

# The arithmetic of discretized rotations

F. Vivaldi

*School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, UK*

**Abstract.** We consider the problem of planar rotation by an irrational angle, where the space is discretized to a lattice by means of a round-off procedure which preserves invertibility. For a dense set of values of the rotational angle, this mapping admits an embedding into a dynamical system which is expanding with respect to a non-archimedean metric, and which has a complete symbolic dynamics. We consider the arithmetical phenomena that arise in such systems, and their relation to the question of pseudo-randomness in discrete dynamics. The exposition is organized around the concept of *minimal modules*, the lattices of minimal complexity which support periodic orbits.

**Keywords:** Round-off errors, discretized rotations,  $p$ -adic numbers

**PACS:** 65P20, 37D20, 11S99

## INTRODUCTION

Dynamical systems with discrete phase space present a specific set of challenges. How does one choose a topology? How does one characterize predictable vs. unpredictable motions? Approaching these questions involves looking at asymptotics, whereby some natural system parameter (the size, typically) becomes large. However, on a discrete phase space, the study of orbit asymptotics is often difficult, sometimes intractable.

In this paper we explore some of these issues in the analysis of the lattice map

$$\Phi : \mathbb{Z}^2 \mapsto \mathbb{Z}^2 \quad (x, y) \mapsto (\lfloor \alpha x \rfloor - y, x) \quad \alpha = 2 \cos(2\pi\theta) \quad (1)$$

where  $\lfloor \cdot \rfloor$  is the floor function —the largest integer not exceeding its argument. One verifies that  $\Phi$  is invertible. Without the floor function, equation (1) represents a one-parameter family of linear maps of the plane, conjugate to rotation by the angle  $\theta$ . The floor function models the effect of round-off, pushing the point  $(\alpha x - y, x)$  to the nearest lattice point on the left.<sup>1</sup> The lattice map should be regarded as a discrete approximation of the planar map: the discretization length is fixed, and the limit of vanishing discretization corresponds to motions at infinity.

The family of maps (1) displays a vast range of mathematical phenomena, which have been object of intense investigations [1, 2, 3, 4, 5, 6, 7, 8]. Here we are interested in a special set of *rational* values of the parameter  $\alpha$ , namely

$$\alpha = \frac{q}{p} \quad p \text{ prime} \quad |q| < 2p. \quad (2)$$

---

<sup>1</sup> This procedure is arithmetically nicer than rounding to the nearest lattice point, while producing analogous dynamical phenomena.

It turns out that, for this choice of parameters, the map  $\Phi$  admits an embedding into an expanding map of the  $p$ -adic integers  $\mathbb{Z}_p$ , which features a complete symbolic dynamics on  $p$  symbols. The set  $\mathbb{Z}_p$  consists of all expressions of the type

$$\chi = \sum_{k=m}^{\infty} c_k p^k \quad c_k \in \{0, \dots, p-1\}, \quad m \geq 0, \quad c_m \neq 0 \quad (3)$$

which converge with respect to the  $p$ -adic absolute value

$$|\chi|_p = \frac{1}{p^m}.$$

The function  $|\cdot|_p$  assumes discrete values, and satisfies the ultrametric inequality

$$|\chi + \chi'|_p \leq \max(|\chi|_p, |\chi'|_p). \quad (4)$$

With the topology induced by  $|\cdot|_p$ , the set  $\mathbb{Z}_p$  is Cantor set.

An expanding map with a complete symbolic dynamics is a very favourable dynamical scenario; it calls to mind the dynamical system given by multiplication by a prime  $p$  on the circle

$$\Psi: \quad x \mapsto px \pmod{1}, \quad (5)$$

also an expanding map with a complete symbolic dynamics on  $p$  symbols [9, section 1.7]. This is a much-studied toy model of ergodic theory, which has direct connections with deep arithmetical phenomena. See [10], for a friendly introduction to the question of algorithmic complexity in this dynamical system.

By comparing and contrasting the behaviour of the maps  $\Phi$  and  $\Psi$ , we will put into perspective the dynamical and arithmetical nature of round-off fluctuations. The exposition will be organized around the concept of *minimal modules*, which are lattices of minimal complexity that support periodic orbits. These are relevant to the study of pseudo-randomness and complexity in discrete dynamical systems. (For a parallel with quantum dynamics, see [11].) In both maps, the positive metric entropy of the embedding dynamical system provides an essential substrate for the existence of irregular motion on a lattice. At the same time, the presence of minimal modules guarantees—in ways which are still not fully understood—good properties of pseudo-randomness. The combined effect of these two ingredients is of great theoretical interest, and also of value in applications.

This paper is a new synthesis of research published elsewhere [12, 5, 6, 7, 13]. I assume some basic knowledge of integer and  $p$ -adic arithmetic: for background bibliography, see [14] and [15].

