The arithmetic structure of discrete dynamical systems on the torus

Dissertation
zur Erlangung des Doktorgrades
der Mathematik

an der Fakultät für Mathematik
der Universität Bielefeld

vorgelegt von

Natascha Neumärker

Bielefeld, im Mai 2012

Erstgutachter: Professor Dr. Michael Baake
Zweitgutachter: Professor John A.G. Roberts, PhD

Gedruckt auf alterungsbeständigem Papier nach ISO 9706.

Contents

1 Introduction

In this thesis, the structure and the distribution of periodic (and preperiodic) orbits in certain discrete dynamical systems are studied. The classes of dynamical systems considered here – toral endomorphisms and the Casati-Prosen triangle map – are maps on the torus, which possess finite invariant subsets, on which the structure of the orbits follows certain organising principles.

Periodic orbits are among the key objects to be studied in a dynamical system; an illustration of this fact is, for instance, given by Devaney's definition of chaos, simplified by Banks, Brooks, Cairns, Davis and Stacey [18]. According to the latter, a continuous map T on a metric space X is chaotic if firstly, T is transitive (i.e. for every open non-empty set U, there is a k such that $T^k(U \cap V) \neq \emptyset$ for every open set $V \neq \emptyset$), and secondly, the periodic points are dense in X.

Another example is the theorem by Bowen and Sinai; compare e.g. [60, Chap. IV, Thm. 9.1]. It states that for an (intrinsically ergodic) topologically mixing hyperbolic homeomorphism, the integral of any continuous function with respect to the intrinsic measure can be expressed as the limit (as $n \to \infty$) of this function averaged over the n-periodic points of the hyperbolic homeomorphism.

A further illustration is provided by semi-classical approximations of quantum mechanical systems, where the density of states is written as a sum over the classical periodic orbits; see [19] and references therein.

In more recent work [70, 71, 72], the limiting periodic distribution of algebraic maps was investigated and it was conjectured that certain (appropriately normalised) distributions of period lengths of "sufficiently random" maps are, possibly universally, determined by generic properties of the map.

The most interesting classes of dynamical systems are the non-linear ones. Although toral endomorphisms are defined by integer matrices, the action modulo 1 introduces non-linearities, and number-theoretic principles govern the period distribution. Toral endomorphisms are a well-studied class of dynamical systems, and serve as a standard example in ergodic theory. A particularly important subclass is given by the hyperbolic toral automorphisms which are topologically mixing and intrinsically ergodic [47, 82]. The most prominent example is Arnold's cat map, which was first introduced by Arnol'd as an example of an Anosov diffeomorphism. Its periodic orbits have been studied on the basis of arithmetic properties of the Fibonacci numbers; see [38, 32] for some results.

The dynamics induced by toral automorphisms has also been studied as a toy model for quantum chaos. In the articles [48, 49, 52, 30], it is described how the quantum operators associated with some (perturbed) cat map are constructed from the classical (perturbed) cat map on a particular rational lattice. The impact of local symmetries on the global eigenvalue statistics is considered in [49, 52, 30], and also highlights the significance of local (reversing) symmetries, that is, in the setting of toral endomorphisms on rational lattices, matrices that conjugate the reduction of a given endomorphism on the lattice into itself or its inverse, respectively.

Another motivation for studying periods of cat maps comes from cryptography, particularly image encryption. In [36], a parameterised version of Arnold's cat map was proposed as a chaotic map to create a certain encryption scheme; [26] presents an image encryption method based on three-dimensional cat maps.

As a consequence of the interest in toral endomorphisms from many very different points

of view, the literature is vast and unsystematic. Methods employed to study the orbit counts and orbit distribution of toral automorphisms are numerous, compare, for instance, [74, 66, 20, 38, 32, 16]. Most accounts specialise on matrices from $\mathrm{SL}(2,\mathbb{Z})$. While this restriction is justified from a dynamical point of view, it is not a natural constraint from an algebraic or number-theoretic one.

The non-invertible case has received comparably little attention; for related questions, although not written from the perspective of toral endomorphisms, see [22, 80]. As long as integer matrices are considered whose determinant is coprime with the denominator associated with some fixed lattice, no structural difference between endomorphisms and autormorphisms is visible on this particular lattice. In contrast, a non-invertible map on a finite set induces a graph that admits 'pretails' to the periodic points consumed in cycles. For toral endomorphisms, the possible structure of the graphs induced on lattices where their restrictions are not invertible is highly constrained due to the linearity. Thus, in this case, toral endomorphisms are among the simplest models possible for non-invertible dynamics on finite spaces. Other recent work on the structure of non-invertible dynamics induced by algebraic maps on finite spaces includes, for instance, [21, 77, 78, 79].

The Casati-Prosen map (CP map) is a two-parameter zero-entropy family of maps on the two-dimensional torus. It can be seen as a special case of classically reversible maps that are compositions of two involutions, and it can be studied within the framework of (discrete) reversible maps on finite spaces, cf. [70, 71, 72]. The dynamical properties of the CP map on the torus were studied in detail in [43], where it was conjectured to be strictly ergodic and mixing for irrational parameter values. For rational parameters, it is known to foliate the phase space into invariant curves (on which it acts as an interval exchange transformation), see [43] and references therein. Restricted to preserved rational lattices, for most parameter values, it displays an orbit statistics which was believed to require more deterministic randomness of the map, see Section 6, and which was proved to be the expected limiting distribution of random reversible maps of asymptotically large sets [72]. Being a parabolic toral endomorphism in the case of vanishing parameters on the one hand, and showing the more random behaviour similar to that of the reduction of rational reversible maps over finite fields on the other hand, the CP map can be seen as a minimal departure from both of these classes of maps. This motivates our interest in this family of maps.

The goal of the thesis is to contribute to the questions discussed above. For the study of toral endomorphisms on the rational lattices, we adopt a normal form approach with respect to conjugacy over the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$. We drop the somewhat artificial constraint of determinant ± 1, a vital theme being the decomposition of a given (prime power) lattice into a sublattice where the endomorphism is invertible and one where it is nilpotent. A central task is to identify characteristic quantities characterising the action of a given endomorphism on a certain lattice and to study them systematically. To this end, we investigate the structure of the graphs induced by toral endomorphisms on rational lattices where it is not locally invertible and classify them according to the invariant factors of their matrix powers.

Since part of the motivation to study toral endomorphisms comes from physical systems, where symmetry and (time) reversing symmetries play an important role, we also investigate the (local) reversing symmetry groups of toral endomorphisms and relate them to their dynamics.

For the Casati-Prosen map, our main concern is the convergence properties of the distributions of period lengths on prime lattices. By performing large-scale exact computations, it is

one of our main objectives to obtain a detailed picture of the period distributions, particularly in the limit of large primes, and to identify parameter values for which the CP map displays the behaviour of random reversible maps.

The thesis is organised as follows. Sections 2-5 are devoted to the study of toral endomorphisms on the rational lattices, while Sections 6 and 7 are concerned with the Casati-Prosen map with rational parameters on lattices of the two-dimensional torus; Section 8 gives a summary and an outlook.

Section 2 introduces the setting and notation, and briefly recalls mathematical concepts and results used throughout. Section 3 compiles the theory of determining order and period lengths of (locally) invertible toral endomorphisms on a given rational lattice and aims at generalising known results as well as unifying known approaches as far as possible. By means of equivalent matrices, we examine the subgroups of the torus and particular rational lattices induced by an integer matrix and consider consequences for the relation between local and global orbit counts (Sections 3.2 and 3.3). We summarise what is known about the order growth of integer matrices modulo prime powers, state a sufficient criterion for a lattice point to have maximal period, and give a formula for matrix powers in terms of its first d powers and an associated recurrence sequence (Sections 3.4 and 3.5). In Sections 3.6–3.8, we turn the problem of determining period lengths on a certain rational lattice into an algebraic one by using the theory of linear recursions, look at simplifications for 2×2 matrices and address the question of general applicability by discussing normal forms over the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$, as well as conjugacy invariants.

Section 4 is focused on general endomorphisms and discusses the structure of the graphs induced on lattices where the restrictions are non-invertible. Applying module theory, we decompose the rational lattices into invariant submodules on which the endomorphism is invertible and nilpotent, respectively (Section 4.1); we note that all periodic points have the same pretail structure, which motivates the assignment of a tree to each endomorphism on a fixed lattice, whose structure is determined by the cardinalities of certain subgroups of the kernel (Section 4.2). On the prime power lattices, the submodules are in fact free, and the trees admit a simple parametrisation in terms of integer partitions (Section 4.3). We calculate the numbers of occurrences of each tree type on the prime lattices, and conclude Section 4 with some remarks on the structure of the global pretail tree.

Section 5 deals with symmetry properties of toral endomorphisms, with focus on the symmetry and reversing symmetry groups of locally invertible endomorphisms on the prime lattices. In Section 5.1, we show that $\mathrm{SL}(2,\mathbb{Z})$ matrices always possess an involutory reversor on each rational lattice (without necessarily being reversible over $\mathbb{Z}$), which determines the structure of their reversing symmetry group as a semi-direct product. In Section 5.2, we calculate the (reversing) symmetry groups of $\mathrm{GL}(2,\mathbb{F}_p)$ matrices and relate it to dynamical properties on the prime lattices. We show that reversibility of 2×2-matrices modulo n essentially depends on the residue class of the determinant modulo all prime powers dividing n (Section 5.3) and finally consider the symmetry groups of $d \times d$ matrices with irreducible characteristic polynomial over $\mathbb{F}_p$, whose structure is determined by the existence of a primitive root (Section 5.4). Sections 2–5 are to some extent based on the paper [15].

In Section 6, we present the Casati-Prosen map on the torus within a large class of classically reversible maps and formulate conjectures about the nature and distribution of periodic orbits on the prime lattices. We briefly review the setting and the combinatorial model on the basis of which we examine the CP map on prime lattices in Section 6.1, and investigate the

symmetry properties of the CP map in Section 6.2. In Section 6.3, we present the different distributions observed for appropriate parameter pairs on the prime lattices and formulate conjectures concerning the parameters leading to the gamma distribution and certain singular distributions, respectively. Section 7 presents data from exact computations that underpin the conjectures stated in Section 6; in Section 7.5 we give concluding remarks. Sections 6 and 7 are essentially based on the paper [62].

Section 8 provides a brief summary and formulates some open questions, as well as starting points for further research.

2 Preliminaries

In this section, the setting and notation for the study of periodic and preperiodic points of toral endomorphisms in Sections 3 to 5 is introduced. While it is mainly written with focus on toral endomorphisms, large parts apply to all of the thesis. Sections 3 to 5 are to some extent based on the article [15]. A table of symbols can be found after the Appendix.

2.1 The torus

The d-dimensional torus $\mathbb{T}^d$ is a compact Abelian group, which is written either multiplicatively or additively, compare [82, §0.8]. Throughout this work, the additive notation $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ will be used, which can be identified with a Cartesian product of the unit interval, $[0,1)^d$, on which the addition of two elements is performed modulo 1, that is, the integer part is dropped and only the fractional part 'survives'. More precisely, two real numbers x_1 and x_2 coincide modulo 1 if and only if $x_1 - x_2 \in \mathbb{Z}$.

*Torus (*or *toral) endomorphisms* are maps on the torus, preserving its group structure. Each toral endomorphism is induced by an integer matrix which acts on the torus modulo 1, [82, Thm. 0.15]. By abuse of notation, we do not distinguish between an integer matrix and the endomorphism it induces. If the determinant of the defining integer matrix is 1 or -1, the matrix has an inverse which is also an integer matrix, and the endomorphism is invertible, hence an *automorphism*. Each endomorphism $M : \mathbb{T}^d \longrightarrow \mathbb{T}^d$ induces the discrete dynamical system $(\mathbb{T}^d, M)$, in which the time evolution is given by the iteration of M on $\mathbb{T}^d$.

2.2 The rational lattices and related rings, modules and groups

Since the torus $\mathbb{T}^d$ is a compact Abelian group, a lattice on the torus is just a discrete subgroup of $\mathbb{T}^d$. The most important lattices on $\mathbb{T}^d$ consist of the n-division points

$$\Lambda_n := \{x \in \mathbb{T}^d \mid nx = 0 \pmod 1\} = \left\{\left(\tfrac{k_1}{n}, \ldots, \tfrac{k_d}{n}\right)^t \mid 0 \leq k_i < n \text{ for all } 1 \leq i \leq d\right\}, \quad (1)$$

with $n \in \mathbb{N}$. For $k|n$, one has $\Lambda_k \subset \Lambda_n$.

Clearly, the Λ_n are invariant under toral endomorphisms (with the action of the representing matrices taken mod 1), hence one can consider the restriction $M : \Lambda_n \longrightarrow \Lambda_n$. It is sometimes easier to replace Λ_n by the set $\tilde{\Lambda}_n := \{(k_1, \ldots, k_d)^t \mid 0 \leq k_i < n\}$, with the equivalent action of M defined mod n. This also applies to various theoretical arguments involving modular arithmetic. Consequently, we use Λ_n (with action of M mod 1) and $\tilde{\Lambda}_n$ (with action mod n) in parallel.

The lattices constitute Abelian groups (or, equivalently, modules over the principal ideal domain $\mathbb{Z}$). By the identification with $\tilde{\Lambda}_n$, it is obvious that Λ_n can as well be identified with the free $\mathbb{Z}/n\mathbb{Z}$ - module $(\mathbb{Z}/n\mathbb{Z})^d$. Hence a large part of the discussion will revolve around the residue class rings $\mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}$, which is a principal ideal ring, but not a domain, unless $n = p$ is a prime. In the latter case, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is the finite field with p elements, while the ring has zero divisors otherwise. For general n, the unit group

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{1 \leq m \leq n \mid \gcd(m,n) = 1\}$$

is an Abelian group (under multiplication) of order $\phi(n)$, where ϕ is Euler's totient function from elementary number theory [42]. In general, it is not a cyclic group.

M has a local inverse on Λ_n if and only if $\det(M) \in (\mathbb{Z}/n\mathbb{Z})^\times$. In other words, if $\det(M)$ is coprime with n, there is an integer matrix N, such that $MN \equiv \mathbb{1} \mod n$.

For a composed number n, the lattice Λ_n can be written as the direct sum of the lattices associated with coprime divisors of n. A consequence of this elementary fact is that the action of an integer matrix on Λ_n can be derived in a purely combinatorial way from that on appropriate sublattices, see Section 3.1 for the explicit dependence.

For this reason, it is clear that the lattices Λ_n where n is a prime power play a decisive role. Moreover, the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$, p a prime, $r \geq 1$, are local rings, that is they have a unique maximal ideal, $(p) = p\,\mathbb{Z}/p^r\mathbb{Z}$, which contains all zero divisors. Results based on this additional structure will be used in Sections 3.6 and 4.3. The development of Galois-theory over local commutative rings is to a large extent parallel with that for finite fields, see [59, Chap. XV] for details and background. In Section 3.6, we will make use of a result on the order of the unit group of the Galois ring $\mathbb{Z}/p^r\mathbb{Z}[x]/\langle F(x)\rangle$, where $F(x) \in \mathbb{Z}[x]$ is a polynomial whose reduction over $\mathbb{Z}/p\mathbb{Z}$ is irreducible.

One way of obtaining the ring of the *p-adic integers* $\mathbb{Z}_p$, is forming the inverse limit of the rings $\mathbb{Z}/p^r\mathbb{Z}$ for $r \to \infty$, compare [54, Chap. III, §10]. If one thinks of the field $\mathbb{Q}_p$ as the set of all power series in p with only finitely many powers of negative exponents, the ring $\mathbb{Z}_p$ is then the subset of all series without terms of negative exponent. The standard projection $\pi : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^r\mathbb{Z}$ is defined by truncating a series after the term with exponent $r-1$. The subset of finite series provides a natural embedding of $\mathbb{Z} \subset \mathbb{Z}_p$.

For an integer $a \in \mathbb{Z}$, the *p-adic valuation* $v_p(a)$ is the largest exponent r such that $p^r|a$. In other words, $p^{v_p(a)}||a$, that is, $p^{v_p(a)}$ is the highest power of p dividing a. The p-adic norm is defined by $|a|_p = p^{-v_p(a)}$. In this norm, all power series associated with the elements of $\mathbb{Q}_p$ converge.

2.3 Integer matrices

2.3.1 Matrix rings

The integer matrices mod n form the finite ring $\mathrm{Mat}(d, \mathbb{Z}/n\mathbb{Z})$ of order n^{d^2}. The invertible elements in it form the group $\mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z}) = \{M \in \mathrm{Mat}(d, \mathbb{Z}/n\mathbb{Z}) \mid \det(M) \in (\mathbb{Z}/n\mathbb{Z})^\times\}$. If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$ is the standard prime decomposition, one finds

$$\left|\,\mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z})\right| \;=\; n^{d^2} \prod_{j=1}^{\ell} \frac{\left|\,\mathrm{GL}(d, \mathbb{F}_{p_j})\right|}{p_j^{d^2}}\,, \tag{2}$$

where

$$\left|\,\mathrm{GL}(d, \mathbb{F}_p)\right| \;=\; (p^d - 1)(p^d - p) \cdot \ldots \cdot (p^d - p^{d-1}) \tag{3}$$

is well-known from the standard literature [54, 56]. Formula (2) follows from the corresponding one for $n = p^r$ via the Chinese remainder theorem, while the simpler prime power case is a consequence of the observation that each element of a non-singular matrix M over $\mathbb{Z}/p^s\mathbb{Z}$ can be covered (independently of all other matrix elements) by p elements in $\mathbb{Z}/p^{s+1}\mathbb{Z}$ without affecting its non-singularity.

Let us finally mention that $\mathrm{SL}(n, \mathbb{Z}/n\mathbb{Z})$, the subgroup of matrices with determinant 1, is a normal subgroup (it is the kernel of $\det\colon \mathrm{GL}(n, \mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$). The factor group is

$$\mathrm{GL}(n, \mathbb{Z}/n\mathbb{Z})/\,\mathrm{SL}(n, \mathbb{Z}/n\mathbb{Z}) \;\simeq\; (\mathbb{Z}/n\mathbb{Z})^\times$$

and thus has order $\phi(n)$.

2.3.2 The Smith normal form

A helpful device when studying the reduction of integer matrices over different residue class rings is the *Smith normal form* (SNF), see [65, 1]. We only need the special case of square matrices over the integers.

Recall that two integer matrices A, B are *equivalent*, if there are invertible integer matrices P, Q, such that $PAQ = B$.

By a *k-minor* of a $d \times d$ integer matrix A, we mean the determinant of any $k \times k$ matrix $A_{\tau,\rho}$, where $\tau = \{\tau_1, \ldots, \tau_k\}$, $\rho = \{\rho_1, \ldots, \rho_k\}$ with $1 \leq \tau_1 < \tau_2 < \ldots < \tau_k \leq d$, $1 \leq \rho_1 < \rho_2 < \ldots < \rho_k \leq d$, which is formed from A by selecting the rows whose indices are elements of τ and the columns whose indices are elements of ρ.

Let M be a $d \times d$ integer matrix and $d_k(M)$ the greatest common divisors of all $\binom{d}{k}^2$ k-minors. One sets $d_k(M) = 0$ if all k-minors vanish and $d_0(M) = 1$. The maximal number r such that $d_r(M) \neq 0$ is the rank of M (over $\mathbb{Z}$). Clearly, $d_i(M) | d_{i+1}(M)$ for $1 \leq i \leq r-1$. For $r \geq k \geq 1$, put $s_k(M) = \frac{d_k(M)}{d_{k-1}(M)}$, which is the *k-th invariant factor* of M. For convenience, we set $s_{r+1}(M) = \ldots = s_d(M) = 0$ and omit the M-dependence in the following. Then M is equivalent with $\mathrm{diag}(s_1, \ldots, s_r, 0, \ldots, 0)$ which is called the *Smith normal form* of M and will be denoted by $\mathrm{SNF}(M)$ in what follows. Hence, we have integer matrices P, Q such that

$$\mathrm{SNF}(M) = \mathrm{diag}(s_1, \ldots, s_r, s_{r+1}, \ldots, s_d) = PMQ. \tag{4}$$

2.4 Orbit counts and generating functions

Among the standard quantities to investigate in a dynamical system are its periodic points, partitioned into periodic orbits. For a general map $T : X \longrightarrow X$ on a set X, a point $x \in X$ is said to be *periodic with period* k, if $T^k x = x$, where T^k denotes, as usually, the k-th iteration of the map T starting from x. The *minimal* or *least period* of x is the least integer k such that x is periodic with period k. The *periodic orbit* (of some periodic point x) is the finite set $\{T^k x \mid k \geq 0\}$. The least period of x is also called the length of the periodic orbit of x under T. The numbers of periodic points of T and the number of periodic orbits of length n will be denoted by a_n and c_n, respectively. They define two sequences of non-negative integers which will also be referred to as *fixed point count sequence* or *fixed point counts* and *orbit count sequence* or *orbit counts*.

Recall that, if a_m and c_m denote the fixed point and orbit count numbers of T, they are related by

$$a_m \;=\; \sum_{d|m} d\, c_d \quad \text{and} \quad c_m \;=\; \frac{1}{m} \sum_{d|m} \mu\big(\tfrac{m}{d}\big)\, a_d, \tag{5}$$

where $\mu(k)$ is the Möbius function from elementary number theory [42]. For further aspects on the interplay of fixed point and orbit count sequences, see [64, 11].

Often, the fixed point count numbers a_n are easiest to access in a dynamical system. However, as expressed by the transformation formulae above, the numbers a_n have the drawback of recounting points of period $d|n$ for every n. For that reason, sometimes the quantity $a_n^* = n \cdot c_n$, the number of points of minimal period n is introduced. Whenever possible, we will work with the orbit count numbers c_n. The fixed point counts admit an Euler product decomposition in which the orbit counts show up.

By the *dynamical zeta function* and its Euler product decomposition, we mean

$$\zeta(t) \coloneqq \exp\left(\sum_{m=1}^{\infty} \frac{a_m}{m} t^m\right) = \prod_{m\geq 1} (1-t^m)^{-c_m}. \tag{6}$$

In the context of toral endomorphisms, where $T = M$ with some matrix $M \in \mathrm{Mat}(d, \mathbb{Z})$, apart from the 'global' fixed point and orbit counts on $\mathbb{T}^d$, one can consider the 'local' ones, defined by the restriction of M on a single lattice Λ_n, $n \in \mathbb{N}$. If the orbit counts of M on the lattice Λ_n are considered, the related (inverse) 'local' version of Equation (6) reads $Z_n(t) = \prod_{m\in\mathbb{N}} (1-t^m)^{c_m^{(n)}}$, where the $c_m^{(n)}$ denote the number of periodic orbits of length m on Λ_n. Despite the way it is written, Z_n is a *finite* product and defines a polynomial of degree at most n^d. Note that the degree of Z_n can be smaller than n^d (as the matrix M need not be invertible on Λ_n), but $Z_n(t)$ is always divisible by $(1-t)$, because 0 is a fixed point of every endomorphism. For further aspects of zeta functions of toral endomorphisms and their systematic calculation, see [16], [10] and references therein. Dynamical zeta functions give access to the distribution and various asymptotic properties of periodic orbits [29, 73], and also relate to topological questions; compare [34] for a systematic exposition of the latter aspect in a more general setting. Throughout this thesis, the words *periodic orbit* and *cycle* will be used interchangeably.

3 Locally invertible toral endomorphisms on the rational lattices

In this section, we investigate what determines the numbers and lengths of periodic orbits of toral endomorphisms on a rational lattice Λ_n in dependence of n.

3.1 Some reductions

By the Chinese remainder theorem [54], one has the ring (and Abelian group) isomorphism

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_s^{r_s}\mathbb{Z},$$

where $n = p_1^{r_1} \cdots p_s^{r_s}$ is the prime decomposition of n. As a consequence, modular arithmetic with respect to a given modulus n can be performed separately for the factors in the prime decomposition of n. In a similar vein, the lattices Λ_n can be decomposed according to coprime factors u, v of n, i.e. for $\gcd(u, v) = 1$, one finds $\Lambda_{uv} = \Lambda_u \oplus \Lambda_v$. Indeed, as one easily checks, every element $z \in \tilde{\Lambda}_{uv}$ can be written $z = vx + uy$ with unique $x \in \tilde{\Lambda}_u, y \in \tilde{\Lambda}_v$. This has the following consequence for periodic points of a matrix M on the lattice Λ_{uv} (or, equivalently, $\tilde{\Lambda}_{uv}$).

Fact 3.1.1. *Let $x \in \tilde{\Lambda}_u$ with minimal period ℓ and $y \in \tilde{\Lambda}_v$ with minimal period k. Then the point $vx + uy \in \tilde{\Lambda}_{uv}$ has minimal period* $\operatorname{lcm}(\ell, k)$.

Proof. This follows from the fact that an exponent j with

$$u(M^j x - x) + v(M^j y - y) \equiv 0 \mod uv,$$

must satisfy $\ell | j$ and $k | j$, and $j = \operatorname{lcm}(\ell, k)$ is the minimal integer with this property. □

Example 3.1. Consider the matrix $M = \left(\begin{smallmatrix} 2 & 3 \\ 1 & 9 \end{smallmatrix}\right)$. On Λ_7, it has six cycles of length 8; on Λ_8, it has one 3-cycle, two 6-cycles and four 12-cycles. The fixed point 0 is an element of any lattice. Consider now the lattice Λ_{56}. Note that choosing $x = 0$ or $y = 0$ in Fact 3.1.1 reproduces the cycles from the sublattices. Composing points of Λ_{56} according to their direct sum structure, the points from the 3-,6- and 12-cycle from Λ_8 together with those of the 8-cycle on Λ_7 go into $6 + 24 + 96 = 126$ cycles of length 24. Summing up all points from all periodic orbits yields $1 \cdot 1 + 1 \cdot 3 + 2 \cdot 6 + 6 \cdot 8 + 4 \cdot 12 + 126 \cdot 24 = 3136 = 56^2$, which is in agreement with $\det(M) = 15$, whence invertibility on Λ_7 and Λ_8, hence also on Λ_{56}, follows.

In general, the number of cycles on Λ_n with n composite can be calculated from those on its sublattices by the following relation.

Corollary 3.1.1. *If $\gcd(u, v) = 1$ and $c_j^{(w)}$ denotes the number of j-cycles on Λ_w, the number of j-cycles on Λ_{uv} is given by*

$$c_j^{(uv)} = \sum_{k,\ell:\operatorname{lcm}(k,\ell)=j} c_\ell^{(u)} c_k^{(v)} \gcd(\ell, k).$$

Proof. The $\ell \cdot k$ points $vx + uy \in \tilde{\Lambda}_{uv}$ such that x is in an ℓ-orbit on $\tilde{\Lambda}_u$ and y in a k-orbit on $\tilde{\Lambda}_v$ go into an $\operatorname{lcm}(\ell, k)$-orbit on $\tilde{\Lambda}_{uv}$, giving $c_\ell^{(u)} c_k^{(v)} \ell \cdot k / \operatorname{lcm}(\ell, k)$ orbits of length $\operatorname{lcm}(\ell, k)$. □

In this way, also orbit lengths show up which are not present on any of the prime power lattices that build Λ_n for a composite n.

Sometimes it is possible to consider general composite moduli n without any extra complications. In these cases, the formulation will be held general. However, whenever it is easier to work over local rings, we restrict ourselves to prime power lattices, having in mind that, in view of Fact 3.1.1 and Corollary 3.1.1, this is no essential loss of generality.

Occasionally, one is interested in the 'original' points on a rational lattice, i.e. the points which are not elements of any non-trivial sublattice.

Fact 3.1.2. *The points on a lattice $\tilde{\Lambda}_n$ which are not elements of any non-trivial sublattice are the points corresponding to d-tuples that have a component which is coprime with n. In particular, $\tilde{\Lambda}_{p^r} \setminus \tilde{\Lambda}_{p^{r-1}} = \{x \in \tilde{\Lambda}_{p^r} \mid x \not\equiv 0 \mod p\}$.* □

The local orbit counts consisting of 'original' lattice points are then related to the cumulative local orbit counts $c_m^{(n)}$ by another Möbius-transformation.

3.2 Subgroups and submodules induced by integer matrices

For an integer matrix M, let $\ker(M)$ and $\ker_n(M)$ denote the preimage of 0 within the set considered, that is

$$\ker(M) = \{x \in \mathbb{T}^d \mid Mx = 0\} \text{ and } \ker_n(M) = \{x \in \Lambda_n \mid Mx = 0\} = \ker(M) \cap \Lambda_n\,.$$

By abuse of notation, we also refer to the according preimage of the restriction of M to $\tilde{\Lambda}_n$ as $\ker_n(M)$, that is $\ker_n(M) \simeq \{\tilde{x} \in (\mathbb{Z}/n\mathbb{Z})^d \mid M\tilde{x} \equiv 0 \mod n\}$. $M(\Lambda_n)$ denotes the image of the lattice Λ_n under the endomorphism M, again, as convenient, identified with $M(\tilde{\Lambda}_n)$. Clearly, both $\ker_n(M)$ and $M(\Lambda_n)$ are submodules of Λ_n. Proposition 3.2.2 below will be useful both for counting fixed points on particular lattices in Section 3.3, as well as determining the size of the kernel of powers of M in Section 4.3. We give a proof based on the following lemma.

Lemma 3.2.1. *Let $a \in \mathbb{Z}$ and $v_p(a) = j \leq r$. Then the equation $ax \equiv 0 \mod p^r$ has p^j solutions x in $\mathbb{Z}/p^r\mathbb{Z}$. In fact, the solutions x form the subgroup $p^{r-j}\mathbb{Z}/p^r\mathbb{Z} \simeq \mathbb{Z}/p^j\mathbb{Z}$.*

Proof. Let $a = p^j\alpha$ with $p \nmid \alpha$. Then $ax = p^j\alpha x \equiv 0 \mod p^r$ if and only if $x \equiv 0 \mod p^{r-j}$, hence $x = p^{r-j}c$ with some $c \in \mathbb{Z}/p^r\mathbb{Z}$, which gives different solutions for $c \in \{0, \ldots, p^j - 1\}$. □

Proposition 3.2.2. *Equation* (4) *gives rise to the following isomorphisms.*

(i) The matrices Q and P induce isomorphisms of the Abelian groups $Q : \ker(M) \longrightarrow \ker(\mathrm{SNF}(M))$, $P : M(\mathbb{T}^d) \longrightarrow \mathrm{SNF}(M)(\mathbb{T}^d)$.

(ii) The reduction of Equation (4) *modulo some integer n admits the isomorphisms $Q : \ker_n(M) \longrightarrow \ker_n(\mathrm{SNF}(M))$, $P : M(\tilde{\Lambda}_n) \longrightarrow \mathrm{SNF}(M)(\tilde{\Lambda}_n)$ of $(\mathbb{Z}/n\mathbb{Z})$-modules. In particular, one has*

$$|\ker_n(\mathrm{SNF}(M))| = |\ker_n(M)| \text{ and } \left|\mathrm{SNF}(M)(\tilde{\Lambda}_n)\right| = \left|M(\tilde{\Lambda}_n)\right|.$$

(iii) Let $n = p^r$ be a prime power for some integer $r \geq 1$, $\mathrm{SNF}(M) = \mathrm{diag}(s_1, \ldots, s_d)$ as in Equation (4) and $t_i = \min(r, v_p(s_i))$ for $1 \leq i \leq d$. Then, one has the following isomorphisms of Abelian groups:

$$\ker_n(M) \simeq \mathbb{Z}/p^{t_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{t_\nu}\mathbb{Z} \quad \text{and} \quad M(\tilde{\Lambda}_{p^r}) \simeq \mathbb{Z}/p^{r-t_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{r-t_\nu}\mathbb{Z}.$$

Proof. As invertible matrices, P and Q have trivial kernels, so $Qx \in \ker(M)$ if and only if $x \in \ker(\mathrm{SNF}(M))$, hence $\ker(M) = Q^{-1}(\ker(\mathrm{SNF}(M)))$ and $Q^{-1} : \ker(\mathrm{SNF}(M)) \longrightarrow \ker(M)$ constitutes an isomorphism. Similarly, $y \in \mathrm{SNF}(M)(\mathbb{T}^d)$ if and only if $P^{-1}y \in M(\mathbb{T}^d)$, giving rise to the isomorphism $P^{-1} : \mathrm{SNF}(M)(\tilde{\Lambda}_n) \longrightarrow M(\tilde{\Lambda}_n)$. For any integer n, the matrix relation (4) reduces to an analogous equation over $\mathbb{Z}/n\mathbb{Z}$, whence (ii) follows. For (iii), we use the isomorphism stated in (ii). According to Lemma 3.2.1, one has

$$\begin{aligned}
\ker_{p^r}(\mathrm{SNF}(M)) &= \{(x_1, \ldots, x_d)^t \in \tilde{\Lambda}_{p^r} \mid x_1 \in p^{r-t_1}\mathbb{Z}/p^r\mathbb{Z}, \ldots, x_d \in p^{r-t_d}\mathbb{Z}/p^r\mathbb{Z}\} \\
&\simeq \mathbb{Z}/p^{t_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{t_d}\mathbb{Z} \text{ and} \\
\mathrm{SNF}(M)(\tilde{\Lambda}_{p^r}) &= \{x = (x_1, \ldots, x_d)^t \in \tilde{\Lambda}_{p^r} \mid x_1 \in p^{t_1}\mathbb{Z}/p^r\mathbb{Z}, \ldots, x_d \in p^{t_d}\mathbb{Z}/p^r\mathbb{Z}\} \\
&\simeq \mathbb{Z}/p^{r-t_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{r-t_d}\mathbb{Z}.
\end{aligned}$$

□

Remark 3.1. The fact that $\mathbb{Z}$-equivalence is a much weaker property than $\mathbb{Z}$-similarity is also illustrated by the implications for projections onto the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$. $\mathbb{Z}$-similarity induces similarity over $\mathbb{Z}/p^r\mathbb{Z}$ for all primes p and all integers r, whence the preservation of arbitrary (local) conjugacy invariants follows. For instance, also powers of locally conjugate endomorphisms share isomorphic kernels, whereas equivalence does not imply equivalence of matrix powers. Furthermore, when a matrix is nilpotent modulo p^r, it can still have entries which are $\not\equiv 0$ modulo p and thus have a unit modulo p as a first invariant factor; consider, for instance, $\left(\begin{smallmatrix} p & 1 \\ 0 & p \end{smallmatrix}\right)$, a nilpotent matrix (modulo p^k for all $k \geq 1$) whose Smith normal form is $\mathrm{diag}(1, p^2)$.

But then, its Smith normal form is clearly not nilpotent, which shows that nilpotency (modulo p^r) is another property which is not preserved under equivalence over $\mathbb{Z}$.

The SNF is multiplicative for matrices with coprime determinants, compare [65, Thm. II.15], but in the generic case, one has $\mathrm{SNF}(M^k) \neq \mathrm{SNF}(M)^k$. Hence, also the isomorphisms of Proposition 3.2.2 clearly do not extend to analogous ones for the powers of M.

Similar as in Section 3.1, the kernel submodule of Λ_{uv} for u, v coprime admits a decomposition according to the sublattices of Λ_{uv}.

Fact 3.2.1. *When* $\gcd(u, v) = 1$, *one has* $\ker_{uv}(M) = \ker_u(M) \oplus \ker_v(M)$.

3.3 Local versus global orbit counts of toral endomorphisms

As was stated in Section 2.1, a toral endomorphism is invertible on the whole torus, and thus on every rational lattice, if and only if its determinant is 1 or -1. If its determinant is non-zero, it is still invertible on some lattices Λ_n, namely for all n that are not divisible by (the finitely many) primes which divide its determinant.

Whenever the matrix $M^k - \mathbb{1}$ has a non-vanishing determinant, there are finitely many (isolated) periodic points of period k, while in the opposite case subtori of k-periodic points

exist, see the appendix of [9] for details. An important class of toral automorphisms whose fixed point counts are all finite are the *hyperbolic* ones, which have no eigenvalue on the unit circle.

Let $\mathrm{Fix}(M^k)$ denote the set of all points of period k,

$$\mathrm{Fix}(M^k) = \{x \in \mathbb{T}^d \mid M^k x = x\} = \ker(M^k - \mathbb{1}).$$

Clearly, $\bigcup_{k\geq 1} \mathrm{Fix}(M^k)$ is the set of all periodic points and

$$\bigcup_{k\geq 1} \mathrm{Fix}(M^k) \subset \bigcup_{n\geq 1} \Lambda_n,$$

with equality in the case of invertible M. Due to the subgroup structure $\Lambda_{n_1} \subset \Lambda_{n_2}$ for $n_1 | n_2$, for each period k, there is some 'maximal' lattice, containing all points of period k. Thus, it is a natural question how the points of a given period distribute to the different lattices.

The global fixed point counts a_k, $k \geq 1$, of a toral endomorphism, induced by an integer matrix M, are the numbers of $x \in \mathbb{T}^d$, that solve the equation $(M^k - \mathbb{1})x = 0 \mod 1$. One finds

$$a_k = \left|\det(M^k - \mathbb{1})\right|,$$

see, for instance, [9, 10, 29].

However, it is also possible to adopt the opposite perspective, and count periodic points modulo each prime power dividing the determinant, in order to finally combine all local fixed points into the set of global ones. The connection is then described by the following theorem, which can be seen as an example of the local-global principle.

Theorem 3.3.1. *Let* $\mathrm{diag}(s_1, \ldots, s_d) = \mathrm{SNF}(M^n - \mathbb{1})$ *be the Smith normal form of* $M^n - \mathbb{1}$ *and* $t_i \coloneqq \min(v_p(s_i), r)$ *for* $i \in \{1, \ldots, d\}$. *Then the number of periodic points with period* n *on* Λ_{p^r} *is given by*

$$a_n^{(p^r)} = \prod_{i=1}^{d} p^{t_i}.$$

Furthermore, if $\det(M^n - \mathbb{1}) \neq 0$, *for* $R = v_p(s_d)$ *the local counts* $a_n^{(p^R)}$ *stabilise, that is,* $a_n^{(p^k)} = a_n^{(p^R)}$ *for all* $k \geq R$, *and* $a_n^{(p^R)} = \prod_{i=1}^{d} p^{v_p(s_i)} = |\det(M^n - \mathbb{1})|_p^{-1}$. *Hence, in this case, the global fixed point count numbers are a product of the local ones:*

$$a_n = \prod_{p|\det(M^n - \mathbb{1})} |\det(M^n - \mathbb{1})|_p^{-1} = |\det(M^n - \mathbb{1})|.$$

Proof. Put $A = M^n - \mathbb{1}$ and recall that $\det(A) = \det(\mathrm{SNF}(A)) = \prod_{i=1}^{d} s_i$, whence $v_p(\det(A)) = v_p(\prod_{i=1}^{d} s_i) = \sum_{i=1}^{d} v_p(s_i)$ follows. The equation for $a_n^{(p^r)}$ immediately follows from Proposition 3.2.2. Further, if $v_p(s_i) < k$ for all i, one has $\left|\ker_{p^k}(A)\right| = \prod_{i=1}^{d} p^{v_p(s_i)} = p^{\sum_{i=1}^{d} v_p(s_i)} = p^{v_p(\det(A))}$, hence $a_n^{(p^k)} = \left|\ker_{p^k}(A)\right| = p^{v_p(\det(A))}$ for $k \geq R$. The formula for a_n then follows from Fact 3.2.1 and the fact that the prime decomposition of any integer m can be written as $m = \prod_{p|m} p^{v_p(m)} = \prod_{p|m} |m|_p^{-1}$. □

Corollary 3.3.2. *An upper bound for the integer* N *for which* Λ_N *contains all points of (not necessarily minimal) period* n *under* M *is* $N = a_n = |\det(M^n - \mathbb{1})|$.

Remark 3.2. Another identity for $|\det(M^n - \mathbb{1})|$ is an immediate consequence of the following well-known fact from linear algebra, which is also stated in [10],

$$\det(\mathbb{1} - A) = \sum_{k=0}^{d} (-1)^k \operatorname{tr}(\Lambda^k(A)), \tag{7}$$

where $\Lambda^k(A)$ is the induced linear mapping on the exterior power, represented by the matrix constructed from all k-minors of A. For dimension $d = 2$, if we plug in M^n for A, one obtains

$$a_n = |1 + \det(M)^n - \operatorname{tr} M^n| = |1 + \lambda_1^n \lambda_2^n - (\lambda_1^n + \lambda_2^n)|\,, \tag{8}$$

where λ_1, λ_2 are the eigenvalues of M.

Remark 3.3. Seibt [74] gives a formula for the order of $\mathrm{SL}(2,\mathbb{Z})$ matrices on the lattices Λ_{a_n} in terms of appropriately renormalised Chebyshew polynomials, evaluated at the trace of the matrix. Note that the relations given in his Observation 1.2 are in fact special cases of Equation (8). A version of Equation (8) for symplectic matrices in general dimensions is also given in [29].

Example 3.2. Consider the prominent example of *Arnold's cat map* $M_A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ whose periodic orbits were extensively studied in [38, 32]. Knowing the global fixed point counts a_n, the potential candidates for lattices containing them can be read off from the prime decomposition of a_n. For the map M_A, Equation (8) yields $a_n = |2 - \operatorname{tr}(M_A^n)| = \left|2 - (f_{2n-1} + f_{2n+1})\right|$, where f_n is the n-th Fibonacci number, compare Appendix A. The following table shows the global fixed point counts a_n of M_A for $1 \le n \le 10$, their prime decomposition, and the lattices, on which 'new' orbits of length n show up.

n	1	2	3	4	5	6	7	8	9	10
a_n	1	5	16	45	121	320	841	2205	5776	15125
factors	1	5	2^4	$3^2 \cdot 5$	11^2	$2^6 \cdot 5$	29^2	$3^2 \cdot 5 \cdot 7^2$	$2^4 \cdot 19^2$	$5^3 \cdot 11^2$
lattices	Λ_1	Λ_5	Λ_2, Λ_4	Λ_3, Λ_{15}	Λ_{11}	Λ_8, Λ_{10}, $\Lambda_{20}, \Lambda_{40}$	Λ_{29}	Λ_7, Λ_{21}, $\Lambda_{35}, \Lambda_{105}$	$\Lambda_{19}, \Lambda_{38}$, Λ_{76}	Λ_5, Λ_{25}, Λ_{275}

A systematic overview of further (partly conjectural) properties of the orbit counts of M_A and its 'squareroot', the Fibonacci matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is listed in the Appendix A. ◊

The decomposition of the global fixed point counts into their local counterparts in fact determines the group structure of $\mathrm{Fix}(M^k)$ in the case of $\det(M^k - \mathbb{1}) \neq 0$. The following proposition connects the group (i.e. $\mathbb{Z}$-module) structure of $\mathrm{Fix}(M^k)$ with the local fixed point counts. Thus, it reformulates Proposition 3 from [16] for general dimensions from the point of view adopted here.

