Dynamics of a quasi-quadratic map

Assis Azevedo[a], Maria Carvalho[b] and António Machiavelo[b]

[a]*Department of Mathematics and Applications, University of Minho, Braga, Portugal*

[b]*Department of Mathematics, University of Porto, Porto, Portugal*

We consider the map $\chi : \mathbb{Q} \to \mathbb{Q}$ given by $\chi(x) = x\lceil x \rceil$, where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x, and study the problem of finding, for each rational, the smallest number of iterations by χ that sends it into an integer. Given two natural numbers M and n, we prove that the set of numerators of the irreducible fractions that have denominator M and whose orbits by χ reach an integer in exactly n iterations is a disjoint union of congruence classes modulo M^{n+1}. Moreover, we establish a finite procedure to determine them. We also describe an efficient algorithm to decide if an orbit of a rational number bigger than one fails to hit an integer until a prescribed number of iterations have elapsed, and deduce that the probability that such an orbit enters $\mathbb{Z}$ is equal to one.

Keywords: discrete dynamical system; ceiling function; density; covering system.

AMS Subject Classification: 11A07, 37P99.

1. Introduction

Let $\chi : \mathbb{Q} \to \mathbb{Q}$ be the map given by $\chi(x) = x\lceil x \rceil$, where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x, and consider the orbits $\left(\chi^n(x)\right)_{n\in\mathbb{N}_0}$ of any $x \in \mathbb{Q}$, where $\mathbb{N}_0$ stands for the set of non-negative integers. We note that $\mathbb{Z}$ is invariant by χ, the fixed points are the rational elements in $[0, 1]$, $\chi^{-1}(\{0\}) =]-1, 0]$, $\chi(-x) = \chi(x) - x$ if $x \in \mathbb{Q} \setminus \mathbb{Z}$, and that, if $x \leq -1$, then $\chi(x) \geq 1$.

For $\frac{p}{q} \in \mathbb{Q} \cap [1, +\infty[$, where p, q belong to $\mathbb{N}$ and $(p, q) = 1$, the iterate $\chi^j\left(\frac{p}{q}\right)$ is an irreducible quotient $\frac{p_j}{q_j}$, where q_{j+1} divides q_j. Therefore the sequence of denominators q_j is decreasing, although not strictly in general. For instance, the first iterates of $\frac{31}{10}$ are

$$\frac{62}{5}, \quad \frac{806}{5}, \quad \frac{130572}{5}, \quad 681977556.$$

The number of iterates needed for the orbit of $\frac{p}{q}$ to hit an integer may be arbitrarily large (see Remark 1). However, numerical evidence suggests that, for any such $\frac{p}{q}$, there is a $j \in \mathbb{N}$ verifying $q_j = 1$. This behaviour bears a resemblance to the dynamics of $G : \mathbb{Q} \cap [0, 1] \to \mathbb{Q} \cap [0, 1]$, $G(x) = 1/x - \lfloor 1/x \rfloor$, $G(0) = 0$, although in this case the orbit of each rational number in $[0, 1]$ is a sequence of irreducible fractions whose denominators decrease strictly before the orbit ends at 0, and so this happens in finite time.

For $x \in \mathbb{Q}$, define the *order of* x as

$$\operatorname{ord}(x) = \min\{k \in \mathbb{N}_0 : \chi^k(x) \in \mathbb{Z}\},$$

if this set is nonempty, and $\operatorname{ord}(x) = \infty$ otherwise. The integers are the elements

of order 0; the rational numbers in $]0,1[$ have infinite order. It is easy to evaluate the order of any irreducible fraction $\frac{a}{2}$ in $\mathbb{Q} \cap [1,+\infty[$: given an odd $a \in \mathbb{N}$, say $a = 2^k b + 1$ for a positive integer k and an odd b, using induction on $k \in \mathbb{N}$ and the equality

$$\chi\left(\frac{a}{2}\right) = \frac{2^{k-1} b \left(2^k b + 3\right) + 1}{2},$$

one deduces that $\operatorname{ord}\left(\frac{a}{2}\right) = k$. In particular, for each $k \in \mathbb{N}$, the smallest positive irreducible fraction with denominator 2 whose order is k is $\frac{2^k+1}{2}$. We note that not only this smallest value increases with k, but it does so exponentially. By contrast, the following table, which displays the smallest integer a such that $1 \leq \operatorname{ord}(\frac{a}{3}) \leq 50$, shows that, within the rational numbers with denominator 3, that exponential growth with k no longer holds.

order	smallest integer a	order	smallest integer a	order	smallest integer a
1	7	18	2 215	35	6 335 903
2	4	19	6 151	36	1 180 939
3	13	20	8 653	37	1 751 431
4	20	21	280	38	10 970 993
5	10	22	28	39	17 545 207
6	5	23	1 783	40	66 269 497
7	29	24	81 653	41	27 952 480
8	76	25	19 310	42	60 284 614
9	50	26	114 698	43	203 071 951
10	452	27	18 716	44	191 482 466
11	244	28	196 832	45	144 756 173
12	830	29	15 214	46	45 781 445
13	49	30	7 148	47	1 343 664 136
14	91	31	273 223	48	223 084 774
15	319	32	3 399 188	49	1 494 753 473
16	2 639	33	398 314	50	20 110 862
17	5 753	34	6 553 568	51	2 736 459 742

Figure 1. Smallest positive integer a such that $\frac{a}{3}$ has order between 1 and 51.

