Periods of discretized linear Anosov maps

Ehrhard Behrends
Bernold Fiedler

Preprint 1/95

Institut für Mathematik I
Freie Universität Berlin
Arnimallee 2-6
D-14195 Berlin
Germany

Abstract

Integer $m \times m$-matrices A with determinant 1 define diffeomorphisms of the m-dimensional torus $T^m = (\mathbb{R}/\mathbb{Z})^m$ into itself. Likewise, they define bijective self-maps of the discretized tori $(\mathbb{Z}/n\,\mathbb{Z})^m = (\mathbb{Z}_n)^m$. We present estimates of the surprisingly low order (or period) $\mathrm{Per}_A(n)$ of the iteration A^r, $r = 1, 2, 3, \ldots$, on the discretized torus $(\mathbb{Z}_n)^m$. We obtain $\mathrm{Per}_A(n) \leq 3n$ for dimension $m = 2$. In the special case of the Anosov map $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, this result is due to [DT92]. For arbitrary dimensions $m > 2$ wo obtain

$$\mathrm{Per}_A(n) \leq const. \cdot n^{m-1},$$

provided n is a power of a prime number. For general n, number theoretic problems arise.

1 Introduction

The linear Anosov map $f : (x, y) \mapsto (2x + y,\ x + y) \bmod 1$, defined for $0 \leq x,\ y \leq 1$ is fundamental in the theory of hyperbolic dynamical systems. [Arn83], [Arn78] illustrate the action of this map by applying f to the two-dimensional caricature of a cat, and f is occasionally also called "Arnold cat map".

The central role of the above Anosov map in the theory of hyperbolic dynamical systems arises from the fact that f constitutes the simplest interesting Anosov diffeomorphism of a compact manifold. The compact manifold, of course, is the two-dimensional torus $T^2 = (\mathbb{R}/\mathbb{Z})^2$. Hyperbolicity means that the tangent space splits into two continuous linear bundles, expanding and contracting, respectively, and both invariant under the linearization of f. In the above example these bundles are given by (appropriately translated) copies of the eigenspaces of the linear map f. On the other hand, f is ergodic with respect to Lebesgue measure, since $detf = 1$.

The periodic points of f are dense in the 2-torus T^2. Indeed, suppose the coordinates x, y are rational with denominator q. Then the components of $f(x, y)$ can likewise be written as rational numbers with denominator q. Since there are at most q^2 such points in T^2, all these points must be periodic with period not exceeding q^2. In particular all points with rational coordinates are periodic under iteration of f. Thus the set of periodic orbits is dense in T^2. Incidentally, it is not difficult to see that the rational points are the only periodic points.

In spite of the countable, dense set of periodic orbits, the dynamics of f is a prototype of chaotic behaviour. For example, consider any periodic orbit. Its stable manifold is given by appropriate translates of the stable eigenspace of the matrix f. Since this eigenspace possesses irrational slope, it is itself

dense in T^2, when considered mod 1. The same holds true for the unstable manifold of any periodic orbit which winds around T^2 densely in the unstable eigendirection. The intersection points of stable and unstable manifolds constitute a dense set of transverse homoclinic points with associated Smale horseshoes and Birkhoff shift dynamics. Moreover there exist trajectories which are dense on T^2, and uncountable subsets such that the trajectories of any two points in such a set possess a *lim inf* of distance which is zero and a *lim sup* of distance which is positive. For more details on the standard Anosov map see [Dev89], [Shu87].

Now consider a finitely discretized version of the map f. By finiteness of state space, any point must then be periodic. Intuitively, however, the chaotic nature of the original map f should be reflected by the fact that periodic points with very large period appear, as the discretization gets finer and finer. Various guesses come to mind as to the period of f itself. Below we will consider an equidistant discretization of the two-torus T^2 by n^2 lattice points. Since the discretized f induces a permutation of the n^2 lattice points, the period of a "chaotic" f might be expected to be of the order of $n^2!$ or, more precisely, of the least common multiple of the cycle lengths in the cycle decomposition of the permutation induced by f. If we consider f as acting on pixel patterns, for example on a discrete version of Arnold's cat, we might expect a period of the arising pattern of the order of 2^{n^2}, the number of $n \times n$ black-and-white-patterns itself. In sharp contrast, another bound of $3n$ was observed in numerical experiments by [HB80] and was proved, in the special case of the above Anosov map, by [DT92]. This surprising observation of very low periods of f motivated our systematic investigation of periods of linear discretized torus maps.

