Periodic points in Markov subshifts on a finite abelian group

C G J Roettger

Mathematics Department, Iowa State University, 50011 Ames, IA, USA

Abstract

F Ledrappier introduced the following space of doubly-indexed sequences over a finite abelian group $G$,

$$X_G := \left\{ (x_{s,t}) \in G^{\mathbb{Z}^2} \mid x_{s,t+1} = x_{s,t} + x_{s+1,t} \text{ for all } s, t \in \mathbb{Z}\right\}$$

The group $\mathbb{Z}^2$ acts naturally on the space $X_G$ via left and upward shifts. We show that the periodic point data of $X_G$ determine the group $G$ up to isomorphism. This is extending work by T B Ward, using a new way to calculate periodic point numbers based on the study of polynomials over $\mathbb{Z}/p^n$ and Teichmüller systems. Our approach unifies Ward’s treatment of the two known Wieferich primes with that of all other primes and settles the cases of arbitrary Wieferich primes and the prime Two.

Key words: Periodic point, Markov Shift, Wieferich prime, Galois Ring, Teichmüller system
MSC 2000: 11B50, 13B40, 37C25, 37E99, 60J10

Email address: roettger@iastate.edu (C G J Roettger).

Preprint submitted to Elsevier Science 27 December 2003
1 Motivation and Background

Let $X := [0, 1]$ and consider the map $T : X \to X$ defined by $T(x) = ax \pmod{Z}$ for some integer $a > 1$. Define $m$-periodic points as those $x \in X$ fixed by $T^m$. Let $F_m$ be the number of $m$-periodic points $x \in X$. It is straightforward to calculate $F_m = a^m - 1$, and therefore

$$h_T = \log(a) = \lim_{m \to \infty} \frac{1}{m} \log(F_m)$$

The number $h_T$ is an important invariant called the entropy of the dynamical system given by $(X, T)$, and the preceding calculation shows that it is encoded in the family of periodic point numbers.

The orbit of $x$ is the sequence $(T^n(x))_{n \geq 0}$. Instead of studying $m$-periodic points $x \in X$, the theory of dynamical systems often studies the corresponding $m$-periodic orbits in the space of sequences over $X$.

From this viewpoint originated the question what information the periodic point data may contain in the setting of doubly-indexed, doubly-infinite sequences. Let $G$ be a finite abelian group. Consider the space $\hat{X}_G = G^{Z^2}$ of doubly-indexed sequences over $G$ and its subspace

$$X_G := \{(x_{s,t}) \in \hat{X}_G| x_{s,t+1} = x_{s,t} + x_{s+1,t}\}$$

Both $X_G$ and $\hat{X}_G$ carry a two-dimensional shift action via left and upward shifts. This allows us to view $X_G$ as a $Z^2$-module. For every subgroup $U$ of $Z^2$, we define $U$-periodic points to be those $x \in X_G$ fixed by the action of the subgroup $U$, as a natural generalization of the one-dimensional case. If $U$ has finite index in $Z^2$, the number $F_U$ of $U$-periodic points $x \in X_G$ is finite. We ask what information about $G$ can be extracted from the knowledge of all periodic point numbers $F_U$.

**Theorem 1** In the above situation, the numbers $(F_U)_U$ determine the group $G$ up to isomorphism.

Compare this situation to the full shift, i.e. the shift action on the space $\hat{X}_G$. If the index of $U$ in $Z^2$ is $m$, then obviously $F_U = |G|^m$ for any group $G$ (even non-abelian) – so the periodic point numbers for the full shift tell us nothing about $G$ except its order $|G|$.

The space $X_G$ was introduced by F Ledrappier in [L78] (for $|G| = 2$), various generalizations have been studied in [SH92,W91,W92] and [W93]. In [S95], K Schmidt gave a more general discussion of higher-dimensional subshifts of finite type.
T B Ward conjectured Theorem 1 in [W98]. There he has already proven the theorem for all groups $G$ such that the order of $G$ is not divisible by 1024 or the square of a Wieferich prime greater than $4 \cdot 10^{12}$. A Wieferich prime is a prime number $p$ such that $p^2$ divides $2^{p-1} - 1$. Known examples are 1093 and 3511. Crandall, Dilcher and Pomerance reported in [CDP97] that there are no further Wieferich primes below $4 \times 10^{12}$.

It is a curious fact that Wieferich primes got their name by causing trouble with a quite different problem, namely Fermat’s Last Theorem (see [R83,W09]).

We shall outline the first part of Ward’s argument in section 2, which should be helpful towards understanding the proof of Theorem 1. Then we aim for a formula describing the number $F_U$ for a known shift subgroup $U$ and $G = \mathbb{Z}/p^e$ with $p$ a prime. To this end, we reduce the problem to single-indexed sequences in section 3 and describe $F_U$ in terms of ideals in $\mathbb{Z}/p^e[T]$, viewing the space of sequences as a module over this ring, $T$ acting as the shift operator. The strategy is very similar to elementary algebraic geometry and has been widely applied to sequences over finite fields. Sequences over $\mathbb{Z}/p^n$ have been studied in this way only recently, see [H92]. Our theorems 5 and 6 give not only the desired formula for $F_U$ but place the problem in a wider context and open up avenues for other applications. We also hope that the proofs will be more readable in this setting. In section 4, we use Hensel’s Lemma for passing from one ’level’ $p^e$ to another. Using Teichmüller systems and Kummer’s result about the highest power of a prime dividing a binomial coefficient, section 5 shows how to choose $U$ so that the associated ideal contains the prime $p$ itself. This will be pivotal in the proof of the main theorem in section 6.