## PERIODIC ORBITS AND MINIMAL MODULES

If we represent the numbers in the unit interval in base  $p$

$$x = c_0 p^{-1} + c_1 p^{-2} + c_2 p^{-3} + \dots \quad c_k \in \{0, \dots, p-1\} \quad (6)$$

we find that the action of  $\Psi$  corresponds to the left digit shift

$$\Psi(x) = c_1 p^{-1} + c_2 p^{-2} + c_3 p^{-3} + \dots$$

The above dynamics is conjugate almost everywhere to the Bernoulli shift  $\sigma$  on the space of semi-infinite  $p$ -symbol sequences. This space, equipped with the usual topology, is a Cantor set. The conjugacy between  $\Psi$  and  $\sigma$  fails on the rationals whose denominator is a power of  $p$ , because these have two distinct representations as digit sequences. Disconnecting the interval at this dense set of points, we obtain a Cantor set.

The periodic orbits of  $\Psi$  comprise the set of rationals with denominator coprime to  $p$ , which is dense on the circle. The restriction of the map to such set is invertible. Because in equation (6) we may choose the coefficients  $c_k$  arbitrarily, the symbolic dynamics is complete. From this one infers that orbits of all periods exist, and that their number grows exponentially with the period. Specifically, given an arbitrary periodic code  $(\overline{c_0, c_1, \dots, c_{t-1}})$  with minimal period  $t$ , which represents a  $t$ -cycle, one finds

$$x = \sum_{k=0}^{\infty} c_k p^{-(k+1)} = \frac{1}{p^t - 1} \sum_{k=0}^{t-1} c_k p^{t-k-1}. \quad (7)$$

As an indicator of complexity, we define the *height*  $h$  of a reduced rational number  $a/b$ , as  $h(a/b) = \max(|a|, |b|)$ . In general, the height of a periodic point grows exponentially with the period; however, for some codes, the numerator and denominators may have a large common factor, resulting in periodic points of small height. Thus, for every positive integer  $t$ , we consider the smallest positive integer  $m$  such that the map  $\Psi$  has a  $t$ -periodic point with denominator  $m$ . We denote such  $m$  by  $M(t)$ .

The  $t$ -periodic points with denominator  $M(t)$  belong to the  $\mathbb{Z}$ -module<sup>2</sup>

$$\Lambda(t) = M(t)^{-1} \mathbb{Z} / \mathbb{Z}$$

which consists of  $M(t)$  equally spaced points on the unit circle. We call such module the *minimal module* for the period  $t$ ; the  $t$ -cycles on  $\Lambda(t)$  are those of minimal height.

**Proposition 1.** *The function  $t \mapsto \Lambda(t)$  is injective.*

This is true, because all points on  $\Lambda(t)$  whose numerator is coprime to  $M(t)$  have the same period  $t$ , from elementary properties of congruences. For all other points, cancellation takes place, and hence  $\Lambda(t)$  cannot be a minimal module for their period.

The quantity  $M(t)$  features wild fluctuations. For instance, for  $p = 2$

$$\begin{array}{c|cccc} t & 17 & 18 & 19 & 20 \\ \hline M(t) & 131071 & 19 & 524287 & 25 \end{array} \quad (8)$$

For general  $p$ , we have the bounds

$$M(1) = 1; \quad t + 1 \leq M(t) \leq p^t - 1 \quad t > 1. \quad (9)$$

---

<sup>2</sup> An additive group, closed under multiplication by integers.

The upper bound follows from (7), while the lower bound derives from the fact that the minimal module  $\Lambda(t)$  always includes the fixed point at zero, and therefore cannot have fewer than  $t + 1$  points. The data in (8) show that these bounds are sharp.

The  $t$ -periodic points with denominator  $M(t)$  are the rationals  $0 < a/M(t) < 1$  with  $a$  coprime to  $M(t)$ . There are  $\phi(M(t))$  of them, where  $\phi$  is Euler's function [14, chapter XVI]; hence the minimal module contains  $\phi(M(t))/t$  cycles of minimal period  $t$ . Roughly speaking, the smaller the number of cycles on the module, the smaller their height, that is, the amount of information needed to specify them. The extreme situation corresponds to the lower bound in (9): this is attained precisely when  $M = t + 1$  is a prime number, and  $p$  is a primitive root modulo  $M$ , namely a generator of the multiplicative group of the ring  $\mathbb{Z}/M\mathbb{Z}$ . At these values of  $t$ , the  $t$ -cycle consists of  $t$  equally spaced points, namely the whole lattice  $\Lambda(t)$ , excluding the origin. This is an extreme form of spatial uniformity, exemplified by the value  $t = 18$  in (8).