Proposition 3.3.3. *Let M be an integer matrix with $\det(M^k - \mathbb{1}) \neq 0$. The structure of the finite Abelian group $\mathrm{Fix}(M^k)$ is completely determined by the set of all local fixed point counts $a_k^{(n)}$.*

Proof. According to Fact 3.2.1, one has $\ker_u(M) \oplus \ker_v(M)$ for integers u, v with $\gcd(u, v) = 1$, hence it suffices to consider prime power lattices. Consider the Smith normal form $\mathrm{SNF}(M^k - \mathbb{1}) = \mathrm{diag}(s_1, \ldots, s_d)$ and fix a prime p.

According to Proposition 3.2.2, one has the isomorphism of Abelian groups $\mathrm{Fix}(M^k) = \ker(M^k - \mathbb{1}) \simeq \ker(\mathrm{SNF}(M^k - \mathbb{1}))$, and $\mathrm{Fix}_n(M^k) \simeq \ker_n(\mathrm{SNF}(M^k - \mathbb{1}))$ for all integers $n \geq 1$. For $n = p$, $\mathrm{Fix}_p(M^k) \simeq \bigoplus_{i=1}^{j} \mathbb{Z}/p\mathbb{Z}$, where j is the number of diagonal elements in $\mathrm{diag}(s_1, \ldots, s_d)$ which is divisible by p. Since $j = v_p(\left|\mathrm{Fix}_p(M^k)\right|) = v_p(a_k^{(p)})$, the group structure of $\mathrm{Fix}_p(M^k)$ is determined by $a_k^{(p)}$.

Assume the group structure of $\mathrm{Fix}_{p^r}(M^k)$ is known to be $\mathbb{Z}/p^{k_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{k_\nu}\mathbb{Z}$ for some $1 \leq \nu \leq d$ and $k_1 \leq k_2 \leq \ldots \leq k_\nu$, such that $\prod_{1 \leq i \leq \nu} p^{k_i} = a_k^{(p^r)}$. Then the number of summands in the decomposition of $\mathrm{Fix}_{p^{r+1}}(M)$ that 'grows' from $\mathbb{Z}/p^r\mathbb{Z}$ to $\mathbb{Z}/p^{r+1}\mathbb{Z}$ is given by the quotient $a_k^{(p^{r+1})}/a_k^{(p^r)}$. Note that only summands of type $\mathbb{Z}/p^r\mathbb{Z}$ in the decomposition of $\mathrm{Fix}_{p^r}(M^k)$ can be replaced by those of type $\mathbb{Z}/p^{r+1}\mathbb{Z}$ in the decomposition of $\mathrm{Fix}_{p^{r+1}}(M^k)$. Hence, the structure of $\mathrm{Fix}_{p^{r+1}}(M)$ is completely determined by its order; this process can be continued inductively for growing K until $\mathrm{Fix}_K(M^k) = \mathrm{Fix}(M^k)$ and the claim follows. □

In view of Corollary 3.3.2, in the situation of Proposition 3.3.3, the group structure of $\mathrm{Fix}(M^k)$ is in fact determined by finitely many numbers $a_m^{(n)}$.

Remark 3.4. Proposition 3.2.2 (iii) can in fact be seen as a special case of the existence of finite free presentations for finitely generated modules over some principal ideal domain. In our setting, this means there is a short exact sequence

$$0 \longrightarrow \mathbb{Z}^d \longrightarrow \mathbb{Z}^d \longrightarrow \mathcal{M} \longrightarrow 0,$$

where $\mathcal{M}$ is one of the submodules of Λ_{p^r} under consideration. The map from $\mathbb{Z}^d \to \mathcal{M}$ maps each element of $\mathbb{Z}^d$ to a relation among the generators of $\mathcal{M}$; the Smith normal form of the map $\mathbb{Z}^d \to \mathbb{Z}^d$ essentially determines the direct summands in the module decomposition of $\mathcal{M}$; see [1, Ch. 5] for details.

At the end of this section, let us look at an example where the fixed point counts are not finite. We consider the parabolic torus automorphism which also shows up as the limiting case of vanishing parameter values of the Casati-Prosen map studied in Section 6.

Example 3.3. Consider the matrix $M_P = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Its k-th power is $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$, whence we have $\mathrm{SNF}(M_P^k - \mathbb{1}) = \left(\begin{smallmatrix} k & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Clearly, it admits a one-dimensional subtorus of fixed points, so in particular, on each lattice Λ_n, it has n fixed points. For the general local fixed point counts on the prime power lattice Λ_{p^r}, one finds $a_k^{(p^r)} = p^{\min(r, v_p(k))} \cdot p^r$. For $p \not| k$, $a_k^{(p^r)}$ just recounts the fixed points; for $k = p^i$, one obtains (by subtraction of the points also fixed under $i-1$ iterations, and dividing by p^i), the local orbit counts $c_{p^i}^{(p^r)} = p^{r-1}(p-1)$. This gives the local version of the (inverse) zeta function

$$Z_{p^r}(t) = (1-t)^{p^r} \prod_{i=1}^{r} (1 - t^{p^i})^{p^{r-1}(p-1)} = Z_{p^{r-1}}(t)^p (1 - t^{p^r})^{p^{r-1}(p-1)}.$$

◊

3.4 Matrix order on lattices and periods of points

Assume that M is invertible on Λ_n (hence also on $\tilde{\Lambda}_n$). Then, its order is given by

$$\mathrm{ord}(M, n) := \gcd\{m \in \mathbb{N}_0 \mid M^m \equiv \mathbb{1} \mod n\}. \tag{9}$$

Clearly, $\mathrm{ord}(M,1)=1$ in this setting. When M is not invertible on Λ_n, the definition results in $\mathrm{ord}(M,n)=0$; otherwise, $\mathrm{ord}(M,n)$ is the smallest $m\in\mathbb{N}$ with $M^m=\mathbb{1} \bmod n$.

Let $M\in\mathrm{GL}(d,\mathbb{Z})$ be arbitrary, but fixed. To determine $\mathrm{ord}(M,n)$ for all $n\geq 2$, it suffices, once more, to do so for n an arbitrary prime power, since the Chinese remainder theorem [42] gives

$$\mathrm{ord}(M,n) \;=\; \mathrm{lcm}\big(\mathrm{ord}(M,p_1^{r_1}),\ldots,\mathrm{ord}(M,p_\ell^{r_\ell})\big) \tag{10}$$

when $n=p_1^{r_1}\cdots p_\ell^{r_\ell}$ is the prime decomposition of n. It is clear that $\mathrm{ord}(M,p^r)\,|\,\mathrm{ord}(M,p^{r+1})$ for all $r\in\mathbb{N}$, see also [22, Lemma 5.2].

Let us now assume that $M\in\mathrm{Mat}(d,\mathbb{Z})$ is *not* of finite order, meaning that $M^k\neq\mathbb{1}$ for all $k\in\mathbb{N}$, which excludes the finite order elements of $\mathrm{GL}(d,\mathbb{Z})$. If p is a prime, we then obtain the unique representation

$$M^{\mathrm{ord}(M,p)} \;=\; \mathbb{1}+p^sB \tag{11}$$

with $s\in\mathbb{N}$ and an integer matrix $B\not\equiv 0 \bmod p$. Starting from this representation, an application of the binomial theorem to powers of $\mathbb{1}+p^sB$, in conjunction with the properties of the binomial coefficients mod p, gives the following well-known result.

Proposition 3.4.1. *Let $M\in\mathrm{Mat}(d,\mathbb{Z})$ be a matrix that is not of finite order. Fix a prime p that does not divide $\det(M)$, and let s be defined as in Equation (11).*

When p is odd or when $s\geq 2$, one has $\mathrm{ord}(M,p^i)=\mathrm{ord}(M,p)$ for $1\leq i\leq s$, together with $\mathrm{ord}(M,p^{s+i})=p^i\,\mathrm{ord}(M,p^s)$ for all $i\in\mathbb{N}$.

In the remaining case, $p=2$ and $s=1$, one either has $\mathrm{ord}(M,2^r)=2^{r-1}\,\mathrm{ord}(M,2)$ for all $r\in\mathbb{N}$, or there is an integer $t\geq 2$ so that $\mathrm{ord}(M,2^i)=2\,\mathrm{ord}(M,2)$ for $2\leq i\leq t$ together with $\mathrm{ord}(M,2^{t+i})=2^i\,\mathrm{ord}(M,4)$ for all $i\in\mathbb{N}$. □

In what follows, we will refer to the structure described in Proposition 3.4.1 as the *plateau phenomenon*. Such a plateau can be absent (p odd with $s=1$, or the first case for $p=2$), it can be at the beginning (p odd with $s\geq 2$), or it can occur after one step ($p=2$ when $t\geq 2$ exists as described), but it cannot occur later on.

Example 3.4. Consider the matrix $\left(\begin{smallmatrix}2&1\\1&0\end{smallmatrix}\right)$. One has $\mathrm{ord}(M,13)=\mathrm{ord}(M,13^2)=28$ and $\mathrm{ord}(M,13^r)=13^{r-2}\cdot 28$. An example that shows the plateau phenomenon particular to $p=2$ is given by $\left(\begin{smallmatrix}3&3\\3&6\end{smallmatrix}\right)$, where the sequence of orders for powers 2^r and $r\in\{1,\ldots,5\}$ is $3,6,6,6,12$ and then follows the regular growth. ♢

Proposition 3.4.1 is a reformulation of [22, Thms. 5.3 and 5.4], which are originally stated for $M\in\mathrm{Mat}(2,\mathbb{Z}/p^r\mathbb{Z})^\times$ for some prime power p^r. As one can easily check, the proofs do not depend on the dimension. In particular, Proposition 3.4.1 contains the order growth of integers modulo prime powers which is treated e.g. in [48, Appendix A], as a special case. Similar versions or special cases were also given in [20] and [74] (with focus on $\mathrm{SL}(d,\mathbb{Z})$-matrices), in [66] (for the order of algebraic integers), in [81] (for the Fibonacci sequence), in [23] (for linear quadratic recursions) and in [33] and [83] (for general linear recursions). In [20], it is shown that an upper bound for $\mathrm{SL}(2,\mathbb{Z})$-matrices on $\mathrm{ord}(M,n)$ is given by $3n$, hence linear in n. Let us also mention that, based on the generalised Riemann hypothesis, Kurlberg has determined a lower bound on the order of unimodular matrices mod N for a density 1 subset of integers N in [51].

The matrix order clearly defines the upper bound of all period lengths on a lattice. For a given point, a sufficient criterion to have the maximal period length is stated in the following

proposition. A special case, formulated for recursive sequences, can be found in [81] and is revisited in Lemma 3.6.3.

Proposition 3.4.2. *Let $M \in \mathrm{GL}(d, \mathbb{Z}/m\mathbb{Z})$, $v \in (\mathbb{Z}/m\mathbb{Z})^d$ and assume the determinant of the matrix with column-wise definition $A \coloneqq (v, Mv, \ldots, M^{d-1}v)$ is coprime with m. Then, the period of v on Λ_m equals the matrix order modulo m.*

Proof. Set $R \coloneqq \mathbb{Z}/m\mathbb{Z}$. The fact that $\gcd(\det(A), m) = 1$ means the module endomorphism of the free R-module R^d with canonical basis $e_1, \ldots, e_d$, defined by $\phi(e_i) = M^{i-1}v$ is in fact an isomorphism. Consequently, there is the inverse isomorphism ϕ^{-1} such that one has, for every $y \in R^d$, a decomposition $y = \sum_{i=1}^{d} y_i e_i = \sum_{i=1}^{d} y_i \phi^{-1}(M^{i-1}v)$ with certain unique $y_i \in R$, hence $\phi(y) = \sum_{i=1}^{d} y_i M^{i-1} v$. Since ϕ is a bijection, for every $z \in R^d$, there is some unique y with $\phi(y) = z$ and every element of R^d has a unique representation as a linear combination of the $v, Mv, \ldots, M^{d-1}v$, whence it is a basis of R^d. Let k denote the period of v on Λ_m, hence k is the smallest integer with $(M^k - \mathbb{1})v \equiv 0$. But this implies, for $0 \leq j \leq d-1$, $M^j(M^k - \mathbb{1})v = (M^k - \mathbb{1})M^j v \equiv 0$ and therefore, by linearity, $M^k x = x$ for all $x \in \Lambda_m$, thus $k = \mathrm{ord}(M, m)$. □

Remark 3.5. Note that Proposition 3.4.2 is only a sufficient criterion for a lattice point $(v_0, \ldots, v_{d-1})^t$ to have maximal period. Consider, for instance, the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -6 & 5 \end{smallmatrix}\right)$ on Λ_7, where its order is 6. The point $(1, 3)^t$ has maximal period 6 but the determinant is $\left|\begin{smallmatrix} 1 & 3 \\ 3 & 2 \end{smallmatrix}\right| = -7$.

3.5 Powers of integer matrices

Consider a matrix $M \in \mathrm{Mat}(d, \mathbb{Z})$ with $d \geq 2$ and characteristic polynomial $P_M(x) = \det(x\mathbb{1} - M)$, which (following [83]) we write as

$$P_M(x) \;=\; x^d - c_1 x^{d-1} - c_2 x^{d-2} - \ldots - c_{d-1} x - c_d, \tag{12}$$

so that $c_d = (-1)^{d+1} \det(M)$. Let us define a recursion by $u_0 = u_1 = \ldots = u_{d-2} = 0$ and $u_{d-1} = 1$ together with

$$u_m \;=\; \sum_{i=1}^{d} c_i u_{m-i} \;=\; c_1 u_{m-1} + c_2 u_{m-2} + \ldots + c_d u_{m-d} \tag{13}$$

for $m \geq d$. This results in an integer sequence $(u_m)_{m \geq 0}$. Moreover, when $c_d \neq 0$, we also define

$$u_m \;=\; c_d^{-1}(u_{m+d} - c_1 u_{m+d-1} - \ldots - c_{d-1} u_{m+1})$$

for $m \leq -1$. In particular, since $d \geq 2$, one always has $u_{-1} = 1/c_d$ and $u_{-2} = -c_{d-1}/c_d^2$, while the explicit form of u_m with $m < -2$ depends on d. Note that the coefficients with negative index are rational numbers in general, unless $|c_d| = 1$.

The Cayley-Hamilton theorem together with (13) can be used to write down an explicit expansion of powers of the matrix M in terms of M^k with $0 \leq k \leq d-1$,

$$M^m \;=\; \sum_{\ell=0}^{d-1} \gamma_\ell^{(m)} M^\ell, \tag{14}$$

where the coefficients satisfy $\gamma_\ell^{(m)} = \delta_{m,\ell}$ (for $0 \le \ell, m \le d-1$) together with the recursion

$$\gamma_\ell^{(n+1)} = c_{d-\ell}\,\gamma_{d-1}^{(n)} + \gamma_{\ell-1}^{(n)}, \tag{15}$$

for $n \ge d-1$ and $0 \le \ell \le d-1$, where $\gamma_{-1}^{(n)} := 0$. In particular, $\gamma_\ell^{(d)} = c_{d-\ell}$. The coefficients are explicitly given as

$$\gamma_\ell^{(m)} \;=\; \sum_{i=0}^{\ell} c_{d-i}\,u_{m-\ell-1+i} \;=\; u_{m+d-\ell-1} \;-\; \sum_{i=1}^{d-\ell-1} c_{d-\ell-i}\,u_{m-1+i}, \tag{16}$$

where $m \ge d$ and the second expression follows from the first by (13). Formulas (14) and (16) can be proved by induction from $M^d = c_1 M^{d-1} + c_2 M^{d-2} + \ldots c_{d-1}M + c_d\mathbb{1}$. Equation (14) holds for all $m \ge 0$ in this formulation.

When $\det(M) \neq 0$, the representation (16) also holds for $m < d$, as follows from checking the cases $0 \le m < d$ together with a separate induction argument for $m < 0$. In particular, one then has

$$\begin{aligned} M^{-1} = {} & c_d u_{-2}\mathbb{1} + (c_{d-1}u_{-2} + c_d u_{-3})M + (c_{d-2}u_{-2} + c_{d-1}u_{-3} + c_d u_{-4})M^2 \\ & + \ldots + (c_2 u_{-2} + c_3 u_{-3} + \ldots + c_d u_{-d})M^{d-2} + u_{-1}M^{d-1}, \end{aligned}$$

which is again an integer matrix when $|c_d| = 1$.

By Dirichlet's pigeon hole principle, it is clear that the reduction of a sequence $(u_m)_{m\ge 0}$ modulo some integer n must be periodic from a certain index on. If c_d is coprime with n, the recursion (13) can be reversed and the sequence $(u_m)_{m\ge 0}$ is purely periodic modulo n, i.e. it returns to its initial value. Assume that the period mod n of the sequence $(u_m)_{m\ge 0}$ is k, i.e. $u_k \equiv 1$ and $u_{k-1} \equiv \ldots \equiv u_{k-d+1} \equiv 0$. Then, obviously, $\gamma_{d-1}^{(k+d-1)} \equiv u_k \equiv 1$ and $\gamma_\ell^{(k+d-1)} \equiv 0 \mod n$ for $0 \le \ell < d-1$, hence $M^{k+d-1} \equiv M^{d-1} \mod n$. M is invertible mod n if and only if c_d is a unit in $\mathbb{Z}/n\mathbb{Z}$. In that case, $M^k \equiv \mathbb{1} \mod n$. Thus, we can give the following summary on the matrix order modulo n.

Corollary 3.5.1. *The order modulo n of a matrix $M \in \mathrm{Mat}(d,\mathbb{Z})$ with characteristic polynomial $P_M(x)$ and $\gcd(\det(M), n) = 1$ divides the period modulo n of the recursive sequence associated with $P_M(x)$.*

The next section shows that, in many cases, the theory of linear recursions provides insight beyond the mere matrix orders, which is helpful in the study of period lengths on certain lattices.

3.6 Results from the theory of linear recursions

Let C_f denote the companion matrix of the polynomial

$$f(x) = x^d - c_1 x^{d-1} - c_2 x^{d-2} - \ldots - c_{d-1}x - c_d,$$

such that

$$C_f\,u = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_d & c_{d-1} & c_{d-2} & \ldots & c_1 \end{pmatrix} \cdot \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{d-1} \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_d \end{pmatrix}$$

'implements' the computation of the next term of the recursive sequence defined by f with the initial values $u_0, \ldots, u_{d-1}$. Consequently, for companion matrices, the problem of finding the period of a point $u = (u_0, \ldots, u_{d-1})^t$ on the lattice Λ_n is equivalent with finding the period of a sequence modulo n with initial values $u_0, \ldots, u_{d-1}$ satisfying the linear recursion induced by f; the number of periodic orbits then corresponds to the number of initial values giving rise to a sequence of that period. This motivates the attempt to determine the local similarity classes of companion matrices (or direct sums of companion matrices) in order to use them as normal forms where possible, a problem which is addressed in Section 3.8.

Particularly well-developed is the theory of linear recursions over finite fields, see e.g. [56, 87]; an account of general linear recursions modulo an integer m is given in [83] and to some extent also in [33].

Applying the theory developed in [83] and [84], we use polynomial arithmetics in $\mathbb{Z}/m\mathbb{Z}[x]$ to study the dynamics of companion matrices on the rational lattices. We adopt the notation of [83] and work with the double modulus modd $m, F(x)$, where $F(x) \in \mathbb{Z}/m\mathbb{Z}[x]$. For two polynomials $f(x), g(x)$, one has $f(x) \equiv g(x) \mod m, F(x)$ if $f(x) - g(x) \equiv F(x)H(x) \mod m$ for some $H(x) \in \mathbb{Z}/m\mathbb{Z}[x]$. Alternatively, one can work with the finite ring $\mathbb{Z}/m\mathbb{Z}[x]/\langle F(x)\rangle$, where $\langle F(x)\rangle$ is the ideal generated by $F(x)$ in the ring $\mathbb{Z}/m\mathbb{Z}[x]$.

Define a polynomial associated with a sequence $(u_n)_{n\geq 0}$ by

$$U(x)^{(n)} = u_n x^{d-1} + (u_{n+1} - c_1 u_n)x^{d-2} + \ldots + (u_{n+d-1} - c_1 u_{n+d-2} - \ldots - c_{d-1}u_n)x^0 \quad (17)$$

The polynomial $U(x) = U^{(0)}(x)$ is called the *generator* of $(u_n)_{n\geq 0}$ in [83]. Note that, with the initial values $u_0 = \ldots = u_{d-2} = 0, u_{d-1} = 1$ from the last paragraph, one has $U(M) = \mathbb{1}$ and $U^{(n)}(M) = M^n$. However, in the following, also sequences with arbitrary initial values are considered.

Theorem 3.6.1. ([83], 'Fundamental Theorem on purely periodic sequences') *Let $U(x)$ denote the generator of the sequence $u = (u_n)_{n\geq 0}$, satisfying the recursive relation defined by* (13) *and $F(X)$ the polynomial in* (12)*. Then, u is purely periodic modulo m with period n if and only if*

$$(x^n - 1)U(x) \equiv 0 \mod m, F(X). \qquad \square$$

Corollary 3.6.2. *The order of a companion matrix C_F modulo m is the least integer n, such that $x^n \equiv 1 \mod F(x), m$, or, equivalently, such that $(x^n - 1) \in F(x)\mathbb{Z}/m\mathbb{Z}[x]$. The point $(0, \ldots, 0, 1)^t$ always has maximal period* $\operatorname{ord}(M, m)$. $\square$

Lemma 3.6.3. ([83, Corollary and Lemma after Thms. 3.1 and 6.1, respectively]) *A sufficient criterion for a sequence u to have the maximal period is that the determinant*

$$\Delta(u) = \begin{vmatrix} u_0 & u_1 & \ldots & u_{k-1} \\ u_1 & u_2 & \ldots & u_k \\ \vdots & \vdots & & \vdots \\ u_{k-1} & u_k & \ldots & u_{2k-1} \end{vmatrix}$$

is coprime with m. Furthermore, the resultant of $U(x)$ and $F(x)$ equals $(-1)^k\Delta(u)$. $\square$

As described in [83], there is an isomorphism between the group of sequences satisfying the given recurrence relation and the polynomials reduced modd $m, F(x)$. Via this identification,

it is possible to turn the question of periodic orbits on a given lattice into a purely algebraic one that revolves around the unit group of certain rings of reduced polynomials. We reformulate and derive a known fact in Theorem 3.6.7 below as a consequence of this identification. A similar approach was also pursued in [80] in order to determine the associated graphs of endomorphisms over finite fields. Related questions for endomorphisms over general modules were studied in [41], using similar methods.

In order to simplify matters, we restrict ourselves to prime powers $m = p^r$ for some positive integer r from now on, and use the abbreviation $R := \mathbb{Z}/p^r\mathbb{Z}$. Consider the elements in the finite residue class ring $R[x]/\langle F(X)\rangle$, where $\langle F(X)\rangle = F(x)R[x]$ is the ideal generated by $F(x)$ in the polynomial ring $R[x]$. Each sequence $(u_n)_{n\geq 0}$ which satisfies the recursive relation defined by $F(x)$ is completely determined by its d initial values. More precisely, let $\Phi : R^d \longrightarrow R[x]/\langle F(x)\rangle$ denote the map which assigns to an element $(u_0, \ldots, u_{d-1})$ the residue class of its generator in $R[x]/\langle F(x)\rangle$. Under this identification, the map realised by the companion matrix $C_F : (\mathbb{Z}/p^r\mathbb{Z})^d \longrightarrow (\mathbb{Z}/p^r\mathbb{Z})^d$ has a counterpart $\mathcal{X}$ in the ring $R[x]/\langle F(x)\rangle$, defined by $\mathcal{X} : U(x) \mapsto xU(x)$. This is summarised in the following

Lemma 3.6.4. *If $U(x)$ is the generator of the sequence u with initial values $u_0, \ldots, u_{d-1}$, the residue class of $xU(x)$ in the ring $R[x]/\langle F(x)\rangle$ corresponds to the sequence u' with initial values $u_1, \ldots, u_d$. In particular, in accordance with Theorem* 3.6.1*, the period of the associated point $(u_0, \ldots, u_{d-1})^t$ is the least integer n such that $x^nU(x) - U(x) \in \langle F(x)\rangle$.*

Proof. Calculating $xU(x)$ shows that its residue class is

$$u_1x^{d-1} + (u_2 - c_1u_1)x^{d-2} + (u_3 - c_1u_2 - c_2u_1)x^{d-3} + \ldots + (u_{d-1} - c_1u_{d-2} - \ldots - c_{d-2}u_1)x + c_du_0,$$

where $c_du_0 = u_d - c_1u_{d-2} - c_2u_{d-3} - \ldots - c_{d-1}u_1$. But this is the generator of the sequence shifted by one, hence of $C_F(u_0, \ldots, u_{d-1})^t$. The rest is clear from the paragraph above. □

In other words, we get the following commutative diagram.

$$\begin{array}{ccc} R^d & \xrightarrow{C_F} & R^d \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} \\ R[X]/\langle F(x)\rangle & \xrightarrow{\mathcal{X}} & R[X]/\langle F(x)\rangle \end{array}$$

Remark 3.6. Strictly speaking, one would have to distinguish between the polynomials in $\mathbb{Z}[x]$, their reductions to $R[x]$, and finally their residue classes in $R[x]/\langle F(x)\rangle$. However, to simplify the notation, we sometimes refer to three different objects by the same symbol.

Assume $G(x)$ is a unit in the ring $R[x]/\langle F(x)\rangle$. Then $(x^n-1)G(x) \equiv 0$ implies $(x^n-1) \equiv 0$, hence the point associated with $G(x)$ has maximal period.

Recall that a Galois ring is a Galois extension of the ring $R_r = \mathbb{Z}/p^r\mathbb{Z}$. The Galois extension of the ring R_r of degree d is denoted by $\mathrm{GR}(p^r, d)$. If $F(X)$ is a monic polynomial of degree d whose reduction modulo p is irreducible, one has $\mathrm{GR}(p^r, d) \simeq R_r[x]/\langle F(x)\rangle \simeq \mathbb{Z}[x]/\langle p^r, F(x)\rangle$; compare [59, Chapters XV and XVI].

One has the following theorem about the unit group of a Galois ring.

Theorem 3.6.5. [59, XVI.9] *Let $\mathfrak{R} = \mathrm{GR}(p^r, d)$. Then the unit group $\mathfrak{R}^\times$ has the following direct product structure,*

$$\mathfrak{R}^\times = G_1 \times G_2,$$

where G_1 is a cyclic group of order $p^d - 1$ and G_2 is a group of order $p^{(r-1)d}$, which, again, is a product of cyclic groups (the precise factors depending on p and r). In particular, one has $|\mathfrak{R}^\times| = |G_1|\,|G_2| = p^{rd} - p^{(r-1)d}$. □

The last theorem gives some insight into the structure of the ring $R_r[x]/\langle F(x)\rangle$. It contains p^{rd} elements, represented by polynomials of degree $< d$.

Corollary 3.6.6. *Assume $F(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$. If the point $v = (g_0, \ldots, g_{d-1})^t$ associated with $G(x)$ does not have maximal period, $G(x)$ is congruent 0 modulo p. Hence v is an element of the sublattice $\Lambda_{p^{r-1}} \subset \Lambda_{p^r}$.*

Proof. Each of the $(p^r - \phi(p^r)) = p^{(r-1)d}$ elements of $\mathfrak{R}$ which are represented by a polynomial congruent 0 modulo p is a zero divisor in $\mathfrak{R}$, hence clearly not a unit. Due to the order of the unit group, all representatives not congruent 0 modulo p must be units, thus correspond to sequences with maximal period. If the generator $G(x)$ of a sequence with the initial value vector v satisfies $G(x) \equiv 0 \mod p$, also, for the associated initial vector v, one finds $v \equiv 0 \mod p$, which, according to Fact 3.1.2, means $v \in \tilde{\Lambda}_{p^{r-1}}$. □

Theorem 3.6.5 and Corollary 3.6.6 imply the following result.

Theorem 3.6.7. *Let $F(x)$ be a polynomial whose reduction modulo p is irreducible and C_F the associated companion matrix. Then, all points on $\Lambda_{p^r} \setminus \Lambda_{p^{r-1}}$ have the maximal period $\mathrm{ord}(C_F, p^r)$ for each integer r.* □

Remark 3.7. Over finite fields, it is well-known that an irreducible polynomial f of degree d has d distinct roots in its splitting field. All of them share the same order, namely the least integer n such that $f(x)|(x^n - 1)$, compare [56, p. 75] and Section 5. This integer n, also referred to as $\mathrm{ord}(f, p)$, is bounded by the order $p^d - 1$ of the cyclic group generated by any of the roots of f. This maximal order is attained if and only if $f(x)$ is a primitive polynomial in which case the roots of f are primitive $(p^d - 1)$-roots of unity, see [87, Thm. 7] and Proposition 5.4.1.

Remark 3.8. Over finite fields, the reasoning can be extended to powers of irreducible polynomials. In conjunction with the normal forms discussed in Section 3.8 below, this provides a complete picture of period lengths on the prime lattices in dependence of polynomial orders, see [87]. In particular, [87, Thm. 4] states the following periods of recursions induced by the polynomial f^t, f irreducible.

period	1	$\mathrm{ord}(f,p)$	$p^j \,\mathrm{ord}(f,p)$	$p^{k+1}\,\mathrm{ord}(f,p)$
multiplicity	1	$p^d - 1$	$p^{dp^j} - p^{dp^{j-1}}$	$p^{dt} - p^{dp^k}$

where k is chosen such that $p^k < t \le p^{k+1}$ and $1 \le j \le k$ and $\mathrm{ord}(f, p)$ as in Remark 3.7.

3.7 Results for $d = 2$

Let us look at matrices from $\mathrm{Mat}(2, \mathbb{Z})$ more closely, and derive an important result on the relation between the matrix order and the period of the associated recursive sequence by elementary means. Consider $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, set $D := \det(M)$, $T := \mathrm{tr}(M)$, and define the matrix gcd as

$$\mathrm{mgcd}(M) := \gcd(b, c, d - a), \tag{18}$$

which is another invariant under $\mathrm{GL}(2,\mathbb{Z})$ conjugation [16, Lemma 2]. Formula (14) simplifies to

$$M^m \,=\, u_m M - D u_{m-1}\mathbb{1}, \tag{19}$$

where now $u_0 = 0$, $u_1 = 1$ and $u_{m+1} = Tu_m - Du_{m-1}$ for $m \in \mathbb{N}$; see [16, Sec. 2.3] for details. Let $n \in \mathbb{N}$ and assume $\gcd(n, D) = 1$. This allows to introduce

$$\kappa(n) \,:=\, \text{period of } (u_m)_{m\geq 0} \bmod n$$

which is well-defined, as the sequence mod n is then indeed purely periodic, see also the end of Section 3.5. Since D is a unit in $\mathbb{Z}/n\mathbb{Z}$, $(u_m)_{m\geq 0} \bmod n$ must thus be periodic, with $\kappa(n)$ being the smallest positive integer k such that $u_k \equiv 0$ and $u_{k+1} \equiv 1 \bmod n$.

One can now relate $\kappa(n)$ and $\mathrm{ord}(M, n)$ as follows, which provides an efficient way to calculate $\mathrm{ord}(M, n)$.

Proposition 3.7.1. *Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ be fixed and let $(u_m)_{m\geq 0}$ be the corresponding recursive sequence from (13). If $n \geq 2$ is an integer with $\gcd(n, D) = 1$, $\mathrm{ord}(M, n)$ divides $\kappa(n)$. Moreover, with $N_n := n/\gcd\big(n, \mathrm{mgcd}(M)\big)$, one has*

$$\mathrm{ord}(M, n) \,=\, \kappa(N_n)$$

whenever $N_n > 1$. In particular, this gives $\mathrm{ord}(M, n) = \kappa(n)$ whenever n and $\mathrm{mgcd}(M)$ are coprime.

In the remaining case, $N_n = 1$, the matrix satisfies $M \equiv \alpha\mathbb{1} \bmod n$ with $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$, so that $\mathrm{ord}(M, n)$ is the order of α modulo n.

Proof. If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the iteration formula (19) implies that $M^m \equiv \mathbb{1} \bmod n$ if and only if

$$u_m a - D u_{m-1} \equiv 1\,, \quad u_m b \equiv 0\,, \quad u_m c \equiv 0\,, \quad \text{and} \quad u_m d - D u_{m-1} \equiv 1 \mod n,$$

so that also $u_m(a - d) \equiv 0 \bmod n$. Consequently, n divides $u_m b$, $u_m c$ and $u_m(a - d)$. This implies that u_m is divisible by $\frac{n}{\gcd(n,b)}$, $\frac{n}{\gcd(n,c)}$ and $\frac{n}{\gcd(n,a-d)}$, hence also by the least common multiple of these three numbers, which is the integer

$$N_n \,=\, \frac{n}{\gcd\big(n, \gcd(b, c, a - d)\big)} \,=\, \frac{n}{\gcd\big(n, \mathrm{mgcd}(M)\big)}.$$

Since $N_n | n$, we now also have $u_m a - D u_{m-1} \equiv 1 \bmod N_n$. When $u_m \equiv 0 \bmod N_n$, the recursion now gives $u_{m+1} \equiv Tu_m - Du_{m-1} \equiv -Du_{m-1} \equiv 1 - u_n a \equiv 1 \bmod N_n$. Consequently, $M^m \equiv \mathbb{1} \bmod n$ is equivalent to $u_m \equiv 0$ and $u_{m+1} \equiv 1 \bmod N_n$. So, for $N_n > 1$, one has

$$\mathrm{ord}(M, n) \,=\, \kappa(N_n),$$

which is the period of the sequence $(u_m)_{m\geq 0}$ modulo N_n. Since $\kappa(N_n)$ clearly divides $\kappa(n)$, one finds $\mathrm{ord}(M, n) \,|\, \kappa(n)$.

Finally, when $N_n = 1$, one has $n \,|\, \mathrm{mgcd}(M)$, which implies $M \equiv \alpha\mathbb{1} \bmod n$, where we have $\alpha^2 \in (\mathbb{Z}/n\mathbb{Z})^\times$ due to $\gcd(n, D) = 1$. Since this also implies $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$, the last claim is clear. □

Remark 3.9. Instead of the characteristic polynomial P_M, any other monic polynomial that annihilates M can be employed to derive a recursive sequence whose period is a multiple of the matrix order modulo n. For $n = p$ a prime, the unique minimal polynomial Q_M of M suggests itself to be chosen. For $d = 2$, Q_M has smaller degree than P_M precisely when $M = \alpha\mathbb{1}$, whence $\mathrm{mgcd}(M) = 0$ and $Q_M(x) = x - \alpha$. Consequently, $\mathrm{ord}(M, p)$ is then always equal to the order of α modulo p.

3.7.1 Generalised Fibonacci sequences

The original Fibonacci sequence is well-studied and many arithmetic properties are classic, cf. [40]. Among the first articles in which the Fibonacci sequences modulo n for some integer n were studied systematically and in terms of their exact representation was [81] by Wall. In conjunction with the analysis of periods of Arnold's cat map, the reasoning in [32] and [38] was also largely based on properties of the reduced Fibonacci sequences.

As is well-known for the original Fibonacci sequence $(f_n)_{n\geq 0}$ with $f_0 = 0, f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$, the entries of the n-th power of the Fibonacci matrix $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ are the terms of the Fibonacci sequence: $A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$. In fact, this is the two-dimensional version $u_{n+1} = Tu_n - Du_{n-1}$ of Equation (13) with $D = -1$ and $T = 1$ and $u_n = f_n$ for all integers $n \geq 0$. In this case, the periodic behaviour of the matrix modulo n is reflected by the behaviour of the Fibonacci sequence modulo n.

The Fibonacci matrix is conjugate over $\mathbb{Z}$ with the companion matrix of its characteristic polynomial, and, using the associated linear recurrence sequence u_n, the n-th power of a general (2×2)-companion matrix $C = \left(\begin{smallmatrix} 0 & 1 \\ -D & T \end{smallmatrix}\right)$ can be written

$$C^m = u_m C - D u_{m-1} \mathbb{1} = \begin{pmatrix} -Du_{m-1} & -Du_m \\ u_m & Tu_m - Du_{m-1} \end{pmatrix}. \tag{20}$$

Linear recurrences can be solved in terms of the roots of the defining polynomials, so for quadratic polynomials it is possible to explicitly write down the sequence elements in terms of the roots $\lambda_{1,2} = \frac{T \pm \sqrt{T^2 - 4D}}{2}$. The n-th term u_n is then given by $u_n = \alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n$ with coefficients $\alpha_{1,2}$ to be determined from the initial values. For the Fibonacci sequence, this is also known as the formula of Binet. A treatment of quadratic recurrences and a generalisation of the investigations of [81] is given in [23]. For the special initial conditions $u_0 = 0, u_1 = 1$ (generalised Fibonacci sequence) and $v_0 = 2, v_1 = T$ (generalised Lucas sequence) one obtains

$$u_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} \text{ and } v_n = \lambda_1^n + \lambda_2^n. \tag{21}$$

As an immediate consequence of Equation (8), one obtains the following

Corollary 3.7.2. *For a companion matrix with trace T and determinant D, the fixed point counts a_n are given by*

$$a_n = \left|1 + D + Tu_n - 2Du_{n-1}\right| = \left|1 + D(1 - 2u_{n-1}) + Tu_n\right| = \left|1 + D^n - v_n\right|.$$

□

The following proposition follows from the explicit representations for u_n and v_n and is essentially a summary of Theorems 7,9 and 10 in [23] or follows from calculations similar to the ones performed there. Recall that, for an odd prime p, the Legendre symbol (α/p) is 1 if α is a quadratic residue modulo p; it is -1 if α is a non-residue, and 0 if $p|\alpha$ [40, Chap. 6.5].

Proposition 3.7.3. *Let $\alpha = T^2 - 4D$ denote the discriminant of the monic polynomial considered and let p be an odd prime with $p \nmid D, p \nmid T$. Then one has the following relations for the periods $\kappa(p)$ of the sequence $(u_m)_{m\geq 0}$ modulo p.*

(a) $(\alpha/p) = -1 \;\Leftrightarrow\; u_{p+1} \equiv 0 \mod p$, and in this case $\kappa(p) | r(p+1), r = \mathrm{ord}(D, p)$.

(b) $(\alpha/p) = 0 \;\Leftrightarrow\; u_p \equiv 0 \mod p$, and in this case $\kappa(p) = \mathrm{ord}(T/2, p) \cdot p$.

(c) $(\alpha/p) = 1 \;\Leftrightarrow\; u_{p-1} \equiv 0 \mod p$, and in this case $\kappa(p) | (p-1)$.

For any p with $p|T$, one has

$$\kappa(p) = \begin{cases} 2\mathrm{ord}(D,p) & \textit{for } \mathrm{ord}(D,p) \textit{ even, } \mathrm{ord}(D,p)/2 \textit{ even} \\ \mathrm{ord}(D,p) & \textit{for } \mathrm{ord}(D,p) \textit{ even, } \mathrm{ord}(D,p)/2 \textit{ odd} \\ 4\mathrm{ord}(D,p) & \textit{for } \mathrm{ord}(D,p) \textit{ odd.} \end{cases}$$

For $p = 2$ and T odd, the cycle length is $\kappa(2) = 3$.

Here, the Legendre symbol enters because, in the representation of the n-th term, powers of the discriminant of the shape $\alpha^{\frac{p-1}{2}} \equiv (\alpha/p) \mod p$, $p \neq 2$, show up. Note that the Legendre symbol also encodes the splitting behaviour of the associated polynomial: if the discriminant $T^2 - 4D$ is a quadratic residue modulo p, the polynomial splits into two different linear factors, while it admits a quadratic factor if p divides the discriminant. The cycle lengths modulo prime powers are then again governed by Proposition 3.4.1.

3.8 Normal forms and conjugacy invariants

As pointed out in Section 3.6, the problem of finding the periodic orbits of companion matrices is equivalent to finding periods of sequences satisfying the recurrence relation induced by its characteristic polynomial. In order to see to what extent the results from Section 3.6 apply to general matrices, it is an obvious next step to identify the similarity classes of direct sums of companion matrices.

Recall that the direct sum of two square matrices $M_1 \in \mathrm{Mat}(d_1, \mathbb{Z})$, $M_2 \in \mathrm{Mat}(d_2, \mathbb{Z})$ is defined as the block-diagonal matrix in $\mathrm{Mat}(d_1 + d_2, \mathbb{Z})$ which has M_1 and M_2 on the diagonal, in the following denoted by $\mathrm{diag}(M_1, M_2)$ or $\bigoplus_{i=1}^{2} M_i$. Clearly, for the characteristic polynomials, one then has $P_{M_1 \oplus M_2}(x) = P_{M_1}(x) \cdot P_{M_2}(x)$, and the extension to more than two matrices is straight-forward.

Over fields, one has the *Frobenius normal form* and the *Weierstraß normal form*, which are direct sums of companion matrices of the invariant factors of the matrix (in the first case) or the elementary divisors (for the latter). Note that, unlike the invariant factors themselves, their factorisation into the elementary divisors depends on the field over which the polynomial is considered.

Let $P_M(x) = i_1(x) \cdot \ldots \cdot i_s(x)$ be the decomposition of the characteristic polynomial of M into invariant factors; that is, $i_j(x)$ is the greatest common divisor of all j-minors of the characteristic matrix $x\mathbb{1} - M$, viewed as a matrix over $K[x]$ for some field K. Then each i_j for $1 \leq j \leq s$ is a product of powers of polynomials which are irreducible over K, the elementary divisors of M. Let $\phi_1^{k_1}, \ldots, \phi_t^{k_t}$ be the elementary divisors, (i.e. the ϕ_i and k_i need not be pairwise distinct). Then the above normal forms are given by

$$M \simeq \mathrm{diag}(C_{i_1}, \ldots, C_{i_s}) = \bigoplus_{j=1}^{s} C_{i_j} \quad \text{and} \quad M \simeq \mathrm{diag}(C_{\phi_1^{k_1}}, \ldots, C_{\phi_s^{k_t}}) = \bigoplus_{i=1}^{t} C_{\phi_i^{k_i}}, \tag{22}$$

see e.g. [37] or [57]. Hence, the problem can be reduced to several lower-dimensional ones, each of which is equivalent to the associated linear recursions. In summary that means, that the action of toral endomorphisms on prime lattices can be reduced to linear recursions over

finite fields, and the following fact describes the important special case where the characteristic polynomial factorises into distinct irreducible polynomials.

Fact 3.8.1. *The orbit lengths of the matrix from Equation* (22) *on the prime lattices* Λ_p *are determined by the table in Remark* 3.8. *When* $P_M(x) = \prod_{i=1}^{s} \phi_i(x) \in \mathbb{F}_p[x]$ *is a product of distinct irreducible factors,* M *is conjugate both with*

$$C_f \quad \textit{and} \quad \operatorname{diag}(C_{f_1}, \ldots, C_{f_s}).$$

The matrix periods on Λ_p *are then given by the orders* $\operatorname{ord}(f_i, p) = \min\{n : f_i(x) | x^n - 1\}$ *for* $1 \leq i \leq s$ *and their least common multiples.* □

As demonstrated in Section 3.6, over the residue class rings as well as over finite fields, the dynamics of companion matrices is equivalent with the properties of the associated linear recursions. However, in general it requires more effort to find out if a matrix over a (local) ring is conjugate with a block diagonal matrix of companion matrices. A partial result for the conjugacy problem is quoted below.