## 2 Ward’s argument

Consider the subgroups $U$ of $\mathbb{Z}^2$ defined as follows

$$U := \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \mathbb{Z}^2$$  \hspace{1cm} (2)

To be an $U$-periodic point, $x \in X_G$ must satisfy

$$x_{r,t} = x_{s,t} \quad \text{and} \quad x_{s,t+k} = x_{s,t}$$  \hspace{1cm} (3)

for all integers $r, s, t$. Using the condition in (1) defining the Ledrappier subshift, together with equation (3), we get $x_{s,t+1} = x_{s,t} + x_{s+1,t} = 2x_{s,t}$ and
iteratively
\[ x_{s,t+j} = 2^j x_{s,t} \quad (5) \]

Put \( j = k \) and combine this with (4) to get
\[ (2^k - 1) x_{s,t} = 0 \quad (6) \]

The number \( F_U \) for the special subgroups \( U \) as in (2) is exactly the number of solutions to equation (6) in \( G \).

Since \( G \) is abelian, it is a direct sum of its \( p \)-Sylow subgroups. Extracting the \( p \)-part from the number \( F_U \), we get the number of \( U \)-periodic points in the \( p \)-Sylow subgroup of \( G \), and so it is enough to show that we can reconstruct all finite abelian \( p \)-groups from their family of periodic point numbers. From now on, we may assume that \( G \) is a \( p \)-group.

Ward defines a \( p \)-good sequence as a sequence of integers \((a_k)\) such that for every integer \( v \) there is an index \( k \) such that \( p^v \) divides \( a_k \), but \( p^{v+1} \) does not divide \( a_k \), and he shows that the sequence \( 2^k - 1 \) is \( p \)-good if \( p \) is neither 2 nor a Wieferich prime. Then he shows

**Lemma 2** For a finite abelian \( p \)-group \( G \), let \( G(m) := |\{g \in G : mg = 0\}| \).

The numbers \( G(p) \), \( G(p^2) \), \ldots, \( G(p^v) \) determine \( G \) up to isomorphism if and only if the order of \( G \) is not divisible by \( p^{2v+2} \).

This settles most of the cases of Ward’s theorem, since for \( p \)-groups \( G(2^k - 1) = G(p^v) \), where \( p^v \) is the largest power of \( p \) dividing \( 2^k - 1 \). These numbers are given by the argument leading up to equation (6). The hardest part of Ward’s work is to find an extra argument to deal with the powers of 2 up to 16 and the two known Wieferich primes. This involves three ingeniously chosen families of subgroups \( U \). However, there are still a lot of subgroups of \( \mathbb{Z}^2 \) which are never used.

### 3 Arbitrary shift subgroups, reduction to single-indexed sequences

Any subgroup of \( \mathbb{Z}^2 \) of finite index can be presented as

\[ U := U_{a,b,d} := \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mathbb{Z}^2 \quad (7) \]

with \( a, d > 0 \) and \( 0 \leq b < a \).

In equation (12), we will give a description of \( F_U \) for an arbitrary subgroup \( U \) as in (7), and in Corollary 7, we will show how to calculate \( F_U \) in special cases.
There is a generalization of (5). For all sequences \( x \in X_G \) and all integers \( s, t \)
\[
x_{s,t+d} = \sum_{i=0}^{d} \binom{d}{i} x_{s+i,t}
\]  
(8)

This follows from the definition of the Ledrappier subshift in (1) and the fact that there are \( \binom{d}{i} \) paths leading from \( x_{s+i,t} \) up and left to \( x_{s,t+d} \) via neighbouring entries. Using (8), we get a criterion for \( x \) to be \( U \)-periodic.

**Lemma 3** A sequence \( x \in X \) is an \( U \)-periodic point for \( U \) as in (7) if and only if for all indices \( s, t \)
\[
x_{s,t} = x_{s+a,t}
\]  
(9)
\[
x_{s-b,t} = \sum_{i=0}^{d} \binom{d}{i} x_{s+i,t}
\]  
(10)

**Proof of Lemma 3** Assume \( x \in X_G \) satisfies (9) and (10). Clearly, \( x \) is invariant under the shift \( \binom{a}{0} \). But from (10) and (8), we get
\[
x_{s-b,t} = x_{s,t+d}
\]
for all integers \( s, t \). Therefore \( x \) is also invariant under the shift \( \binom{b}{d} \). These two shifts generate the group \( U \). The converse statement is then obvious.

Note that equations (9) and (10) have been written so that the second subscript involved is exactly \( t \). If we have an \( U \)-periodic sequence \( x \in X_G \), it is completely determined by its entries on 'row zero' \( (x_{s,0})_s \) because of the Ledrappier condition (1) and \( U \)-periodicity. Conversely, every ordinary sequence \( (x_{s,0})_s \) satisfying (9) and (10) can be uniquely extended to a doubly-indexed \( U \)-periodic sequence \( x \in X_G \). To determine \( F_U \), we may now count the number of such single-indexed sequences.

