Journal of Statistical Physics, Vol. 54, Nos. 3/4, 1989

p-Adic Dynamics

E. Thiran,[1,*] D. Verstegen,[2] and J. Weyers[1]

Received August 8, 1988

The quadratic map over p-adic numbers is studied in some detail. We prove that near almost all indifferent fixed points it is topologically conjugate to a quasiperiodic linear map. We also establish the existence of chaotic behavior and describe it using symbolic dynamics.

KEY WORDS: p-adic numbers; dynamical systems; chaos; quasiperiodicity.

1. INTRODUCTION

The purpose of this paper is to investigate the asymptotic behavior of nonlinear p-adic mappings. Our motivation for such an investigation is based on the following considerations. First of all, the discovery of "chaos" (see, e.g., refs. 1) as well as of universal features in chaotic behavior (e.g., ref. 2) is undoubtedly a major achievement in the study of dynamical systems. It is certainly an interesting question, for its own sake, to ask whether chaos is a property of real or complex mappings or whether it also occurs in mappings defined over other continuous number fields, such as p-adics.[3,4] We will show that indeed it does.

It is obvious that in the description of physical phenomena one needs a "number field." Without getting too philosophical about the merits of various number fields, a rather minimal requirement would be that it contain the rational numbers, since, after all, the result of any measurement can be expressed as such. It turns out that there are only two types of complete extensions of the rationals: one is given by the real numbers and the other by p-adic numbers. Their essential difference comes from the property of the metric with respect to which they complete or fill the holes in the

[1] Institut de Physique Théorique, Université Catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium.
[2] Present address: NIKHEF-H, P.O. Box 41882, 1009 DB Amsterdam, The Netherlands.
[*] Aspirant F.N.R.S.

rational numbers: in the case of the reals, the metric, given by the absolute value, is Archimedean, while in the case of p-adics the metric is non-Archimedean or ultrametric!

Quite recently, in string theory as in lattice gauge theories, there has been a growing interest[5–8] in exploring properties of physical systems when defined over p-adic (or even finite)[9] number fields. In the case of strings,[6–8] for example, since the world sheet parameters are not, intrinsically, observable quantities, it is certainly legitimate to investigate the structure of the theory when these parameters are p-adic. So one is naturally led to the idea that a truly fundamental theory of the structure of matter should not only be independent of the parametrization used (which is certainly a key input of general relativity or of conformal invariant theories) but also of the number field in which this parametrization is expressed! This is a rather fascinating idea.

As another motivation for the use of p-adics in the study of physical systems, it may be useful to remember the role of complex numbers in classical and quantum physics. Complex numbers are a quadratic extension of real numbers, but the added number i has of course no place in any classical phenomenon. Nevertheless, it is a triviality to point out that complex numbers and complex analysis have been useful and powerful tools in almost all branches of classical physics. In quantum physics, the situation is of course fundamentally different: from a tool, which they were in classical physics, complex numbers are promoted to an essential and unescapable ingredient of the physical picture of the quantum world. Quantum amplitudes are, fundamentally, complex numbers (see, e.g., ref. 10). We will not suggest that history may repeat itself and that p-adic numbers will turn out to be an essential ingredient in the description of physical reality. However, the discovery of the ultrametric structure of the ground states in spin glasses[11] makes one wonder. Ultrametricity is such an inherent property of p-adics that one cannot help speculating on the possibility of a sharper and more complete description of spin glasses in terms of them. It still remains to be done.

There is a road leading back from p-adics to real numbers: it is the so-called adelic construction (see, e.g., ref. 4). Unfortunately, it is infinitely more complicated than, say, "taking the real part," which brings us back from the complex plane to the real line. The adelic construction has been explicitly performed in the case of four-point functions in string theory[7] and the result is rather spectacular: the product of all four-point functions on all p-adics and on the reals is equal to one! For five-point amplitudes, a similar result does not seem to hold, however. Anyway, whether a p-adic formulation of physical problems will remain a mathematical curiosity, a useful tool, or a fundamental step, only the future will tell.

Our main result in this paper is that p-adic dynamics exhibits striking similarities with real or complex dynamics[1]: attractive or indifferent cycles, quasiperiodicity,[12],[3] and chaos all occur. There are some important differences, however: we do not find a cascade of period-doubling bifurcations as a road to chaos.

The analysis is also much simpler on p-adics than on the real or complex numbers. A similar observation had already been made in string theory, where p-adic amplitudes involve simpler functions. This also suggests that new concepts for dealing with nonlinear dynamics might be tested first on p-adics.

For simplicity we mainly restrict our discussion to quadratic p-adic maps, although, clearly, our methods and results can be extended to other mappings as well. We do not aim at the most general analysis of p-adic maps, but rather at illustrating different characteristic patterns of such mappings.

The paper is organized as follows: in Section 2 we briefly list some pertinent properties of p-adic numbers and in Section 3 we describe some general features of quadratic iterations. In Section 4, we analyze the behavior of the system near indifferent fixed points and prove, quite generally, that the quadratic mapping is topologically conjugate to a quasiperiodic linear one. Finally, in Section 5, we turn our attention to another region of parameter space of the quadratic map. Here, most points end up at infinity except for a Cantor set on which the iteration is equivalent to a simple "shift map" and hence is chaotic. We end up by giving a simple example of a (nonpolynomial) map which has chaotic behavior on a set of finite (Haar) measure.[3,4]

2. THE p-ADIC NUMBERS: Q_p

In this section we briefly review some properties of p-adic numbers which are relevant to our problem. For more details, we refer the reader to the mathematical literature.[3,4]

Let p be an arbitrary but fixed prime number. Any rational number r can be written uniquely as

$$r = p^{\alpha} a/b \tag{2.1}$$

where α, a, $b \in \mathbb{Z}$ and p does not divide a or b. The integer α is called the ordinal of r (at p).

The p-adic norm $|r|_p$ of r is defined as follows:

$$|r|_p = p^{-\alpha}; \qquad |0|_p = 0 \tag{2.2}$$

[3] Some of our results agree with those obtained in ref. 12.

