ANNALES MATHÉMATIQUES BLAISE PASCAL

MARCUS NILSSON

Cycles of monomial and perturbated monomial p-adic dynamical systems

Annales mathématiques Blaise Pascal, tome 7, n° 1 (2000), p. 37-63

<http://www.numdam.org/item?id=AMBP_2000__7_1_37_0>

Ann. Math. Blaise Pascal, Vol. 7, N° 1, 2000, pp.37-63

Cycles of monomial and perturbated monomial p-adic dynamical systems

Marcus Nilsson

Abstract

Discrete dynamical systems over the field of p-adic numbers are considered. We will concentrate on the study of periodic points of monomial and perturbated monomial system. Similarities between these two kinds of systems will be investigated. The conditions of the perturbation and the choice of the prime number p plays an important role here. Our considerations will lead to formulas for the number cycles of a specific length and for the total number of cycles. We will also study the distribution of cycles in the different p-adic fields.

1 Introduction

Discrete dynamical systems have a lot of applications, for example in biology and physics, [7]. Dynamical systems over the p-adic numbers (see for example [11] and [2] for a general introduction to p-adic analysis) can also be used for modelling psychological and sociological phenomena, see [7] and [6]. Especially, in [6] a modell of the human memory, using p-adic dynamical system, is presented.

The most studied p-adic dynamical systems are the so called monomial systems. A (discrete) monomial system is defined by a function $f(x) = x^n$. In [9] there is a stochastic approach to such systems. In [10] dynamical systems (not only monomial) over finite field extensions of the p-adic numbers are considered.

By using theorems from number theory, we will be able to prove formulas for the number of cycles of a specific length to a given system and the total number of cycles for monomial dynamical systems. We will also investigate the number of cycles of a specific length to a system for different choices of the prime number p. Here some remarkable asymptotical results occur.

We will also study perturbated monomial dynamical systems defined by functions, $f_q(x) = x^n + q(x)$, where the perturbation $q(x)$ is a polynomial whose coefficients have small p-adic absolute value. We investigate the connection between monomial and perturbated monomial systems. In this investigations we will use Hensel's lemma. As in the monomial case the interesting dynamic of some perturbated systems are located on the unit sphere in $\mathbb{Q}_p$. Sufficient conditions on the perturbation for the two systems to have similar properties are derived. By similar properties we mean that there is a one to one correspondence between fixed points and cycles of the two kinds of systems.

2 Properties of monomial systems

Everywhere below we will use the following notations: The field of p-adic numbers is denoted by $\mathbb{Q}_p$, the ring of p-adic integers is denoted $\mathbb{Z}_p$. We will use $|\cdot|_p$ to denote the p-adic valuation. The sphere, ball and open ball with radius ρ and center at a, with respect to the p-adic metric induced by the p-adic valuation, are denoted by $S_\rho(a)$, $U_\rho(a)$ and $U_\rho^-(a)$ respectively. We use the notation $a \equiv b \,(\mathrm{mod}\, p^k\mathbb{Z}_p)$ if and only if $|a-b|_p \leqslant 1/p^k$.

In this article we will first consider the dynamical systems $f : \mathbb{Q}_p \to \mathbb{Q}_p$ where

$$f(x) = x^n \tag{2.1}$$

and $n \in \mathbb{N}$ such that $n \geqslant 2$. In [7] there is an extensive investigation of these systems. Most of the theorems in this section come from this book. In the following we will use the notation f^r to denote the composition of f with itself r times. By $\lim_{r\to\infty} f^r(x) = x_0$ we mean that $\lim_{r\to\infty} |f^r(x) - x_0|_p = 0$.

Definition 2.1. Let $x_r = f^r(x_0)$. If $x_r = x_0$ for some positive integer r then x_0 is said to be a *periodic point* of f. If r is the least natural number with this property, we call r the *period* of x_0. A periodic point of period 1 is called a *fixed point* of f.

Definition 2.2. Let r be a positive integer. The set $\gamma = \{x_0, \ldots, x_{r-1}\}$ of periodic points of period r is said to be a *cycle* to the dynamical system determined by f if $x_0 = f(x_{r-1})$ and $x_j = f(x_{j-1})$ for $1 \leqslant j \leqslant r-1$. The *length of the cycle* is the number of elements in γ.

Definition 2.3. A fixed point x_0 to a function f is said to be an *attractor* if there exists a neighbourhood $V(x_0)$ such that for every $y \in V(x_0)$ holds that

$$\lim_{r\to\infty} f^r(y) = x_0.$$

By the basis of attraction we mean the set

$$A(x_0) = \{y \in \mathbb{Q}_p; \lim_{r\to\infty} f^r(y) = x_0\}.$$

It is known that for a monomial system (2.1) 0 and ∞ are attractors and that $A(0) = U_1^-(0)$ and $A(\infty) = \mathbb{Q}_p \setminus U_1(0)$. The rest of the periodic points are located on $S_1(0)$.

Fixed points of (2.1) on $S_1(0)$ are solutions of the equation $x^{n-1} = 1$, hence $(n-1)$th roots of unity. Periodic points, with period $r \geqslant 2$, are solutions of

$$x^{n^r-1} = 1. \tag{2.2}$$

It follows directly from the definition of the periodic points that the set of solutions to equation (2.2) not only contains the periodic points of period r but also the periodic points with periods that divides r. We have the following theorem about the roots of (2.2) in $\mathbb{Q}_p$. (We use $\gcd(m,n)$ to denote the greatest common divisor of two positive integers m and n.)

Theorem 2.4. *The equation $x^k = 1$ has $\gcd(k, p-1)$ solutions in $\mathbb{Q}_p$ when $p > 2$. If $p = 2$ then $x^k = 1$ has two solutions ($x = 1$ and $x = -1$) if k is even and one solution ($x = 1$) if k is odd.*

Let $N(n,r,p)$ denote the number of periodic points of period r in (2.1). Each cycle of length r contains r periodic points with period r. If we denote by $K(n,r,p)$ the number of cycles of length r then

$$K(n,r,p) = N(n,r,p)/r. \tag{2.3}$$

In [7] we find the following theorem about the existens of cycles.

Theorem 2.5. *Let $p > 2$ and let $m_j = \gcd(n^j - 1, p-1)$. The dynamical system $f(x) = x^n$ has r-cycles ($r \geqslant 2$) in $\mathbb{Q}_p$ if and only if m_r does not divide any m_j, $1 \leqslant j \leqslant r-1$.*

We have the following relation between m_j, $N(n,j,p)$ and $K(n,j,p)$

$$m_j = \sum_{i|j} N(n,i,p) = \sum_{i|j} iK(n,i,p). \tag{2.4}$$

Here follow some more facts about the monomial systems:

Theorem 2.6. *If $p = 2$ then the dynamical system* (2.1) *has no cycles of order $r \geqslant 2$.*

Proof. If n is even then it follows from Theorem 2.4 that (2.1) has only one fixed point in $\mathbb{Q}_2$. It also follows that n^r is even for all $r \geqslant 2$ and this implies that $f^r(x) = x^{n^r}$ only has one fixed point in $\mathbb{Q}_2$ which also is the fixed point of $f(x) = x^n$. Hence f has no periodic points of period r. The case when n is odd is proved in a similar way. □

Theorem 2.7. *Let x and y be two nth roots of unity in $\mathbb{Q}_p$ and let $x \neq y$. If $p > 2$ then $|x - y|_p = 1$. If $p = 2$ then $|x - y|_p = 1/2$.*

3 Number of cycles

In this section we will derive a formula for the number of cycles of the dynamical system (2.1). To do this we need some results from number theory. See for example [5] and [1]. Let us begin with a review of the Möbius inversion formula.

Definition 3.1. Let $n \in \mathbb{Z}^+$ then we can write $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where p_j, $1 \leqslant j \leqslant r$ are prime numbers and r is the number of different primes. The function μ on $\mathbb{Z}^+$ defined by $\mu(1) = 1$, $\mu(n) = 0$ if any $e_j > 1$ and $\mu(n) = (-1)^r$, if $e_1 = \ldots = e_r = 1$ is called the *Möbius function.*

The Möbius function has the following property

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1, \end{cases}$$

where d is a positiv divisor of n.

