ON RESIDUES OF POLYNOMIAL SEQUENCES

BY

AARON E. WITTRIG

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2012

Urbana, Illinois

Advisor:

Assistant Professor Jayadev Athreya

Abstract

Given $f(x) \in \mathbb{Q}[x]$, graphing the doubly infinite sequence $f\big|_{\mathbb{Z}}$ mod 1 can often produce interesting and even surprising results. In this paper, we will give some examples of such sequences, introduce some techniques for their analysis and construction, and will provide an easy method for distinguishing them from other sequences taking values in $\mathbb{Q} \cap [0, 1)$.

Table of Contents

Chapter 1

Introduction

Watch a video of a propellor (or a spoked wheel, a fan, etc.) Pausing the video on any frame, we see two somewhat blurry propellors. Playing the video at normal speed however, we usually see four or six propellors at once, at times seeming to move clockwise and at other times counter-clockwise. This illusion is called the "wagon wheel effect", or temporal aliasing. Of course, the simple explanation of the effect is that our eyes can only perceive so much visual information in a given period of time, and our brains percieve even less. Thus, successive frames of the video blend together. But why do we see four or six evenly spaced propellors most of the time instead of an unpredictable maelstrom of blades, and what happens in the transitions between these "states"? Let us work out an example to see why. Consider a propellor blade being accelerated at 2 rev/sec^2. Then the angle the blade makes with its starting position after t seconds is $2\pi t^2$. Thus, the position of the end of the blade (on the unit circle) can be given by the equation $f(t) = e^{2\pi i t^2}$. If we film the spoke at 400 fps for 5 seconds and plot the positions recorded, we will get a pretty accurate representation of the actual continuous path of the blade, as shown in Figure 1.1.

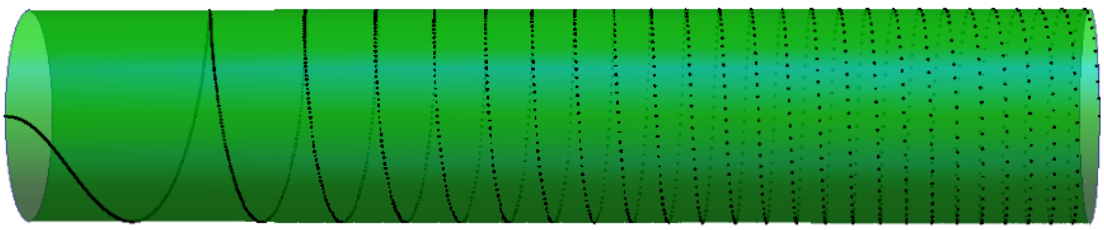


Figure 1.1: $\{(t, f(t/400)) : t \in \{0, ..., 2000\}\}$

If however, we film the blade for 20 seconds and plot these positions, the blade begins to appear to take several positions at once, moving forwards then backwards in even, parabolic paths along the circle.

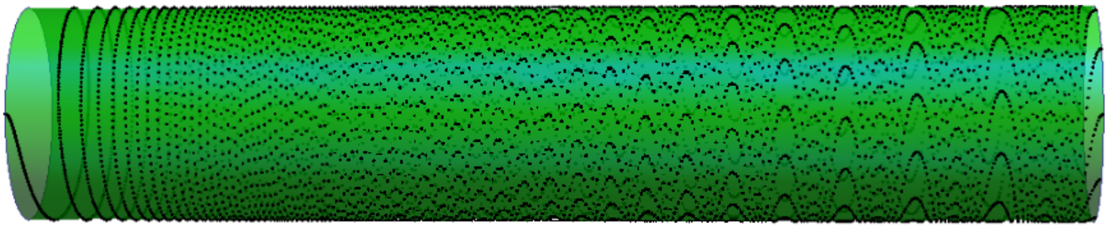


Figure 1.2: $\left\{\left(t, e^{2\pi i(t/400)^2}\right) : t \in \{0, ..., 8000\}\right\}$

In the remainder of this paper we shall, for ease of representation, identify the circle with the unit interval $[0, 1)$ with addition mod 1. In this framework, the motion of the propellor blade in the above example would be given by $t \mapsto t^2 \mod 1$, and the graph in Figure 1.2 would look like this.

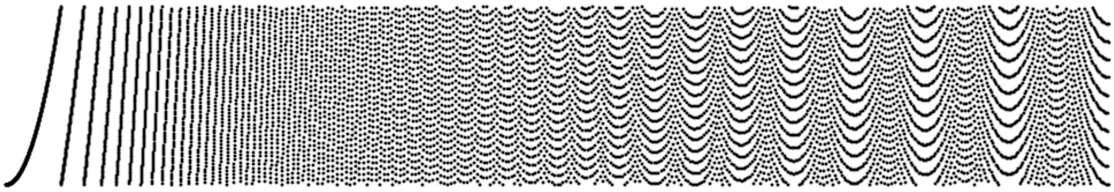


Figure 1.3: $\{(t, (t/400)^2 \mod 1) : t \in \{0, ..., 20\}\}$

This paper will be focused on the set of functions from $\mathbb{Z} \to [0, 1)$ (that is, $[0, 1)$-valued doubly infinite sequences) of the form $x \mapsto f(x) \mod 1$, where f is a polynomial function. Figures 1.4- 1.11 illustrate the diversity of images inscribed by the graphs of these sequeces.

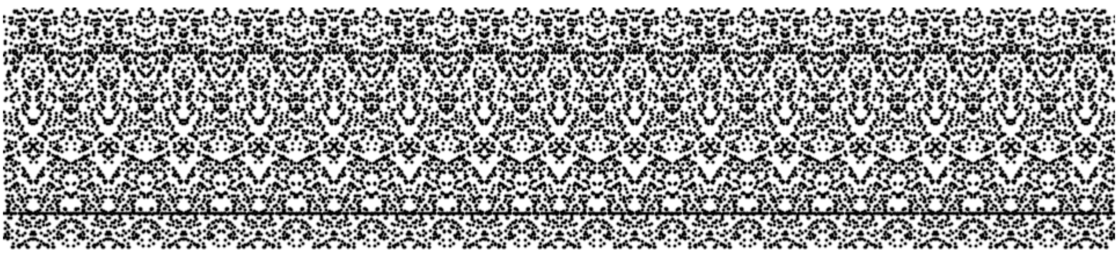


Figure 1.4: $\{(x, \frac{241}{1083}x^2 + \frac{13}{16} \mod 1) : x \in \{-8000, ..., 8000\}\}$

We will show more such maps, but first, let us return for a moment to the propellor example. Recall that the position of the propellor was defined by $f(x) \equiv \left(\frac{x}{400}\right)^2 = \frac{x^2}{160000}$. Here and in the

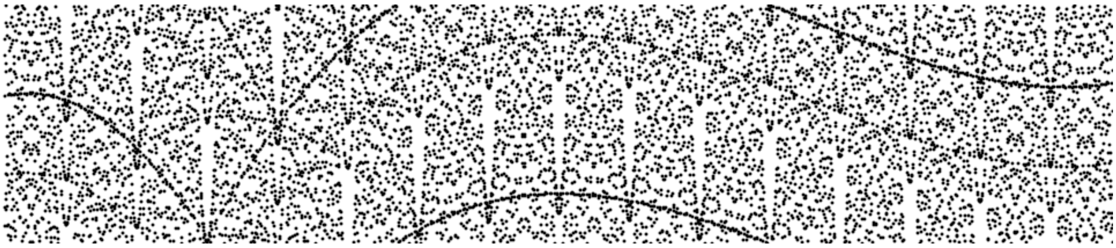


Figure 1.5: $\left\{\left(x, \frac{1}{43589145600}x^3 + \frac{447887}{551162}x^2 + \frac{7}{8} \mod 1\right) : x \in \{-4000, ..., 4000\}\right\}$

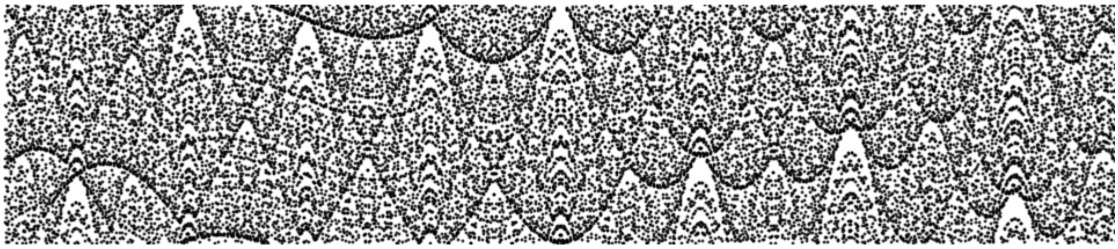


Figure 1.6: $\left\{\left(x, \frac{x^3}{65383718400} + \frac{140489x^2}{388797} + \frac{7}{8} \mod 1\right) : x \in \{-10000, ..., 10000\}\right\}$

sequel, $\equiv$ will denote equivalence mod 1, unless otherwise noted. Figure 1.12 shows a plot of f from 0 to 20000 (50 seconds). The highlighted region ($[15600, 16400] \times [0, 1)$) contains what seems to be 5 parabolas centered at 16000. To see why, let $\varphi_k(x) = 16000 + k + 5x$ for $k \in \{-2, ..., 2\}$, $x \in \mathbb{Z}$. Then

$$\begin{aligned} f(\varphi_k(x)) &\equiv 1600 + x + \frac{k}{5} + \frac{k^2}{160000} + \frac{kx}{16000} + \frac{x^2}{6400} \\ &\equiv \frac{x^2}{6400} + \frac{k}{5} + \frac{k^2}{160000} + \frac{kx}{16000} \\ &= f(5x) + \frac{k}{5} + \frac{k^2}{160000} + \frac{kx}{16000}. \end{aligned}$$

But then for $x \in \{-80, ..., 80\}$ (so that $(x, f(x))$ is in the highlighted region), we have that $\left|\frac{k^2}{160000} + \frac{kx}{16000}\right| \leq 401/40000$, so

$$f(\varphi_k(x)) = f(5x) + \frac{k}{5} + \epsilon(x, k)$$

where $|\epsilon(x, k)| \leq 401/40000$ for all x, k in their prescribed domains. Thus, within the highlighted region, each point on the graph is on one of 5 parabolas, indexed by k, and to a high degree of approximation these parabolas are all similar and evenly spaced. Figure 1.13 shows a graph of

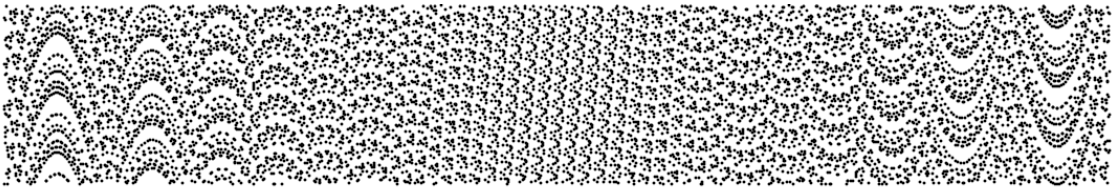


Figure 1.7: $\left\{\left(x, \frac{111111111}{2000000000}x^3 + \frac{6}{11}x^2 + \frac{23}{121}x + \frac{866}{1331} \mod 1\right) : x \in \{-4238, ..., 4238\}\right\}$

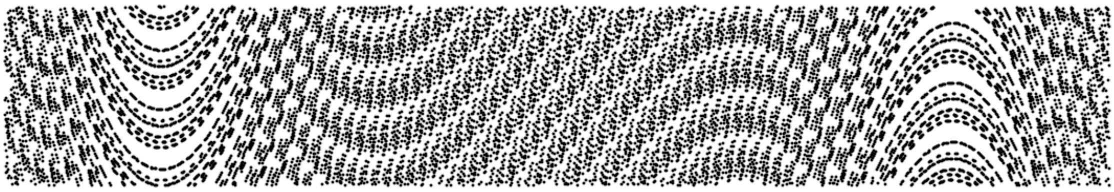


Figure 1.8: $\left\{\left(x, \frac{1}{2000000000}x^3 + \frac{6}{11}x^2 + \frac{23}{121}x + \frac{866}{1331} \mod 1\right) : x \in \{-4238, ..., 4238\}\right\}$

$f \circ \varphi_2$ embedded in a graph of f.

Now to conclude this introduction, we will show a few more examples of sequences like the one in the previous example (that is, sequences of the form $x \mapsto \alpha x^2$ for $\alpha \in \mathbb{Q}$).

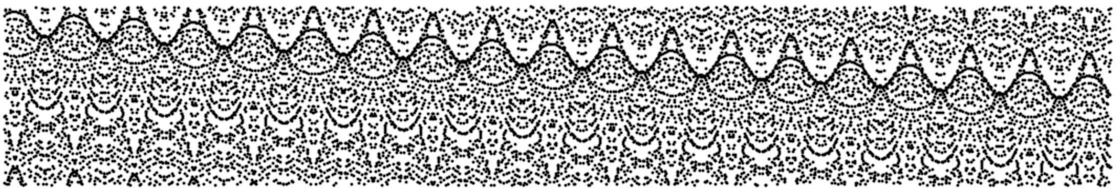


Figure 1.9: $\left\{\left(x, \left(x-\frac{250}{601}\right)^3 \mod 1\right) : x \in \{-5570, ..., 5570\}\right\}$

Figure 1.10: $\left\{\left(x, \left(x-\frac{9445}{1651}\right)^3 \mod 1\right) : x \in \{-4571, ..., 4571\}\right\}$

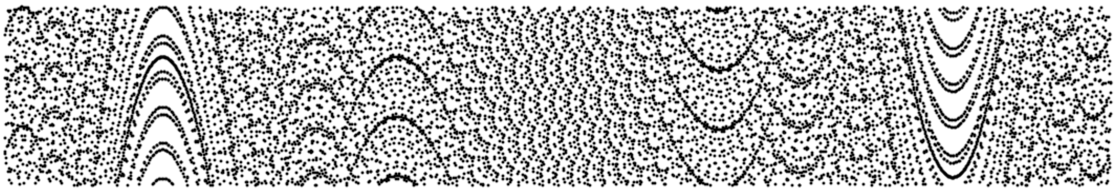


Figure 1.11: $\left\{\left(x, \frac{16000001}{2000000000}x^3 + \frac{3}{125}x^2 + \frac{3}{125}x + \frac{1}{125} \mod 1\right) : x \in \{-4571, ..., 4571\}\right\}$