Just as for the ordinary absolute value, which is now denoted $|\cdot|_\infty$, it is straightforward to check that $|\cdot|_p$ does indeed define a norm on the field Q of rational numbers, namely

$$|x|_p = 0 \text{ iff } x = 0 \tag{2.3a}$$

$$|xy|_p = |x|_p\,|y|_p \tag{2.3b}$$

$$|x+y|_p \leqslant |x|_p + |y|_p \tag{2.3c}$$

In fact, one easily shows that (2.3c) takes an even stronger form

$$|x+y|_p \leqslant \max\{|x|_p, |y|_p\} \tag{2.3d}$$

Norms with this last property are called *non*-Archimedean.

With the help of the p-adic norm, one can easily define a distance, Cauchy sequences, etc. It is well to be aware of the fact that two rational numbers can be very close p-adically—e.g., when they differ by a large power of p—while very far apart in terms of absolute values and vice versa.

It is also worth pointing out that $|\cdot|_\infty$ and $|\cdot|_p$ (for all primes p) are the only inequivalent norms on Q.[3,4]

The field of real numbers $\mathbb{R}$ can be defined as the completion of Q with respect to $|\cdot|_\infty$. In precisely the same way, the field of p-adic numbers Q_p is the completion of Q with respect to $|\cdot|_p$. In particular, Q is dense in Q_p (with respect to $|\cdot|_p$) as well as in $\mathbb{R}$ (with respect to $|\cdot|_\infty$).

A less abstract definition of a p-adic number, which can be shown to be equivalent, is based on the following property: every p-adic number can be written in a *unique* way as a power series

$$x = \sum_{j=\alpha}^{\infty} x_j p^j \tag{2.4}$$

where $\alpha \in \mathbb{Z}$ is again called the ordinal of x and where the x_j (called the digits) take integer values

$$0 \leqslant x_j \leqslant p-1, \qquad 0 < x_\alpha \leqslant p-1 \tag{2.5}$$

The series (2.4) always converges (with respect to $|\cdot|_p$) and provides us with a very concrete realization of Q_p. Note that it is unique, while in the case of $\mathbb{R}$, ambiguities are possible: 1 and 0.999... define the same real number.

It is important to realize that while the absolute value $|\cdot|_\infty$, when extended from Q to $\mathbb{R}$, can take any positive (real) value, the p-adic norm $|\cdot|_p$ even when extended from Q to Q_p keeps on taking a *discrete* set of values, namely powers of p. It follows that many elements of Q_p have the same norm. For example, there are an infinite number of "units" (i.e., numbers of norm $|x|_p = 1$) given by

$$x = x_0 + \sum_{j=1}^{\infty} x_j p^j \tag{2.6}$$

where the digit x_0 is different from zero.

There is *no ordering* among p-adic numbers with the same norm. In this respect Q_p is similar to the complex numbers $\mathbb{C}$. The relevance of this remark comes from the fact that it is the ordered character of $\mathbb{R}$ which lies at the heart of, e.g., Sarkovskii's theorem.[1]

The Q_p's and $\mathbb{R}$ are all *distinct* number fields. For example, $\pm i$ and $\pm\sqrt{6}$ belong to Q_5 but $\pm\sqrt{5}$ does not! What these assertions precisely mean is that the equations $x^2 - 6 = 0$ and $x^2 + 1 = 0$ do admit solutions on Q_5 while $x^2 - 5 = 0$ does not! More generally, one can show, as a consequence of Hensel's lemma,[3,4] that for any p-adic number $a \in Q_p$, its square root $\sqrt{a}$ will belong to Q_p $(p \geqslant 3)$ if a has an even ordinal *and* if its first digit is a square *modulo p*!

The non-Archimedean nature of the p-adic norm has of course far-reaching consequences. First of all, it implies what is usually called "ultrametricity": any "triangle" with "sides" x, y, and $x - y$ is necessarily, isosceles, i.e., if, say, $|x|_p < |y|_p$, then $|x - y|_p = |y|_p$! It follows that Q_p is a *disconnected* field: subsets of Q_p have no boundaries, or, more precisely, they are *both* open and closed with respect to the topology induced by $|\cdot|_p$. For example, the so-called p-adic integers $\mathbb{Z}_p = \{x \mid x \in Q_p,\ |x|_p \leqslant 1\}$ can also be defined as $\mathbb{Z}_p = \{x \mid x \in Q_p, |x|_p < p\}$. This implies in particular that a "large" p-adic number cannot be constructed as the sum of many "small" ones or, in other words, that there is no "path" in Q_p since the "path" concept relies on the possibility of covering a big distance in many small steps. These consequences of the non-Archimedean nature of the p-adic norm are somewhat counterintuitive and take a while to get used to. But there are also enormous simplifications that come with them. First, approximations are much easier to control than on $\mathbb{R}$, since small errors do not add up to give bigger ones. Similarly, the convergence of series is significantly simpler to study on Q_p than on $\mathbb{R}$: the series $\sum a_n q^n$ will converge on Q_p iff $\lim_{n\to\infty} |a_n q^n|_p \to 0$.

It should be clear from the preceding remarks that all theorems of real analysis which rely on the "connectedness" of $\mathbb{R}$ will have no p-adic counterparts. In particular, there is no intermediate value or mean value theorem and hence continuous functions from, say, $\mathbb{Z}_p$ to $\mathbb{Z}_p$ will not necessarily have a fixed point.

The field of complex numbers $\mathbb{C}$ is a "quadratic extension" of $\mathbb{R}$. The field $\mathbb{C}$ has the rather remarkable properties of being complete [with respect to the extended absolute value: $|a+bi|_\infty=(a^2+b^2)^{1/2}$] as well as algebraically closed (every polynomial equation on $\mathbb{C}$ admits a solution in $\mathbb{C}$). For each Q_p, there is also an algebraically closed and complete extension Ω_p, which is, however, considerably more complicated to construct than $\mathbb{C}$. We will have no use of Ω_p in this paper.

Despite all the differences between $\mathbb{R}$ and Q_p we will show in the next sections that simple nonlinear mappings on Q_p present astonishing similarities with similar mappings on $\mathbb{R}$! If nothing else, this strongly suggests that there are "characteristic features" of dynamical systems which do not even depend on the number fields used to model them.