We have also verified that, for $a \leq 4\,000\,000\,000$, the order of $\frac{a}{3}$ is equal or less than 56, and is different from 52, 54 and 55. Clearly, this computation was not achieved directly from the definition of order, because the iterates grow very rapidly: for example, $\frac{28}{3}$ has order 22 and $\chi^{22}(\frac{28}{3})$ is an integer with 4 134 726 digits. Our numerical experiments were possible due to two redeeming features: the dynamical nature of the problem, which allowed us to reduce the difficulty in each iteration; and, moreover, the location of the numerators of rational numbers with given denominator and a fixed order among the elements of specific congruence classes modulo a certain power of the denominator. This enabled us to deal only with numerators that are bounded by that power.

In what follows, and after showing that the elements of order n, with a fixed de-

nominator, have numerators that belong to some union of congruence classes, we give in Theorem 2.3 a recursive formula for the number of those classes. We use it to attest that the natural, or asymptotic, density (see [3], p. 270) of the elements of $\mathbb{Q}\cap]1,+\infty[$ that have infinite order is zero (see Theorem 3.1). Next we present an efficient algorithm to determine if a rational number has an order below a given bound. Finally we comment on some alternative approaches and affinities that this problem seems to have with the Collatz conjecture and the Erdös-Straus conjecture on unit fractions.

2. Numbers of order n

We are not aware of any efficient algorithm to evaluate the order of a rational number. We also do not know if there are numbers, besides the ones in the interval $]0,1[$, with infinite order. But we do have two algorithms to decide if a rational $\frac{a}{M}$ has order n, for a fixed n. We will see that, in both cases, one only needs to consider $a < M^{n+1}$.

The first algorithm provides a way to find all the elements of order n if one knows all the elements of order $n-1$, and it is a sub-product of the results in this section. It relies on the resolution of a (finite) number of quadratic congruences that increases exponentially with n. Through this procedure one gets substantial knowledge on the structure of the elements of order n, which is sufficient to prove that, with probability one (details in the next section), an element has finite order. The second algorithm checks if a rational number has an order less then a fixed bound and will be presented in Section 4.

The underlying basic idea is simply to use the obvious fact that $\operatorname{ord}(\chi(x)) = \operatorname{ord}(x) - 1$, for each $x \in \mathbb{Q}\setminus\mathbb{Z}$, to find information about the elements of order n from the ones of order $n-1$, somehow reversing the dynamics of the map χ. Surely, given $y \in \mathbb{Q}$, in general, there is no rational x such that $\chi(x) = y$ (consider $y = \frac{5}{3}$, for example). But, in the proof of Theorem 2.3, we show that, in some sense, the process is reversible.

We start by characterizing the elements that have order equal to 1.

LEMMA 2.1. *Let $x = \frac{a}{M}$, where $a \in \mathbb{Z}$, $M \in \mathbb{N}$, with $M > 1$, and $(a, M) = 1$. Then $ord(x) = 1$ if and only if there exists $r \in \{1, 2, \ldots, M-1\}$ such that $(r, M) = 1$ and $a \equiv -r \pmod{M^2}$.*

Proof. We note first that $x \notin \mathbb{Z}$, and also that x has order 1 if and only if $\chi(x) \in \mathbb{Z}$, which is equivalent, since $(a, M) = 1$, to the condition that M divides $\lceil \frac{a}{M} \rceil$. Consider $k \in \mathbb{Z}$ and $0 \le r < M^2$ such that $a = kM^2 - r$. Observe that, as $(a, M) = 1$, we have $(r, M) = 1$ and $r \neq 0$. Then $\lceil \frac{a}{M} \rceil = kM + \lceil \frac{-r}{M} \rceil$ and so

$$\begin{aligned} M \text{ divides } \lceil \tfrac{a}{M} \rceil &\Leftrightarrow M \text{ divides } \lceil -\tfrac{r}{M} \rceil \\ &\Leftrightarrow \lceil -\tfrac{r}{M} \rceil = 0, \quad \text{as } -M < -\tfrac{r}{M} < 0 \\ &\Leftrightarrow r \in \{1, 2, \ldots, M-1\}. \end{aligned}$$

□

This lemma provides the basis for the induction in the proof of the following result.

PROPOSITION 2.2. *If $n \in \mathbb{N}$, then, for all $M \in \mathbb{N}$, the set*

$$\mathcal{A}_{n,M} = \left\{ a \in \mathbb{Z} : \ (a, M) = 1, \ ord\left(\frac{a}{M}\right) = n \right\} \tag{1}$$

is a disjoint union of congruence classes modulo M^{n+1}.