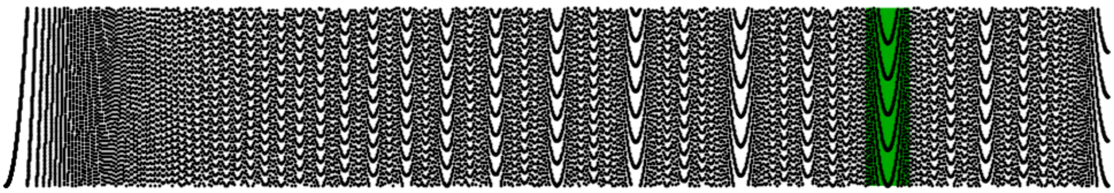


Figure 1.12: $\{(x, f(x)) : x \in \{0, ..., 20000\}\}$

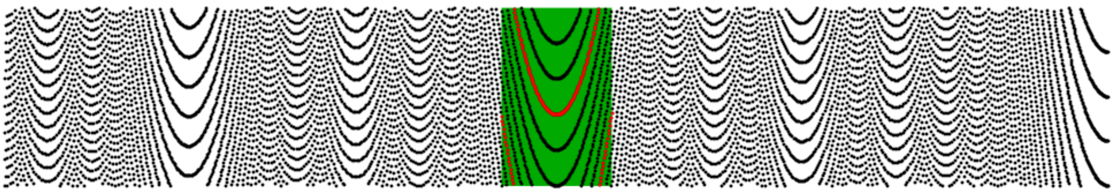
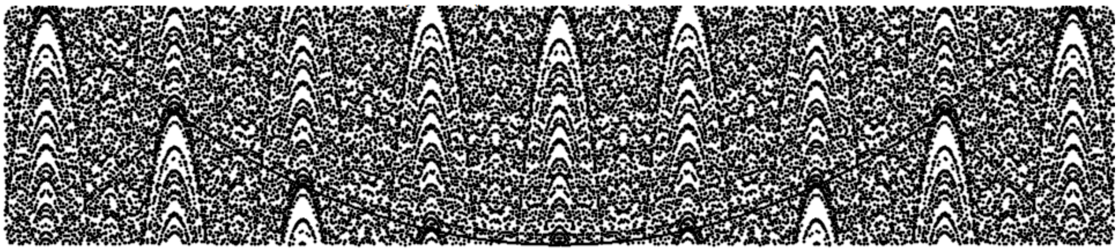
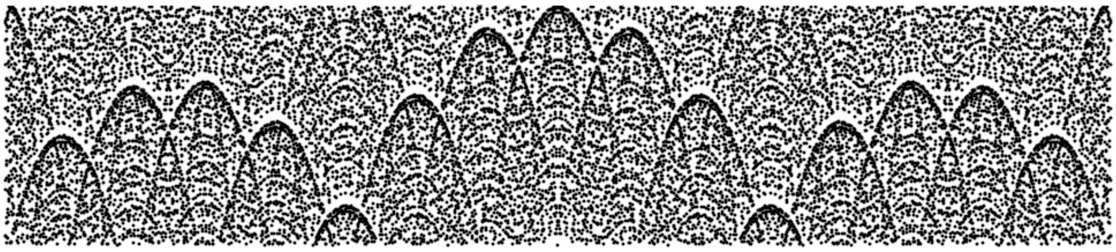
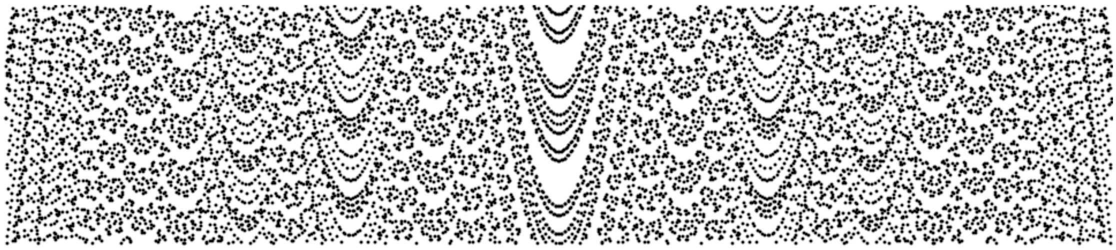
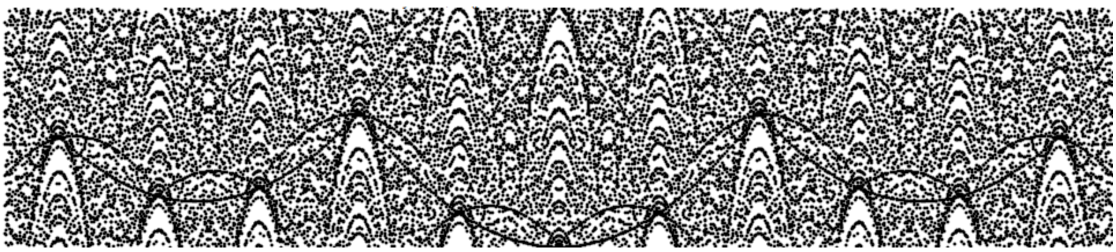


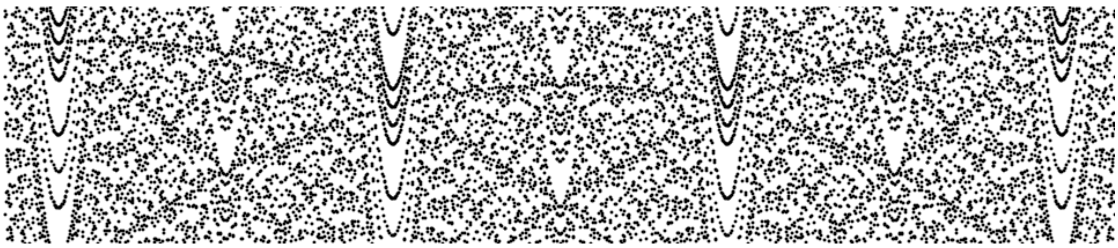
Figure 1.13: $\{(x, f(x)) : x \in \{12000, ..., 20000\}\}$
$\{(\varphi_2(x), f(\varphi_2(x)))\, |x \in \{-80, ..., 80\}\}$

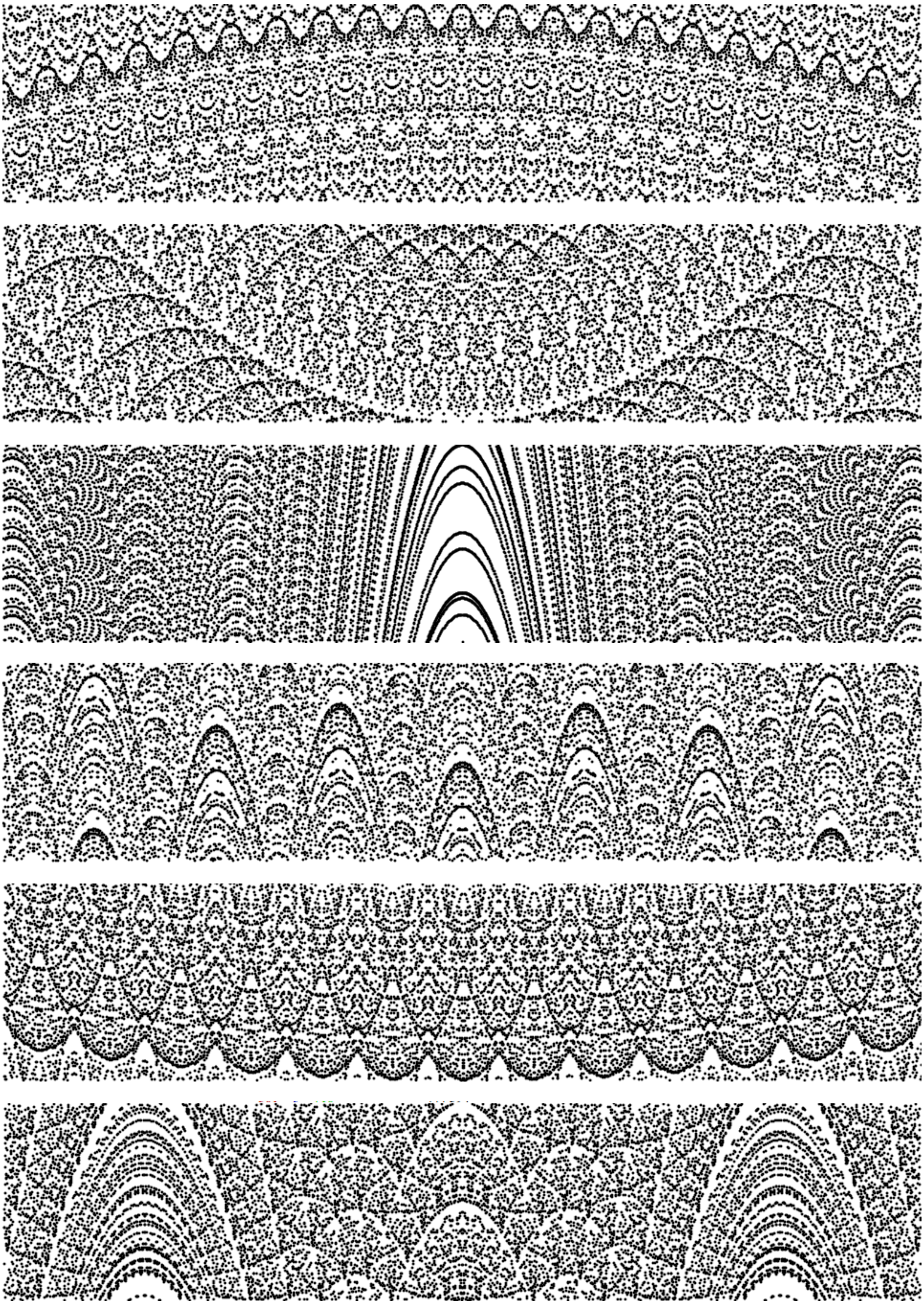


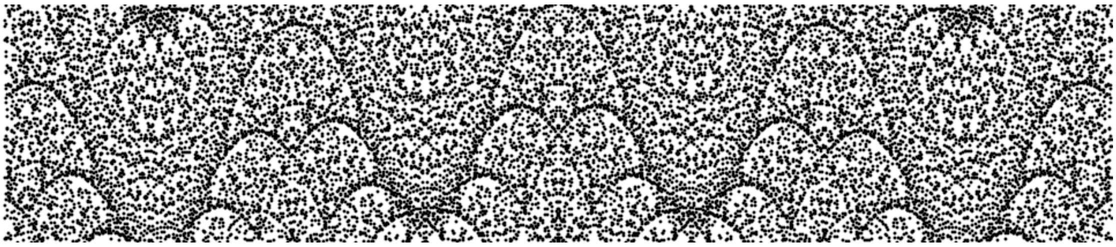


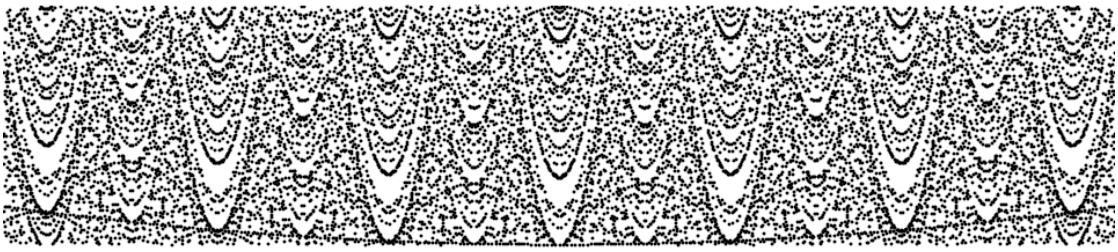


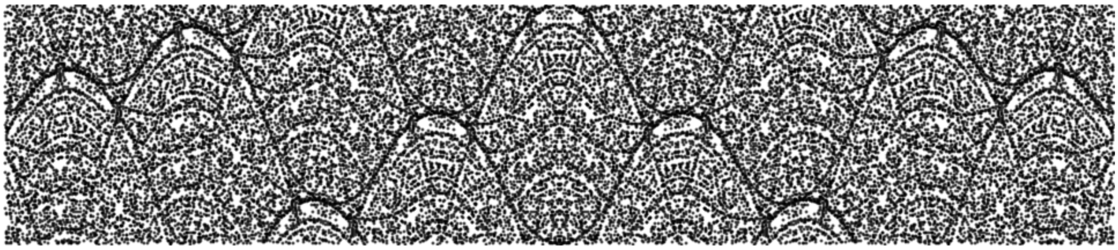


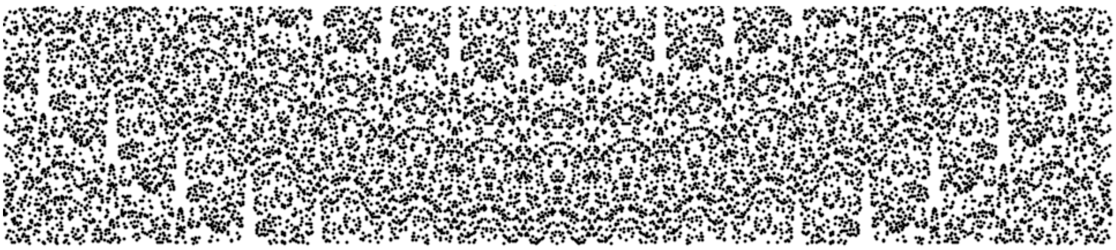


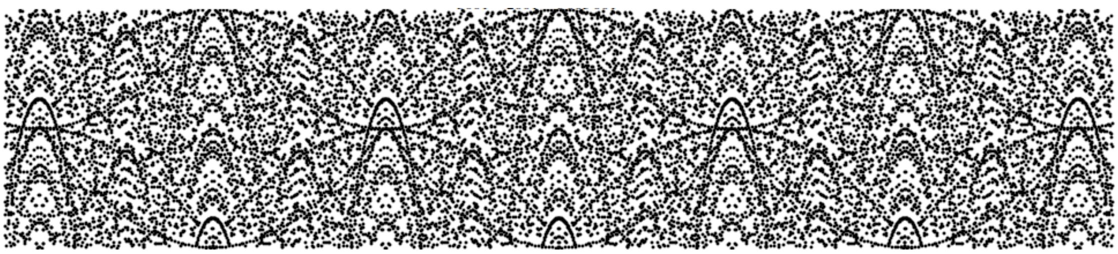


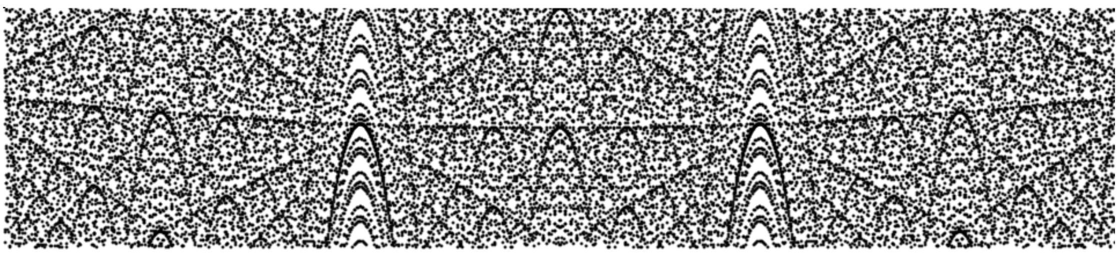












Chapter 2

Background & Definitions

To begin with, we will get a few notations and conventions out of the way. For $a, b \in \mathbb{N}$, we write

- For $x \in \mathbb{R}, m > 0 \in \mathbb{Q}$, $[x]_m$ shall denote the residue of q mod m, that is the unique non-negative rational number $\tilde{x} < m$ such that $\tilde{x} \equiv x \bmod m$.
- If $m \in \mathbb{N}$ and x is invertible mod m, we will let $[x^{-1}]_m$ denote the unique non-negative rational number $\tilde{x} < m$ such that $x\tilde{x} \equiv 1 \bmod m$.
- $a \cap b = \gcd(a, b)$,
- $a \cup b = \operatorname{lcm}(a, b)$,
- $a \backslash b = \frac{a}{a \cap b}$.
- We will make sparing use of the Peano notation $\backepsilon$ for "such that".
- As mentioned in the introduction, $\equiv$ shall denote equivalence mod 1 unless otherwise noted.
- For a function f, we define $f(\bullet) = f$. For instance if $f(x) = x + 3$, we may write $\bullet + 3$ instead of f.
- We will write $\mathfrak{I}$ for the identity function when the set it acts on is clear

Now we will define some subsets relevant to the sequence residues we will be discussing in this paper.