Möbius inversion formula. *Let f and g be functions defined for each $n \in \mathbb{Z}^+$. Then,*

$$f(n) = \sum_{d|n} g(d) \tag{3.1}$$

if and only if

$$g(n) = \sum_{d|n} \mu(d) f(n/d). \tag{3.2}$$

We are now ready to derive a formula for the number of periodic points to the monomial system (2.1). Observe that according to Theorem 2.4 we have for $p > 2$ that $\gcd(n^r - 1, p - 1)$ gives the number of periodic points of period r and periods that divides r. We have the following theorem.

Theorem 3.2. *Assume that $p > 2$. The number of periodic points of period r of (2.1) is then given by*

$$N(n, r, p) = \sum_{d|r} \mu(d) \gcd(n^{r/d} - 1, p - 1). \tag{3.3}$$

Proof. The theorem follows directly from Möbius inversion formula. □

The number of cycles of lenght r of (2.1) is given by

$$K(n, r, p) = \frac{N(n, r, p)}{r} = \frac{1}{r} \sum_{d|r} \mu(d) \gcd(n^{r/d} - 1, p - 1). \tag{3.4}$$

Remark 3.3. If we assume that $r \geqslant 2$ then it follows from Theorem 2.6 that $N(n, r, 2) = 0$. If we take $p = 2$ in (3.3) we get that $N(n, r, 2) = 0$. Hence we can use formula (3.3) also for $p = 2$ if $r \geqslant 2$.

Remark 3.4. Formula (3.4) implies the following result which may be interesting for number theory: For every natural number $n \geqslant 2$ and prime number $p > 2$ the number $N(n, r, p)$ is divisible by r.

We will now determine the maximum of numbers of cycles, of any length, in $\mathbb{Q}_p$ for a fixed p. Let $n \geqslant 2$ be a natural number. Denote by $p^*(n)$ the number we get if we remove, from the prime factorisation of $p - 1$, the factors dividing n. That is $p^*(n)$ is the largest divisor of $p - 1$ which is relatively prime to n. We also recall the definition of Euler's φ-function and Euler's Theorem.

Definition 3.5. Let n be a positive integer. Henceforth, we will denote by $\varphi(n)$ the number of natural numbers less than n which are relatively prime to n. The function φ is called *Euler's φ-function.*

An equivalent definition of φ is that $\varphi(n)$ is the number of elements in $\mathbb{F}_n$ which are not divisors of zero. If p is a prime number then $\varphi(p^l) = p^{l-1}(p - 1)$.

Theorem 3.6 (Euler's Theorem). *If a is an integer relatively prime to b then $a^{\varphi(b)} \equiv 1 \pmod{b}$.*

Lemma 3.7. *With the above notation we have for each* $r \in \mathbb{N}$

$$\gcd(n^r - 1, p - 1) = \gcd(n^r - 1, p^*(n)). \tag{3.5}$$

Proof. Since $n^r - 1 \equiv -1 \pmod q$ if $q \mid n$ it follows that we can remove the prime factors from $p-1$ which divides n and it would not change the value of $\gcd(n^r - 1, p - 1)$. □

Lemma 3.8. *There is a least integer* $\hat{r}(n)$, *such that*

$$\gcd(n^{\hat{r}(n)} - 1, p^*(n)) = p^*(n).$$

Proof. Since $\gcd(n, p^*(n)) = 1$ it follows from Theorem 3.6 that $n^{\varphi(p^*(n))} \equiv 1 \pmod{p^*(n)}$. It is then clear that there exists a smallest $\hat{r}(n)$ such that $n^{\hat{r}(n)} \equiv 1 \pmod{p^*(n)}$ and $\hat{r}(n) \leqslant \varphi(p^*(n))$. (It is also true that $\hat{r}(n) \mid \varphi(p^*(n))$.) Hence $p^*(n) \mid n^{\hat{r}(n)} - 1$ and the theorem follows. □

Theorem 3.9. *Let* $p > 2$ *be a fixed prime number, let* $n \geqslant 2$ *be a natural number. If* $R \geqslant \hat{r}(n)$ *then*

$$\sum_{r=1}^{R} N(n, r, p) = p^*(n). \tag{3.6}$$

Proof. We first prove that $N(n, r, p) = 0$ if $r > \hat{r}(n)$. Since $\gcd(n^{\hat{r}(n)} - 1, p - 1) = p^*(n)$ and every $m_r = \gcd(n^r - 1, p - 1) \mid p^*(n)$, $r > \hat{r}(n)$, it follows from Theorem 2.5 that $N(n, r, p) = 0$.

Next we want to prove that if $r \nmid \hat{r}(n)$ then $N(n, r, p) = 0$. Let l_1 be a divisor of $p^*(n)$. Let q be the least integer such that $n^q - 1 \equiv 0 \pmod{l_1}$. Since $n^{\hat{r}(n)} \equiv 1 \pmod{p^*(n)}$ it follows that $n^{\hat{r}(n)} \equiv 1 \pmod{l_1}$. By the division algorithm we have $\hat{r}(n) = kq + r_1$. This implies that

$$1 \equiv n^{kq+r_1} \equiv (n^q)^k n^{r_1} \equiv n^{r_1} \pmod{l_1}.$$

Since q was the least non-negative integer such that $n^q \equiv 1 \pmod{l_1}$ it follows that $r_1 = 0$. That is $q \mid \hat{r}(n)$.

The only possible values of $\gcd(n^r - 1, p - 1)$ are the divisors of $p^*(n)$. In the paragraph above we showed that the least number q such that $\gcd(n^q - 1, p - 1) = l_1$, where $l_1 \mid p^*(n)$, must be a divisor of $\hat{r}(n)$. Hence if $r \nmid \hat{r}(n)$ then $N(n, r, p) = 0$.

So far we have proved that

$$\sum_{r=1}^{R} N(n, r, p) = \sum_{r \mid \hat{r}(n)} N(n, r, p).$$

We have left to prove that

$$\sum_{r|\hat{r}(n)} N(n,r,p) = p^*(n).$$

From (2.4) we know that

$$\gcd(n^r - 1, p^*(n)) = \sum_{d|r} N(n,d,p)$$

If we set $r = \hat{r}(n)$ we have proved the theorem. □

Corollary 3.10. *Let $p > 2$. The dynamical system (2.1) has $p^*(n)$ periodic points in $\mathbb{Q}_p$.*

Theorem 3.11. *Let $p > 2$. The total number, $K_{Tot}(n,p)$, of cycles of (2.1) is given by*

$$K_{Tot}(n,p) = \sum_{r|\hat{r}} K(n,r,p) = \sum_{r|\hat{r}} \frac{1}{r} \sum_{d|r} \mu(d) \gcd(n^{r/d} - 1, p-1). \quad (3.7)$$

Proof. From the proof of Theorem 3.9 we know that we only have cycles of lengths that divides $\hat{r}(n)$. From (3.4) it follows that

$$K(n,r,p) = \frac{1}{r} \sum_{d|r} \mu(d) \gcd(n^{r/d} - 1, p-1).$$

The theorem is proved. □

Example 3.12. Let us consider the monomial system $f(x) = x^2$ $(n = 2)$. If $p = 137$ then it follows from Corollary 3.10 that the dynamical system has $p^*(2) = 17$ periodic points and from Theorem 3.11 it follows that it has $K_{\text{Tot}}(2, 137) = 3$ cycles. In fact the monomial system $f(x) = x^2$ has one cycle of length 1 (one fixed point) and two cycles of length 8.

If we consider the same system, but let $p = 1999$ instead, then the number of periodic points is $p^*(2) = 999$ and the number of cycles is $K_{\text{Tot}}(2, 1999) = 31$. In fact the system has one cycle of length 1, 2, 6 and 18 and also 27 cycles of length 36.