To analyze uniform distribution we proceed as follows. We choose, for definiteness, the point  $M(t)^{-1}$  as the initial condition for a representative  $t$ -cycle on the minimal module; then we consider the Weil sum

$$W(t, n) = \frac{1}{t} \sum_{k=0}^{t-1} e^{2\pi i n x_k} \quad x_k = \Psi^k(M(t)^{-1}) \quad (10)$$

where  $n$  is an integer. The function  $W(t, n)$  is periodic in  $n$  with period  $M$ , and its values belong to the closed unit circle. Let now  $T$  be an infinite set of positive integers. Then, according to Weil's criterion [16], the sequence of  $t$ -cycles with  $t \in T$  is uniformly distributed iff

$$\lim_{\substack{t \rightarrow \infty \\ t \in T}} W(t, n) = 0 \quad \forall n \neq 0. \quad (11)$$

If on the minimal module there is a single  $t$ -cycle, then the Weil's sum becomes a Ramanujan's sum [14, section 16.6], which can be evaluated explicitly. Let  $d = \gcd(n, M)$ . We have

$$\begin{aligned} W(t, n) &= \frac{1}{t} \sum_{\substack{0 \leq k < M \\ \gcd(k, M) = 1}} \exp\left(2\pi i \frac{kn}{M}\right) \\ &= \frac{d}{t} \sum_{\substack{0 \leq k < M/d \\ \gcd(k, M/d) = 1}} \exp\left(2\pi i \frac{kn/d}{M/d}\right) \\ &= \frac{d}{t} \mu(M/d) \quad t = \phi(M(t)), \quad d = \gcd(n, M) \end{aligned} \quad (12)$$

where  $\mu$  is the Möbius function [14, chapter XVI]. Because  $|\mu(x)| \leq 1$ , large values of the Weil's sum occur only if  $\gcd(n, M)$  is large. As  $t$  goes to infinity, so does  $M$ , so any sequence of orbits with a single  $t$ -cycle on the minimal module is uniformly distributed. Uniform distribution in the sense (11) holds for a much larger set of orbits than the one described above, namely orbits for which  $M(t)/t$  is small enough —see [17, 18] for details and generalizations.

So, in equation (11), we are led to consider the set  $T = T^*$  of periods  $t$  at which the function  $M(t)$  attains the lower bound in (9). We have seen that these are precisely the integers  $t$  for which  $r = t + 1$  is prime, and  $p$  is a primitive root modulo  $r$ . The study of such primes  $r$  is a classic arithmetical problem, known under the heading of Artin's conjecture [19]. If one assumes the generalized Riemann hypothesis<sup>3</sup> (GRH), then it is possible to show that the set  $T^*$  is not only infinite, but also has positive density among the primes (see below); this density is given by the so-called *Artin's constant* [20, page 304]

$$A = 0.373955813619202 \dots$$

Combining the above with the prime number theorem [21], we have that the number of periods  $t < N$  for which the minimal module  $\Lambda(t)$  achieves the lower bound in (9) admits the asymptotic estimate

$$\#\{t : t \in T^*, t < N\} \sim A \frac{N}{\log(N)}. \quad (13)$$

Without GRH, we do not even know if the set  $T^*$  is infinite. Defining the *density*  $D(X)$  of a set  $X \subset \mathbb{N}$  as

$$D(X) = \lim_{N \rightarrow \infty} \frac{1}{N} \#\{n < N : n \in X\} \quad (14)$$

we see that  $D(T^*) = 0$ . The notion of density can be defined in an obvious way on sets other than  $\mathbb{N}$ , such as the primes,  $\mathbb{Z}$ ,  $\mathbb{Z}^2$ , etc.

With a bit of extra work, one could also arrive to a conjectured asymptotic form for the set of periods  $t$  satisfying (12), which involves considering the moduli  $m$  having cyclic multiplicative group. We shall not pursue this matter here.

Minimal modules are difficult to compute, in the sense that they lead to non-polynomial time algorithms. A direct approach consists of constructing the ascending sequence  $d_i(t)$  of the divisor of  $p^t - 1$  greater than  $t$ , and then determining the multiplicative order of  $p$  modulo each of them. The smallest  $d_i(t)$  for which  $p$  has order  $t$  is  $M(t)$ . This procedure requires factoring  $p^t - 1$ , which for large  $t$  is plainly unfeasible. Alternatively, one may construct the elements of the ascending sequence of the integers  $m_i(t)$  such that  $t \mid \phi(m_i(t))$ , which lie in the range  $t + 1 \leq m_i \leq p^t - 1$ . For each  $m_i$ , we check whether or not the order of  $p$  modulo  $m_i$  is  $t$ : the smallest  $m_i$  for which this is true is  $M(t)$ . Constructing the  $m$ -sequence requires evaluating  $\phi(kt)^{-1}$  for  $k = 1, 2, \dots$  (or  $k = 2, 4, \dots$ , if  $t$  is odd); the difficulty originates from the need of knowing the prime factorization of  $t$ , which is a non-polynomial time problem [22].