Let us consider the case that the group \( G \) is cyclic, i.e. \( G = \mathbb{Z}/p^n \) for some \( n \). We are seeking to determine the number of sequences over \( G \) which are \( a \)-periodic in the usual sense and satisfy
\[
x_{s-b} = \sum_{i=0}^{d} \binom{d}{i} x_{s+i}
\]  
(11)
for every integer \( s \). It helps to use the ring structure of \( \mathbb{Z}/p^n \). So consider \( R = \mathbb{Z}/p^n \) as a ring and the space of sequences \( Y = R^\mathbb{Z} \) as an \( R[T] \)-module, where \( T \) is the left shift. Then the sequences in question are precisely those annihilated by the two polynomials \( T^a - 1 \) and \( T^b(T+1)^d - 1 \).
It is worthwhile to investigate this in greater generality. We use the same notation as in elementary algebraic geometry.

**Definition 4** Let $I$ be an ideal of $R[T]$, $f_1, \ldots, f_k \in R[T]$ and $V$ an $R[T]$-submodule of $Y = \mathbb{R}^\mathbb{Z}$. Writing $(f_1, \ldots, f_k)$ for the ideal generated by $f_1, \ldots, f_k$, we define

$$
V(I) := \{ x \in Y : fx = 0 \text{ for all } f \in I \}
$$

$$
V(f_1, \ldots, f_k) := V((f_1, \ldots, f_k))
$$

$$
I(V) := \{ f \in R[T] : fx = 0 \text{ for all } x \in V \}
$$

Using this notation, the space $V$ of $U$-periodic points is given by

$$
V = V(T^a - 1, T^b(T + 1)^d - 1) \quad (12)
$$

Let us list some elementary properties of the two operators $I$ and $V$. We call two ideals $I, J$ coprime if $I + J = (1)$. Two polynomials $f, g$ are called coprime if $(f, g) = (1)$ (the notation $(f, g)$ means the same as $(f)+(g)$). In any principal ideal ring, this notion has the familiar meaning of having no proper common divisor, but here the ideal $(f, g)$ is not necessarily principal.

**Theorem 5** If $I$ is any ideal of $R[T]$, then $V(I)$ is an $R[T]$-submodule of $Y$. This correspondence between ideals and $R[T]$-submodules is inclusion-reversing. Furthermore, for any two ideals $I$ and $J$ of $R[T]$ and $R[T]$-submodules $U$ and $V$ of $Y$,

$$
V(I + J) = V(I) \cap V(J) \quad (13)
$$

$$
I(U + V) = I(U) \cap I(V) \quad (14)
$$

$$
V(I) + V(J) \subseteq V(I \cap J) \quad (15)
$$

$$
I(U) + I(V) \subseteq I(U \cap V) \quad (16)
$$

Finally, if $I + J = (1)$, then for all ideals $K$ of $R[T]$

$$
V(IJ + K) = V((I + K) \cap (J + K)) = V(I + K) + V(J + K) \quad (17)
$$

In the last term, the sum is direct.

**Proof of Theorem 5** It is clear that $V(I)$ is an $R[T]$-submodule of $Y$, that $I(V)$ is an ideal of $R[T]$, and that the correspondence is inclusion-reversing. To prove (13), suppose $x \in V(I + J)$. Then $x$ is both in $V(I)$ and $V(J)$. On the other hand, if $x$ is in both of these, then it is annihilated by any polynomial in $I$ or $J$, so annihilated by $I + J$. The proofs of the remaining statements
are similar except for the last one. To prove that statement, we recall from elementary ring theory that \( I + J = (1) \) implies

\[
IJ + K = (I + K)(J + K) = (I + K) \cap (J + K)
\]

By hypothesis, there exist \( i \in I \) and \( j \in J \) such that \( i + j = 1 \). Suppose \( x \in V(IJ + K) \). Put \( y = ix \) and \( z = jx \). Then \( x = y + z \) and \( y \in V(J + K) \), \( z \in V(I + K) \), showing \( V(IJ + K) \subseteq V(I + K) + V(J + K) \). The reverse inclusion follows from (15). Since \( (I + K) + (J + K) = (1) \), \( V(I + K) \cap V(J + K) = V(1) = \{0\} \), and the sum is direct. This completes the proof of Theorem 5.

The observations in Theorem 5 could be made for any module \( Y \) over a commutative ring, and indeed they are fairly well-known. We now ask what are more specific features of our situation with \( Y = R^n \) as a module over \( R[T] \), \( R = \mathbb{Z}/p^n \). An ideal or a polynomial in \( R[T] \) is called regular if it is non-zero modulo \( p \).

**Theorem 6** If \( I \) is a regular ideal, then \( V(I) \) is a finite \( R[T] \)-submodule of \( Y \). If \( V \) is a finite \( R[T] \)-submodule of \( Y \), then \( I(V) \) is a regular ideal of \( R[T] \).