Proof. If $n = 1$, the result is given by the previous Lemma. When $n > 1$, we only need to guarantee that, if $a \in \mathbb{Z}$, $(a, M) = 1$ and $\operatorname{ord}\left(\frac{a}{M}\right) = n$, then $\operatorname{ord}\left(\frac{a}{M} + tM^n\right) = n$, for all $t \in \mathbb{Z}$. Now, if $\chi\left(\frac{a}{M}\right) = \frac{a'}{M'}$, where $a' \in \mathbb{Z}$ is such that $(a', M') = 1$, and M' is a divisor of M, then

$$\begin{aligned}
\chi\left(\frac{a}{M} + tM^n\right) &= \left(\frac{a}{M} + tM^n\right) \left\lceil \frac{a}{M} + tM^n \right\rceil \\
&= \left(\frac{a}{M} + tM^n\right) \left(\left\lceil \frac{a}{M} \right\rceil + tM^n \right) \\
&= \chi\left(\frac{a}{M}\right) + mM^{n-1}, \text{ for some } m \in \mathbb{Z} \\
&= \frac{a'}{M'} + mM^{n-1}.
\end{aligned}$$

As $\operatorname{ord}\left(\frac{a'}{M'}\right) = n - 1$, the result follows by induction on n. □

From this proposition we conclude that, when looking for rational numbers with order n in $\frac{1}{M}\mathcal{A}_{n,M}$, we need only to deal with irreducible fractions $\frac{a}{M}$ such that

$$a \in \{0, 1, \ldots, M^{n+1} - 1\}.$$

It is easy to exhibit examples of elements with order n. For instance, it is straightforward to conclude by induction on n that, if p is an odd prime number, then the following numbers have order n:

$$\frac{(p-1)p^n + 1}{p} \ (\forall_{n \geq 0}) \ ; \ \frac{(-1)^n p^n + p - 1}{p} \ (\forall_{n \geq 0}) \ ; \ \frac{-(n+1)p^n + p^{n-1} + 1}{p} \ (\forall_{n \geq 2}) \, .$$

Denote by $A(n, M)$ the number of congruence classes modulo M^{n+1} in $\mathcal{A}_{n,M}$ and by φ the Euler function. We have already seen that

$$\begin{cases} A(0,1) = 1, \\ A(n,1) = 0 \ \forall n \in \mathbb{N}, \end{cases} \text{ and, for } M > 1, \begin{cases} A(0, M) = 0 \\ A(1, M) = \varphi(M) \text{ (by Lemma 2.1).} \end{cases} \tag{2}$$

It turns out that the sequence $(A(n, M))_{n \in \mathbb{N}_0}$ satisfies a recurrence relation, for all $M > 1$, as shown in the following result.

THEOREM 2.3. *For $M, n \in \mathbb{N}$, with $M > 1$ or $n > 1$,*

$$A(n, M) = \varphi(M) \sum_{d \mid M} A(n-1, d) \left(\frac{M}{d}\right)^{n-1}. \tag{3}$$

Proof. For $n = 1$, the result is a consequence of (2). When $n > 1$, we can ignore the divisor 1 in the sum in (3), since $A(n-1, 1) = 0$. For each divisor $d > 1$ of M, let

$$Y_d = \mathcal{A}_{n-1,d} \cap [1, M^{n-1}d[.$$

Also set

$$W = \{c \in \mathbb{N} : (c, M) = 1\} \cap [1, M[\,,$$

$$X = \mathcal{A}_{n,M} \cap [1, M^{n+1}[\,.$$

Observe that $\#W = \varphi(M)$ and, as $n > 1$, that $Y_1 = \emptyset$. Besides, by Proposition 2.2, the set Y_d has precisely $A(n-1,d)\left(\frac{M}{d}\right)^{n-1}$ elements.

Consider now the map

$$\Phi = (\Phi_1, \Phi_2) : X \longrightarrow \left(\bigcup_{d|M} Y_d\right) \times W$$

defined as follows. Given $a \in X$, if $k = \lceil \frac{a}{M} \rceil$, $d = \frac{M}{(k,M)}$ and $s = \frac{k}{(k,M)}$, take

$$\Phi_1(a) = \frac{r}{d}\,, \text{ where } r \text{ is the remainder of the division of } as \text{ by } M^{n-1}d,$$

$$\Phi_2(a) = \text{ the remainder of the division of } a \text{ by } M.$$

Notice that $\chi\left(\frac{a}{M}\right) = \frac{as}{d}$, $(as, d) = 1$ and, by Proposition 2.2, $\Phi_1(a) \in Y_d$.

In order to prove that Φ is bijective, which proves (3), consider a divisor d of M and $\left(\frac{r}{d}, c\right) \in Y_d \times W$. If $a \in X$ then, by definition,

$$\Phi(a) = \left(\frac{r}{d}, c\right) \Longleftrightarrow \begin{cases} \frac{M}{(\lceil \frac{a}{M} \rceil, M)} = d \\ \frac{a\lceil \frac{a}{M} \rceil}{(\lceil \frac{a}{M} \rceil, M)} \equiv r \pmod{M^{n-1}d} \\ a = \left(\lceil \frac{a}{M} \rceil - 1\right) M + c. \end{cases}$$

In particular, $\lceil \frac{a}{M} \rceil$ must be a multiple of $\frac{M}{d}$, so we have $\Phi(a) = \left(\frac{r}{d}, c\right)$ if and only if there exists $y \in \mathbb{N}$ such that $\lceil \frac{a}{M} \rceil = y\frac{M}{d}$ and

$$\begin{cases} (y, d) = 1 \\ \frac{M^2}{d} y^2 + (c - M)y \equiv r \pmod{M^{n-1}d} \\ a = \left(y\frac{M}{d} - 1\right) M + c. \end{cases}$$