We conclude this section with some brief remarks on related problems.

The constructions described above can be reformulated in higher dimensions, for hyperbolic toral automorphisms [23, 24]. The rationals  $\mathbb{Q}$  on the circle are replaced by algebraic numbers  $\mathbb{Q}(\lambda)$  on the torus, where  $\lambda$  is an eigenvalue of the automorphism. The multiplicative constant  $p$  in (5) is replaced by  $\lambda$ ; the periodic orbits with prime denominator—out of which the set  $T^*$  was constructed—are replaced by the so-called

---

<sup>3</sup> The analogue of the celebrated conjecture of Riemann, for the the zeta function of an algebraic number field.

*ideal orbits*, which belong to prime ideals in the ring  $\mathbb{Z}[\lambda]$  (see below, for explanation of the terminology). The arithmetical properties of  $T^*$  are similar, involving again Artin’s constant.

The upper bound in (9) is also of interest. It is attained precisely when  $p = 2$ ,  $t$  is prime, and  $2^t - 1$  is also prime —a so-called *Mersenne prime*. The orbit with initial condition  $M(t)^{-1}$  now has the same symbolic sequence as a rotation: these are the *sturmian sequences*, of minimal complexity [25]. The spatial distribution of these orbits is, in a sense, as far as possible from being uniform. The problem of the infinitude of Mersenne primes —the largest know primes— is also unsolved [20].

Finally, the map  $\Psi$ , which is defined over the circle, may also be represented over the  $p$ -adics. It is a contraction on  $\mathbb{Q}_p$  (the field of fractions of  $\mathbb{Z}_p$ , obtained by removing the constraint  $m \geq 0$  in (3)), and an isometry on  $\mathbb{Q}_r$ , for all primes  $r \neq p$ . In the former case, the dynamics is trivial, since every point is attracted to the origin at a constant rate. In the latter case, the dynamics is an ‘irrational rotation’. This terminology is justified as follows. For  $r \neq p$ , we have  $|p|_r = 1$ , namely  $p$  lies on the unit circle in  $\mathbb{Q}_r$ . Equivalently,  $p$  is a *unit* in  $\mathbb{Z}_r$ .<sup>4</sup> Furthermore,  $p$  is not a root of unity, because there is no positive integer  $k$  for which  $p^k = 1$ ; as a result, the only periodic point in  $\mathbb{Q}_r$  is the fixed point at the origin. Thus the space foliates into the union of invariant circles, and each circle in turn decomposes into a finite number of uniquely ergodic components, the same number of components for each circle [12]. This dynamical system has zero metric entropy; some aspects of computational complexity emerging in this context are discussed in [13]. Here we just mention that, in the limit of large  $k$ , the period of orbits of  $\Psi$  with denominator  $r^k$  is computable in polynomial time, thanks to the analytical properties of the  $p$ -adic logarithmic function. For this reason, these discrete motions should be regarded as being regular, predictable.

## DISCRETIZED ROTATIONS

The current state of affairs regarding the round-off map  $\Phi$  defined in (1) is summarized by the following

**Conjecture 1.** *All orbits of  $\Phi$  are periodic.*

This conjecture has been proved only for finitely many parameter values, corresponding to the rotation number  $\theta$  being rational with denominator 5, 8, 10, 12 (eight cases in all) [8]. For these values,  $\alpha$  is a quadratic irrational, and one can exploit the presence of exact scaling to develop computer-assisted proofs. Such proofs apply to a set of full density of initial conditions; the more tedious (albeit conceptually similar) proof for all initial conditions was carried out only in one case:  $\theta = 3/10$ . Although unbounded orbits have not been found, the possibility that boundedness could fail for a zero-density set should not be discounted. In [8], an unbounded orbit was constructed for a map obtained from (1) via a simple modification of the rounding procedure.

---

<sup>4</sup> A unit  $\eta$  in the ring  $\mathbb{Z}_r$  is a number such that  $\eta^{-1} \in \mathbb{Z}_r$ .

The periodicity conjecture was recently formulated for a system closely related to (1), with the ceiling instead of the floor function [26]. This dynamical system originated in number theory, in connection with the so-called shift radix systems, and the theory of Pisot and Salem numbers. A boundedness proof for the parameter  $\theta = 1/5$  is given in [27].

In the present case —cf. equation (2)— the parameter  $\alpha$  is rational; from (1) it then follows that  $\theta$  is irrational, apart from finitely many exceptions [28, chapter 2]. Proving the periodicity conjecture for irrational rotational angles seems quite difficult.

When  $\alpha = q/p$  in (1), we define a symbolic dynamics on  $p$  symbols as follows

$$c : \mathbb{Z}^2 \rightarrow \{0, \dots, p-1\} \quad (x, y) \mapsto x \pmod{p}. \quad (15)$$

The next three theorems were proved in [5] (in a slightly more general setting). The first result characterizes the cylinder sets of the symbolic dynamics, namely the set of lattice points whose symbol sequence begins with a specified code.