Definition We define

- $\mathcal{Q} = \mathbb{Q}^{\mathbb{Z}}$
- $\mathcal{P} = \left\{ f \in \mathcal{Q} \middle| \exists d \in \mathbb{Z}_0, a_1, ..., a_d \in \mathbb{Q} : f(x) = \sum_{k=0}^{d} a_k x^k \quad (\forall x \in \mathbb{Z}) \right\}$

- $\mathcal{Z} = \mathbb{Z}^{\mathbb{Z}}$
- $\mathcal{N} = \mathcal{P} \cap \mathcal{Z}$

and for $n > 0 \in \mathbb{Q}$, we define

- $\mathbb{Q}_n = \mathbb{Q} \cap [0, n)$ (this is contrary to the notation $\mathbb{Q}_p$ for the p-adic field)
- $\mathbb{Z}_n = \mathbb{Z} \cap [0, n)$ (though we will write $\mathbb{N}_0$ and not $\mathbb{Z}_\infty$ for $\mathbb{N} \cup \{0\}$)
- $\mathcal{Q}_n = (\mathbb{Q}_n)^{\mathbb{Z}}$
- $\mathcal{Z}_n = (\mathbb{Z}_n)^{\mathbb{Z}}$

Clearly, $\mathcal{Q}$ is a commutative ring with pointwise addition and multiplication, and $\mathcal{P}$ and $\mathcal{N}$ are subrings of $\mathcal{Q}$. The ring structure of $\mathcal{P}$ is identical to that of $\mathbb{Q}[X]$, the ring of polynomials in some indefinate variable X. In particular, each polynomial function has an associated polynomial.

For $n \in \mathbb{N}$, $\mathcal{Q}_n$ does not have a ring structure as $\mathcal{Q}$ does (though $\mathcal{Z}_n$ does), but it is still an abelian group with addition mod n, and this is all we need it to be. There is a natural projection μ_n from $\mathcal{Q}$ to $\mathcal{Q}_n$, which sends each sequence into its residue mod n.

Definition Let $n > 0 \in \mathbb{Q}$. We define $\mu_n : \mathcal{Q} \to \mathcal{Q}_n$ by

$$\mu_n(f)(x) = [f(x)]_n$$

By the above definition, $\mathcal{Q}_n = \mu_n(\mathcal{Q})$, and $\mathcal{Z}_n = \mu_n(\mathcal{Z})$. Accordingly, we define

- $\mathcal{P}_n = \mu_n(\mathcal{P})$
- $\mathcal{N}_n = \mu_n(\mathcal{N})$

We shall refer to elements of $\mathcal{P}$ as (Rational) Polynomial Sequences (PSs), and accordingly, we shall refer to elements of $\mathcal{P}_n$ as Polynomial Sequence Residues mod n, or PSR$_n$s. In the introduction, we mentioned that we would henceforth identify the circle with the unit interval $[0, 1)$ with addition modulo 1, so we can represent all polynomial sequences on the circle as PSR$_1$s, but as we shall see in Lemma 2.0.5.i, $\mathcal{Q}_1 \simeq \mathcal{Q}_n$ and $\mathcal{P}_1 \simeq \mathcal{P}_n$ for all $n \in \mathbb{N}$, so we could have said this paper was about PSR_{47}s, or whatever. That being said, we will be working enough in $\mathcal{Q}_1$ that it is worthwhile to assign symbols to some of its important subsets.

Definition Let $n \in \mathbb{N}$. We define

- $\Phi = \mathcal{Q}_1$
- $\Phi_n = \{f \in \Phi \big| n(f(x) - f(0)) \in \mathbb{Z} \ \forall x \in \mathbb{Z}\}$
- $\Phi_{n^\infty} = \bigcup_{k=0}^{\infty} \Phi_{n^k}$
- $\Pi = \mathcal{P}_1$
- $\Pi_n = \Pi \cap \Phi_n$
- $\Pi_{n^\infty} = \Pi \cap \Phi_{n^\infty}$

We also define $\mathfrak{I}_n = \mu(\mathfrak{I}/n) \in \Phi$. That is,

$$\mathfrak{I}_n(x) \equiv x/n \ \forall x \in \mathbb{Z}$$

Now, since the objects we are dealing with are functions of $\mathbb{Z}$, the the forward difference operator Δ will come in handy. Δ is to these functions essentially what the derivative is to differentiable functions of $\mathbb{R}$.

Definition We define $\Delta : \mathcal{Q} \to \mathcal{Q}$ by

$$\Delta[f](x) = f(x+1) - f(x).$$

We also let

- $\Delta^0[f](x) = f(x)$
- $\Delta^n[f](x) = \Delta[\Delta^{n-1} f](x)$

for $n \in \mathbb{N}$.

Summing the recursive definition of Δ^n yields the following expression.

Lemma 2.0.1 *For $n \in \mathbb{N}_0, x \in \mathbb{Z}, f \in \mathcal{Q}$,*

$$\Delta^n[f](x) = \sum_{k=0}^{n}(-1)^k \binom{n}{k} f(x+n-k)$$
$$= \sum_{k=-\infty}^{\infty}(-1)^k \binom{n}{k} f(x+n-k)$$

For $n \in \mathbb{Z}$, reader probably recognises the binomial coefficient $\binom{n}{k}$ as the X^k coefficient of the expression $(1+X)^n$, or as the number of ways we can pull k rabbits out of a hat consisting of n rabbits. Since these numbers are integers, the function $\binom{\bullet}{k} \in \mathcal{Z}$. A more general definition of $\binom{x}{k}$ for all $x \in \mathbb{C}$ is

$$\binom{x}{k} = \frac{1}{k!}\prod_{j=0}^{k-1}(x-j)$$

where we adopt the convention that $\prod_{j=0}^{-1}(x-j) = 1$.

Since the RHS is a polynomial, $\binom{\bullet}{k} \in \mathcal{N}$. Substituting 0 for x and x for n in Lemma 2.0.1, we get the following corollary, which asserts that for $n \in \mathbb{N}, f \in \mathcal{Q}$, if we are given the values $f(0), ..., f(n-1)$, the value of $f(n)$ is uniquely determined by $\Delta^n[f](0)$.

Corollary 2.0.2 *For $x \in \mathbb{N}_0, f \in \mathcal{Q}$,*

$$f(x) = \Delta^x[f](0) + \sum_{k=1}^{x}(-1)^{k-1}\binom{x}{k} f(x-k).$$

Applying Corollary 2.0.2 recursively yields the fact that for $n \in \mathbb{N}, f \in \mathcal{Q}$, the value of $f(n)$ is uniquely determined by the differences $\Delta^k[f](0)$ for $0 \le k \le n$. In particular, this implies that if f is a periodic sequence with period n, the differences $\Delta^k[f](0)$ for $0 \le k \le n$ uniquely determines f. This is important because as we shall see shortly (Lemma 2.0.5.ii), every PSR_1 is periodic. Periodic sequences will be important enough to our considerations that it is worthwhile to make the following definitions.

Definition For any $S \subset \mathcal{Q}$, we define

- $S^m = \left\{ f \in \mathcal{Q} \middle| f(x+m) = f(x) \ \forall x \in \mathbb{Z} \right\}$

- $S^{m^\infty} = \bigcup_{k=0}^{\infty} S^{m^k}$

So for instance, $(\Phi_5)^7 = \Phi_5^7$ is the set of doubly infinite sequences taking values in $\{0, 1/5, 2/5, 3/5, 4/5\}$ which repeat every 7 terms. We will refer to the sets Π^m as *periodic domains.* If $f \in \Pi$, then there is a $d \in \mathbb{N}$ and $\tilde{f}(x) \in \mathbb{Z}[x]$ such that $f \equiv \frac{\tilde{f}}{d}$. It is not hard to see that for any such d, $f \in \Pi_d$ The relationship between the non-negative values of f and its differences at 0 can be made explicit via the following formula due to Isaac Newton.

$$\begin{aligned} f(x) &= \sum_{k=0}^{\infty} \Delta^k[f](0)\binom{x}{k} \\ &= \sum_{k=0}^{x} \Delta^k[f](0)\binom{x}{k} \end{aligned}$$

for all $f \in \mathcal{Q}, x \in \mathbb{Z}$, the second equality being due to the fact that $\binom{x}{k} = 0$ for $k > x$. In slightly more generality, the formula goes as follows.

Theorem 2.0.3 (Newton's forward difference formula) *Let $f \in \mathcal{Q}$. Then for all $x \geq a \in \mathbb{Z}$*

$$f(x) = \sum_{k=0}^{\infty} \Delta^k[f](a)\binom{x-a}{k}$$

The following corollary is an easy consequence of Theorem 2.0.3.

Corollary 2.0.4 *Let $f \in \mathcal{Q}$. Then*

- *$f \in \mathcal{P}$ iff $\exists! \nu_k \in \mathbb{Q}$ such that*

$$f(x) = \sum_{k=0}^{d} \nu_k \binom{x}{k} \;\; \forall x \in \mathbb{Z} \tag{2.1}$$

  where d is the smallest non-negative integer such that $\Delta^k f(0) = 0$ for all $k > d$.

- *$f \in \mathcal{N}$ iff $\exists! \nu_k \in \mathbb{Z}$ satisfying Equation 2.1*

- *$f \in \mathcal{P}_n$ iff $f \in \mathcal{Q}_n$ and $\exists! \nu_k \in \mathbb{Q}_n$ such that*

$$f(x) \equiv \sum_{k=0}^{d} \nu_k \binom{x}{k} \mod n \;\; \forall x \in \mathbb{Z}$$

where d is the smallest non-negative integer such that $\Delta^k[f](0) \equiv 0 \mod n$ for all $k > d$.

For $f \in \mathcal{P}$, the number d from the previous corollary is clearly equal to the degree of its corresponding polynomial, which suggests the following definition

Definition For $f \in \mathcal{Q}$, we define

- $\deg f$ to be the smallest non-negative integer d such that $\Delta^k[f](0) = 0$ for all $k > d$.
- $\deg_n f$ to be the smallest non-negative integer d such that $\Delta^k[f](0) \equiv 0 \mod n$ for all $k > d$.

Accordingly, we definec for $S \subset \mathcal{Q}$

- $S[d] = \{f \in S \big| \deg(f) < d\}$
- $S[d, n] = \{f \in S \big| \deg_n(f) < d\}$

We note that for $f \in \mathcal{P}_n$,

$$\deg_n f = \min_{\bar{f} \in \mathcal{P}} \left\{\deg \bar{f} | \bar{f} \equiv f \mod n\right\}$$

We will now state a few easy but important facts about some of the subgroups we have defined.

Lemma 2.0.5 *Let $m, n \in \mathbb{N}$, p prime. Then*

i. The mapping $f \to f/n$ is an isomorphism of abelian groups from $\mathcal{Q}_n$ to $\Phi(= \mathcal{Q}_1)$, $\mathcal{P}_n$ to Π, and an injective homomorphism from $\mathcal{Z}_n$ to Φ_n, and $\mathcal{N}_n$ to Π_n, both with kernel $\Phi^1 = \Pi^1 \simeq \mathbb{Q}_1$.

ii. $\Pi = \bigcup_{n=1}^{\infty} \Pi^n = \bigcup_{n=1}^{\infty} \Pi_n$

iii. $\Pi^{p^\infty} = \Pi_{p^\infty} + \Pi^1$

iv. $\Pi^m = \{f \in \Pi \big| f \circ \mu_m = f\}$

Now, it is clear from lemma 2.0.5.iii that

$$\Pi^{p^n} \subset \Phi_{p^\infty}^{p^n}.$$

In chapter 4, we will show that the opposite inclusion is also true, so that we have the following theorem.

Theorem 2.0.6 *Let p be a prime, and let $n \in \mathbb{N} \cup \{\infty\}$. Then*

$$\Pi^{p^n} = \Phi^{p^n}_{p^\infty},$$

Thus, we will completely classify the set of PSR_1's with prime power period. In chapter 5, we will show (among other things) that this suffices to classify all of Π. In particular, we will prove the following.

Theorem 2.0.7 *Let m, n coprime in $\mathbb{N}$ and $f_m \in \Pi^m, f_n \in \Pi^n$ with $f_m(0) = f_n(0)$. Then there is a unique function $f \in \Pi^{mn}$ such that*

$$f(qx) = f_r(x),$$
$$f(rx) = f_q(x)$$

$\forall x \in \mathbb{Z}$.

This property not only provides a decomposition of Π into factors of $\Pi^{p^\infty} = \Phi^{p^\infty}_{p^\infty}$, but is also useful for constructing PSR_1s with interesting graphs.

