefore it is enough (when $p \nmid m$) to check all polynomials

$$\psi(x) = x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0$$

where $a_{m-1} = 0$. The number of found polynomials of this kind is then multiplied by p.

For certain values of m and p, we do not need to investigate possible polynomials for irreducibility, since there there are none to be found.

Theorem 5.2. *Let m be a positive integer, p an odd prime, and $n = mp$. Then $N(m, p) = 0$, whenever*

$$(n+1)(n(p-1)-4) \not\equiv 0 \pmod 8.$$

Before we prove this theorem, we need to do some preparations. First, we recall the notion of the resultant of two polynomials: Let F be any field, and $q(x), r(x) \in F[x]$ two polynomials. Suppose

$$q(x) = a(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) \quad \text{and} \quad r(x) = b(x-\beta_1)(x-\beta_2)\dots(x-\beta_m)$$

over a field that is large enough to contain the splitting fields of both $q(x)$ and $r(x)$. Then the resultant of $q(x)$ and $r(x)$ is given by

$$\operatorname{res}(q,r) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = a^m \prod_{i=1}^{n} r(\alpha_j) = b^n (-1)^{mn} \prod_{j=1}^{m} q(\beta_j).$$

where a and b are the leading coefficients of $q(x)$ and $r(x)$, respectively. (Alternatively, one can define $\operatorname{res}(q,r)$ as the determinant of the eliminant matrix of $q(x)$ and $r(x)$, see e.g. Ribenboim [13, p. 22].)

The discriminant of a polynomial $f(x) \in F[x]$ of degree n and leading coefficient c can now be defined, by means of the discriminant, as

$$\operatorname{disc}(f) = \frac{1}{c} \cdot (-1)^{n(n-1)/2} \cdot \operatorname{res}(f, f'),$$

where $f'(x)$ is the (formal) derivative of $f(x)$.

Lemma 5.3. *Let F be a field with $\operatorname{char} F = p > 0$. If $f(x) = \psi(x^p) - x$ for some monic polynomial $\psi(x) \in F[x]$, then*

$$\operatorname{disc}(f) = (-1)^{n(n+1)/2},$$

where $n = p \cdot \deg \psi(x)$.

Proof. We have $f'(x) = -1$ and thereby $\operatorname{res}(f, f') = (-1)^n$, from which the lemma follows. □

Next we state a lemma that can be found, along with a proof, in von zur Gathen [16] (see also Swan [15]).

Lemma 5.4. *Let $f(x) \in \mathbb{F}_q[x]$ be a monic square-free polynomial of degree n, where q is supposed to be odd. Suppose furthermore, that the factorization of $f(x)$ into irreducibles over $\mathbb{F}_q$ consists of r factors. Then r is odd, if and only if* $\operatorname{disc}(f)^{(q-1)/2} = (-1)^{n+1}$.

We are now prepared to prove the theorem on the previous page.

Proof of Theorem 5.2. Suppose $N(m,p) > 0$. Then there is at least one monic polynomial $\psi(x) \in \mathbb{F}_p[x]$ of degree $m \geq 1$, such that $\psi(x^p) - x$ is irreducible over $\mathbb{F}_p$. We note that the degree of this polynomial is $mp = n$. By Lemma 5.4 and Lemma 5.3,

$$(-1)^{n+1} = [\operatorname{disc}(\psi(x^p)-x)]^{(p-1)/2} = \left((-1)^{n(n+1)/2}\right)^{(p-1)/2} = (-1)^{n(n+1)(p-1)/4},$$

whence

$$\frac{n(n+1)(p-1)}{4} - n - 1 = 2k,$$

for some integer k. But then $(n+1)(n(p-1)-4)$ is divisible by 8. □

Corollary. *Depending of the remainder of m when divided by* 4*, we can make the following conclusions:*

(i) *If $m \equiv 0 \pmod 4$, then $N(m,p) = 0$ for all $p \neq 2$;*
(ii) *If $m \equiv 2 \pmod 4$, then $N(m,p) = 0$ whenever $p \equiv 1 \pmod 4$;*
(iii) *If $m \equiv 3 \pmod 4$, then $N(m,p) = 0$ whenever $p \equiv 3 \pmod 4$.*