**Theorem 1.** *There exists a nested sequence of lattices*

$$L_1 \supset L_2 \supset L_3 \supset \dots$$

with  $|\mathbb{Z}^2/L_k| = p^k$ , with the property that two points in  $\mathbb{Z}^2$  have the same  $k$ -code if and only if they are congruent modulo  $L_k$ .

It follows that *all* finite codes of the symbolic dynamics (15) are represented by orbits in  $\mathbb{Z}^2$ ; furthermore, any  $k$ -cylinder set in  $\mathbb{Z}^2$  has density  $p^{-k}$  —see equation (14), and the following remark.

Consider now the identity

$$f(x) = x^2 - qx + p^2 \equiv x(x - q) \pmod{p}. \quad (16)$$

The polynomial  $f(x)$  is irreducible in  $\mathbb{Q}$ , having negative discriminant. Moreover, the factors of  $f(x)$  modulo  $p$  are *distinct*, because  $p$  and  $q$  are coprime. Let  $\lambda$  be a root of  $f(x)$ , and consider the ring

$$\mathbb{Z}[\lambda] = \{m + n\lambda : m, n \in \mathbb{Z}\}.$$

The factorization (16) implies that the prime  $p$  splits in  $\mathbb{Z}[\lambda]$  into the product of two distinct prime ideals:  $p\mathbb{Z}[\lambda] = P\bar{P}$  (see, e.g., [28, chapter 3]). Recall that an ideal in a ring is an additive group closed under multiplication by ring elements. Geometrically, these ideals are two-dimensional lattices, and the product  $P\bar{P}$  alluded above is defined as the set of all finite sums  $\pi_1\bar{\pi}_1 + \dots + \pi_s\bar{\pi}_s$  with  $\pi_i \in P$  and  $\bar{\pi}_i \in \bar{P}$ .

The next result shows that the discrete phase space  $\mathbb{Z}^2$ , as well as the lattices  $L_k$ , are in fact more than two-dimensional lattices

**Theorem 2.** *The embedding*

$$\mathcal{L}_1 : \mathbb{Z}^2 \rightarrow \mathbb{Z}[\lambda] \quad (x, y) \mapsto px - \lambda y$$

defines an isomorphism  $\mathbb{Z}^2 \sim P$  of  $\mathbb{Z}$ -modules such that, for all  $k \geq 1$ , we have  $L_k \sim p^{k+1}$ .

This result provides the phase space with a multiplicative structure. Now, for all positive  $k$ , the finite ring  $\mathbb{Z}[\lambda]/P^k$  is isomorphic to  $\mathbb{Z}/p^k\mathbb{Z}$ . Under this isomorphism, an element  $\zeta$  in  $\mathbb{Z}[\lambda]$  maps to a unique residue class modulo  $p^k$ , and the sequence of these residue classes converges to a  $p$ -adic number. In particular, the roots of  $f(x)$  in  $\mathbb{C}$  correspond to the roots of  $f(x)$  in  $\mathbb{Q}_p$ . We denote the latter by  $\varphi$  and  $\bar{\varphi}$ ; they are identified as follows (cf. (16)):

$$\varphi \equiv 0 \pmod{p} \quad \bar{\varphi} \equiv q \pmod{p}. \quad (17)$$

Because  $q$  is coprime to  $p$ , we have that  $|\bar{\varphi}|_p = 1$ , that is,  $\bar{\varphi}$  is a  $p$ -adic unit, while  $|\varphi|_p < 1$ . The computation of  $\varphi$  and  $\bar{\varphi}$  is performed efficiently with the  $p$ -adic Newton's method, which is superconvergent [29, chapter 2]. From equations (17) we see that the initial condition for the Newton recursive sequence  $\varphi_k \rightarrow \varphi$  is  $\varphi_0 = 0$ , whereas  $\bar{\varphi}_0 = q$ .

Identifying  $\lambda$  with  $\varphi$  defines an embedding  $\mathcal{L}_2$  of  $\mathbb{Z}[\lambda]$  into the ring  $\mathbb{Z}_p$  of  $p$ -adic integers

$$\mathcal{L}_2 : \mathbb{Z}[\lambda] \rightarrow \mathbb{Z}_p \quad x + \lambda y \mapsto x + \varphi y.$$

Composing  $\mathcal{L}_1$  and  $\mathcal{L}_2$ , and scaling gives us the following

**Theorem 3.** *The dense embedding*

$$\mathcal{L} : \mathbb{Z}^2 \mapsto \mathbb{Z}_p \quad (x, y) \mapsto \frac{1}{p} \mathcal{L}_2(\mathcal{L}_1(x, y)) = x - \frac{\varphi}{p} y \quad (18)$$

has the property that the mapping  $\Phi^* = \mathcal{L} \circ \Phi \circ \mathcal{L}^{-1}$  can be extended continuously from  $\mathcal{L}(\mathbb{Z}^2)$  to the whole of  $\mathbb{Z}_p$ , giving

$$\chi_{t+1} = \Phi^*(\chi_t) = \sigma(\bar{\varphi} \chi_t) \quad (19)$$

where  $\bar{\varphi} = \mathcal{L}(n, p)$  and  $\sigma$  is the shift mapping.