Since $(r, d) = 1$, any y satisfying $\frac{M^2}{d} y^2 + (c - M)y \equiv r \pmod{M^{n-1}d}$ has to be coprime to d. So we only need to prove that this congruence has only one solution modulo $M^{n-1}d$, or equivalently, that each congruence of the form

$$\frac{M^2}{d}\, y^2 + (c - M)\, y \equiv r \pmod{p^t},$$

has a unique solution (modulo p^t), where p is a prime and t is the larger positive integer such that p^t divides $M^{n-1}d$. This is due to the fact that this congruence reduces modulo p to $cy \equiv r \pmod{p}$, and $c \not\equiv 0 \pmod{p}$ since $c \in W$; moreover, the formal derivative modulo p of the quadratic polynomial on y is $(c - M)$, which is not a multiple of p (details in [5]). □

As a consequence of the surjectivity of the function Φ defined in the proof just presented, we have:

Remark 1. If $n \in \mathbb{N}$ and $(q_j)_{1 \le j \le n}$ is a finite sequence of positive integers where q_{j+1} divides q_j for any j, then there exists $x \in \mathbb{Q}$ such that $\chi^j(x) = \frac{p_j}{q_j}$ and $(p_j, q_j) = 1$, for all $1 \le j \le n$.

In the particular case of M being equal to a power of a prime, we get a closed formula for $A(n, M)$.

COROLLARY 2.4. *If p is a prime and $k, n \in \mathbb{N}$, then $A(n, p^k) = \binom{n+k-2}{n-1} \left(\varphi(p^k)\right)^n$.*

Proof. Firstly recall that the map φ verifies

$$\varphi(x^{k+1}) = x^k \varphi(x), \quad \text{for } x, k \in \mathbb{N}. \tag{4}$$

As mentioned before, $A(1, M) = \varphi(M)$, and therefore the formula is valid for $n = 1$ and all $k \in \mathbb{N}$. Let us proceed by induction on n. If $k \in \mathbb{N}$ and $n \geq 1$, then, by Theorem 2.3, we have

$$\begin{aligned} A(n+1, p^k) &= \varphi(p^k) \sum_{d|p^k} \left(\frac{p^k}{d}\right)^n A(n, d) \\ &= \varphi(p^k) \sum_{i=1}^{k} p^{(k-i)n} \binom{n+i-2}{n-1} \varphi(p^i)^n, \quad \text{by induction} \\ &= \varphi(p^k)^{n+1} \sum_{i=1}^{k} \binom{n+i-2}{n-1}, \quad \text{by (4)} \\ &= \binom{n+k-1}{n} \varphi(p^k)^{n+1}. \end{aligned}$$

□

Using the recurrence formula given by Theorem 2.3, we have easily obtained the values of $A(n, M)$, with $1 \leq n \leq 5$ and $M \leq 20$, as displayed in Figure 2.

n \ M	2	3	4	5	6	7	8	9	10	11	12
1	1	2	2	4	2	6	4	6	4	10	4
2	1	4	8	16	18	36	48	72	68	100	112
3	1	8	24	64	86	216	384	648	628	1000	1424
4	1	16	64	256	354	1296	2560	5184	5060	10000	13952
5	1	32	160	1024	1382	7776	15360	38880	39124	100000	120768

n \ M	13	14	15	16	17	18	19	20
1	12	6	8	8	16	6	18	8
2	144	150	240	256	256	270	324	416
3	1728	2058	3872	5120	4096	5670	5832	9952
4	20736	24774	52800	81920	65536	93798	104976	184576
5	248832	287466	668288	1146880	1048576	1396278	1889568	3048576

Figure 2. The value of $A(n, M)$ for $1 \leq n \leq 5$ and $M \leq 20$.

The proof of the previous theorem provides an algorithm to explicitly compute all the congruence classes of all elements $a \in \mathbb{Z}$ such that $\frac{a}{M}$ has a certain order. This might be used to decide whether a rational number has a given order n, but it has the drawback that it would require solving a number of congruences that grows exponentially with n.

Example 2.5 From Corollary 2.4, we know that, if p is prime and $n \in \mathbb{N}$, then $A(n, p) = (p-1)^n$. This means that the set of irreducible fractions $\frac{a}{p}$ with order n is a disjoint union of $(p-1)^n$ arithmetic progressions of ratio p^{n+1}. For instance, given

$a \in \mathbb{Z}$,

$$\begin{aligned}
\operatorname{ord}\left(\frac{a}{2}\right) = n &\iff a \equiv 2^n + 1 \pmod{2^{n+1}} \\
\operatorname{ord}\left(\frac{a}{3}\right) = 1 &\iff a \equiv 7, 8 \pmod{3^2} \\
\operatorname{ord}\left(\frac{a}{3}\right) = 2 &\iff a \equiv 4, 11, 14, 19 \pmod{3^3} \\
\operatorname{ord}\left(\frac{a}{3}\right) = 3 &\iff a \equiv 13, 22, 55, 56, 59, 64, 74, 77 \pmod{3^4} \\
\operatorname{ord}\left(\frac{a}{3}\right) = 4 &\iff x \equiv 20, 23, 40, 83, 86, 109, 118, 128, 131, 157, 163, 172, \\
&\qquad 191, 194, 211, 229 \pmod{3^5} \\
\operatorname{ord}\left(\frac{a}{5}\right) = 1 &\iff a \equiv 21, 22, 23, 24 \pmod{5^2} \\
\operatorname{ord}\left(\frac{a}{5}\right) = 2 &\iff a \equiv 18, 29, 32, 37, 44, 52, 56, 58, 66, 78, 86, 92, 101, 109, \\
&\qquad 113, 114 \pmod{5^3}
\end{aligned}$$