Example 3.13. Let us now instead consider the dynamical system $f(x) = x^3$. If $p = 137$ then there are 136 periodic points and 13 cycles. In fact we have two fixed points, three cycles of length 2 and 8 cycles of length 16. If instead $p = 1999$ then there are two fixed points and four cycles of length 18, so we have 74 periodic points and six cycles.

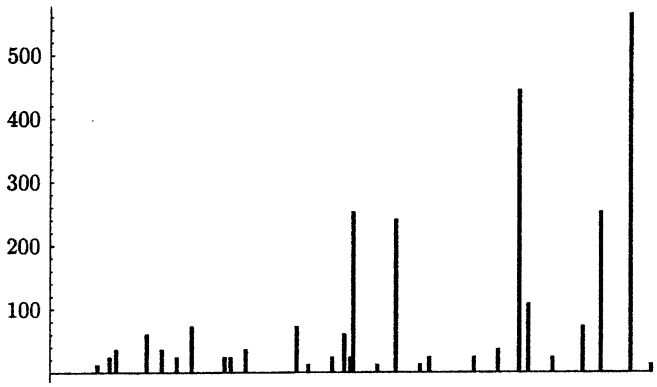

Figure 4.1: The number of periodic points of period 12 for the first 200 primes.

4 Distribution of cycles

In this section we will discuss the distribution of periodic points and cycles, of a specific period and length, in $\mathbb{Q}_p$ for different choices of p. We denote by $\tau(m)$ the number of positive divisors of the positive integer m.Henceforth we let p_M denote the Mth prime and P_M denote the set of the first M prime numbers.

Example 4.1. Let $f(x) = x^2$. We are interested in how many periodic points of period 12 there are to this system for different primes p. We can use formula (3.3) and plot the number of periodic points of period 12 as a function of p. See Figure 4.1 and Figure 4.2. Let

$$S(M, 12) = \sum_{p \in P_M} N(2, 12, p).$$

In Figure 4.3 we have plot $S(M, 12)$ for the first 10,000 primes (that is $M \leqslant 10,000$). It seems that the asymptotical inclination of the graph should be a constant.

We will prove that the asymptotical inclination is in fact a constant and that this constant can be expressed rather easily. We will prove the following theorem:

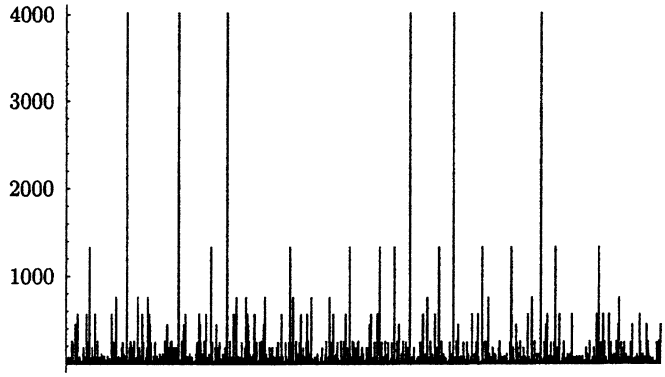

Figure 4.2: The number of periodic points of period 12 for the first 10,000 primes.

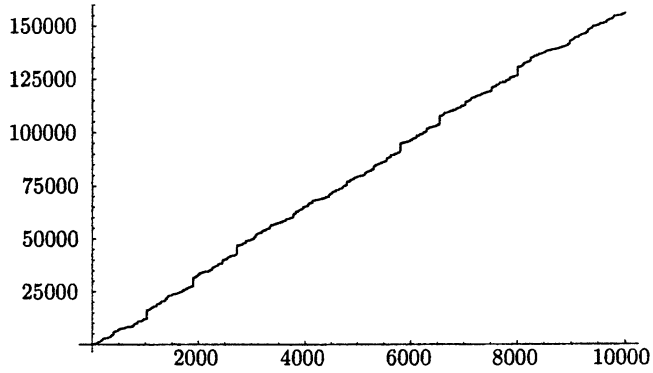

Figure 4.3: The graph of $S(M, 12)$ for $M \leqslant 10,000$.

Theorem 4.2. *Let n and r be positive integers such that $n \geqslant 2$ and $r \geqslant 2$. We then have*

$$\lim_{M\to\infty} \frac{1}{M} \sum_{p\in P_M} \sum_{d|r} \mu(d) \gcd(n^{r/d} - 1, p - 1) = \sum_{d|r} \mu(d)\tau(n^{r/d} - 1),$$

where μ is Möbius function.

Before we start to prove this theorem we need some results from number theory. We will use the arithmetical functions φ, μ and τ.

We first recall some simple connections between φ and μ which will be useful to us later on, see [1].

Theorem 4.3. *For each positive integer n we have*

$$\sum_{d|n} \varphi(d) = n. \tag{4.1}$$

By Möbius formula we have

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}. \tag{4.2}$$

We will also need some results from number theory concerning the distribution of primes. Henceforth we will use the notation $f(x) \sim g(x)$ if $f(x)/g(x) \to 1$ when $x \to \infty$.

Definition 4.4. For $x > 0$ we define $\pi(x)$ to be the number of primes less or equal to x.

Theorem 4.5 (Prime number theorem). *Let $\pi(x)$ be as above then*

$$\pi(x) \sim \frac{x}{\log x} \tag{4.3}$$

The proof of this theorem can be found in [4], [13] and [1].

Definition 4.6. Let k and a be positive integers such that $\gcd(a, k) = 1$. Let $\pi_{a,k}(x)$ be the number of primes p less or equal to x such that $p \equiv a \pmod{k}$.

The number $\pi_{a,k}(x)$ is the number of primes less or equal to x which can be written as $kn + a$, where n is a natural number. Dirichlet proved the following theorem:

Theorem 4.7. *If* $\gcd(a,k)=1$ *then there are infinitely many prime numbers* p *which can be written* $p=kn+a$.

The following theorem is a generalization of the prime number theorem.

Theorem 4.8. *Let* $\pi_{a,k}(x)$ *be as above. Then,*

$$\pi_{a,k}(x) \sim \frac{\pi(x)}{\varphi(k)}. \tag{4.4}$$

A proof of this theorem can be found in [14].

We are now ready to prove the main part of Theorem 4.2. We state it as a theorem.

Theorem 4.9. *Let* m *be a positive integer then*

$$\lim_{M\to\infty} \frac{1}{M} \sum_{p\in P_M} \gcd(m,p-1) = \tau(m). \tag{4.5}$$

Proof. Let

$$B(m,M) = \sum_{p\in P_M} \gcd(m,p-1).$$

The possible values of $\gcd(m,p-1)$ are of course the divisors of m. Let d be a divisor of m and denote by $A(d,M)$ the number of primes $p\in P_M$ satisfying $\gcd(m,p-1)=d$. It is easy to see that

$$B(m,M) = \sum_{d|m} dA(d,M) \tag{4.6}$$

Let $\pi(d,M)=\pi_{1,d}(p_M)$. That is, $\pi(d,M)$ is the number of prime numbers $p\in P_M$ such that $d \mid p-1$. Observe that $\pi(1,M)=\pi(p_M)$. In the first part of this proof we will derive a relation between $A(d,M)$ and $\pi(d,M)$.