3. QUADRATIC MAPPINGS AND CYCLES

Our main interest will be in quadratic mappings

$$x \to g(x) = a_2x^2 + a_1x + a_0 \tag{3.1}$$

where x, a_0, a_1, a_2 all belong to Q_p and $p \geqslant 3$.[4]

Through a simple conjugacy, (3.1) can be brought to the canonical form

$$x \to f(x) = x^2 + a \tag{3.2}$$

Indeed, let T be the linear transformation on Q_p,

$$T(x) = \lambda x + \mu \tag{3.3}$$

and thus

$$T^{-1}(x) = (x-\mu)/\lambda \tag{3.4}$$

Choosing $\lambda = a_2$ and $\mu = a_1/2$, one easily obtains

$$(TgT^{-1})(x) = x^2 + a \tag{3.5}$$

with

$$a = a_0a_2 + a_1/2 - a_1^2/4 \tag{3.6}$$

More generally one has

$$Tg^n = f^nT \tag{3.7}$$

[4] As is often the case in number theory, $p=2$ is somewhat special and we prefer to ignore it.

where g^n denotes, as usual, the nth iteration of the map g. Conjugate maps are of course equivalent[1] in the sense that they exhibit the same dynamical properties such as cycles, fixed points, etc.

Let us consider the mapping (3.2) starting from some initial p-adic number x_{in}. If $|a|_p \leqslant 1$, we have

$$|f^n(x_{\text{in}})|_p \leqslant 1 \qquad \text{if} \quad |x_{\text{in}}|_p \leqslant 1 \tag{3.8}$$

and

$$|f^n(x_{\text{in}})|_p \to \infty \qquad \text{if} \quad |x_{\text{in}}|_p > 1 \tag{3.9}$$

On the other hand, if $|a|_p > 1$, starting with $|x_{\text{in}}^2|_p > |a|_p$ or $|x_{\text{in}}^2|_p < |a|_p$ leads to

$$\lim_{n\to\infty} |f^n(x_{\text{in}})|_p \to \infty$$

If $|x_{\text{in}}^2|_p = |a|_p$, the iterative process will not diverge if and only if there is a "conspiracy" at each step such that

$$|[f^q(x_{\text{in}})]^2 + a|_p = |a|_p^{1/2} \tag{3.10}$$

This is possible only if $\sqrt{-a}$ belong to Q_p.

In the following we will be concerned only with orbits $\{x, f(x), f^2(x),..., f^n(x)\}$ which remain bounded when $n \to \infty$.

Fixed points of the map (3.2) are solutions of $f(x) = x$, i.e., they are given by

$$x_{\pm} = \frac{1 \pm (1-4a)^{1/2}}{2} \tag{3.11}$$

where the square root may or may not exist in Q_p depending on the values of a and p. Clearly, if this square root does not exist in Q_p, there is no fixed point.

Similarly,[12] points of primitive period 2 are solutions of

$$\frac{f^2(x) - x}{f(x) - x} = 0, \qquad \text{i.e.,} \qquad x_{\pm} = \frac{-1 \pm (-3-4a)^{1/2}}{2} \tag{3.12}$$

For higher-order cycles, of course, exact formulas do not exist, in general. A cycle of order n, with $f^n(\tilde{x}) = \tilde{x}$, is attractive if, for x close to $\tilde{x}$, $f^n(x)$ is closer. For a smooth enough map, this is equivalent to $|f^n(\tilde{x})'|_p < 1$ and since

$$f^n(x)' = f'(f^{n-1}(x))\, f'(f^{n-2}(x)) \cdots f'(x) \tag{3.13}$$

and

$$|f'(x)|_p = |2x|_p = |x|_p \tag{3.14}$$

one easily concludes that when $|a|_p \leqslant 1$, there are two possibilities for a given cycle: either it wanders through some x with $|x|_p < 1$ and is attractive, or it does not cross such an x and is then indifferent, meaning that

$$|f^n(x) - \tilde{x}|_p = |x - \tilde{x}|_p \tag{3.15}$$

On the other hand, when $|a|_p > 1$, only repelling cycles are possible, since one necessarily has values of x with $|x|_p = |a|_p^{1/2} > 1$.

From the previous remarks, one derives an easy procedure for finding all attractive cycles (remember $|a|_p \leqslant 1$): start from $x_{\text{in}} = 0 \bmod p$ and compute its orbit $f^k(x_{\text{in}})$ modulo p as well. We know after at most p steps whether the orbit passes through $x = 0 \bmod p$ again or not, i.e., if there is an attractive cycle or not.

As an example, let us take $p = 5$. If $|a|_5 = 1$, the first digit of a must be 1, 2, 3, or 4, or, in other words, $a = 1, 2, 3$, or $4 \bmod p$. We successively compute the orbits mod p:

For $a = 1 \bmod p$:

$$x_{\text{in}} = 0 \to f(0) = 1 \to f^2(0) = 2 \to f^3(0) = 0$$

Hence, there is an attractive cycle of order 3.

For $a = 2 \bmod p$:

$$x_{\text{in}} = 0 \to f(0) = 2 \to f^2(0) = 1 \to f^3(0) = 3 \to f^4(0) = 1$$

which shows an indifferent cycle of order 2.

Similarly, in a simplified notation, for $a = 3 \bmod p$:

$$x_{\text{in}} = 0 \to 3 \to 2 \to 2 \qquad \text{(indifferent fixed point)}$$

For $a = 4 \bmod p$:

$$x_{\text{in}} = 0 \to 4 \to 0 \qquad \text{(attractive cycle of order 2)}$$

On the other hand, if $|a|_5 < 1$, $a = 0 \pmod p$ and $x_{\text{in}} = 0 \to 0$, which indicates an attractive fixed point.

In general, one finds, of course, following Eq. (3.11), that there is always a fixed point at $\frac{1}{2}[1 - (1 - 4a)^{1/2}] \simeq a$ when $|a|_p < 1$ and, in this case, there is obviously no other attractive cycle.

What the example also shows is that there are only two subregions of values of a, with $|a|_5 = 1$, for which an attractive cycle is possible. For arbitrary p, there will be $(p-1)/2$ such subregions. Indeed, for the orbit to pass through $x=0 \pmod p$ again, there must clearly be a solution to $f(x)=x^2+a=0 \pmod p$. Thus, an attractive cycle is possible only if $-a$ is a square in Q_p and this is the case for precisely half the mod p values of a with $|a|_p=1$.

As a last remark, let us point out that an important feature of the p-adic quadratic map, in contradistinction with the real case, is the absence of bifurcations: there is no value of a for which an attractive fixed point splits into an attractive cycle of order 2. This is an unavoidable consequence of the disconnected nature of Q_p.