**Proof of Theorem 6** Proof of Theorem 6. Suppose \( I \) is a regular ideal. If \( I = (f) \) is principal, then we may multiply \( f \) by a unit, and without loss of generality \( f \) is monic (see [McD, Theorem XIII.6]). Choose any \( x_k, \ldots, x_{k+d-1} \) \((d = \deg(f)) \) as entries of \( x \in V(f) \). For any such choice there is exactly one possible choice of \( x_{k+d} \), which gives exactly one choice of \( x_{k+d+1} \) and so on. Consider the reciprocal polynomial \( f^* \) of \( f \), defined by

\[
f^*(T) = T^{\deg f} f(T^{-1})
\]

and replace the variable \( T \) by \( S \). If \( S \) acts on \( Y \) as the right shift instead of left shift, then \( f^*(S) \) annihilates \( V(f) \) (up to a factor of \( T^{\deg f} \), \( f(T) \) and \( f^*(S) \) are the same operators on \( Y \)). Multiplying by some unit, we can make \( f^*(S) \) monic. This could shrink the degree, but the same argument as above shows that the starting values \( x_k, \ldots, x_{k+d-1} \) determine \( x_s \) for all \( s < k \) as well. Since the starting values determine the whole sequence \( x \), \( V(f) \) is finite. In the general case, the ideal \( I \) is finitely generated, \( I = (f_1, \ldots, f_k) \) and therefore \( V(I) \) is contained in \( V(f_1) \) where \( f_1 \) may be assumed to be regular. Since the latter module is finite, \( V(I) \) is finite.

For the second assertion, let \( V \) be a finite \( R[T] \)-submodule of \( Y \). For every \( x \in V \), \( Tx \in V \), \( T^2 x \in V \) etc, and from the finiteness of \( V \) follows \( T^i x = T^j x \) for some \( i \neq j \). The action of \( T \) is invertible, hence \((T^a - 1)x = 0 \) for some \( a \neq 0 \). Taking the least common multiple \( A \) of all these numbers \( a \), we get a
polynomial \( T^A - 1 \) that annihilates all of \( V \), and so \( I(V) \) is not contained in \((p)\), hence regular.

**Corollary 7** Call a polynomial in \( R[T] \) strongly regular if its leading and constant coefficients are non-zero modulo \( p \). If \( f \) is strongly regular, then

\[
|V(p^e, f)| = \begin{cases} 
p^{e \deg(f)} & \text{for } e < n \\
p^{n \deg(f)} & \text{for } e \geq n.
\end{cases}
\]

**Proof of Corollary 7** Read again the proof of the first statement of Theorem 6. Every choice of a \( \deg(f) \)-tuple determines exactly one sequence \( x \in V(p^e, f) \). The choice is limited by the prime power \( p^e \) – in every coordinate there are exactly \( p^e \) choices.

Corollary 7 implies

\[
|V(p^e, f)| = G(p^e)^{\deg(f)}
\]

where the numbers \( G(m) \) are defined as in Lemma 2. So far, we looked only at the special case \( G = \mathbb{Z}/p^n \). But equation (19) is still true for arbitrary finite abelian \( p \)-groups, since both sides behave multiplicatively when forming direct products of such groups (note that (19) no longer depends on \( n \)).

### 4 Raising the level – from \( p^e \) to \( p^{e+1} \)

A polynomial \( f \in R[T] \) is called **basic irreducible** if it is irreducible modulo \( p \). It is called **separable** if it has no repeated factors modulo \( p \). Equivalently, it factorizes modulo \( p \) into pairwise coprime irreducible factors. It is well-known that \( f \) is separable if and only if \( f \mod p \) is a function of \( T^p \).

**Theorem 8 (Hensel’s Lemma)** Let \( f \in R[T] \) be monic and separable. If there exists a factorization \( f \equiv gh \pmod{p} \) with monic factors \( g, h \) then there exist uniquely determined monic polynomials \( \tilde{g}, \tilde{h} \in R[T] \) such that \( g \equiv \tilde{g} \pmod{p} \), \( h \equiv \tilde{h} \pmod{p} \) and \( f = \tilde{g}\tilde{h} \) in \( R[T] \).

For a proof, see [McD, Theorem XIII.4]. A well-known related 'lifting' result is

**Theorem 9** Two polynomials \( f, g \in R[T] \) are coprime modulo \( p \) if and only if they are coprime in \( R[T] \).

Theorem 9 implies for the problem at hand
Corollary 10 If \( f, g \in R[T] \) are coprime modulo \( p \), then \( V(f, g) = \{0\} \).

So for our purposes, only those parameters \((a, b, d)\) are interesting where the polynomials \( T^a - 1 \) and \( T^b(T + 1)^d - 1 \) are not coprime modulo \( p \).

Lemma 11 For the prime \( p = 2 \) and \( e \geq 1 \), put \( a = 3 \cdot 2^{e-1} \). Then

\[
(T^a - 1, T(T + 1) - 1) = (2^e, T(T + 1) - 1)
\]

Proof of Lemma 11 We use induction over \( e \). The case \( e = 1 \) is a simple calculation. Modulo \( T(T + 1) - 1 \),

\[
T^3 - 1 = (T - 1)(T^2 + T + 1) \equiv 2(T - 1) \tag{20}
\]

and \( T - 1 \) is a unit modulo \( T(T + 1) - 1 \) (same as coprime to \( T(T + 1) - 1 \) - this is an easy check by Theorem 9). Therefore \( T^3 - 1 \) and \( 2 \) generate the same ideal modulo \( T(T + 1) - 1 \). Take the pre-image of this ideal in \( R[T] \) to obtain the desired equality.