To be specific, let $m \in \mathbb{N}$, $m \geq 2$, and let A be an $m \times m$-matrix with integer coefficients and determinant 1, that is $A \in SL(m, \mathbb{Z})$. For every $n \in \mathbb{N}$, let

A_n denote the induced map

$$A_n : \quad (\mathbb{Z}/n\mathbb{Z})^m \to (\mathbb{Z}/n\mathbb{Z})^m$$

defined by $x \mapsto Ax \bmod n$. Denote the period of A_n by $\mathrm{Per}_A(n)$: this is the smallest integer $r > 0$ such that the iterate $(A_n)^r$ is the identity on $(\mathbb{Z}/n\mathbb{Z})^m$. We have already mentioned that $\mathrm{Per}_A(n)$ is "small" (that is, of the order of n) if A is the cat map $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in SL(2,\mathbb{Z})$.

A number of papers concerning special cases of $\mathrm{Per}_A(n)$ have been published. For example, in [DT92], the cat map is discussed in detail. The main idea there is to use that the cat map A is the square of $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. The iterates of this latter matrix generate the Fibonacci numbers; hence one can use known results on the distribution of Fibonacci numbers mod n. In [HB80], [Kea91], and [PV87] more general matrices $A \in SL(2,\mathbb{Z})$ are discussed. However, the results on $\mathrm{Per}_A(n)$ are restricted to the case of prime numbers $n = p$ or prime powers $n = p^\alpha$. In this connection it should also be noted that general theorems on p-Sylow-subgroups can be used, if $n = p$ is prime, to obtain estimates on $\mathrm{Per}_A(n)$; see section 8, chapter II in [HB80].

In contrast to other approaches we are going to use methods from Galois theory.

This will provide results on $\mathrm{Per}_A(n)$ for arbitrary dimensions m, at least in the case of prime numbers and prime powers n. An extension to arbitrary n seems to involve certain number theoretical problems which are not yet resolved.

Our main results are the following:

Theorem 1.1 *For $A \in SL(2,\mathbb{Z})$ one has $\mathrm{Per}_A(n) \leq 3n$ for all n, and this estimate is sharp.*

Theorem 1.2 *For any $m \in \mathbb{N}$ there exists a constant C_m such that*

$$\mathrm{Per}_A(p^\alpha) \leq \mathrm{C}_m p^{m+\alpha-2}$$

uniformly for all prime powers p^α and all $A \in SL(m, \mathbb{Z})$.

Theorem 1.i will be proved in section i+1 below. We recall that the special case $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ was treated in [DT92]. Impressive and very insightful numerical evidence on $\mathrm{Per}_A(n)$ has been accumulated in the context of quantum theoretical models and discrete approximations to quantum chaos; see [HB80], [Kea91], [PV87]. In conclusion, our theorems exhibit a curious interaction between linearity of the iteration and equidistant lattice discretisation, which sheds some light on the intricacies involved in the discretisation of continuous systems. For further discussion see section 4.

2 The two-dimensional case

The main ideas of our approach will now be explained in detail for the case $m = 2$. See for example [Lan68] for a general introduction to Galois theory.

Let $A \in SL(2, \mathbb{Z})$ be fixed. The characteristic polynomial of A has the form

$$\mathrm{Per}_A(\lambda) = \lambda^2 - \sigma\lambda + 1,$$

where σ is the trace of A. We analyse the behavior of $\mathrm{Per}_A(n)$, first, for prime numbers $n = p$, then for prime powers $n = p^\alpha$, and finally for arbitrary n.

$\underline{\mathrm{Per}_A(n) \text{ for } n = p \text{ prime}}$

Let p be a fixed prime number. We consider

$$A_p : \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$$

as a linear map on the two-dimensional $\mathbb{Z}_p$-vector space $\mathbb{Z}_p^2$, where $\mathbb{Z}_p$ stands for the finite Galois field $\mathbb{Z}/p\mathbb{Z} = GF(p)$.