4. INDIFFERENT FIXED POINTS AND TOPOLOGICAL CONJUGACY

In this section we analyze in some detail the quadratic map near an indifferent fixed point. At the price of some extra algebra, a similar analysis could be made near indifferent periodic points.

Assume thus that one computes the orbit of a point x near an indifferent fixed point to a given accuracy, say modulo p^{n+1},

$$x=x_0+x_1 p+\cdots+x_n p^n, \qquad 0\leqslant x_i\leqslant p-1 \tag{4.1}$$

p-adically, this is quite meaningful, since the map involves only p-adic integers and since terms of norm $p^{-(n+1)}$ can never add up to give a contribution of norm p^{-n}.

To the approximation defined by Eq. (4.1), x can only take a finite number of values (precisely p^{n+1}) and its orbit, i.e., $\{x, f(x), f^2(x),...\}$ will inevitably start repeating itself, after at most p^{n+1} terms. Iterations performed on a few examples suggest that these orbits are approximately periodic, with periods growing regularly with the accuracy of the computation, and that the orbit of any point covers densely some subinterval of $\mathbb{Z}_p$. These are precisely the required conditions for having a "quasiperiodic" behavior. We will first show that the possible approximate periods are $r\cdot p^\lambda$ $(\lambda\geqslant 0)$, where r is the smallest divisor of $p-1$ for which $[f'(x)]^r=1 \pmod p$.

To prove this statement, assume that

$$f(x)=x+\sigma(x)\, p^\alpha \tag{4.2}$$

with

$$|f'(x)|_p=1, \qquad f'(x)\neq 1 \pmod p, \qquad |\sigma(x)|_p=1, \qquad \alpha\geqslant 1$$

Then

$$f^2(x) \simeq f(x) + f'(x)\,\sigma(x)\,p^\alpha + \cdots$$
$$\simeq x + \sigma(x)\,p^\alpha + f'(x)\,\sigma(x)\,p^\alpha + \cdots \tag{4.3}$$

Iterating this computation, one finds

$$f^m(x) \simeq x + [1 + f'(x) + \cdots + f'^{m-1}(x)]\,\sigma(x)\,p^\alpha + \cdots$$
$$\simeq x + \frac{1 - f'(x)^m}{1 - f'(x)}\,\sigma(x)\,p^\alpha + \cdots \tag{4.4}$$

Now, if r is the smallest divisor of $p-1$ such that $f'(x)^r = 1 \pmod p$, then

$$f^r(x) \approx x + \mu(x)\,p^{\alpha+1} + \cdots \tag{4.5}$$

with $|\mu(x)|_p \leqslant 1$ and the first approximate period is thus r. Define

$$h(x) = f^r(x) \tag{4.6}$$

Clearly,

$$h'(x) = f'(f^{r-1}(x)) \cdots f'(x)$$
$$\simeq [f'(x)]^r = 1 \pmod p \tag{4.7}$$

Repeating for $h(x)$ the calculation done above for $f(x)$ gives

$$h^m(x) \simeq x + [1 + h'(x) + \cdots + h'^{m-1}(x)]\,\mu(x)\,p^{\alpha+1} + \cdots$$
$$\simeq x + m\mu(x)\,p^{\alpha+1} + ,\ldots, \qquad |\mu(x)|_p \leqslant 1 \tag{4.8}$$

A more accurate approximate periodicity occurs for $m = p^\lambda$ and this completes the proof of the statement.

However, this does not prove that the mapping is truly quasiperiodic: the chosen point x could be an element of a higher-order cycle, namely, it might happen that Eq. (4.8) reads

$$h^m(x) = x \quad \text{exactly } [\mu(x) = 0] \text{ for some large } m$$

In the remainder of this section, we will show how topological conjugacy[1] can be used to solve the problem. Rather than argue in full generality, we will show that in a suitable range of the parameter a and the point x, the quadratic map is equivalent to a linear map (actually the "derivative" map) and that this map is quasiperiodic. The conjugacy relating these two maps is of course nonlinear.

Let $\tilde{x}$ be the *exact* indifferent fixed point of the quadratic map [Eq. (3.2)]. Thus, $f(\tilde{x}) = \tilde{x}$ and $|f'(\tilde{x})|_p = 1$. We consider a set of points close to $\tilde{x}$, i.e.,

$$x = \tilde{x} + \delta \qquad \text{with} \quad |\delta|_p \leqslant 1/p \tag{4.9}$$

On this set, $f(x)$ is linearly conjugate to $g(\delta)$,

$$g(\delta) = 2\tilde{x}\delta + \delta^2 \tag{4.10}$$

Indeed, with

$$T(\delta) = \tilde{x} + \delta \tag{4.11}$$

$$T^{-1}fT = g \tag{4.12}$$

Our next task is to show that under certain conditions, $g(\delta)$ is topologically conjugate to the linear map $L(\delta)$ with

$$L(\delta) = 2\tilde{x}\delta := \omega\delta \tag{4.13}$$

This linear map is of course much easier to study. In almost all cases, there are only two kinds of points: (i) $\delta = 0$, which is the fixed point; and (ii) all other points are quasiperiodic: their period increases forever as the accuracy defined by Eq. (4.1) improves.[12]

The only exceptions occur when ω^r is exactly equal to 1 for a divisor r of $p-1$. If ω^r is only approximately equal to 1, we may write

$$\omega^r = 1 + \gamma p^\beta \tag{4.14}$$

with $|\gamma|_p = 1$ and $\beta \geqslant 1$, and, using the binomial expansion,

$$(\omega^r)^{p^\lambda} \simeq 1 + p^\lambda \gamma p^\beta + \cdots \neq 1 \tag{4.15}$$

Let us assume, for definiteness, that $|\delta|_p = p^{-\alpha}$. To prove the topological conjugacy of L and g, we must construct an homeomorphism U from $p^\alpha \mathbb{Z}_p \to p^\alpha \mathbb{Z}_p$ such that

$$U^{-1}LU = g \tag{4.16}$$

Writing

$$U(\delta) = q_1\delta + q_2\delta^2 + q_3\delta^3 + \cdots \tag{4.17}$$

this series will converge if $\lim_{n\to\infty} |q_n\delta^n|_p \to 0$.