3. Numbers of infinite order

We could not find any number outside $]0, 1[$ with infinite order. Nevertheless, we were able to show that, with probability one, a number has finite order. The proof of this statement is the aim of this section.

Given $M \in \mathbb{N}$, $a \in \mathbb{Z}$ with $(a, M) = 1$ and $x = \frac{a}{M}$,

a) for any $n \in \mathbb{N}_0$, the probability that x has order n as $\frac{A(n,M)}{\varphi(M^{n+1})}$;

b) the probability that x has finite order as $\displaystyle\sum_{n=0}^{\infty} \frac{A(n,M)}{\varphi(M^{n+1})}$,

where we use here the term probability in the usual sense of natural density (see [3], p. 270). We now prove that this last probability is equal to one.

THEOREM 3.1. *If $M \in \mathbb{N}$, then the probability that $\frac{a}{M} \in]1, +\infty[$, with $(a, M) = 1$, has finite order is equal to* 1.

Proof. Given $M \in \mathbb{N}$, it is clear that the partial sums of the series

$$\mathcal{P}(M) = \sum_{n=0}^{\infty} \frac{A(n, M)}{\varphi(M^{n+1})}$$

are bounded by 1, so this series converges. We need to show that its sum is 1. We will prove it by induction on M. Obviously $\mathcal{P}(1) = 1$, as $A(0, 1) = 1$ and $A(n, 1) = 0$

if $n \geq 1$. Consider $M > 1$ and assume that $\mathcal{P}(M') = 1$ for all $M' < M$. Then

$$\begin{aligned}
\mathcal{P}(M) &= \sum_{n=1}^{\infty} \frac{A(n,M)}{\varphi(M^{n+1})}, \quad \text{as } A(0,M) = 0 \\
&= \frac{1}{M} \sum_{n=1}^{\infty} \sum_{d|M} \varphi(d) \, \frac{A(n-1,d)}{\varphi(d^n)}, \quad \text{by (3) and (4)} \\
&= \frac{1}{M} \sum_{d|M} \varphi(d) \sum_{n=1}^{\infty} \frac{A(n-1,d)}{\varphi(d^n)} \\
&= \frac{1}{M} \sum_{d|M} \varphi(d) \sum_{n=0}^{\infty} \frac{A(n,d)}{\varphi(d^{n+1})}.
\end{aligned}$$

By hypothesis, $\displaystyle\sum_{n=0}^{\infty} \frac{A(n,d)}{\varphi(d^{n+1})} = \mathcal{P}(d) = 1$ if $d < M$; therefore, using Gauss' Lemma,

$$\sum_{d|x} \varphi(d) = x, \quad \text{for } x \in \mathbb{N},$$

we deduce that

$$\begin{aligned}
\mathcal{P}(M) &= \frac{1}{M} \left(\sum_{d|M} \varphi(d) - \varphi(M) + \varphi(M)\mathcal{P}(M) \right) \\
&= \frac{1}{M} \left(M - \varphi(M) + \varphi(M)\mathcal{P}(M) \right) \\
&= 1 - \frac{\varphi(M)}{M} + \frac{\varphi(M)}{M} \mathcal{P}(M)
\end{aligned}$$

and so, as $\varphi(M) < M$, we have $\mathcal{P}(M) = 1$. □

Remark 2. From Proposition 2.2 and the previous theorem it is easy to infer that, for any denominator M and $n \in \mathbb{N}$,

(1) $\displaystyle\lim_{k \to +\infty} \frac{\#\{1 \leq a \leq k : a \in \mathcal{A}_{n,M}\}}{k} = \frac{A(n,M)}{M^{n+1}}.$

(2) $\displaystyle\lim_{k \to +\infty} \frac{\#\{1 \leq a \leq k : \ \exists n \in \mathbb{N}_0 : \ a \in \mathcal{A}_{n,M}\}}{k} = \frac{\varphi(M)}{M}.$

(3) The density of the numerators of the irreducible fractions $\frac{a}{M}$ bigger than one whose orbits do not reach $\mathbb{Z}$ is zero.