Chapter 3

Embeddings

Recall the example in the introduction in which we let $f(x) \equiv \frac{x^2}{160000}$ and $\varphi_k(x) = 16000 + k + 5x$ for $k \in \{-2, ..., 2\}$. We showed that the graph of f embeds the five parabolas $\{\varphi_k(x), f \circ \varphi_k(x) | x \in \mathbb{Z}\}$ and that these parabolas are approximately similar and evenly spaced for $x \approx 16000$. The action

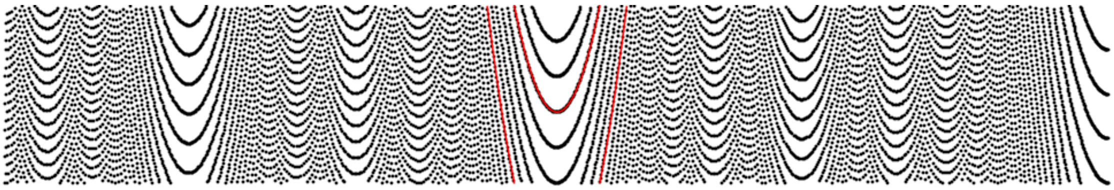


Figure 3.1: $\{(x, f(x)) : x \in \{12000, ..., 20000\}\}$
$\{(\varphi_2(x), f(\varphi_2(x))) | x \in [-101, 101]\}$

$f \mapsto f \circ \varphi$ will be important enough to give it its own operation symbol, $\star$

Definition We define $\star : \mathcal{Z} \to \mathrm{End}_{\mathrm{Ab}}(\mathcal{Q})$ by

$$\star(\varphi) = \varphi^\star$$

where $\varphi^\star : \mathcal{Q} \to \mathcal{Q}$ is defined by

$$\varphi^\star(f) = f \circ \varphi$$

for all $f \in \mathcal{Q}$. We will call such a $\varphi^\star$ an *embedding*. If for $f, g \in \mathcal{Q}$, $\exists \varphi \in \mathcal{Z}$ such that $\varphi^\star(f) = g$, we say that f *embeds* g.

The following lemma contains some easy but useful facts about embeddings.

Lemma 3.0.8 *For* $\varphi \in \mathcal{N}, n \in \mathbb{N}$

i. $\varphi^\star \circ \mu_n = \mu_n \circ \varphi^\star$

ii. $\varphi^\star(\mathcal{P}) \subset \mathcal{P}$

iii. $\varphi^\star(\mathcal{P}_n) = \mathcal{P}_n$

iv. $\varphi^\star(\Pi_n) = \Pi_n$

v. $\forall n \in \mathbb{N}\ \exists r \in \mathbb{N} \ni \varphi^\star(\Pi^n) = \Pi^{n^r}$

We will be particularly interested in the action of $\star$ on $\mathcal{N}$, owing to to the following easy lemma.

Lemma 3.0.9 *Let $\varphi \in \mathcal{Z}$. TFAE*

i $\varphi \in \mathcal{N}$

ii $\varphi^\star(\mathfrak{I}) \in \mathcal{P}$

iii $\varphi^\star(\mathcal{P}) \subset \mathcal{P}$

Proof *i* $\Longleftrightarrow$ *ii*. $\varphi^\star(\mathfrak{I}) = \varphi \in \mathcal{Z}$ and $\mathcal{N} = \mathcal{Z} \cap \mathcal{P}$, so clearly, $\varphi \in \mathcal{N}$ iff $\varphi^\star(\mathfrak{I}) \in \mathcal{P}$.

iii $\Longleftrightarrow$ *ii*. Obvious.

i $\Longleftrightarrow$ *iii*. If $\varphi \in \mathcal{N}, f \in \mathcal{P}$, then $\varphi^\star f = f \circ \varphi$ which is obviously a polynomial sequence since f and φ are.

■ We have an analogous lemma concerning the action of $\star$ on $\mathcal{N}_n$ for $n \in \mathbb{N}$.

Lemma 3.0.10 *Let $\varphi \in \mathcal{Z}_n$. TFAE*

i $\varphi \in \mathcal{N}_n$

ii $\varphi^\star(\mathfrak{I}_n) \in \Pi$

iii $\varphi^\star(\Pi) \subset \Pi$

We can see that $\star$ is an injection of $\mathcal{N}$ by noticing that the function, $\star^{-1} : \mathrm{End}_{\mathrm{Ab}}(\mathcal{Q}) \to \mathcal{Q}$, given by

$$\star^{-1}(\psi) = \psi(\mathfrak{I})$$

is the inverse of $\star$ on its range $\mathcal{N}^\star$ since

$$\begin{aligned}\star^{-1}(\varphi^\star) &= \varphi^\star(\mathfrak{I})\\ &= \mathfrak{I}\circ\varphi\\ &= \varphi.\end{aligned}$$

In fact, we have the following lemma

Lemma 3.0.11 *$\star$ is an anti-isomorphism of the composition semigroups $\mathcal{N}$ and $\mathcal{N}^\star$*

Proof φ is a homomorphism since

$$\begin{aligned}(\varphi^\star\circ\psi^\star)\,f(x) &= \varphi^\star\,(\psi^\star f)\,(x)\\ &= (\psi^\star f)\,(\varphi(x))\\ &= f\,(\psi(\varphi(x))\\ &= f\,((\psi\circ\varphi)(x))\\ &= (\psi\circ\varphi)^\star f\,(x)\,,\end{aligned}$$

and since we already know that $\star$ is a bijection between $\mathcal{N}$ and $\mathcal{N}^\star$, φ is an isomorphism.
■

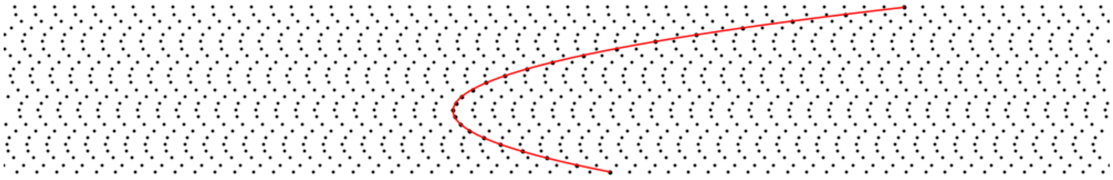
As a second example of embeddings, let $f\in\mathcal{P}_1$ be defined by

$$f(x)\equiv(x+2/5)^3$$

and for $k\in\mathbb{Z},x\in\mathbb{R}$, let

$$\varphi_k(x)=\frac{5x^2}{2}+\frac{x}{2}+5k-1.$$

Since $\varphi_k(\mathbb{Z})\subset\mathbb{Z}$, $\varphi\in\mathcal{N}$, so $\varphi^\star f\in\mathcal{P}_1$. The sets $\{(\varphi_k(x),\varphi_k^\star f(x))\,|x\in\mathbb{Z}\}$ cover the graph of f



$\{(x, f(x)) \,|x \in \{-700, ..., 700\}\}$
$\left\{\left(\varphi_{-26}(x), \frac{1}{25}x + \frac{48}{125}\right) |x \in \{-9, ..., 15\}\right\}$

with horizontal parabolas. It is not difficult to see why. First note that for $x \in \mathbb{Z}$,

$$\begin{aligned}(x + 2/5)^3 &= x^3 + \frac{6}{5}x^2 + \frac{12}{25}x + \frac{8}{125} \\ &\equiv \frac{1}{5}x^2 + \frac{12}{25}x + \frac{8}{125},\end{aligned}$$

so

$$\begin{aligned}\varphi_k^\star f(x) &\equiv \frac{1}{5}\varphi_k(x)^2 + \frac{12}{25}\varphi_k(x) + \frac{8}{125} \\ &\equiv \frac{5}{4}x^4 + \frac{1}{2}x^3 + \left(5k\frac{1}{4}\right)x^2 + \left(k + \frac{1}{25}\right)x + 5k^2 + \frac{2}{5}k - \frac{27}{125} \\ &= 30\binom{x}{4} + 48\binom{x}{3} + (21 + 10k)\binom{x}{2} + \left(\frac{51}{25} + 6k\right)x + 5k^2 + \frac{50k - 27}{125} \\ &\equiv \frac{1}{25}x + \frac{50k - 27}{125}.\end{aligned}$$

Thus,

$$\left\{(\varphi_k(x), \varphi_k^\star f(x)) \,|x \in \mathbb{Z}\right\} \equiv \left\{\left(\frac{5}{2}x^2 + \frac{1}{2}x + 5k - 1, \frac{1}{25}x + \frac{50k - 27}{125}\right) \middle| x \in \mathbb{Z}\right\}.$$

So, since these sets are quadratic in the first variable and affine in the second, they are horizontal parabolas, and the parameter k appears only in the constant term of both variables, so the parabolas are all similar. Finally, since $\frac{5}{2}x^2 + \frac{1}{2}x$ takes every value mod 5, $\{\varphi_k(x) \middle| x, k \in \mathbb{Z}\} = \mathbb{Z}$ so the sets $\{(\varphi_k(x), \varphi_k^\star f(x)) \,|x \in \mathbb{Z}\}$ cover the graph of f.

Affine Embeddings

If $\varphi \in \mathcal{N}$ is an affine/linear function, we call $\varphi^\star$ an affine/linear embedding. If φ is linear with $\varphi(x) = \alpha x$, we will sometimes write $\alpha^\star$ instead of $\varphi^\star$. Unlike general embeddings, affine embeddings all commute with each other, and are easier to work with. The set of affine embeddings is an abelian (composition) subgroup of $\mathcal{N}^\star$, and in turn, the set of linear embeddings is a subgroup of the set of affine embeddings. The embeddings $\varphi_k^\star$ are affine in the first example and not in the second, As another example of affine embeddings, let $f \in \mathcal{P}_1$ with

$$f(x) \equiv \frac{241x^2}{1734}$$

and consider the embeddings $\varphi_+^\star$, $\varphi_-^\star$ and $\psi_k^\star$ where

$$\varphi_\pm(x) = 17x \pm 3$$

$$\psi_k(x) = 3x + k$$

Then

$$\varphi_\pm^\star f(x) \equiv \frac{x^2}{6} \pm \frac{3x}{17} + \frac{145}{578} \tag{3.1}$$

This is illustrated in the following graph. The sets $\big(\varphi_\pm(x), \varphi_\pm^\star f(x)\big)$ (in red and blue above)

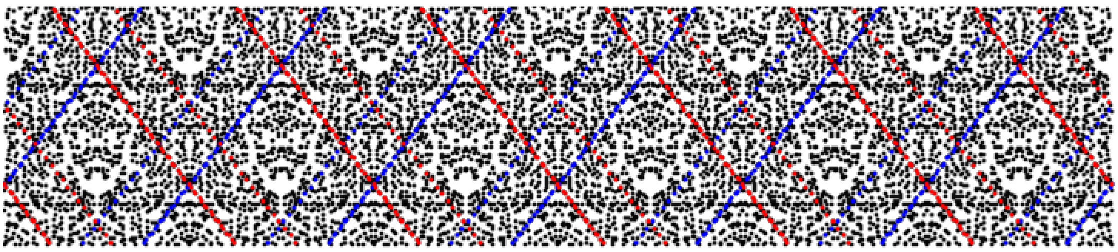


Figure 3.2: $\left\{(x, f(x))\,|x \in \mathbb{Z}_{-5202}^{5202}\right\}$
$\left\{\big(\varphi_+(x), \varphi_+^\star f((x))\big)\,|x \in \mathbb{Z}_{-306}^{306}\right\}$
$\left\{\big(\varphi_-(x), \varphi_-^\star f((x))\big)\,|x \in \mathbb{Z}_{-306}^{306}\right\}$

embed a lattice pattern into the graph of f, but the functions $\varphi_\pm^\star f$ are not affine (mod 1).

However, they do embed such functions. Indeed,

$$\begin{aligned}\psi_k^\star\left(\varphi_\pm^\star f\right)(x) &\equiv \frac{(3x+k)^2}{6} \pm \frac{3(3x+k)}{17} + \frac{145}{578}\\ &\equiv \frac{9x^2}{6} \pm \frac{9x}{17} + \frac{k^2}{6} \pm \frac{3k}{17} + \frac{145}{578}\\ &\equiv \frac{x^2}{2} \pm \frac{9x}{17} + \varphi_\pm^\star f(k)\\ &\equiv \left(\frac{1}{2} \pm \frac{9}{17}\right) x + \varphi_\pm^\star f(k)\end{aligned}$$

So, the embedded sets $\psi_k^\star\left(\varphi_\pm^\star f\right)(x) = \left(\varphi_\pm \circ \psi_k\right)^\star f(x)$ are all self-collinear (mod 1). Furthermore the sets $\left(\varphi_\pm(x), \varphi_\pm^\star f(x)\right)$ are covered by the sets $\bigcup\limits_{k=0}^{2} \left(\varphi_\pm \circ \psi_k\right)^\star f(x)$. This is illustrated below. In

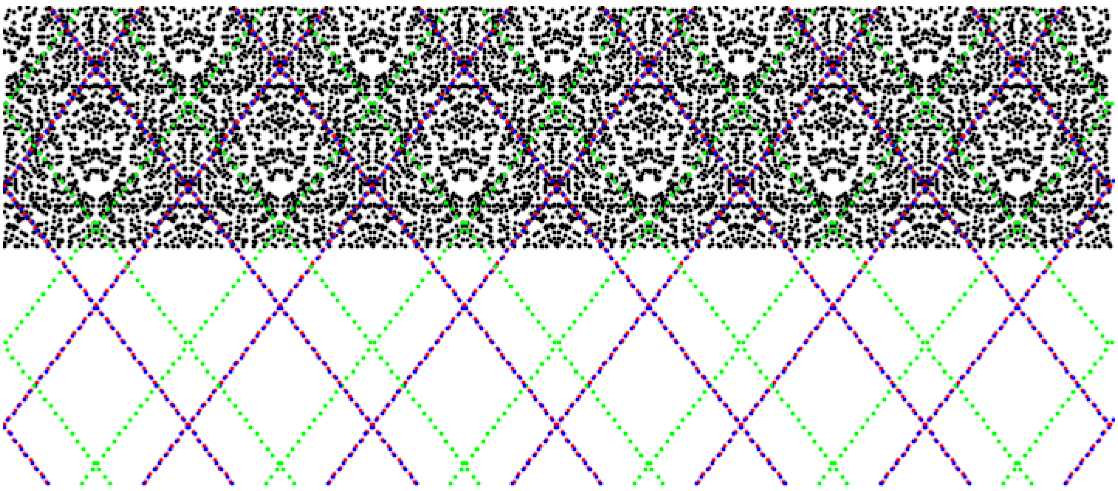


Figure 3.3: $\left\{\left(\varphi_\pm(x), \varphi_\pm^\star f(x)\right) | x \in \mathbb{Z}_{-306}^{306}, \pm \in \{+,-\}\right\}$
$\left\{\left(\left(\varphi_\pm \circ \psi_0\right)(x), \left(\varphi_\pm \circ \psi_0\right)^\star f(x)\right) | x \in \mathbb{Z}_{-102}^{102}, \pm \in \{+,-\}\right\}$
$\left\{\left(\left(\varphi_\pm \circ \psi_{\pm 1}\right)(x), \left(\varphi_\pm \circ \psi_{\pm 1}\right)^\star f(x)\right) | x \in \mathbb{Z}_{-102}^{102}, \pm \in \{+,-\}\right\}$
$\left\{\left(\left(\varphi_\pm \circ \psi_{\pm 2}\right)(x), \left(\varphi_\pm \circ \psi_{\pm 2}\right)^\star f(x)\right) | x \in \mathbb{Z}_{-102}^{102}, \pm \in \{+,-\}\right\}$

the foregoing example, we saw that applying any of the embeddings $\psi_k^\star$ to either of the functions $\varphi_\pm^\star f$ yields an affine function mod 1. This is because

$$\begin{aligned}\frac{(3x+k)^2}{6} &= \frac{9x^2+6kx+k^2}{6}\\ &\equiv \frac{x^2}{2} + \frac{k^2}{6}\\ &\equiv \frac{x}{2} + \frac{k^2}{6}\end{aligned}$$

for all $x, k \in \mathbb{Z}$. More generally, for any integer α and odd integer β,

$$\frac{(\alpha + \beta x)^2}{2\beta} \equiv \frac{x}{2} + \frac{\alpha^2}{6} \tag{3.2}$$

Thus, functions of the form $x \mapsto \mu\left(\frac{x^2}{2\beta} + bx + c\right)$ should all embed lines at intervals of β. This is a good example of how we can choose coefficients to find PSR_1s with certain graphical features. Equation 3.2 is a special case of the following theorem.