The unknown coefficients q_n are determined recursively from the identity

$$(LU)(\delta) = (Ug)(\delta) \tag{4.18}$$

or

$$\omega(q_1\delta + q_2\delta^2 + q_3\delta^3 + \cdots) = q_1(\omega\delta + \delta^2) + q_2(\omega\delta + \delta^2)^2 + q_3(\omega\delta + \delta^2)^3 + \cdots \tag{4.19}$$

This yields (q_1 may always be taken $= 1$)

$$\begin{aligned} \omega q_2 &= q_1 + q_2\omega^2 \\ \omega q_3 &= 2q_2\omega + q_3\omega^3 \\ \omega q_4 &= q_2 + 3q_3\omega^2 + q_4\omega^4, \ldots \end{aligned} \tag{4.20}$$

In general, we have

$$(\omega - \omega^{2n})\, q_{2n} = \sum_{j=n}^{2n-1} \lambda_j q_j \tag{4.21}$$

$$(\omega - \omega^{2n+1})\, q_{2n+1} = \sum_{j=n+1}^{2n} \lambda'_j q_j \tag{4.22}$$

and, remembering that $|\omega|_p = 1$,

$$|\lambda_j|_p \quad \text{and} \quad |\lambda'_j|_p \leqslant 1 \tag{4.23}$$

It easily follows from these equations that, for $n \geqslant 2$,

$$|q_n|_p \leqslant \frac{1}{|(1-\omega)(1-\omega^2)\cdots(1-\omega^{n-1})|_p} \tag{4.24}$$

$$\leqslant \frac{1}{|(1-\omega^r)(1-\omega^{2r})\cdots|_p} \tag{4.25}$$

Equation (4.14) yields

$$1 - \omega^{\lambda r} \simeq -\lambda\gamma p^\beta \tag{4.26}$$

and thus

$$|q_n|_p \leqslant \prod_{\lambda=1}^{[(n-1)/r]} |\lambda\gamma p^\beta|_p^{-1} = |p^{[(n-1)/r]\beta}|_p^{-1} \cdot \left| \left[\frac{n-1}{r}\right]! \right|_p^{-1} \tag{4.27}$$

$\{[(n-1)/r]$ is the integral part of $(n-1)/r\}$.

Using the result[4] that for $p^k \leqslant m < p^{k+1}$

$$|m!|_p \geqslant p^{-m(1-p^{-k})/(p-1)} \tag{4.28}$$

we finally obtain that

$$|q_n \delta^n|_p \leqslant C p^{-\{(n-1)/r(p-1)\}\{(p-1)(r\alpha-\beta)-1\}} \tag{4.29}$$

Hence, the series for U converges if $r\alpha - \beta > 0$ (for $p \geqslant 3$).

We now specialize to the cases $r = 1$ and $r = 2$ and we show that the lack of convergence of (4.17) for $r\alpha \leqslant \beta$ is related to the appearance of other cycles in the neighborhood of the fixed point. If $r = 1$, then $\omega \equiv 1 \pmod p$ and the fixed point satisfies $\tilde{x} = 1/2 \pmod p$. The second fixed point thus has the same first digit as $\tilde{x}$ [remember (3.11)]. Since the linear map $L(\delta) = 2\tilde{x}\delta$ has only one fixed point, it can be topologically conjugate to the quadratic map only in a neighborhood of $\tilde{x}$ that excludes the other fixed point. It might be interesting to investigate the case $a = 1/4$, for which the two fixed points coincide and $\omega = 1$ ($\beta \to \infty$). If $r = 2$, then $\omega = -1 \bmod p$. This implies $a = -3/4 \bmod p$ and $\tilde{x} = -1/2 \bmod p$. But if $a = -3/4 - d^2/4$ ($|d| \leqslant p^{-1}$), there is a 2-cycle at $x_\pm = (-1 \pm d)/2$, i.e., close to the fixed point $\tilde{x} = -1/2 \bmod p$. Once again one can verify that the condition "x belongs to a 'ball' centered at $\tilde{x}$ and excluding the 2-cycle" is equivalent to $r\alpha - \beta > 0$.

We illustrate this on two examples (both for $p = 5$, $r = 2$).

First, consider $a = -3/4 - 1 \cdot 5^2 + \dots$. There is a 2-cycle at $x_\pm = -1/2 \pm 1.5 + \dots$, and the fixed point is $\tilde{x} = -1/2 - 1/2 \cdot 5^2 \dots$, giving $\omega^2 = 1 + 2 \cdot 5^2 \dots$, that is, $\beta = 2$. Hence, the condition $2 \cdot \alpha - \beta > 0$ requires $\alpha \geqslant 2$, so that the quasiperiodic behavior is achieved for any point x strictly closer to the fixed point than the 2-cycle.

On the other hand, if $a = -3/4 + a_1 \cdot 5 + \dots$ ($a_1 \neq 0$) (i.e., the 2-cycle does not exist), with the fixed point $\tilde{x}$ now around $-1/2 + a_1/2 \cdot 5$, then $\omega^1 = -1 + a_1 \cdot 5$, so that $\beta = 1$. Here the condition $2 \cdot \alpha - \beta > 0$ is fulfilled for any $\alpha \geqslant 1$: the map is quasiperiodic for every x such that $|x - \tilde{x}|_5 < 1 (x = 2 + \dots)$.

Our method for analyzing the behavior of a map around an indifferent fixed point is similar to the one used on $\mathbb{C}$, with the role of ω being played by a complex phase: $\exp(2\pi i \gamma)$. But finding which γ's lead to a convergent homeomorphism [see (4.16) and (4.17)] is a delicate matter,[13] in contrast with the simplicity of the p-adic case.