Replacing A_p by SA_pS^{-1} with an invertible $\mathbb{Z}_p - \text{matrix } S$ does not change the periods. Therefore we can assume, without loss of generality, that A_p is given in its Jordan canonical matrix form. Four cases arise:

(i) $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ (one eigenvalue a in $\mathbb{Z}_p$, with two-dimensional geometric eigenspace $\mathbb{Z}_p^2$). Since $1 = \det A = a^2$ it follows that $0 = (a-1)\cdot(a+1)$ and hence $a = 1$ or $a = -1$, i.e. $\mathrm{Per}_A(p) \in \{1, 2\}$ in this case.

(ii) $A = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ (one eigenvalue a in $\mathbb{Z}_p$, with algebraic multiplicity two, but a one-dimensional geometric eigenspace).

Here the characteristic polynomial is of the form $\mathrm{Per}_A(\lambda) = (\lambda - a)^2$. As in (i), $a = 1$ or $a = -1$. Thus $\sigma = 2$ or $\sigma = -2$ mod p, i.e. the discrimant $D = \sigma^2 - 4$ vanishes mod p. (Note that $D = 0$ mod p can happen for at most finitely many p if $D \neq 0$ in $\mathbb{Z}$.) Since $A^k = \begin{pmatrix} a^k & ka^{k-1} \\ 0 & a^k \end{pmatrix}$, the period $\mathrm{Per}_A(p)$ will will be given by the smallest positive integer $k = 0 \pmod{p}$ such that $a^k = 1$. Hence $\mathrm{Per}_A(p) = p$ or $2p$.

It is also easy to analyse the (minimal) periods $\mathrm{Per}_A(x, p)$ of individual points. Along the geometric eigenspace of a we find, in $\mathbb{Z}_p^2 \setminus \{0\}$, $p-1$ points with period 1 or 2 (if $a = 1$ or -1, respectively). For the remaining x one has $\mathrm{Per}_A(x, p) = \mathrm{Per}_A(p)$.

(iii) $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ (two distinct eigenvalues $a \neq b$ in $\mathbb{Z}_p$).

This happens if, and only if, $\lambda^2 - \sigma\lambda + 1$ possesses two different roots in $\mathbb{Z}_p$, i.e. if and only if $p > 2$ and D is a nonzero quadratic remainder. We have $\det A = ab = 1$ and, by Fermat's Theorem, $a^{p-1} = b^{p-1} = 1$. Therefore, $\mathrm{Per}_A(p)$ divides $p - 1$.

We also note that

$$\mathrm{Per}_A(x, p) = \mathrm{Per}_A(p),$$

for all $x \neq 0$ in $\mathbb{Z}_p^2$.

(iv) $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ (two distinct eigenvalues in a suitable Galois extension of $\mathbb{Z}_p$).

This is the case if, and only if, the discriminant D is not a quadratic remainder mod p. The Galois extension can be chosen to be isomor-

phic to the Galois field $GF(p^2)$. The order of the multiplicative group $GF(p^2)^*$ is p^2-1. In particular $a^{p^2-1} = b^{p^2-1} = 1$.

We claim that in fact

a) $\mathrm{Per}_A(p)$ divides $p+1$, and

b) $\mathrm{Per}_A(x,p) = \mathrm{Per}_A(p)$, for all nonzero $x \in \mathbb{Z}_p^2$.

To prove b), just note that $ab = \det A = 1$ and hence a and b have the same multiplicative order. To prove a) we invoke the Frobenius theorem:

$$\varphi : x \mapsto x^p$$

is an automorphism of $GF(p^2)$ leaving each element of $\mathbb{Z}_p$ fixed. In fact, φ generates the cyclic Galois group $\mathbb{Z}_2$ of $GF(p^2)$ over $\mathbb{Z}_p = GF(p)$. Since $\mathbb{Z}_2$ is realized by interchanging the roots a, b of the characteristic polynomial, this implies

$$a^p = \varphi(a) = b,$$

$$b^p = \varphi(b) = a.$$

Therefore

$$a^{p+1} = ab = b^{p+1} = 1,$$

proving claim a).

We summarize the preceding results.

Proposition 2.1 *Let p be prime and $A \in SL(2,\mathbb{Z})$. Then* $\mathrm{Per}_A(p)$ *divides* $p, 2p, p-1$ or $p+1$. *If $p = 2$, then $Per_A(p) \in \{1,2,3\}$.*

If the discriminant $D \neq 0 \pmod p$, then

$$\mathrm{Per}_A(x,p) = \mathrm{Per}_A(p),$$

for all nonzero $x \in \mathbb{Z}_p^2$.