Theorem 3.0.12 *Let $f \in \mathcal{P}$, let d be the degree of f, and let $\alpha \in \mathbb{Z}$. Then for all $\beta \in \mathbb{Z}$ such that $\beta^\star f \in \mathcal{N}$,*

$$f(\alpha + \beta x) \equiv \sum_{k=0}^{d-1} \Delta^k \left[\beta^\star f\right](\alpha/\beta) \binom{x}{k}.$$

Proof Since $\beta^\star f \in \mathcal{N}$ (so that $f \in \ker(\beta^\star) + f(0)$), f must be of the form

$$f(x) \equiv \sum_{n=0}^{d} \nu_n \binom{x/\beta}{n}$$

where $\nu_0 \equiv f(0)$ and $\nu_n \in \mathbb{Z}$ for $n \in \mathcal{N}$. Thus,

$$f(\alpha + \beta x) \equiv \sum_{n=0}^{d} \nu_n \binom{x + \alpha/\beta}{n}.$$

But by the Chu-Vandermonde Identity,

$$\begin{aligned}\binom{x + \alpha/\beta}{n} &= \sum_{k=0}^{n} \binom{\alpha/\beta}{n-k}\binom{x}{k} \\ &= \sum_{k=0}^{\infty} \binom{\alpha/\beta}{n-k}\binom{x}{k}\end{aligned}$$

and

$$\begin{aligned}
\binom{\alpha/\beta}{n-k} &= \binom{\bullet}{n-k}(\alpha/\beta) \\
&= \Delta^k \left[\binom{\bullet}{n}\right](\alpha/\beta) \\
&\equiv \Delta^k \left[\beta^\star \binom{\bullet/\beta}{n}\right](\alpha/\beta)
\end{aligned}$$

so

$$\begin{aligned}
f(\alpha+\beta x) &\equiv \sum_{n=0}^{d} \nu_n \sum_{k=0}^{\infty} \Delta^k \left[\beta^\star \binom{\bullet/\beta}{n}\right](\alpha/\beta)\binom{x}{k} \\
&\equiv \sum_{k=0}^{\infty} \Delta^k \left[\beta^\star \left(\sum_{n=0}^{d} \nu_n \binom{\bullet/\beta}{n}\right)\right](\alpha/\beta)\binom{x}{k} \\
&\equiv \sum_{k=0}^{\infty} \Delta^k \left[\beta^\star f\right](\alpha/\beta)\binom{x}{k}
\end{aligned}$$

Now, clearly $\Delta^k [\beta^\star f](\alpha/\beta)\binom{x}{k} = 0$ for all $k, x \in \mathbb{Z}$ with $k > d$, since f has degree d. On the other hand, when $k = d$, we have that for all $t \in \mathbb{Q}$,

$$\begin{aligned}
\Delta^k [\beta^\star f](t) &= \Delta^d \left[\beta^\star \sum_{n=0}^{d} \nu_n \binom{\bullet/\beta}{n}\right](t) \\
&= \Delta^d \left[\beta^\star \nu_d \binom{\bullet/\beta}{d}\right](t) \\
&= \nu_d \Delta^d \left[\binom{\bullet}{d}\right](t) \\
&= \nu_d \binom{\bullet}{0}(t) \\
&= \nu_d \binom{t}{0} \\
&= \nu_d \\
&= 0
\end{aligned}$$

Thus, letting $t = \alpha/\beta$, we see that $\Delta^n \left[\beta^\star f\right](\alpha/\beta)\binom{x}{n} \equiv 0$ for all $x \in \mathbb{Z}$, and thus that

$$f(\alpha + \beta x) \equiv \sum_{k=0}^{d-1} \Delta^k \left[\beta^\star f\right](\alpha/\beta)\binom{x}{k}.$$

■

Fibers under Embeddings

Let $f, \tilde{f} \in \mathcal{P}$ and φ non-constant in $\mathbb{N}$, and suppose $\varphi^\star\left(\tilde{f}\right) = f$. Then $\tilde{f}$ is unique among PSs in this respect, for suppose $g \in \mathcal{P}_1$ with $\varphi^\star(g) = f$. Then

$$\begin{aligned} 0 &= \varphi^\star(g)(x) - \varphi^\star\left(\tilde{f}\right)(x) \\ &= \varphi^\star(g - \tilde{f})(x) \\ &= \left(g - \tilde{f}\right)(\varphi(x)) \end{aligned}$$

So $g - \tilde{f}$ has infinitely many roots and therefore must be identically 0.

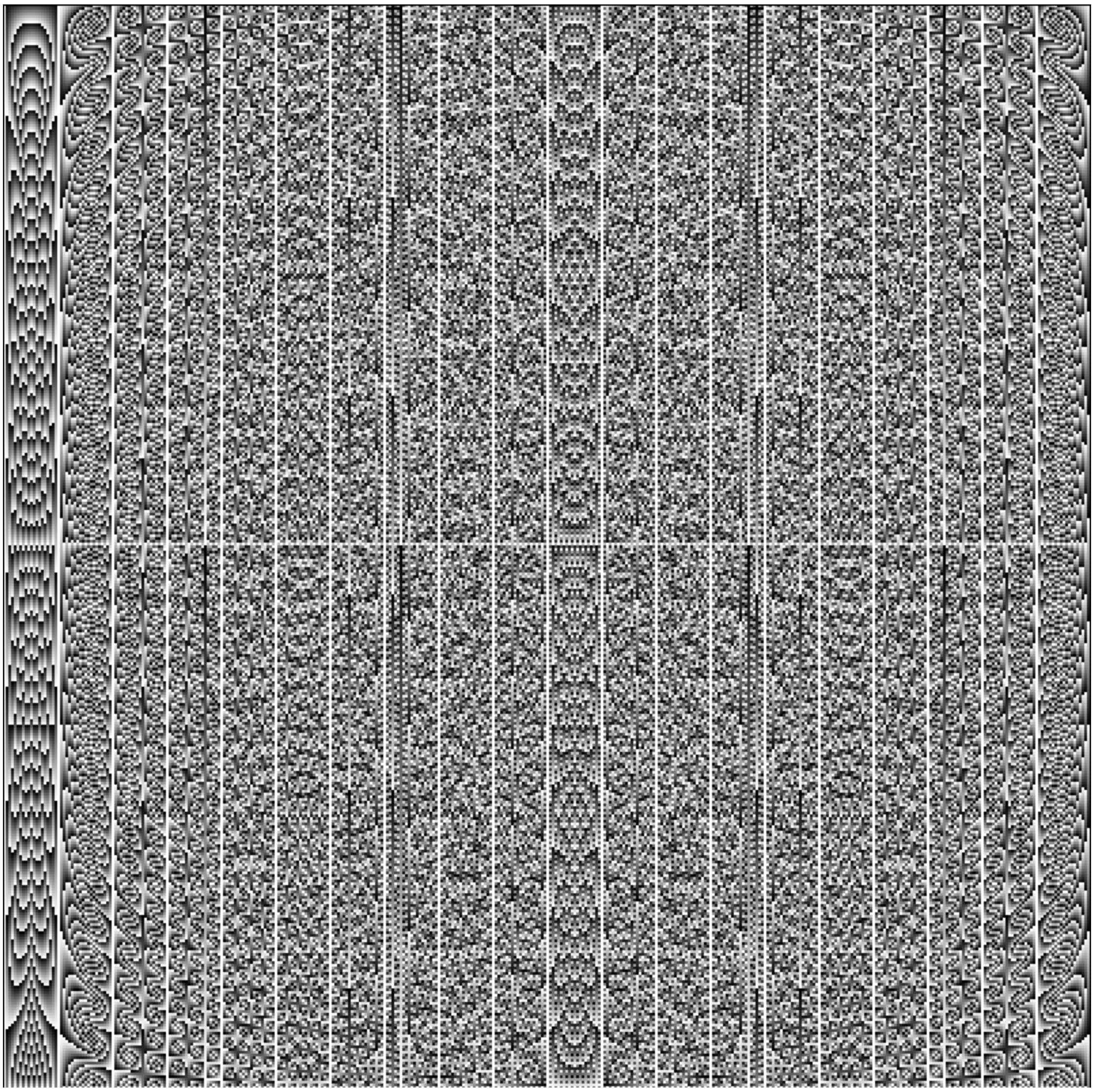


Figure 3.4: $\left\{\nu\binom{x/20}{2}|x,\nu \in \{0,400\}\right\}$

This uniqueness does not hold for $f, \tilde{f} \in \mathcal{P}_1$. Indeed, we will show that the set of functions $g \in \mathcal{P}_1$ such that $\varphi^\star g = f$ is typically infinite. The above mentioned set, denoted $(\varphi^\star)^{-1}\{f\}$, is called the fiber of f under φ. This next easy lemma will be helpful in finding fibers.

Lemma 3.0.13 *Let* $f, \tilde{f} \in \mathcal{P}_1$ *and* $\varphi \in \mathbb{N}$. *Then*

$$(\varphi^\star)^{-1}\{f\} \equiv \tilde{f} + \ker \varphi^\star$$

This reduces the problem of finding $(\varphi^\star)^{-1}\{f\}$ to finding one of its elements along with the set $\ker\varphi^\star = \{g \in \mathcal{P}_1 \big| \varphi^\star g = f\}$. Both these tasks are easy if φ is an affine function. For example, consider the embedding $20^\star$. The linear elements of $\ker 20^\star$ are of the form $x \mapsto \nu x/20$. Not very exciting. The quadratic elements are these plus a term of the form $\nu\binom{x/20}{2} = \frac{\nu x(x-20)}{800}$. Figure 3.4 shows a color plot, the rows of which are these terms for $x = 0$ to 400, indexed by ν. Notice the white vertical stripes. These are where x is a multiple of 20.

The following corollary is an easy consequence of Proposition 3.0.14.

Proposition 3.0.14 *Let $\varphi(x) = \alpha x + \beta$. Then $\forall f \in \ker\varphi^\star\ \exists! d \in \mathbb{N}_0, \nu_1, ..., \nu_d \in \mathbb{Z}$ with $0 \leq \nu_k < \alpha^k k!$ such that*

$$f(x) \equiv \sum_{k=1}^{d} \frac{\nu_k}{\alpha^k k!} \prod_{j=0}^{k-1} x - j\alpha - \beta$$

for all $x \in \mathbb{Z}$.

Thus, for $f \in \mathcal{P}_1$ with $f \equiv \bar{f} \in \mathcal{P}$, we have that for all $g \in (\varphi^\star)^{-1}\{f\}\ \exists! d \in \mathbb{N}_0, \nu_1, ..., \nu_d \in \mathbb{Z}$ with $0 \leq \nu_k < \alpha^k k!$ such that

$$g(x) \equiv \bar{f}\left(\frac{x-\beta}{\alpha}\right) + \sum_{k=1}^{d} \frac{\nu_k}{\alpha^k k!} \prod_{j=0}^{k-1} x - j\alpha - \beta$$

Corollary 3.0.15 *Let $f \in \mathcal{P}_1$, and $\varphi(x) = \alpha x + \beta$ with $\alpha \in \mathbb{N}, \beta \in \mathbb{Z}$. Then $(\varphi^\star)^{-1}\{f\}$ has precisely $\alpha^{\frac{d^2+d}{2}} d\$$ elements of order d or less, where $d\$$ is (not a Latex error but) the superfactorial of d, defined by $d\$ = \prod_{k=1}^{d} k!$.*

In particular, $(\varphi^\star)^{-1}\{f\}$ has infinitely many elements if $a > 1$, and only one element if $a = 1$.

For example, let $f \in \mathcal{P}_1$ with $f(x) \equiv \frac{x^2}{15000}$, and let $\varphi(x) = 41x$. Now, suppose $g \in (\varphi^\star)^{-1}\{f\}$. Then according to Proposition 3.0.14, $\exists d \in \mathbb{N}, \nu_1, ..., \nu_d \in \mathbb{Z}$ such that

$$g(x) \equiv \frac{x^2}{25215000} + \sum_{k=1}^{d} \frac{\nu_k}{41^k k!} \prod_{j=0}^{k-1} (x - 41j)$$

Figure 3.5: $\left\{\left(x, \frac{x^2}{15000} \mod 1\right) : x \in \{-170, 170\}\right\}$

for all $x \in \mathbb{Z}$.

Now, according to Corollary 3.0.15, there are 137842 such functions of order 2 or less. These functions are of the form

$$\begin{aligned} g(x) &\equiv \frac{x^2}{25215000} + \frac{\nu_1}{41}x + \frac{\nu_2}{3362}x(x-41) \\ &= \frac{1+7500\nu_2}{25215000}x^2 + \frac{2\nu_1 - \nu_2}{82}x \end{aligned}$$

Here are plots of some such functions for various values of ν_1 and ν_2 on the domain $x \in \{-6965, 6965\}$.