For the induction step, suppose \((T^a - 1, T(T + 1) - 1) = (2^e, T(T + 1) - 1)\) for \( a = 3 \cdot 2^{e-1} \). This means

\[
T^a \equiv 1 + 2^e u(T) \pmod{T(T + 1) - 1} \tag{21}
\]

with a polynomial \( u \) which is a unit modulo \( T(T + 1) - 1 \). Square this equation to get

\[
T^{2a} \equiv (1 + 2^e u(T))^2 \equiv 1 + 2^{e+1} \tilde{u}(T) \pmod{T(T + 1) - 1} \tag{22}
\]

with some polynomial \( \tilde{u} \in R[T] \). In case \( e \geq 2 \), we have \( \tilde{u} \equiv u \pmod{2} \) and \( \tilde{u} \) is also a unit modulo \( T(T + 1) - 1 \) by Theorem 9. If \( e = 1 \), then \( a = 3 \) and \( u(T) = T - 1 \) from equation (20). Again, \( \tilde{u} = u + u^2 = u(u + 1) \) is a unit modulo \( T(T + 1) - 1 \). In both cases, \( T^{2a} - 1 \) generates the same ideal as \( 2^{e+1} \) modulo \( T(T + 1) - 1 \) and the proof goes through as before.

Obviously, Lemma 11 and Corollary 7 allow us to calculate \( F_U = G(2^e) \) for subgroups \( U \) as in (7) with parameters \((2^{e-1} \cdot 3, 1, 1)\). We need a similar family of subgroups for every odd prime \( p \). See remark 17 for possible choices for the two known Wieferich primes. For non-Wieferich primes, we can simply choose \( a = 1, b = 0 \) and \( d = p^{e-1}k \) where \( k \) is the order of 2 in the multiplicative group \((\mathbb{Z}/p)^*\), which is essentially Ward’s argument. We will deal with all odd primes simultaneously, including the elusive 'large' Wieferich primes. In the remainder of this section, we will show that we can determine \( G(p^{e+1}) \) once we have \( G(p^e) \). Using equation (19), we may always suppose \( G = R = \mathbb{Z}/p^n \).
Recall the factorization of $T^a - 1$ in $\mathbb{Z}[T]$}

$$T^a - 1 = \prod_{m|a} \Phi_m(T) \quad (23)$$

where $\Phi_m(T)$ is the $m$-th cyclotomic polynomial.

**Lemma 12** Let $g$ be any polynomial of $R[T]$. If all the numbers $F_U = |V(T^a - 1, g)|$ are known, then the numbers $|V(\Phi_a, g)|$ are also known for all $a$ not divisible by $p$. We call these the primitive $U$-periodic point numbers $F'_U$.

**Proof of Lemma 12** The factorization (23) is valid modulo $p^n$, too, only the factors $\Phi_m$ may now become reducible. However this may be, the cyclotomic polynomials for different divisors $m$ of $a$ are mutually coprime modulo $p$ since their product is $T^a - 1$, which is separable. By Theorem 9, they are mutually coprime in $R[T]$. Applying equation (17) repeatedly, we get an expression for $V(T^a - 1, g)$ as a direct sum. One of the summands is $V(\Phi_a, g)$, and the cardinality of all the others may be assumed to be known by induction over $a$. This allows to deduce $|V(\Phi_a, g)|$.

The last tool from elementary number theory we need is the well-known fact

$$f(T^p) \equiv f(T)^p \pmod{p} \quad (24)$$

for all $f \in R[T]$.

Recall equation (18), stated here in the form we will need later on. If two polynomials $f, g$ in $R[T]$ are coprime, then for all polynomials $h$

$$\langle fg, h \rangle = \langle f, h \rangle \langle g, h \rangle \quad (25)$$

**Lemma 13** Suppose $p$ is odd and $(f, (T + 1)^d - 1) = (g, p^e)$ for monic polynomials $f, g \in R[T]$ and $d > 0$. If $f$ is separable, then

$$(f, (T + 1)^{pd} - 1) = (\tilde{g}, p^{e+1})$$

for some monic polynomial $\tilde{g}$ such that $\tilde{g} \equiv g \pmod{p^e}$.