By Hensel's Lemma [59, XIII.4], for a factorisation of f in the polynomial ring over $\mathbb{Z}/p\mathbb{Z}$, $f(x) \equiv f_1(x) \ldots f_s(x)$ into coprime factors f_i, there is an extension to $\mathbb{Z}/p^r\mathbb{Z}$, namely a factorisation $f(x) \equiv F_1(x) \ldots F_s(x) \mod p^r$ such that $F_i \equiv f_i \mod p$. On the basis of lifting factorisations, Davis [28] showed that, if the reduction modulo p of the polynomial considered does not have any multiple factors, conjugacy over $\mathbb{Z}/p\mathbb{Z}$ extends to conjugacy over the p-adic integers. As a by-product, one obtains a complete set of normal forms for matrices over $\mathbb{Z}/p^r\mathbb{Z}$ whenever the reduction of the characteristic polynomial does not have any quadratic factors.

Theorem 3.8.1. [28, Thm. 2, Thm. 3 and Corollary] *Matrices which are annihilated by a common polynomial* $f \in \mathbb{Z}_p[x]$ *whose reduction modulo* p *does not have any quadratic factors over* $\mathbb{F}_p$ *are conjugate over* $\mathbb{Z}_p$ *if and only if they are conjugate mod* p. *Furthermore, if* $f(x) \equiv g_1(x) \ldots g_s(x) \mod p^r$ *is a factorisation which is in one-to-one correspondence with the factorisation of* $f \mod p$, *then a complete set of normal forms with respect to conjugacy over* $\mathbb{Z}/p^r\mathbb{Z}$ *is given by all direct sums*

$$\bigoplus_{i=1}^{s} k_i C_{g_i}, \quad \sum_{i=1}^{s} k_i \deg(g_i) = d. \qquad \square$$

Remark 3.10. The k_i in Theorem 3.8.1 can only be larger than 1 if the degree of f is less than the dimension d. This case corresponds to a minimal polynomial over $\mathbb{F}_p$ which is a true divisor of the characteristic polynomial and has a proper extension to the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$. Note however, that in general, the notion of a minimal polynomial over arbitrary rings is not well-defined, since it is no longer unique.

Fact 3.8.1 together with Theorem 3.8.1 shows how in particular cases the problem of period determination can be reduced to the dynamics of companion matrices and thus to the determination of orders of (irreducible) polynomials modulo prime powers. It is worth stating the following two special cases explicitly.

Theorem 3.8.2. *Let* p *be a fixed rational prime. Let* M *be an integer matrix whose characteristic polynomial* f *is irreducible modulo* p *and hence also modulo* p^r. *Then all non-trivial periodic orbits on* $\Lambda_{p^r} \setminus \Lambda_{p^{r-1}}$ *share the same length* $\operatorname{ord}(M, p^r) = \operatorname{ord}(C_f, p^r)$. *The number of orbits of length* $\operatorname{ord}(M, p^r)$ *is then* $\left|\Lambda_{p^r} \setminus \Lambda_{p^{r-1}}\right| / \operatorname{ord}(M, p^r) = (p^{rd} - p^{(r-1)d}) / \operatorname{ord}(M, p^r)$.

Proof. Let $f \in \mathbb{Z}[x]$ be the characteristic polynomial of $M \in \mathrm{Mat}(d, \mathbb{Z})$ and C_f the companion matrix of f over $\mathbb{Z}$. Then $(C_f \mod p^r) = C_{(f \mod p^r)}$. Clearly, $f(M) = f(C_f) = 0$ in $\mathbb{Z} \subset \mathbb{Z}_p$. If f is irreducible modulo p, it does not have any non-trivial quadratic factors over $\mathbb{F}_p$, hence the conditions of Theorem 3.8.1 are satisfied and $M \simeq C_f \mod p^r$ if and only if $M \simeq C_f \mod p$. But over $\mathbb{F}_p$, the companion matrix is the Frobenius normal form of M, (which coincides with the Weierstraß normal form, in this case), hence M is conjugate to its companion matrix and shares the same orbit lengths with it. For companion matrices, the claim follows from Theorem 3.6.7. □

Proposition 3.8.3. *Assume that the characteristic polynomial of M admits a linear factorisation $f(x) = \prod_{j=1}^{d}(x - a_j) \mod p$ where the a_j, for $1 \le j \le d$ are distinct modulo p. Then, for each $r \ge 1$, there are elements $a_j^{(r)} \in \mathbb{Z}/p^r\mathbb{Z}$ and $1 \le j \le d$ with $a_j^{(r)} \equiv a_j \mod p$ such that M is conjugate to $\mathrm{diag}(a_1^{(r)}, \ldots, a_d^{(r)})$ modulo p^r. In particular, all period lengths of M on Λ_{p^r} are the orders of $a_j^{(r)}$ and their common multiples.* □

Remark 3.11. Theorem 3.8.2 and Proposition 3.8.3 are in fact generalisations of [22, Thms.6.3 and 6.4] which are stated for 2×2 matrices only. The argumentation in the proof of Theorem 6.3 of [22] in essence only makes use of polynomial division in $\mathbb{Z}[x]$ and $\mathbb{F}_p[x]$, the Smith normal form and Proposition 3.4.1, hence it is straight-forward to rewrite the proof given in [22] for $d \times d$ integer matrices.

For the diagonal matrix, some cases of an extensive case distinction are stated in [22]. Even for 2×2 matrices, it is not instructive to spell out all possible period lengths in terms of the orders of the diagonal elements in the general case. However, it is clear that the observed period lengths are the orders $\mathrm{ord}(a_i^{(r)}, p^r)$ and the least common multiples of arbitrary subsets. In view of $\mathrm{ord}(a_i^{(r)}, p) = \mathrm{ord}(a_i, p)$ and Proposition 3.4.1, it is also clear that one expects a period growth analogously to the order growth.

Example 3.5. Consider the polynomial $f(x) \in \mathbb{Z}[x]$ whose reduction modulo p is $f(x) \equiv (x - a)(x - b)$ where $a \not\equiv b \mod p$. Viewed over $\mathbb{F}_p$, a matrix with characteristic polynomial f is conjugate to $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. Consider the matrix $\left(\begin{smallmatrix} a & p \\ p & b \end{smallmatrix}\right)$ whose characteristic polynomial $P_M(x) = (x - a)(x - b) - p^2$ is congruent to $f(x)$ modulo p^2. Hence, over $\mathbb{Z}/p^2\mathbb{Z}$, these matrices are conjugate, as they are to their companion matrix over $\mathbb{Z}/p^2\mathbb{Z}$. Using a standard algorithm, see e.g. [17], to find a factorisation $P_M(x) = g(x)h(x)$ over $\mathbb{Z}/p^3\mathbb{Z}$ such that $g(x) \equiv (x-a), h(x) \equiv (x - b) \mod p$ yields

$$g(x) = x - a + \frac{p^2}{b - a} \text{ and } h(x) = x - b - \frac{p^2}{b - a}.$$

Explicit calculation gives the equality

$$S \begin{pmatrix} a & p \\ p & b \end{pmatrix} S^{-1} \equiv \begin{pmatrix} a - \frac{p^2}{b-a} & 0 \\ 0 & b + \frac{p^2}{b-a} \end{pmatrix} \mod p^3,$$

where $S = \begin{pmatrix} 1 & -\frac{p}{b-a} \\ \frac{p}{b-a} & 1 \end{pmatrix}$. Since one even has $f(x) \equiv g(x)h(x) \mod p^4$, the above congruence extends to $\mathbb{Z}/p^4\mathbb{Z}$ and for $\mathbb{Z}/p^5\mathbb{Z}$, $\mathbb{Z}/p^6\mathbb{Z}$ the factorisation becomes $f(x) \equiv (x - a + \frac{p^2}{b-a} - \frac{p^4}{(b-a)^3})(x - b - \frac{p^2}{b-a} + \frac{p^4}{(b-a)^3})$, from which the diagonal elements for conjugacy over $\mathbb{Z}/p^6\mathbb{Z}$ can

be read off. The period lengths are then the orders of the diagonal elements and their least common multiples; upper bounds for the order of the diagonal elements modulo p^r are given by $p^{r-1}\operatorname{ord}(a,p)$ (and $p^{r-1}\operatorname{ord}(b,p)$). ◊

Remark 3.12. In a similar vein, Appelgate and Onishi [3] show that conjugacy in $\mathrm{SL}(d,\mathbb{Z}_p)$ can be reduced to conjugacy over $\mathbb{Z}/p^\nu\mathbb{Z}$ for some finite ν. In particular, there exists an exponent ν, such that conjugacy in $\mathrm{SL}(d,\mathbb{Z}/p^\nu\mathbb{Z})$ implies conjugacy within $\mathrm{SL}(d,\mathbb{Z}_p)$, and hence modulo p^r for all $r \geq \nu$. Also, in agreement with Davis' results, they conclude that for matrices with characteristic polynomials whose discriminant is not divisible by p, the characteristic polynomial is a complete conjugacy invariant for $\mathrm{SL}(d,\mathbb{Z}_p)$ conjugacy.

3.8.1 Normal forms in two and three dimensions

For matrices of size 2×2 and 3×3 over local rings, the conjugacy problem is in principle solved completely, see [6]. In order to avoid notational complications, we formulate results from [6] in the more specialised form for the residue class rings $\mathbb{Z}/p^r\mathbb{Z}$ instead of general local rings. Recall that a 2×2 matrix M over a ring R is called *cyclic*, if there is a vector $v\in R^2$ such that $\{v, Mv\}$ is a basis of the free module R^2. For a general (2×2)-matrix M, viewed as a matrix over $\mathbb{Z}/p^r\mathbb{Z}$, the conjugacy classes can be summarised in the following

Theorem 3.8.4. [6, Lemma 2.1, Thm. 2.2] *A matrix $M\in \mathrm{Mat}(2,\mathbb{Z}/p^r\mathbb{Z})$ can be written as $M = d\mathbb{1}+p^jB$, where $d\in\{0,\dots,p^j\}$, $0\leq j\leq r$, and B is a cyclic matrix, which is conjugate to its companion matrix. Hence, one has the conjugacy*

$$M \simeq d\mathbb{1} + p^j \begin{pmatrix} 0 & 1 \\ -D & T \end{pmatrix}$$

such that the conjugacy class is completely determined by d, j, D, T. □

Note that, in the situation of toral endomorphisms where M is an integer matrix, one has the decomposition $M = d\mathbb{1} + \operatorname{mgcd}(M)B$ over $\mathbb{Z}$. This shows that the primes modulo which M reduces to a scalar matrix and thus has a characteristic polynomial with a quadratic factor are precisely the divisors of $\operatorname{mgcd}(M)$.

Example 3.6. Consider Example 3.5 again. The matrix $\left(\begin{smallmatrix} a & p \\ p & b \end{smallmatrix}\right)$ coincides with the cyclic matrix B in its decomposition according to Theorem 3.8.4, hence it is conjugate to the companion matrix with trace $a+b$ and determinant $ab-p^2$ modulo p^r for all $r\geq 1$. From the assumption $a-b\not\equiv 0 \mod p$ it also follows for the diagonal matrices that their scalar part $d\mathbb{1}$ vanishes, as well as the exponent j of p in the coefficient of the cyclic matrix. This yields the stated conjugacies again. ◊

For larger matrices it is easiest to classify them according to their conjugacy class over the residue class fields $\mathbb{F}_p$. For 3×3 matrices over $\mathbb{F}_p$, one has the four types

$$\text{I. } a\mathbb{1}, a\in\mathbb{F}_p, \quad \text{II. } \operatorname{diag}(a,b,b),\ a\neq b, a,b\in\mathbb{F}_p, \quad \text{III. } \begin{pmatrix} a & 0 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix},\ a\in\mathbb{F}_p, \quad \text{and} \quad \text{IV. } C_f, f\in\mathbb{F}_p[x].$$

An extension of Theorem 3.8.4 is given by [6, Proposition 3.2]: a 3×3 matrix M can be decomposed $M = d\mathbb{1}+p^jB$ over $\mathbb{Z}/p^r\mathbb{Z}$, where j is a similarity invariant, B is not a scalar matrix modulo p and the conjugacy class of M is completely determined by d, j and B. Note

that, unlike in the two-dimensional case, B need not be cyclic. However, it is when B is lying above a type IV matrix, hence in this case, B is determined by its characteristic polynomial. In summary, the above decomposition reduces the conjugacy problem to the case of matrices that do not lie above scalar matrices modulo p. If the matrix B lies over a matrix of type II, it is similar over $\mathbb{Z}/p^r\mathbb{Z}$ to a matrix of the shape $\mathrm{diag}(a, b\mathbb{1} + p^j \left(\begin{smallmatrix} 0 & 1 \\ c & d \end{smallmatrix}\right))$, where $1 \le j \le r$, $c, d, \in \mathbb{Z}/p^{r-j}\mathbb{Z}$, $a \in \mathbb{Z}/p^r\mathbb{Z}$ and $b \in \mathbb{Z}/p^j\mathbb{Z}$. Furthermore, a, b are congruent modulo p with the diagonal elements of the matrices over $\mathbb{Z}/p\mathbb{Z}$.

The remaining hard cases are thus matrices B lying above a matrix of type III. In [6] it is shown that a matrix whose reduction modulo p is conjugate with $\left(\begin{smallmatrix} \bar{d} & 0 & 0 \\ 0 & \bar{d} & 1 \\ 0 & 0 & \bar{d} \end{smallmatrix}\right)$ over $\mathbb{F}_p$ is similar to a matrix $d\mathbb{1} + \left(\begin{smallmatrix} 0 & p^m & 0 \\ 0 & 0 & 1 \\ a & b & c \end{smallmatrix}\right)$, with $m \ge 1$ and $a, b, c, d - \bar{d} \equiv 0 \mod p$ over $\mathbb{Z}/p^r\mathbb{Z}$ (which again splits up into four classes of representatives of conjugacy classes).

The transition from the two- to the three-dimensional case suggests that in each dimension some 'original' hard cases show up, which cannot be reduced to lower dimensional subproblems, but for many integer matrices, their type over the residue class field $\mathbb{F}_p$ reveals the existence of invariant submodules of $(\mathbb{Z}/p^r\mathbb{Z})^d$, and thus gives a way of reduction to lower dimensions. Dynamically, the 'reducible' cases correspond to invariant sublattices of lower dimensional tori, on which the action of the matrix can be studied separately. However, since the decomposition is local, i.e. different for different primes, this does not imply the existence of invariant subtori.

One might try to find a systematic way of identifying all 'hard' cases in dimension d for growing d and thus solve the conjugacy problem 'recursively'. This interesting question is not pursued any further here.

3.8.2 Conjugacy invariants

In [16], the mgcd from Equation (18) was introduced as a further conjugacy invariant which, together with the trace and determinant, gives a complete set of invariants which is sufficient for conjugacy over $\mathbb{Z}/m\mathbb{Z}$ for all integers m (without forcing the matrices to be conjugate over $\mathbb{Z}$.)

Example 3.7. When $\mathrm{mgcd}(M)$ is not divisible by p, the conjugacy class of M over $\mathbb{Z}/p^r\mathbb{Z}$ is determined by the reductions of $\det(M)$ and $\mathrm{tr}(M)$ modulo p^r. It is clear from Theorem 3.8.4 that in this case M is cyclic, hence conjugate to a companion matrix, and therefore determined by the reduction of its characteristic polynomial modulo p^r.

Consider the integer matrices

$$M_1 = \left(\begin{smallmatrix} 5 & -2 \\ -2 & -3 \end{smallmatrix}\right) = -3 \cdot \mathbb{1} + 2\left(\begin{smallmatrix} 4 & -1 \\ -1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad M_2 = \left(\begin{smallmatrix} 5 & -2 \\ 0 & -3 \end{smallmatrix}\right) = -3 \cdot \mathbb{1} + 2\left(\begin{smallmatrix} 4 & -1 \\ 0 & 0 \end{smallmatrix}\right).$$

Modulo 4, their traces and determinants coincide, being congruent to 1 and 2, respectively. However, as one immediately sees from the decomposition, M_1 and M_2 are not conjugate on Λ_4 since the non-scalar summand is invertible in the case of M_1 and singular for M_2. Indeed, one finds that also the orbit counts on Λ_4 differ; for M_1, one has $Z_4(M_1, t) = (1-t)^4(1-t^2)^6$, for M_2, in contrast, $Z_4(M_2, t) = (1-t)^8(1-t^2)^4$. This example illustrates that, for the case of the mgcd not being coprime with the modulus considered, the reduced invariants are not sufficient for determining the local conjugacy class and thus the local orbit counts. ◊

It is natural to ask whether there is an extension of the mgcd to higher dimensions. More specifically, one would look for a conjugacy invariant or a set of invariants, which can be

calculated from the integer matrix and determines, together with the characteristic polynomial, the conjugacy class modulo all integers m or an appropriate subset thereof.

When considering a matrix M over some commutative ring R, the k-th *Fitting invariant* is defined as the ideal in $R[x]$ generated by all k-minors of the characteristic matrix $x\mathbb{1} - M$. Clearly, the Fitting invariants are conjugacy invariants, but in general, they are not strong enough to determine the conjugacy class of a matrix. Nechaev [61] calls a matrix over a commutative Artinian local ring R *canonically determined* if the Fitting invariants of the matrix determine its conjugacy class. He conjectures and proves in some special cases, including 2×2 matrices over R, that a matrix is canonically determined if and only if all Fitting invariants are principal ideals.

Lemma 3.8.5. *The Fitting invariants $D_1(M), D_2(M)$ of a matrix $M \in \mathrm{Mat}(2,\mathbb{Z})$ are all principal ideals in $\mathbb{Z}/p^r\mathbb{Z}[x]$ if and only if $v_p(\mathrm{mgcd}(M)) = 0$.*

Proof. For a matrix $M \in \mathrm{Mat}(2,\mathbb{Z})$ with $M = d \cdot \mathbb{1} + \mathrm{mgcd}(M)B$, one has $D_1(M) = (x - d, \mathrm{mgcd}(M))$, which is a principal ideal if and only if $\mathrm{mgcd}(M)$ is a unit in $\mathbb{Z}/p^r\mathbb{Z}$. □

Lemma 3.8.5 justifies to consider the Fitting invariants as an extension of the mgcd in so far, as these invariants 'mark' the ambiguous cases in a similar way the mgcd does for 2×2 matrices. However, they are not complete in the sense that coinciding Fitting ideals are in general not sufficient for conjugacy.

Kurakin [50] refines the notion of Fitting invariants by lifting the ideals to polynomial rings over the p-adics and shows that for 2×2 matrices, these *Kurakin invariants* form a complete set of invariants. In fact, we have the following lemma, which follows from the explicit representation of the Kurakin invariants given in [50, Thm. 2].

Lemma 3.8.6. *The Kurakin-invariants in $\mathbb{Z}_p[x]$ of two matrices $M_1, M_2 \in \mathrm{Mat}(2,\mathbb{Z})$ coincide if $\mathrm{tr}(M_1) = \mathrm{tr}(M_2)$, $\det(M_1) = \det(M_2)$ and $v_p(\mathrm{mgcd}(M_1)) = v_p(\mathrm{mgcd}(M_2))$.*

But as is shown in [50, Example 2], already for 3×3 matrices, the Kurakin invariants fail to determine the conjugacy class.

Remark 3.13. The original motivation in this work to study conjugacy classes and normal forms over finite local rings was the interest in periodic orbits on the rational lattices of the torus. Since conjugacy of two matrices is only a sufficient, but not a necessary condition for sharing the same orbit counts, one could wonder whether conjugacy is the right notion to study and if so, within which matrix group. In view of Sections 3.2 and 3.3, instead of studying conjugacy over $\mathbb{Z}/p^r\mathbb{Z}$, one could focus on equivalence of $M^n - \mathbb{1}$ over $\mathbb{Z}/p^r\mathbb{Z}$. However, since the equivalence depends on n, the sequence of matrices $M^n - \mathbb{1}$ is more difficult to study.

Furthermore, conjugacy over $\mathbb{Z}/p^r\mathbb{Z}$ is the only 'structural' reason behind two matrices sharing the same orbit counts; for different roots, their orders coincide only 'randomly'.

The approach chosen here puts into perspective that the dynamics of two integer matrices can be the same on the sequence of prime power lattices Λ_{p^r} for some prime p, $r \geq 1$, and differ on Λ_{q^s}, $s \geq 1$, for another prime q; whether or not the dynamics is determined by the characteristic polynomial crucially depends on the factorisation of the latter modulo the prime. The existence of the mgcd as a third invariant for 2×2 matrices which determines conjugacy mod n for all $n \in \mathbb{N}$ but not over $\mathbb{Z}$ illustrates that $\mathbb{Z}$-conjugacy is too strong a restriction for two toral endomorphisms to have the same orbit counts.

In [16], it was stated that conjugacy of 2×2 matrices modulo n for all $n \in \mathbb{N}$ is equivalent to conjugacy over the Prüfer-ring $\widehat{\mathbb{Z}} \simeq \prod_{p \text{ prime}} \mathbb{Z}_p$, i.e. in $\mathrm{GL}(2, \widehat{\mathbb{Z}})$. This result extends to general dimensions, and illustrates that, for studying the local behaviour on all rational lattices at the same time, $\mathrm{GL}(d, \widehat{\mathbb{Z}})$ is (in theory) the right matrix group to consider, rather than $\mathrm{GL}(d, \mathbb{Z})$.

Remark 3.14. As a final remark for Sections 3.6–3.8, let us briefly review the approach by Percival and Vivaldi [66]. Their results for $\mathrm{SL}(2, \mathbb{Z})$ matrices with real eigenvalues are similar to those obtained by studying recursive sequences, which is not surprising as both are essentially determined by the roots of the characteristic polynomial. For the matrix class under consideration, the two eigenvalues are conjugates of each other, hence, by choosing one (e.g. in the real case the larger one), one can refer to 'the' eigenvalue of such a matrix. A central aspect of the investigations in [66] is the fact that the dynamics of $\mathrm{SL}(2, \mathbb{Z})$-matrices on rational lattices can be reduced to the periods of the eigenvalue λ modulo ideals in the associated quadratic number fields. The eigenvalue λ, in turn, is determined by the characteristic polynomial, and due to the connection between polynomials over $\mathbb{Z}$ and algebraic integers, the approach of Section 3.6 is closely related to the eigenvalue ansatz in two-dimensional systems.

The considerations concerning conjugacy (which in [66] means $\mathrm{GL}(2, \mathbb{Z})$-conjugacy) again underline the difference between 'local' and 'global' conjugacy. When the dependence of periods on particular lattices is studied, local invariants determine the behaviour. As is said in [66, Section 4.1], for the dynamics induced by an $\mathrm{SL}(2, \mathbb{Z})$-matrix on prime lattices, more important than the $\mathrm{GL}(2, \mathbb{Z})$-conjugacy class is the eigenvalue.

For further connections between ideal theory, integer matrices and algebraic number theory see also [76] and [55].

4 Orbit pretail structure of toral endomorphisms

In this section, the action of general endomorphisms $M \in \mathrm{Mat}(d, \mathbb{Z})$ on a lattice Λ_n on which M is *not* locally invertible is examined. When M is not invertible, this manifests itself in the existence of 'pretails' to periodic orbits, with rather characteristic properties. More precisely, given a periodic point y of M, a finite set of iterates (or suborbit)

$$O = \{x, Mx, M^2x, \ldots, M^t x = y\} \tag{23}$$

is called a *pretail* (of y) if y is the only periodic point of M in O.

In the following sections, if not stated otherwise, we fix an integer n and suppress indices at sets, that is, $\ker_n(M)$ will be written as $\ker(M)$ and $\mathrm{per}(M) = \{x \in \tilde{\Lambda}_n \mid x \text{ is periodic under } M\}$. (However, in Section 4.3 where we restrict ourselves to prime power lattices Λ_{p^r}, we will write $\ker_r(M)$.)

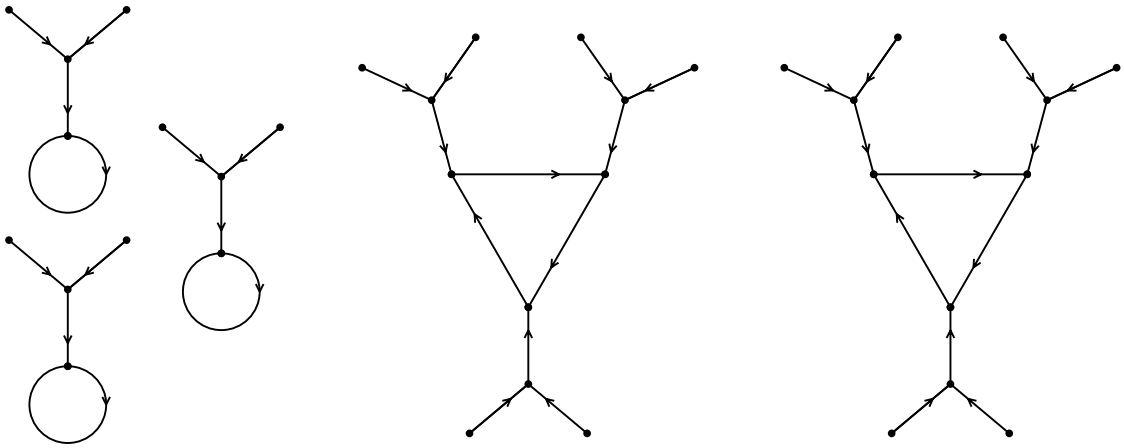


Figure 1: Example of an orbit graph with pretails: the image shows the directed graph induced by the action of $M = \left(\begin{smallmatrix} 4 & 0 \\ 1 & 4 \end{smallmatrix}\right)$ on the lattice $\tilde{\Lambda}_6$, which has three fixed points and 3-cycles. Each path from a node with in-degree 0 to one of the periodic points is a pretail.

4.1 General structure

Let M and n be fixed, and define $R = \mathbb{Z}/n\mathbb{Z}$. Let $\mathrm{per}(M)$ denote the set of periodic points on the lattice $\tilde{\Lambda}_n$, under the action of M mod n. Due to the linear structure of M, $\mathrm{per}(M)$ is an M-invariant submodule of $\tilde{\Lambda}_n$. It is the maximal submodule on which M is invertible. The kernel $\ker(M^k) \subset \tilde{\Lambda}_n$ denotes the set of points that are mapped to 0 under M^k. One has $\ker(M^k) \subset \ker(M^{k+1})$ for all $k \geq 0$, and this chain stabilises, so that $\bigcup_{k\geq 0} \ker(M^k)$ is another well-defined and M-invariant submodule of $\tilde{\Lambda}_n$. This is then the maximal submodule on which the restriction of M acts as a nilpotent map. Note that $\mathrm{per}(M) \cap \ker(M^k) = \{0\}$ for all $k \geq 0$.

Consider an arbitrary $x \in \tilde{\Lambda}_n$ and its iteration under M. Since $|\tilde{\Lambda}_n| = n^d$ is finite, Dirichlet's pigeon hole principle implies that this orbit must return to one of its points. Consequently, every orbit is a cycle or turns into one after finitely many steps, i.e. it is eventually periodic. By elementary arguments, one then finds the following result.

Fact 4.1.1. *There are minimal integers $m \geq 0$ and $k \geq 1$ such that $M^{k+m} \equiv M^m \bmod n$. The number k is the least common multiple of all cycle lengths on $\tilde{\Lambda}_n$, while m is the maximum of all pretail lengths. Clearly,* $\mathrm{per}(M) = \mathrm{Fix}(M^k)$. □

The lattice $\tilde{\Lambda}_n = R^d$ is a free R-module. The modules $\mathrm{per}(M)$ as well as $\mathrm{Fix}(M^j)$ and $\ker(M^j)$ for $j \geq 1$ are submodules of it, with $\mathrm{Fix}(M^i) \cap \ker(M^j) = \{0\}$ for all $i \geq 1$ and $j \geq 0$. Recalling some results on modules from [54, Ch. III] now leads to the following consequences.

Fact 4.1.2. *Let m and k be the integers from Fact* 4.1.1. *If $m \geq 1$, one has*

$$\{0\} \subsetneq \ker(M) \subsetneq \ker(M^2) \subsetneq \ldots \subsetneq \ker(M^m) \subseteq \tilde{\Lambda}_n,$$

while $\ker(M^{m+j}) = \ker(M^m)$ *for all $j \geq 0$. Moreover, one has*

$$\tilde{\Lambda}_n = \mathrm{Fix}(M^k) \oplus \ker(M^m),$$

which is the direct sum of two M-invariant submodules. Hence, $\mathrm{per}(M)$ *and* $\ker(M^m)$ *are finite projective R-modules.* □

Remark 4.1. We excluded the trivial case $m = 0$, which corresponds to $\ker(M) = \{0\}$ and $\mathrm{Fix}(M^k) = \tilde{\Lambda}_n$, hence M invertible on $\tilde{\Lambda}_n$. The case of $\mathrm{Fix}(M^k) = \{0\}$ and $\ker(M^m) = \tilde{\Lambda}_n$, which corresponds to the restriction of M to $\tilde{\Lambda}_n$ being nilpotent, is included, though.

In general, the projective summands need not be free. As a simple example, consider $\tilde{\Lambda}_6$ with $d = 1$ and $M = 2$. Here, $\mathrm{per}(M) = \{0, 2, 4\}$ covers the fixed point 0 and a 2-cycle, while $\ker(M) = \{0, 3\}$. Both are modules (and also principal ideals, hence generated by a single element) over $\mathbb{Z}/6\mathbb{Z}$, but do not have a basis, hence are not free. Nevertheless, one has $\mathbb{Z}/6\mathbb{Z} = \mathrm{per}(M) \oplus \ker(M)$. Note that even if $\ker(M^m)$ is a free module for some $m > 1$, $\ker(M)$ need not be free. In fact, this is the generic case, compare also Example 4.1. As needed, the submodules from above may be viewed as Abelian groups (or, equivalently, as $\mathbb{Z}$-modules) instead of $\mathbb{Z}/n\mathbb{Z}$-modules. In line with this, also the restriction of a toral endomorphism M on some particular lattice $\tilde{\Lambda}_n$ can be viewed as a $\mathbb{Z}/n\mathbb{Z}$-module endomorphism as well as a homomorphism of the Abelian group $(\mathbb{Z}/n\mathbb{Z})^d$. It is well-known that a group (module) homomorphism induces an isomorphism between the factor group by its kernel and its image (also known as *Fundamental Homomorphism Theorem*). The isomorphisms induced by M and its powers are the following.

Fact 4.1.3. *For a toral automorphism M and each $i \in \{1, \ldots, m\}$, one has the isomorphisms*

$$\tilde{\Lambda}_n / \ker(M^i) \simeq M^i(\tilde{\Lambda}_n)$$
$$\ker(M^{i+1}) / \ker(M^i) \simeq M^i(\ker(M^{i+1})).$$

Note that the groups $M^i(\ker(M^{i+1}))$ are subgroups of $\ker(M)$.

For the implications of these isomorphisms on the graphs see also Figure 4.

4.2 The pretail tree

In the following, M is some fixed integer matrix, defining a toral endomorphism, whose restriction to some fixed lattice $\tilde{\Lambda}_n$ is considered. In general, the preimage $M^{-\ell}(y) \subset \tilde{\Lambda}_n$ of a single point $y \in \tilde{\Lambda}_n$ can be the empty set. However, if there is some x with $M^\ell x = y$,

one has $M^{-\ell}(y) = x + \ker(M^\ell)$. Thus, for the cardinality of the preimage, one obtains $\left|M^{-\ell}(y)\right| \in \{0, \left|\ker(M^\ell)\right|\}$.

A point y, which is periodic under M^ℓ, always has a periodic ℓ-th predecessor, and consequently, there are $\left|\ker(M^\ell)\right|$ points mapped to y in ℓ iterations of M. Due to the linearity of M and its powers, the structure of the set of pretails of a periodic point y must be the same for all $y \in \mathrm{per}(M)$ (note that there is precisely one predecessor of y in the periodic orbit, which might be y itself, while all points of the pretail except y are from the complement of the periodic orbit).

Consequently, it suffices to study the pretail structure for $y = 0$. The union of all pretails of the fixed point 0 defines a (directed) graph, called the *pretail graph* from now on; see [85] for general background on graph theory. A single pretail is called *maximal* when it is not contained in any longer one. By construction, there can be no cycle in the pretail graph, while $y = 0$ plays a special role. Viewing each maximal pretail of 0 as an 'ancestral line', we see that this approach defines a rooted tree with root 0. Note that an isomorphic tree also 'sits' at every periodic point y. As a consequence of the above, we formulate the following

Corollary 4.2.1. *Every periodic point of M on $\tilde{\Lambda}_n$ has a directed pretail graph that is isomorphic to that of the fixed point 0. Up to graph isomorphism, it thus suffices to analyse the latter. By reversing the direction, it is a rooted tree with root 0. This tree is trivial if and only if M is invertible on $\tilde{\Lambda}_n$.* □

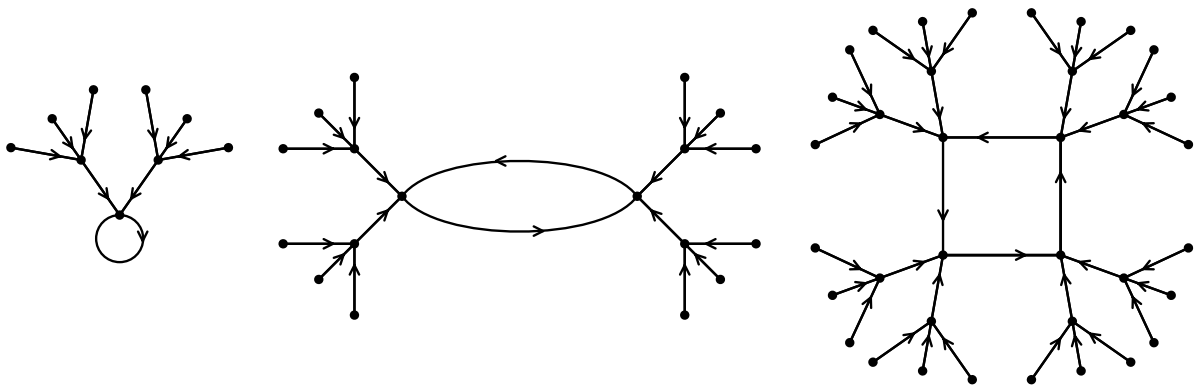


Figure 2: The directed graph for the action of $M = \left(\begin{smallmatrix} 0 & 12 \\ 1 & 6 \end{smallmatrix}\right)$ on the lattice $\tilde{\Lambda}_{15}$. The only fixed point of M is 0, while it has two 2-cycles and five 4-cycles (each shown once only). All pretail trees have the same height.

The directed tree associated with an endomorphism M (on a given lattice) will be referred to as its *pretail tree* (on this lattice).

A *complete subtree* of a tree $\mathcal{T}$ originating at a node v is the tree consisting of v and all of its descendants in $\mathcal{T}$. When the root v of a subtree is not important, it will be suppressed. The terms *node* and *vertex* will be used interchangeably.

Recall that terminal nodes of a rooted tree (excluding the root in the trivial tree) are called *leaves*. With this definition, the total number of leaves on $\tilde{\Lambda}_n$ is $|\tilde{\Lambda}_n \setminus M(\tilde{\Lambda}_n)|$.

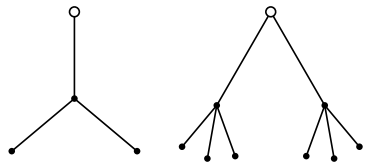


Figure 3: Pretail trees extracted from Figures 1 and 2. The white node represents 0.

Nodes that are not leaves are also called internal (or inner) nodes. It is clear that the set of all internal nodes in a pretail tree corresponds to the image of the restriction of M on the kernel summand from Fact 4.1.2, see also Figure 4. The *height* of a node is the graph distance of the longest downward path from that node to a leaf. In particular, the height of the root is the height of the tree. The *depth* of a node is its graph distance to the root of the tree. By a truncation of a pretail tree at depth k, we mean the subtree consisting of all nodes that have at most graph distance k from the root.

4.2.1 Characterisation of the pretail tree

Let $\mathcal{T}$ denote some fixed pretail tree of height h. As discussed at the beginning of Section 4.2, the subtree originating at x either has no nodes at depth k at all, or precisely $\left|\ker(M^k)\right|$ ones. Consequently, the structure of a subtree of given height b can be read off from the first b levels of the tree. This will be made more precise in Proposition 4.2.2 and Corollary 4.2.3 below. Consider the sequence of sets

$$C_i = \{x \in \ker(M) \mid x \text{ is root of a subtree of height } \geq i\},\ i = 0, \ldots, h. \tag{24}$$

Clearly, $\ker(M) = C_0 \supseteq C_1 \supseteq C_2 \supseteq \ldots \supseteq C_h = \{0\}$, where h is the height of $\mathcal{T}$. In fact, this is a sequence of subgroups of $\ker(M)$, since $C_i = M^i(\ker(M^{i+1})) = M^i(\tilde{\Lambda}_{p^r}) \cap \ker(M)$. Note that according to Fact 4.1.3, $C_i \simeq \ker(M^{i+1})/\ker(M^i)$. Let $\beta_i = |C_i| = \frac{\left|\ker(M^{i+1})\right|}{\left|\ker(M^i)\right|}$ for $0 \leq i \leq h$. For each individual internal node $\neq 0$, the number of children is $\beta_0 \coloneqq |\ker(M)|$ and for 0, it is $|\ker(M)| - 1$ (since the loop from the original graph has been discarded). Consequently, one has $\left|\ker(M^2)\right| = |\ker(M)| + (\beta_1 - 1)\left|\ker(M)\right|$. Similarly, $\left|\ker(M^3)\right| = \left|\ker(M^2)\right| + (\beta_2 - 1)\left|\ker(M^2)\right|$, since each node in C_2 has $\left|\ker(M^2)\right|$ 'grandchildren', the ones of 0 being already counted in $\left|\ker(M^2)\right|$. Continuing this process, one inductively obtains the following product for the cardinality of $\ker(M^i)$, for $1 \leq i \leq h$,

$$\begin{aligned}\left|\ker(M^i)\right| &= \left|\ker(M^{i-1})\right| + (\beta_{i-1} - 1)\left|\ker(M^{i-1})\right| \\ &= |\ker(M)| \prod_{j=1}^{i-1} \beta_j = \prod_{j=0}^{i-1} \beta_j.\end{aligned}$$

Example 4.1. Consider the matrix $M = \left(\begin{smallmatrix} 4 & 4 \\ 1 & 4 \end{smallmatrix}\right)$ on $\tilde{\Lambda}_8$, where it is nilpotent (mod 8) with nil-degree 4. The (directed) pretail graph spans the entire lattice and is shown at the top of Figure 4. Here, $C_0 = \ker(M) = \left\langle \binom{0}{2} \right\rangle$ and $\beta_0 = 4$; $C_1 = C_0$, $C_2 = \left\langle \binom{0}{4} \right\rangle$, hence $\beta_2 = 2$; finally, $C_3 = C_2$ and $C_4 = \{0\}$. Furthermore, $\ker(M^2) = \left\langle \binom{0}{2} \right\rangle \oplus \left\langle \binom{2}{0} \right\rangle$, $\ker(M^3) = \left\langle \binom{0}{1} \right\rangle \oplus \left\langle \binom{2}{0} \right\rangle$, and $\ker(M^4) = \left\langle \binom{0}{1} \right\rangle \oplus \left\langle \binom{1}{0} \right\rangle = \tilde{\Lambda}_8$, which illustrates that $\ker(M^2)/\ker(M) \simeq C_0 = C_1 \simeq \mathbb{Z}/4\mathbb{Z}$, and $\ker(M^3)/\ker(M^2) \simeq \ker(M^4)/\ker(M^3) \simeq C_2 = C_3 \simeq \mathbb{Z}/2\mathbb{Z}$. ◊

The contents of the following proposition is illustrated schematically in Figure 5.