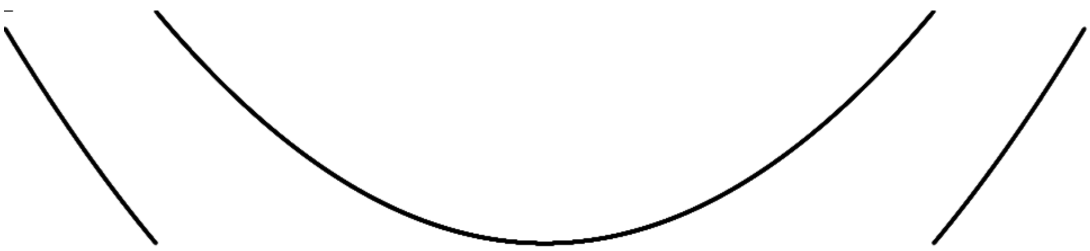


Figure 3.6: $\nu_1 = 0, \nu_2 = 0$

Figure 3.7: $\nu_1 = 0, \nu_2 = 10$

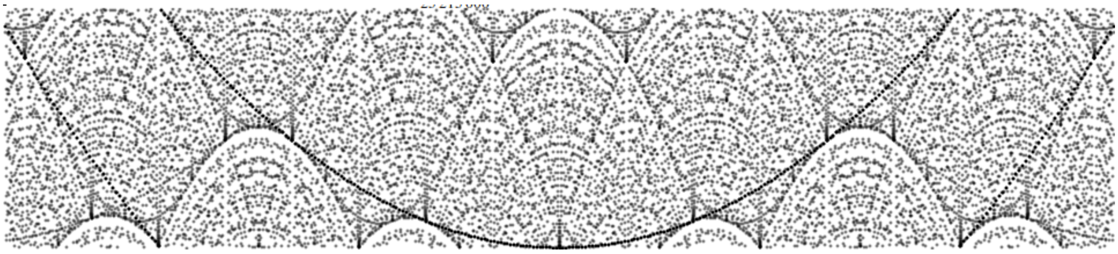


Figure 3.8: $\nu_1 = 1, \nu_2 = 2$

Figure 3.9: $\nu_1 = 5, \nu_2 = 7$

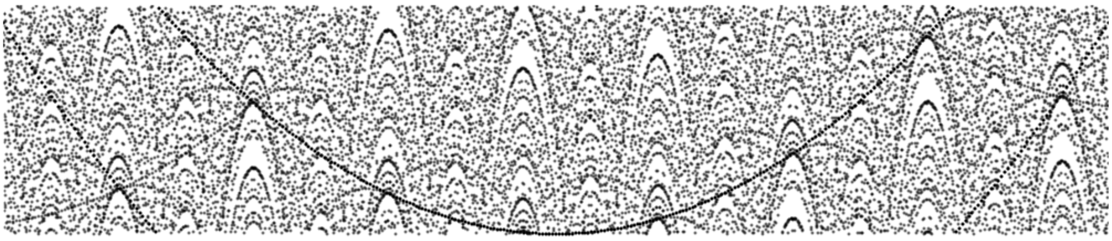


Figure 3.10: $\nu_1 = 5, \nu_2 = 20$

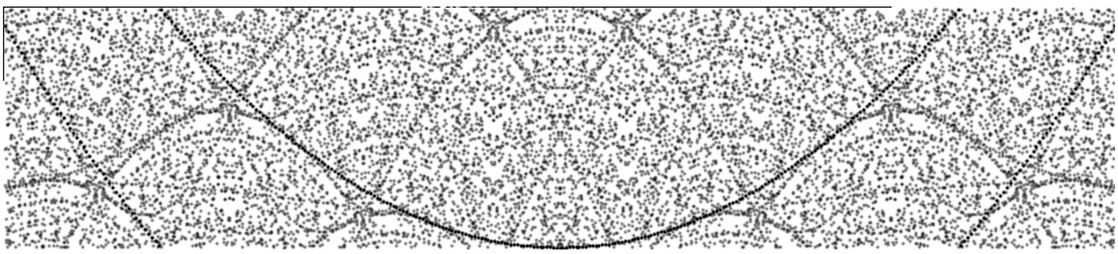


Figure 3.11: $\nu_1 = 26, \nu_2 = 52$

Figure 3.12: $\nu_1 = 12, \nu_2 = 24$

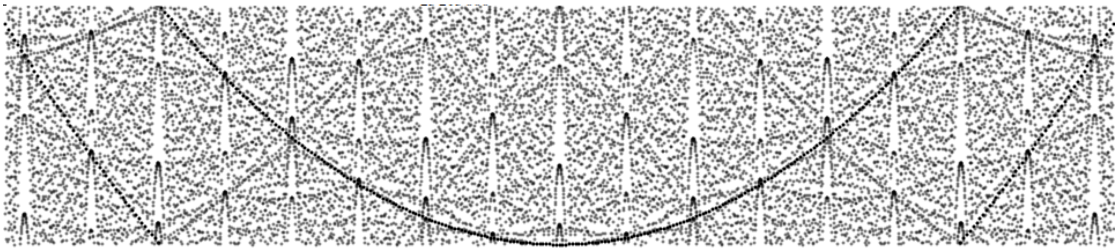


Figure 3.13: $\nu_1 = 140, \nu_2 = 280$

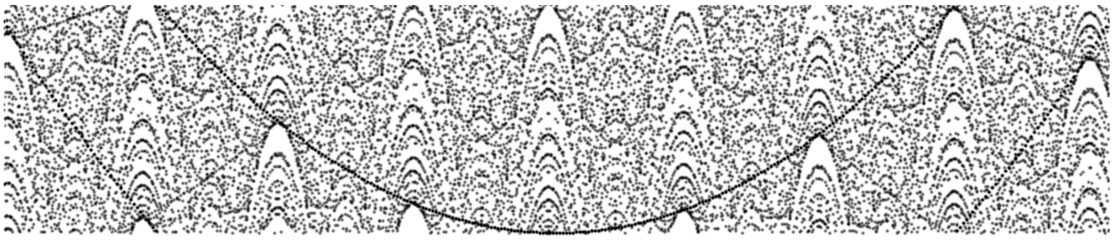


Figure 3.14: $\nu_1 = 7, \nu_2 = 16$

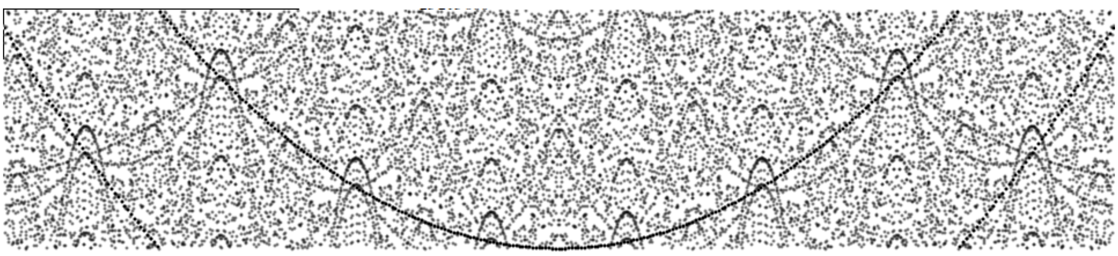


Figure 3.15: $\nu_1 = 882, \nu_2 = 1764$

Chapter 4

The Category of Periodic Domains

For any $\varphi \in \mathcal{N}$, the embedding $\varphi^\star$ acts as an endomorphism of the group Π. To better understand this action, we can look at the action of $\varphi^\star$ on the various periodic domains Π^n. In fact, it will behoove us to consider the subcategory $\mathcal{PD}$ of $\mathcal{AB}$ whose set of objects is $\{\Pi^n | n \in \mathbb{N}\}$, and whose morphisms are polynomial embeddings. More precisely, we define $\mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n)$ to be the embeddings in $\mathcal{N}^\star$ modulo equivalence on Π^m. In other words, for $\psi \in \mathrm{Hom}_{\mathcal{AB}}(\Pi^m, \Pi^n)$ we will say that $\psi \in \mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n)$ iff there exists some $\varphi \in \mathcal{N}$ such that

$$\psi(f) = \varphi^\star(f) \quad \forall f \in \Pi^m. \tag{4.1}$$

Under this equivalence, we may make the identification $\mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n) = (\mathcal{N}^n_m)^\star$ since by part *ii* of the following lemma, we have for each $\psi \in \mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n)$ a $\varphi \in \mathcal{N}^n_m$ satisfying Equation 4.1. In particular, if $\varphi \in \mathcal{N}$ satisfies the equation, then $\mu_m(\varphi) \in \mathcal{N}^n_m$.

Lemma 4.0.16 *Let $\varphi^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n)$. Then*

i. $\mu_m(\varphi)$ *is the unique* $\psi \in \mathcal{N}^n_m$ *satisfying equation 4.1.*

ii. $\mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n) \simeq (\mathcal{N}^n_m)^\star$

iii. $l \subset n \Longrightarrow l \subset m \quad \forall l \in \mathbb{N}$

iv. $n \subset m \Longrightarrow \exists \tilde{\varphi} \in \mathcal{N} \ni \varphi = (m/n)\tilde{\varphi}$

The simplest and most important elements of these Hom classes are the linear embeddings the form $a^\star$ for $a \in \mathbb{Z}$. There are at most m such elements (up to equivalence) in $\mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n)$ since $(a+m)^\star \equiv a^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi^m, \Pi^n)$. If $a \cap m = 1$, then $a^\star$ is a period preserving automorphism of Π^m, whereas if $a \cap m = m$, $a^\star = 0^\star$ on Π_m. In general, $a^\star$ maps Π^m surjectively to $\Pi^{m \backslash a}$.

Linear embeddings will be useful in several of the forthcoming proofs, including that of the following lemma, with which we shall conclude this chapter.

Lemma 4.0.17 *Let $m, n \in \mathbb{N}$. Then*

$$\Pi^{m \cap n} = \Pi^m \cap \Pi^n$$

$$\Pi^{m \cup n} = \Pi^m + \Pi^n$$

Proof *The first equation is easy, so we will prove the second. Stated another way, it asserts that for $l, m, n \in \mathbb{N}$ all pairwise coprime, $\Pi^{lmn} = \Pi^{lm} + \Pi^{ln}$, and by induction, it suffices to prove this when $l = 1$. Now clearly, $\Pi^m + \Pi^n \subset \Pi^{mn}$, so we must prove the opposite inclusion. So, suppose $f \in \Pi^{mn}$. Then $f \equiv \frac{\tilde{f}}{lm^r n^s}$, for some $l, r, s \in \mathbb{N}$ with $l \cap m = l \cap n = 1$ and $\tilde{f}(x) \in \mathbb{Z}[x]$. Now, there exist $a, b, c \in \mathbb{N}$ such that and*

$$\frac{1}{d} = \frac{a}{m^r} + \frac{b}{n^s} + \frac{c}{l},$$

so that

$$f \equiv \frac{a\tilde{f}}{m^r} + \frac{b\tilde{f}}{n^s} + \frac{c\tilde{f}}{l}.$$

Now $n^\star f \in \Pi_m$, so $n^\star$ must send the second two terms to constants mod 1, since n^s and l are both coprime to m, but n is also coprime to l, so $n^\star$ preserves its period (of 1), so it is constant to begin with. Thus

$$f \equiv \frac{a\tilde{f}}{m^r} + \frac{b\tilde{f}}{n^s} + C,$$

and

$$n^\star f \equiv n^\star \frac{a\tilde{f}}{m^r} + B + C,$$

but $n^\star$ preserves the period of the first term just as it does the third. Therefore, the first term mod 1 is in Π^m, and by a similar argument, the second term mod 1 is in Π^n. Thus, the inclusion is proved. ■

Chapter 5

Prime Power Periodic Domains

The main thrust of this chapter will be to prove Theorem 2.0.6, but we will attain some results along the way about the residues of binomial coefficients modulo prime powers, which are well-researched in their own right (see [1], [2])

We shall soon have need of Kummer's theorem, which can be found (e.g.) in [3]

Theorem 5.0.18 *[Kummer's Theorem] Let p be a prime, $r < n \in \mathbb{N}$, and $s = n - r$. Also for $j \in \mathbb{N}_0$, let n_j be defined such that $n = \sum_{j=0}^{\infty} n_j p^j$, and let r_j, s_j be defined similarly. Let q be the smallest number such that n_j, r_j, and s_j are all 0 for $j > q$. Then*

$$\frac{1}{p-1}\sum_{j=0}^{q}(r_j + s_j - n_j) = \max\left\{m \in \mathbb{N} \middle| p^m \subset \binom{n}{r}\right\}$$

the LHS being the number of 'carries' involved in subtracting r from n in base p.

We shall also make use of the following fact which can be found in [2].

Lemma 5.0.19 *If n and k are positive integers and p is a prime, then*

$$\binom{pn}{pk} \equiv \binom{n}{k} \mod p^r$$

for any $r \in \mathbb{N}$ such that $p^r \subset pnk(n-k)$.

Lemma 5.0.20 *For p prime, $k \in \mathbb{Z}$, $l, m, q \in \mathbb{N}_0$ with $l < p^m \leq p^q$,*

$$\binom{p^q}{kp^m + l} \equiv \binom{p^{q-m}}{k}\binom{0}{l} \mod p^{q-m+1} \tag{5.1}$$

Proof We begin by noting that if $k < 0$ or $k \geq p^{q-m}$, Equation 5.1 is trivially true, so we may assume that $0 \leq k < p^{q-m}$. Now, suppose $l > 0$. $\binom{0}{l} = 0$ for all integers $l \neq 0$, so for $0 < l < p^m$, Equation 5.1 turns into

$$\binom{p^q}{kp^m + l} \equiv 0 \mod p^{q-m+1}.$$

To prove this equivalence, we will use Kummer's theorem (Theorem 5.0.18). Let $n = p^q$, and let $r = kp^m + l$. Note that because of our assumptions on k, $r < n$. Accordingly, define $s = n - r$ and let n_j, r_j, and s_j be as in the theorem. With these numbers so defined, q matches the definition of q in the theorem as well. Now, let ξ be the least positive integer j such that $r_j \neq 0$, so that $r = \sum_{j=\xi}^{q-1} r_j p^j$. Then

$$\begin{aligned}
s - 1 &= (n-1) - r \\
&= \sum_{j=0}^{q-1} (p-1)p^j - \sum_{j=\xi}^{q-1} r_j p^j \\
&= \sum_{j=0}^{\xi-1} (p-1)p^j + \sum_{j=\xi}^{q-1} (p-1-r_j)p^j
\end{aligned}$$

But then

$$\begin{aligned}
s &= p^{\xi} + \sum_{j=\xi}^{q-1} (p-1-r_j)p^j \\
&= (p - r_{\xi})p^{\xi} + \sum_{j=\xi+1}^{q-1} (p-1-r_j)p^j
\end{aligned}$$

Thus, the number of times p divides $\binom{p^q}{kp^m+l}$ is

$$\begin{aligned}
\frac{1}{p-1}\sum_{j=0}^{q}(r_j+s_j-n_j) &= \frac{1}{p-1}\left(\sum_{j=0}^{q-1}(r_j+s_j)-n_q\right)\\
&= \frac{1}{p-1}\left(\sum_{j=0}^{\xi-1}(r_j+s_j)+(r_\xi+s_\xi)+\sum_{j=\xi+1}^{q-1}(r_j+s_j)-1\right)\\
&= \frac{1}{p-1}\left(0+p+\sum_{j=\xi+1}^{q-1}(p-1)-1\right)\\
&= q-\xi.
\end{aligned}$$

But because $r-kp^m=l<p^m$, we must have that $kp^m=\sum_{j=m}^{q-1} r_j$, and therefore that $l=\sum_{j=\xi}^{m-1} r_j$. But then, since we are assuming that $l>0$, we must have that $\xi\le m-1$. Thus, $p^{q-m+1}\subset p^{q-\xi}\subset\binom{p^q}{kp^m+l}$ so that

$$\binom{p^q}{kp^m+l}\equiv 0 \mod p^{q-m+1},$$

as desired.