**Proof of Lemma 13** Modulo $p^e$, $g$ divides $f$. Modifying $g$ modulo $p^e$ to $\tilde{g}$, we may assume that $\tilde{g}$ divides $f$ in $R[T]$ by Hensel’s Lemma. The hypothesis of $f$ being separable is used here, and it even tells us $f = \tilde{g} \tilde{h}$ for some polynomial $\tilde{h}$ coprime to $\tilde{g}$. Taking everything modulo $p$, we get that $\tilde{g}$ is the greatest
common divisor of \( f \) and \((T + 1)^d - 1\) and that \( \tilde{h} \) is coprime to \((T + 1)^d - 1\). Using equation (25), this means
\[
(f, (T + 1)^d - 1) = (\tilde{g}, (T + 1)^d - 1) \tag{26}
\]
Combine this with the hypothesis \((f, (T + 1)^d - 1) = (g, p^e) = (\tilde{g}, p^e)\) and take everything modulo \( \tilde{g} \). This implies
\[
(T + 1)^d \equiv 1 + p^e u(T) \pmod{\tilde{g}} \tag{27}
\]
with a polynomial \( u(T) \) which is a unit modulo \( \tilde{g} \) (coprime to \( \tilde{g} \)). Raise this equation to the \( p \)-th power to get
\[
(T + 1)^{pd} \equiv (1 + p^e u(T))^p \equiv 1 + p^{e+1} \tilde{u}(T) \pmod{\tilde{g}} \tag{28}
\]
with some polynomial \( \tilde{u} \in R[T] \). Since \( p \geq 3 \), \( \tilde{u} \equiv u \pmod{p} \) and \( \tilde{u} \) is also a unit modulo \( \tilde{g} \). This says that \((T + 1)^{pd} - 1\) and \( p^{e+1} \) generate the same ideal in \( R[T]/(\tilde{g}) \). Take the pre-image of that ideal in \( R[T] \) to get
\[
(\tilde{g}, (T + 1)^{pd} - 1) = (\tilde{g}, p^{e+1}) \tag{29}
\]
From equation (24) follows
\[
(T + 1)^{pd} - 1 \equiv ((T + 1)^{pd} - 1)^p \pmod{p}
\]
Therefore \( \tilde{g} \) is the greatest common divisor of \( f \) and \((T + 1)^{pd} - 1\) modulo \( p \) and \( \tilde{h} \) as defined above is even coprime to \((T + 1)^{pd} - 1\). Using equation (25) once more, this means
\[
(f, (T + 1)^{pd} - 1) = (\tilde{g}, (T + 1)^{pd} - 1)
\]
and together with (29), the proof is complete.

5 The number \( G(p) \) for odd primes

We are still considering \( G = R = \mathbb{Z}/p^n \). Let \( \alpha \) be a root of some basic irreducible polynomial \( f \in R[T] \) in an extension ring of \( R \). The finite ring \( S = R[\alpha] \) is a so-called Galois ring. It contains a special set of representatives of the field \( S/(p) \) given by
\[
\mathbb{T} := \{ \beta \in S : \beta^p = \beta \} \tag{30}
\]
where \( q = p^r \) and \( r = \deg(f) \). This is called the Teichmüller system. Note that \( \mathbb{T} \) is closed under multiplication, but in general not under addition.

The following theorem proves a 'scattering' result about the Teichmüller system. Note that it is uniform in \( n \).
Theorem 14 Let $\mathbb{T}$ be the Teichmüller system of $S$ as defined in (30). If $n \geq 2$, then the number of elements of $\mathbb{T} \cap (\mathbb{T} - 1)$ — that is, the number of $\beta \in \mathbb{T}$ such that $\beta + 1 \in \mathbb{T}$ — is at most $p - 1$.

Proof of Theorem 14 The $q$ elements of $\mathbb{T}$ are precisely the roots of $T^q - T$ in $S$. The elements $\beta$ such that $\beta + 1 \in \mathbb{T}$ are just the roots of $(T+1)^q - (T+1)$. Those which satisfy both equations must be a root of every polynomial in the ideal $(T^q - T, (T + 1)^q - (T + 1))$ — in particular, a root of the difference between these two polynomials. It is a famous result of Kummer that the highest power of $p$ to divide the binomial coefficient $\binom{q}{i}$ is exactly $p^k$, where $k$ is the number of ‘carries’ when doing the sum $i + (q - i) = q$ in base $p$ (see [G95]). Apart from the cases $i = 0$ and $i = q$, $k$ is always at least One. $k$ is strictly greater than One iff $i$ is not divisible by $p^{n-1}$. Modulo $p^2$, the difference of $T^q - T$ and $(T + 1)^q - (T + 1)$ is therefore $p$ times a polynomial in $T^{p^{n-1}}$, say $h(T^{p^{n-1}})$, whose degree is exactly $p - 1$. Roots of $ph(T^{p^{n-1}})$ modulo $p^2$ are roots of $h(T^{p^{n-1}})$ modulo $p$. By repeatedly applying the identity (24),

$$h \left( T^{p^{n-1}} \right) \equiv h(T)^{p^{n-1}} \pmod{p}$$

and it follows that $h(T^{p^{n-1}})$ has at most $p - 1$ distinct roots modulo $p$. All roots which are at the same time roots of $T^q - T$ must be distinct modulo $p$, since the latter polynomial is separable.

Theorem 15 Let $a$ be any prime larger than $p^{a-1}$. Then for a suitably chosen integer $d$ there exists a strongly regular, monic polynomial $g$ such that

$$(\Phi_a, (T + 1)^d - 1) = (g, p)$$

Proof of Theorem 15 The case $n = 1$ is trivial. Consider the case $n = 2$. For any root $\alpha$ of $\Phi_a$, write $\mathbb{T}$ for the Teichmüller system of $R[\alpha] = S$ as above. Let $m$ be any monic, basic irreducible factor of $\Phi_a$. Note that $m$ splits into linear factors over $S$ because all its roots are powers of $\alpha$. From Galois theory we know that the degree of $m$ equals the order of $p$ in the multiplicative group $\mathbb{Z}/a^*$. By our choice of $a$, $m$ has at least degree $p$. Theorem 14 says at least one root $\beta$ of $m$ satisfies $\beta + 1 \notin \mathbb{T}$. The set $\mathbb{T}$ is invariant under automorphisms of $S$, so all the conjugates of $\beta$ enjoy the same property. The automorphism group of $S$ operates transitively on the roots of $m$ (see [McD, Theorems XV.2, XV.5]). Since $m$ was arbitrary, all roots $\beta$ of $\Phi_a$ satisfy $\beta + 1 \notin \mathbb{T}$ (whereas $\beta \in \mathbb{T}$, since $a$ divides $p^{a-1} - 1 = q - 1$).