Proposition 4.2.2. *The orders $\beta_0, \beta_1, \ldots, \beta_{h-1}$ of the sequence of subgroups $C_0, C_1, \ldots, C_{h-1}$ of $\ker(M)$ characterise the pretail tree on a fixed lattice up to graph isomorphism.*

Proof. The pretail tree $\mathcal{T}$ associated with the numbers $\beta_0, \ldots, \beta_{h-1}$ can be constructed level-wise, that is, by uniquely extending the truncation $\mathcal{T}^{(k)}$ of $\mathcal{T}$ at depth k to $\mathcal{T}^{(k+1)}$, the truncation of $\mathcal{T}$ at depth $k+1$. The graph on $\ker(M)$ is determined by β_0. Each of the $\beta_1 - 1$

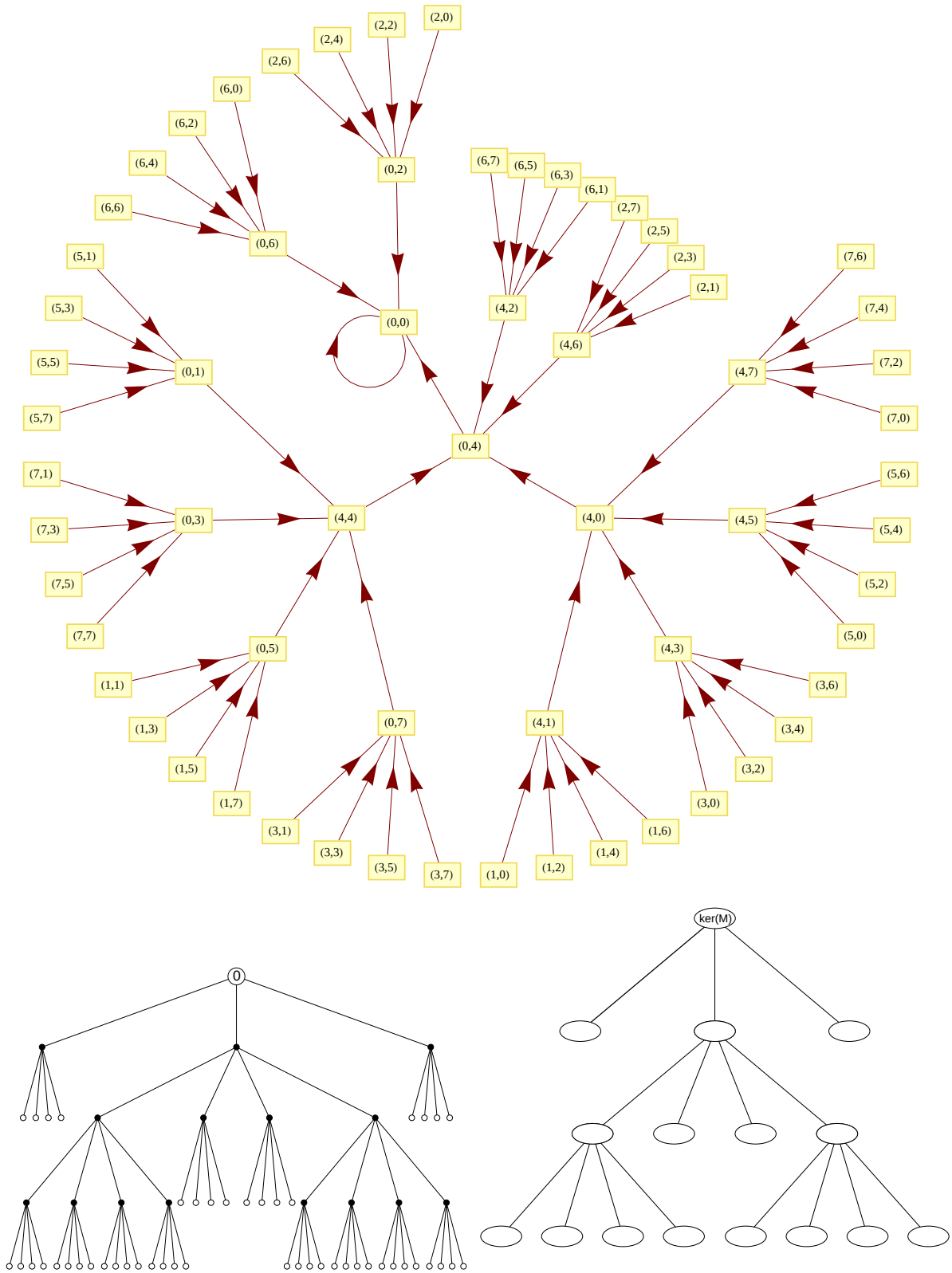
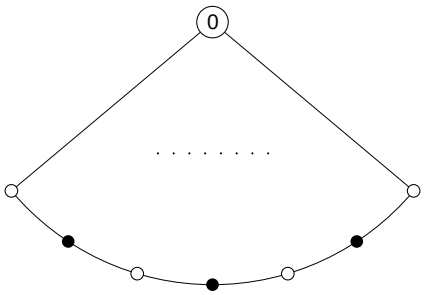
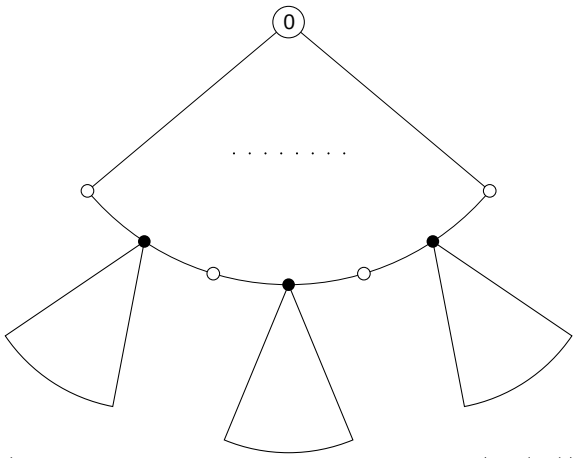


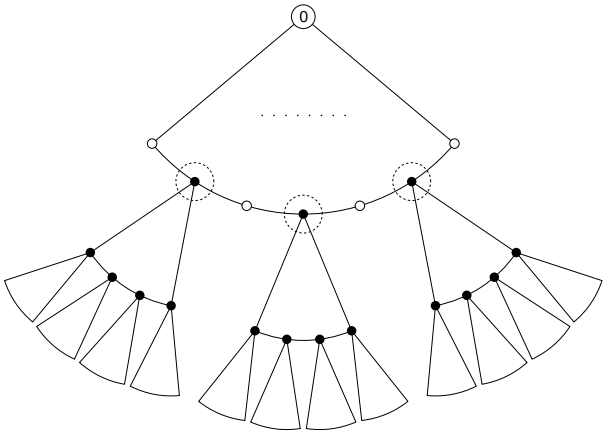
Figure 4: The pretail graph for Example 4.1, with coordinates for the action of the matrix M on $\tilde{\Lambda}_8$ (above), where it is nilpotent with nil-degree 4. Below, the left graph highlights the tree structure, the black nodes constituting the image $M(\tilde{\Lambda}_8)\setminus\{0\}$. The left hand side (lhs) illustrates that the isomorphisms from Fact 4.1.3 extend to graph isomorphisms for the induced maps, here the one on $\tilde{\Lambda}_8/\ker_8(M) \simeq M(\tilde{\Lambda}_8)$, (i.e. black nodes on the lhs define a graph which is isomorphic to that on the rhs). Each ellipse on the rhs represents an equivalence class modulo $\ker(M)$.



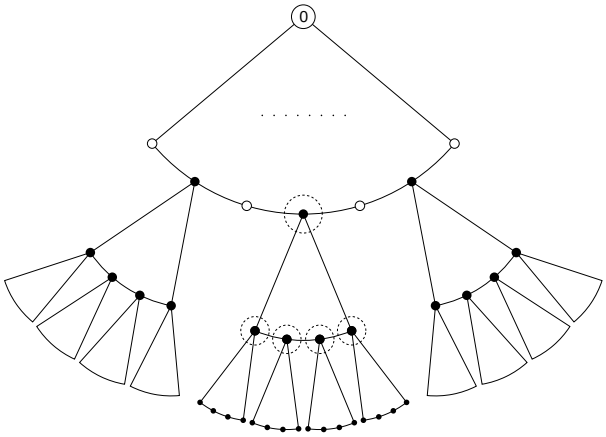
(a) $\ker(M)$ with non-trivial elements of C_1 marked.



(b) Each attached 'cone' consists of precisely $|\ker(M)|$ nodes.



(c) Elements of $C_2 \setminus \{0\}$ encircled. Here, $C_1 = C_2$. Each subtree rooted at element of $C_2 \setminus \{0\}$ has $|C_1|\,|\ker(M)|$ nodes at depth 2.



(d) C_3 is a true subgroup of C_2. Among the children of elements from $C_3 \setminus \{0\}$, there are $|C_1|$ internal nodes, among which $|C_2|$ are roots of subtrees of height ≥ 2. The black nodes at distance 3 from 0 indicate internal nodes (i.e. they are not leaves).

Figure 5: Schematic step-wise construction of the pretail tree.

elements in $\ker(M) \setminus \{0\}$ that are not terminal nodes have precisely β_0 children each, which all have graph distance 2 from the root 0. Thus, by β_0 and β_1, the truncation of $\mathcal{T}$ at depth 2 is completely determined.

Assume now that the tree is determined up to depth k (counted from 0). There are $\beta_k - 1$ vertices in $\ker(M) \setminus \{0\}$ that are roots of subtrees of height at least k, extending the truncated pretail tree $\mathcal{T}^{(k)}$ to $\mathcal{T}^{(k+1)}$. Let v be one of these $\beta_k - 1$ elements of $\ker(M)$ and let $\mathcal{T}_v$ denote the subtree rooted at v. $\mathcal{T}_v$ is related to $\mathcal{T}^{(k)}$ in the following way. The out-degree of v is larger than that of 0 by one, due to the special role of 0 (being its own predecessor in the original pretail graph). In a similar vein, among the children of v, there are β_i nodes that admit subtrees of height at least i, instead of $\beta_i - 1$ (for all i small enough for v to have offspring at distance i in the tree under construction). Thus, by comparison with $\mathcal{T}^{(k)}$, it is clear how to extend $\mathcal{T}_v$ to depth k (counted from v) or depth $k+1$, counted from 0. Since the

construction of the subtree starting at a vertex v does not depend on the choice of v among all vertices that admit subtrees of height at least k, all possible pretail trees that can be created by this process are isomorphic as trees. Thus, the claim follows. □

The linearity of M constrains the possible structure of the induced pretail tree, hence the set of all pretail trees on a given lattice is a class of trees with characteristic properties.

Corollary 4.2.3. *Let $\mathcal{T}$ denote the pretail tree of a toral endomorphism. Two complete subtrees of $\mathcal{T}$ are isomorphic as trees, whenever they share the same height. Two truncated complete subtrees of the same height are isomorphic if neither of them is rooted at 0.* □

Remark 4.2. Let $N = |\ker(M)|$ and h be the height of the pretail tree $\mathcal{T}_M$. Note that $\mathcal{T}_M$ is an N-ary tree (i.e. a rooted tree in which each node has at most N children), but, due to the special role of 0, not a *full* N-ary tree (the latter meaning each node has either 0 or N children), although all complete subtrees are. However, it could be turned into one by duplicating 0 and adding it as a further child to the root. Append a copy of the kernel to the 0-duplicate, and within this copy, attach copies of the children of the nodes in the original kernel. If this procedure is repeated until the 0-duplicate is the root of a subtree of height $h-1$, the resulting tree is a full N-ary tree with the property, that the i-th level accommodates a copy of $\ker(M^i)$ (instead of $\ker(M^i) \setminus \ker(M^{i-1})$ as $\mathcal{T}_M$). For the tree resulting of this procedure, the last corollary can be extended to appropriate truncations of the full tree instead of the restriction to complete subtrees.

Following the terminology for N-ary trees, a pretail tree will be called *perfect*, if all leaf nodes are at the same depth, i.e. if all maximal pretails share the same length. It will be called *perfect up to depth k*, if the tree resulting from truncation at level k is perfect. The following lemma states some equivalent criteria for pretail trees to be perfect up to depth k.

Lemma 4.2.4. *Let $\mathcal{T}_M$ be the pretail tree induced by the integer matrix M on $\tilde{\Lambda}_n$. Then the following properties are equivalent.*

(i) $\mathcal{T}_M$ *is perfect up to depth k*

(ii) One has $\ker(M^{k-1}) \subset M(\tilde{\Lambda}_n)$

(iii) One has $\ker(M^{k-1}) \setminus \ker(M^{k-2}) \subset M(\tilde{\Lambda}_n)$.

(iv) The homomorphisms $\ker(M^j)/\ker(M) \longrightarrow \ker(M^{j-1})$ *induced by M for $1 \leq j \leq k$ are isomorphisms.*

(v) The homomorphisms $\ker(M^j)/\ker(M^{j-1}) \longrightarrow \ker(M)$ *induced by M^{j-1} for $1 \leq j \leq k$ are isomorphisms.*

(vi) The subgroups $C_0, \ldots, C_{k-1}$ of $C_0 = \ker(M)$ defined in Equation (24) are the full kernel C_0, hence $\beta_0 = \beta_1 = \ldots = \beta_{k-1}$.

(vii) One has $|\ker(M^{i+1})| = |\ker(M)|\,|\ker(M^i)| = |\ker(M)|^{i+1}$ *for all $0 \leq i < k$.*

In particular, $\mathcal{T}_M$ is perfect if the conditions are true for $k = m$, where m is the integer from Fact 4.1.1.

Proof. When M is invertible, the pretail tree is trivial and the claims are obviously true for $k = 0$. We therefore assume M is not invertible on $\tilde{\Lambda}_n$. Our argumentation will be to show the equivalence of (i) through (iv), (v) through (vii), as well as (iv)⇒(vii) and (vi)⇒ (i).

$\mathcal{T}_M$ is perfect up to depth k if and only if each node at each depth $\leq k$ has $|\ker(M)|$ children, hence $\ker(M^j)$ is a subset of the image of M on $\tilde{\Lambda}_{p^r}$, and (i) and (ii) are equivalent. If all nodes at depth $k-1$ have $|\ker(M)|$ children, the same holds for all nodes at depth $j < k-1$, due to the linearity of M, hence (iii) is equivalent with the first two statements. The map given in (iv) is an isomorphism, if and only if M maps $\ker(M^j)$ onto $\ker(M^{j-1})$. In this case, $\ker(M^{j-1}) \subset M(\tilde{\Lambda}_n)$ and (ii) and (iv) are equivalent. (iv) clearly implies (vii). $C_i \simeq \ker(M^{i+1})/\ker(M^i)$, so (v) and (vi) are equivalent. In view of Equation (24), and since $\beta_i \leq \beta_0$ for all i, it is clear that (vi) and (vii) are equivalent. That (vi) implies (i) follows from Proposition 4.2.2, since a tree that is perfect up to depth k has $\beta_0 = \ldots = \beta_{k-1}$. □

On the prime power lattices $\tilde{\Lambda}_{p^r}$, the chains of subgroups are constrained by being p-groups. The following proposition gives a sufficient condition for a pretail tree on $\tilde{\Lambda}_{p^r}$ to be perfect. We will return to the prime power lattices in a more detailed way in the next section.

Proposition 4.2.5. *Consider the action of M on the lattice $\tilde{\Lambda}_{p^r}$. When $|\ker(M)| = p$, one has $|\ker(M^i)| = p^{\min(i,m)}$ for all $i \geq 0$, where m is the integer from Fact 4.1.1 for $n = p^r$. This means $C_i = \ker(M)$ for $1 \leq i \leq m-1$, and all maximal pretails share the same length m.*

Proof. Since a group of order p only has trivial subgroups, the subgroups C_i are restricted to being $\{0\}$ or $\ker(M)$. For all i with $C_i = \ker(M)$, all vertices at graph distance i have children and $\left|\ker(M^i)\right| = |\ker(M)|^i$, whence the tree is perfect up to depth k. Once $C_i = \{0\}$ for some i, the height of the tree is i and $\ker(M^{i+j}) = \ker(M^i)$ for all $j \geq 0$. □

In general, the maximal pretails need not share the same length, as Example 4.1 shows. More precisely, the tree in this example is perfect up to depth 2.

So far, we have looked at a single lattice $\tilde{\Lambda}_n$. However, any given matrix M immediately defines a *sequence* of trees via $\tilde{\Lambda}_n$ with $n \in \mathbb{N}$. When $d = 2$, the result of [16, Thm. 2] implies the following result.

Corollary 4.2.6. *Let $M, M' \in \mathrm{Mat}(2, \mathbb{Z})$ be two matrices with the same trace, determinant and* mgcd. *Then, they have the same sequence of pretail trees on the lattices $\tilde{\Lambda}_n$.* □

The most important class of subsequences of pretail trees associated with an integer matrix M arises from the sequence of prime powers p^r for a fixed prime p and growing $r \in \mathbb{N}$, which we will consider in Section 4.5.

4.3 Decomposition and parametrisation on $\tilde{\Lambda}_{p^r}$

When the integers u, v are coprime, one has $\Lambda_{uv} \simeq \Lambda_u \oplus \Lambda_v$, cf. Section 3.1, wherefore the action on Λ_n with $n \in \mathbb{N}$ is completely determined by that on Λ_{p^r}, for all $p^r || n$. In particular, the pretail orbit structure on an arbitrary Λ_n can be derived from that on the sublattices associated with the factors in the prime factorisation of n.

Define $R_r = \mathbb{Z}/p^r\mathbb{Z}$, which is a *local* ring, with unique maximal ideal $(p) = pR_r$. By [54, Thm. X.4.4], we then know that the two projective modules $\mathrm{per}(M)$ and $\ker(M^k)$ of Fact 4.1.2 are *free*, so each has a basis. Consequently, one knows that the linear map on $\tilde{\Lambda}_{p^r}$ defined

by M induces unique linear maps on $\mathrm{Fix}(M^{k(r)})$ and $\ker(M^{m(r)})$, and M is conjugate to the direct sum of these maps, compare [1, Prop. 4.3.28]. Each of the latter, in turn, admits a matrix representation with respect to any chosen basis of the corresponding submodule. As in the case of vector spaces, different choices of bases lead to conjugate matrices [1, Prop. 4.3.23]. The *nil-degree* of a matrix B over some ring R denotes the least integer n such that $B^n = 0$.

Note that indices at all names of sets like $\ker_r$ and per_r refer to the ring R_r, hence they denote subgroups of $\tilde{\Lambda}_{p^r}$.

Corollary 4.3.1. *On $\tilde{\Lambda}_{p^r}$, M is similar to a block diagonal matrix $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ over R_r, where A is invertible and B is nilpotent of nil-degree $n(B)$ say. The block matrices A and B are unique up to similarity. The direct sum from Fact* 4.1.2 *now reads*

$$\tilde{\Lambda}_{p^r} = \mathrm{Fix}(M^{\mathrm{ord}(A,p^r)}) \oplus \ker(M^{n(B)}),$$

where the concrete form of the exponents k and m of Fact 4.1.2 *follows from the block diagonal structure of M chosen. Here, $\mathrm{Fix}(M^{\mathrm{ord}(A,p^r)}) \simeq R_r^{d'}$ and $\ker(M^{n(B)}) \simeq R_r^{d-d'}$, where one has $d' = \mathrm{rank}\,(\mathrm{per}(M)) \leq d$.*

Furthermore, d' is independent of r. When comparing the above objects as modules over the ring R_s for different s, one has

$$\mathrm{rank}_1(\mathrm{per}_1(M)) = \mathrm{rank}_r(\mathrm{per}_r(M)) = d' \quad \textit{and}$$
$$\mathrm{rank}_1(\ker_1(M^{m(1)})) = \mathrm{rank}_r(\ker_r(M^{m(r)})) = d - d',$$

where an index s at per, ker *or* rank *refers to R_s as the underlying ring.*

Proof. The diagonal block-matrix structure is clear from [1, Props. 4.3.28 and 4.3.23], while the isomorphism claim follows from [54, Cor. III.4.3].

For the last claim, observe that A and B can be viewed as integer matrices acting on $R_r^{d'}$ and $R_r^{d-d'}$, respectively. Here, $B^s = 0 \bmod p^r$ for some $s \in \mathbb{N}$ and $\gcd(\det(A), p) = 1$, because A is invertible mod p^r and $\det(A)$ must be a unit in R_r. But this means that the reduction of $A \bmod p$ is also invertible over $R_1 = \mathbb{Z}/p\mathbb{Z}$, while the reduction of $B \bmod p$ is still nilpotent. Consequently, these reductions provide the blocks for the direct sum over $\tilde{\Lambda}_p$, and the claim is obvious. □

Since two free modules of the same rank are isomorphic [54, Cor. III.4.3], we also have the following consequence.

Corollary 4.3.2. *One has the following isomorphisms of R_1-modules (as $\mathbb{F}_p$-vector spaces),*

$$\mathrm{per}_r(M)/p\,\mathrm{per}_r(M) \simeq \mathrm{per}_1(M) \quad \textit{and} \quad \ker_r(M^{m(r)})/p\ker_r(M^{m(r)}) \simeq \ker_1^{(d)}(M^{m(1)}).$$

This implies

$$\left|\mathrm{per}_r(M)\right| = p^{rd'} = \left|\mathrm{per}_1(M)\right|^r \quad \textit{and} \quad \left|\ker_r(M^{m(r)})\right| = p^{r(d-d')} = \left|\ker_1(M^{m(1)})\right|^r$$

for the cardinalities of the finite modules. □

At this point, it is reasonable to link the properties of M on $\tilde{\Lambda}_{p^r}$ to its minimal polynomial over $\mathbb{F}_p$.

Lemma 4.3.3. *If M is similar mod p to the block diagonal matrix of Corollary 4.3.1, its minimal polynomial over $\mathbb{F}_p$ is $\mu_M(x) = x^s f(x)$, where f is a monic polynomial of order k over $\mathbb{F}_p$ with $f(0) \neq 0$. When M is invertible, one has $s = 0$ and $k = \gcd\{\ell \in \mathbb{N} \mid M^\ell \equiv \mathbb{1} \bmod p\}$. When M is nilpotent, $f = 1$ and $s = \gcd\{t \in \mathbb{N} \mid M^t \equiv 0 \bmod p\}$. In all remaining cases, s and k are the smallest positive integers such that $B^s \equiv 0$ and $A^k \equiv \mathbb{1} \bmod p$. If μ_M equals the characteristic polynomial, s and $\deg(f)$ are the dimensions of $\ker(M^s)$ and $\mathrm{per}(M)$, respectively.*

Proof. Recall from [56, Def. 3.3.2] that the order of a polynomial $f \in \mathbb{F}_p[x]$ with $f(0) \neq 0$, denoted by $\mathrm{ord}(f, p)$, is the smallest positive integer ℓ such that $f(x)|(x^\ell - 1)$. When M is invertible and k as claimed, the polynomial $x^k - 1$ annihilates M. Since $\mu_M(0) \neq 0$ in our case, we have $\mu_M = f$ with $f(x)|(x^k - 1)$, so that $\mathrm{ord}(f, p)|k$ by [56, Lemma 3.3.6]. By construction, k is also the minimal positive integer such that $x^k - 1$ annihilates M, hence $k = \mathrm{ord}(f, p)$.

When M is nilpotent, the claim is obvious, because 0 is then the only possible root of the minimal polynomial over $\mathbb{F}_p$, as all other elements of the splitting field of f are units.

In all remaining cases, M is similar to $A \oplus B$ with A invertible and B nilpotent, by Corollary 4.3.1. We thus know that $\mu_M(x)|x^s(x^k - 1)$ with s and k as claimed, since the latter annihilates both A and B. Observe that $B^s(B^k - \mathbb{1}) \equiv 0 \bmod p$ means $B^{k+s} \equiv B^s \bmod p$. Since B is nilpotent, its powers cannot return to a non-zero matrix, hence $B^s \equiv 0 \mod p$. Similarly, $A^{s+k} \equiv A^s \bmod p$ is equivalent with $A^k \equiv \mathbb{1} \bmod p$, as A is invertible. This shows that we must indeed have $\mu_M(x) = x^s f(x)$ with $\mathrm{ord}(f, p) = k$. □

This implies the following bound on the nil-degree of the nilpotent part of M on $\tilde{\Lambda}_{p^j}$.

Corollary 4.3.4. *Let M, B and s as in the last lemma. Then for all $j \geq 1$, an upper bound on the nil-degree modulo p^j of B, is given by sj.* □

The decomposition of $\tilde{\Lambda}_{p^r}$ given in Corollary 4.3.1 justifies to focus on (locally) invertible maps on the one hand (as happened in most of Section 3) and nilpotent maps on the other hand.

The decomposition of the kernel of the powers is analogous with that of $\mathrm{Fix}(M^k)$.

Recall from Proposition 3.2.2 that, for M an integer matrix with Smith normal form $\mathrm{SNF}(M) = \mathrm{diag}(a_1, \ldots, a_d)$ over $\mathbb{Z}$, and $j_i = \min(r, v_p(a_i))$, one has the following isomorphism of Abelian groups,

$$\ker_r(M) \simeq \mathbb{Z}/p^{j_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{j_d}\mathbb{Z} \quad \text{and} \quad M(\tilde{\Lambda}_{p^r}) \simeq \mathbb{Z}/p^{r-j_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{r-j_d}\mathbb{Z}.$$

In particular, for the orders, one has

$$|\ker_r(M)| = \prod_{j=1}^{d} p^{j_i} = p^{\sum_{i=1}^d j_i} \quad \text{and} \quad \left|M(\tilde{\Lambda}_{p^r})\right| = \prod_{j=1}^{d} p^{r-j_i} = p^{dr - \sum_{i=1}^d j_i}.$$

Thus, the group types, which determine a p-group up to isomorphism can be read off from the SNF of the corresponding powers of M.

Since for the lattices $\tilde{\Lambda}_{p^r}$, all kernels are p-groups, the orders β_i from Proposition 4.2.2 are powers of p. Hence, in order to characterise a tree up to isomorphism, only the exponents of the subgroup orders are necessary. Let $\beta_i = p^{\ell_i}$ for $0 \leq i \leq h-1$, then $\left|\ker(M^h)\right| = \prod_{i=0}^{h-1} \beta_i = p^{\ell_0 + \ldots + \ell_{h-1}}$. Consequently, each tree induced by a locally nilpotent toral endomorphism on the lattice $\tilde{\Lambda}_{p^r}$ corresponds to a partition of $r\,d$. In this case, Proposition 4.2.2 reads

Proposition 4.3.5. *The pretail tree of a nilpotent $d \times d$ matrix is characterised up to isomorphism by a sequence of integers $\ell_0 \geq \ell_1 \geq \ldots \geq \ell_{h-1}$ such that $\sum_{i=0}^{h-1} \ell_i = rd$. In particular, two matrices have isomorphic pretail trees on $\tilde{\Lambda}_{p^r}$, if and only if the kernels of all of their powers share the same cardinalities.*

The number of non-isomorphic trees induced on $\tilde{\Lambda}_{p^r}$ is thus bounded by

$$\sum_{d'=0}^{d} \mathfrak{p}(d'r) = 1 + \sum_{d'=1}^{d} \mathfrak{p}(d'r),$$

where $\mathfrak{p}(n)$ is the partition function that counts how many different partitions of n exist (cf. A000041 from [75]). □

Example 4.2. Since the possible partitions induced by integer matrices M are constrained by the growth of the minors of powers of M with respect to their p-valuation, not all combinatorially possible partitions are realised on each lattice $\tilde{\Lambda}_{p^r}$, p prime, $r \in \mathbb{N}$. Consider, for instance, the lattice $\tilde{\Lambda}_{p^4}$. The number of combinatorially possible pretail trees is $1 + \mathfrak{p}(4) + \mathfrak{p}(8) = 1 + 5 + 22 = 28$. However, the complete enumeration of all 2×2 integer matrices on $\tilde{\Lambda}_{p^4}$ for $p = 3$ shows that the partitions $\{2, 1, 1\}$ (of 4) and $\{2, 1, 1, 1, 1, 1, 1, 1\}$, $\{2, 2, 1, 1, 1, 1\}$, $\{3, 1, 1, 1, 1, 1\}$, $\{3, 2, 2, 1\}$ and $\{6, 1, 1\}$ (of 8) do not show up. ◊

In terms of the above parametrisation of pretail trees, it is clear that a pretail tree is perfect up to depth k if and only if $\ell_0 = \ldots = \ell_{k-1}$, so precisely the partitions with only identical elements correspond to perfect trees.

It is a natural question to ask which partitions are realised on the lattice $\tilde{\Lambda}_{p^r}$ and with what frequencies (that is, their distribution). A necessary condition for the existence of an endomorphism inducing a certain tree associated with some given partition is the existence of a chain of subgroups H_i that have types and cotypes (that is, the types of the factor groups $\tilde{\Lambda}_{p^r}/H_i$) which are compatible with the orders of kernel and image of powers of the endomorphism. Note that different group types can induce the same partition and thus isomorphic pretail trees. For enumerations of subgroups of given types and related questions see e.g. [24]. This question, in generality, will be pursued elsewhere.

For the prime lattices $\tilde{\Lambda}_p$, it is considerably easier to enumerate all possible tree structures; all submodules are in fact vector spaces and thus have a basis. In the next section, the formulae for calculating the numbers of occurrences of each partition will be given.

4.4 Classification on $\tilde{\Lambda}_p$

Working over the finite field $\mathbb{F}_p$, nilpotent matrices can be classified according to their Jordan normal form. This follows from the fact that 0 is the only possible eigenvalue of a nilpotent matrix over a field. Recall that an *elementary shift matrix* is an upper triangular matrix with entries 1 on the upper super-diagonal and 0 everywhere else (this includes the 0-matrix in one dimension). An elementary $(d \times d)$ shift matrix is nilpotent, with nil-degree d. The following result is now a standard consequence of the Jordan normal form over fields [45, 54].

Fact 4.4.1. *The nilpotent matrices in $\mathrm{Mat}(d, \mathbb{F}_p)$ are conjugate to block-diagonal matrices, where each block is an elementary shift matrix.* □

Some of this structure survives also for general n. For instance, the 0-matrix in dimension $d \geq 1$ leads to the regular $(n^d - 1)$-star as its pretail tree on $\tilde{\Lambda}_n$. When $d \geq 2$, the d-dimensional

elementary shift matrix, on $\tilde{\Lambda}_n$, results in a perfect pretail tree of height d. Note however, that for general n, the elementary shift matrices do not provide a complete set of normal forms for nilpotent matrices, whereas on $\tilde{\Lambda}_p$, one could go through all possible block-diagonal combinations of such elementary shift matrices to obtain the possible pretail trees on $\tilde{\Lambda}_p$.

In the following paragraph, we will count the ways to construct all linear mappings that induce a certain pretail tree on $\tilde{\Lambda}_p$ by means of choosing subspaces, and thus also get the 'class sizes'.

4.4.1 Numbers of tree types

Over $\mathbb{F}_p$, all submodules are vector spaces and thus free. In particular, the submodules $\ker(M^j)$ for $j \geq 1$ can be identified with a subspace of $\mathbb{F}_p^d$, which admits a basis. Consequently, the number of occurrences of each tree, parametrised by the partitions from Section 4.3, can be calculated in terms of choices of subspaces of $\mathbb{F}_p^d$, and possible images for basis vectors.

Let $S_{d,\ell}$ denote the number of subspaces of $\mathbb{F}_p^d$ of dimension ℓ, which is given in terms of the Gaussian binomial coefficients $\left[\begin{smallmatrix} d \\ \ell \end{smallmatrix}\right]_p$, also known as q-analogues of the binomial coefficients. More precisely, one has

$$S_{d,\ell} = \left[\begin{smallmatrix} d \\ \ell \end{smallmatrix}\right]_p = \frac{(1-p^d)(1-p^{d-1})\cdot\ldots\cdot(1-p^{d-\ell+1})}{(1-p)(1-p^2)\cdot\ldots\cdot(1-p^\ell)},$$

see, for instance, [67]. As an immediate consequence, one obtains the number of subdivisions into vector spaces corresponding to a partition $\{\ell_0, \ell_1, \ldots, \ell_{h-1}\}$ in the sense of the previous section.

Lemma 4.4.1. *Let $1 \leq \ell_0 \leq \ell_1 \leq \ldots \leq \ell_{h-1}$, $h \geq 1$, such that $\sum_{i=0}^{h-1} \ell_i \leq d$, and let $V_0 \subset V_1 \subset V_2 \subset \ldots \subset V_{h-1}$ be a sequence of subspaces of Λ_p such that $\dim(V_j) = d(j) \coloneqq \sum_{i=0}^{j-1} \ell_i$. The number of choices of such sequences is given by*

$$\prod_{j=0}^{h-1} S_{d-d(j),\ell_j} = \prod_{j=0}^{h-1} \left[\begin{smallmatrix} d-d(j) \\ \ell_j \end{smallmatrix}\right]_p.$$

Proof. Each vector space V_i can be extended to V_{i+1} by choosing ℓ_{i+1} basis vectors in the complement of V_i. □

The following lemma states the number of nilpotent endomorphisms that can be defined on a fixed sequence of subspaces in the sense of the last lemma. Again, let $\dim(V_j) = d(j)$ and, equivalently, $|V_i| = p^{\sum_{k=0}^{i-1} \ell_k}$.

Lemma 4.4.2. *Let $N_{\{\ell_0,\ldots,\ell_{h-1}\}}$ denote the number of endomorphisms that can be built on a fixed sequence of subspaces as in* Lemma 4.4.1. *Then one obtains*

$$N_{\{\ell_0,\ldots,\ell_{h-1}\}} = \prod_{i=1}^{h-1} \prod_{j=0}^{\ell_i - 1} (p^{\sum_{k=1}^{i-1} \ell_k} - p^{\sum_{k=0}^{i-2} \ell_k + j}).$$

Proof. Choose a basis of $\mathbb{F}_p^d$ such that the first $d(j)$ basis vectors are a basis of V_j for $0 \leq j \leq h-1$. Each element in V_0 is mapped to 0. The restriction of an endomorphism to V_i is determined, once an image has been assigned to each basis vector in $V_i \setminus V_{i-1}$. To

extend an endomorphism which is defined on V_i to V_{i+1}, one has to choose images for ℓ_i basis vectors. For the first one, there are $|V_i \setminus V_{i-1}| = p^{\sum_{j=0}^{i-1}\ell_i} - p^{\sum_{j=0}^{i-2}\ell_j}$ choices, for the second one $p^{\sum_{j=0}^{i-1}\ell_i} - p^{1+\sum_{j=0}^{i-2}\ell_j}$ and for the last one $p^{\sum_{j=0}^{i-1}\ell_i} - p^{\ell_i-1+\sum_{j=0}^{i-2}\ell_j}$. That means, one finds

$$\begin{aligned} N_{\{\ell_0,\ldots,\ell_{h-1}\}} &= (p^{\ell_0}-1)(p^{\ell_0}-p)\cdot\ldots\cdot(p^{\ell_0}-p^{\ell_1-1}) \\ &\quad\cdot(p^{\ell_0+\ell_1}-p^{\ell_0})(p^{\ell_0+\ell_1}-p^{\ell_0+1})\cdot\ldots\cdot(p^{\ell_0+\ell_1}-p^{\ell_0+\ell_2-1}) \\ &\quad\vdots \\ &\quad\cdot(p^{\ell_0+\ell_1+\ldots+\ell_{h-2}}-p^{\ell_0+\ldots+\ell_{h-3}})\cdot\ldots\cdot(p^{\ell_0+\ldots+\ell_{h-2}}-p^{\ell_0+\ldots+\ell_{h-3}+\ell_{h-1}-1}) \\ &= \prod_{i=1}^{h-1}\prod_{j=0}^{\ell_i-1}(p^{\sum_{k=0}^{i-1}\ell_k}-p^{\sum_{k=0}^{i-2}\ell_k+j}), \end{aligned}$$

and the formula follows. □

Finally, let $U_{d,d'}$ denote the number of invertible maps on a fixed $(d-d')$-dimensional subspace of $\mathbb{F}_p^d$. By a counting argument (similar to the one for the order of $\mathrm{GL}(d,\mathbb{F}_p)$), one has

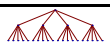
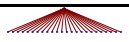
$$U_{d,d'} = (p^d - p^{d'})(p^d - p^{d'+1})\cdot\ldots\cdot(p^d - p^{d-1}).$$

Proposition 4.4.3. *On the prime lattices $\tilde{\Lambda}_p$, all possible partitions are realised. A tree associated with the partition $\{\ell_0,\ldots,\ell_{h-1}\}$ is induced by*

$$\left(\prod_{j=0}^{h-1} S_{d-d(j),\ell_j}\right) N_{\{\ell_0,\ldots,\ell_{h-1}\}} U_{d,\sum_{i=0}^{h-1}\ell_i}$$

different matrices from $\mathrm{Mat}(d,\mathbb{F}_p)$. □

Example 4.3. If $d=2$, the possible pretail trees of endomorphisms on $\tilde{\Lambda}_p$ are characterised by the partition exponents $\{0\},\{1\},\{1,1\}$ and $\{2\}$, corresponding to kernels of order 1, p, p and p^2, respectively. The following table gives the 'class sizes' for each type of pretail tree. In the second column, the trees are drawn for $p=5$.

partition	graph	class size	examples			
			p=2	p=3	p=5	p=7
$\{0\}$		$\lvert\mathrm{GL}(2,\mathbb{F}_p)\rvert = (p^2-1)(p^2-p)$	6	48	480	2016
$\{1\}$		$\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p p(p-1)$	6	24	120	336
$\{1,1\}$		$\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p-1)$	3	8	24	48
$\{2\}$		1	1	1	1	1

A list of the class sizes for $d=3$ and $d=4$ can be found in Appendix B. ◊

4.5 Sequences of pretail trees and the 'global' pretail tree

For the periodic orbits of toral endomorphisms, we have put special emphasis on the local-global picture, whereas for the preperiodic points, we have thus far focused on their local structure. However, considering the union of all rational lattices, it makes sense to define the notion of a *global pretail tree*, consisting of all (rational) points that are finally mapped to 0.

The following corollary is an analogue of Theorem 3.3.1 for locally non-invertible endomorphisms. In the rest of this section, $\ker(M)$ denotes the set of all torus points which are mapped to 0 and $\ker_n(M) = \ker(M) \cap \Lambda_n$ (with the identifications from Section 3.2).

Corollary 4.5.1. *Consider the action of the matrix $M \in \mathrm{Mat}(d, \mathbb{Z})$ on the lattice $\tilde{\Lambda}_n$. Let $\mathrm{SNF}(M) = \mathrm{diag}(a_1, \ldots, a_d)$ and $t_i^{(p)} = \min(v_p(a_i), v_p(n))$. For the kernel $\ker_n(M) \subset \tilde{\Lambda}_n$, one has*

$$|\ker_n(M)| = \prod_{p|n} \prod_{i=1}^{d} p^{t_i^{(p)}} \leq \prod_{p|n} p^{v_p(\det(M))} = \gcd(n, \det(M)).$$

The upper bound is attained if and only if $v_p(a_i) \leq v_p(n)$ for $1 \leq i \leq d$. If the rank of M over $\mathbb{Z}$ is d, one has $|\ker_n(M)| = |\det(M)|$ for $n = |\det(M)|$. In particular, for the global kernel, one has

$$\left|\ker(M^\ell)\right| = \prod_{i=1}^{s} \left|\ker_{p_i^{k_i}}(M^\ell)\right| = \prod_{i=1}^{s} p_i^{v_{p_i}(D^\ell)} = D^\ell,$$

where $D = |\det(M)| = \prod_{i=1}^{s} p_i^{k_i}$ is the prime decomposition of D.

Proof. As Theorem 3.3.1, the case of n being a prime power directly follows from Proposition 3.2.2. Fact 3.2.1 then implies the product formula. □

Let $\{\mathcal{T}_r\}_{r\geq 1}$ denote the sequence of pretail trees on $\tilde{\Lambda}_{p^r}$ of an integer matrix whose determinant does not vanish in $\mathbb{Z}$. Corollary 4.5.1 implies that there is some trivial 'limit' of the sequence of truncated pretail trees for any fixed truncation depth. Let $C_i(p^r)$ be, as in Equation (24), the subgroup of $\ker_{p^r}(M)$ which consists of all nodes that are roots of trees of height $\geq i$, and $\beta_i(p^r) = |C_i(p^r)|$. In fact, we have the following

Theorem 4.5.2. *Let $\{\mathcal{T}_r\}_{r\geq 1}$ be the pretail graph sequence of an integer matrix M on the lattices $\tilde{\Lambda}_{p^r}$ for a fixed prime p. Further assume $\det(M) \neq 0$ in $\mathbb{Z}$.*

(i) For each $k \in \mathbb{N}$, there is some $r \in \mathbb{N}$ such that the pretail graph $\mathcal{T}_r$ is perfect up to depth k. In particular, one has $\left|\ker_{p^r}(M^j)\right| = |\ker_{p^r}(M)|^j$ for $j \in \{1, \ldots, k\}$. For the sequence $\{\beta_i^{(r)}\}_r$, one has $\lim_{r\to\infty} \beta_i^{(r)} = |\ker(M)|$ for all i.

(ii) The global pretail tree is a perfect pretail tree of infinite height. In particular, $\bigcup_{n\geq 1} \Lambda_n \subset M(\mathbb{T}^d)$.

Proof. The first part follows from Corollary 4.5.1 and the multiplicativity of the determinant together with Lemma 4.2.4, which imply $\left|\ker_n(M^j)\right| = |\ker_n(M)|^j$ for all $j \geq 1$ and n sufficiently large, as well as $\beta_0 = \ldots = \beta_{k-1}$. The second part follows from the last equation in Corollary 4.5.1. Since the global pretail tree does not have any leaves, the rational lattices are a subset of the image of $\mathbb{T}^d$ under M. □

Due to the linearity of M, the number of preperiodic points of distance k to some periodic point, i.e. the number of points $x \in \mathbb{T}^d$ such that $M^k x$ is periodic, is infinite whenever the number of periodic points is infinite, as there is a copy of each predecessor of 0 attached to every periodic point. However, these points can be 'grouped' according to the periodic orbits they are attached to. If $\alpha_{n,k}$ denotes the number of preperiodic points x such that $M^k x$ is in an orbit of length n, but $M^{k-1}x$ is not, one has

$$\alpha_{n,k} = n c_n(|D|^k - |D|^{k-1}),$$

where c_n denotes the global orbit counts.

Example 4.4. Reconsider the matrix $M = \left(\begin{smallmatrix} 12 & 4 \\ 1 & 4 \end{smallmatrix}\right)$ whose reduction modulo 8 was the subject of Example 4.1. Let $P_0 = \mathrm{diag}(1, 2^2)$ and $P_1 = \mathrm{diag}(2^2, 1)$, and denote by $n_p(\cdot)$ the componentwise application of $|\cdot|_p^{-1}$ to an integer matrix, i.e. $n_p(A)$ is the matrix whose entries are the powers of p dividing the corresponding entries of the matrix A. One finds $n_p(\mathrm{SNF}(M)) = \mathrm{diag}(1, 2^2)$, $n_p(\mathrm{SNF}(M^2)) = \mathrm{diag}(2^2, 2^2)$, $n_p(\mathrm{SNF}(M^3)) = \mathrm{diag}(2^2, 2^4)$, $n_p(\mathrm{SNF}(M^4)) = \mathrm{diag}(2^4, 2^4)$ and so on, which suggests the general rule

$$n_p(\mathrm{SNF}(M^{k+1})) = P_{(k \bmod 2)} \cdot n_p(\mathrm{SNF}(M^k)).$$

Under the assumption that this is true for general k, we obtain

$$n_p(\mathrm{SNF}(M^{2k})) = \mathrm{diag}(2^{2k}, 2^{2k}) \quad \text{and} \quad n_p(\mathrm{SNF}(M^{2k+1})) = \mathrm{diag}(2^{2k}, 2^{2k+1}). \tag{25}$$

The height of a pretail tree on $\tilde{\Lambda}_n$ for any $n \in \mathbb{N}$, is the largest integer h such that $\left|\ker_n(M^h)\right| > \left|\ker_n(M^{h-1})\right|$. Hence, on $\tilde{\Lambda}_{2^{2k}}$, the pretail tree induced by M has height $2k$; on $\tilde{\Lambda}_{2^{2k+1}}$, it has height $2k + 2$.

Further, still assuming (25), on $\tilde{\Lambda}_{p^{2k}}$, one has $\left|\ker_{p^{2k}}(M^{2k})\right| = 2^{4k} = \left|\ker_{p^{2k}}(M)\right|^{2k}$, which means the pretail tree is perfect according to Lemma 4.2.4.