The shift  $\sigma$  is defined like its archimedean counterpart; if  $\chi = c_0 + c_1 p + c_2 p^2 + \dots$ , then

$$\sigma(\chi) = c_1 + c_2 p + c_3 p^2 + \dots \quad (20)$$

The  $p$ -adic shift mapping has been studied in [30, 31, 32].

The above result represents the round-off problem on  $\mathbb{Z}^2$  as a sub-system of an expanding map over the  $p$ -adics, featuring a complete symbolic dynamics over  $p$  symbols, and a dense set of unstable periodic orbits. It preserves the standard probability measure on  $\mathbb{Z}_p$  (the additive Haar measure), obtained by assigning to each residue class modulo  $p^k$  the measure  $p^{-k}$ . This is just the natural measure on  $\mathbb{Z}_p$  as a Cantor set.

This system has a lot in common with the Bernoulli shift on  $p$ -symbols. For instance, the metric entropy is the same, namely  $\log(p)$ ; the periodic points also have a similar structure, as we shall see below.

## CODING FUNCTION AND PERIODIC ORBITS

We consider the function  $\mathcal{C}$  that maps the initial point  $\chi \in \mathbb{Z}_p$  of an orbit of  $\Phi^*$  into the corresponding symbolic code  $(c_0, c_1, \dots)$  —cf. equation (15). The latter is easily

defined, for instance, as the limit of the codes through the points  $(x^{(k)}, 0) \in \mathbb{Z}^2$ , for a rational sequence  $x^{(k)} \rightarrow \chi$ . If we represent the code as a  $p$ -adic integer

$$\mathcal{C}(\chi) = \sum_{k=0}^{\infty} c_k p^k,$$

then we have

**Theorem 4.** *The function  $\mathcal{C}$  defines an isometric bijection of  $\mathbb{Z}_p$ , which is nowhere differentiable.*

Of interest is the fact that a similar property holds for the coding function of the  $p$ -adic version of the so-called  $3x + 1$  problem [33, theorem 10.4].

This result establishes a one-to-one correspondence between periodic codes and periodic orbits, while the metric-preserving property of  $\mathcal{C}$  show that the periodic orbits are dense and uniformly distributed with respect to the Haar measure. Just like for the  $t$ -cycle of  $\Phi$ , those of  $\Phi^*$  are all unstable, with multiplier  $p^{-t}$ , where  $t$  is the period.

Next we characterize the periodic points arithmetically. We define

$$a_1 = 1; \quad b_1 = 0; \quad \begin{cases} a_{k+1} = qa_k + pb_k \\ b_{k+1} = -pa_k \end{cases} \quad k \geq 1, \quad (21)$$

and

$$U_{t,r} = p^r a_{t-r} + p^{t-r} a_r \quad r \geq 0, \quad t \geq 1. \quad (22)$$

**Theorem 5.** *The periodic point  $\chi$  corresponding to the  $t$ -periodic code  $(\overline{c_0, \dots, c_{t-1}})$  takes the form*

$$\chi = \frac{1}{B(t)} \left( x - \frac{\varphi}{p} y \right) \quad (23)$$

where  $x$  and  $y$  are integers given by

$$x = \sum_{r=0}^{t-1} c_r U_{t,r} \quad y = \sum_{r=0}^{t-1} c_r U_{t,r+1} \quad (24)$$

while

$$B(t) = a_t q + 2pb_t - 2p^t \quad (25)$$

is an integer coprime to  $p$ .

We verify directly that the periodic points  $\chi$  in equation (23) are  $p$ -adic integers. Firstly, we note that  $|\varphi|_p < 1$ , and hence  $|\varphi/p|_p \leq 1$ , while  $|B(t)|_p = 1$ . Using the ultrametric inequality (4), we then get  $|\chi|_p \leq 1$ . Comparison with (3) confirms that  $\mathbb{Z}_p$  is precisely the closed  $p$ -adic unit disc.

Comparing expressions (7) and (23) we see that the structure of the cycles of the maps  $\Phi^*$  and  $\Psi$  is very similar. The role of the exponential sequence  $p^t - 1$  at denominator is here played by the sequence  $B(t)$ , which grows exponentially at the same rate. The numerators of the periodic points store code information in a similar manner.