Remark 3. When $M = p^k$, with p prime and $k \in \mathbb{N}$, the probability that x has order

greater than N is

$$\sum_{n=N+1}^{\infty} \frac{A(n,p^k)}{\varphi((p^k)^{n+1})} = \left[\sum_{t=0}^{k-1} \binom{N-1+t}{t} p^{-t}\right] \left(\frac{p-1}{p}\right)^N. \tag{5}$$

This can be directly checked for $N = 1$, using Theorem 3.1, and then by induction on N, together with Corollary 2.4. Since the expression in brackets is a polynomial in N of degree $k-1$ (it is in fact the Taylor polynomial of degree $k-1$ of $(1-x)^{-N}$ evaluated at p^{-1}), one concludes that the probability just mentioned decreases exponentially to 0 as N goes to infinity. Moreover, one can show that this exponential decay also holds for arbitrary M. In fact, setting

$$P(n,M) = \frac{A(n,M)}{\varphi(M^{n+1})} \quad \text{and} \quad P_{\leq n}(M) = \sum_{k=0}^{n} P(k,M),$$

one easily deduces from the relation (3) that, for all $M, n \in \mathbb{N}$ with M, n not both equal to 1,

$$P_{\leq n}(M) = \frac{1}{M} \sum_{d|M} P_{\leq n-1}(d)\varphi(d).$$

Besides, this relation still holds when $M = n = 1$, as one can readily verify. It then follows, by induction and the fact that $P_{\leq 0}$ is a multiplicative function, that $P_{\leq n}$ is a multiplicative function for all $n \in \mathbb{N}_0$. This multiplicativity can then be used to conclude from (5) that the analogous probability decreases exponentially to 0, as N goes to infinity, for arbitrary M, as claimed.

From Theorem 3.1 one can now deduce a minor but curious fact about possible elements of infinite order.

COROLLARY 3.2. *There is no infinite arithmetic progression in $\mathbb{Q}$ whose elements have infinite order.*

Proof. Any arithmetic progression in $\mathbb{Q}$ contains an arithmetic progression of the form $\left(\frac{s+nrM}{M}\right)_{n\in\mathbb{N}}$, with $M \in \mathbb{N}$, $s, r \in \mathbb{Z}$ and $(s, M) = 1$. We note that one has $(s + nrM, M) = 1$, and that a number of the form $\frac{a}{M} > 1$, with $(a, M) = 1$, has probability $\frac{1}{r\varphi(M)}$ of belonging to this arithmetic progression. Using Theorem 3.1, we conclude that the arithmetic progression must include elements of finite order. □

For a while we were tempted to believe that if, for a fixed $M \in \mathbb{N}$ and for all $n \in \mathbb{N}_0$, one has c_n disjoint congruence classes modulo M^{n+1} such that $\sum_{n\geq 0} \frac{c_n}{M^{n+1}} = 1$, then the union of all those classes is all of $\mathbb{Z}$, with the possible exception of a finite set. Yet, this is not true, as can be confirmed by the next example, in which we chose $M = 3$ to simplify matters, but where we could just as well have taken an arbitrary M.

Example 3.3 Our aim is to show that one can inductively construct, for each $n \in \mathbb{N}_0$ and $k \in \{1, 2, 3, \ldots, 2^n\}$, an element $x_{n,k}$ in $\{1, 2, \ldots, 3^{n+1}\}$ in such a way that, if $(n, k) \neq (m, s)$, then the classes modulo $3^{\min\{m,n\}+1}$ of $x_{n,k}$ and $x_{m,s}$ are disjoint. Moreover, one wishes to select those elements so that the union of all these congruence classes does not contain any number of, say, the set $Y = \{1 + 3^n : n \in \mathbb{N}_0\}$.

We start with $x_{0,1} = 3$. For a given $n \geq 1$, suppose that we have already defined $x_{m,k} \in \{1, 2, \ldots, 3^{m+1}\}$, for all $m < n$, satisfying the above mentioned conditions. In the set $\{1, 2 \ldots, 3^{n+1}\}$, there are $n+1$ elements of Y and, for each $0 \leq i \leq n-1$, we have 3^{n-i} elements in the class of $x_{i,j}$ modulo 3^{i+1}. We thus have a total of $(n+1)+3^n+2\times 3^{n-1}+2^2\times 3^{n-2}+\cdots+2^{n-1}\times 3$, that is $3^{n+1}-3\times 2^n+(n+1)$ elements already "used". Then $x_{n,k}$, for $1 \leq k \leq 2^n$, can be selected among the remaining $3^{n+1} - \left(3^{n+1} - 3 \times 2^n + (n+1)\right)$ elements of $\{1, 2 \ldots, 3^{n+1}\}$. This is possible since $3^{n+1} - \left(3^{n+1} - 3 \times 2^n + (n+1)\right) = 3 \times 2^n - (n+1) \geq 2^n$.

We therefore obtain 2^n classes modulo 3^{n+1}, for all $n \in \mathbb{N}_0$, which are all disjoint and whose complement contains the infinite set Y.

This example shows that if indeed it is true that all rational numbers bigger than 1 have finite order, as the numerical computations suggest, then in order to prove it one has to better understand the relationships among the congruence classes that frame the sets $\mathcal{A}_{n,M}$.

4. An efficient algorithm

In this section we describe a simple algorithm that verifies if a rational number has an order less than a fixed bound. It was precisely this algorithm that allowed us to obtain the entries of the previous tables. It runs very quickly, as long as the computer is able to store the appropriate numbers.