The set $\pi(d,M)$ contains not only the set $A(d,M)$ but also all sets $A(k,M)$ where $d \mid k$. We can write this

$$\pi(d,M) = \sum_{rd|m} A(dr,M). \tag{4.7}$$

We will now prove that this implies

$$A(d,M) = \sum_{kd|m} \mu(k)\pi(dk,M). \tag{4.8}$$

From (4.7) it follows that

$$\pi(dk, M) = \sum_{rdk|m} A(dkr, M).$$

The right-hand side of (4.8) is therefore

$$\sum_{kd|m} \mu(k) \sum_{rdk|m} A(dkr, M) = \sum_{kd|m} \sum_{rdk|m} \mu(k) A(dkr, M).$$

Let $k' = rk$. We can then write

$$\sum_{kd|m} \mu(k) \sum_{rdk|m} A(dkr, M) = \sum_{k'd|m} \sum_{k|k'} \mu(k) A(dk', M)$$
$$= \sum_{k'd|m} A(dk', M) \sum_{k|k'} \mu(k).$$

By the properties of the Möbius function we have

$$\sum_{k|k'} \mu(k) = \begin{cases} 0 \text{ if } k' > 1, \\ 1 \text{ if } k' = 1. \end{cases}$$

Therefore

$$\sum_{kd|m} \mu(k) \sum_{rdk|m} A(dkr, M) = \sum_{kd|m} \mu(k) \sum_{dk'|m} A(dk', M) = A(d, M).$$

Formula (4.8) is proved. If we use (4.8) we can write (4.6) as

$$B(m, M) = \sum_{d|m} d \sum_{kd|m} \mu(k) \pi(dk, M)$$
$$= \sum_{d|m} \sum_{kd|m} d\mu(k) \pi(dk, M).$$

Let $r = kd$. It is easy to see that

$$B(m, M) = \sum_{r|m} \sum_{k|r} \frac{r}{k} \mu(k) \pi(\frac{r}{k} k, M) = \sum_{r|m} \sum_{k|r} \frac{r}{k} \mu(k) \pi(r, M)$$
$$= \sum_{r|m} \pi(r, M) \sum_{k|r} \frac{r}{k} \mu(k).$$

From (4.2) we get

$$B(m,M)=\sum_{r|m}\pi(r,M)\varphi(r).$$

Since

$$\lim_{M\to\infty}\frac{1}{M}\sum_{r|m}\pi(r,M)\varphi(r)=\sum_{r|m}\lim_{M\to\infty}\frac{1}{M}\pi(r,M)\varphi(r)$$

and the sum has $\tau(m)$ elements we have proved the theorem if we can show that

$$\lim_{M\to\infty}\frac{1}{M}\pi(r,M)\varphi(r)=1. \tag{4.9}$$

Since

$$\pi(r,M)\varphi(r)=\frac{\pi(r,M)\varphi(r)}{\pi(p_M)}\pi(p_M),$$

and $\pi(p_M)=M$ it follows from Theorem 4.8 that

$$\lim_{n\to\infty}\frac{1}{M}\pi(r,M)\varphi(r)=1.$$

This proves (4.9) and the theorem. □

Theorem 4.2 now follows directly since

$$N(n,r,p)=\sum_{d|r}\mu(d)\gcd(n^{r/d}-1,p-1).$$

For the distribution of cycles we have the following theorem, which follows directly from Theorem 4.2.

Theorem 4.10. *We have*

$$\lim_{M\to\infty}\frac{1}{M}\sum_{p\in P_M}K(n,r,p)=\frac{1}{r}\sum_{d|r}\mu(d)\tau(n^{(r/d)}-1). \tag{4.10}$$

5 Perturbation of monomial systems

In [7] there is an extensive investigation of monomial dynamical systems over the field of p-adic numbers, $\mathbb{Q}_p$. In this section we will follow the ideas from [7] for investigations of perturbations of such systems. We will use the following theorems a lot.

Theorem 5.1. *Let $F(x)$ be a polynomial over $\mathbb{Z}_p$. Assume that there exists $\alpha_0 \in \mathbb{Z}_p$ such that*

$$F(\alpha_0) \equiv 0 \,(\mathrm{mod}\, p^{2\delta+1}\mathbb{Z}_p), \tag{5.1}$$

$$F'(\alpha_0) \equiv 0 \,(\mathrm{mod}\, p^{\delta}\mathbb{Z}_p), \tag{5.2}$$

$$F'(\alpha_0) \not\equiv 0 \,(\mathrm{mod}\, p^{\delta+1}\mathbb{Z}_p), \tag{5.3}$$

where $\delta \in \mathbb{N}$. Then there exists $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $\alpha \equiv \alpha_0 \,(\mathrm{mod}\, p^{\delta+1}\mathbb{Z}_p)$.

Corollary 5.2 (Hensel's Lemma). *Let F be a polynomial over $\mathbb{Z}_p$. Assume that there exists $\alpha_0 \in \mathbb{Z}_p$ such that $F(\alpha_0) \equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$ and $F'(\alpha_0) \not\equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$. Then there exists a p-adic integer α such that $F(\alpha) = 0$ and $\alpha \equiv \alpha_0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$.*

By a perturbation we mean a polynomial with small coefficients in the p-adic sense. More formally:

Definition 5.3. A polynomial

$$q(x) = \sum_{j=0}^{N} q_j x^j$$

over $\mathbb{Z}_p$ ($N \in \mathbb{N}$) is said to be a *k-perturbation* if

$$\|q\| = \max_j |q_j|_p \leqslant \frac{1}{p^{2k+1}} \tag{5.4}$$

where $k \in \mathbb{N}$. If $\|q\| \leqslant 1/p$ ($k = 0$) then q is called a *perturbation.*

Henceforth we will consider the dynamical system

$$f_q(x) = x^n + q(x) \tag{5.5}$$

where $n \in \mathbb{N}$, $n \geqslant 2$ and $q(x)$ is a k-perturbation where k is the unique number satisfying $n - 1 = p^k m$, where $p \nmid m$.

Theorem 5.4. *Consider the dynamical system* (5.5). *If* $x \in S_1(0)$ *then* $f_q(x) \in S_1(0)$.

Proof. Since $\|q\| \leqslant 1/p$ and $|x|_p = 1$,

$$|q(x)|_p \leqslant \max_{0 \leqslant j \leqslant N} (|q_j x^j|_p) \leqslant 1/p.$$

Because $|x^n|_p = |x|_p^n = 1$ and $|q(x)|_p < 1$ it follows that

$$|f_q(x)|_p = \max(|x^n|_p, |q(x)|_p) = |x|_p^n = 1.$$

□

Theorem 5.5. *The dynamical system* (5.5), *has a fixed point* α *such that* $|\alpha|_p \leqslant 1/p$. *This fixed point is an attractor and* $U_1^-(0) \subseteq A(\alpha)$.

Proof. Let $\varphi(x) = f_q(x) - x$. Since $\varphi(0) = f_q(0) = q_0$ and $\|q\| \leqslant 1/p$ we have $\varphi(0) \equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$. Since $\varphi'(x) = nx^{n-1} + q'(x) - 1$ and $\varphi'(0) = q'(0) - 1 = q_1 - 1$ we have $|\varphi'(0)|_p = \max(|q_1|_p, |1|_p) = 1$, that is $\varphi'(0) \not\equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$. The two conditions in Hensel's Lemma (Corollary 5.2) are satisfied and from this Lemma we conclude that there exists $\alpha \in \mathbb{Z}_p$ such that $\varphi(\alpha) = 0$ and $\alpha \equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$. That is, the dynamical system (5.5) has a fixed point α and $|\alpha|_p < 1$.

Let $x \in U_1^-(0)$, that is $|x|_p \leqslant 1/p$. It then follows that

$$|f_q(x)|_p = |x^n + q(x)|_p \leqslant \max(|x^n|_p, |q(x)|_p) \leqslant \frac{1}{p}.$$

By induction it follows that $|f_q^r(x)|_p \leqslant 1/p$ for all $r \in \mathbb{Z}_+$. We will now prove that $U_1^-(0) \subseteq A(\alpha)$. Observe first that

$$\begin{aligned}
|f_q(x) - \alpha|_p &= |f_q(x) - f_q(\alpha)|_p = |x^n - \alpha^n + q(x) - q(\alpha)|_p \\
&= |x^n - \alpha^n + \sum_{j=1}^{N} q_j (x^j - \alpha^j)|_p \\
&= |(x - \alpha) \sum_{j=0}^{n-1} x^j \alpha^{n-j-1} + \sum_{j=1}^{N} q_j (x - \alpha) \sum_{i=0}^{j-1} x^i \alpha^{j-1-i}|_p \\
&= |x - \alpha|_p |\sum_{j=0}^{n-1} x^j \alpha^{n-j-1} + \sum_{j=1}^{N} q_j \sum_{i=0}^{j-1} x^i \alpha^{j-1-i}|_p.
\end{aligned}$$

Since each term in the second factor on the right in the equation above contains at least one x or one α we have for all $x \in \mathbb{Q}_p$, such that $|x|_p < 1$, that there exists a real number $c < 1$ such that

$$|f_q(x) - \alpha|_p < c|x - \alpha|_p.$$

Since $|f_q^r(x)|_p \leqslant 1/p$ for all $r \in \mathbb{Z}_+$ it follows from

$$|f_q^r(x) - \alpha|_p = |f_q(f_q^{r-1}(x)) - \alpha|_p \leqslant c|f_q^{r-1}(x) - \alpha|_p$$

that

$$|f_q^r(x) - \alpha|_p < c^r|x - \alpha|_p, \tag{5.6}$$

by induction. Hence $f_q^r(x) \to \alpha$ when $r \to \infty$ for all $x \in U_1^-(0)$, that is $U_1^-(0) \subseteq A(\alpha)$. The proof is complete. □

In the above theorem we only need q to be a perturbation, not a k-perturbation.