Choose $d$ to be the order of $\beta + 1 \pmod{p}$ in the multiplicative group of the field $S/(p)$, for some root $\beta$ of $\Phi_a$ as above. Note that $p \nmid d$, so $(T + 1)^d - 1$ is
separable. We proceed to factorize the ideal $(\Phi_a, (T + 1)^d - 1)$ over $R[T]$. By repeatedly using equation (25),
\[(\Phi_a, (T + 1)^d - 1) = \prod_{i,j} (f_i, g_j)\]
where the product runs over a factorization $\Phi_a = \prod_i f_i$ and $(T + 1)^d - 1 = \prod_j g_j$ into monic basic irreducibles. For all those pairs $(i, j)$ where $f_i \not\equiv g_j \pmod{p}$, the ideal $(f_i, g_j)$ is One. So we only have to consider the pairs $(i, j)$ with $f_i \equiv g_j \pmod{p}$. If we had in fact $f_i = g_j$ for some $i, j$, then some root $\gamma$ of $\Phi_a$ would satisfy $((\gamma + 1)d - 1, p) = (p, g_j)$ for some polynomial $h_{ij} \not\equiv 0 \pmod{p}$. Since $f_i$ and $g_j$ are monic, $\deg(h_{ij}) < \deg(f_i)$. This means $(h_{ij}, g_j) = (1)$ and it is easy to see
\[(f_i, g_j) = (ph_{ij}, g_j) = (pg_j, g_j) = (p, g_j)\]
Applying equation (25) backwards several times, we get
\[(\Phi_a, (T + 1)^d - 1) = (p, g)\]
for some divisor $g$ of $(T + 1)^d - 1$ (the product of all those $g_j$ dividing $\Phi_a$ modulo $p$, so $g$ is monic and strongly regular). Now consider the case of $n \geq 3$. Working modulo $p^2$, we would obtain equation (31) modulo $p^2$. Take the pre-image in $R[T]$ of both sides modulo $p^2$ to get
\[(\Phi_a, (T + 1)^d - 1, p^2) = (p, g)\]
so there exist $u, v, w \in R[T]$ such that $u\Phi_a + v((T + 1)^d - 1) + wp^2 = p$. This implies
\[u\Phi_a + v((T + 1)^d - 1) = p(1 - wp)\]
and since $1 - wp$ is a unit in $R[T]$, the ideal $(\Phi_a, (T + 1)^d - 1)$ contains $p$, hence also $g$, completing the proof.

6 Proof of the main result

**Theorem 16** Suppose that for a given prime $p$ there exists a strongly regular polynomial $h \in R[T]$ such that the cardinality $|V(p^e, h(T))|$ can be derived from the knowledge of all $U$-periodic point numbers, for all $e \geq 1$. Then every abelian $p$-group $G$ is determined up to isomorphism by the system of $U$-periodic point numbers $(F_U)_U$. 

13
Proof of Theorem 16 From equation (19), we may assume that we know $G(p^e)$ for all $e \geq 0$. By Lemma 2, this determines the group $G$ up to isomorphism.

For the proof of Theorem 1, it remains to check that the hypothesis of Theorem 16 is satisfied for every prime $p$. We constantly use equation (19) to translate the knowledge of various $U$-periodic point numbers $F_U$ into knowing some number $G(p^e)$. For $p = 2$, we have done it all in Lemma 11. For odd primes, we may assume that the primitive periodic point numbers

$$F_U' = |V(\Phi_a, (T + 1)^d - 1)|$$

are known for all $a$ not divisible by $p$, by Lemma 12. In Theorem 15, we obtain $G(p)$ from the primitive periodic point numbers. Then all numbers $G(p^e)$ can be obtained by induction as in Lemma 13. As explained in section 2, it is enough to deal with the case of $G$ being a $p$-group.

Remark 17 If we know parameters $(a, b, d)$ such that $(T^a - 1, T^b(T + 1)^d - 1) = (p, h(T))$ for a monic, strongly regular polynomial $h$, then we can proceed as in Lemma 11 and choosing the parameters $(p^{e-1}a, b, d)$ will give the ideal $(p^e, h(T))$ with some suitably modified monic polynomial $\tilde{h}$ congruent to $h$ modulo $p$. For non-Wieferich primes $p$, we can choose $a = 1$, $b = 0$ and $d$ the order of 2 in the multiplicative group $\mathbb{Z}/p^*$ as described in section 2. For the two known Wieferich primes, we could choose the following parameters.