$\underline{\mathrm{Per}_A(n) \text{ for } n = p^\alpha}$

The results for prime powers $n = p^\alpha$ we summarize next.

Proposition 2.2 *Let p be prime, α any positive integer. Then*

$$Per_A(p^\alpha) \quad divides \quad p^{\alpha-1} Per_A(p).$$

Proof: We proceed by induction on α. The case $\alpha = 1$ is trivial. Suppose the proposition holds for the exponent α. Let $r = p^{\alpha-1}\mathrm{Per}_A(p)$. Then the induction hypothesis implies

$$A^r = Id \pmod{p^\alpha},$$

that is, there exists an integer matrix B such that

$$A^r = Id + p^\alpha B.$$

The binomial theorem then implies

$$A^{rp} = (Id + p^\alpha B)^p = Id + p \cdot p^\alpha B + \sum_{k=2}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) p^{k\alpha} B^k.$$

In other words

$$A^{pr} = Id \pmod{p^{\alpha+1}},$$

and hence $\mathrm{Per}_A(p^{\alpha+1})$ divides $pr = p^\alpha \mathrm{Per}_A(p)$. This completes the induction and the proof.

$\underline{\mathrm{Per}_A(n) \text{ for } n \text{ arbitrary}}$

Here is our main result for the two-dimensional case:

Proposition 2.3

(i) $\mathrm{Per}_A(n) \leq 3n$ for every n.

(ii) $\underline{\lim}\ \mathrm{Per}_A(n)/n = 0$, *if the discriminant* $D \neq 0$ *in* $\mathbb{Z}$.

If the trace σ *of* A *is even then (i) can be sharpened to become* $\mathrm{Per}_A(n) \leq 2n$.

Proof: We prove (i) first. Suppose n_1 and n_2 are relatively prime. Then $\mathrm{Per}_A(n_1 \cdot n_2)$ divides the least common multiple $\mathrm{lcm}(\mathrm{Per}_A(n_1), \mathrm{Per}_A(n_2))$ of the periods associated to the factors. We therefore decompose

$$n = 2^{\alpha_0} n_1 \cdot \ldots \cdot n_k$$

with $n_j = p_j^{\alpha_j}$ and mutually distinct prime factors $p_j > 2$.

Propositions 2.1 and 2.2 imply that there exist $\epsilon_j \in \{1, 2\}$ and $\mu_j \leq n_j$ such that

$$\mathrm{Per}_A(n_j) = \epsilon_j \mu_j.$$

For the even part $n_0 = 2^{\alpha_0}, \alpha_0 > 0$, this estimate can be improved:

$$\mathrm{Per}_A(n_0) \leq \frac{3}{2} n_0.$$

We therefore distinguish two cases.

Case 1: n **is odd.**

Then $2n$ is a common multiple of all $\mathrm{Per}_A(n_j)$, and hence $\mathrm{Per}_A(n_j)$ divides $2n$. Therefore

$$\mathrm{Per}_A(n) \leq 2n.$$

Case 2: n **is even.**

As above, it is sufficient to prove

$$\mathrm{lcm}(\mathrm{Per}_A(n_0),\ \mathrm{Per}_A(n_1), \ldots, \mathrm{Per}_A(n_k)) \leq 3n.$$

This is immediate from the representation $\mathrm{Per}_A(n_j) = \epsilon_j \mu_j, j \geq 1$, and the estimate $\mathrm{Per}_A(n_0) \leq \frac{3}{2} n_0$. This completes the proof of (i).

We prove (ii) next. Since $D \neq 0$ (in $\mathbb{Z}$), we have $D \neq 0 \pmod{n}$ for all but finitely many n, as we recall. Choose $n = p_1 \cdot \ldots \cdot p_k$ to be a product of k mutually distinct odd primes, with nonzero $D \pmod{p_j}$. Then $\mathrm{Per}_A(p_j)$ divides $p_j \pm 1$. Moreover, as above, $\mathrm{Per}_A(n)$ divides

$$\mathrm{lcm}\{\mathrm{Per}_A(p_j) \mid j = 1, \ldots, k\} \quad \leq \quad 2 \prod_{j=1}^{k} \frac{p_j + 1}{2}.$$