Theorem 5.6. *Consider the dynamical system* (5.5) *and assume that the degree of q is less or equal to n. We have that $|f_q^r(x)|_p \to \infty$ when $r \to \infty$ if and only if $|x|_p > 1$, so $A(\infty) = \mathbb{Q}_p \setminus U_1(0)$.*

Proof. Assume first that $|x|_p > 1$. Since $x \in \mathbb{Q}_p$ it is true that $|x|_p \geqslant p$. If we use the inverse triangle inequality we get

$$|f_q(x)|_p = |x^n + \sum_{j=0}^{n} q_j x^j|_p = |(1+q_n)x^n + \sum_{j=0}^{n-1} q_j x^j|_p \geqslant |x^n|_p - |\sum_{j=0}^{n-1} q_j x^j|_p$$
$$\geqslant |x^n|_p - \max_j |q_j x^j|_p \geqslant |x^n|_p - \|q\||x^{n-1}|_p = |x|_p^{n-2}(|x|_p - \|q\|)|x|_p.$$

Since the parenthesis in the last expression is positive, there is a constant, $c > 1$, such that

$$|f_q(x)|_p > c|x|_p.$$

for all x satisfying $|x|_p > 1$. By induction it is easy to prove that

$$|f_q^r(x)|_p > c^r|x|_p.$$

Hence, $|f_q^r(x)|_p \to \infty$ as $r \to \infty$ if $|x|_p < 1$.

If $|x|_p \leqslant 1$ it follows directly from the strong triangle inequality that $|f_q(x)|_p \leqslant 1$ and by induction that $|f_q^r(x)|_p \leqslant 1$. □

If we assume that the degree of the perturbation polynomial q is less or equal to n it follows from Theorem 5.4 and Theorem 5.6 that $A(\alpha) = U_1^-(0)$. If we assume that $\deg q \leqslant n$, we can say that α and ∞ are attractors to the dynamical system $f(x) = x^n + q(x)$, and that the basins of attraction are $U_1^-(0)$ and $\mathbb{Q}_p \setminus U_1(0)$ respectively. If $\deg q > n$ we do not always have $A(\alpha) = U_1^-(0)$, see the following example.

Example 5.7. Let p be a fixed prime number and let $n \geqslant 2$ be an integer such that $p \nmid n-1$. Let $q(x) = cx^{n+1}$, where $c = \sum_{i=1}^{\infty}(p-1)p^i$. It is clear that q is a perturbation to the dynamical system $f(x) = x^n$. Consider the dynamical system $f_q(x) = x^n + q(x)$. Let $x = 1/p$ ($|x|_p = p$) then

$$f_q(1/p) = 1/p^n + \sum_{i=1}^{\infty}(p-1)p^{i-(n+1)} = 0.$$

From Theorem 5.5 it follows that there is a fixed point $\alpha \in U_1^-(0)$ and that $U_1^-(0) \subseteq A(\alpha)$. Since $0 \in A(\alpha)$ it follows that $1/p \in A(\alpha)$.

We will now start to investigate the behaviour of the dynamical system on the sphere $S_1(0)$.

Theorem 5.8. *Let $a \in S_1(0)$ be a fixed point of the dynamical system (2.1). Then there exists a fixed point, $\alpha \in \mathbb{Z}_p$, to the dynamical system (5.5) such that $\alpha \equiv a \,(\mathrm{mod}\, p^{k+1}\mathbb{Z}_p)$.*

Proof. Let $\psi(x) = f(x) - x = x^n - x$ and let $\varphi(x) = f_q(x) - x = \psi(x) + q(x)$. Since $\|q\| \leqslant 1/p^{2k+1}$ it follows that

$$\varphi(a) = \psi(a) + q(a) \equiv \psi(a) \,(\mathrm{mod}\, p^{2k+1}\mathbb{Z}_p),$$

and since $\psi(a) = 0$ (a is a fixed point to that dynamical system) it follows that $\varphi(a) \equiv 0 \,(\mathrm{mod}\, p^{2k+1}\mathbb{Z}_p)$. We also have that $\varphi'(x) = \psi'(x) = nx^{n-1} - 1 + q'(x)$, this implies that

$$\varphi'(a) = na^{n-1} - 1 + q'(a) = n - 1 + q'(a),$$

since $a^{n-1} = 1$ ($a^n = a$). It follows now, from the fact that $p^k \mid n-1$ and $p^{k+1} \nmid n-1$, that

$$\varphi'(a) \equiv 0 \,(\mathrm{mod}\, p^k\mathbb{Z}_p), \tag{5.7}$$

$$\varphi'(a) \not\equiv 0 \,(\mathrm{mod}\, p^{k+1}\mathbb{Z}_p). \tag{5.8}$$

From Theorem 5.1 it follows that there exists $\alpha \in \mathbb{Z}_p$ such that $\varphi(\alpha) = 0$ (that is, a fixed point to $f(x)$) and $\alpha \equiv a \,(\mathrm{mod}\, p^{k+1}\mathbb{Z}_p)$. □

We now prove the converse to this theorem.

Theorem 5.9. *If $\alpha \in S_1(0)$ is a fixed point to the dynamical system* (5.5), *then there exists a fixed point, a, (a root of unity) to* (2.1) *such that $a \equiv \alpha \,(\mathrm{mod}\, p^{k+1}\mathbb{Z}_p)$.*

Proof. We will use Theorem 5.1 to prove this. Let

$$\psi(x) = f(x) - x = x^n - x = f_q(x) - q(x) - x$$

and observe that $f_q(\alpha) = \alpha$. First of all we have

$$|\psi(\alpha)|_p = |f_q(\alpha) - q(\alpha) - \alpha|_p = |q(\alpha)|_p \leqslant \frac{1}{p^{2k+1}},$$

that is, $\psi(\alpha) \equiv 0 \,(\mathrm{mod}\, p^{2k+1}\mathbb{Z}_p)$. If we observe that

$$\alpha^{n-1} = -\frac{q(\alpha)}{\alpha} + 1$$

then

$$\begin{aligned} |\psi'(\alpha)|_p &= |n(-\frac{q(\alpha)}{\alpha} + 1) - 1|_p \\ &= |\frac{1}{\alpha}|_p |n(-q(\alpha) + \alpha) - \alpha|_p = |-nq(\alpha) + (n-1)\alpha|_p. \end{aligned}$$

Since $|q(\alpha)|_p \leqslant 1/p^{2k+1}$ and $|n-1|_p = 1/p^k$ we have $|\psi'(\alpha)|_p = 1/p^k$. Hence $\psi'(\alpha) \equiv 0 \,(\mathrm{mod}\, p^k\mathbb{Z}_p)$ and $\psi'(\alpha) \not\equiv 0 \,(\mathrm{mod}\, p^{k+1}\mathbb{Z}_p)$. From Theorem 5.1 it follows that there exists $a \in \mathbb{Z}_p$ such that $\psi(a) = 0$ and $a \equiv \alpha \,(\mathrm{mod}\, p^{k+1}\mathbb{Z}_p)$. □

Theorem 5.10. *If $p > 2$ there is a one to one correspondence between the fixed points on $S_1(0)$ of the dynamical systems* (5.5) *and* (2.1).