<table>
<thead>
<tr>
<th>Prime $p$</th>
<th>$a$</th>
<th>$b$</th>
<th>$d$</th>
<th>$h(T)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1093</td>
<td>273</td>
<td>0</td>
<td>2</td>
<td>$T - 33$</td>
</tr>
<tr>
<td>1093</td>
<td>91</td>
<td>9</td>
<td>1</td>
<td>$T - 528$</td>
</tr>
<tr>
<td>1093</td>
<td>84</td>
<td>28</td>
<td>1</td>
<td>$T^2 + 3T + 3$</td>
</tr>
<tr>
<td>3511</td>
<td>39</td>
<td>3</td>
<td>1</td>
<td>$T - 244$</td>
</tr>
<tr>
<td>3511</td>
<td>45</td>
<td>8</td>
<td>1</td>
<td>$T - 103$</td>
</tr>
<tr>
<td>3511</td>
<td>819</td>
<td>2</td>
<td>1</td>
<td>$T - 1524$</td>
</tr>
</tbody>
</table>

The computations have been done using the number theory package KASH. One example for each prime would have been enough, but we wanted to illustrate that there are lots of choices with small parameters, that they do not follow an obvious pattern, and that the polynomial $h$ can indeed have degree Two. The first and last lines specify the parameters that Ward used to treat the primes 3511 and 1093, although in a different guise.
7 Conclusion

(1) Our strategy is capable of being extended to higher-dimensional systems, which carry an action of $\mathbb{Z}^d$ rather than $\mathbb{Z}^2$. One should introduce shifts $T_1, \ldots, T_d$, one for each dimension, and study ideals in the polynomial ring $R[T_1, \ldots, T_d]$. In our case $d = 2$, one could have translated the definition of the Ledrappier subshift into

$$x \in X_G \iff T_2x = (1 + T_1)x$$

or $X_G = V(T_2 - 1 - T_1)$.

(2) Algebraically, it would be convenient to replace $R[T]$ by the localization of $R[T]$ with respect to $T$, since $T$ acts invertibly on $\hat{X}_G$. This is the ring of Laurent polynomials $R[T, T^{-1}]$. Its usefulness becomes apparent in the proof of Theorem 6. Another bonus is that the correspondence between regular ideals and finite $R[T]$-submodules of $Y$ introduced in that theorem actually becomes one-to-one. Third, one could describe periodic point numbers entirely within the ring $R[T, T^{-1}]$ as follows. Suitably redefining the operator $I$, it is not hard to see

$$|V| = \left| R[T, T^{-1}]/I(V) \right|$$

for any finite $R[T, T^{-1}]$-submodule $V$ of $Y$. We did not use Laurent polynomials, since the additional notation required was too clumsy in comparison to the gains. This approach could also be combined with polynomial rings in several variables as in the preceding remark.

(3) Not all ideals of $R[T]$ have a nice representation as $(p^e, h(T))$. Counterexamples are $(pT, T^2)$ or $(p(T+1), (T+1)^2)$ – for the latter, even localizing with respect to $T$ does not help.

(4) In the context of Theorem 15, a curious question arises: is it possible to choose for every given prime $p$ some prime $q$ such that $\Phi_q$ is irreducible modulo $p$? This would simplify the proof only slightly, but it is worthwhile noting that this is still an open question, even though this is a much weaker than the famous Artin conjecture on there being infinitely many such primes $q$.

Acknowledgements

My heartfelt thanks to Clifford Bergman for being an enthusiastic listener and to Tom Ward for introducing me to those two troublemaking primes 1093 and 3511.
References

[CDP97] R Crandall/K Dilcher/C Pomerance,
A search for Wieferich and Wilson primes,
Math Comp 66 (1997), 433-449

[G95] A Granville,
Arithmetic properties of binomial coefficients. I. Binomial coefficients
modulo prime powers.
Organic mathematics (Burnaby, BC, 1995), 253–276,

[H92] M Q Huang,
Maximal period polynomials over \(\mathbb{Z}/(p^d)\),

[L78] F Ledrappier,
Un champ markovien peut être d’entropie nulle et melangeant,
C R Acad Sci Paris A 287 (1978), 561-562

[McD] B McDonald,
Finite Rings with Identity,
Dekker 1974

[R83] P Ribenboim,
“1093”,
Math Intelligencer 5 (1983), 28-33

[S95] K Schmidt,
Algebraic ideas in ergodic theory,
Birkhäuser, Basel 1995

[SH92] M A Shereshevsky,
On the classification of some two-dimensional Markov shifts with group
structure,
Ergod Th and Dyn Sys 12 (1992), 823-833

[W91] T B Ward,
Almost block-independence for the three dot \(\mathbb{Z}^2\) dynamical system,

[W92] T B Ward,
Periodic points for expansive actions of \(\mathbb{Z}^d\) on compact abelian groups,

[W93] T B Ward,
An algebraic obstruction to isomorphism of Markov shifts with group
alphabets,
[W98] T B Ward,
A family of Markov subshifts (almost) classified by periodic points,

[W09] A Wieferich,
Zum letzten Fermatschen Theorem,
Crelle 136 (1909), 293-302

[ZW03] Y Zhou/X Wang,
A Criterion for Primitive Polynomials over Galois Rings,
Proceedings for Com2Mac 2002, to appear