The domain of definition of the embedding map  $\mathcal{L}$ , defined in equation (18), can be extended from  $\mathbb{Z}^2$  to the set  $\mathbb{U}_p^2$ , where  $\mathbb{U}_p$  is the set of rationals with denominator coprime to  $p$ , that is,  $\mathbb{U}_p = \mathbb{Q} \cap \mathbb{Z}_p$ . The map  $\mathcal{L}$  remains invertible on the extended domain, and since  $B(t)$  is coprime to  $p$ , using  $\mathcal{L}^{-1}$ , all the  $p$ -adic periodic orbits of  $\Phi^*$  can be lifted to the plane.<sup>5</sup> Specifically, the  $t$ -cycles belong to the  $\mathbb{Z}$ -module  $B(t)^{-1}\mathbb{Z}^2$ . Those corresponding to orbits of the round-off mapping  $\Phi$  must lie in the sub-module  $\mathbb{Z}^2$ , which is the case when both  $x$  and  $y$  are divisible by  $B(t)$ . Thus, for any positive integer  $t$ , we consider the smallest integer  $m$  such that there exists a  $t$ -cycle in  $\frac{1}{m}\mathbb{Z}^2$ . We denote such  $m$  by  $M(t)$ , and —as we did before— we call  $\Lambda(t) = M(t)^{-1}\mathbb{Z}^2$  the *minimal module* of the map  $\Phi^*$  for the period  $t$ .

In place of (9) now we have the bounds

$$1 \leq M(t) \leq B(t).$$

As noted above, the sequence  $B(t)$  plays the role of the sequence  $p^t - 1$  for the shift map. Comparing the respective lower bounds is rather more interesting. The set  $T^*$  for the shift map —the set of integers  $t$  for which  $p$  is a primitive root modulo  $t + 1$ — is here represented by the set of periods  $t$  for which the minimal module of  $\Phi^*$  is equal to  $\mathbb{Z}^2$ . In other words,  $T^*$  are the periods the orbits of the round-off mapping!

Plainly, the function  $t \rightarrow \Lambda(t)$  is not injective —cf. proposition 1. The permitted periods  $T^*$  are characterized via the multiplicity function  $\kappa$ , which counts the number of distinct orbits on  $\mathbb{Z}^2$  having period  $t$ . Thus, letting  $\tau : \mathbb{Z}^2 \rightarrow \mathbb{N} \cup \infty$  be the (possibly infinite) period of the orbit through  $z$ , we define

$$\kappa : \mathbb{N} \rightarrow \mathbb{N} \quad t \mapsto \frac{\#\{z \in \mathbb{Z}^2 : \tau(z) = t\}}{t}. \quad (26)$$

Using diophantine approximations, it is not difficult to show that the function  $\kappa$  is well-defined —the numerator in (26) is finite — for a set of (irrational) rotation angles  $\theta$  having full Lebesgue measure [1]. The periodicity of the round-off map was briefly investigated in [6]; roughly speaking,  $T^*$ , which is the support of  $\kappa$ , consists of denominators of good rational approximants of  $\theta$ . The best approximants —the denominators of the convergents of  $\theta$ — were found to correspond to the local maxima of the multiplicity function. As for the map  $\Psi$ , the density of  $T^*$  in  $\mathbb{N}$  appears to be zero, but with a faster decay rate than (13). However, the deep structure of the function  $\kappa$  remains unexplored; this investigation seems very worthwhile, involving probabilistic aspects of diophantine approximations.

The symbol sequences generated by the round-off orbits are good pseudo-random sequences (a comparison with [32] is instructive). Some rigorous results will be found in [7], most notably a central limit theorem governing the departure of round-off orbits from exact orbits. However, as is often the case in this type of problems, the most interesting properties are difficult to analyze. Experimentally, the period of the sequences is found to grow —on average— proportionally to the height of the initial condition

---

<sup>5</sup> One could also extend the round-off mapping  $\Phi$  to  $\mathbb{U}_p^2$ , as the conjugate of  $\Phi^*$  under  $\mathcal{L}^{-1}$  —see [5].

(the ‘seed’ of the pseudo-random sequence), while displaying at the same time huge fluctuations. The latter are symptoms of difficulties in computing the period function  $\tau$ , which is a good candidate for a non-polynomial time problem. The symbol sequences corresponding to  $\alpha = 1/2$  were tested at Hewlett Packard [34]. They show an optimal degree of pseudo-randomness for short times, and some faint correlations at certain larger times, related to the local maxima of the multiplicity function  $\kappa$ .