Proof. Let a and b ($a \neq b$) be two fixed points in $S_1(0)$ to the monomial dynamical system (2.1). According to Theorem 5.8 there are fixed points α and β on $S_1(0)$ to (5.5) such that $|a - \alpha|_p \leqslant 1/p$ and $|b - \beta|_p \leqslant 1/p$. From Theorem 2.7 it follows that $|a - b|_p = 1$. We therefore have

$$|\alpha - \beta|_p = |(\alpha - a) + (a - b) + (b - \beta)|_p = 1,$$

since $|(\alpha - a) + (b - \beta)|_p \leqslant 1/p$. Hence $\alpha \neq \beta$.

The second part of the theorem is proved similarily. □

Remark 5.11. If $\|q\| \geqslant 1$, Theorem 5.10 no longer holds.

Example 5.12. Let $p = 3$, $f(x) = x^2$ and $f_q(x) = x^2 - 2$. The dynamical system f has only one fixed point ($x = 1$) on $S_1(0)$. But the dynamical system f_q has the fixed points $x = 2$ and $x = -1$ on $S_1(0)$.

6 Cycles of perturbated systems

In this section we will start to study the dynamical system

$$f_q(x) = x^n + q(x), \tag{6.1}$$

where q is a perturbation, $f(x) = f_0(x) = x^n$. To study cycles of length r to this system, we look for fixed points to f_q^r. We can write

$$f_q^r(x) = x^{n^r} + q_r(x), \tag{6.2}$$

where q_r is a new perturbation. Let C_r denote the set of fixed points to (6.2). All periodic points of period r are contained in C_r, but this set also contains periodic points of periods that divides r.

Theorem 6.1. *Assume that* $n^r - 1 \not\equiv 0 \,(\mathrm{mod}\, p)$. *Then* $f_q^r(x)$ *has a fixed point* $b \in S_1(0)$ *if and only if* f_0^r *has a fixed point* $a \in S_1(0)$ *such that* $|a - b|_p \leqslant 1/p$.

Proof. Let

$$g_r(x) = x^{n^r} - x$$

and let

$$g_{q,r}(x) = x^{n^r} - x + q_r(x) = g_r(x) + q_r(x).$$

First, let us assume that a is a fixed point to f_0^r that is $g_r(a) = 0$. The fact that $|a|_p = 1$ implies that

$$g_{q,r}(a) \equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$$

and that

$$g_r'(a) = n^r a^{n^r - 1} = n^r - 1.$$

So if $n^r - 1 \not\equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$ (which is an assumption) we have that

$$g_r'(a) \not\equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$$

and of course

$$g_{q,r}'(a) \not\equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p).$$

Hence, by Hensel's lemma there exists $b \in S_1(0)$ such that $g_{q,r}(b) = 0$ and $|a - b|_p \leqslant 1/p$.

Let us now assume that there is $b \in S_1(0)$ such that $g_{q,r}(b) = 0$, that is b is a fixed point on $S_1(0)$ to the function f_q^r. Since

$$g_r(x) = g_{q,r}(x) - q_r(x)$$

we get $g_r(b) \equiv 0 \,(\mathrm{mod}\, p\mathbb{Z}_p)$. Observe that

$$g_r'(b) = n^r b^{n^r-1} - 1.$$

From the fact that $g_{q,r}(b) = 0$ we get

$$b^{n^r-1} - b = -q_r(b)$$

which in turn implies that $b^{n^r} \equiv b \,(\mathrm{mod}\, p\mathbb{Z}_p)$ and that $b^{n^r-1} \equiv 1 \,(\mathrm{mod}\, p\mathbb{Z}_p)$. All this give us that

$$g_r'(b) = n^r b^{n^r-1} - 1 \equiv n^r - 1 \,(\mathrm{mod}\, p\mathbb{Z}_p).$$

The theorem now follows from Hensel's lemma. □

We have not this results in the case $n^r - 1 \equiv 0 \,(\mathrm{mod}\, p)$.

Example 6.2. Let $p = 3$, $f(x) = x^2$ and $f_q(x) = x^2 - 39/4$. We are going to show that f has no cycles of length 2 but f_q has one cycle of length 2. From the fact that $\gcd(n^2 - 1, p - 1) = 1$ we immediately have that f has no cycles of length 2. Since

$$f_q^2(x) = f_q(f_q(x)),$$

has two fixed points, $x = 5/2$ and $x = -7/2$, and none of them are fixed points to $f_q(x)$ it follows that f_q has one cycle of length 2.

Theorem 6.3. *Let p be a fixed prime number and let $n \in \mathbb{N}$ and $n \geqslant 2$. If $p \nmid n$ there is a least $\bar{r}$ such that $n^{\bar{r}} - 1 \equiv 0 \,(\mathrm{mod}\, p)$ and $2 \leqslant \bar{r} \leqslant p - 1$. If $\bar{r} \nmid r$ then $n^r - 1 \not\equiv 0 \,(\mathrm{mod}\, p)$.*

Proof. Consider the multiplicativ group $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$, of the field of residue classes $\mathbb{F}_p$. We know that $\mathbb{F}_p^*$ is a cyclic group under multiplication. Let d be the remainder when n is divided by p, of course $d \in \mathbb{F}_p^*$. Due to Fermat we have $d^{p-1} - 1 \equiv 0 \,(\mathrm{mod}\, p)$. That is, there exits r such that $n^r - 1 \equiv 0 \,(\mathrm{mod}\, p)$. Since the set $\{2, 3, \ldots, p-1\}$ is finite there exists a least r, say $\bar{r}$. It is clear that $\bar{r}$ is the order of the cyclic subgroup generated by

d. (Accordning to the Theorem of Lagranges $\bar{r}$ must be a divisior of $p-1$.) Assume that $n^r - 1 \equiv 0 \pmod{p}$, then there is a cyclic subgroup of order r. Let $r = q_1\bar{r} + r_1$. We then have

$$1 \equiv (n^{\bar{r}})^{q_1} n^{r_1} \equiv n^{r_1},$$

but since $r_1 < \bar{r}$ this is only possible if $r_1 = 0$, that is $\bar{r} \mid r$. The proof is complete. □

Example 6.4. Let $p = 3$ and let $f(x) = x^2$ and $f_q(x) = x^2 + q(x)$ where $\delta_q \leqslant 1/p$. We then have

$$m_r = (2^r - 1, p - 1) = (2^r - 1, 2) = 1.$$

Thus the function $f^r(x) = x^{2^r}$ has no fixed points on $S_1(0)$ according to Theorem 2.5. By using Theorem 6.1 we conclude that $f_q^r(x) = x^{2^r} + q_r(x)$ has no fixed points on $S_1(0)$ if $2^r - 1 \not\equiv 0 \pmod{3}$. Since $2^r - 1 \equiv (-1)^r - 1 \pmod{3}$ we have that

$$2^r - 1 \equiv \begin{cases} 0 \pmod{3}, & \text{if } r \text{ is even,} \\ 1 \pmod{3}, & \text{if } r \text{ is odd.} \end{cases}$$

So, the dynamical system f_q has no cycles of odd length on the sphere $S_1(0)$.

Example 6.5. Let f and f_q be as in the example above, but let $p = 7$. It is easy to show that $2^r - 1 \not\equiv 0$ if and only if $3 \nmid r$. Since $2^r - 1$ does not contain any factor of 2 we have

$$\gcd(2^r - 1, 6) = \gcd(2^r - 1, 3).$$

Let us now study two cases: (i) If $r = 2l$ then $2^r - 1 \equiv 0 \pmod{3}$, so $\gcd(2^r - 1, 3) = 3$. (ii) If $r = 2l+1$ then $2^r - 1 \equiv 1 \pmod{3}$, so $\gcd(2^r - 1, 3) = 1$. We can now make the following conclusions: The dynamical system f_q has cycles of order 2 and there exists no cycles of order r if $2 \nmid r$ and $3 \nmid r$ (or $r \not\equiv 3 \pmod{6}$).