The strategy behind this procedure is the following. Take $\frac{a}{M}$ and consider the sequence $(a_n)_{n\in\mathbb{N}_0}$ defined by

$$a_0 = a$$
$$a_{n+1} = M\,\chi\left(\frac{a_n}{M}\right).$$

If we know that $\frac{a}{M}$ has order less or equal to N, then, for $1 \leq s < N$, the order of $\frac{a_s}{M}$ is less or equal to $N - s$. Hence, using Proposition 2.2, we can replace a_s by the remainder of the division of a_s by M^{N+1-s}. The order of $\frac{a}{M}$ will then be the first s such that a_s is a multiple of M. We summarize this as follows:

Algorithm: Given $M \in \mathbb{N}$, $a \in \mathbb{Z}$ and $N \in \mathbb{N}$, consider $\frac{a}{M}$ and define the sequence $(r_n)_{n\in\mathbb{N}_0}$ as

$$r_0 = \text{ the remainder of the division of } a \text{ by } M^{N+1}$$
$$r_{n+1} = \text{ the remainder of the division of } M\,\chi\left(\tfrac{a_n}{M}\right) \text{ by } M^{N+1-n}.$$

Then

$$\operatorname{ord}\left(\frac{a}{M}\right) = \begin{cases} k, & \text{if } \exists k \leq N:\ M \mid r_k \text{ and } M \nmid r_s, \text{ for all } s < k, \\ > N, \text{ otherwise.} \end{cases}$$

We highlight the fact that this algorithm only needs to deal with numbers of length less or equal to M^{N+1}, and that each step reduces the bounds involved.

5. Other approaches

An alternative approach to study the dynamics of the map χ would be to use the finite expansions of the successive numerators in the bases given by the respective

denominators. One of the problems with this procedure is that χ involves a multiplication in which carries intervene. In the particular case where the initial point is a fraction with denominator equal to a prime number p, the dynamics of χ without the carries would be one of an infinite dimensional linear cocycle with base space equal to the set of almost zero sequences on p symbols and with fibers over the field $\mathbb{F}_p$. This sounds already intricate, but the carries are a source of additional difficulties, causing χ to resemble a generalized shift with sensitive dependence on initial conditions [2]. This seems to hint, once more, that the question of determining whether or not there are rational numbers bigger than 1 of infinite order is a knotty problem.

For each prime p there is a map related to χ defined on the field of p-adic numbers as follows. Given

$$x = \sum_{j \geq k} a_j p^j \in \mathbb{Q}_p,$$

where $k \in \mathbb{Z}$ and $a_j \in \{0, 1, ..., p-1\}$ for all j, set

$$\lceil x \rceil_p = 1 + \sum_{j \geq 0} a_j p^j$$

and let $\chi_p : \mathbb{Q}_p \to \mathbb{Q}_p$ be the map given by $\chi_p(x) = x\lceil x \rceil_p$. This function coincides with the quasi-quadratic map when restricted to the rational numbers that are not integers and whose denominator is a power of p. Moreover, χ_p is continuous and, to find how it behaves on the fractions $\frac{a}{p}$, we have just to study χ_p on the compact set $\{x \in \mathbb{Q}_p : |x|_p \leq p\}$, where $|.|_p$ is the p-adic absolute value. One may now address the question if, for any p-adic number x, there exists $n \in \mathbb{N}_0$ such that $\chi_p^n(x)$ is a p-adic integer. It turns out that there are p-adic elements of infinite order other than the rational numbers in $]0, 1[$. This can be seen as follows.

By an argument similar to the one used to prove Theorem 2.3, we can verify that, given $k, n \in \mathbb{N}$, the set

$$\Lambda_{k,n} = \left\{ a \in \mathbb{Z}_p : \ \chi_p^n\left(\frac{a}{p^k}\right) \notin \frac{1}{p^{k-1}}\mathbb{Z}_p \right\}$$

is nonempty and a finite union of congruence classes in $\mathbb{Z}_p$ modulo $p^{(n+1)k}$. Therefore, it is compact. Moreover, it is clear that $\Lambda_{k,n+1} \subset \Lambda_{k,n}$. Besides, one can show that the disjoint congruence classes that constitute $\Lambda_{k,n+1}$ are equally distributed inside the ones that form $\Lambda_{k,n}$. Therefore, for any fixed k, the set $\bigcap_{n \in \mathbb{N}} \Lambda_{k,n}$ is nonempty. Since it is the intersection of a nested sequence of compact nonempty sets, each one formed by an increasing number of balls with decreasing radius, that are scattered through the balls of the previous set, we see that this intersection is a perfect subset (with zero Haar measure) of the locally compact group $\mathbb{Q}_p$. So, it is uncountable, which ensures that there are elements of infinite order in $\mathbb{Q}_p$ besides the ones in $\mathbb{Q} \cap]0, 1[$.