To complete the proof of the topological conjugacy of the linear and quadratic maps, under the conditions just stated, it remains to be shown that $U^{-1}(\delta)$ exists or that the expansion for $U^{-1}(\delta)$ converges as well. Writing

$$U^{-1}(\delta)=r_1\delta+r_2\delta^2+r_3\delta^3+\ldots \tag{4.30}$$

and identifying coefficients of the powers of δ in the identity

$$U^{-1}(U(\delta))=\delta \tag{4.31}$$

gives recursive relations for the r_n:

$$r_1=q_1=1 \tag{4.32}$$

$$r_n=-\sum_{j=1}^{n-1} r_j \sum_{\alpha_1,\alpha_2\cdots=0}^{p-1} K^j_{\alpha_1\cdots\alpha_{n-j+1}} q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_{n-j+1}^{\alpha_{n-j+1}} \tag{4.33}$$

where the sums over α_k are restricted to

$$\begin{aligned} \alpha_1+\alpha_2+\cdots+\alpha_{n-j+1}&=j \\ 1\cdot\alpha_1+2\cdot\alpha_2+\cdots+(n-j+1)\,\alpha_{n-j+1}&=n \end{aligned} \tag{4.34}$$

The coefficients $K^j_{\alpha_1\cdots\alpha_{n-j+1}}$ are p-adic integers. From (4.33) one deduces that

$$|r_n|_p\leqslant \max_{1\leqslant j\leqslant n-1}\{|r_j|_p\,|q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_{n-j+1}^{\alpha_{n-j+1}}|_p\}$$

and using the bound previously derived on $|q_k|_p$, namely

$$|q_k^{\alpha_k}|_p\leqslant p^{[(k-1)/r]\alpha_k\mu}, \qquad \mu=\beta+(p-1)^{-1}\geqslant 1 \tag{4.35}$$

with the constraints on the α_k,

$$|q_1^{\alpha_1}\cdots q_{n-j+1}^{\alpha_{n-j+1}}|_p\leqslant p^{(\mu/r)(n-j)} \tag{4.36}$$

which leads to

$$|r_n|_p\leqslant \max_{1\leqslant j\leqslant n-1}\{|r_j|_p\,p^{(\mu/r)(n-j)}\} \tag{4.37}$$

To find this maximum, consider the last term in this expression, namely $|r_{n-1}|_p\,p^{\mu/r}$. One has, from Eq. (4.37),

$$|r_{n-1}|_p\,p^{\mu/r}\leqslant \max_{1\leqslant j\leqslant n-2}\{|r_j|_p\,p^{(\mu/r)(n-j)}\} \tag{4.38}$$

Hence, this last term is not larger than any other one. Repeating the argument, one concludes that no term in Eq. (4.37) is larger than the first. This finally leads to the same condition as before ($r\alpha > \beta$) and concludes the proof.

5. CHAOS

In this last section, we concentrate our attention on the quadratic map f [Eq. (3.2)] in the region $|a|_p > 1$. As mentioned in Section 3, initial values of x such that $|x^2_{\text{in}}|_p > |a|_p$ or $|x^2_{\text{in}}|_p < |a|_p$ lead to diverging sequences $|f^n(x_{\text{in}})|_p \to \infty$. More precisely, bounded orbits are possible only if $a = -\gamma^2$ with γ an element of Q_p.

Let I be the compact set

$$I = \{x \mid \ |x|_p \leqslant |\gamma|_p\} \tag{5.1}$$

It splits into three disjoint subsets, namely

$$I_+ = \{x \mid x = \gamma + y, \ |y|_p \leqslant 1\} \tag{5.2a}$$

$$I_- = \{x \mid x = -\gamma + y, \ |y|_p \leqslant 1\} \tag{5.2b}$$

$$I_0 = I \backslash (I_+ \cup I_-) \tag{5.2c}$$

This last set contains the points which escape from I after one iteration of f and thus eventually end up at infinity. On the other hand, I_+ is mapped exactly once by f on the whole of I:

(i) $f(x) = f(\gamma + y) = 2y\gamma + y^2$, hence $|f(x)|_p \leqslant |\gamma|_p$.

(ii) The equation $f(x) = z$ for any z in I admits a unique solution in I_+. Indeed,

$$2y\gamma + y^2 = z \tag{5.3}$$

gives

$$y = -\gamma + \gamma\left(1 + \frac{z}{\gamma^2}\right)^{1/2} \simeq \frac{z}{2\gamma} + \dots$$

where the square root always exists since $|z/\gamma^2|_p \leqslant p^{-1}$ and $p \geqslant 3$. The sign is chosen in such a way that $|y|_p \leqslant 1$.

The same proof obviously holds for I_- as well.

The points of I can now be split further according to their fate after two iterations. Focusing on the points which remain in I, let us denote by I_{++} (respectively I_{+-}) the subset of points in I_+ which is mapped onto I_+

(respectively I_-). The corresponding subsets of I_- will be denoted I_{-+} and I_{--}, respectively.

Repeating the procedure, it is clear that 2^n subsets of I are mapped onto I by f^n and each of these subsets can be put into a one-to-one correspondence with a specific sequence of n +'s and −'s.

It will be convenient to introduce two (commuting) maps σ and τ from the space of sequences of length n to the space of sequences of length $n-1$: σ will be the map corresponding to the "omission" of the first entry of a sequence, while τ will omit the last entry. Thus, for example,

$$\sigma(++-)=(+-), \qquad \tau(++-)=(++)$$

Let us now assume that the following properties hold for all sequences s of length n:

(a) Subsets of I corresponding to different sequences are disjoint.

(b) $f(I_s)=I_{\sigma(s)}$, which implies that $f^n(I_s)=I$.

(c) $I_s \subset I_{\tau(s)} \subset I_{\tau(\tau(s))} \cdots \subset I$.

These properties are trivially true for $n=1$ and 2 as indicated above. We will now show that if they are true for sequences of length n, they also hold for sequences of length $n+1$ and hence they are valid for any length.

Any sequence of length $n+1$ can be written as $s+$ or $s-$, where s is a sequence of length n. Property (c) implies that

$$I_{\sigma(s)} \supset (I_{\sigma(s)+} \cup I_{\sigma(s)-}) \tag{5.4}$$

The other points in $I_{\sigma(s)}$ escape from I after n iterations. Property (b) and Eq. (5.4) allow us to define two subsets I_{s+} and I_{s-} of I_s with

$$f(I_{s+}) := I_{\sigma(s)+} = I_{\sigma(s+)}$$
$$f(I_{s-}) := I_{\sigma(s)-} = I_{\sigma(s-)}$$

I_{s+} and I_{s-} are clearly disjoint since $I_{\sigma(s)+}$ and $I_{\sigma(s)-}$ were assumed to be and this completes the recursive proof of (a)–(c).