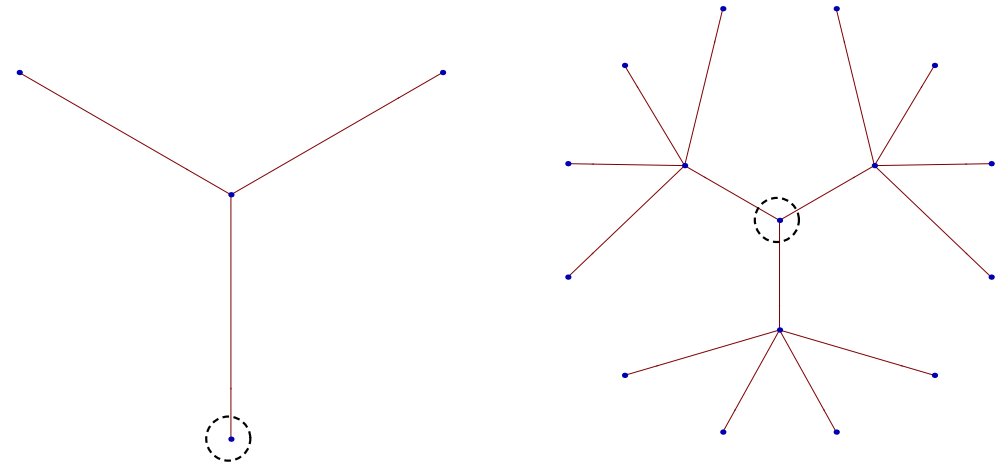
On $\tilde{\Lambda}_{2^{2k+1}}$, one has $\left|\ker_{p^{2k+1}}(M^{2k})\right| = 2^{4k} = \left|\ker_{p^{2k}}(M)\right|^{2k}$, and $\left|\ker_{p^{2k+1}}(M^{2k+1})\right| = 2^{4k+1} \neq \left|\ker_{p^{2k}}(M)\right|^{2k+1}$. Thus, on $\tilde{\Lambda}_{2^{2k+1}}$, the pretail tree is not perfect, but only perfect up to depth $2k-1$. In particular, the difference between the minimal and maximal pretail length is 2.

The first six trees of the sequence are shown in Figure 6. ◊

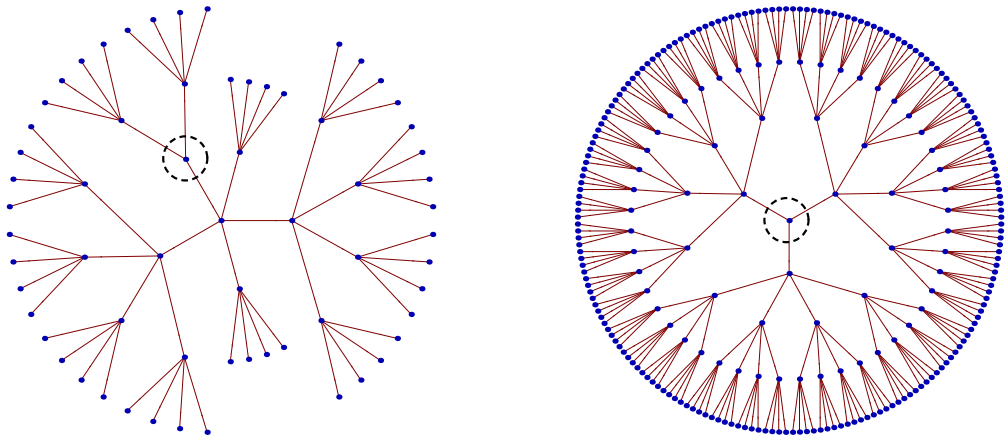
Due to the regular p-growth of the minors of powers of M, one observes a similar behaviour for arbitrary pretail tree sequences, and this gives a heuristic explanation for the "self-similarity" of the growing trees. Note however, that in general there need not be any lattices on which the pretail tree is perfect.

In the remaining case of $\det(M) = 0$, most of the above said is still true as long as only an individual lattice is considered. However, analogously with M having eigenvalues on the unit circle, the kernel of M is dense if $\det(M) = 0$. While in the former case, one has subtori of fixed points, in the latter case, subtori exist which are completely mapped to 0. As a consequence, the kernel $\ker_{p^r}(M^j)$ does not stabilise then, i.e. $\left|\ker_{p^r}(M^j)\right|$ is not bounded in r.

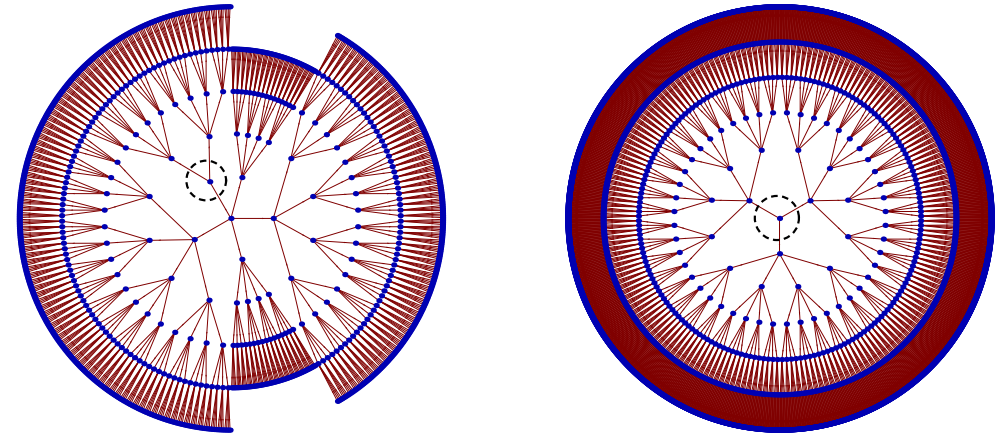
Remark 4.3. As one can see from the fact that only the orders, not the group structures are relevant for the structure of the pretail tree, any single local pretail tree is a rather weak invariant of a toral endomorphism. However, the sequence of pretail trees also reveals the group structure of the kernels of the matrix powers, and is thus a characteristic invariant.



(a) $\tilde{\Lambda}_2$ (b) $\tilde{\Lambda}_4$



(c) $\tilde{\Lambda}_8$ (d) $\tilde{\Lambda}_{16}$



(e) $\tilde{\Lambda}_{32}$ (f) $\tilde{\Lambda}_{64}$

Figure 6: The pretail tree sequence of $\left(\begin{smallmatrix}12 & 4\\ 1 & 4\end{smallmatrix}\right)$ on $\tilde{\Lambda}_2$ through $\tilde{\Lambda}_{2^6}$. The node corresponding to 0 is encircled in each graph.

5 Symmetry and reversibility

Reversibility is an important concept in dynamics, compare [69] and references therein for background, and [31] for an early study in continuous dynamics. Here, we focus on discrete dynamics, as, for instance, induced by toral auto- and endomorphisms.

A matrix M is called *reversible*, within a given or specified matrix group $\mathcal{G}$, if it is conjugate to its inverse within $\mathcal{G}$. Clearly, this is only of interest when $M^2 \neq \mathbb{1}$. To put this into perspective, one usually defines

$$\mathcal{S}(M) = \{G \in \mathcal{G} \mid GMG^{-1} = M\} \quad \text{and} \quad \mathcal{R}(M) = \{G \in \mathcal{G} \mid GMG^{-1} = M^{\pm 1}\}$$

as the *symmetry* and *reversing symmetry* groups of M; see [14] and references therein for background and [12, 13] for examples in our present context. In particular, one always has $\mathcal{R}(M) = \mathcal{S}(M)$ when $M^2 = \mathbb{1}$ or when M is not reversible, while $\mathcal{R}(M)$ is an extension of $\mathcal{S}(M)$ of index 2 otherwise.

The groups $\mathcal{S}(M)$ and $\mathcal{R}(M)$ are clearly conjugacy invariants of M up to isomorphism. Indeed, if $M_2 = TM_1T^{-1}$ with some invertible matrix T, then for every (reversing) symmetry S of M_1, the matrix TST^{-1} is a (reversing) symmetry for M_2.

In the context of physical systems, time reversal symmetry is an important property, and the corresponding symmetry T is then an involution, i.e. $T^2 = \mathrm{id}$. When a reversing symmetry (of a map M) is an involution, we will also say that M has an *involutory reversor*. More generally, when an automorphism F with $F^2 \neq \mathrm{id}$ of some (topological) space has an involutory reversor, its reversing symmetry group has the structure of a semidirect product, $\mathcal{R}(F) \simeq \mathcal{S}(F) \rtimes C_2$, where C_2 denotes the cyclic group of order 2, see [12, Lemma 2]. Here, $\mathcal{S}(F)$ is the normal subgroup of $\mathcal{R}(F)$ and C_2 is generated by the involutory reversor. In the following, direct products of groups will be denoted by '$\times$', and for $i \geq 1$, C_i denotes the cyclic group with i elements. (It is unrelated to the groups C_i in Section 4.2).

Note that a nilpotent matrix M (or a matrix with nilpotent summand, as in Corollary 4.3.1) cannot be reversible in this sense. However, it can still possess interesting and revealing symmetry groups, although it is often more natural to look at the ring of matrices that commute with M in this case.

Example 5.1. Reconsider the matrix $M = \left(\begin{smallmatrix} 4 & 4 \\ 1 & 4 \end{smallmatrix}\right)$ from Example 4.1, and its action on $\tilde{\Lambda}_8$. Clearly, M commutes with every element of the ring $\mathbb{Z}/8\mathbb{Z}\,[M]$, which contains 64 elements. This follows from the existence of a cyclic vector, but can also be checked by a simple direct calculation. Consequently, the symmetry group (in our above sense) is the intersection of this ring with $\mathrm{GL}(2, \mathbb{Z}/8\mathbb{Z})$, which results in

$$\mathcal{S}(M) \,=\, \left\langle \left(\begin{smallmatrix} 1 & 4 \\ 1 & 1 \end{smallmatrix}\right), 3{\cdot}\mathbb{1}, 5{\cdot}\mathbb{1} \right\rangle \,\simeq\, C_8 \times C_2 \times C_2,$$

which is an Abelian group of order 32. The matrices in $\mathcal{S}(M)$ have either determinant 1 or 5, with $\{A \in \mathcal{S}(M) \mid \det(A) = 1\} \simeq C_4 \times C_2 \times C_2$.

One can now study the action of $\mathcal{S}(M)$ on the pretail graph of Figure 4, which actually explains all its symmetries. $\Diamond$

In what follows, we derive certain general properties, where we focus on the reversing symmetry group, with invertible matrices M in mind.

5.1 Reversibility of $\mathrm{SL}(2,\mathbb{Z})$-matrices mod n

Recall the matrix mgcd from Equation (18), which is a conjugacy invariant. It can be used to solve the reversibility at hand as follows.

Theorem 5.1.1. *Let $M \in \mathrm{SL}(2,\mathbb{Z})$ and $n \in \mathbb{N}$ be arbitrary. Then, the reduction of M mod n is conjugate to its inverse within the group $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$. The action mod 1 of any $M \in \mathrm{SL}(2,\mathbb{Z})$ on Λ_n is thus reversible for all $n \in \mathbb{N}$.*

Moreover, if $M \in \mathrm{SL}(2,\mathbb{Z})$ has $\mathrm{mgcd}(M) = r \neq 0$, its reduction mod n, for every $n \in \mathbb{N}$, possesses an involutory reversor.

Proof. When $M \in \mathrm{SL}(2,\mathbb{Z})$, also its inverse is in $\mathrm{SL}(2,\mathbb{Z})$, and M and M^{-1} share the same determinant and trace. Moreover, they also have the same mgcd, so that the first claim follows from [16, Thm. 2]. This immediately implies, for all $n \in \mathbb{N}$, the reversibility of the action mod n of M on the lattice $\tilde{\Lambda}_n$, so that the statement on the equivalent action of M mod 1 on Λ_n is clear.

Now, let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, so that $M^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, and M and M^{-1} share the same determinant (1), trace $(a+d)$ and mgcd (r). Assume $r \neq 0$, let $n \geq 2$ be fixed and consider the matrices mod n. Recall the normal forms

$$N(M) = \begin{pmatrix} a & \frac{bc}{r} \\ r & d \end{pmatrix} \quad \text{and} \quad N(M^{-1}) = \begin{pmatrix} d & \frac{bc}{r} \\ r & a \end{pmatrix},$$

as defined in the proof of [16, Prop. 6], and note that they are not inverses of each other. However, by [16, Prop. 5], there is some matrix $P_n \in \mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ with $M = P_n N(M) P_n^{-1}$, hence we also have $M^{-1} = P_n \big(N(M)\big)^{-1} P_n^{-1}$. Observe next that

$$\big(N(M)\big)^{-1} = \begin{pmatrix} d & -\frac{bc}{r} \\ -r & a \end{pmatrix} = C \begin{pmatrix} d & \frac{bc}{r} \\ r & a \end{pmatrix} C^{-1} = C N(M^{-1}) C^{-1},$$

where $C = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is an involution. On the other hand, $N(M)$ and $N(M^{-1})$ satisfy the assumptions of [16, Prop. 6], so that

$$N(M^{-1}) = A N(M) A^{-1} \quad \text{with} \quad A = \begin{pmatrix} 1 & \frac{d-a}{r} \\ 0 & 1 \end{pmatrix},$$

where we globally have $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ whenever $d = a$ in the original matrix M. Together with the previous observation, this implies $\big(N(M)\big)^{-1} = (CA) N(M) (CA)^{-1}$ where

$$CA = \begin{pmatrix} 1 & \frac{d-a}{r} \\ 0 & -1 \end{pmatrix}$$

is an involution. Putting everything together, we have

$$M^{-1} = \big(P_n (CA) P_n^{-1}\big) M \big(P_n (CA) P_n^{-1}\big)^{-1},$$

which is the claimed conjugacy by an involution (which depends on n in general). □

Note that the matrix M in Theorem 5.1.1 need not be reversible in $\mathrm{GL}(2,\mathbb{Z})$, as the example $M = \left(\begin{smallmatrix} 4 & 9 \\ 7 & 16 \end{smallmatrix}\right)$ from [12, Ex. 2] shows. Nevertheless, for any $M \in \mathrm{SL}(2,\mathbb{Z})$ with $\mathrm{mgcd}(M) \neq 0$ and $n \geq 2$, the (finite) reversing symmetry group of M within $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ is always of

the form $\mathcal{R}(M) \simeq \mathcal{S}(M) \rtimes C_2$, with C_2 being generated by the involutory reversor. In fact, admitting local symmetries on all ("relevant") lattices despite the absence of global symmetries, may have consequences for the eigenvalue statistics in the corresponding quantised systems, cf. [49]. The structure of $\mathcal{S}(M)$ remains to be determined.

In the formulation of Theorem 5.1.1, we have focused on matrices $M \in \mathrm{SL}(2,\mathbb{Z})$ because the condition $\mathrm{tr}(M) = \mathrm{tr}(M^{-1})$ for a matrix M with $\det(M) = -1$ forces $\mathrm{tr}(M) = 0$, which means that M is itself an involution (and thus trivially reversible in $\mathrm{GL}(2,\mathbb{Z})$). More interesting (beyond Theorem 5.1.1) is the question which matrices $M \in \mathrm{Mat}(2,\mathbb{Z})$, when considered mod n for some $n \in \mathbb{N}$, are reversible in $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$. Let us begin with $n = p$ being a prime, where $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$ is the finite field with p elements.

5.2 Reversibility in $\mathrm{GL}(2,\mathbb{F}_p)$

Let us consider the symmetry and reversing symmetry group of an element of $\mathrm{GL}(2,\mathbb{F}_p)$ with p prime, the latter being a group of order

$$|\mathrm{GL}(2,\mathbb{F}_p)| \,=\, (p^2-1)(p^2-p) \,=\, p(p-1)^2(p+1),$$

compare Equation (3). For our further discussion, it is better to distinguish $p = 2$ from the odd primes. For convenience, we summarise the findings also in Table 1.

Example 5.2. For $p = 2$, one has $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) \simeq D_3$, the latter denoting the dihedral group of order 6. There are now three conjugacy classes to consider, which may be represented by the matrices $\mathbb{1}$, the involution $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and the matrix $M = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ of order 3. The corresponding cycle structure on Λ_2 is encapsulated in the generating polynomials $Z_2(t)$. They read

$$(1-t)^4\,, \quad (1-t)^2(1-t^2) \quad \text{and} \quad (1-t)(1-t^3),$$

respectively, and apply to entire conjugacy classes of matrices.

For the (reversing) symmetry groups, one clearly has $\mathcal{R}(\mathbb{1}) = \mathcal{S}(\mathbb{1}) = \mathrm{GL}(2,\mathbb{F}_2)$, while $\mathcal{R}(R) = \mathcal{S}(R) = \langle R\rangle \simeq C_2$. The only nontrivial reversing symmetry group occurs in the third case, where $\mathcal{S}(M) = \langle M\rangle \simeq C_3$. Since $RMR = M^2 = M^{-1}$, one has $\mathcal{R}(M) = \mathrm{GL}(2,\mathbb{F}_2) \simeq C_3 \rtimes C_2$. So, all elements of $\mathrm{GL}(2,\mathbb{F}_2)$ are reversible, though only M and M^2 are nontrivial in this respect. $\Diamond$

For p an odd prime, one can use the normal forms for $\mathrm{GL}(2,\mathbb{F}_p)$, see [54, Ch. XVIII.12], to formulate the results; compare Table 1. We summarise the reversibility and orbit structure here, but omit proofs whenever they emerge from straight-forward calculations. Recall that, for an element of $\mathrm{Mat}(d,\mathbb{Z})$, viewed as a matrix over $\mathbb{Z}/p\mathbb{Z}$, the type of equivalence class is essentially determined by the splitting behaviour of the characteristic polynomial. Specifically, for 2×2 matrices, the Legendre symbol encodes the splitting behaviour, cf. section 3.7.1.

I. The first type of conjugacy class is represented by matrices $M = a\mathbb{1}$ with $a \in \mathbb{F}_p^\times \simeq C_{p-1}$. The order of M coincides with the order of a mod p, $\mathrm{ord}(a,p)$, which divides $p-1$. One clearly has $\mathcal{R}(M) = \mathcal{S}(M) = \mathrm{GL}(2,\mathbb{F}_p)$ in this case, either because $a^2 = 1$ (so that $M = M^{-1}$) or because $a^2 \neq 1$ (so that no reversors are possible). The corresponding orbit structure on Λ_p comprises one fixed point ($x = 0$) together with $\frac{p^2-1}{\mathrm{ord}(a,p)}$ orbits of length $\mathrm{ord}(a,p)$. The non-trivial orbits starting from some $x \neq 0$ must all be of this form, as x gets multiplied by a under the action of M and returns to itself precisely when $a^k = 1$, which first happens for $k = \mathrm{ord}(a,p)$.

II. The next type of conjugacy class is represented by matrices $M = \left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ with $a \in \mathbb{F}_p^\times$. Its symmetry group is given by

$$\mathcal{S}(M) \,=\, \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right) \,\middle|\, \alpha \in \mathbb{F}_p^\times,\, \beta \in \mathbb{F}_p \right\} \,\simeq\, C_p \times C_{p-1},$$

which is Abelian. As generators of the cyclic groups, one can choose $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, which has order p in $\mathrm{GL}(2,\mathbb{F}_p)$, and $\gamma\mathbb{1}$, with γ a generating element of $\mathbb{F}_p^\times$. The reversible cases are precisely the ones with $a^2 = 1$ in $\mathbb{F}_p$, hence with $\det(M) = 1$. Here, $R = \mathrm{diag}(1,-1)$ is a possible choice for the (involutory) reversor, so that $\mathcal{R}(M) = \mathcal{S}(M) \rtimes \langle R \rangle \simeq (C_p \times C_{p-1}) \rtimes C_2$.

A matrix M of type II (in its normal form as in Table 1) satisfies

$$M^k = \begin{pmatrix} a^k & k a^{k-1} \\ 0 & a^k \end{pmatrix} \qquad \text{for } k \geq 0\,,$$

whence a point $(x,0)$ with $x \neq 0$ is fixed by M^k if and only if $k = \mathrm{ord}(a,p)$, and a point (x,y) with $xy \neq 0$ if and only if $p|k$ and $\mathrm{ord}(a,p)|k$. Since $\mathrm{ord}(a,p)|(p-1)$, one has $\mathrm{lcm}(p,\mathrm{ord}(a,p)) = 1$, wherefore this gives $\frac{p-1}{\mathrm{ord}(a,p)}$ orbits of length $p-1$ and $\frac{p\cdot(p-1)}{p\cdot\mathrm{ord}(a,p)} = \frac{p-1}{\mathrm{ord}(a,p)}$ orbits of length $p\,\mathrm{ord}(a,p)$ in total.

III. The third type of conjugacy class is represented by $M = \mathrm{diag}(a,b)$ with $a,b \in \mathbb{F}_p^\times$ and $a \neq b$. This results in $\mathcal{S}(M) = \{\mathrm{diag}(\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_p^\times\} \simeq C_{p-1}^2$. The condition for reversibility leads either to $a^2 = b^2 = 1$, hence to $b = -a$, or to $ab = 1$. In the former case, M itself is an involution, so that $\mathcal{R}(M) = \mathcal{S}(M)$ is once again the trivial case, while $\det(M) = ab = 1$ leads to genuine reversibility, with involutory reversor $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and hence to $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$.

For a type III matrix, one has $M^k(x,y)^t = (a^k x, b^k y)^t$, so each of the $p-1$ non-zero points $(x,0)^t$ is fixed by $M^{\mathrm{ord}(a,p)}$; analogously, each of the $p-1$ non-zero points $(0,y)^t$ is fixed by $M^{\mathrm{ord}(b,p)}$. The remaining points that are non-zero in both coordinates have period $\mathrm{lcm}(\mathrm{ord}(a,p),\mathrm{ord}(b,p))$. In summary, this gives one fixed point, $\frac{p-1}{\mathrm{ord}(a,p)}$ orbits of length $\mathrm{ord}(a,p)$, $\frac{p-1}{\mathrm{ord}(b,p)}$ orbits of length $\mathrm{ord}(b,p)$, and $\frac{(p-1)^2}{\mathrm{lcm}(\mathrm{ord}(a,p),\mathrm{ord}(b,p))}$ orbits of length $\mathrm{lcm}(\mathrm{ord}(a,p),\mathrm{ord}(b,p))$.

IV. Finally, the last type of conjugacy class can be represented by companion matrices of the form $\left(\begin{smallmatrix} 0 & -D \\ 1 & T \end{smallmatrix}\right)$ with the condition that the characteristic polynomial $z^2 - Tz + D$ is irreducible over $\mathbb{F}_p$. The determinant and the trace satisfy $D = \eta\eta'$ and $T = \eta + \eta'$, where η and η' are not in $\mathbb{F}_p$, but distinct elements of the splitting field of the polynomial, which can be identified with $\mathbb{F}_{p^2}$. One consequence is that $1 + D \pm T = (1 \pm \eta)(1 \pm \eta') \neq 0$.

The symmetry group is $\mathcal{S}(M) = \{\alpha\mathbb{1} + \gamma M \mid \alpha,\gamma \in \mathbb{F}_p, \text{ not both } 0\}$, which is an Abelian group with $p^2 - 1$ elements. The order follows from the observation that $\det(\alpha\mathbb{1} + \gamma M) = (\alpha + \gamma\eta)(\alpha + \gamma\eta')$ vanishes only for $\alpha = \gamma = 0$ in this case. In fact, one has $\mathcal{S}(M) \simeq C_{p^2-1}$, as any matrix $\left(\begin{smallmatrix} 0 & -\eta\eta' \\ 1 & \eta+\eta' \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_p)$ with $\eta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ has order $p^2 - 1$ or possesses a root in $\mathrm{GL}(2,\mathbb{F}_p)$ of that order. This relies on the facts that we can always write $\eta = \lambda^m$, where λ is a generating element of $\mathbb{F}_{p^2}^\times \simeq C_{p^2-1}$, and that $\lambda\lambda'$ and $\lambda + \lambda'$ are in $\mathbb{F}_p$. This is a special case of Fact 5.4.2 below and of a statement on the existence of roots in $\mathrm{GL}(d,\mathbb{Z})$; see Lemma 5.4.1 below.

The condition for reversibility, in view of the above restriction on D and T, can only be satisfied when $D = 1$, in which case $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ turns out to be an involutory reversor, so that again $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$ in this case.

Table 1: Summary of conjugacy structure for $\mathrm{GL}(2,\mathbb{F}_p)$ via normal forms. Note that class III is absent for $p=2$. The second possibility for $\mathcal{R}(M)$ always applies when $\det(M)=1$. Only non-trivial orbits are counted.

class	I	II	III	IV
normal form	$a\mathbb{1}$	$\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & -D \\ 1 & T \end{smallmatrix}\right)$
of matrix class	$a \in \mathbb{F}_p^\times$	$a \in \mathbb{F}_p^\times$	$a \neq b \in \mathbb{F}_p^\times$	$z^2 - Tz + D$ irred.
min. polynomial	$(z-a)$	$(z-a)^2$	$(z-a)(z-b)$	$z^2 - Tz + D$
size of class	1	p^2-1	p^2+p	p^2-p
no. of classes	$p-1$	$p-1$	$\frac{1}{2}(p-1)(p-2)$	$\frac{1}{2}p(p-1)$
$\mathcal{S}(M)$	$\mathrm{GL}(2,\mathbb{F}_p)$	$C_p \times C_{p-1}$	$C_{p-1} \times C_{p-1}$	C_{p^2-1}
$\mathcal{R}(M)$	$\mathcal{S}(M)$	$\mathcal{S}(M)$ or $\mathcal{S}(M) \rtimes C_2$	$\mathcal{S}(M)$ or $\mathcal{S}(M) \rtimes C_2$	$\mathcal{S}(M)$ or $\mathcal{S}(M) \rtimes C_2$
orbit length	$\mathrm{ord}(a,p)$	see text	see text	$\mathrm{ord}(\chi_M, p)$
orbit count	$\frac{p^2-1}{\mathrm{ord}(a,p)}$	see text	see text	$\frac{p^2-1}{\mathrm{ord}(\chi_M,p)}$

Matrices with irreducible characteristic polynomial χ_M produce orbits of one length r only, cf. also Theorem 3.8.2, where r is the smallest integer such that $\chi_M(z)|(z^r-1)$, or, equivalently, the order of its roots in the extension field $\mathbb{F}_{p^2}$.

Putting these little exercises together gives the following result.

Theorem 5.2.1. *A matrix $M \in \mathrm{GL}(2,\mathbb{F}_p)$ is reversible within this group if and only if $M^2 = \mathbb{1}$ or $\det(M) = 1$. Whenever $M^2 = \mathbb{1}$, one has $\mathcal{R}(M) = \mathcal{S}(M)$. If $\det(M) = 1$ with $M^2 \neq \mathbb{1}$, there exists an involutory reversor, and one has $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$.* □

Remark 5.1. Since $\mathbb{F}_p$ is a field, we can use the following dichotomy to understand the structure of $\mathcal{S}(M)$, independently of the chosen normal forms. A matrix $M \in \mathrm{GL}(2,\mathbb{F}_p)$ is either a multiple of the identity (which then commutes with every element of $\mathrm{Mat}(2,\mathbb{F}_p)$) or it possesses a cyclic vector (meaning an element $v \in \mathbb{F}_p^2$ such that v and Mv form a basis of $\mathbb{F}_p^2$), see also Section 3.8.1. In the latter case, M commutes precisely with the matrices of the ring $\mathbb{F}_p[M]$, and we have $\mathcal{S}(M) = \mathbb{F}_p[M]^\times = \mathbb{F}_p[M] \cap \mathrm{GL}(2,\mathbb{F}_p)$. This systematic approach provides an alternative (but equivalent) parametrisation of the above results for the normal forms.

The question for reversibility in $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ with general n is more complicated. The matrix $M = \left(\begin{smallmatrix} 0 & -4 \\ 1 & 0 \end{smallmatrix}\right)$ is reversible over $\mathbb{Z}/3\mathbb{Z}$ (where it is an example of type IV), but fails to be reversible over $\mathbb{Z}/9\mathbb{Z}$, as one can check by a direct computation. Here, zero divisors show up via non-zero matrices A with $AM = M^{-1}A$, but all of them satisfy $\det(A) \equiv 0 \bmod 9$. In fact, one always has $A(\Lambda_9) \subset \Lambda_3$ here.

In general, the relation $AMA^{-1} = M^{-1}$ with $A, M \in \mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ implies $MAM = A$ and hence $\det(M)^2 = 1$, because $\det(A) \in (\mathbb{Z}/n\mathbb{Z})^\times$. Over $\mathbb{F}_p$, this gives $\det(M) = \pm 1$, with reversibility precisely for $\det(M) = 1$ according to Theorem 5.2.1. In general, one has further solutions of the congruence $m^2 \equiv 1 \bmod n$, such as $m = 3$ for $n = 8$ or $m = 4$ for $n = 15$.

In any such case, $M = \left(\begin{smallmatrix} 0 & -m \\ 1 & 0 \end{smallmatrix}\right)$ is a matrix with $M^2 = -m\mathbb{1}$. When $m \not\equiv -1 \bmod n$, M is of order 4 in $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$. It is easy to check that $RMR = M^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -m & 0 \end{smallmatrix}\right)$ in $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$, with the involution $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. This establishes reversibility with $\mathcal{R}(M) = \mathcal{S}(M) \rtimes C_2$.

Reversibility can be viewed as a structural property that reflects additional 'regularity' in the dynamics, in the sense that it typically reduces the spread in the period distribution. This can be interpreted as a weak analogy of toral endomorphisms, showing a "highly structured" lattice dynamics, with the family of maps presented in Section 6.1, for which the period distribution is believed to be (possibly universally) determined by structural properties like reversibility.

For 2×2 matrices, the normal form approach gives the following generalisation of a result Gaspari derived for Arnold's cat map, compare [38, Thm. 3.1.7] .

Theorem 5.2.2. *Every matrix $M \in \mathrm{GL}(2,\mathbb{F}_p)$, which is reversible in this group, has only one non-trivial period length on Λ_p. Every matrix $M \in \mathrm{SL}(2,\mathbb{Z})$ has only one non-trivial period length on each prime lattice Λ_p for which p does not divide the discriminant of the characteristic polynomial χ_M of M.*

Proof. On every prime lattice Λ_p for which the discriminant $\mathrm{tr}(M)^2 - 4$ is not divisible by p, the characteristic polynomial is either irreducible modulo p or splits into two different linear factors, both of which, due to the reversibility, have the same order modulo p. Hence in both cases all points $\neq 0$ share the same minimal period given by $\mathrm{ord}(\chi_M, p)$ in the irreducible case, and by $\mathrm{ord}(a,p)$ if $\chi_M(x) = (x-a)(x-a^{-1})$. According to Theorem 5.1.1, each $M \in \mathrm{SL}(2,\mathbb{Z})$ is reversible on each rational lattice and the claim follows. □

Remark 5.2. As the normal form approach from Section 3.8 shows, similar reasoning can be applied to the prime lattices in higher dimensions. The analysis of block diagonal matrices can be done block-wise, and in particular, the (reversing) symmetry groups are direct products of those of the individual blocks, possibly augmented by additional symmetries that emerge from equal blocks that can be permuted.

For matrices from $\mathrm{Mat}(2,\mathbb{Z}/p^r\mathbb{Z})$, the normal form stated in Theorem 3.8.4 can be employed to trace back over which matrix type a given 2×2 integer matrix lies, and in the simple cases, the analysis is similar to that over $\mathbb{F}_p$.

As could be expected from Section 3.8.1, the hardest case is when M is a matrix which is scalar modulo p^i for some i, or, in other words, admits a decomposition $d\mathbb{1} + p^j C$ where $j \geq 1$. Since $d\mathbb{1}$ and C commute, powers of M can be expanded via the binomial theorem. Using that the binomials satisfy $\frac{n}{\gcd(n,k)} \mid \binom{n}{k}$, the period $\mathrm{per}(x,p^r)$ of all $x \in \Lambda_{p^r}$ is bounded by

$$\mathrm{per}(x,p^r) \leq \mathrm{ord}(d,p^r) \cdot p^{r-\ell}.$$

What is more, the only period lengths that can occur, are p-power multiples of $\mathrm{ord}(d,p)$, which is also the matrix order modulo p. Since the matrix order can only grow by a factor of p in the transition from p^r to p^{r+1}, all period lengths are of the form $p^\ell \,\mathrm{ord}(d,p)$.

The symmetry group can be put down to the symmetry group of the cyclic part. Let $\Pi_j : \mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ denote the canonical projection, and let $\mathcal{S}_j(A)$ be the symmetry group of an integer matrix A, viewed as a matrix over $\mathbb{Z}/p^j\mathbb{Z}$. Then, for $p \neq 2$ and $\ell \geq 1$, one obtains $\mathcal{S}_r(M) = \Pi_\ell^{-1}(\mathcal{S}_\ell(C))$ from the symmetry equations.

5.3 Reversibility mod n

Let M be a general integer matrix, with determinant D.

Fact 5.3.1. *If $M \in \mathrm{Mat}(d,\mathbb{Z})$ is reversible mod n, one has $D^2 \equiv 1$ mod n. Moreover, reversibility for infinitely many n implies $D = 1$ or $D = -1$.*

Proof. The reversibility equation yields $\det M \equiv \det M^{-1}$, hence $D^2 \equiv 1 \mod n$. If $D^2 - 1$ has infinitely many divisors, one has $D^2 = 1$, hence $D = 1$ or $D = -1$. □

Before we continue with some general result, let us see what Fact 5.3.1 specifically implies for $d = 2$.

Fact 5.3.2. *If $M \in \mathrm{Mat}(2,\mathbb{Z})$ with $D \equiv -1$ mod n is reversible mod n, one has $2\,\mathrm{tr}(M) \equiv 0$ mod n. In particular, $\mathrm{tr}(M) \equiv 0$ mod n holds whenever n is odd.*

Proof. The trace is a conjugacy invariant, so reversibility mod n implies $\mathrm{tr}(M) \equiv \mathrm{tr}(M^{-1})$ mod n. The inversion formula for 2×2 matrices yields $\mathrm{tr}(M^{-1}) \equiv \frac{\mathrm{tr}(M)}{D} \equiv -\mathrm{tr}(M) \mod n$, and thus $2\,\mathrm{tr}(M) \equiv 0 \mod n$. □

Fact 5.3.3. *Consider $M \in \mathrm{Mat}(2,\mathbb{Z})$ with $D \equiv -1$ mod n. Then, M is an involution mod n if and only if $\mathrm{tr}(M) \equiv 0$ mod n.*

Proof. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. With $D \equiv -1$, the inversion formula for M shows that $M \equiv M^{-1}$ is equivalent to $d \equiv -a$. Thus, $M^2 \equiv \mathbb{1}$ if and only if $\mathrm{tr}(M) \equiv 0$. □

The previous two facts imply

Corollary 5.3.1. *Let $M \in \mathrm{Mat}(2,\mathbb{Z})$ be reversible mod $n > 2$ with $D \equiv -1$ mod n. Then, $M^2 \equiv \mathbb{1}$ mod n for n odd, and $M^2 \equiv \mathbb{1}$ mod $n/2$ for n even.* □

Let us continue with the general arguments and formulate a necessary condition for local reversibility.

Lemma 5.3.2. *Let $p \neq 2$ be a prime. If $M \in \mathrm{Mat}(d,\mathbb{Z})$ is reversible mod p^r, one has $D \equiv \pm 1$ mod p^r. If $d = 2$, M is reversible mod p^r if and only if $D \equiv 1$ or $M^2 \equiv \mathbb{1}$ mod p^r.*

If $M \in \mathrm{Mat}(d,\mathbb{Z})$ is reversible mod 2^r, then $D \equiv \pm 1$ mod 2^{r-1}. When $d = 2$ and M is reversible with $D \equiv -1$ mod 2^{r-1}, one has $M^2 \equiv \mathbb{1}$ mod 2^{r-2}.

Proof. For $p \neq 2$, Fact 5.3.1 implies $D^2 \equiv 1 \bmod p^r$. Since p cannot divide both $D - 1$ and $D + 1$, one has $p^r | (D-1)$ or $p^r | (D+1)$, which gives the first claim. When $2^r | (D-1)(D+1)$, 2 divides one of the factors and 2^{r-1} the other one, so $D \equiv 1$ or $D \equiv -1 \bmod 2^{r-1}$. If $D \equiv -1 \bmod 2^{r-1}$, Fact 5.3.2 gives $2\,\mathrm{tr}(M) \equiv 0 \bmod 2^{r-1}$ and thus $M^2 \equiv \mathbb{1} \bmod 2^{r-2}$ by Fact 5.3.3. □

One immediate consequence for $d = 2$ is the following.

Corollary 5.3.3. *If $M \in \mathrm{GL}(2,\mathbb{Z})$ with $D = -1$ is reversible for infinitely many $n \in \mathbb{N}$, one has $M^2 = \mathbb{1}$.* □

Fact 5.3.4. *Let A be an integer matrix whose determinant is coprime with $n \in \mathbb{N}$. The reduction of the inverse of A over $\mathbb{Z}/n\mathbb{Z}$, taken modulo $k|n$, is then the inverse of A over $\mathbb{Z}/k\mathbb{Z}$.* □

Lemma 5.3.4. *Let $n = p_1^{r_1} \dots p_s^{r_s}$ be the prime decomposition of $n \in \mathbb{N}$. Then, two matrices $M, M' \in \mathrm{Mat}(d, \mathbb{Z})$ are conjugate mod n if and only if they are conjugate mod $p_i^{r_i}$ for all $1 \leq i \leq s$.*

Proof. $M \sim M' \bmod n$ means $M' = AMA^{-1}$ for some $A \in \mathrm{GL}(n, \mathbb{Z})$, which implies conjugacy mod k for all $k|n$.

For the converse, let $A_i \in \mathrm{GL}(d, \mathbb{Z}/p_i^{r_i}\mathbb{Z})$ denote the conjugating matrix mod $p_i^{r_i}$. The Chinese remainder theorem, applied to each component of the matrices A_i and A_i^{-1}, respectively, gives matrices A and B that reduce to A_i and A_i^{-1} modulo $p_i^{r_i}$, respectively. By construction, $AB \equiv \mathbb{1} \mod p_i^{r_i}$ for all i, hence also $AB \equiv \mathbb{1} \mod n$ and thus $B = A^{-1}$ in $\mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z})$. □

Proposition 5.3.5. *With n as in Lemma 5.3.4, a matrix $M \in \mathrm{Mat}(d, \mathbb{Z})$ is reversible mod n if and only if M is reversible mod $p_i^{r_i}$ for all $1 \leq i \leq s$.*

Proof. The claim is a statement about the conjugacy of M and M^{-1} in the group $\mathrm{GL}(d, \mathbb{Z}/n\mathbb{Z})$, which is thus a consequence of Lemma 5.3.4. We just have to add that, by Fact 5.3.4, the inverse of M mod n reduces to the inverse mod $p_i^{r_i}$, so $MR \equiv RM^{-1} \mod p_i^{r_i}$ for all i. □

Corollary 5.3.6. *Consider a matrix $M \in \mathrm{Mat}(2, \mathbb{Z})$ with $D = \det(M)$ and let $n = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_s^{r_s}$. When n is not divisible by 4, M is reversible mod n if and only if, for each $1 \leq i \leq s$, $D \equiv 1$ or $M^2 \equiv \mathbb{1}$ mod $p_i^{r_i}$. When $n = 2^{r_1} p_2^{r_2} \dots p_s^{r_s}$ with $r_1 \geq 2$, M is reversible mod n if and only if it is reversible mod 2^{r_1} and, for all $i > 1$, $D \equiv 1$ or $M^2 \equiv \mathbb{1}$ mod $p_i^{r_i}$.*

Proof. According to Lemma 5.3.4, the matrix M is reversible mod n if and only if it is reversible mod $p_i^{r_i}$ for all $1 \leq i \leq s$. By Lemma 5.3.2, this is equivalent with $D \equiv 1$ or $M^2 \equiv 1 \bmod p_i^{r_i}$ for all i with $4 \nmid p_i^{r_i}$. □

Remark 5.3. To see that reversibility mod p for all primes p which divide n is not sufficient for reversibility mod n, one can consider a locally reversible matrix M with $\det M \neq 1$. According to Fact 5.3.1, only finitely many n exist such that M is reversible mod n, so for each prime p there must be a maximum r for which M is reversible mod p^r. Recalling an example from above, $M = \left(\begin{smallmatrix} 0 & -4 \\ 1 & 0 \end{smallmatrix}\right)$ is reversible mod 3 but not mod 9 as can be verified by explicit calculation. It is an involution mod 5, hence also reversible mod 15, but not mod 45.

5.4 Matrix order and symmetries over $\mathbb{F}_p$

Let us discuss the order of a matrix $M \in \mathrm{GL}(d, \mathbb{F}_p)$, where p is a prime, in conjunction with the existence of roots of M in that group. We begin by recalling the following result from [56, Thm. 2.14, Cor. 2.15 and Cor. 2.16].

Fact 5.4.1. *If f is an irreducible polynomial of degree d over $\mathbb{F}_p$, its splitting field is isomorphic with $\mathbb{F}_{p^d}$. There, it has the d distinct roots $\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$ that are conjugates and share the same order in $(\mathbb{F}_{p^d})^\times$.*

In particular, two irreducible polynomials over $\mathbb{F}_p$ of the same degree have isomorphic splitting fields. □

From now on, we will identify isomorphic fields with each other. In particular, we write $\mathbb{F}_{p^d}$ for the splitting field of an irreducible polynomial of degree d over $\mathbb{F}_p$.

Next, let K be an arbitrary finite field, consider an irreducible, monic polynomial $f \in K[x]$ of degree d, and let L be the splitting field of f. When $\lambda_1, \lambda_2, \ldots, \lambda_d$ are the roots of f in L, one has the well-known factorisation

$$f(x) \,=\, \prod_{j=1}^{d} (x - \lambda_j) \,=\, x^d - e_1(\lambda_1, \ldots, \lambda_d) + \ldots + (-1)^d e_d(\lambda_1, \ldots, \lambda_d), \tag{26}$$

where the e_i denote the elementary symmetric polynomials,

$$e_1(x_1, \ldots, x_d) = x_1 + x_2 + \ldots + x_d\,,\ \ldots\ , e_d(x_1, \ldots, x_d) = x_1 \cdot x_2 \cdot \ldots \cdot x_d.$$

The elementary symmetric polynomials, when evaluated at the roots of f, are fixed under all Galois automorphisms of the field extension L/K, so that the following property is clear.

Fact 5.4.2. *An irreducible, monic polynomial $f \in K[x]$ satisfies* (26) *over its splitting field L. In particular, the elementary symmetric polynomials $e_1, \ldots, e_d$, evaluated at the d roots of f in L, are elements of K.* □

Let M be a $d \times d$ integer matrix with irreducible characteristic polynomial χ_M over $\mathbb{F}_p$. Let α be a root of χ_M in $\mathbb{F}_{p^d}$ and λ a generating element of the unit group $(\mathbb{F}_{p^d})^\times$. Clearly, there is an $n \in \mathbb{N}$ with $\alpha = \lambda^n$. By Fact 5.4.1, one has $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d} = \mathbb{F}_p(\lambda)$, where the degree of the extension field over $\mathbb{F}_p$ equals d. Consequently, the minimal polynomial of λ over $\mathbb{F}_p$ is an irreducible monic polynomial of degree d over $\mathbb{F}_p$, and the conjugates of α are powers of the conjugates of λ. Let $\alpha_1, \ldots, \alpha_d$ and $\lambda_1, \ldots, \lambda_d$ denote the respective collections of conjugates. Thus, over $\mathbb{F}_{p^d}$, one has the matrix conjugacy

$$M \,\sim\, \mathrm{diag}(\alpha_1, \ldots, \alpha_d) \,=\, \mathrm{diag}(\lambda_1, \ldots, \lambda_d)^n \,\sim\, C(f)^n,$$

with $f(x) \in \mathbb{F}_p[x]$ as in (26) and $C(f)$ denoting the companion matrix of f. Here, it was exploited that a $d \times d$ matrix whose characteristic polynomial f has d distinct roots is always similar to the companion matrix of f. Note that $C(f) \in \mathrm{GL}(d, \mathbb{F}_p)$ by Fact 5.4.2.