For instance, when $p = 3$, then

$$\chi_p(x) = \begin{cases} x(x+1) & \text{if } x \equiv 0 \pmod{\mathbb{Z}_3} \\ x\left(x + \frac{2}{3}\right) & \text{if } x \equiv \frac{1}{3} \pmod{\mathbb{Z}_3} \\ x\left(x + \frac{1}{3}\right) & \text{if } x \equiv \frac{2}{3} \pmod{\mathbb{Z}_3} \end{cases}$$

The restriction of this function to $\{x \in \mathbb{Q}_3 : |x|_3 \leq 3\}$ is locally scaling on the balls $B_1 = \frac{1}{3} + \mathbb{Z}_3$ and $B_2 = \frac{2}{3} + \mathbb{Z}_3$, with scaling rate equal to 3. The dynamics in $\mathbb{Z}_3$ has been described in [1]. The intersection of $\{x \in \mathbb{Q}_3 : |x|_3 \leq 3\}$ with the Cantor set we have just mentioned, whose elements are the 3-adic numbers whose orbits by χ_3 never reach $\mathbb{Z}_3$, is precisely $\Sigma = \bigcap_{n=0}^{+\infty} \chi_3^{-n}(B_1 \cup B_2)$. Here the dynamics of χ_3 is conjugate to a full shift on an alphabet with four symbols. The orbits of all the points of $B_1 \cup B_2 \setminus \Sigma$ eventually fall in $\mathbb{Z}_3$, but we do not know if it contains all the rational real numbers bigger than one. We guess that the wild nature of the orders we found among the fractions $\frac{a}{3}$ (see Fig. 1) is related to the complicated dynamical behaviour of the map χ_3, but we were not able to find an explicit formula of the stopping time in $B_1 \cup B_2 \setminus \Sigma$.

6. Final comments and remarks

Given an integer M, suppose one randomly chooses an integer a_1, sets $M_1 = M/(M, a_1)$, and then repeats the process by randomly choosing a_2, letting $M_2 = M_1/(M_1, a_2)$, and so on. Note this process somehow emulates what happens to the successive denominators of $\chi(\frac{a}{M})$. Fixing M and n, consider the question of determining the probability that $M_n = 1$, which we denote by $\mathcal{P}(n, M)$. Clearly: $\mathcal{P}(1, M) = 1/M$; $\mathcal{P}(0, M) = 1$ if $M = 1$ and $\mathcal{P}(0, M) = 0$ otherwise; and, if p is a prime number, then $\mathcal{P}(n, p) = (1 - 1/p)^{n-1}/p$. It is easy to show that the numbers $P(n, M)$ obey the following recurrence relation

$$\mathcal{P}(n, M) = \sum_{d|M} \frac{\varphi(d)}{M} \mathcal{P}(n-1, d),$$

that is also satisfied by the numbers $A(n, M)/\varphi(M^{n+1})$, as induction on M, using Theorem 2.3, proves. Thus, the probability that a rational number $\frac{a}{M} > 1$, with $(a, M) = 1$, has order n under χ is exactly the probability that the random process just described ends up after n steps after starting with M. This reveals that the map χ behaves, at least in this respect, just like a random procedure.

There are also some curious analogies between our query, if χ has no elements of infinite order, and both the Collatz problem and the Erdös-Straus conjecture. The similarities may be only superficial, but are nevertheless of some interest. In the Collatz problem, Riho Terras has shown that the set of elements that have a finite stopping time n, a notion analogous to our concept of order, is a disjoint union of congruence classes (see Theorem 1.2 in [4]). The issue is then whether these cover all integers. This is an open question, but Terras has also proved that the density of the integers that do not have finite stopping time is zero. Both these results are similar to what has been shown in the present paper. As for the Erdös-Straus conjecture, William Webb proved in [6] that the density of the numbers for which the conjecture is false is zero, using the fact that one can attest its validity for an infinite set of congruence classes (see Lemma 2 in [6]). The connection with our problem is here less obvious, but in all three cases, ours and these other two, one could solve the respective conundrum by showing that a certain system of congruences is a covering

of the integers[1].

Finally, we mention that our methods also apply to the map $x \mapsto x\lfloor x \rfloor$, since $x\lfloor x \rfloor = \chi(-x)$, for any $x \in \mathbb{Q} \setminus \mathbb{Z}$.

Acknowledgements

Research partially funded by the European Regional Development Fund through the programme COMPETE and by the Portuguese Government through the FCT — *Fundação para a Ciência e a Tecnologia*, under the projects PEst-C/MAT/UI0144/2011 (CMUP — "Centro de Matemática da Universidade do Porto") and PEst-C/MAT/UI0013/2011 (CMAT — "Centro de Matemática da Universidade do Minho").

References

[1] A. H. Fan and L. M. Liao, *On minimal decomposition of p-adic polynomial dynamical systems*, Adv. Math., Vol. 228, 4 (2011) 2116–2144.
[2] C. Moore, *Generalized shifts: unpredictability and undecidability in dynamical systems*, Nonlinearity 4 (1991) 199–230.
[3] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.
[4] R. Terras, *A stopping time problem on the positive integers*, Acta Arith. XXX (1976) 241–252.
[5] I. M. Vinogradov, *Elements of number theory*, Dover Publications, 1954.
[6] W. A. Webb, *On* $4/n = 1/x + 1/y + 1/z$, Proc. of the Amer. Math. Soc. 25 (1970) 578–584.

[1]The question of whether one can prove the Erdös-Straus conjecture by showing its validity on an infinite covering system of congruences is unclear, although there are good reasons to believe it to be an approach riddled with difficulties: see Terrence Tao considerations on this matter in his blog, at `http://terrytao.wordpress.com/2011/07/07/on-the-number-of-solutions-to-4p-1n_1-1n_2-1n_3`.