The image under f of a small interval of Haar measure δ around a point x in I_+ or I_- is an interval of measure $|f'(x)|_p\,\delta=|\gamma|_p\,\delta$: all regions of I_+ and I_- get "blown up" by the same factor $|\gamma|_p$. The measure of the subset of I corresponding to a sequence of length n in thus

$$|\gamma|_p^{-n+1} \; (I_+ \text{ and } I_- \text{ have measure } 1) \tag{5.5}$$

By property (c), the set of points which do not escape from I lies in infinite intersections of nested closed intervals. These points, which are associated with infinite sequences of +'s or −'s, form a closed, nonempty set which, because of (5.5), contains no intervals. This set is clearly "perfect": every point is an accumulation point. There are indeed an infinity of points within a distance $|\gamma|_p^{-n+1}$ of any point of this set since the corresponding sequences need only have identical first n entries.

This set of accumulation points, which we will call Λ, is thus a Cantor set. To compute its Hausdorff dimension D_Λ, we cover it with intervals of measure $\delta = |\gamma|_p^{-n+1}$. The Hausdorff dimension D measures the growth of the number N of such intervals when $\delta \to 0$,

$$N \sim (\delta)^{-D}$$

Here, we have

$$2^n = 2(|\gamma|_p^{-n+1})^{-(\ln 2)/\ln |\gamma|_p}$$

and hence

$$D_\Lambda = \frac{\ln 2}{\ln |\gamma|_p} \qquad \text{with} \quad |\gamma|_p \geqslant p \geqslant 3 \tag{5.6}$$

It may be useful to summarize what has been proven so far. When $|a|_p > 1$, most points of Q_p eventually end up at infinity under iterations of f. Points with a bounded orbit exist only if $a = -\gamma^2$. They belong to a Cantor set Λ and each point of this set is in one-to-one correspondence with an infinite sequence s of +'s and −'s. Two points in Λ are close to each other if the first few entries of the corresponding sequences are identical. On the set Λ, f takes the particularly simple form of the shift map σ,

$$\sigma(+s) = \sigma(-s) = s \tag{5.7}$$

It is quite remarkable that these results precisely correspond to those of the *real* map $x \to \mu x(1-x)$ when $\mu > 2 + \sqrt{5}$. Equation (5.7) is an example of symbolic dynamics.[1] This particular dynamical system is simple enough to be completely understood.

Before discussing the properties of such a system, let us first derive a more explicit expression for the points in the set Λ. A point x which remains in I after one iteration must be of the form

$$x = \lambda_{-1}\gamma + x_0 + x_1\gamma^{-1} + x_2\gamma^{-2} + \ldots \tag{5.8}$$

with $\lambda_{-1} = \pm 1$. Demanding that this point x belongs to Λ yields recursive equations for the "generalized digits" x_i. These equations can be solved by introducing for each i a new dichotomic variable λ_i, with possible values ± 1. Then x_i is expressed in terms of $\lambda_{-1}, \lambda_0, \dots, \lambda_i$. The λ_i can be chosen to be precisely the entries of the sequence s previously associated with the point x of Λ. Equation (5.8) gives

$$f(x) = x^2 - \gamma^2 = 2x_0 \lambda_{-1} \gamma + \dots$$

which must satisfy the same constraints as x, i.e., $2x_0\lambda_{-1}$ must be equal to $\lambda_0 = \pm 1$:

$$2x_0 \lambda_{-1} = \lambda_0 \qquad \text{or} \qquad x_0 = \lambda_{-1}\lambda_0/2 \tag{5.9}$$

The next step gives

$$x = \lambda_{-1}\gamma + \lambda_{-1}\lambda_0/2 + x_1\gamma^{-1} + \dots \tag{5.10}$$

$$f(x) = \lambda_0\gamma + (1/4 + 2\lambda_{-1}x_1) + \dots \tag{5.11}$$

and once again, $1/4 + 2\lambda_{-1}x_1$ must have the same form in terms of λ_0 and λ_1 as the corresponding element x_0 of the expansion of x had in terms of λ_{-1} and λ_0.

Precisely, one must have

$$\tfrac{1}{4} + 2\lambda_{-1}x_1 = \lambda_0\lambda_1/2 \qquad \text{or} \qquad x_1 = \tfrac{1}{4}\lambda_{-1}\lambda_0\lambda_1 - \tfrac{1}{8}\lambda_{-1} \tag{5.12}$$

This procedure can obviously be repeated indefinitely. In general, the coefficient of order j of x, x_j, is some expression $A_j(\lambda_{-1}, \lambda_0, \dots, \lambda_j)$ and the coefficient of the same order j of $f(x)$ has the form

$$B_j(\lambda_{-1}, \lambda_0, \dots, \lambda_j) + 2\lambda_{-1}x_{j+1} \tag{5.13}$$

It is always possible to solve the linear equation

$$B_j(\lambda_{-1}, \dots, \lambda_j) + 2\lambda_{-1}x_{j+1} = A_j(\lambda_0, \lambda_1, \dots, \lambda_{j+1}) \tag{5.14}$$

for x_{j+1}. It is straightforward to show that $|x_j|_p \leqslant 1$. This proves that the points in Λ are given by convergent series

$$x = \sum_{j=-1}^{\infty} x_j \gamma^{-j} \simeq \lambda_{-1}\gamma + \frac{\lambda_{-1}\lambda_0}{2} + \frac{1}{4}\left(\lambda_{-1}\lambda_0\lambda_1 - \frac{1}{2}\lambda_{-1}\right)\gamma^{-1}$$
$$+ \frac{1}{8}\lambda_{-1}\lambda_1(\lambda_0\lambda_2 - 1)\gamma^{-2} + \dots \tag{5.15}$$

where x_j is a function of $\lambda_{-1}, \lambda_0, \dots, \lambda_j$. The sequence of dichotomic variables $(\lambda_{-1}, \lambda_0, \lambda_1, \dots)$ is precisely the sequence s which was defined previously and which was associated with the point x belonging to Λ. On the sequence $(\lambda_{-1}, \lambda_0, \lambda_1, \ldots)$, the dynamics is given by the shift map σ, since, by construction, the point $f(x)$ depends on $\lambda_0, \lambda_1, \lambda_2, \ldots$ in exactly the way the point x depends on $\lambda_{-1}, \lambda_0, \lambda_1, \ldots$.

Let us distinguish three types of points in the set Λ:

(i) *Periodic* points: they correspond to sequences s with $\sigma^n(s) = s$; $(+, +, +, +, \ldots)$ and $(-, -, -, -, \ldots)$ are the fixed points; $(+-+-+-+-+\ldots)$ and $(-+-+-+-+-\ldots)$ make up the cycle of order 2, and so on. In particular, there are 2^n points of period n.