On the other hand, if $l=0$ then $\binom{0}{l}=1$, so Equation 5.1 becomes.

$$\binom{p^q}{kp^m}\equiv\binom{p^{q-m}}{k} \mod p^{q-m+1}$$

To prove this equality, we will show by induction that for $j\in\{0,...,m\}$,

$$\binom{p^{q-m+j}}{kp^j}\equiv\binom{p^{q-m}}{k} \mod p^{q-m+1}$$

Indeed, the base case ($j=0$) is tautologically true, so suppose that for some $j\in\{0,...,m-1\}$, we have that

$$\binom{p^{q-m+j}}{kp^j}\equiv\binom{p^{q-m}}{k} \mod p^{q-m+1}.$$

Then by Lemma 5.0.19, we have that

$$\begin{aligned}\binom{p^{q-m+j+1}}{kp^{j+1}} &\equiv \binom{p(p^{q-m+j})}{p(kp^{j})}\\ &\equiv \binom{p^{q-m+j}}{kp^{j}} \mod p^{r}.\end{aligned}$$

for any $r \in \mathbb{N}$ such that

$$\begin{aligned}p^{r} &\subset p(p^{q-m+j})(kp^{j})(p^{q-m+j} - kp^{j})\\ &= k(p^{q-m+2j+1})(p^{q-m+j} - kp^{j})\end{aligned}$$

In particular, we can choose $r = q - m + 1$, and so by our induction hypothesis,

$$\begin{aligned}\binom{p^{q-m+j+1}}{kp^{j+1}} &\equiv \binom{p^{q-m+j}}{kp^{j}}\\ &\equiv \binom{p^{q-m}}{k} \mod p^{q-m+1},\end{aligned}$$

which completes the proof.

Theorem 5.0.21 *For p prime, $l, m, q, n \in \mathbb{N}_0$ with $l \leq p^m \leq p^q \leq n$,*

$$\sum_{k=-\infty}^{\infty} (-1)^{kp^m+l}\binom{n}{kp^m+l} \equiv 0 \mod p^{q-m+1} \tag{5.2}$$

Proof We will first show by induction on n that it suffices to prove the theorem for $n = p^q$. Indeed, suppose the theorem holds for some $n \geq p^q$. Then by Pascal's Rule,

$$\begin{aligned}\sum_{k=-\infty}^{\infty} (-1)^{kp^m+l}\binom{n+1}{kp^m+l} &= \sum_{k=-\infty}^{\infty} (-1)^{kp^m+l}\binom{n}{kp^m+l-1} + \sum_{k=-\infty}^{\infty} (-1)^{kp^m+l}\binom{n}{kp^m+l}\\ &\equiv \sum_{k=-\infty}^{\infty} (-1)^{kp^m+l}\binom{n}{kp^m+l-1} \mod p^{q-m+1}\end{aligned}$$

since the second summand on the RHS of the first equality is equivalent to 0 mod p^{q-m+1} by the induction hypothesis. Now, in the case that $l = 0$,

$$\begin{aligned}\sum_{k=-\infty}^{\infty}(-1)^{kp^m+l}\binom{n}{kp^m+l-1} &= \sum_{k=-\infty}^{\infty}(-1)^{kp^m}\binom{n}{(k-1)p^m+(p^m-1)}\\ &= -\sum_{k=-\infty}^{\infty}(-1)^{(k-1)p^m+(p^m-1)}\binom{n}{(k-1)p^m+(p^m-1)}\\ &\equiv 0,\end{aligned}$$

by the induction hypothesis. On the other hand, if $l \neq 0$,

$$\begin{aligned}\sum_{k=-\infty}^{\infty}(-1)^{kp^m+l}\binom{n}{kp^m+l-1} &= \sum_{k=-\infty}^{\infty}(-1)^{kp^m+l}\binom{n}{kp^m+(l-1)}\\ &= -\sum_{k=-\infty}^{\infty}(-1)^{kp^m+(l-1)}\binom{n}{kp^m+(l-1)}\\ &\equiv 0,\end{aligned}$$

again by the induction hypothesis. Thus it suffices to prove that for p, l, m, q as above,

$$\sum_{k=-\infty}^{\infty}(-1)^{kp^m+l}\binom{p^q}{kp^m+l} \equiv 0 \mod p^{q-m+1}.$$

Furthermore, we may assume in this case that $l = 0$, since if $l > 0$, Lemma 5.0.20 guarantees that

$$\binom{p^q}{kp^m+l} \equiv 0 \mod p^{q-m+1}.$$

for all $k \in \mathbb{Z}$. So it suffices to prove that for p, m, q as above,

$$\sum_{k=-\infty}^{\infty}(-1)^{kp^m}\binom{p^q}{kp^m} \equiv 0 \mod p^{q-m+1}.$$

For this, we will first assume that p=2 and m=0. Then

$$\begin{aligned}
\sum_{k=-\infty}^{\infty} (-1)^{kp^m} \binom{p^{q-m}}{k} &= \sum_{k=-\infty}^{\infty} (-1)^k \binom{2^{q-m}}{k} \\
&= \sum_{k=0}^{2^q-m} (-1)^k \binom{2^q}{k} x^{2^q-m-k} \Big|_{x=1} \\
&= (x-1)^{2^{q-m}} \Big|_{x=1} \\
&= 0.
\end{aligned}$$

If, on the other hand, $p = 2$ but $m > 0$,

$$\begin{aligned}
\sum_{k=-\infty}^{\infty} (-1)^{kp^m} \binom{p^{q-m}}{k} &= \sum_{k=-\infty}^{\infty} \binom{2^{q-m}}{k} \\
&= \sum_{k=0}^{2^q-m} \binom{2^{q-m}}{k} x^{2^q-m-k} \Big|_{x=1} \\
&= (x+1)^{2^{q-m}} \Big|_{x=1} \\
&= p^{p^{q-m}} \\
&\equiv 0 \mod p^{q-m+1}.
\end{aligned}$$

Now suppose $p > 2$. We will show that in this case, it suffices to prove the theorem for $m = 0$, for assume we have indeed proven this. Then for all $p > 2, q \in \mathbb{N}_0$,

$$\sum_{k=-\infty}^{\infty} (-1)^k \binom{p^q}{k} \equiv 0 \mod p^{q+1}.$$

But then

$$\begin{aligned}
\sum_{k=-\infty}^{\infty} (-1)^{kp^m} \binom{p^q}{kp^m} &\equiv \sum_{k=-\infty}^{\infty} (-1)^k \binom{p^{q-m}}{k} \\
&\equiv 0 \mod p^{(q-m)+1}
\end{aligned}$$

where the first equivalence is due to Lemma 5.0.20 and the second follows from our assumption.

Thus, we have only left to prove that for all $p > 2, q \in \mathbb{N}_0$,

$$\sum_{k=-\infty}^{\infty} (-1)^k \binom{p^q}{k} \equiv 0 \mod p^{q+1}.$$

But indeed,

$$\begin{aligned}
\sum_{k=-\infty}^{\infty} (-1)^k \binom{p^q}{k} &= \sum_{k=0}^{p^q} (-1)^k \binom{p^q}{k} \\
&= \sum_{k=0}^{\frac{p^q-1}{2}} (-1)^k \binom{p^q}{k} + \sum_{k=0}^{\frac{p^q-1}{2}} (-1)^{p^q-k} \binom{p^q}{p^q-k} \\
&= \sum_{k=0}^{\frac{p^q-1}{2}} (-1)^k \binom{p^q}{k} + \sum_{k=0}^{\frac{p^q-1}{2}} (-1)^{-k} \binom{p^q}{k} \\
&= 0
\end{aligned}$$

as desired.

$\blacksquare$

Theorem 5.0.22 *For $m \in \mathbb{N}_0, r \in \mathbb{N}$, and p prime,*

$$\mathcal{Z}_{p^r}^{p^m} = \mathcal{N}_{p^r}^{p^m}[p^{r+m-1}, p^r].$$

Proof $\mathcal{N}_{p^r}^{p^m}[p^{r+m-1}, p^r] \subset \mathcal{Z}_{p^r}^{p^m}$ by definition, so we only need to prove the opposite inclusion.

So, suppose $f \in \mathcal{Z}_{p^r}^{p^m}$. Then by Lemma 2.0.1, we have that for arbitrary $n \in \mathbb{N}_0$,

$$
\begin{aligned}
\Delta^n[f](0) &= \sum_{j=-\infty}^{\infty} (-1)^j \binom{n}{j} f(n-j) \\
&= \sum_{l=0}^{p^m-1} \sum_{k=-\infty}^{\infty} (-1)^{kp^m+l} \binom{n}{kp^m+l} f\left(n-(kp^m+l)\right) \\
&\equiv \sum_{l=0}^{p^m-1} \sum_{k=-\infty}^{\infty} (-1)^{kp^m+l} \binom{n}{kp^m+l} f\left(n-l\right) \\
&\equiv \sum_{l=0}^{p^m-1} f\left(n-l\right) \left(\sum_{k=-\infty}^{\infty} (-1)^{kp^m+l} \binom{n}{kp^m+l} \right) \mod p^r.
\end{aligned}
$$

But if $n \geq p^{r+m-1}$, then by substituting $q = r+m-1$ into Theorem 5.0.21, we get that

$$
\sum_{k=-\infty}^{\infty} (-1)^{kp^m+l} \binom{n}{kp^m+l} \equiv 0 \mod p^r
$$

so that

$$
\begin{aligned}
\Delta^n[f](0) &\equiv \sum_{l=0}^{p^m-1} f\left(n-l\right)(0) \\
&\equiv 0 \mod p^r.
\end{aligned}
$$

■

By Theorem 5.0.22 and Lemma 2.0.5.i, we have the next theorem, whence immediately follows the assertion of Theorem 2.0.6.

Theorem 5.0.23 *For $m, r \in \mathbb{N}$, and p prime,*

$$
\Phi_{p^r}^{p^m} = \Pi_{p^r}^{p^m}[p^{r+m-1}, 1] = \Pi_{p^r}^{p^m}.
$$

The following corollary is immediate.

Corollary 5.0.24 *For $m \in \mathbb{N}$ and p prime,*

$$
\Pi^{p^m} = \Phi_{p^\infty}^{p^m}.
$$

We can cheaply derive another result from the above which seems somewhat surprising at first glance.

Theorem 5.0.25 *Every rational-valued sequence with a prime power period is the residue of a polynomial modulo some rational number.*

Proof Let $f \in \mathcal{Q}^{p^m}$. First, we will deal with the case when $f \in \mathcal{Z}^{p^m}$. In this case, $f \in \mathcal{Z}_{p^r}^{p^m} = \mathcal{N}_{p^r}^{p^m}$, where r is the least positive integer such that $f(x) < p^r \ \forall x \in \mathbb{Z}$. Now, for general $f \in \mathcal{Q}^{p^m}$, let d be the smallest positive integer such that $df \in \mathcal{Z}$, and let r be the least positive integer such that $df(x) < p^r \ \forall x \in \mathbb{Z}$. Then $df \in \mathcal{N}_{p^r}^{p^m}$ so $f \in \mathcal{N}_{p^r/d}^{p^m}$. ■

Chapter 6

Entwining Products & General Periodic Domains

Theorem 6.0.26 *Let $m \cap n = 1$, and let $f_m \in \Pi^m$, and $f_n \in \Pi^n$ have equal values at 0. Then there is a unique sequence $f = f_m \,{}_m\!\oplus_n f_n \in \Pi_{mn}$ such that*

$$m^\star(f) = f_n \tag{6.1}$$

$$n^\star(f) = f_m \tag{6.2}$$

Proof First, we will prove the case when $f_m(0) = 0 = f_n(0)$. In this case, define

$$f_m \,{}_m\!\oplus_n f_n = [n^{-1}]_m^\star f_m + [m^{-1}]_n^\star f_n. \tag{6.3}$$

Then

$$\begin{aligned} n^\star(f_m \,{}_m\!\oplus_n f_n)(x) &= f_m([n^{-1}]_m nx) + f_n([m^{-1}]_n nx) \\ &= f_m((1+km)x) + f_n(0) \\ &= f_m(x). \end{aligned}$$

So $f_m \,{}_m\!\oplus_n f_n$ satisfies Equation 6.2, and satisfies Equation 6.1 by a similar calculation. Thus, we have proved existance. To prove uniqueness, suppose $g \in \Pi_{mn}$ satisfies the equations. By Lemma 4.0.17, $g = g_m + g_n$ for some $g_m \in \Pi_m, g_n \in \Pi_n$. Thus, by our assumption,

$$\begin{aligned} f_m &= n^\star g \\ &= n^\star g_m + n^\star g_n \\ &= n^\star g_m. \end{aligned}$$

But then since $m \cap n = 1$, we have that $[n^{-1}]^{\star}_{m} f_m = g_m$. Similarly, $[m^{-1}]^{\star}_{n} f_n = g_n$, so $g = f_m \; {}_m\!\oplus_n \; f_n$. Thus, we have proved the theorem in the case where $f_m(0) = f_n(0) = 0$. To prove the general theorem, suppose $f_m(0) = f_n(0) = c \in \mathbb{Q}_1$. Then we define

$$f_m \; {}_m\!\oplus_n \; f_n = (f_m - c) \; {}_m\!\oplus_n \; (f_n - c) + c. \tag{6.4}$$

This function clearly satisfies the desired Equations 6.1 and 6.2 and is unique by the above arguments.

The partial functions ${}_m\!\oplus_n : \Pi^m \times \Pi^n \to \Pi^{mn}$, which we shall call *entwining products*, have a few interesting applications, the first of which is that they provide a tool to construct new PSR_1s which embed any given pair of old ones with coprime periods. It is easy to see by induction that given any finite set of PSR_1s with pairwise coprime periods, we may entwine them into a PSR_1 which embeds them all.