Now, M and $C(f)$ are matrices over $\mathbb{F}_p$ that are conjugate over $\mathbb{F}_{p^d}$, so (by a standard result in algebra, see [1, Thm. 5.3.15]) they are also conjugate over $\mathbb{F}_p$, which means that we have the relation

$$M \,=\, A^{-1} C(f)^n A \,=\, (A^{-1} C(f) A)^n \,=:\, W^n \tag{27}$$

with some $A \in \mathrm{GL}(d, \mathbb{F}_p)$. By similarity, $\mathrm{ord}(W) = \mathrm{ord}(C(f)) = \mathrm{ord}(\mathrm{diag}(\lambda_1, \ldots, \lambda_d)) = p^d - 1$. This gives the following result.

Lemma 5.4.1. *A matrix $M \in \mathrm{GL}(d, \mathbb{F}_p)$ with irreducible characteristic polynomial either has the maximally possible order $p^d - 1$, or admits an n-th root $W \in \mathrm{GL}(d, \mathbb{F}_p)$ as in* (27)*. Here, n can be chosen as $n = \frac{p^d - 1}{\mathrm{ord}(M)}$, so that the root has order $p^d - 1$.* □

Fact 5.4.3. *Let A be a matrix over $\mathbb{F}_p$ with minimal polynomial of degree d. Then, the ring*

$$\mathbb{F}_p[A] \,=\, \{\xi_1 \mathbb{1} + \ldots + \xi_d A^{d-1} \mid \xi_j \in \mathbb{F}_p\}$$

has precisely p^d elements, which correspond to the different d-tuples $(\xi_1, \ldots, \xi_d)$.

Proof. Two distinct d-tuples producing the same matrix would give rise to a non-trivial linear combination that vanishes, involving powers of A of degree $d - 1$ at most, which contradicts the minimal polynomial having degree d. □

Lemma 5.4.2. *Let $W, M \in \mathrm{GL}(d, \mathbb{F}_p)$ satisfy $W^n = M$ and $\mathrm{ord}(W) = p^d - 1$. Then, $\mathbb{F}_p[M] = \mathbb{F}_p[W]$ and*

$$\mathbb{F}_p[M]^\times \;=\; \mathbb{F}_p[M] \setminus \{0\} \;=\; \langle W \rangle \;\simeq\; C_{p^d-1},$$

where $\langle W \rangle$ denotes the cyclic group generated by W.

Proof. Clearly, $\mathbb{F}_p[M] = \mathbb{F}_p[W^n] \subset \mathbb{F}_p[W]$, while Fact 5.4.3 implies $|\mathbb{F}_p[M]| = |\mathbb{F}_p[W]| = p^d$, whence we have equality. Further,

$$\langle W \rangle \;\subset\; \mathbb{F}_p[W]^\times \;\subset\; \mathbb{F}_p[W] \setminus \{0\} \;=\; \mathbb{F}_p[M] \setminus \{0\},$$

and again, comparing cardinalities, one finds $|\langle W \rangle| = p^d - 1 = |\mathbb{F}_p[M] \setminus \{0\}|$, from which the claim follows. □

Let us summarise and extend the above arguments as follows.

Corollary 5.4.3. *A $d \times d$ integer matrix M with irreducible characteristic polynomial over the field $\mathbb{F}_p$ has a primitive root $W \in \mathrm{GL}(d, \mathbb{F}_p)$ with $\mathrm{ord}(W) = p^d - 1$. Moreover, one then has $\mathbb{F}_p[M]^\times = \mathbb{F}_p[M] \setminus \{0\} = \langle W \rangle \simeq C_{p^d-1}$. In particular, $\mathcal{S}(M) \simeq C_{p^d-1}$ in this case.*

More generally, we have $\mathcal{S}(M) = \mathbb{F}_p[M]^\times$ whenever the minimal polynomial has degree d.

Proof. Since we work over the field $\mathbb{F}_p$, the irreducibility of the characteristic polynomial of M means that the minimal polynomial agrees with the characteristic polynomial and has thus maximal degree d. This situation is equivalent with M being cyclic [45, Thm. III.2]. By Thm. 17 of [45] and the Corollary following it, we know that any matrix which commutes with M is a polynomial in M, so that $\mathcal{S}(M) = \mathbb{F}_p[M]^\times$ is clear.

The claim for matrices M with an irreducible characteristic polynomial follows by Lemmas 5.4.1 and 5.4.2. □

When a matrix $M \in \mathrm{Mat}(d, \mathbb{F}_p)$ fails to be cyclic, there are always commuting matrices that are not elements of $\mathbb{F}_p[M]$, see Thm. 19 of [45] and the following Corollary. In such a case, $\mathcal{S}(M)$ is a true group extension of $\mathbb{F}_p[M]^\times$. The situation is particularly simple for matrices $M \in \mathrm{Mat}(2, \mathbb{F}_p)$: either they are of the form $M = a\mathbb{1}$ (then with $\mathcal{S}(M) = \mathrm{GL}(2, \mathbb{F}_p)$), or they are cyclic (then with $\mathcal{S}(M) = \mathbb{F}_p[M]^\times$), cf. also Section 3.8.1.

6 The Casati-Prosen map on rational lattices of the torus

This section is concerned with the Casati-Prosen triangle map [25, 43] (CP map) on rational lattices of the two-dimensional torus for special parameter pairs. It is essentially based on the article [62].

In Section 6.1, a family of "classically" reversible maps will be introduced and the CP map will be set in the context thereof; in Section 6.2, certain reversibility and symmetry properties of the CP map will be presented; in Section 6.3, we state several conjectures about the parameter-dependent convergence of the CP map and in Section 7 we give evidence for the conjectures formulated below, which are based on excessive numerical studies.

6.1 Reversibility and symmetric orbits

In physical systems, reversibility is often given as time reversal symmetry which then implies the existence of an involutory reversor. The algebraic meaning of the existence of involutory reversors was discussed in Section 5 in the context of toral automorphisms. Whenever an involutory reversor G of a map L exists, that is, $G^2 = Id$ and $G \circ L \circ G = L^{-1}$, also $G \circ L$ is an involution, as $G \circ L = L^{-1} \circ G = (G \circ L)^{-1}$.

In the following, we specialise the notion of reversibility in the above sense, that is, a map L is said to be *reversible* if it is the composition of two involutions G and $H = L \circ G$. The involution G conjugates the map to its inverse, namely

$$G \circ L \circ G \;=\; L^{-1} \qquad\qquad G^2 = Id. \tag{28}$$

Any G that satisfies (28) is called a *reversing symmetry* for L. For further background information on reversibility in a similar or more general setting, see [53, 58, 69], and references therein.

We consider reversible twist maps of the so-called generalised standard form

$$L:\; x' = x + y', \qquad\qquad y' = y + f(x). \tag{29}$$

We regard L as a map of $\mathbb{R}^2$ or $\mathbb{C}^2$, or indeed of $\mathbb{F}^2$, where $\mathbb{F}$ is any field. If f is periodic, then L commutes with a discrete group of translations, and may be reduced to a map of the cylinder or the torus. The map L is reversible for any choice of the function f, since we can write $L = H \circ G$, where

$$G:\; x' = x, \quad y' = -y - f(x) \qquad\qquad H:\; x' = x - y, \quad y' = -y. \tag{30}$$

One verifies that G and H are orientation-reversing involutions. The family (29) includes well-known maps such as the Chirikov-Taylor standard map of the cylinder or torus, for which $f(x) = \alpha \sin(x)$, and the area-preserving Hénon map of the plane, corresponding to $f(x) = x^2 + \alpha$. For $f(x) = cx$, $c \neq 0$, one recovers the case of hyperbolic toral automorphisms. From Section 6.2 on, the map L will be specialised to the Casati-Prosen (CP) triangle map T of the two-dimensional torus $\mathbb{T}^2$, for which the function f is given by [43]:

$$f(x) = \alpha\, \theta(x) + \beta \qquad\qquad \theta(x) = \begin{cases} 1 & x \in [0, \frac{1}{2}) \\ -1 & x \in [\frac{1}{2}, 1). \end{cases}$$

As in the case of toral endomorphisms, both variables x and y are taken modulo 1, and the parameters α, β are real numbers. The CP map has zero entropy, being piecewise parabolic,

and it is conjectured to be uniquely ergodic and mixing for almost all choices of parameters. However, these properties appear to be very difficult to establish rigorously [43]. There is a growing interest in the ergodic properties of two-dimensional maps with zero entropy, stimulated by recent developments in the one-dimensional case [5].

Here, we will study the *rational* periodic orbits of the CP map.

This map has no periodic orbits at all if $\beta \notin \mathbb{Z} + \alpha\mathbb{Z}$ [43, Lemma 1], and this condition requires that at least one of α, β is irrational. If, on the other hand, both parameters are rational, then all rational points on the torus are periodic. To see this, we consider the rational lattice Λ_N on the 2-torus,

$$\Lambda_N \;=\; \left\{ \left(\tfrac{k}{N}, \tfrac{\ell}{N}\right) \,|\, 0 \leq k, \ell < N \right\} \qquad N \in \mathbb{N}. \tag{31}$$

Then we let

$$\gamma = \beta + \alpha \qquad\qquad \delta = \beta - \alpha. \tag{32}$$

(Here, we omit the superscript 't' at the 2-tuples referring to the coordinates of a point, and simply denote points on the torus as row vectors in the following.) From an algebraic viewpoint, the parameters γ, δ are more natural than α and β; the latter, however, are more significant dynamically. We will use both, as appropriate.

The map T preserves Λ_N if and only if $(\gamma, \delta) \in \Lambda_N$; if α and β are rational, then, without loss of generality, we may assume that this is the case. All orbits of T on Λ_N are periodic, being the orbits of an invertible map over a finite set. We can therefore consider the distributional properties of their periods, which we characterise by means of the period distribution function

$$\mathcal{D}_N(x) = \frac{|\{z \in \Lambda_N \,:\, t(z) \leqslant \kappa x\}|}{N^2} \tag{33}$$

where $t(z)$ is the minimal period of the point z, and the constant κ is a normalisation parameter to be determined below. The function $\mathcal{D}_N$, which depends on α and β, is a step function, with the number of steps being equal to the number of distinct periods of T on Λ_N at the chosen parameter values.

Since we study the CP map within the framework of reversible maps and their symmetry properties, we briefly review the aspects of the combinatorial model presented in [72] which are relevant to the questions pursued here.

For $L = H \circ G$, let $\mathsf{Fix}(H)$ and $\mathsf{Fix}(G)$ denote the subsets of elements of the finite set Ω, which are fixed by H and G, respectively. A *symmetric orbit* is a periodic orbit which is invariant under G (and hence also under $H = L \circ G$). These orbits are determined uniquely by their intersections with the symmetry lines [31]. Clearly, a symmetric orbit must have two points in $\mathsf{Fix}(G) \cup \mathsf{Fix}(H)$, and the complete orbit can be reconstructed by the *arc* between the two points in the fixed sets, see Figure 7. More precisely, a symmetric periodic orbit with odd period $2k-1$ has one point (x, y) on the symmetry line $\mathsf{Fix}(G)$ and one point $L^k(x, y)$ on $\mathsf{Fix}(H)$. One of even period $2k$ has two points (x, y) and $L^k(x, y)$ both on $\mathsf{Fix}(G)$ or both on $\mathsf{Fix}(H)$. The ability to find symmetric periodic orbits by searching along the one-dimensional symmetry lines gives a considerable (computational) advantage compared to finding asymmetric periodic orbits, which requires a two-dimensional search.

In [72], the period distribution in the ensemble of all pairs of random involutions (G, H) on a finite phase space Ω was studied and the limit of $|\Omega| \longrightarrow \infty$ considered. A typical situation in which this scenario arises is in the study of polynomial automorphisms which decompose

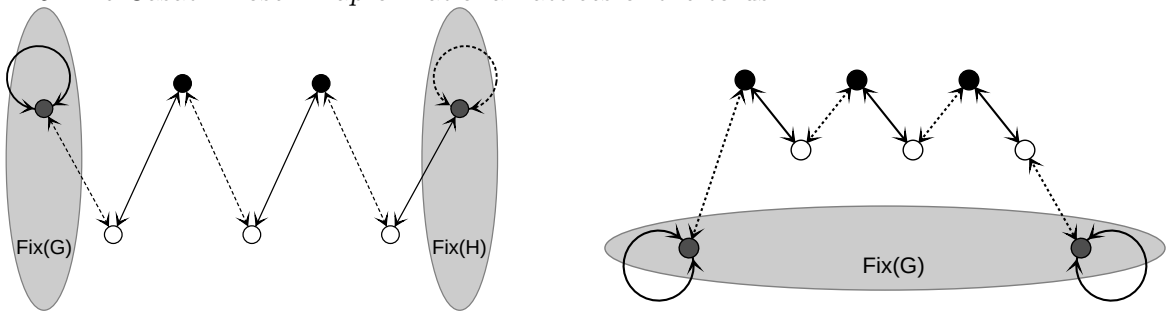


Figure 7: Odd and even symmetric orbit: the left figure shows a 7-arc from $\mathsf{Fix}(G)$ to $\mathsf{Fix}(H)$, the right figure an 8-arc from $\mathsf{Fix}(G)$ to itself. The solid and dashed lines represent the action of G and H, respectively. In general, $\mathsf{Fix}(G)$ and $\mathsf{Fix}(H)$ need not be disjoint; in that case, the intersection consists of fixed points of L. In the case of even symmetric orbits, the start and endpoint of an arc of length ≥ 2 can never coincide since both G and H are involutions, which 'swap' any two points $x, G(x)$ (or $x, H(x)$).

into two involutions G and H, such that the reduced dynamics over the finite fields $\mathbb{F}_p$ for growing p provides a sequence of finite dynamical systems whose phase spaces grow to infinity.

More concretely, for some fixed pair of involutions (G, H) acting on a finite space Ω with $|\Omega| = \nu$, let

$$P_t = \frac{|\{x \in \Omega \mid x \text{ has minimal period } t \text{ under } H \circ G\}|}{\nu}$$

and $\langle P_t \rangle$ the average over all possible pairs of involutions (G, H) on Ω (uniformly weighted). Let $g(\nu) = |\mathsf{Fix}(G)|$ and $h(\nu) = |\mathsf{Fix}(H)|$ denote the cardinalities of the fixed sets in Ω. Define, for $x \geq 0$, $\mathcal{R}_\nu(x) = \sum_{t=1}^{\lfloor x z_\nu \rfloor} \langle P_t \rangle$, where $z_\nu = \frac{2\nu}{g(\nu)+h(\nu)}$.

Theorem 6.1.1. [72, Thm. A] *Assume (G, H) is a pair of random involutions on a set Ω with cardinality ν, such that $\lim_{\nu\to\infty} g(\nu) + h(\nu) = \infty$ and $\lim_{\nu\to\infty} \frac{g(\nu)+h(\nu)}{\nu} = 0$. Then*

$$\lim_{\nu\to\infty} \mathcal{R}_\nu(x) = \mathcal{R}(x) = 1 - e^{-x}(1 + x).$$

Moreover, asymptotically, almost all points in Ω belong to symmetric cycles. □

The function $\mathcal{R}(x)$ is the cumulative distribution of the gamma-density with shape and scaling parameters equal to 2 and 1, respectively [44]. When referring to the gamma distribution below, we always mean $\mathcal{R}(x)$ from Theorem 6.1.1.

For maps having a single family of reversing symmetries, it has been conjectured [70, 71, 72, 63] and experimentally observed that asymptotically the period length distribution follows $\mathcal{R}(x)$, where the normalisation constant κ was chosen to be the mean period $\bar{t}$ of orbits, i.e. $\bar{t} = \nu/(\#\text{orbits})$. In the following, we will use this scaling constant most of the time, that is, in the setting studied here, where $\Omega = \Lambda_N$ and $\nu = N^2$, we scale by

$$\kappa = \bar{t} = \frac{\nu}{\#\text{cycles}} = \frac{N^2}{\#\text{cycles}}. \tag{34}$$

For the typical case in the plane where both fixed sets have N points in reduction, hence precisely N symmetric cycles, one has $\approx N$ cycles, see also Section 6.2. The scaling factor $z(\nu)$ from Theorem 6.1.1 then becomes $z(N^2) = 2N^2/(|\mathsf{Fix}(G)| + |\mathsf{Fix}(H)|) = N$.

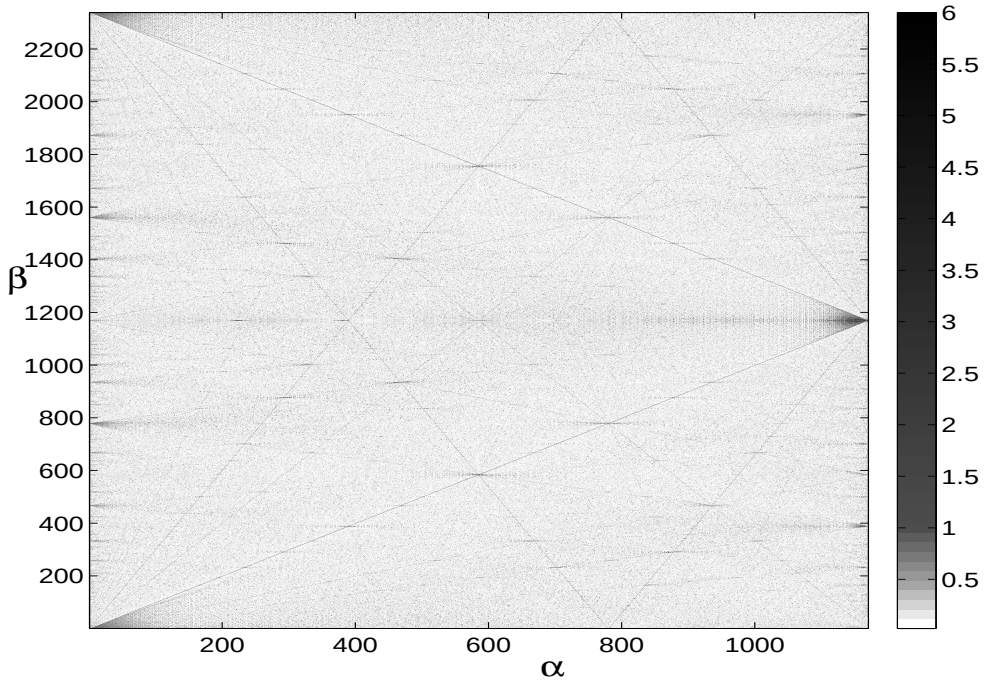


Figure 8: Parameter space of the CP map for $N = p = 2339$, a prime number, each pixel representing a parameter pair (α, β). The value of the norm of the difference $\mathcal{D}_p(\alpha, \beta) - \mathcal{R}$ (Equation (41)) is coded on a grey scale, the darker a pixel, the larger the deviation from the gamma distribution $\mathcal{R}(x)$. Two blow-ups of this image are shown in Figure 12; for parameters (α, β) near $(0, 0)$ (left frame, for the larger prime $p = 9011$), and near $(1/4, 1/4)$ (right frame, for the prime $p = 11433$).

A way to keep track of the fraction of points in symmetric orbits is the function

$$\mathcal{A}_N = \frac{|\{x \in \Lambda_N \mid x \text{ belongs to asymmetric cycle}\}|}{N^2}.$$

Throughout the next sections, we will investigate to what extent the CP map on the rational lattices behaves like a random reversible map in the above sense. To this end, a main objective will be to analyse the behaviour of $\mathcal{E}_N$, i.e. the L^1-norm of $\mathcal{D}_N - \mathcal{R}$, and $\mathcal{A}_N$, two characteristic quantities for reversible maps. Most of the time we assume N to be a prime. The parameter dependence of $\mathcal{E}_N$ and $\mathcal{A}_N$ for the CP map is shown in Figures 8 and 9, which will be discussed in more detail below.

In the following, the word *orbit* always means periodic orbit or cycle.

6.2 Reversibility and symmetry of the Casati-Prosen map

The family of maps (29) can be written as the composition of two shears, one in y followed by one in x, that is, $L = S_x \circ S_y$, where

$$S_y : x' = x, \quad y' = y + f(x)$$
$$S_x : x' = x + y, \quad y' = y.$$

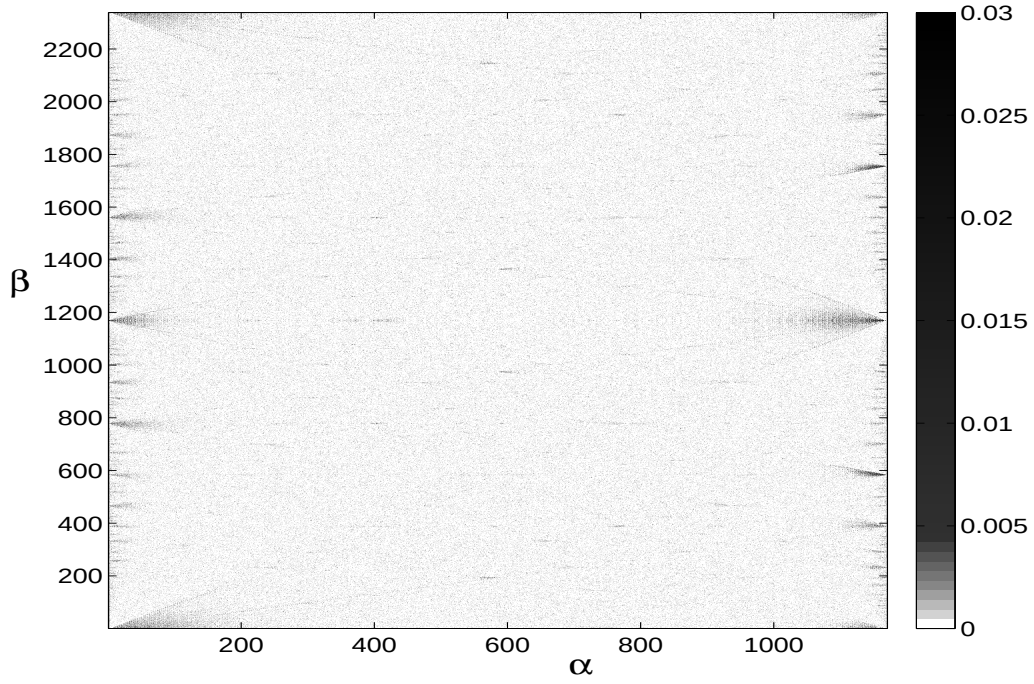


Figure 9: Parameter dependence of the function $\mathcal{A}_p(\alpha, \beta)$ (Equation (61)) for $N = p = 2339$, a prime number. The value of $\mathcal{A}_p$ is coded on a grey scale, the darker a pixel, the larger the fraction of asymmetric orbits at the corresponding parameter pair (α, β).

We have pointed out that these maps are reversible for any choice of f, with the involutions G and H given by (30). (The shears S_x and S_y are clearly not involutions.) Because the involutions G and H are orientation-reversing (their Jacobian determinant is equal to -1), their fixed sets $\mathsf{Fix}(G)$ and $\mathsf{Fix}(H)$ —the so-called *symmetry lines*— are one-dimensional [35]. The symmetry lines of the involutions (30) are given by

$$\mathsf{Fix}(G) = \{(x, y) \mid (x, y) \in \mathbb{T}^2, 2y = -f(x)\} \qquad \mathsf{Fix}(H) = \{(x, 0) \mid x \in \mathbb{T}\}, \tag{35}$$

where f is an arbitrary 1-periodic map.

Specialising Equations (29) and (35) to the CP map T (31), we have:

$$\begin{array}{ll} G : x' = x, \quad y' = -y - \alpha\,\theta(x) - \beta & \mathsf{Fix}(G) : \{(x, y) \mid (x, y) \in \mathbb{T}^2, 2y = -\alpha\,\theta(x) - \beta\} \\ H : x' = x - y, \quad y' = -y & \mathsf{Fix}(H) : \{(x, 0) \mid x \in \mathbb{T}\}. \end{array} \tag{36}$$

For rational parameters α and β, we consider the action of T over the lattice Λ_N, given in (31), where N is the least common denominator of α and β. Clearing denominators in (31), we obtain the integer lattice $\tilde{\Lambda}_n$, which we still denote by Λ_N. The action of $T \mod 1$ on this invariant integer lattice can now be described by the permutation T_N, given by

$$T_N : x' \equiv x + y' \mod N \qquad y' \equiv y + \alpha\,\theta_N(x) + \beta \mod N \tag{37}$$

where we now abuse notation by identifying x, y, α and β with their respective numerators

over the common denominator N, so in (37)

$$x, y, \alpha, \beta \in \{0, 1, 2, \dots N-1\},$$

and

$$\theta_N(x) = \begin{cases} 1 & x \in \{0, 1, \dots, \lceil N/2 \rceil - 1\} \\ -1 & x \in \{\lceil N/2 \rceil, \dots, N-1\}. \end{cases}$$

The permutation T_N inherits the corresponding reversibility (36) with

$$\begin{array}{rcl} \mathsf{Fix}(H) & = & \{(x,0) \mid x = 0, \dots, N-1\}, \\ \mathsf{Fix}(G) & = & \{(x,y) \mid (x,y) \in \{0, \dots, N-1\}^2,\ 2y \equiv -\alpha\,\theta_N(x) - \beta \mod N\}. \end{array} \tag{38}$$

$\mathsf{Fix}(H)$ and $\mathsf{Fix}(G)$ are finite sets, with $\mathsf{Fix}(H)$ being a line with N lattice points. When N is odd, the integer 2 has a modular inverse, and $\mathsf{Fix}(G)$ is the union of two 'half-lines' on the lattice, the $\lceil N/2 \rceil$ lattice points with height $y \equiv -(\alpha+\beta)/2 \mod N$ on the left, and the $\lfloor N/2 \rfloor$ lattice points with height $y \equiv (\alpha-\beta)/2 \mod N$ on the right. In this case,

$$(|\mathsf{Fix}(G)| + |\mathsf{Fix}(H)|)/2 = N$$

and by [71, Lemma 1], there are precisely N symmetric cycles. When N is even, $\mathsf{Fix}(G)$ is empty if $\alpha + \beta \mod N$ is odd, and there are exactly $N/2$ symmetric cycles. When N and $\alpha + \beta \mod N$ are both even, then

$$\mathsf{Fix}(G) = \{(x, -(\alpha\,\theta_N(x) + \beta)/2 \mod N/2)\} \cup \{(x, -(\alpha\,\theta_N(x) + \beta)/2 \mod N/2 + N/2)\},$$

that is, four 'half-lines' on the lattice, so again there are N symmetric cycles.

In the next section, we study the dynamics of T_N over the entire parameter space $\{(\alpha, \beta) : \alpha, \beta \in \{0, 1, 2, \dots N-1\}\}$. Using $T_N^{\alpha,\beta}$ to highlight the explicit dependence of T_N on its parameters, we have

Lemma 6.2.1. *For odd N, the maps $T_N^{\alpha,\beta}$ and $T_N^{-\alpha,-\beta}$ are conjugate permutations of the N^2 points of Λ_N, hence have the same cycle structure. For even N, the same is true for $T_N^{\alpha,\beta}$, $T_N^{-\alpha,-\beta}$ and $T_N^{-\alpha,\beta}$ —they are all conjugate on Λ_N— and $T_N^{\alpha,\beta} = T_N^{\alpha+N/2,\beta+N/2}$.*

Proof. Consider the invertible change of coordinates $\Phi : x = aX + b$, $y = aY$. With $a = \pm 1$, Φ also defines an invertible map of the torus. The transformed version of T is then:

$$\Phi^{-1} \circ T \circ \Phi : X' = X + Y', \qquad Y' = Y + \frac{1}{a}[\alpha\,\theta(aX + b) + \beta]. \tag{39}$$

For the choice $a = -1$, $b = \lfloor N/2 \rfloor$, we have

$$\Theta(X) := \frac{1}{a}[\theta(aX + b)] = -\theta(X) \tag{40}$$

because of the invariance $\theta(x) \equiv \theta(-x + \lfloor N/2 \rfloor) \mod N$ for odd or even N. Consequently, with these choices of a and b,

$$\Phi^{-1} \circ T_N^{\alpha,\beta} \circ \Phi = T_N^{-\alpha,-\beta},$$

showing that a change of sign in parameters makes $T_N^{\alpha,\beta}$ and $T_N^{-\alpha,-\beta}$ conjugate permutations for any N. For N even, one additionally has $\theta(x) \equiv -\theta(x + N/2) \mod N$, which corresponds to the choice $a = 1$, $b = N/2$ in (40), so that $T_N^{\alpha,\beta}$ and $T_N^{-\alpha,\beta}$ are also conjugate permutations. The last statement of the lemma, for N even, is obvious. □

From this lemma it follows that, for N even, one need only consider parameters lying in the triangle with vertices $(0,0)$, $(N/2,0)$, and $(N/2,N/2)$. If N is odd, then $\theta(x)$ and $-\theta(x+\lceil N/2\rceil) \mod N$ agree on all sites except $x = \lceil N/2\rceil - 1$ when the former gives $+1$ and the latter gives -1. Thus for large odd N, there is an approximate symmetry between the maps $T_N^{-\alpha,\beta}$ and $T_N^{\alpha,\beta}$, or, equivalently, between $T_N^{\alpha,\beta}$ and $T_N^{\alpha,-\beta}$ —see Figure 8.

6.3 Characterising convergence

In this section we formulate precisely the conjectures mentioned in the introduction, and develop the analysis that will support the computations described in the next section.

6.3.1 Convergence to the gamma distribution

We consider the convergence properties of the empirical distributions $\mathcal{D}_p$ given in (33), for the CP map on the prime lattice Λ_p (see Equation (31)). The parameters have the same prime denominator, $(\alpha,\beta) \in \Lambda_p$, and to make the parameter dependence explicit, we use the notation $\mathcal{D}_{p,\alpha,\beta}$. We want to determine whether or not convergence of $\mathcal{D}_p$ to the gamma distribution of Theorem 6.1.1 will occur for a typical choice of parameters.

To make this idea precise, we first introduce the quantity

$$\mathcal{E}_p(\alpha,\beta) = \int_0^\infty |\mathcal{D}_{p,\alpha,\beta}(x) - \mathcal{R}(x)|\, dx \tag{41}$$

which measures the distance of the distribution $\mathcal{D}_{p,\alpha,\beta}$ (with scaling constant (34)) from $\mathcal{R}$ in the L^1-norm.

Now fix a real constant $c > 0$, and consider the function

$$E_p(c) = \frac{|\{(\alpha,\beta) \in \Lambda_p \,:\, \mathcal{E}_p(\alpha,\beta) < c\}|}{p^2}. \tag{42}$$

This is the proportion of rational parameter pairs with common denominator p, for which the period distribution function lies at distance smaller than c from $\mathcal{R}$. For fixed p, the function $E_p(c)$ is a distribution function: it is non-decreasing, and it is equal to 1 for all sufficiently large c. Then we define

$$E(c) = \liminf_{p\to\infty} E_p(c) \qquad c > 0. \tag{43}$$

The function E is non-decreasing. Numerical evidence suggests that E has a much stronger property:

Conjecture 1. *The function E is identically equal to* 1.

This conjecture states that the period distribution of the rational cycles of the CP map, is, for almost all rational parameters with prime denominator, the same as that of a random reversible map [72]. The potential convergence of E_p to 1 is necessarily non-uniform, because, due to the finite parameter set, for any finite p, the value of $E_p(c)$ must be zero in a small neighbourhood of the origin. We shall also see that the convergence is very slow.

By construction, the function E is not affected by contributions from possible 'anomalous' distributions, which may appear for sets of parameters of size $o(p^2)$. A class of anomalous distributions is found over lines in parameter space with (low-order) rational slope; we deal with them in the next section. A second class of anomalous distributions appears in certain two-dimensional regions in parameter space, located in the vicinity of low-order rationals.

6.3.2 Singular distributions on rational lines

An infinite sequence of anomalous distributions originates from parameters of the form $\beta = k\alpha$, for $k = 1, 2, \ldots$. These are singular distributions, whose asymptotic properties appear to depend only on k. Moreover, it turns out that, in the limit of large k, these distributions converge to the gamma distribution (see below). Thus, within a single family of maps, one can observe the transition from a singular orbit statistics to the smooth orbit statistics of random reversible maps.

We begin with the simple case of $\alpha = 0$, whence the discontinuity disappears, and the asymptotic period distributions can be calculated exactly. Note that, when also $\beta = 0$, one is in the situation of the parabolic torus automorphism from Example 3.3.

We define the step-functions

$$\mathcal{D}_1(x) = \begin{cases} 0 & \text{if } x < 1 \\ 1 & \text{if } x \geqslant 1 \end{cases} \tag{44}$$

$$\mathcal{D}_p^{(m)}(x) = \begin{cases} 0 & \text{if } 0 \leqslant x < \frac{1}{p^m} \\ \frac{1}{p^i} & \text{if } \frac{1}{p^i} \leqslant x < \frac{1}{p^{i-1}}, \quad i = 1, 2, \ldots, m \\ 1 & \text{if } x \geqslant 1 \end{cases} \tag{45}$$

$$\mathcal{D}_p^{(\infty)}(x) = \lim_{m\to\infty} \mathcal{D}_p^{(m)}(x). \tag{46}$$

The following result establishes the limiting behaviour of the empirical distribution function $\mathcal{D}_{N,\alpha,\beta}$ for some special choice of parameters. In order to achieve simple limiting distributions, we need to adopt a normalisation distinct from (34).

Theorem 6.3.1. *Let $N = p^n$ be a prime power, let $(\alpha, \beta) \in \Lambda_{p^n}$, with $\alpha = 0$, and let $x \geqslant 0$. Build the distribution* (33) *with $\kappa = N = p^n$.*

For $\beta = 0$ the following holds:

$$\lim_{p\to\infty} \mathcal{D}_{p^n,0,0}(x) = \mathcal{D}_1(x) \tag{47}$$

$$\lim_{n\to\infty} \mathcal{D}_{p^n,0,0}(x) = \mathcal{D}_p^{(\infty)}(x). \tag{48}$$

For $\beta > 0$, and p odd, we have

$$\begin{aligned} \lim_{p^n\to\infty} \mathcal{D}_{p^n,0,\beta}(x) &= \mathcal{D}_1(x) \qquad \gcd(\beta, p) = 1 \\ \lim_{p\to\infty} \mathcal{D}_{p^n,0,\beta}(x) &= \mathcal{D}_1(x) \qquad \gcd(\beta, p) \neq 1 \\ \lim_{n\to\infty} \mathcal{D}_{p^n,0,\beta}(x) &= \mathcal{D}_p^{(m)}(x) \qquad \beta = p^m \qquad m = 1, \ldots, n-1. \end{aligned} \tag{49}$$

(The case $p = 2$ is omitted for the sake of brevity.)

Proof. When $\alpha = 0$, the CP map is

$$x' \equiv x + y' \mod N \qquad y' \equiv y + \beta \mod N. \tag{50}$$

and the t-th iterate of an initial point (x_0, y_0) is given by

$$x_t \equiv x_0 + y_0 t + \frac{\beta}{2} t(t+1) \mod N \qquad y_t \equiv y_0 + \beta t \mod N. \tag{51}$$

Consider firstly $\beta = 0$. Then the map (50) is an integrable twist map modulo N. Indeed every line $y = y_0$ is invariant, and on each line the x-dynamics is a translation, namely the y_0-fold composition of the generating translation $x' = x + 1$. These translations represent the full ensemble of N possible translations modulo N.

As can be seen from Equation (51), the period of the point (x_0, y_0) is given by the smallest positive solution t to the congruence $y_0\, t \equiv 0 \mod N$. Dividing through by a common factor yields

$$t\frac{y_0}{d} \equiv 0 \mod \frac{N}{d}, \qquad d = \gcd(y_0, N), \tag{52}$$

which gives the period $t = N/d$, independent of x_0, and there are d orbits with that period.

For every divisor d of N, the number of lines $y = y_0$ such that $\gcd(y_0, N) = d$ is equal to $\phi(N/d)$ where ϕ is Euler's totient function. In particular, the choice $d = N$ ($y_0 = 0$) gives a single line with N fixed points for the map. If $N = p$ is prime, the only other possibility is $d = 1$, corresponding to $p - 1$ lines each containing one orbit of maximal period $t = N$. For general N, the N^2 points of Λ_N are accounted for courtesy of the divisor sum [40, Thm. 63]

$$\sum_{d|N} d\frac{N}{d}\phi\left(\frac{N}{d}\right) = N\sum_{d|N}\phi\left(\frac{N}{d}\right) = N\sum_{d|N}\phi(d) = N^2.$$

For every divisor t of N, the number of points of period t is $N\phi(t)$, and hence the fraction $\mu(t)$ of phase space occupied by points of period at most t is equal to

$$\mu(t) = \frac{1}{N}\sum_{\substack{t'|N \\ t'\le t}} \phi(t'). \tag{53}$$

Specialising to $N = p^n$, we have the periods $t_i = p^i$ $(i = 0, \ldots, n)$, and the sum (53) becomes

$$\mu(p^i) = \frac{1}{p^n}\sum_{j=0}^{i}\phi(p^j) = p^{i-n}.$$

We consider the limit of large N with n fixed and $p \to \infty$. The natural period normalisation is N, consistent with the map (50) with $\beta = 0$ being an ensemble of N translations. Taking $\kappa = N$ gives the distribution (47).

Next we take p fixed and $n \to \infty$. Normalising periods by N, the proportion of phase space consumed in cycles with normalised period less than or equal to p^i/p^n is p^i/p^n for $i = 0, 1, \ldots, n$, leading to (48).

Consider now the case of (50) when $\beta > 0$. From the second equation in (51), a necessary condition for an orbit to be periodic is $\beta\, t \equiv 0 \mod N$, independent of y_0. By analogy with Equation (52) above, we find that the smallest positive solution is $t = \tau = N/r$ where $r = \gcd(\beta, N)$. From (51), we obtain the time-τ map

$$x_\tau \equiv x_0 + y_0\tau + \frac{\beta}{2}\tau(\tau+1) \mod N \qquad\qquad y_\tau \equiv y_0 \mod N. \tag{54}$$

The y-component is constant, while the x-component is a translation by U, where

$$U = U(y_0) \equiv y_0\tau + \frac{\beta}{2}\tau(\tau+1) \mod N.$$

It follows that all orbits of (51) have period equal to a multiple of τ, the multiple being the additive order of U modulo N, which is N/s where $s = s(y_0) = \gcd(U, N)$. We see that when $\beta > 0$, the N horizontal lines are partitioned into r invariant sets, each consisting of τ lines, for a total of τN points. These points are consumed in s cycles of period $\tau N/s$.

Several cases arise:

(i) If β is coprime to N and N is odd, then $r = 1$, $\tau = N$ and $U \equiv 0 \mod N$, independent of x_0 and y_0. The x_τ-translation is the identity, $s = N$, and the CP map (50) has N orbits of period N.
(ii) If β is coprime to N and N is even, then $r = 1$, $\tau = N$ and $U \equiv \beta N/2 \mod N$, independent of x_0 and y_0. We have $s = N/2$, and the CP map has $N/2$ orbits of period $2N$.
(iii) If $\gcd(\beta, N) = r > 1$ and $\tau = N/r$ is odd, then $U \equiv y_0\tau \mod N$. Then $s = \gcd(y_0\tau, r\tau) = \tau \gcd(y_0, r)$, contributing a period $N/\gcd(y_0, r) = \tau r/\gcd(y_0, r)$ for the CP map.
(iv) If $\gcd(\beta, N) = r > 1$ and $\tau = N/r$ is even, then $U \equiv y_0\tau + \beta\tau/2 \mod N$. Then $s = \gcd(y_0\tau + \beta\tau/2, r\tau) = (\tau/2)\gcd(2y_0 + \beta, 2r)$, contributing a period $2N/\gcd(2y_0 + \beta, 2r) = 2\tau r/\gcd(2y_0 + \beta, 2r)$ for the CP map.

We specialise to $N = p^n$ with p odd. If β and N are coprime (that is, $\beta \neq p^m$, $m = 1, \ldots, n-1$), then case (i) above applies, yielding the distribution $\mathcal{D}_1(x)$ in the limit $N \to \infty$ with p fixed or n fixed. Otherwise, if $\beta = p^m$, then case (iii) applies with $r = \beta$. Normalising periods by N, the allowable normalised periods take the form $1/\gcd(y_0, p^m) = p^{-l}$, $l = 0, \ldots, m$, consuming proportions of phase space equal to $p^{-m}\phi(p^m/\gcd(y_0, p^m)) = (1 - p^{-1})p^{-l}$, for $l < m$, and to p^{-m} for $l = m$. This reverts to the problem considered above, and the corresponding distribution functions in the remaining two limits in (49). □

Remark 6.1. The above proposition raises the question as to the choice of an appropriate normalisation parameter for the distribution function (33). In the case of the gamma distribution from Theorem 6.1.1, one verifies that the expectation value $\langle x \rangle$ of the normalised period with respect to the associated gamma-density xe^{-x} is equal to 2. This implies that the expected period $\langle t \rangle$ equals $2\bar{t}$, where the mean period $\bar{t}$ is given in (34).

We now study the respective quantities $\bar{t}$ and $\langle t \rangle$ for the singular distributions from Theorem 6.3.1. When $\alpha = \beta = 0$, the number of periodic orbits of minimal period t (or *t-cycles*) of the CP map over Λ_N is equal to

$$\#t\text{-cycles} = \frac{N}{t}\phi(t) = \begin{cases} N & \text{if } t = 1 \\ N \prod_{p|t} \left(1 - p^{-1}\right) & \text{if } t > 1 \end{cases} \tag{55}$$

where the product is taken over all prime divisors p of t. Hence the mean cycle length $\bar{t}$, given in Equation (34), is

$$\bar{t} = \frac{N^2}{\#\text{cycles}} = \frac{N}{1 + \sum\limits_{\substack{t|N \\ t>1}} \prod\limits_{p|t} \left(1 - p^{-1}\right)}. \tag{56}$$

As noted above, the number of points of period t over Λ_N is equal to $N\phi(t)$ if t divides N, and zero otherwise. It follows that the expectation value $\langle t \rangle$ for the period, with respect to the uniform measure on Λ_N, is given by

$$\langle t \rangle = \sum_{t|N} t \, \frac{\phi(t)}{N}. \tag{57}$$

Specialising the above quantities to the parameters $N = p^n$, we find

$$\begin{aligned} \bar{t} &= \frac{p^n}{1+\sum_{j=1}^{n}(1-p^{-1})} = \frac{p^{n+1}}{p(n+1)-n} \\ \langle t \rangle &= \sum_{i=0}^{n} p^i \frac{\phi(p^i)}{p^n} = \frac{1}{p^n} + \frac{p-1}{p^{n+1}} \sum_{i=1}^{n} p^{2i} = \frac{1}{p^n} + \frac{1}{p^{n-1}} \frac{p^{2n}-1}{p+1}. \end{aligned}$$

In the limit of large N with n fixed and $p \to \infty$, we have

$$\bar{t} \sim \frac{N}{n+1} \qquad \langle t \rangle \sim N.$$

In this case, the scaling parameter $\kappa = N = \langle t \rangle$ gives the simple limiting distribution $\mathcal{D}_1$, whereas the choice $\kappa = \bar{t}$ would lead to a shifted singularity.