Here we have used the fact that all $p_j \pm 1$ are even. Letting $k \to \infty$ and using $p_j > j$ we obtain

$$0 \ \leq \ \overline{\lim_{k \to \infty}} \ \frac{1}{n} \mathrm{Per}_A(n) \ \leq \ \overline{\lim_{k \to \infty}} \ 2^{1-k} \ \prod_{j=1}^{k} (1 + \frac{1}{p_j}) \ = 0.$$

This proves (i).
If the trace σ is even, then $D = \sigma^2 - 4 = 0 \pmod{2}$ and

$$\mathrm{Per}_A(2) \in \{1, 2\},$$

rather than $\{1, 2, 3\}$. With this modification, cases 1,2 above combine as

$$\mathrm{Per}_A(n) \leq 2n.$$

This completes the proof of the proposition, and of theorem 1.1.

3 The m-dimensional case

Fix $m \in \mathbb{N}$, $m \geq 2$, and $A \in SL(m, \mathbb{Z})$. In order to determine $\mathrm{Per}_A(p)$ for fixed prime p we want to describe A_p (the action of A on $(\mathbb{Z}/p\mathbb{Z})^m$), as simply as possible. Denote by $P_A(\lambda) := \det(\lambda Id - A)$ the characteristic polynomial of A; the complexity of the Jordan canonical form of A will depend on the roots of $P_A(\lambda)$ and the multiplicity of the eigenvalues.

Choose any splitting field F_p of $P_A \bmod p$. This might be quite large, but $GF(p^{m!})$ will do for all P_A. In F_p the polynomial $P_A \bmod p$ splits as

$$\Pi_{i=1}^{k}(\lambda - \lambda_i)^{n_i}$$

with $\lambda_1, \ldots, \lambda_k \in F_p$, $\lambda_i \neq \lambda_j$ for $i \neq j$. With respect to a suitably chosen basis, A_p can be built up using $s \times s$ Jordan blocks of the form (λ_i) or

$$\begin{pmatrix} \lambda_i & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{pmatrix},$$

an $s \times s$-matrix which we will call $M(\lambda_i, s)$.

In order to find $\mathrm{Per}_A(p)$ we will again use the fact that the Frobenius map $\varphi : x \mapsto x^p$ is an isomorphism on F_p which leaves $\mathbb{Z}_p$ pointwise fixed. Moreover, φ is an element of the Galois group of P_A over $\mathbb{Z}/p\mathbb{Z}$. Therefore

(a) For every $i \in \{1, \ldots, k\}$ there is $j \in \{1, \ldots, k\}$ with $\lambda_i^p = \lambda_j$.

Also it will be important that $\det A = 1$, hence

(b) $\Pi_1^k \lambda_i^{n_i} = 1.$

Whereas the (λ_0)-blocks behave quite simply under iterations, the $M(\lambda_0, s)$-blocks are a little bit more complicated. A routine calculation shows that $M(\lambda_0, s)^r$ is the matrix for which the j-th row is given by $j-1$ zeros followed by $s-j+1$ elements of the sequence $\lambda_0^r, \binom{r}{1}\lambda_0^{r-1}, \binom{r}{2}\lambda_0^{r-2}, \cdots, \binom{r}{r-1}\lambda_0, 1, 0, 0 \ldots$. Here $\binom{r}{j}$ are again the binomial coefficients. We conclude

(c) $M(\lambda_i, s)^r = Id \bmod p$ iff $\lambda_i^r = 1$ and p divides r.

We are now ready for the proof of our main result.

Theorem 3.1 *For any $m \geq 2$, there is a constant C depending only on m such that*

$$\mathrm{Per}_A(p) \leq C p^{m-1}$$

for all $A \in SL(m, \mathbb{Z})$ and all prime numbers p.

Proof: By (a) we can renumber and rearrange $\{\lambda_1, \ldots, \lambda_k\}$ as $\lambda_1, \lambda_1^p, \ldots, \lambda_1^{p^{\alpha_1}}, \lambda_2, \lambda_2^p, \ldots, \lambda_2^{p^{\alpha_2}}, \ldots, \lambda_t, \lambda_t^p, \ldots, \lambda_t^{p^{\alpha_t}}$ with $\alpha_\tau \geq 0$, $((\lambda_\tau)^{p^{\alpha_\tau}})^p = \lambda_\tau$ for $\tau = 1, \ldots, t$. It will be convenient to consider the following three cases.