Example 6.6. Let $p = 43$ and let f and f_q be as above. One can show (or use a computer) that $2^r - 1 \not\equiv 0 \pmod{43}$ if and only if $14 \nmid r$. We have the following values for m_r:

$$\begin{aligned} r &\equiv 0 \,(\mathrm{mod}\, 6) \quad m_r = 21 \\ r &\equiv 1 \,(\mathrm{mod}\, 6) \quad m_r = 1 \\ r &\equiv 2 \,(\mathrm{mod}\, 6) \quad m_r = 3 \\ r &\equiv 3 \,(\mathrm{mod}\, 6) \quad m_r = 7 \\ r &\equiv 4 \,(\mathrm{mod}\, 6) \quad m_r = 3 \\ r &\equiv 5 \,(\mathrm{mod}\, 6) \quad m_r = 1 \end{aligned}$$

The dynamical system f_q therefore has cycles of order 2, 3 and 6. If $r > 3$, $r \neq 6$ and $14 \nmid r$, then the dynamical system f_q has no cycles of order r.

To get more information about the cycles of the dynamical system (6.1) we have to use stronger conditions on the perturbation polynomial.

Theorem 6.7. *Let $n^r - 1 = p^\kappa m$, where $p \nmid m$, and let q be a κ-perturbation. If $a \in S_1(0)$ is a fixed point to the dynamical system f^r then there is a fixed point $\alpha \in S_1(0)$ to the dynamical system f_q^r and $|a - \alpha|_p \leqslant 1/p^{\kappa+1}$. Conversely, if $b \in S_1(0)$ is a fixed point to f_q^r then there is a fixed point $\beta \in S_1(0)$ to f^r such that $|b - \beta|_p \leqslant 1/p^{\kappa+1}$.*

Proof. We begin this proof by introducing two functions:

$$g_r(x) = f^r(x) - x = x^{n^r} - x$$

and

$$g_{q,r}(x) = f_q^r(x) - x = g_r(x) + q_r(x).$$

Let us first assume that $a \in S_1(0)$ is a fixed point to f^r, that is $g_r(a) = 0$. We have that

$$g_{q,r}(a) = q_r(a) \equiv 0 \,(\mathrm{mod}\, p^{2\kappa+1}\mathbb{Z}_p).$$

Since $(d/dx)g_{q,r}(x) = n^r x^{n^r-1} - 1 + q_r'(x)$ we also have $(d/dx)g_{q,r}(a) \equiv 0 \,(\mathrm{mod}\, p^\kappa \mathbb{Z}_p)$ and $(d/dx)g_{q,r}(a) \not\equiv 0 \,(\mathrm{mod}\, p^{\kappa+1}\mathbb{Z}_p)$. According to Theorem 5.1 there is $\alpha \in S_1(0)$ such that $g_{q,r}(\alpha) = 0$ and $|a - \alpha|_p \leqslant 1/p^{\kappa+1}$.

Assume now that $b \in S_1(0)$ is a fixed point to f_q^r. If we observe that $g_r(x) = g_{q,r}(x) - q_r(x)$, we can make the conclusion that

$$g_r(b) = -q_r(b) \equiv \,(\mathrm{mod}\, p^{2\kappa+1}\mathbb{Z}_p).$$

Since $b^{n^r} \equiv b \,(\mathrm{mod}\, p^{2\kappa+1})$, and therefore $b^{n^r-1} \equiv 1 \,(\mathrm{mod}\, p^{2\kappa+1})$ we have

$$(d/dx)g_r(b) = n^r b^{n^r-1} - 1 \equiv n^r - 1 \equiv 0 \,(\mathrm{mod}\, p^\kappa \mathbb{Z}_p)$$

and $(d/dx)g_r(b) \not\equiv 0 \,(\mathrm{mod}\, p^{\kappa+1}\mathbb{Z}_p)$. The conditions in Theorem 5.1 are satisfied, so there exists $\beta \in S_1(0)$ such that $g_r(\beta) = 0$ and $|b-\beta|_p \leqslant 1/p^{\kappa+1}$. The proof is complete. □

Observe that for $p > 2$ we have a one-to-one correspondence between the cycles of a specific length to the dynamical system f_q and f. This follows directly from Theorem 5.10. Before we present some examples we state some theorems which will help us in the construction of these examples.

Theorem 6.8. *Let p be a fixed prime number and let $l \geqslant 2$, $n \geqslant 2$. If p is not a divisor of n, then there is a least integer $\bar{r}$ such that $n^{\bar{r}} - 1 \equiv 0 \pmod{p^l}$, $1 \leqslant \bar{r} \leqslant \varphi(p^l)$. If $n^r - 1 \equiv 0 \pmod{p^l}$ then $\bar{r} \mid r$.*

Proof. According to Theorem 3.6 we have $n^{\varphi(p^l)} - 1 \equiv 0 \pmod{p^l}$, since $\gcd(n, p^l) = 1$. The existence of a least integer $\bar{r}$ such that $n^{\bar{r}} - 1 \equiv 0 \pmod{p^l}$ is therefore obvious. Of course $1 \leqslant \bar{r} \leqslant \varphi(p^l)$.

Assume $n^r \equiv 1 \pmod{p^l}$. If we divide r by $\bar{r}$ we get $r = c\bar{r} + d$. Since $d < \bar{r}$ and $\bar{r}$ is the least integer such that $n^{\bar{r}} \equiv 1 \pmod{p^l}$ we must have $d = 0$ and hence $\bar{r} \mid r$. The theorem is proven. □

Theorem 6.9. *Let n, m and l be positive integers. If $n \equiv 1 \pmod{m^l}$, then $n^m \equiv 1 \pmod{m^{l+1}}$. If $m = p$ is a prime number and $n \not\equiv 1 \pmod{p^{l+1}}$ then p is the least m such that $n^m \equiv 1 \pmod{p^{l+1}}$.*

Proof. Since $n \equiv 1 \pmod{m^l}$ we can write $n = qm^l + 1$. By use of the binomial theorem we have

$$\begin{aligned} n^m =& (qm^l + 1)^m = \sum_{j=0}^{m} \binom{m}{j} (qm^l)^j \\ =& 1 + \binom{m}{1} qm^l + \sum_{j=2}^{m} \binom{m}{j} (qm^l)^j \\ \equiv& 1 \pmod{m^{l+1}}. \end{aligned}$$

This proves the first part of the theorem. Let us now assume that $m = p$ is a prime number. The fact that $n \equiv 1 \pmod{p^l}$ implies that n and p are relatively prime. According to Theorem 6.8 there is a least r such that $n^r \equiv 1 \pmod{p^{l+1}}$. If $n \not\equiv 1 \pmod{p^{l+1}}$ then it is obvious that the least r must be p since the only positive divisors of p are p and 1.(We know that $n^p \equiv 1 \pmod{p^{l+1}}$ from the first part of this theorem.) □

Theorem 6.10. *Assume that $n \equiv 1 \pmod{p^l}$ for some $l \in \mathbb{Z}^+$, where p is a prime number. Assume also that this prime number is the least positive integer d such that $n^d \equiv 1 \pmod{p^{l+1}}$. The least positive integer k such that $(n^p)^k \equiv 1 \pmod{p^{l+2}}$ is then p.*

Proof. We can write $n = qp^l + 1$. Since p is the least positive integer d such that $n^d \equiv 1 \,(\mathrm{mod}\, p^{l+1})$ it follows that $n \not\equiv 1 \,(\mathrm{mod}\, p^{l+1})$, hence $p \nmid q$. We have

$$n^p = \sum_{k=0}^{p} \binom{p}{k} (qp^l)^k = 1 + \binom{p}{1} qp^l + \sum_{k=2}^{p} \binom{p}{k} (qp^l)^k.$$

If $n^p \equiv 1 \,(\mathrm{mod}\, p^{l+2})$ then $qp^{l+1} \equiv 0 \,(\mathrm{mod}\, p^{l+2})$ which is a contradiction to the fact that $p \nmid q$. Hence, the least positive integer k such that $(n^p)^k \equiv 1 \,(\mathrm{mod}\, p^{l+2})$ is p, by Theorem 6.9. □