(ii) *Eventually periodic* points, which correspond to sequences with $\sigma^n(\sigma^k(s)) = \sigma^k(s)$.

(iii) *Nonperiodic* points.

The following properties are easily proved:

1. Periodic points are dense in Λ

2. The orbit of any point is highly unstable: the tiniest change of the initial point will have a large effect in the long run. This is usually called "sensitive dependence on initial conditions."

3. There are (nonperiodic) points whose orbit is dense in Λ, i.e., the orbit of one point comes arbitrarily close to any point in Λ. A simple example is provided by the sequence constructed by successively listing all "blocks" of $+$'s and $-$'s of length 1, 2, 3,...:

$$s = (+, -; +, +; +, -; -, +; -, -; +, +, +; +, +, -; + \; - \; +; \text{etc.})$$

Following Devaney,[1] a map with such properties is *chaotic*. We have thus proved that the p-adic quadratic map with $|a|_p > 1$ is chaotic on the Cantor set Λ. This disproves a conjecture made in ref. 12.

It is clear that the techniques developed in this paper can be applied to other mappings. As an example consider

$$f(x) = x^3 - \gamma^3, \qquad |\gamma|_p > 1 \tag{5.16}$$

If 1 is the only cubic root of 1 belonging to Q_p, only a single point has a bounded orbit: the fixed point. The situation is much more interesting if the other cubic roots of 1, $(-1 \pm \sqrt{-3})/2$, also belong to Q_p. The points which do not escape to infinity can be written as $(p > 3)$

$$x \simeq \lambda_{-1}\gamma + \tfrac{1}{3}\lambda_{-1}\lambda_1\gamma^{-1} + \tfrac{1}{3}(\tfrac{1}{3}\lambda_{-1}\lambda_1\lambda_3 - \lambda_{-1}\lambda_1^2)\,\gamma^{-3} + \ldots \tag{5.17}$$

with $\lambda_{-1}^3 = \lambda_1^3 = \lambda_3^3 = \ldots = 1$. This is again a Cantor set and the parametrization can be chosen in such a way that the action of f on the point x is equivalent to that of the shift map on the sequence $(\lambda_{-1}, \lambda_1, \lambda_3, ...)$.

An obvious question is whether chaotic behavior can occur not only on a Cantor set, but on sets of nonzero measure as well. The answer to this question is yes. Consider the following map from $\mathbb{Z}_p$ to $\mathbb{Z}_p$:

$$x = x_0 + x_1 p + x_2 p^2 + \dots \xrightarrow{h} x_1 + x_2 p + x_3 p^2 + \dots \tag{5.18}$$

This map is p-adically continuous and differentiable,

$$h'(x) = p^{-1} \tag{5.19}$$

$$h''(x) = 0 \tag{5.20}$$

Nevertheless, because of the disconnectedness of the p-adic field Q_p, the map is *not* trivial: $h(x)$ is not the map x/p and it does not have a continuous real counterpart.[3,4] The map h is again the shift map, but this time it acts on infinite sequences $(x_0, x_1, x_2, ...)$, where x_i are the digits of a p-adic number, i.e., $0 \leqslant x_i \leqslant p-1$. Clearly, the periodic or eventually periodic points for h are the rational numbers, while the nonperiodic points are those of $Q_p \backslash Q$. The conclusion is the same as before: the map h is chaotic!

ACKNOWLEDGMENTS

We thank C. Alacoque and P. Ruelle for interesting discussions and J. Bricmont for reading the manuscript.

REFERENCES

1. R. L. Devaney, *An Introduction to Chaotic Dynamical Systems* (Benjamin/Cummings, 1986); H. O. Peitgen and P. H. Richter, *The Beauty of Fractals* (Springer-Verlag, Berlin, 1986).
2. P. Cvitanovic, *Universality in Chaos* (Adam Hilger, Bristol, 1984), and references therein.
3. N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta Functions* (Springer-Verlag, Berlin, 1984); K. Malher, *p-adic Numbers and their Functions* (Cambridge University Press, Cambridge, 1983).
4. I. M. Gel'fand, M. I. Graev, and I. I. Pyatetskii-Shapiro, *Representation Theory and Automorphic Functions* (Saunders, London, 1966).
5. I. V. Volovich, *Classical Quantum Gravity* **4**:L83 (1987); B. Grossmann, Rockefeller University Preprint DOE/ER/40325-7-TASK B (1987); P. G. O. Freund and M. Olson, *Nucl. Phys. B* **297**:86 (1988); Y. Meurice, Argonne National Laboratory Preprint ANL-HEP-PR-87-114 (1987); G. Parisi, *Mod. Phys. Lett. A* **1988**:639; V. S. Vladimirov and I. V. Volovich, Preprint SMI O1/88 (1988); C. Alacoque *et al.*, UCL-IPT-88-05, *Phys. Lett. B* **211**:59 (1988).

6. P. G. O. Freund and M. Olson, *Phys. Lettt. B* **199**:186 (1987).
7. P. G. O. Freund and E. Witten, *Phys. Lett. B* **199**:191 (1987).
8. J. L. Gervais, *Phys. Lett. B* **201**:306 (1988); E. Marinari and G. Parisi, *Phys. Lett. B* **203**:52 (1988); H. Yamakoshi, *Phys. Lett. B* **207**:426 (1988); I. Ya. Aref'eva, B. G. Dragovic, and I. V. Volovich, Preprint IF-14/88 (1988); L. Brekke, P. G. O. Freund, M. Olson, and E. Witten, *Nucl. Phys. B* **302**:365 (1988).
9. J. H. Hannay and M. V. Berry, *Physica* **1D**:267 (1980); Y. Nambu, Field theory of Galois' fields, in *E. S. Fradkin Festschrift.*
10. C. N. Yang, in *Schrödinger, Centenary Celebration of a Polymath* (Cambridge University Press, Cambridge, 1987).
11. R. Rammal, G. Toulouse, and M. A. Virasoro, *Rev. Mod. Phys.* **58**:765 (1986); B. Grossmann, Rockefeller University Preprint DOE/ER/40325-8-TASK *B* (1987).
12. S. Ben-Menahem, *p*-adic Iterations, Preprint TAUP 1627-88 (1988).
13. C. L. Siegel and J. Moser, *Lectures on Celestial Mechanics* (Springer-Verlag, New York, 1971).