Case 1: $k \leq m-2$.
This is the simplest case: The $\lambda_\tau, \lambda_\tau^p, \ldots, \lambda_\tau^{p^{\alpha_\tau}}$ each have an order which divides $p^{\alpha_\tau+1}-1$. Therefore the least common multiple r of the numbers $p^{\alpha_1+1}-1, \ldots, p^{\alpha_t+1}-1$ satisfies $\lambda_i^r = 1$ for $i = 1, \ldots, k$. But r divides

$$\tilde{r} := (p-1)(1+p+\ldots+p^{\alpha_1}) \ldots (1+p+\ldots+p^{\alpha_t}).$$

By (c), we conclude

$$A^{p\tilde{r}} = \mathrm{Id} \pmod p.$$

Now we can estimate

$$p\tilde{r} \leq Cp^{2+\alpha_1+\ldots+\alpha_t} = Cp^{2+k-t} \leq Cp^{m-1},$$

completing the proof in case 1.

Case 2: $k = m$

In this case A_p has m eigenvalues which are pairwise distinct. In Jordan form, A is a diagonal matrix with entries $\lambda_1, \ldots, \lambda_m$. We renumber the eigenvalues as above.

If $t > 1$ we conclude again that $\lambda_i^{\tilde{r}} = 1$, for all i, if we define

$$\tilde{r} = (p-1)(1 + p + \ldots + p^{\alpha_1}) \ldots (1 + p + \ldots + p^{\alpha_t}).$$

Since A is diagonal, $\mathrm{Per}_A(p)$ divides $\tilde{r}$, and we can estimate

$$\tilde{r} \leq C\, p^{1+\alpha_1+\ldots+\alpha_t} = C_1\, p^{1+m-t} \leq Cp^{m-1}.$$

It remains to treat the case $t = 1$ (which occurs, e.g., if P_A is irreducible mod p). This time we use (b) to conclude that $1 = \lambda_1\, \lambda_2 \ldots \lambda_m = \lambda_1^{(1+p+\ldots+p^{m-1})}$. It follows that $\mathrm{Per}_A(p)$ divides

$$1 + p + \ldots + p^{m-1} \leq mp^{m-1}.$$

Case 3: $k = m - 1$

If $t \geq 2$ we conclude as in the first case that $\mathrm{Per}_A(p) \leq Cp^{m-1}$. So let $t = 1$. This means that the different roots of P_A mod p are given by $\lambda_1, \lambda_1^p, \ldots, \lambda_1^{p^{m-2}}$ and that, wlog, λ_1 has multiplicity 2. this implies $\lambda_1^{2+p+\cdots p^{m-2}} = 1$, and therefore $\tilde{r} := p(2 + p + \ldots p^{m-2})$ is a number such that $\lambda_i^{\tilde{r}} = 1$ as well as $M(\lambda_1, 2)^{\tilde{r}} = \mathrm{Id}$ mod p. Hence $\mathrm{Per}_A(p)$ divides $\tilde{r}$, and $\tilde{r} \leq Cp^{m-1}$. This completes the proof of Theorem 3.1.

As in section 2 it is easy to generalize our results to prime powers. Repeating the above proof one arrives at $\mathrm{Per}_A(p^\alpha) \mid p^{\alpha-1}\mathrm{Per}_A(p) \leq Cp^{\alpha-1}p^{m-1}$. This proves theorem 1.2.

It is, however, considerably more difficult to deal with arbitrary numbers n. Again it is obvious that $\mathrm{Per}_A(n_1n_2)$ divides the least common multiple of $\mathrm{Per}_A(n_1), \mathrm{Per}_A(n_2)$ if n_1, n_2 are relatively prime. But the estimate $\mathrm{Per}_A(n_j) \leq Cn_j^{m-1}$ only implies $\mathrm{Per}_A(n_1n_2) \leq C^2(n_1n_2)^{m-1}$. Therefore it remains an open question, whether there exists a uniform $\tilde{C}$ such that $\mathrm{Per}_A(n) \leq \tilde{C}n^{m-1}$ for all n.

Let us have a closer look at the case $m = 3$. From the proof of our theorems one concludes that for any p one of the following possibilities occurs: $\mathrm{Per}_A(p)$ divides $p-1, p^2-1, p(p-1)$, or $1+p+p^2$. This is in contrast to the situation of section 2 where all possible $\mathrm{Per}_A(p)$ could be written as $\epsilon_p\mu_p$ with $\epsilon_p \in \{1,2\}, \mu_p \leq p$. Whereas the terms $p-1, p^2-1, p(p-1)$ can be treated easily, there seems to be no simple way to treat the $1+p+p^2$ similarly.