Finally, we examine the question of uniform distribution. Let  $z \in \mathbb{Z}^2$ , and  $z_k = \Phi^k(z)$ . Using the code (15), we construct the symbol sequence  $(c_0, c_1, \dots)$ , where  $c_k = c(z_k)$ . Using this sequence in the representation (6), we define a real number  $x = x(z)$  in the unit interval. By analogy with (10), we then let

$$W(z, n) = \frac{1}{\tau} \sum_{k=0}^{\tau-1} e^{2\pi i n x_k} \quad x_k = x(z_k) \quad (27)$$

where  $\tau = \tau(z)$  is the period of the orbit through  $z$ . In accordance with conjecture 1, we assume that  $\tau$  is finite. It is clear that the value of the sum (27) depends only on the orbit  $\mathcal{O}$  of  $z$  and not on the choice of the point  $z$  within  $\mathcal{O}$ ; accordingly, we write  $W = W(\mathcal{O}, n)$ . Let now  $(\mathcal{O}_0, \mathcal{O}_1, \dots)$  be an infinite sequence of distinct  $\Phi$ -orbits. We say that this sequence is *uniformly distributed* if

$$\lim_{k \rightarrow \infty} W(\mathcal{O}_k, n) = 0 \quad \forall n \neq 0$$

which should be compared with (11). We conclude this paper with the following

**Conjecture 2.** *Any sequence of distinct  $\Phi$ -orbits is uniformly distributed.*

## ACKNOWLEDGMENTS

This work was partially supported by EPSRC grant No GR/S62802/01.

## REFERENCES

1. F. Vivaldi, *Exp. Math.* **3**, 303–315 (1994).
2. J. H. Lowenstein, S. Hatjispyros, and F. Vivaldi, *Chaos* **7**, 49–66 (1997).
3. J. H. Lowenstein, and F. Vivaldi, *Nonlinearity* **11**, 1321–1350 (1998).
4. J. H. Lowenstein, and F. Vivaldi, *Chaos* **10**, 747–755 (2000).
5. D. Bosio, and F. Vivaldi, *Nonlinearity* **13**, 309–322 (2000).
6. D. Bosio, *Round-off errors and p-adic numbers*, Ph.D. thesis, Queen Mary, University of London (2000).
7. F. Vivaldi, and I. Vladimirov, *Int. J. of Bifurcations and Chaos* **13**, 3373–3393 (2003).
8. K. L. Kouptsov, J. H. Lowenstein, and F. Vivaldi, *Nonlinearity* **15**, 1795–1482 (2002).
9. A. Katok, and B. Hasselblat, *Introduction to the modern theory of dynamical systems*, Cambridge University Press, Cambridge, 1997.
10. J. Ford, *Physics Today* **36**, 40–47 (1983).
11. B. Chirikov, and F. Vivaldi, *Physica D* **129**, 223–235 (1999).
12. D. K. Arrowsmith, and F. Vivaldi, *Physica D* **71**, 222–236 (1994).
13. J. Pettigrew, J. A. G. Roberts, and F. Vivaldi, *Chaos* **11**, 849–857 (2001).

14. G. H. Hardy, and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 1979.
15. F. Q. Gouvêa, *p-adic numbers: an introduction*, Springer-Verlag, Berlin, 1993.
16. L. Kuipers, and Niederreiter, *H. Uniform Distribution of Sequences*, Wiley, New York, 1974.
17. J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Math. Comp.* **70**, 1591–1605 (2001).
18. J. B. Friedlander, and I. E. Shparlinski, *Math. Comp.* **70**, 1575–1589 (2001).
19. M. RamMurty, *Math. Intelligencer* **10**, 59–67 (1988).
20. P. Ribenboim, *The book of prime number records*, Springer-Verlag, New York, 1988.
21. G. Tenenbaum, and M. M. France, *The prime numbers and their distribution*, AMS, Providence, Rhode Island, 2000.
22. H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, New York, 1996.
23. M. Bartuccelli, and F. Vivaldi, *Physica D* **39**, 194–204 (1989).
24. M. D. Esposti, and S. Isola, *Nonlinearity* **8**, 827–842 (1995).
25. N. P. Fogg, *Substitutions in Dynamics, Arithmetics and Combinatorics*, Springer-Verlag, Berlin, 2002.
26. S. Akiyama, H. Brunotte, A. Pethö, and J. M. Thuswaldner, Generalized radix representations and dynamical systems ii (2005), to appear in *Acta Arith.*
27. V. Akiyama, H. Brunotte, A. Pethö, and W. Steiner, Remarks on a conjecture on certain integer sequences (2005), preprint, Niigata University.
28. D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.
29. D. A. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973.
30. E. Thiran, D. Versteegen, and J. Weyers, *J. Stat. Phys.* **54**, 893–913 (1989).
31. D. K. Arrowsmith, and F. Vivaldi, *Phys. Lett. A* **176**, 292–294 (1993).
32. F. Woodcock, and N. P. Smart, *Exp. Math.* **7**, 334–342 (1998).
33. G. J. Wirsching, *The dynamical system generated by the  $3n + 1$  function*, Springer-Verlag, Berlin, 1998.
34. J. Castejon (2001), private communication.