Example 6.11. Let $f_q(x) = x^2 + q(x)$, where q is a perturbation. Due to Theorem 2.5, $f(x) = x^2$ has no cycles of any lenght. According to Example 6.4, f_q has no cycles of odd length. Assume that $r = 2r_1$, $r_1 \in \mathbb{Z}^+$, then we have that

$$2^r - 1 \equiv (2^2)^{r_1} - 1 \equiv 0 \,(\mathrm{mod}\, 3). \tag{6.3}$$

That is, Theorem 6.1 tells us nothing about possible cycles of f_q in this case. Since $4 \not\equiv 1 \,(\mathrm{mod}\, 3^2)$ we have that $4^3 \equiv 1 \,(\mathrm{mod}\, 3^2)$, and 3 is the least positive integer, d, such that $4^d \equiv 1 \,(\mathrm{mod}\, 3^2)$, by Theorem 6.9. Due to this remark it is easy to see that if $r = 2(3r_2 + \alpha)$, ($r_2 \in \mathbb{Z}^+$ and $\alpha = 0, 1, 2$) then $2^r \equiv 1 \,(\mathrm{mod}\, 3^2)$ if and only if $\alpha = 0$. That is

$$2^r - 1 \not\equiv 0 \,(\mathrm{mod}\, 3^2). \tag{6.4}$$

If we assume that q is a 1-perturbation, that is $\|q\| \leqslant 1/3^3$, then it follows from (6.3), (6.4) and Theorem 6.7 that if $6 \nmid r$ then f_q has no cycles of order r.

We can continue this investigations by repeating the above arguments. If we assume that q is a 2-perturbation then we can make the conclusion that f_q has no cycles of length r if $18 \nmid r$.

More general, if we assume that $\|q\| \leqslant 1/3^{2\kappa+1}$ then there are no cycles of length r if $2 \cdot 3^\kappa \nmid r$, by Theorem 6.10.

Example 6.12. Let $p = 7$ and let $f_q(x) = x^2 + q(x)$, where q is a perturbation. According to Theorem 6.3 the dynamical system $f(x) = x^2$ has cycles only of length 2. Accordning to Example 6.5, f_q has a cycles of length 2 and we also know that f_q has no cycles of order r if $r > 2$ and $3 \nmid r$. Let us now assume that $r = 3r_1$, where $r_1 \in \mathbb{Z}^+$, then $2^{3r_1} - 1 \equiv 0 \,(\mathrm{mod}\, 7)$. Since $8 \not\equiv 1 \,(\mathrm{mod}\, 49)$ we have that 7 is the least positive integer d such that $8^d \equiv 1 \,(\mathrm{mod}\, 49)$, by Theorem 6.9. We therefore

have that $2^{3(7r_2+\alpha)} - 1 \not\equiv 0 \pmod{49}$ if $1 \leqslant \alpha \leqslant 6$. If $\|q\| \leqslant 1/p^3$ it follows from Theorem 6.7 that there are no cycles of order r to the dynamical system f_q if $r > 2$ and $21 \nmid r$.

If we assume that $\|q\| \leqslant 1/7^{2\kappa+1}$ then it follows from Theorem 6.7 and 6.10 that the dynamical system f_q has no cycles of length r if $3 \cdot 7^\kappa \nmid r$.

Example 6.13. Let $n = 10$ and let $p = 3$. Since

$$m_r = \gcd(n^r - 1, p - 1) = \gcd(10^r - 1, 2) = 1$$

it follows from Theorem 2.5 that the dynamical system $f(x) = x^{10}$ has no cycles. We have that $n^r - 1 \equiv 0 \pmod 9$ for every $r \geqslant 2$ and if $3 \nmid r$ we have $n^r - 1 \not\equiv 0 \pmod{27}$. If we assume that $\|q\| \leqslant 1/3^5$ we have by Theorem 6.7 that f_q has no cycles of length r if $3 \nmid r$. If $\|q\| \leqslant 1/3^{2\kappa+1}$ then f_q has no cycles of length r if $3^{\kappa-1} \nmid r$.

Example 6.14. Let $n = 2$ and $p = 251$. Computer calculations show that $r = 50$ is the least positive integer such that $n^r - 1 \equiv 0 \pmod{251}$. According to Theorem 2.5 we have that f only has cycles of lengths 4, 20 and 100. Due to Theorem 6.1 we can make the conclusion that f_q has cycles of order 4 and 20, and that f_q has no cycles of order r if $r \neq 4$, $r \neq 20$ and $50 \nmid r$. By using a computer we get that $n^{100} - 1 \not\equiv 0 \pmod{251^2}$. So, if q is a 1-perturbation we have according to Theorem 6.7 that f_q also has a cycle of order 100.

Since $2^{50} - 1 \equiv 0 \pmod{251}$ and $2^{50} - 1 \not\equiv 0 \pmod{251^2}$ we have by Theorem 6.9 that $d = 251$ is the least positive integer such that $(2^{50})^d - 1 \equiv 0 \pmod{251^2}$. So, if we assume that q is a 1-perturbation we have that f_q has no cycles of order r if $r \neq 4$, $r \neq 20$, $r \neq 100$ and $12550 \nmid r$.

It is possible to generalize the theorems in Section 3 and 4 to some perturbated monomial systems. Assume that $p > 2$. Let $\hat{r}$ denote the length of the longest cycle of f and let $N_q(n, r, p)$ denote the number of periodic points on $S_1(0)$ of period r of f_q (a corresponding perturbated system). If $n^{r_j} - 1 = p^\kappa n_j$, $p \nmid n_j$ for all $r_j \mid \hat{r}$ then it follows from Theorem 5.10 that

$$N_q(n, r_j, p) = N(n, r_j, p),$$

if q is a κ-perturbation.

7 Acknowledgement

I would like to thank my supervisor Prof. Andrei Khrennikov for introducing me to the subject and for guidance during the work and Prof. Labib Haddad, University of Clermont-Ferrand, France for his advices on computing the number of cycles. I would also like to thank my collegues at the department of mathematics, statistics and computer science at Växjö University for many helpful and amusing discussions. Finally I thank Prof. Bertin Diarra, University of Clermont-Ferrand, France and Prof. Mikihiko Endo, Rikkyo Univerity Tokyo for suggesting improvements.

References

[1] Apostol T.M., *Introduction to analytic number theory.* Springer, 1976.

[2] Escassut A., *Analytic elements in p-adic analysis.* World Scientific, Singapore, 1995.

[3] Gouvêa F. Q., *p-adic Numbers.* Springer, 1997.

[4] Hadamard J., *Sur la distribution des zros de la fonction $\zeta(s)$ et ses consquences arithmtiques.* Bull. Soc. Math. France, **24**:199-220. 1896.

[5] Hall M., *Combinatorial Theory.* Blaisdell, 1967.

[6] Khennikov A., *Human memory as a p-adic dynamical system.* Reports from MASDA **9818**, Växjö University, 1998.

[7] Khrennikov A., *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models.* Kluwer, 1997.

[8] Khrennikov A., *p-adic Valued Distributions in Mathematical Physics.* Kluwer, 1994.

[9] Lindahl K.O., *On Markovian properties of the dynamics on attractors of random dynamical systems over the p-adic numbers.* Reports from Växjö University, **8**: 1999.

[10] Nyqvist R., *Dynamical systems in Finite Field Extensions of p-adic numbers.* Reports from Växjö University, **12**: 1999.

[11] Schikhof W.H., *An introducton to p-adic analysis.* Cambrige, 1984.

[12] Tambour Torbjörn, *Introduction to finite groups and their representation.* Lund, 1994.

[13] Valle Poussin Ch. de la, *Recherches analytiques sur la thorie des nombers premiers.* Ann. Soc. Sci. Bruxelles, **20**: 183-256, 281-297. 1896.

[14] Le Veque W.J., *Topics in Number Theory.* Reading Mass. Addison-Wesley Publishing co. 1956.

Marcus Nilsson
School of Mathematics and System Engineering
Växjö University
SE-35 195 VÄXJÖ
Sweden

E-mail: Marcus.Nilsson@msi.vxu.se