Corollary 6.0.27 *Let $m_1, ..., m_r \in \mathbb{N}$ be pairwise coprime, let $m = \prod_{k=1}^{r} m_k$, and $f_k \in \Pi^{m_k}$ for $k \in \{1, ..., r\}$. Then there is a unique sequence $f_1 \; {}_{m_1}\!\oplus_{m_2} \cdots {}_{m_{r-1}}\!\oplus_{m_r} \; f_r \in \Pi$ such that*

$$(m/m_k)^{\star}(f_1 \; {}_{m_1}\!\oplus_{m_2} \cdots {}_{m_{r-1}}\!\oplus_{m_r} \; f_r) = f_k \tag{6.5}$$

Not only may we use entwinement to construct PSR_1s of period mn from those with periods m and n whenever $m \cap n = 1$, but *all* such PSR_1s may be constructed this way, since by theorem 6.0.26, we have that for any $f \in \Pi^{mn}$, $f = n^{\star} f \; {}_m\!\oplus_n m^{\star} f$. In other words, for $f_1, f_2 \in f_{mn}$ (with $m \cap n = 1$), $f_1 = f_2$ iff $m^{\star} f_1 = m^{\star} f_2$ and $n^{\star} f_1 = n^{\star} f_2$ We may use this fact, along with Corollary 5.0.24, to classify all periodic domains. Now we will give an example of some "entwined" PSR_1s. Let $f, g, h, j \in \Pi$ with $f(x) \equiv \frac{2x^2}{359}, g(x) \equiv \frac{x^2}{361}, h(x) \equiv \frac{x^2}{2}$, and $j(x) \equiv \frac{x^2}{3}$. f, g, j, and h all map 0 to itself, and their periods are the same as their denominators, and are therefore pairwise coprime, so we may entwine any combination of them into a new function using i from the definition. Four such entwinements are plotted in figures 6.1-6.4. Notice that with the given domains, the second and third graphs above cover the first, and are in turn covered by the fourth.

Figure 6.1: $\{(x, f\ _{359}\oplus_{361}\ g(x) \mod 1) : x \in x \in \{-2500, ..., 2500\}\}$

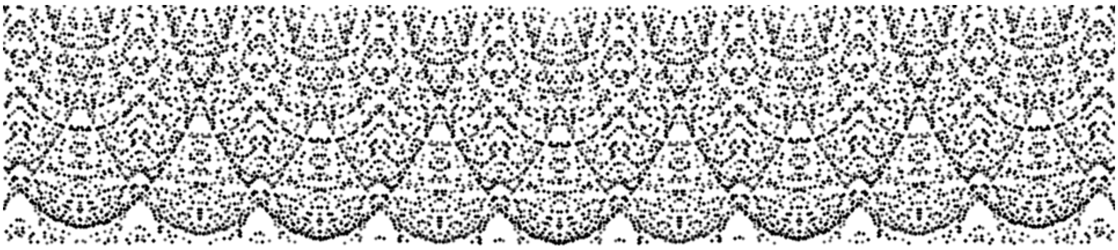


Figure 6.2: $\{(x, f\ _{359}\oplus_{361}\ g\ _{361}\oplus_{2}\ h(x) \mod 1) : x \in x \in \{-5000, ..., 5000\}\}$

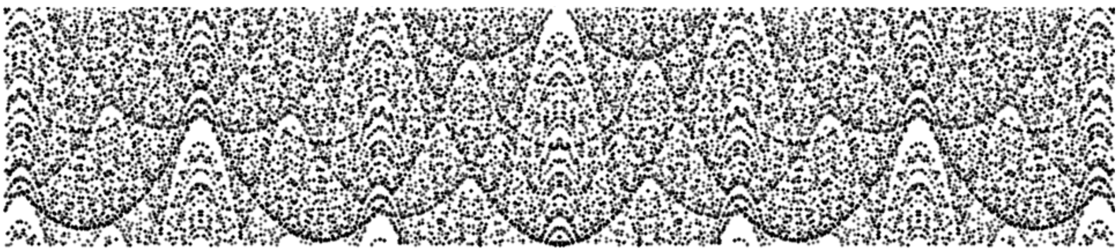


Figure 6.3: $\{(x, f\ _{359}\oplus_{361}\ g\ _{361}\oplus_{3}\ j(x) \mod 1) : x \in \{-7500, ..., 7500\}\}$

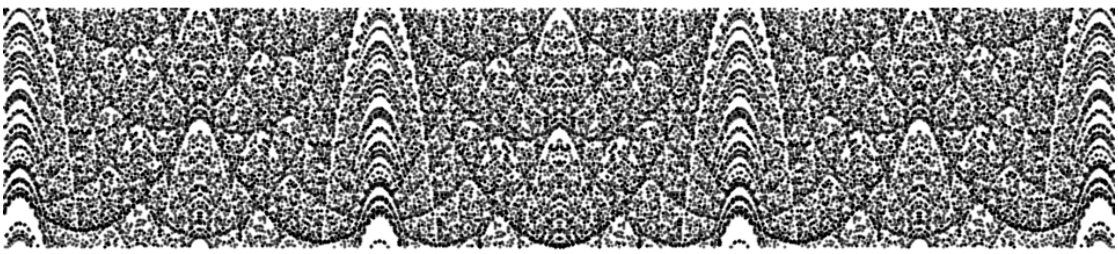


Figure 6.4: $\{(x, f\ _{359}\oplus_{361}\ g\ _{361}\oplus_{2}\ h\ _{2}\oplus_{3}\ j(x) \mod 1) : x \in \{-15000, ..., 15000\}\}$

The following theorem will show precisely how periodic domains relate to their sub-objects.

Theorem 6.0.28 *Let $l, m, n \in \mathbb{N}$ be pairwise coprime. Then Π_{lmn} (along with the morphisms $m^\star : \Pi_{lm} \to \Pi_l$ and $n^\star : \Pi_{ln} \to \Pi_l$) is a fiber product (pullback) of the abelian groups Π_{ln} and Π_{lm} over Π_l.*

Proof First, we will prove the theorem in the case that $l = 1$. To do this, we must show that for any abelian group X and any two homomorphisms $\psi_n : X \to \Pi_n$ and $\psi_m : X \to \Pi_m$, there exists a unique homomorphism $\psi : X \to \Pi_{mn}$ such that the diagram in Figure 6.5 commutes. It is easy to see that the bottom square commutes regardless of ψ, so we need only that for any $\xi \in X$, ψ satisfies the system

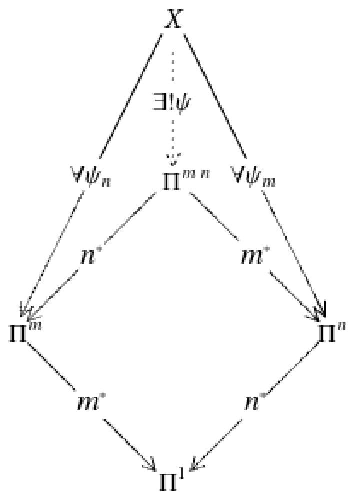


Figure 6.5

$$\begin{aligned} n^\star \psi(\xi) &= \psi_m(\xi) \\ m^\star \psi(\xi) &= \psi_n(\xi). \end{aligned}$$

So by Theorem 6.0.26,

$$\psi(\xi) = \psi_m(\xi) \; {}_m\!\oplus_n \; \psi_n(\xi).$$

Thus, we have a unique function $\psi : X \to \Pi_{mn}$ such that the diagram commutes, so we need only to prove that ψ is a homomorphism of abelian groups. So let $\xi, \eta \in X$. Then

$$\begin{aligned} \psi(\xi + \eta)(mx) &= (\psi_m(\xi + \eta) \; {}_m\!\oplus_n \; \psi_n(\xi + \eta))(mx) \\ &= \psi_n(\xi + \eta)(x) \\ &= \psi_n(\xi)(x) + \psi_n(\eta)(x) \\ &= \psi(\xi)(mx) + \psi(\eta)(mx), \end{aligned}$$

so $m^\star \psi(\xi + \eta) = m^\star(\psi(\xi) + \psi(\eta))$ and similarly $n^\star \psi(\xi + \eta) = n^\star(\psi(\xi) + \psi(\eta))$. Thus, $\psi(\xi + \eta) = \psi(\xi) + \psi(\eta)$ so ψ is indeed a homomorphism.

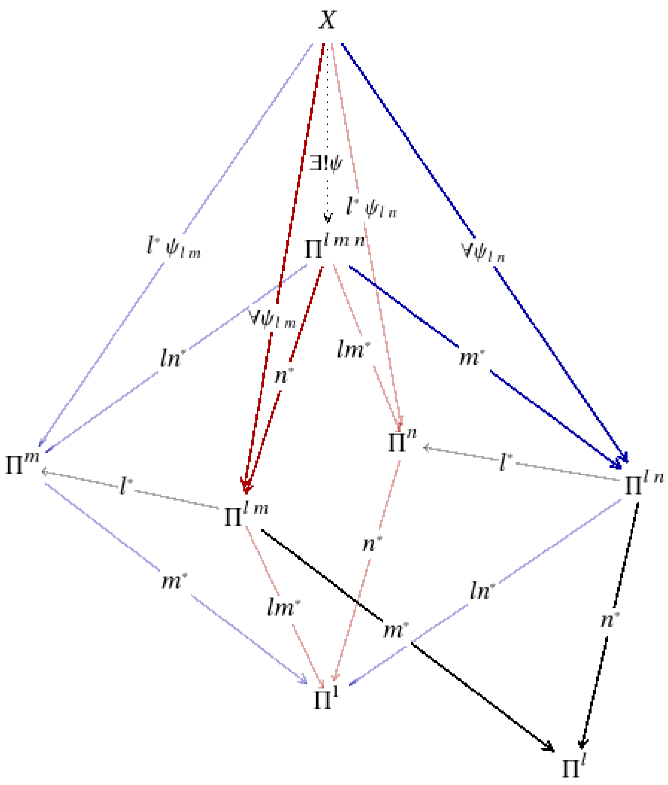


Figure 6.6

Now that we have proven the theorem for $l = 1$, proving the general theorem is only a matter of chasing the diagram in Figure 6.6. The blue and red diamonds within the diagram commute by what we have already proven. Thus, there exists a unique $\psi : X \to \Pi_{lmn}$ making both diamonds commute. But then the same ψ makes the diamond in the foreground commute, as the lower square in the foreground clearly commutes just as the lower square in Figure 6.5 does. Thus, the theorem is true in general. ■

By the above theorem, along with the usual construction of fiber products of general abelian groups (see e.g. p. 81 of [4]) and the fact that all fiber products of a given pair of objects and morphisms are isomorphic, we have the following corollary.

Corollary 6.0.29 *Let $l, m, n \in \mathbb{N}$ be pairwise coprime. Then*

$$\Pi_{lmn} \simeq \{(f_{lm}, f_{ln}) \in \Pi_{lm} \times \Pi_{ln} | m^\star f_{lm} = n^\star f_{ln}\}.$$

The following theorem defines entwining products for suitable sequences in $\mathcal{N}_r$ just as Theorem 6.0.26 did for those in Π. The proof is analogous.

Theorem 6.0.30 *$\varphi_m \in \mathcal{N}_r^m$ and $\varphi_n \in \mathcal{N}_r^n$. Then there exists a unique sequence $\varphi = \varphi_m \; {}_m\!\oplus_n \; \varphi_n \in \mathcal{N}_r^{mn}$ such that*

$$m^\star(\varphi) = \varphi_n$$
$$n^\star(\varphi) = \varphi_m$$

This version of the entwining product will help us show that the fiber product from Theorem 6.0.28 is not only a fiber product $\mathcal{AB}$, but in $\mathcal{PD}$ as well. To see this, we must verify that if we replace the general abelian group X in Figure 6.5 by a periodic domain Π_r, and the homomorphisms ψ_m and ψ_n by morphisms $\varphi_m^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi_r, \Pi_m)$ and $\varphi_n^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi_r, \Pi_n)$, then the mediating morphism $\psi : f \mapsto \varphi_m^\star(f) \; {}_m\!\oplus_n \varphi_n^\star(f)$ is equivalent to some $\varphi^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi_r, \Pi_{mn})$

Lemma 6.0.31 *Let $m, n, r \in \mathbb{N}$ with $m \cap n = 1$ and let $\varphi_m^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi_r, \Pi_n)$ and $\varphi_n^\star \in \mathrm{Hom}_{\mathcal{PD}}(\Pi_r, \Pi_m)$. Then for all $f \in \Pi_r$,*

$$(\varphi_m \; {}_m\!\oplus_n \; \varphi_n)^\star(f) = \varphi_m^\star(f) \; {}_m\!\oplus_n \; \varphi_n^\star(f).$$

Proof

$$\begin{aligned}
m^\star(\varphi_m \; {}_m\!\oplus_n \; \varphi_n)^\star(f))(x) &= \varphi_m \; {}_m\!\oplus_n \; \varphi_n)^\star(f)(mx) \\
&= (\varphi_m \; {}_m\!\oplus_n \; \varphi_n)^\star(f)(mx) \\
&= f((\varphi_m \; {}_m\!\oplus_n \; \varphi_n)(mx)) \\
&= f(\varphi_n(x)) \\
&= \varphi_n^\star f(x) \\
&= (\varphi_m^\star(f) \; {}_m\!\oplus_n \; \varphi_n^\star(f))(mx) \\
&= m^\star(\varphi_m^\star(f) \; {}_m\!\oplus_n \; \varphi_n^\star(f))(x),
\end{aligned}$$

and similarly, $n^\star(\varphi_m \ {}_m\!\oplus_n \varphi_n)^\star(f)) = n^\star(\varphi_m^\star(f) \ {}_m\!\oplus_n \varphi_n^\star(f))$. Thus, since the sequences agree on multiples of m and n and $m \cap n = 1$, the sequences are equal. ■

Thus, our fiber product is universal with respect to periodic domains as well as abelian groups.

References

[1] A. Granville, “Binomial coefficients modulo prime powers,” *Canadian Mathematical Society Conference Proceedings*, vol. 20, pp. 253–275, 1997.

[2] A. D. Loveless, “A congruence for products of binomial coefficients modulo a composite,” *Electronic Journal of Combinatorial Number Theory*, vol. 7, no. A44, 2007.

[3] K. R. McLean, “Divisibility properties of binomial coefficients,” *The Mathematical Gazette*, vol. 58, no. 403, pp. 17–24, 1974.

[4] S. Lang, *Algebra, Revised Third Edition*. Springer, 2002.