4 Discussion

Here we will discuss a slight generalization as well as some sharper results on $\mathrm{Per}_A(n)$, provided that additional information on A is available. We conclude with a brief discussion of nonlinear aspects.

We have restricted attention to $A \in SL(m, \mathbb{Z})$. But our results apply to $A \in GL(m, \mathbb{Z})$ as well because for these A one has $A^2 \in SL(m, \mathbb{Z})$ and thus – up to a factor 2 – similar estimates.

The proof of theorem 3.1 is particularly simple when all roots of $P_A \bmod p$ are simple, see case 2, $k = m$. There is a standard criterion for simplicity of zeros of a polynomial P: the discriminant D associated to P must be nonzero. Recall that the *discriminant* D of $P(\lambda) = \prod(\lambda - \lambda_i)$ is defined as the product

$$D = \prod_{i<j} (\lambda_i - \lambda_j)^2.$$

The discriminant D can be expressed as a polynomial in the coefficients of P, namely as the resultant of P and its formal derivative P'. In other words $D \neq 0$ if, and only if, P and P' are relatively prime (see e.g. [vdW71] where also some explicit formulas are derived).

Suppose now that A is such that the discriminent D_A of P_A is nonzero. Then $D_A \bmod p$, being a polynomial in the coefficients of $P_A \bmod p$, is nonzero for all but finitely many p. For p with $D_A \neq 0 \bmod p$, the roots of $P_A \bmod p$ are necessarily all distinct. This circumvents the discussion of cases 1 and 3 in the proof of theorem 3.1, and the constant C in the assertion of this theorem can therefore be reduced considerably. However, the explicit determination of D_A may be quite cumbersome in practice.

In the case of the Anosov map, $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, we observe that $\mathrm{Per}_A(p)$ can

be significantly smaller than predicted by our general theory. Specifically, computer tests have indicated that $\mathrm{Per}_{A_0}(p)$ divides $(p-1)/2$ if $D=5$ is a quadratic remainder mod p. In contrast, our theory only yields that $\mathrm{Per}_{A_0}(p)$ divides $(p-1)$. The reason for the reduced period is the following number theoretical assertion.

Lemma 4.1 *Let p be prime such that $x+\frac{1}{x}=3$ possesses a solution x in $\mathbb{Z}_p$. Then x is a square, and in particular $x^{(p-1)/2}=1$.*

First proof (V. Schulze): Only note that $\left(\frac{1\pm\sqrt{5}}{2}\right)^2=\frac{3\pm\sqrt{5}}{2}$ in any field. So $x+\frac{1}{x}=3$ implies that $x=\frac{3\pm\sqrt{5}}{2}$ is a square (mod p).

Second proof: Note that $A=B^2$ with the notation

$$A=\begin{pmatrix}2&1\\1&1\end{pmatrix},\qquad B=\begin{pmatrix}1&1\\1&0\end{pmatrix}.$$

For both matrices the discriminant of the characteristic poloynomial is 5. Thus, if 5 is a quadratic remainder mod p, then B can be diagonalized mod p. With respect to the same basis, A is also diagonal and the diagonal entries are squares. But these entries are just the eigenvalues, viz. the solutions of $x+\frac{1}{x}=3$. More generally, suppose A is such that $A=B^2$ for some $B\in SL(m,\mathbb{Z})$. Further suppose that $\mathrm{Per}_B(n)$ is even, say $\mathrm{Per}_B(n)=2k$. Then $A^k=\mathrm{Id}$ mod n, that is $\mathrm{Per}_A(n)$ divides k. In this way it is possible to obtain better estimates on $\mathrm{Per}_A(n)$ provided $A=B^2$ (or more generally $A=B^r$) can be solved for B in $SL(m,\mathbb{Z})$ or in $GL(m,\mathbb{Z})$.