If instead we take p fixed and $n \to \infty$, we find

$$\bar{t} \sim \frac{N}{\log_p(N)} \frac{p}{p-1} \qquad \langle t \rangle \sim N \frac{p}{p+1}.$$

Here, the presence of the logarithmic term in $\bar{t}$ would shift the singularities of $\mathcal{D}_p^{(m)}$ to infinity.

Remark 6.2. When $\alpha = 0$ in the CP map, many additional reversing symmetries are present because the CP map has many non-trivial symmetries, that is, the symmetry group $\mathcal{S}(T_N^{0,\beta})$ contains elements apart from the powers of $T_N^{0,\beta}$. When $\alpha = \beta = 0$, the x translation on any line, $x' = x + y_0$, commutes with any other translation on that line and has the involution $x' = -x$ as a reversing symmetry. Consequently, the CP map on Λ_N with $\alpha = \beta = 0$ commutes with any map $S_u : x' \equiv x + u(y) \mod N,\ y' \equiv y \mod N$, where u is any integer-valued function, and has the reversing symmetry $R : x' \equiv -x \mod N,\ y' \equiv y \mod N$. The latter is a different reversing symmetry to G of (36). As already discussed in the context of toral automorphisms in Section 5, the set of all symmetries and reversing symmetries together forms the reversing symmetry group. For instance, the composition of two reversing symmetries commutes with the map, so we see that $R \circ G : x' = -x, y' = -y$ also commutes with $T_N^{0,0}$. When $\alpha = 0$ but $\beta \neq 0$, the proof above shows that the τ-th iterate of the CP map again reduces to x-translations on each horizontal line, and then inherits the aforementioned commuting maps and reversing symmetries (in this case, we say that the CP map has (reversing) τ-symmetries [14]). The appearance of the gamma distribution $\mathcal{R}(x)$ has been confined to maps T that have no non-trivial commuting maps (other than their powers, that is $\mathcal{S}(T) = \langle T \rangle \simeq C_\infty$) and a single generating reversing symmetry.

As already stated at the beginning of Section 6.3.2, the case $\alpha = \beta = 0$ is very special among all (rational) parameter pairs. We now return to the CP map for general α, β and their anomalous distributions on some lines in parameter space. As a first example, let us have a closer look at the case $\alpha = \beta \neq 0$ on the prime lattice Λ_p.

Example 6.1. In the case $\alpha = \beta$, the dynamics on Λ_p of the two variables on either side of the discontinuity can be partly decoupled. The action of $T_p^{\alpha,\alpha}$ becomes $T_p^{\alpha,\alpha}\binom{x}{y} = \binom{x+y+2\alpha}{y+2\alpha}$ if $x \leq \frac{p-1}{2}$ and $T_p^{\alpha,\alpha}\binom{x}{y} = \binom{x+y}{y}$ otherwise. Points of the shape $(x, 0)$ for $x > \frac{p-1}{2}$ are elements of $\mathsf{Fix}(G) \cap \mathsf{Fix}(H)$, hence fixed points of $T_N^{\alpha,\alpha}$. Consequently, the non-trivial rest of $\mathsf{Fix}(H)$

consists of the points $(x, 0)$ with $x \leq \frac{p-1}{2}$; the non-fixed points of $\mathsf{Fix}(G)$ are the pairs $(x, -\alpha \mod p)$, for $x \leq \frac{p-1}{2}$.

For the dynamics, one finds that the y-coordinate is increased by 2α (modulo p) in each iteration as long as the current point is in the left half, and does not change anymore to the right of $1/2$. Let k denote the number of iterations on the left hand side. Then $2\alpha k \equiv -\alpha \mod p$, or $\alpha(2k+1) \equiv 0 \mod p$. Consequently, each arc has precisely $k = \frac{p-1}{2}$ points on the left hand side. Moreover, all arcs of symmetric orbits start from a point $(x_1, 0) \in \mathsf{Fix}(H)$ and end on $(x_2, -\alpha \mod p)$ for some $x_1, x_2 \leq \frac{p-1}{2}$. In particular, all symmetric orbits are odd.

If we assume some 'orbit-wise balance' with respect to the number of points on each side of the discontinuity, that would mean there are also roughly $p/2$ points on the right hand side for 'most' non-trivial orbits, giving a total number iterations of $T_p^{\alpha,\alpha}$ in one arc close to p. Recall that the number of iterations between two points on the fixed lines is about half the orbit lengths, see Section 6.1. Hence, under this assumption of 'orbit-wise balance', as well as the dominance of symmetric orbits, we would expect most non-trivial orbits to cluster around the orbit length of $\approx 2p$. With the scaling according to Equation (34), this would give an orbit distribution function close to a step function with 'jump' at value two. Indeed, this is what numerical enumeration of the periodic orbits for large primes and arbitrary $\alpha = \beta$ suggests, compare Conjecture 4 below. ◊

To deal with anomalous distributions on more general lines, we consider the following sequence of functions

$$\mathcal{R}^{(k)}(x) = \sum_{j=1}^{n(x)} \frac{j(k-1)^{j-1}}{k^{j+1}}\,, \qquad n(x) = \lceil kx \rceil - 1, \qquad k = 2, 4, 6, \ldots. \tag{58}$$

For $x \leqslant 1/k$ the sum is empty, and $\mathcal{R}^{(k)}$ is defined to be zero. These are step-functions, with steps at the integer multiples of k^{-1}. The index k is restricted to even values because for odd k these functions are not relevant to the periodic orbits of the CP map. The functional form of these singular distributions is an educated guess, based on the results of accurate numerical calculations (see Section 7). At the end of this section, we offer a heuristic argument to justify the location of the singularities of these distributions.

Next we show that the functions $\mathcal{R}^{(k)}$ are distribution functions that converge to the gamma distribution as $k \to \infty$. For each k, the function $\mathcal{R}^{(k)}$ is non-negative and non-decreasing; to show that $\mathcal{R}^{(k)}$ is a distribution function we must verify that $\lim_{x\to\infty} \mathcal{R}^{(k)}(x) = 1$.

Lemma 6.3.2. *The following limits hold for the functions from Equation* (58)*,*

$$\lim_{x\to\infty} \mathcal{R}^{(k)}(x) = 1 \qquad \textit{and} \qquad \lim_{k\to\infty} \mathcal{R}^{(k)}(x) = \mathcal{R}(x), \quad x \geqslant 0.$$

Proof. Using the derivative of the geometric series to evaluate the sum, one obtains

$$\begin{aligned}\sum_{j=1}^{n} \frac{j(k-1)^{j-1}}{k^{j+1}} &= \frac{1}{k^2} \cdot \frac{n\left(\frac{k-1}{k}\right)^{n+1} - (n+1)\left(\frac{k-1}{k}\right)^{n} + 1}{(\frac{k-1}{k} - 1)^2} \\ &= 1 - \left(1 - \frac{1}{k}\right)^{n+1} \left(\frac{k}{k-1} + \frac{n}{k-1}\right).\end{aligned}$$

Using (58), and noting that $n(x) = kx + O(1)$, with kx being a lower bound, we obtain

$$\lim_{x\to\infty} \mathcal{R}^{(k)}(x) = 1 - \lim_{n\to\infty} \left(1 - \frac{1}{k}\right)^{n+1} \left(\frac{k}{k-1} + \frac{n}{k-1}\right) = 1$$

as desired. Likewise, we find

$$\begin{aligned}\lim_{k\to\infty} \mathcal{R}^{(k)}(x) &= 1 - \lim_{k\to\infty} \left(1 - \frac{1}{k}\right)^{kx} \left(1 - \frac{1}{k}\right)^{O(1)} \left(\frac{k}{k-1} + \frac{k}{k-1}x + \frac{O(1)}{k-1}\right) \\ &= 1 - e^{-x}(1+x) = \mathcal{R}(x),\end{aligned}$$

which completes the argument. □

Let us now return to the CP map. We construct a sequence of lines in parameter space, with integer slope, again limiting ourselves to rational numbers with prime denominator $N = p$.

$$\Lambda_p^{(k)} = \{(\alpha, \beta) \in \Lambda_p \setminus \{(0,0)\} \,:\, \beta = k\alpha\} \qquad p \text{ prime}, \quad k = 1, \ldots, p-1.$$

The discrete lines $\Lambda_p^{(k)}$ are disjoint, and their union is the whole of Λ_p, apart from the set $\alpha\beta = 0$ (the union of two lines). For fixed k, we examine the period distributions for parameter pairs restricted to $\Lambda_p^{(k)}$, and then we let p go to infinity. We shall repeat the procedure used for unconstrained parameter pairs, with the obvious modifications.

We fix a positive real constant c, and consider the quantity

$$E_p^{(k)}(c) = \frac{\left|\{(\alpha, \beta) \in \Lambda_p^{(k)} \,:\, \mathcal{E}_p^{(k)}(\alpha) < c\}\right|}{p-1}$$

where the L^1-norm

$$\mathcal{E}_p^{(k)}(\alpha) = \int_0^\infty |\mathcal{D}_{p,\alpha,k\alpha}(x) - \mathcal{R}^{(k)}(x)|\, dx \tag{59}$$

measures the distance between the empirical and the theoretical values.

Finally, we define

$$E^{(k)}(c) = \liminf_{p\to\infty} E_p^{(k)}(c) \qquad c > 0.$$

Numerical evidence suggests the following

Conjecture 2. *For every even integer k, the function $E^{(k)}$ is identically equal to* 1.

Thus letting p and then k go to infinity (in that order) we recover the gamma distribution.

There is a sequence of distributions analogous to (58) for odd k. However, we have been only able to identify precisely the first few terms of this sequence. A restricted version of Conjecture 2 for odd k will be stated in Section 7.

The appearance of singular distributions along the lines $\beta = k\alpha$ can be justified heuristically, assuming ergodicity. From [43, Eq. (3)], we find, for the t-th iterate of the initial point (x_0, y_0),

$$y_t(x_0, y_0) = y_0 + \beta t + \alpha S_t \;\text{ with }\; S_t = \sum_{k=0}^{t-1} \theta(x_k).$$

Let $\beta = k\alpha$, for some $k = 1, \ldots, p-1$, and assume that both numerator and denominator of β are co-prime to p. The above equation becomes a congruence modulo p, and for periodicity ($y_t = y_0$), we require

$$tk + S_t = tk\left(1 + \frac{S_t}{tk}\right) \equiv 0 \mod p$$

to be solved for the smallest $t > 0$. Suppose now that the sequence (x_k) is uniformly distributed in the unit interval. This implies that, as $t \to \infty$, we have $S_t = o(t)$, and hence, asymptotically, kt is an integer multiple of p. After scaling the periods by p, the distribution function approaches a step function, with steps at (some) integer multiples of k^{-1}.

6.3.3 Asymmetric orbits

The CP map shares another property of random reversible maps, namely the fact that, losely speaking, almost all cycles are symmetric. More precisely, one finds that typically, for almost any choice of parameters, the fraction of points that lie in a symmetric orbit of the CP map is very close to 1. Thus, for rational α and β with common prime denominator p, we consider the proportion $\mathcal{A}_p(\alpha, \beta)$ of points z on the prime lattice Λ_p which belong to asymmetric periodic orbits (this means that $G(z)$ is not in the orbit of z),

$$\mathcal{A}_p(\alpha, \beta) = \frac{|\{z \in \Lambda_p \,:\, z \text{ belongs to an asymmetric cycle}\}|}{p^2}. \tag{60}$$

As done above, we fix a real constant $c \geqslant 0$ and define

$$A_p(c) = \frac{|\{(\alpha, \beta) \in \Lambda_p \,:\, \mathcal{A}_p(\alpha, \beta) \leqslant c\}|}{p^2} \tag{61}$$

which is the fraction of parameter pairs for which the proportion of asymmetric orbits does not exceed c. The function $\mathcal{A}_p$ is non-decreasing, and it is equal to 1 for $c \geqslant 1$. After defining

$$A(c) = \liminf_{p \to \infty} A_p(c) \qquad c \geqslant 0 \tag{62}$$

we can formulate our third conjecture.

Conjecture 3. *The function A from Equation* (62) *is identically equal to* 1.

In the next section, evidence in support of the conjectures stated above is provided.

7 Supporting evidence

A typical computation consists of determining the period of all symmetric periodic orbits of the map T on a prime lattice Λ_p, for some large prime number p, and a rational parameter pair $(\alpha, \beta) \in \Lambda_p$. This process involves a one-dimensional search along the symmetry lines $\mathsf{Fix}(G)$ and $\mathsf{Fix}(H)$, given by Equation (38). All computations entail integer arithmetic modulo p, as described in Section 6.2.

It turns out that the fraction of points from phase space that are consumed in symmetric orbits (in the sense of Section 6.1) is close to 1 (Conjecture 3), and so the total number of iterations of the map is typically very close to $p^2/2$. The required storage is only $2p$ —the combined size of the symmetry lines— since there is no need to record the points in the orbits which lie outside the symmetry lines.

Let us comment on some details of computational nature, as they are relevant to the algorithmic implementation. From the period data we compute the distribution function $\mathcal{D}_p$, and its distance $\mathcal{E}_p(\alpha, \beta)$ from the gamma distribution $\mathcal{R}$, or the distance $\mathcal{E}_p^{(k)}(\alpha)$ from the singular distribution $\mathcal{R}^{(k)}$, as appropriate —see Equations (41) and (59). In addition, we compute the fraction $\mathcal{A}_p$ of the space occupied by asymmetric orbits, and monitor the rate at which this quantity converges to zero. For large values of p, the actual period data are discarded, to reduce the size of the output data files.

From Lemma 6.2.1, to obtain a complete representation of parameter space for given p, it suffices to consider the restricted range

$$0 \leqslant \alpha < \lfloor p/2 \rfloor \qquad\qquad 0 \leqslant \beta < p - 1.$$

7.1 Convergence to the gamma distribution

An overview of the behaviour of the function $\mathcal{E}_p(\alpha, \beta)$ over the entire parameter space is illustrated in Figure 8. These data, and all the data in the rest of this section, correspond to the scaling constant $\kappa = \bar{t}$, see Equation (34). Each pixel in the figure represents a pair (α, β), and the value of $\mathcal{E}_p(\alpha, \beta)$ is encoded on a grey scale. The larger the deviation from the gamma distribution, the darker the pixel. Thus the white areas correspond to small values of $\mathcal{E}$, which indicate proximity to $\mathcal{R}$, while the black pixels represent the largest deviations.

Before examining the nature of the large deviations from the gamma distribution, we consider the typical behaviour of the distribution function, using the construct developed in Section 6.3. In Figure 10, we show the function $E_p(c)$, for three increasing values of p. Details of this figure are displayed in Figure 11, showing the behaviour near the origin and near the top. Near the origin, the empirical distribution remains zero (or very small) over a gradually shrinking interval. At the same time, the graph of E_p raises towards 1, while anomalies are smoothed out. In addition (not evident from the picture), the smallest value of c for which one has $E_p(c) = 1$ migrates to the right (see below). These data provide convincing evidence for the convergence of E_p to 1, which is Conjecture 1. The overall rate of convergence is slow —approximately logarithmic in p.

Large deviations from the gamma distribution originate from two distinct phenomena, which we describe in the next two sections.

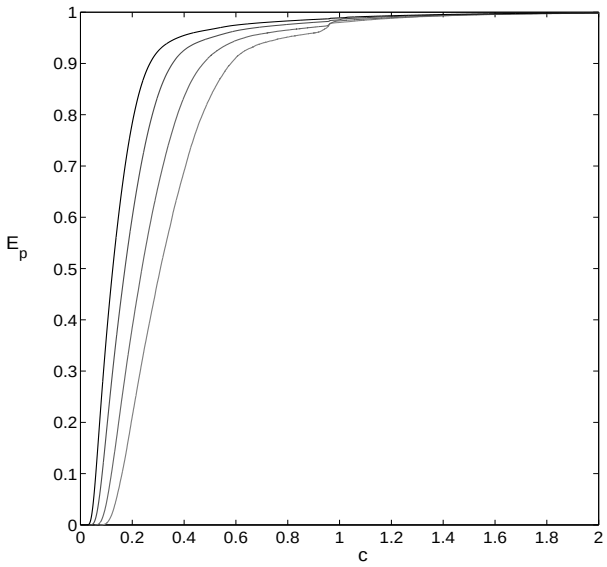


Figure 10: The function $E_p(c)$ —see Equation (42)— for $p \in \{251, 499, 1103, 2339\}$ (right to left). As p increases, we see non-uniform convergence of $E_p(c)$ to 1 (cf. Section 6.3.1), supporting Conjecture 1.

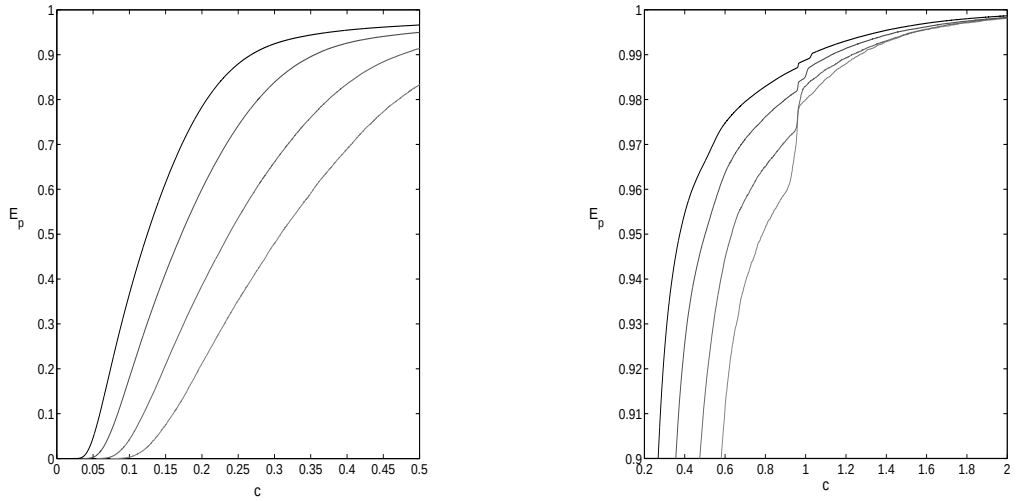


Figure 11: Details of Figure 10. Left: the behaviour of $E_p(c)$ near the origin. Right: behaviour near the top. The curves in the right image do not intersect.

7.2 Anomalous sectors

Data from exact numerical computations show that there are anomalous distributions in the vicinity of many low-order (i.e., small denominator) rational parameter pairs, which we call *cluster points*. The most prominent cluster points are $(0, 0)$ and $(1/2, 1/2)$ but several others are visible elsewhere (see Figure 8). However, cluster points are missing at some low-order rational parameters, such as those of the form $(0, m/n)$, with even n.

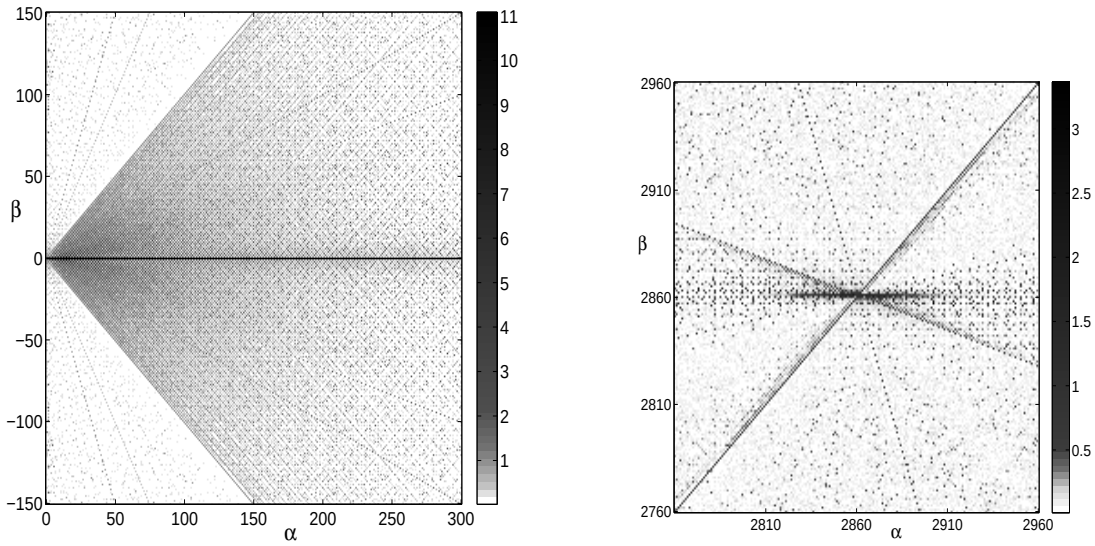


Figure 12: Details of the anomalous sectors of two cluster points. The values of the function $\mathcal{E}_p(\alpha, \beta)$, are represented on a grey scale, with the largest values in black. Left: the sectors of the cluster point $(\alpha, \beta) = (0, 0)$, for $p = 9011$. Right: the sectors of the cluster point $(1/4, 1/4)$, but now shown for the larger prime $p = 11433$.

To each cluster point we associate two rational lines, one with positive slope, and one with negative slope. These lines divide the neighbourhood of a cluster into four *sectors* (taking into account the periodicity of parameter space, if necessary). For instance, the sectors of the clusters at $(0, 0)$ and $(1/2, 1/2)$ are determined by the lines with slope ± 1.

Details of the cluster points at $(0, 0)$ and $(1/4, 1/4)$ are shown in Figure 12. The behaviour of $\mathcal{E}$ changes markedly and abruptly from sector to sector. The East and West sectors, which we call the *anomalous sectors,* feature deviations from the gamma distribution which are not only larger in value, but which also affect a two-dimensional region in parameter space. By contrast, the large fluctuations within the North and South sectors —the *regular sectors*— are confined to one-dimensional rational lines (see below).

Thus, near the $(0, 0)$ cluster point, convergence to the gamma distribution is much faster for $|\beta| > |\alpha|$ than for $|\beta| \leqslant |\alpha|$. Within the former domain, the lines $\alpha = 0$ and $3\alpha = \pm\beta$ feature the most prominent fluctuations, while all other rational lines give much smaller deviations. On the other hand, within the anomalous sector $|\beta| \leqslant |\alpha|$, large deviations are found to occur for even values of $\gamma = \alpha + \beta$. There are also large fluctuations on rational lines, most notably the lines $\beta = 0$ and $|\beta| = \alpha/3$.

In the anomalous sectors, a mechanism is at work which delays convergence of averages. In order to reconcile these findings with the data shown previously, we provide evidence that these fluctuations do indeed decay to zero, as $p \to \infty$. In Figure 13, we compare the value of $\mathcal{E}_p$ in the anomalous and regular sectors near $(0, 0)$, for increasing values of p. To isolate the dominant features, we perform a double average. First, we average $\mathcal{E}_p$ over the lines $\gamma = const$ (cf. Equation (32)), because we found that the variations of $\mathcal{E}$ are much stronger along the

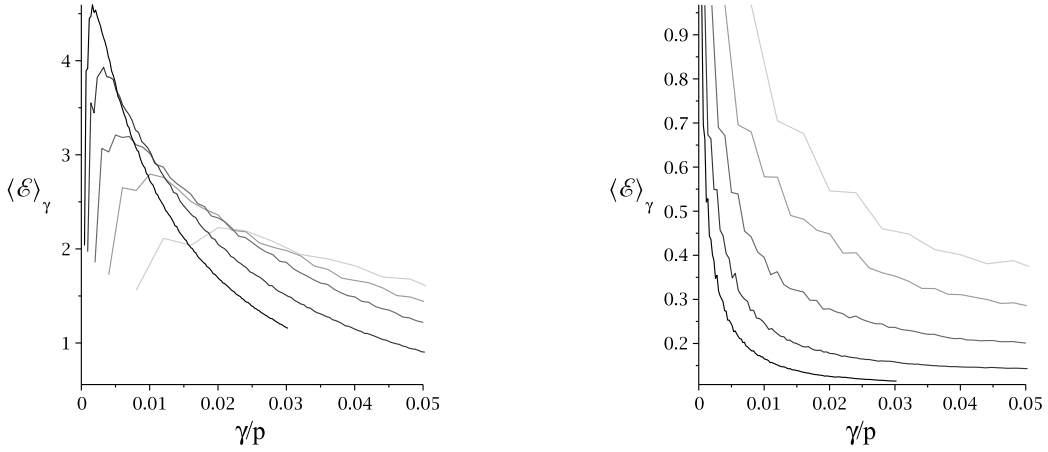


Figure 13: Left: Non-uniform convergence to the gamma distribution for parameters pairs (α, β) within an anomalous sector of the cluster point $(0, 0)$ $(0 < \beta < \alpha)$. The five curves in increasing darkness correspond to the primes $p \in \{499, 997, 1999, 4297, 8599\}$. In each case we plot the Cesàro sum $\langle \mathcal{E} \rangle_\gamma$, given in Equation (63), as a function of γ/p for even values of γ (the odd values of γ give much lower values of $\bar{\mathcal{E}}_\gamma$). Right: the same functions, within the regular sector $(0 < \alpha < \beta)$.

orthogonal coordinate δ. Thus, inside the anomalous sector, we compute

$$\bar{\mathcal{E}}_\gamma = \frac{1}{n} \sum_{\alpha=1}^{n} \mathcal{E}_p(\alpha, \gamma - \alpha) \ , \qquad n(\gamma) = \left\lfloor \frac{\gamma - 1}{2} \right\rfloor .$$

(The quantity $\mathcal{E}_p(\gamma - \alpha, \alpha)$ is used for the regular sector.) Then we perform a Cesàro sum over γ

$$\langle \mathcal{E} \rangle_\gamma = \frac{1}{\gamma - 2} \sum_{\gamma'=3}^{\gamma} \bar{\mathcal{E}}_{\gamma'}. \tag{63}$$

As p increases, the function $\langle \mathcal{E} \rangle_\gamma$ develops a singular profile within the anomalous sector, within an overall logarithmic convergence to zero. This behaviour is indeed consistent with Conjecture 1, but it suggests that the smallest value of c for which $E_p(c) = 1$, diverges to infinity, as $p \to \infty$. Equivalently, there exist sequences of rational parameter values, converging to $(0, 0)$, along which the distance from the gamma distribution diverges to infinity. These anomalous distributions are dominated by the presence of few very large cycles.

7.3 Singular distributions on rational lines

A second source of large fluctuations are anomalous distributions along lines with rational slope, the most prominent of which are

$$\beta = \pm\alpha, \quad \beta = \pm 3\alpha.$$

On these lines, the distribution function has a step-like behaviour, which accounts for the large value of $\mathcal{E}$.

There are in fact singular distributions on all parametric lines of the form $\beta = k\alpha$. The corresponding empirical distributions are defined as

$$\mathcal{R}^{(k)}_{p,\alpha}(x) := \mathcal{D}_{p,\alpha,k\alpha}(x) \tag{64}$$

where $\mathcal{D}$ was defined in (33), and the parameter dependence has been made explicit (see also Equation (59)). Some empirical singular distribution are plotted in Figure 14. The conjectured analytical form $\mathcal{R}^{(k)}$ of the distributions corresponding to even values of k is given in Equation (58). These functions have been determined by an educated guess on the basis of examining empirical distributions for large primes.

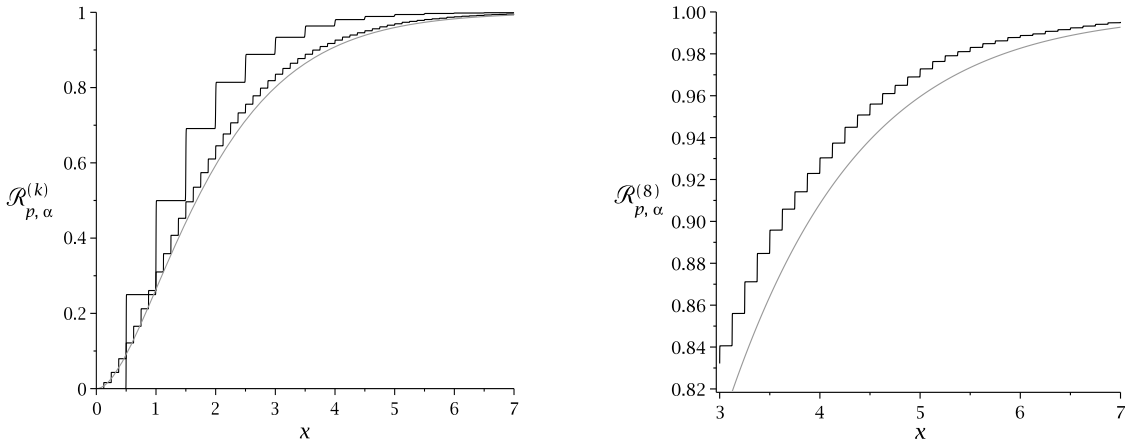


Figure 14: Empirical period distribution functions $\mathcal{R}^{(k)}_{p,\alpha}$ on rational lines $\beta = k\alpha$, for even k. Left: for the prime $p = 81799$ and $\alpha = 70$, we display the distributions for $k = 2$ (large steps) and $k = 8$ (small steps). The smooth curve is the gamma distribution. Right: blow-up of the fine structure of the function $\mathcal{R}^{(8)}_{p,\alpha}$, in the range $3 \leqslant x \leqslant 7$, showing the 32 steps predicted by formula (58). Again, the smooth curve is the gamma distribution.

Our experiments show that there are analogous distributions on prime lattices also for odd k. However, apart from the values $k = 1, 3$, we could only locate the singularities of these distributions, but not their analytical form. The empirical distributions for $k = 1, 3, 5$ are shown in Figure 15. Of note is the fact that $\mathcal{R}^{(1)}_{p,\alpha}$ and $\mathcal{R}^{(3)}_{p,\alpha}$ have finitely many steps; by contrast $\mathcal{R}^{(5)}_{p,\alpha}$ appears to have infinitely many steps at the integer multiples of $2/5$, although the value of the heights of the steps is not obvious.

The result for $k = 1, 3$ leads to the following

Conjecture 4. *In the limit of large primes p, and independent of α, the empirical period distribution $\mathcal{R}^{(k)}_{p,\alpha}$ for the Casati-Prosen map with parameters $\beta = k\alpha$, for $k = 1$ and $k = 3$ converges, respectively, to the functions*

$$\mathcal{R}^{(1)}(x) = \begin{cases} 0 & \text{if } x < 2 \\ 1 & \text{if } x \geqslant 2 \end{cases} \qquad \mathcal{R}^{(3)}(x) = \begin{cases} 0 & \text{if } x < \frac{2}{3} \\ \frac{1}{3} & \text{if } \frac{2}{3} \leqslant x < \frac{4}{3} \\ 1 & \text{if } \frac{4}{3} \leqslant x. \end{cases} \tag{65}$$

In Figure 16, we analyse the emergence of the singularity at $x = 2$ for the distribution $\mathcal{R}^{(1)}_{p,\alpha}$, for two primes and a sample of values of α. The build-up of the step in the distribution function is quite regular, and seems to be optimal for $\alpha = 1$.

To gain an overview of this phenomenon, we plot the value of the norm $\mathcal{E}^{(k)}_p(\alpha)$ ((59) with (64)) for two large primes p, for $k = 1$ and $k = 3$, over the full range of α values (Figure 17). The convergence of the empirical distributions $\mathcal{R}^{(k)}_{p,\alpha}$ to their conjectured value (65) is noticeably faster for $k = 3$ (and, in both cases, roughly algebraic in p, with exponent

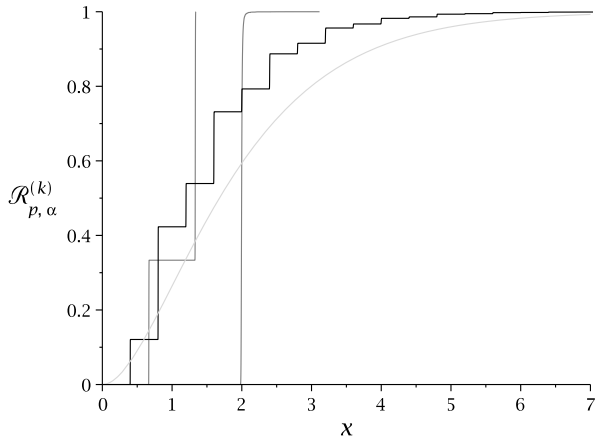


Figure 15: Empirical period distribution functions $\mathcal{R}^{(k)}_{p,\alpha}$ on rational lines $\beta = k\alpha$, for odd k. For the prime $p = 81799$ and $\alpha = 5$, we display the empirical distributions for $k = 1$ (one step), $k = 3$ (two steps), and $k = 5$ (several steps). The smooth curve is the gamma distribution.

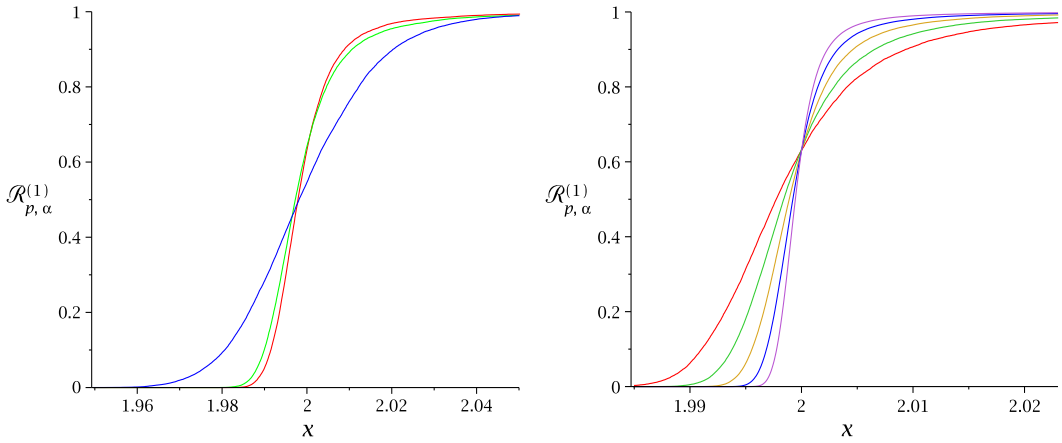


Figure 16: Convergence of the empirical distribution $\mathcal{R}^{(1)}_{p,\alpha}$ to $\mathcal{R}^{(1)}$ ($\beta = \alpha$), in the proximity of the step at $x = 2$. Left: The prime $p = 53993$ is fixed and shown are the distributions for $\alpha \in \{1, 2, 23936\}$. The steepest curves correspond to the values $\alpha \in \{1, 2\}$. Right: Shown are the distributions $\mathcal{R}^{(1)}_{p,\alpha}$ for fixed $\alpha = 1$ and the sequence of primes $p \in \{50021, 100043, 200023, 400033, 800077\}$. The convergence to the step function improves with the prime.

close to $-1/2$). Convergence is uniform in α, and the data show evidence of scaling in the fluctuations. For $k = 1$, the fastest convergence takes place near the endpoints of the line, which are the cluster points $(0, 0)$ and $(1/2, 1/2)$.

7.4 Asymmetric orbits

Here, we provide evidence for the validity of Conjecture 3. From the knowledge of the periods of all symmetric orbits, one determines the value of the expression $\mathcal{A}_p(\alpha, \beta)$ for the desired set of parameters.

Numerical calculations show that, much like for the distance from the gamma distribution,

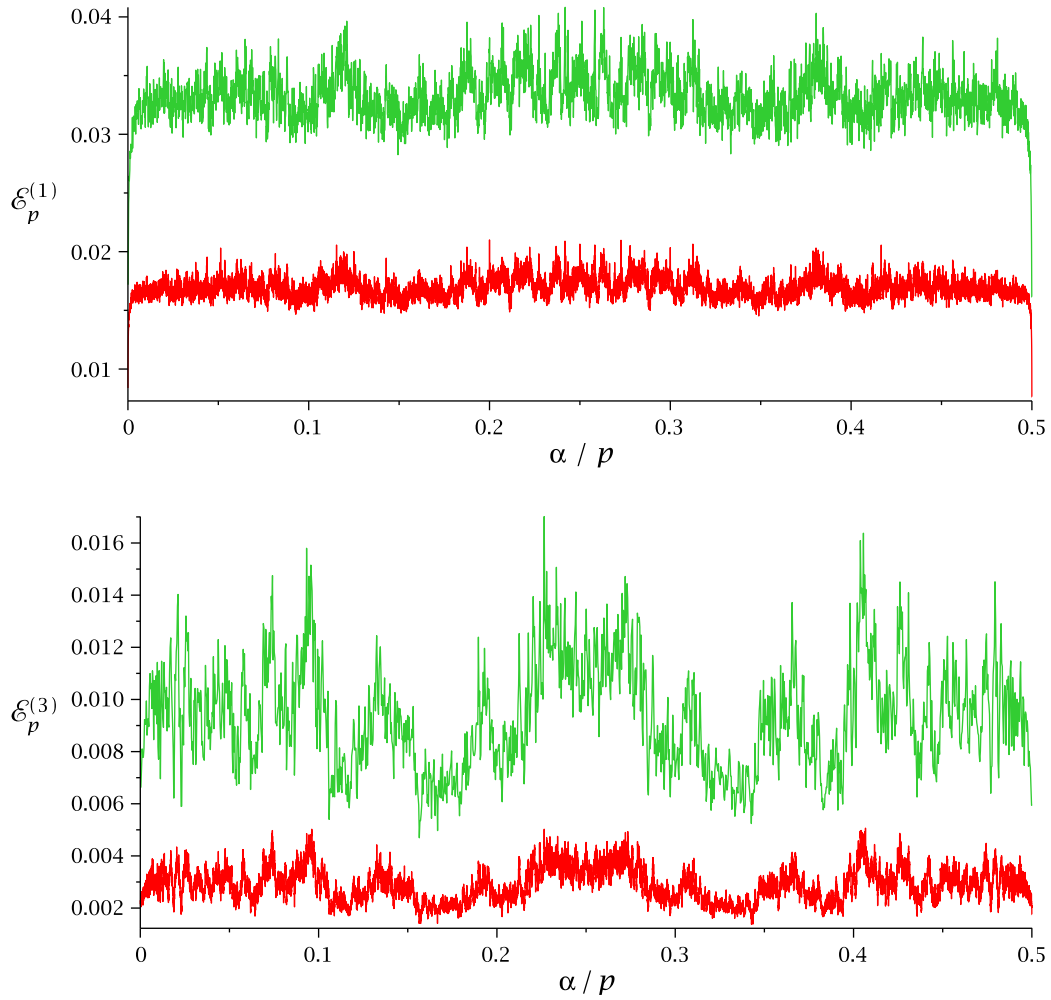


Figure 17: In the top figure, we plot the norm $\mathcal{E}_p^{(1)}(\alpha)$ as a function of $\alpha/p \in [0, \frac{1}{2}]$ for the primes $p = 7699$ and $p = 33521$, the latter giving the smaller norm. In the bottom figure, we plot the norm $\mathcal{E}_p^{(3)}(\alpha)$ as a function of α/p for the primes $p = 2927$ and $p = 33521$. The convergence for $\mathcal{E}_p^{(3)}(\alpha)$ is noticeably better than for $\mathcal{E}_p^{(1)}(\alpha)$, as can be seen from the smaller values of $\mathcal{E}_p^{(3)}(\alpha)$.

the proportion of asymmetric periodic orbits is small on average, but also far from uniform in parameter space. We first consider the distribution function $A_p(c)$, defined in Equation (61). In Figures 18 and 19, we show the empirical function $A_p(c)$, for three increasing values of p. As for E_p, the convergence to 1 is non-uniform, and approximately logarithmic. Note that, as p increases, the value of $A_p(0)$ decreases, because, due to the improved statistics, a small number of asymmetric orbits appears for an increasing fraction of parameter values.

Figure 9 is the analogue of Figure 8 for asymmetric orbits. The function $\mathcal{A}_p(\alpha, \beta)$ is coded on a grey scale; the zones with the highest proportion of asymmetric orbits, the darkest pixels, form anomalous sectors, which develop around cluster points. The structure of the function $\mathcal{A}_p$ is similar to that of $\mathcal{E}_p$, with two important differences. First, the rational lines are not anomalous. Second, the anomalous sectors include sectors which are not anomalous for $\mathcal{E}_p$, such as those of the form $(0, m/n)$, with even n.

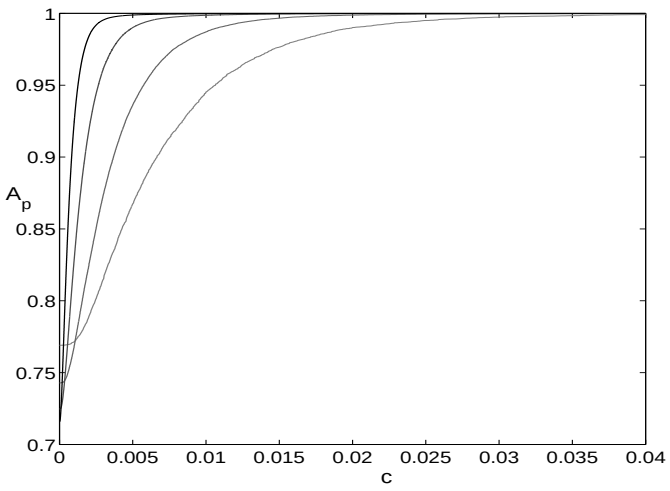


Figure 18: Details of the functions $A_p(c)$ —see Equation (61)— near the origin, for $p \in \{251, 499, 1103, 2339\}$ (right to left). As p increases, we see non-uniform convergence of $A_p(c)$ to 1, supporting Conjecture 3.