Example 5.5. According to the Corollary, $N(4,p) = 0$ whenever p is odd. If $p = 2$, we have to check $g(x) = \psi(x^2) - x$ for irreducibility, where

$$\psi(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + 1, \qquad a_1, a_2, a_3 \in \mathbb{F}_2.$$

If all or exactly one of a_1, a_2, and a_3 is non-zero, then $g(x)$ has a zero in $\mathbb{F}_2$. The remaining four polynomials to check, i.e.

$$\begin{aligned}
x^8 + x^4 + x^2 + x + 1 &= (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)\\
x^8 + x^6 + x^2 + x + 1 &= (x^3 + x + 1)(x^5 + x^2 + 1)\\
x^8 + x^6 + x^4 + x + 1 &= (x^3 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1)\\
x^8 + x + 1 &= (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1)
\end{aligned}$$

are all reducible. Hence $N(4,p) = 0$ for all p. ◊

Remark. A natural question is whether 'whenever' can be replaced with the phrase 'if and only if' in (ii) and (iii) of the Corollary above. We believe that this is possible for the statement (iii).

When it comes to (ii), there are a number of known counterexamples, but all of them occurs when $m = 2$. For instance, when it comes to primes less than 100, $N(2, p) = 0$ if $p \in \{19, 23, 31, 47, 67, 83\}$, and among the 265 primes used for Figure 4.1 on page 6, there are 44 primes such that $N(2, p) = 0$ even though $p \equiv 3 \pmod 4$. If $m > 2$, no counterexample is known.

It is also an open question if $N(m, p) > 0$ for all $p \neq 2$, if $m \equiv 1 \pmod 4$.

References

[1] V. Anashin, *Uniformly Distributed Sequences of p-adic Integers, ii*, Discrete Math. Appl. **12** (2002), no. 6, 527–590.

[2] D. K. Arrowsmith and F. Vivaldi, *Geometry of p-adic Siegel Discs*, Physica D **71** (1994), 222–236.

[3] R. Benedetto, *Hyperbolic Maps in p-adic Dynamics*, Ergodic Theory and Dynamical Systems **21** (2001), 1–11.

[4] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[5] A. Yu. Khrennikov, *Non-archimedean Analysis: Quantum Paradoxes, Dynamical systems and Biological Models*, Kluwer Academic Publishers, 1997.

[6] ———, *p-adic Discrete Dynamical Systems and Their Applications in Physics and Cognitive Sciences*, Russian Journal in Mathematical Physics **11** (2004), no. 1, 45–70.

[7] A. Yu. Khrennikov and M. Nilsson, *On the Number of Cycles of p-adic Dynamical Systems*, Journal of Number Theory **90** (2001), no. 2, 255–264.

[8] ———, *Behaviour of Hensel perturbations of p-adic monomial dynamical systems*, Analysis Mathematica **29** (2003), 107–133.

[9] A. Yu. Khrennikov and P.-A. Svensson, *Attracting fixed points of polynomial systems in fields of p-adic numbers*, Izvestiya RAN: Ser. Mat. **71** (2007), no. 4, 103–114.

[10] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, revised ed., Cambridge University Press, 1994.

[11] J. Lubin, *Nonarchimedean Dynamical Systems*, Compositio Math. **94** (1994), 321–346.

[12] R. Nyqvist, *Asymptotic Behavior of Number of Cycles of Dynamical Systems in Finite Fields*, Proceedings of the Jangjeon Mathematical Society **10** (2007), no. 1, 1–6.

[13] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer Verlag, 2001.

[14] P.-A. Svensson, *Dynamical Systems in Local Fields of Characteristic Zero*, Ph.D. thesis, Växjö University, 2004.

[15] R. G. Swan, *Factorization of Polynomials over Finite Fields*, Pacific Journal of Mathematics **12** (1962), no. 3, 1099–1106.

[16] J. v. z. Gathen, *Irreducible Trinomials Over Finite Fields*, Mathematics of Computation **72** (2003), no. 244, 1987–2000.