Structural stability is a prominent aspect of Anosov theory for hyperbolic diffeomorphismus of compact manifolds. In our original, continuous setting,

this means the following. Let

$$A: \quad T^2 \to T^2$$

be linear hyperbolic, that is, $A \in SL(2, \mathbb{Z})$ with simple real eigenvalues λ and λ^{-1}. Consider a C^1-small pertubation f of A, that is,

$$f = A + \epsilon g,$$

where $g : T^2 \to T^2$ is continuously differentiable, but nonlinear, and $|\epsilon|$ is small. Then there exists $\epsilon_0 > 0$ and, for any $|\epsilon| < \epsilon_0$, a homeomorphism h_ϵ of T^2 which conjugates f and the linear Anosov map A:

$$f = h_\epsilon^{-1} \circ A \circ h_\epsilon.$$

In particular, periodic orbits, dense orbits, stable and unstable foliations, Markov partitions, shift dynamics of A and f correspond, via h_ϵ. See [Arn83], [Dev89], [Shu87] for a reference.

Our results demonstrate how dramatically the complicated dynamics of A on T^2 collapses under equidistant discretization, replacing T^2 by $T_n^2 = (\mathbb{Z}_n)^2$. It seems natural to investigate the fate of structural stability under discretization. A discrete version of f can be obtained, for example, via the pairwise disjoint boxes covering T^2 and centered around the points of the discrete lattice $\mathbb{Z}_n^2$. Any lattice point maps to some box, under f, to which we can then assign its central lattice point again in a unique way. Let f_n denote this discretized map associated to f.

Shadowing is a concept which applies to individual discretized trajectories [Pal84]. Let $|\epsilon| < \epsilon_0$, so that f is still uniformly hyperbolic on T^2. For $n \geq n_0$, the discrete trajectories of f_n described above can be viewed as pseudo-orbits of f. By shadowing, there exists a true orbit of f, on T^2, which remains uniformly close to the pseudo-orbit under *all* iterates f_n, $n \in \mathbb{Z}$ of f: the

true orbit of f *shadows* the discrete pseudo-orbit. By definition, the shadow orbit is periodic with minimal period bounded by n^2.

Under (discrete) conjugation, the period of a map remains unchanged:

$$A_n^r = \mathrm{Id} \qquad \Rightarrow \qquad (h^{-1} \circ A_n \circ h)^r = \mathrm{Id}$$

for any bijection $h : T_n^2 \to T_n^2$. So: how small are the periods of the discretized maps f_n on T^2? Shadowing does not address this question. Moreover, the period of f_n is the least common multiple of the periods of *all* orbits of f_n.

Since A maps lattice points to lattice points, the same holds true for f_n associated to $f = A + \epsilon g$, of course, provided that $|\epsilon| < \epsilon_n$. Indeed, we can guarantee $f_n = A_n$. Note that $\epsilon_n \to 0$ for $n \to \infty$. Therefore, this is not a statement resembling structural stability of A. First computer experiments seem to indicate that, in fact, periods of f_n can become very large as soon as ϵ is chosen large enough to make f_n deviate from A_n. But, at present, we are not able to provide any theoretical corroboration of these experiments.

References

[Arn78] V.I. Arnol'd. *Ordinary Differential Equations.* MIT Press, Cambridge Massachusetts, 1978.

[Arn83] V.I. Arnol'd. *Geometrical Methods in the Theory of Ordinary Differential Equations.* Springer Verlag, New York, 1983.

[Dev89] Robert L. Devaney. *Chaotic Dynamical Systems.* Addison-Wesley, New York, 1989.

[DT92] F.J. Dyson and H. Talk. Period of a discrete cat mapping. *Am. Math. Monthly*, (**99**):603–614, (1992).

[HB80] J.H. Hannay and M.V. Berry. Quantization of linear maps on the torus-fresuel diffraction by a periodic grating. *Physica D*, (**1**):267–291, (1980).

[Kea91] J. Keating. The cat maps: quantum mechanics and classical motion. *Nonlinearity*, (**4**):309–341, (1991).

[Lan68] S. Lang. *Algebra.* Addison-Wesley, New York, 1968.

[Pal84] K. J. Palmer. Exponential dichotomies and transversal homoclinic points. *J. Diff. Eq.*, (**55**):225–256, (1984).

[PV87] I. Percival and F. Vivaldi. Arithmetic properties of strongly chaotic motions. *Physica D*, (**25**):105–130, (1987).

[Shu87] Michael Shub. *Global Stability of Dynamical Systems.* Springer Verlag, New York, 1987.

[vdW71] B.L. van der Waerden. *Algebra I.* Springer Verlag, Berlin, 1971.