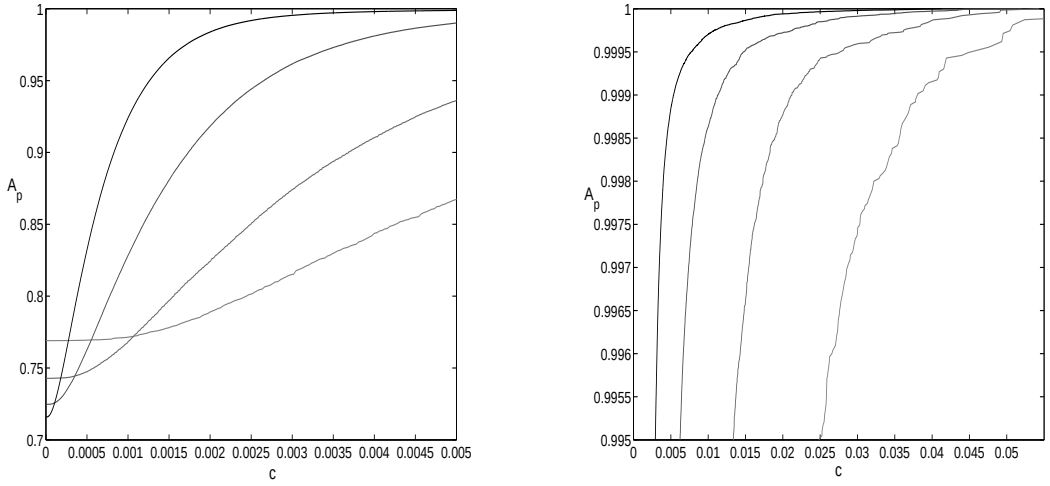


Figure 19: Details of Figure 18. Left: the behaviour of $A_p(c)$ near the origin. Right: behaviour near the top.

The neighbourhood of the $(0, 0)$ cluster is shown in Figure 20, for the prime $p = 8599$. The structure is rather similar to that of Figure 12, even though the boundary of the anomalous sector seems somewhat shifted away from the line $\alpha = \beta$. Finally, in Figure 21, the analogue of Figure 13, we compare the value of $\mathcal{A}_p$ in the anomalous and regular sectors near $(0, 0)$, for increasing values of p. The averaging procedure to determine $\langle \mathcal{A} \rangle_\gamma$ is the analogue of that described by Equation (63).

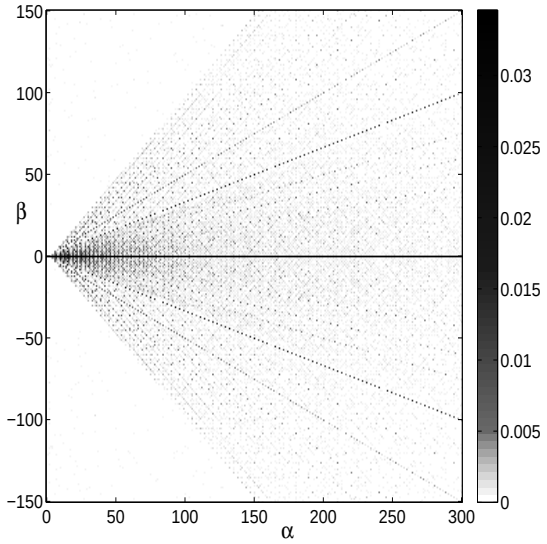


Figure 20: Details of the parameter dependence of the function $\mathcal{A}_p(\alpha, \beta)$, for the prime $p = 9011$, in the vicinity of the origin. The darker dots represent the parameter pairs corresponding to a relatively large proportion of asymmetric orbits. The corresponding picture for $\mathcal{E}_p(\alpha, \beta)$ for this prime was shown in the left frame of Figure 12.

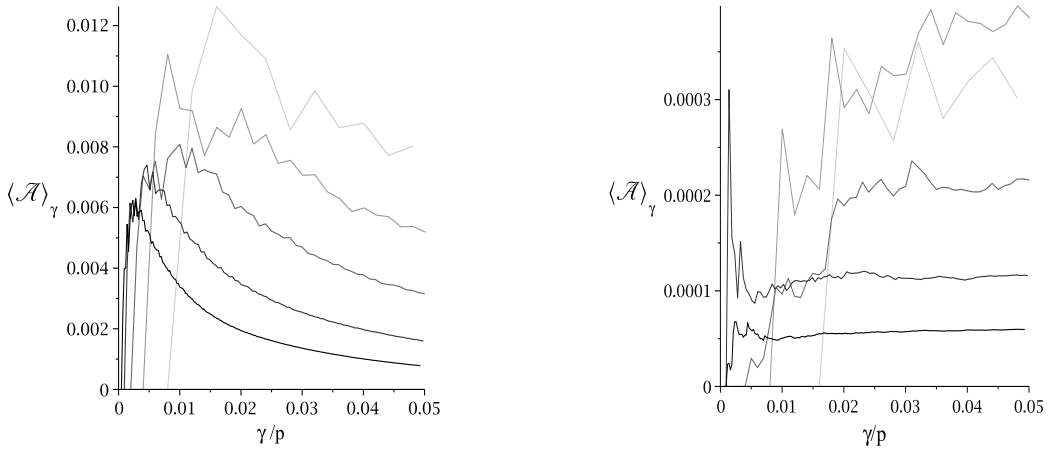


Figure 21: Left: Analogous to Figure 13, but now considering proportion of asymmetric periodic points for parameters pairs (α, β) within an anomalous sector of the cluster point $(0, 0)$ $(0 < \beta < \alpha)$. The five curves in increasing darkness correspond to the primes $p \in \{499, 997, 1999, 4297, 8599\}$. In each case we plot the Cesàro average $\langle \mathcal{A} \rangle_\gamma$ of $\mathcal{A}_p(\alpha, \beta)$, over the parameter pairs satisfying $\alpha + \beta = \gamma$, as a function of γ/p. The dominant contribution to the nature of each curve comes again from the even values of γ, whereas averages over odd values of γ give systematically lower values of $\langle \mathcal{A} \rangle_\gamma$. Right: the same functions, within the regular sector $(0 < \alpha < \beta)$.

7.5 Concluding remarks

Our study of the CP map provides further evidence of the ubiquity and universality of the gamma distribution $\mathcal{R}(x)$ for periodic orbits of reversible maps. This asymptotic distribution

had not been previously observed on a zero-entropy map, and it seems to require milder ergodic properties than originally thought. We have also shown that, within the same two-parameter family of maps, it is possible to observe a transition from singular distributions to the gamma distribution.

The restriction to prime lattices has been necessary to obtain well-behaved singular distributions $\mathcal{R}^{(k)}$ along rational lines. For composite values of N, things are more difficult. Unlike endormorphisms of the torus, the CP map does not respect the direct product structure of lattices Λ_N for composite N, such that the dynamics cannot be decomposed from that on sublattices. Explicit computation suggests that the orbit distribution crucially depends on the fact whether N is coprime with the parameter values α, β or shares a common factor with either of them. A source of strong deviation from the gamma distribution seems to come from the (approximate) absence of symmetric orbits for certain parameter pairs. Figure 22 illustrates the additional symmetries in parameter space for N even from Lemma 6.2.1, as well as horizontal lines of parameter pairs that induce period length distributions that drastically differ from the gamma distribution.

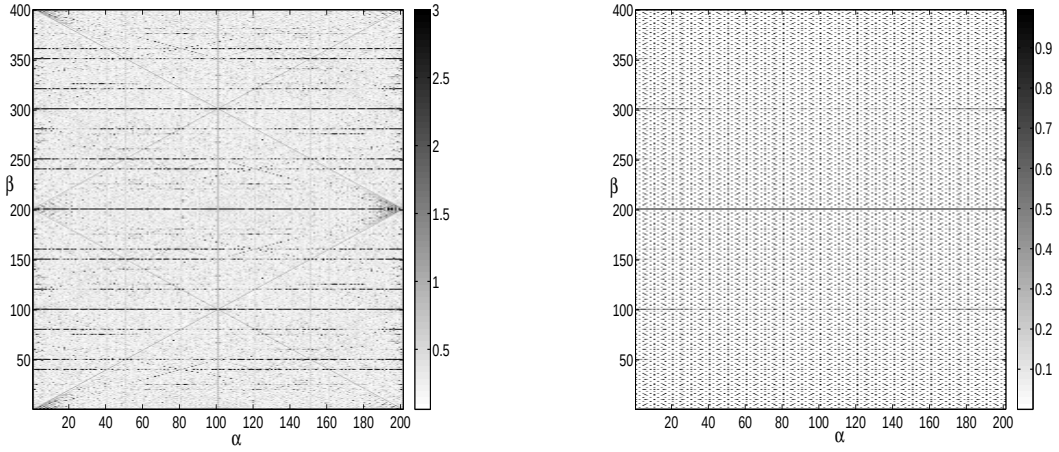


Figure 22: The analogues of Figures 8 and 9 for the composite $N = 400$. The left image illustrates the additional symmetries from Lemma 6.2.1; the values of $\mathcal{E}_p$ were truncated at 3, in order to obtain a clearer picture, the true maximum lies at ≈ 70. The right image shows that, for composite N, there are many parameter values for which the symmetric orbits do not dominate the orbit statistics any longer.

Our computations further suggest that also the precise location of the discontinuity within the interval $(0, 1)$ could be treated as another parameter without essentially altering the qualitative behaviour of the period distribution. For "most" parameter pairs, one still sees the gamma distribution, and for the singular distributions found for parameter pairs on certain rational lines in parameter space, only the positions of the singularities seems to be affected, not the type of the distribution.

Many questions raised by our findings remain unanswered, the main issue being a rigorous justification of the asymptotic emergence of the gamma distribution. Another intriguing problem is the identification of the mechanism responsible for slow convergence to averages in the anomalous sectors of parameter space. Within these sectors we observe a large variety of orbit distributions, which differ considerably from the singular distributions seen on rational

lines.

The conjectured form of singular distributions $\mathcal{R}^{(k)}$ is attractively simple, yet at present we have no rigorous explanation of their origin. We note that singular period distributions often have an arithmetical characterisation. We have pointed out that in the case of toral automorphisms, the singular behaviour results from the presence of Abelian groups, whose normalised order depend on the prime factorisation of the lattice size N. Singular distributions also appear for integrable rational maps acting over finite fields [70, 46]. The underlying Abelian groups now are addition over the elliptic curves that foliate the phase space. The Hasse-Weil bound ensures that, asymptotically, the normalised order of these groups is the same, leading again to steps in the period distribution function.

From an ergodic-theoretic viewpoint, all phenomena described in this work refer to exceptional values, both in parameter space, and in phase space. However, looking at rationals in order to understand irrationals is natural, and it is quite possible that our findings are the manifestation of phenomena that concern generic parameter values as well.

8 Summary and outlook

In this thesis, we have investigated selected aspects concerning the structure and distribution of periodic orbits in certain discrete dynamical systems.

In the first part, we have given an account of the structure and numbers of finite orbits of toral endomorphisms on the rational lattices of the d-dimensional torus.

We have discussed the relation between global and local fixed point counts and studied the subgroups of the lattices induced by toral endomorphisms by means of matrix equivalence over $\mathbb{Z}$; we have provided an algebraic formulation of the problem of fixed point counting by relating it to linear recursions and conjugacy problems, and given an interpretation of known conjugacy invariants within the framework of conjugacy over local rings.

For the investigation of non-invertible endomorphisms, we used module theory to decompose the lattices into subspaces where the restriction of a toral endomorphism is invertible or nilpotent, respectively, and found that on the prime power lattices, due to working over local rings, the cases of invertible and nilpotent endomorphisms can be considered separately.

We identified the (local) kernel sizes as the quantities that determine the associated tree structures on a particular rational lattice and showed that a pretail tree is determined up to graph isomorphism by the orders of certain subgroups of the local kernel. We derived criteria for the trees to have a balanced ("perfect") structure on a certain lattice (i.e. no leaves above a certain depth), and noticed that, due to the multiplicativity of the determinant, the depth up to which a pretail tree is perfect grows with the lattice size and is essentially governed by the p-growth (i.e. growth with respect to the p-adic valuation) of the invariant factors of growing matrix powers. In a similar vein, we have also considered sequences of pretail trees defined by the sequence of prime power lattices Λ_{p^r} and noted that they 'converge' to a perfect pretail tree. For the prime lattices, we have stated the numbers of occurrences of the possible pretail trees (up to graph isomorphism).

For the Casati-Prosen map with rational parameters on the prime lattices, our exact computations suggest that, in many respects, the CP map behaves like a random reversible map, both with the consequence that asymptotically almost all periodic points are symmetric, and that the orbit length distribution seems to follow $\mathcal{R}(x) = 1 - e^{-x}(1 + x)$ for asymptotically almost all parameter pairs. We also identified exceptional rational parameter values on certain lines in parameter space that give rise to different period distributions. Among the latter, we observed a transition from singularly distributed orbit lengths to the generic distribution of random reversible maps according to $\mathcal{R}(x)$.

The problems considered here relate to several open questions and possible starting points for future research.

Even for automorphisms of $\mathbb{T}^2$, it cannot be expected to find an analytic solution to the orbit counting problem, as the latter essentially amounts to order finding, a problem which is also computationally hard, i.e. no classical polynomial time algorithm is known. In dimensions greater than 2, many further questions remain open. Although most of the approaches used in two dimensions have an extension to higher dimensions, one cannot expect to obtain concrete results as the algebraic objects involved become more difficult, (e.g. non-quadratic polynomials). The same holds for the conjugacy problem; while there is only one possibility for a quadratic polynomial to have a multiple factor, the number of possibilities explodes with growing dimension. Thus, it cannot be assumed that a neat characterisation in form of complete invariants for local conjugacy exists in the general case. However, among the most

interesting questions remains the task to find good, if not complete, invariants for the different notions of conjugacy in higher dimensions.

The induced graph structure of non-invertible maps on finite spaces (possibly in the framework of finite invariant subsets as they show up for toral endomorphisms) may become of future interest as recent work by e.g. Benedetto/Ghioca/Hutz/Kurlberg/Scanlon/Tucker [21] and Ugolini [77, 78, 79] suggests.

In the context of toral endomorphisms, it may be possible to solve the realisation and distribution problem within the ensemble of all pretail trees induced by integer matrices on a given prime power lattice (from which the general case then follows).

For the Casati-Prosen map, it would be desirable to rigorously derive the asymptotical period distribution, at least for special cases. So far, the period distribution has not been proved to follow $\mathcal{R}(x)$ for any concrete system, but the fact that $\mathcal{R}(x)$ shows up as the limit of a sequence of singular distributions for appropriately related parameter pairs gives cause for the hope that CP provides a class of maps for which a structural argument for the limiting distribution $\mathcal{R}(x)$ might be within reach.

From a more general point of view, it would be worthwhile to also look for other interpretations of the combinatorial model for random reversible maps. Possibly, the action of the two involutions on a growing finite phase space could be intepreted as the realisation of a stochastic process in which the gamma distribution has a natural meaning.

A more concrete way to generalise the combinatorial model is to account for possible singularities of the reversible map, which naturally arises in the context of the reduction of rational maps over finite fields when the prime characteristic of the latter divides the denominator. The expected distributions were observed numerically for classes of rational maps; this is work in progress [63].

Appendix A: Two classic examples of cat maps

In the literature related to toral automorphisms, two matrices are omnipresent as examples, the Arnold and the Fibonacci cat map. Still, several aspects of them are unclear or conjectural, despite the effort of many. Let us sum up some aspects, with focus on properties in line with our above reasoning.

A.1. Arnold's cat map

Here, we collect some results for the matrix $M_{\mathrm{A}} = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ in an informal manner. This case was studied in [66, 32, 38] and appeared in many other articles as main example. It was introduced in [4, Example 1.16] as a paradigm of (discrete) hyperbolic dynamics.

The integer matrix M_{A} is reversible within the group $\mathrm{GL}(2,\mathbb{Z})$, with a reversor of order 4, but none of order 2. One has $\mathcal{S}(M_{\mathrm{A}}) \simeq C_2 \times C_\infty$, where $C_2 = \{\pm 1\}$ and the infinite cyclic group is generated by the unique square root of M_{A} in $\mathrm{GL}(2,\mathbb{Z})$ (see below), while $\mathcal{R}(M_{\mathrm{A}}) = \mathcal{S}(M_{\mathrm{A}}) \rtimes C_4$; see [12] for more. In particular, M_{A} inherits local reversibility in $\mathrm{GL}(2,\mathbb{Z}/p\mathbb{Z})$ for all primes p from its 'global' reversibility within $\mathrm{GL}(2,\mathbb{Z})$.

Based on properties of the Fibonacci numbers, in [38] it was shown that M_{A}, except for the trivial fixed point 0, has orbits of only one period length on each prime lattice Λ_p, $p \neq 5$. In view of Theorem 5.2.2, this can be seen as a consequence of its reversibility. Even for primes with $\left(\frac{5}{p}\right) = -1$, modulo which the characteristic polynomial splits, both roots have to be of the same order.

The iteration numbers from Section 3.7.1 are $u_m = f_{2m}$, where the f_k are the Fibonacci numbers, defined by the recursion $f_{k+1} = f_k + f_{k-1}$ for $k \in \mathbb{N}$ with initial conditions $f_0 = 0$ and $f_1 = 1$. Since $\mathrm{mgcd}(M_{\mathrm{A}}) = 1$, Proposition 3.7.1 implies

$$\mathrm{ord}(M_{\mathrm{A}}, n) \,=\, \kappa_{\mathrm{A}}(n) \,=\, \mathrm{period}\big\{(f_{2m})_{m\geq 0} \bmod n\big\},$$

where the periods for prime powers (with $r \in \mathbb{N}$) are given by

$$\kappa_{\mathrm{A}}(2^r) = 3 \cdot 2^{\max\{0,r-2\}} \quad \text{and} \quad \kappa_{\mathrm{A}}(5^r) = 10 \cdot 5^{r-1}$$

together with

$$\kappa_{\mathrm{A}}(p^r) \,=\, p^{r-1}\, \kappa_{\mathrm{A}}(p)$$

for all remaining plateau-free primes. It has been conjectured that this covers all primes [81]. No exception is known to date; the conjecture was tested for all $p < 10^8$ in [7]. Note that each individual prime can be analysed on the basis of Proposition 3.4.1.

The periods mod p are $\kappa_{\mathrm{A}}(2) = 3$, $\kappa_{\mathrm{A}}(5) = 10$, together with

$$\kappa_{\mathrm{A}}(p) \,=\, \frac{p - \left(\frac{5}{p}\right)}{2m_p - \frac{1}{2}\Big(1 - \left(\frac{5}{p}\right)\Big)}$$

for odd primes $p \neq 5$, where $\left(\frac{5}{p}\right)$ denotes the Legendre symbol and $m_p \in \mathbb{N}$ is a characteristic integer that covers the possible order reduction. It is 1 in 'most' cases (in the sense of a density definition), but there are infinitely many cases with $m_p > 1$; this integer is tabulated to some extent in [81, 38].

Let us write down the generating polynomials for the distribution of cycles on the lattices Λ_n. Once again, this is only necessary for n a prime power. We use a formulation with a

factorisation that shows the structure of orbits on $\Lambda_{p^r} \setminus \Lambda_{p^{r-1}}$. In the notation of [16], one finds $Z_1(t) = (1-t)$ and

$$Z_{2^r}(t) \;=\; (1-t)(1-t^3) \prod_{\ell=0}^{r-2} \bigl(1 - t^{3\cdot 2^\ell}\bigr)^{4\cdot 2^\ell}$$

with $r \geq 1$ for the prime $p = 2$, as well as

$$Z_{5^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl((1 - t^{2\cdot 5^\ell})(1 - t^{10\cdot 5^\ell})\bigr)^{2\cdot 5^\ell}$$

with $r \geq 1$ for $p = 5$. As usual, we adopt the convention to treat an empty product as 1. The remaining polynomials read

$$Z_{p^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl(1 - t^{\kappa_{\mathrm{A}}(p) p^\ell}\bigr)^{\frac{p^2-1}{\kappa_{\mathrm{A}}(p)}\, p^\ell},$$

as long as the plateau phenomenon is absent (see above).

A.2. Fibonacci cat map

Closely related is the matrix $M_{\mathrm{F}} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$, which is the unique square root of the Arnold cat map M_{A} in $\mathrm{GL}(2,\mathbb{Z})$. It appears in numerous applications; see [68, 8, 9, 27] and references therein for some of them. Here, the iteration numbers are the Fibonacci numbers themselves, and the periods are the so-called *Pisano periods*; compare [75, A001175] and references given there, or [81].

The matrix M_{F} is not reversible in $\mathrm{GL}(2,\mathbb{Z})$ (while its square M_{A} is, see above), and has the same symmetry group as M_{A}. In fact, $\pm M_{\mathrm{F}}$ are the only roots of M_{A} in $\mathrm{GL}(2,\mathbb{Z})$. This situation implies that the orbit structure for M_{F} must be such that the iteration of its square gives back the counts we saw in the previous example.

For prime powers p^r, with $r \in \mathbb{N}$, one finds $\kappa_{\mathrm{F}}(5^r) = 20 \cdot 5^{r-1}$ together with

$$\kappa_{\mathrm{F}}(p^r) \;=\; p^{r-1}\, \kappa_{\mathrm{F}}(p)$$

for all remaining primes, with the same proviso as for the Arnold cat map. The periods $\kappa_{\mathrm{F}}(p)$ are given by $\kappa_{\mathrm{F}}(2) = \kappa_{\mathrm{A}}(2) = 3$ together with

$$\kappa_{\mathrm{F}}(p) \;=\; 2\, \kappa_{\mathrm{A}}(p)$$

for all odd primes, which is not surprising in view of the relation between the two matrices M_{F} and M_{A}.

The orbit distribution is more complicated in this case, as usually orbits of two possible lengths arise in each step. One finds

$$Z_{2^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl(1 - t^{3\cdot 2^\ell}\bigr)^{2^\ell}$$

and

$$Z_{5^r}(t) \;=\; (1-t) \prod_{\ell=0}^{r-1} \bigl((1 - t^{4\cdot 5^\ell})(1 - t^{20\cdot 5^\ell})\bigr)^{5^\ell}$$

for the primes 2 and 5 (with $r \in \mathbb{N}_0$ as before), as well as

$$Z_{p^r}(t) \;=\; (1-t)\prod_{\ell=0}^{r-1}\bigl(1-t^{\frac{1}{2}\,\kappa_{\mathrm{F}}(p)p^\ell}\bigr)^{2n_p}\bigl(1-t^{\kappa_{\mathrm{F}}(p)p^\ell}\bigr)^{\frac{p^2-1}{\kappa_{\mathrm{F}}(p)}\,p^\ell-n_p}$$

for all remaining primes that are free of the plateau phenomenon (which possibly means all, see above). Here, $n_p \in \mathbb{N}_0$ is a characteristic integer which often takes the values 1 or 0, but does not seem to be bounded.

Appendix B: Numbers of pretail trees on prime lattices

The following tables list the number of occurrences of each tree type on the prime lattices, parametrised by the corresponding partitions. The numbers for $p = 2$ and $p = 3$, which have been obtained by the complete enumeration of all matrices and the calculation of their pretail trees confirm the general expressions.
Table for $d = 3$.

partition	class size	$p=2$	$p=3$
$\{0\}$	$\lvert\mathrm{GL}(3,\mathbb{F}_p)\rvert = (p^3-1)(p^3-p)(p^3-p^2)$	168	11232
$\{1\}$	$\left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]_p (p^3-p)(p^3-p^2)$	168	5616
$\{1,1\}$	$\left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p-1)(p^3-p^2)$	84	1872
$\{2\}$	$\left[\begin{smallmatrix}3\\2\end{smallmatrix}\right]_p (p^3-p^2)$	28	234
$\{1,1,1\}$	$\left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p-1)(p^2-p)$	42	624
$\{2,1\}$	$\left[\begin{smallmatrix}3\\2\end{smallmatrix}\right]_p (p^2-1)$	21	104
$\{3\}$	1	1	1
sum	p^9	512	19683

Table for $d = 4$.

partition	class size	$p=2$
$\{0\}$	$\lvert\mathrm{GL}(4,\mathbb{F}_p)\rvert = (p^4-1)(p^4-p)(p^4-p^2)(p^4-p^3)$	20160
$\{1\}$	$\left[\begin{smallmatrix}4\\1\end{smallmatrix}\right]_p (p^4-p)(p^4-p^2)(p^4-p^3)$	20160
$\{1,1\}$	$\left[\begin{smallmatrix}4\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]_p (p-1)(p^4-p^2)(p^4-p^3)$	10080
$\{2\}$	$\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]_p (p^4-p^2)(p^4-p^3)$	3360
$\{1,1,1\}$	$\left[\begin{smallmatrix}4\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p-1)(p^2-p)(p^4-p^3)$	5040
$\{2,1\}$	$\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]_p \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p^2-1)(p^4-p^3)$	2520
$\{3\}$	$\left[\begin{smallmatrix}4\\3\end{smallmatrix}\right]_p (p^4-p^3)$	120
$\{1,1,1,1\}$	$\left[\begin{smallmatrix}4\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]_p \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p-1)(p^2-p)(p^3-p^2)$	2520
$\{2,1,1\}$	$\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]_p \left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]_p (p^2-1)(p^3-p^2)$	1260
$\{2,2\}$	$\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]_p (p^2-1)(p^2-p)$	210
$\{3,1\}$	$\left[\begin{smallmatrix}4\\3\end{smallmatrix}\right]_p (p^3-1)$	105
$\{4\}$	1	1
sum	p^{16}	65536

Table of Symbols

$\mathbb{N}$	the set of natural numbers, understood to *not* contain 0
$\mathbb{Z}$	the set of integers
$\mathbb{T}$	the one-dimensional torus
$\mathbb{T}^d$	the d-dimensional torus
$\mathbb{1}$	the $d \times d$ identity matrix, where d is the dimension of the space considered
$\mathrm{Mat}(d, R)$	the ring of $d \times d$ matrices over the ring R
$\mathrm{Mat}(d, R)^\times$	invertible $d \times d$ matrices over the ring R
$\mathrm{GL}(d, R)$	the same
$\mathrm{SL}(d, R)$	subgroup of matrices from $\mathrm{GL}(d, R)$ with determinant 1
$\det(M)$	the determinant of the matrix M
$\mathrm{tr}(M)$	the trace of the matrix M
$\mathbb{Z}/n\mathbb{Z}$	the residue class ring of integers modulo $n \in \mathbb{Z}$
$\mathbb{Z}_p$	the ring of p-adic integers
v_p	the p-adic valuation
$\lvert\cdot\rvert_p$	the p-adic norm
Λ_n	the lattice of n-division points, i.e. rational points with denominator n
$\tilde{\Lambda}_n$	the free $\mathbb{Z}/n\mathbb{Z}$-module $(\mathbb{Z}/n\mathbb{Z})^d$ (identified with Λ_n)
$a \mid b$	a divides b
$p^r \mid\mid b$	$p^r \mid b$ but $p^{r+1} \not\mid b$
$\mathrm{lcm}(a, b)$	least common multiple of a and b
$\gcd(a, b)$	greatest common divisor of a and b
$Z_n(t)$	local version of the inverse zeta function of some matrix
$Z_n(M, t)$	local version of the inverse zeta function of the matrix M
$\ker_n(M)$	the kernel of M on Λ_n, $\ker_n(M) = \{x \in \Lambda_n \mid Mx = 0\}$
$\ker(M)$	if not specified otherwise, the kernel on the whole torus
$\mathrm{Fix}(M^k)$	submodule/subgroup of fixed points of M^k
$\mathrm{per}(M)$	periodic points of M; possibly for M restricted to some lattice Λ_n
$\mathrm{ord}(M, n)$	the order of the matrix M modulo the integer n, i.e. the smallest integer ℓ such that $M^\ell \equiv \mathbb{1} \mod n$
$\mathrm{ord}_n(M)$	the same
$R[x]$	the polynomial ring over the ring R
$P_M(x)$, $\chi_M(x)$	the characteristic polynomial of the matrix M; if not indicated otherwise, understood as an element of $\mathbb{Z}[x]$
modd	double modulus with respect to polynomial and integer
$\mathrm{ord}(f, p)$	minimal integer n such that $f(x) \mid (x^n - 1)$ in $\mathbb{F}_p[x]$
$\deg(f)$	degree of the polynomial f
$\kappa(n)$	the period of a (given) linear recursion modulo n
(α/p)	the Legendre symbol for odd primes p
$\bigoplus_{i=1}^n M_i$	the direct sum of the n matrices $M_1, \ldots, M_n$; that is, the block diagonal matrix built from the matrices M_i
$\mathrm{diag}(a_1, \ldots, a_d)$	diagonal matrix with ring elements or (square) matrices a_i on the diagonal
$\begin{bmatrix} d \\ \ell \end{bmatrix}_q$	Gaussian binomial coefficient (q-analogue of binomial coefficient)
$N \rtimes H$	semi-direct product of N and H, where N is the normal subgroup
$\mathcal{S}(M)$	the symmetry group of M within the matrix group considered
$\mathcal{R}(M)$	the reversing symmetry group of M within the matrix group considered
$\mathsf{Fix}(G)$	fixed set of the involution G
$\mathcal{R}(x)$	gamma distribution for parameters 2 and 1, $\mathcal{R}(x) = 1 - e^{-x}(1 + x)$

Acknowledgements

First of all, I thank my supervisors Michael Baake and John Roberts for supervising this thesis and for their encouragement and support. I gratefully acknowledge the funding received from the Sonderforschungsbereich 701 at the University of Bielefeld and from project number DP0774473 of the Australian Research Council Discovery Projects Scheme.

I am particularly indebted to John and Michael for making it possible for me to spend about 16 months at the School of Mathematics and Statistics at the University of New South Wales. Due to both John's and the School's great hospitality, my stay there was an extremely enjoyable experience.

I also thank Christian Huck and Johan Nilsson for providing helpful comments on the manuscript.

Furthermore, I thank Franco Vivaldi and Tom Ward for discussions related to my work.

Finally, it is my pleasure to thank Christian, Johan, Markus and Venta for all of their non-mathematical support.

References

[1] W.A. Adkins and S.H. Weintraub, *Algebra – An Approach via Module Theory*. corr. 2nd printing, Springer, New York (1999).

[2] R. Adler, C. Tresser and P.A. Worfolk, Topological conjugacy of linear endomorphisms of the 2-torus. *Trans. AMS* **349** (1997) 1633–1652.

[3] H. Appelgate and H. Onishi, Similarity problem over $\mathrm{SL}(n, \mathbb{Z}_p)$. Proc. AMS **87** (1983) 233–238.

[4] V.I. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics*. reprint, Addison-Wesley, Redwood City, CA (1989).

[5] A. Avila and G. Forni, Weak mixing for interval exchange transformations and translation flows. *Ann. Math.* **165** (2007) 637–664.

[6] N. Avni, U. Onn, A. Prasad and L. Vaserstein, Similarity classes of 3×3 matrices over a local principal ideal ring. *Commun. Algebra* **37** (2009) 2601–2615.

[7] H. Aydin, R. Dikici and G.C. Smith, Wall and Vinston revisited. In: *Applications of Fibonacci numbers*. vol. 5 (St. Andrews, 1992), Kluwer, Dordrecht (1993), pp. 61–68.

[8] M. Baake, U. Grimm and D. Joseph, Trace maps, invariants, and some of their applications. *Int. J. Mod. Phys. B* **7** (1993) 1527–1550; `arXiv:math-ph/9904025`.

[9] M. Baake, J. Hermisson and P.A.B. Pleasants, The torus parametrization of quasiperiodic LI-classes. *J. Phys. A: Math. Gen.* **30** (1997) 3029–3056; `mp_arc/02-168`.

[10] M. Baake, E. Lau and V. Paskunas, A note on the dynamical zeta function of general toral endomorphisms. *Monatsh. Math.* **161** (2010) 33–42; `arXiv:0810.1855`.

[11] M. Baake and N. Neumärker, A note on the relation between fixed point and orbit count sequences. *J. Integer Seq.* **12** (2009) 09.4.4.

[12] M. Baake and J.A.G. Roberts, Reversing symmetry group of $\mathrm{GL}(2, \mathbb{Z})$ and $\mathrm{PGL}(2, \mathbb{Z})$ matrices with connections to cat maps and trace maps. *J. Phys. A: Math. Gen.* **30** (1997) 1549–1573.

[13] M. Baake and J.A.G. Roberts, Symmetries and reversing symmetries of toral automorphisms. *Nonlinearity* **14** (2001) R1–R24; `arXiv:math.DS/0006092`.

[14] M. Baake and J.A.G. Roberts, The structure of reversing symmetry groups. *Bull. Austral. Math. Soc.* **73** (2006) 445–459; `arXiv:math.DS/0605296`.

[15] M. Baake, N. Neumärker and J.A.G. Roberts, Orbit structure and (reversing) symmetries of toral endomorphisms on rational lattices. To appear in *Discrete Contin. Dyn. Syst.*

[16] M. Baake, J.A.G. Roberts and A. Weiss, Periodic orbits of linear endomorphisms of the 2-torus and its lattices. *Nonlinearity* **21** (2008) 2427–2446; `arXiv:0808.3489`.

[17] E. Bach and J. Shallit, *Algorithmic Number Theory*. vol. 1, The MIT Press, Cambridge, MA (1996).

[18] J. Banks, J. Brooks, G. Cairns, G. Davis and P. Stacey, On Devaney's definition of chaos. *Amer. Math. Monthly* **99** (1992) 332–334.

[19] M. V. Berry and M. Tabor, Closed Orbits and the regular bound spectrum. *Proc. Roy. Soc. London Ser. A* **349** 101–123.

[20] E. Behrends and B. Fiedler, Periods of discretized linear Anosov maps. *Ergod. Th. & Dynam. Syst.* **18** (1998) 331–341.

[21] R.L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon and T.J. Tucker, Periods of rational maps modulo primes. arXiv:1107.2816v1 (2011).

[22] E. Brown and T.P. Vaughan, Cycles of directed graphs defined by matrix multiplication (mod n). *Discr. Math.* **239** (2001) 109–120.

[23] P. Bundschuh and J.-S. Shiue, A generalization of a paper by D.D. Wall. *Rendiconti Accademia Nazionale dei Lincei, Roma, Classe di Scienze Fisiche, Matematiche e Naturali* **56** (1974) 135–144.

[24] L. M. Butler, *Subgroup Lattices and Symmetric Functions*. Memoirs AMS vol. 112, no. 539, AMS, Providence, RI (1994).

[25] G. Casati and T. Prosen, Triangle map: A model for quantum chaos. *Phys. Rev. Lett.* **85** (2000) 4261–4264.

[26] G. Chen, Y. Mao and C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals* **21** (2004) 749–761.

[27] D. Damanik, Gordon-type arguments in the spectral theory of one-dimensional quasicrystals. In: *Directions in Mathematical Quasicrystals*. eds. M. Baake and R.V. Moody, CRM Monograph Series **13**, AMS, Providence, RI (2000), pp. 277–305.

[28] R. Davis, Certain matrix equations over rings of integers. *Duke Math. J.* **35** (1968) 49–59.

[29] M. Degli Esposti and S. Isola, Distribution of closed orbits for linear automorphisms of tori. *Nonlinearity* **8** (1995) 827–842.

[30] M. Degli Esposti and B. Winn, The quantum perturbed cat map and symmetry. *J. Phys. A: Math. Gen.* **38** (2005) 5895–5912.

[31] R. DeVogelaere, On the structure of symmetric periodic solutions of conservative systems, with applications. Ch. IV of *Contributions to the Theory of Nonlinear Oscillations*, vol. IV, ed. S. Lefschetz, Princeton Univ. Press, Princeton (1958) 53–84.

[32] F.J. Dyson and H. Falk, Period of a discrete cat mapping. *Amer. Math. Monthly* **99** (1992) 603–614.

[33] H.T. Engstrom, On sequences defined by linear recurrence relations. *Trans. AMS* **33** (1931) 210–218.

[34] A. Fel'shtyn, *Dynamical Zeta Functions, Nielsen Theory and Reidemeister Torsion*. Memoirs AMS vol. 147, no. 699, AMS, Providence, RI (2000).

[35] J. M. Finn, PhD Thesis, University of Maryland (1974).

[36] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps. *Internat. J. Bifur. Chaos Appl. Sci. Engrg.*, **8** (1998) 1259–1284.

[37] F.R. Gantmacher, *Matrix Theory*. vol. I, Chelsea, New York (1960).

[38] G. Gaspari, The Arnold cat map on prime lattices. *Physica* **73D** (1994) 352–372.

[39] J. H. Hannay and M. V. Berry, Quantisation of linear maps on the torus - Fresnel diffraction by a periodic grating. *Physica* **1D** (1980) 267–290.

[40] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford (1979).

[41] J.A. Hermida-Alonso and M. Pisonero, Invariant Factors of an Endomorphism and Finite Free Resolutions. *Lin. Alg. Appl.* **187** (1993) 201–226.

[42] H. Hasse, *Number Theory*. Springer, Berlin (1980).

[43] M. Horvat, M. Degli Esposti, S. Isola, T. Prosen, and L. Bunimovich, On ergodic and mixing properties of the triangle map. *Physica D* **238** (2009) 395–415.

[44] R. V. Hogg and A. T. Craig, *Introduction to Mathematical Statistics*. 4th edition, Macmillan, New York (1978).

[45] N. Jacobson, *Lectures in Abstract Algebra. II. Linear Algebra*. reprint, Springer, New York (1975).

[46] D. Jogia, J. A. G. Roberts, and F. Vivaldi, Algebraic geometric approach to integrable maps of the plane. *J. Phys. A: Math. Gen.* **39** (2006) 1133–1149.

[47] A. Katok and B. Hasselblatt, *Introduction to the Modern Theory of Dynamical Systems*. Cambridge University Press, Cambridge (1995).

[48] J.P. Keating, Asymptotic properties of the periodic orbits of the cat maps. *Nonlinearity* **4** (1991) 277–307.

[49] J.P. Keating and F. Mezzadri, Pseudo-symmetries of Anosov maps and spectral statistics. *Nonlinearity* **13** (2000) 747–775.

[50] V.L. Kurakin, Similarity invariants for matrices over an Artinian ring. *Mathematical Notes* **80** (2006) 387–395.

[51] P. Kurlberg, On the order of unimodular matrices modulo integers. *Acta Arithm.* **110** (2003) 141–151.

[52] P. Kurlberg and Z. Rudnick, Hecke theory and equidistribution for the quantization of linear maps of the torus. *Duke Math. J.* **103** (2000) 47–77.

[53] J. S. W. Lamb and J. A. G. Roberts, Time-reversal symmetry in dynamical systems: A survey. *Physica D* **112** (1998) 1–39.

[54] S. Lang, *Algebra*. rev. 3rd ed., Springer, New York (2002).

[55] C.G. Latimer and C. C. McDuffee, A correspondence between classes of ideals and classes of matrices. *Annals Math.* **34** (1933) 313–316.

[56] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge (1986).

[57] F. Lorenz, *Lineare Algebra*. Spektrum Akademischer Verlag, 3rd edition (1996).

[58] R.S. MacKay, *Renormalisation in Area-Preserving Maps*. World Scientific, Singapore (1993).

[59] B.R. McDonald, *Finite Rings with Identity*. Marcel Dekker, New York (1974).

[60] R. Mañe, *Differentiable Dynamics*. Springer, New York (1987).

[61] A.A. Nechaev, Similarity of matrices over a commutative artinian local ring. *Trudy Seminara imeni I.B. Petrovskogo* **9** (1983) 81–101.

[62] N. Neumärker, J. A. G. Roberts, F. Vivaldi, Distribution of periodic orbits for the Casati-Prosen map on rational lattices. *Physica D* **241** (2012) 360–371.

[63] N. Neumärker, J. A. G. Roberts, C.-M. Viallet, and F. Vivaldi, The dynamics of reversible rational maps over finite fields: experimental results. in preparation.

[64] N. Neumärker, *Orbitstatistik und relative Realisierbarkeit*. Diploma Thesis, Univ. Bielefeld (2007).

[65] M. Newman, *Integral Matrices*. Academic Press, New York and London (1972).

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

[67] A. Prasad, Counting subspaces of a finite vector space – 1. *Resonance* **15** (2010) 977–987.

[68] J.A.G. Roberts and M. Baake, Trace maps as 3D reversible dynamical systems with an invariant. *J. Stat. Phys.* **74** (1994) 829–888.

[69] J.A.G. Roberts and G.R.W. Quispel, Chaos and time-reversal symmetry. Order and chaos in reversible dynamical systems. *Phys. Rep.* **216** (1992) 63–177.

[70] J.A.G. Roberts and F. Vivaldi, Arithmetical Methods to detect integrability in maps. *Phys. Rev. Lett* **90** (2003) [034102].

[71] J.A.G. Roberts and F. Vivaldi. Signature of time-reversal symmetry in polynomial automorphisms over finite fields. *Nonlinearity* **18** (2005) 2171–2192.

[72] J.A.G. Roberts and F. Vivaldi, A combinatorial model for reversible rational maps over finite fields. *Nonlinearity* **22** (2009) 1965–1982.

[73] D. Ruelle, *Dynamical Zeta Functions for Piecewise Monotone Maps of the Interval*. CRM Monograph Series, vol. 4, AMS, Providence, RI (1994).

[74] P. Seibt, A period formula for torus automorphisms. *Discrete Cont. Dynam. Syst.* **9** (2003) 1029–1048.

[75] N.J.A. Sloane, *The Online Encyclopedia of Integer Sequences*, available at `http://www.research.att.com/~njas/sequences/`

[76] O. Taussky, Introduction into connections between algebraic number theory and integral matrices. 2nd appendix to: H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, 2nd printing, Springer, New York (1988), pp. 305–321.

[77] S. Ugolini, Graphs associated with the map $X \mapsto X + X^{-1}$ in finite fields of characteristic two. arXiv:1107.4565v3 (2011).

[78] S. Ugolini, Graphs associated with the map $X \mapsto X + X^{-1}$ in finite fields of characteristic three. arXiv:1108.1763v1 (2011).

[79] S. Ugolini, Graphs associated with the map $X \mapsto X + X^{-1}$ in finite fields of characteristic five. arXiv:1110.0968v1 (2011).

[80] E. Ventura, Dynamic structure of matrices over finite fields. EAMA-97 (1997) 413–420.

[81] D.D. Wall, Fibonacci series modulo m. *Amer. Math. Monthly* **67** (1960) 525–532.

[82] P. Walters, *An Introduction to Ergodic Theory*. reprint, Springer, New York (2000).

[83] M. Ward, The arithmetic theory of linear recurring sequences. *Trans. Amer. Math. Soc.* **35** (1933) 600–628.

[84] M. Ward, The cancellation law in the theory of congruences to a double modulus. *Trans. Amer. Math. Soc.* **35** (1933) 254–260.

[85] R.J. Wilson, *Introduction to Graph Theory*. 4th ed., Prentice Hall, Harlow (1996).

[86] X-S Zhang and F Vivaldi, Small pertubations of a discrete twist map. *Ann. Inst. Henry Poincaré.* **68** (1998) 507–523.

[87] N. Zierler, Linear recurring sequences. *J. Soc. Indust. Appl. Math.* **7** (1959) 31–48.