SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Iteration of Polynomials

av

Joel Fredin

2017 - No 40

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Iteration of Polynomials

Joel Fredin

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Samuel Lundqvist

2017

Abstract

We define a function which takes a polynomial with coefficients from the integers modulo a prime number and sends it to another polynomial with coefficients from the integers modulo the same prime number. Our main focus is to find the inverse to the function. We will see that the function is linear and so we can represent it as a matrix. Our problem then becomes to find the inverse to the matrix representation. We then start to study, and investigate, the fixed points but also how many times we have to apply the function to an element until we can be certain that we are back at the same element we started at.

Contents

0 Acknowledgement

I would like to thank Samuel Lundqvist for introducing me to this project. I have, during this semester, learned a lot from him and all the work on this thesis.

I am truly grateful for the meetings we've been having every week to discuss my work and which troubles I have run into. The discussions have been really rewarding and which, I think, have made me into a slightly better mathematician.

Samuel has really inspired me and this thesis wouldn't exist if it wasn't for him. Thank you for giving me the opportunity to explore this fascinating project.

1 Introduction

Throughout this paper, we will assume p is a prime. Let $\mathcal{A}_n = \{f \in \mathbb{Z}_n[x], \ \deg f < n\}$ and define a function

$$\begin{aligned} \varphi_p : \mathcal{A}_p &\to \mathcal{A}_p \\ f(x) &\mapsto \sum_{a \in \mathbb{Z}_p} f(a)x^a. \end{aligned}$$

We are interested in studying this function when p is a general prime number. To do so we will see that the function is linear and, hence, we can convert this into a linear algebra problem. Due to this, we can represent φ_p as a matrix and the polynomials as vectors. Then we can use standard methods from linear algebra to get information about our initial problem.

A main question we will examine in this paper is to find the inverse of φ_p (call it M_p). But we will also take a look at another problem.

A description of this problem is as follows. We will start by applying φ_p to a polynomial f, this will give us another polynomial f_1. Apply φ_p to f_1 to get another polynomial f_2. We will see that, eventually, we will come back to the same polynomial we started at. This is due to invertibility of φ_p and that the set A_p is finite.

A simple example is when $p = 2$. Take $f(x) = 1 + x \in \mathcal{A}_2$ and apply φ_2 on f. This gives us

$$\varphi_2(f(x)) = f(0)x^0 + f(1)x^1 = 1 + 0x = 1.$$

If we now apply φ_2 on 1, we see that we end up at $f(x)$, which is where we started. Thus, we see there is a "connection" between 1 and $1 + x$ under this function. Both $0 \in \mathcal{A}_2$ and $x \in \mathcal{A}_2$ stays fixed since $\varphi_2(0) = 0$ and $\varphi_2(x) = x$. Since there are only four elements in $\mathcal{A}_2$, there are no polynomials left.

We want to understand the behaviour of this function when we apply this algorithm in general. We will take a look at how many times we have to apply φ_p until we can be certain that we are back to the same polynomial we started at, no matter which polynomial we started from. We will also investigate the eigenvalues and eigenvectors corresponding to the matrix representation of φ_p, which we define by M_p. We will see that 1 is an eigenvalue to M_p, and we want to answer what the corresponding eigenspace will look like. This is the same as asking, which polynomials satisfies $\varphi_p(f) = f$? To gain intuition and in the hope to see patterns, I have done some programming in Mathematica for some specific values for p.

Finally, the definition of φ_p was suggested by Mats Boij as a variation of a similar iteration process due to Samuel Lundqvist.

2 Representing φ_p as a matrix

We will in this section transform φ_p into a matrix. But first, let us prove the linearity.

Theorem 1. *Let n be any natural number. Then the function φ_n is linear.*

Proof: Let $f(x) = a_0x^0 + a_1x^1 + ... + a_{n-1}x^{n-1}$ and $g(x) = b_0x^0 + b_1x + ... + b_{n-1}x^{n-1}$. We have to show that

$$(1)\ \varphi_p(f) + \varphi_p(g) = \varphi_p(f + g)$$

$$(2)\ \varphi_p(cf) = c\varphi_p(f) \text{ where } c \in \mathbb{Z}_n.$$

(1)

$$
\begin{aligned}
&\varphi_p(f(x)) + \varphi_p(g(x)) \\
&= \varphi_p(a_0x^0 + a_1x^1 + ... + a_{n-1}x^{n-1}) + \varphi_p(b_0x^0 + b_1x + ... + b_{n-1}x^{n-1}) \\
&= \sum_{a\in\mathbb{Z}_n} ((a_0a^0 + a_1a^1 + ... + a_{n-1}a^{n-1})x^a + (b_0a^0 + b_1a + ... + b_{n-1}a^{n-1})x^a) \\
&= \sum_{a\in\mathbb{Z}_n} ((a_0a^0 + a_1a^1 + ... + a_{n-1}a^{n-1}) + (b_0a^0 + b_1a + ... + b_{n-1}a^{n-1}))x^a \\
&= \sum_{a\in\mathbb{Z}_n} (((a_0 + b_0)a^0 + (a_1 + b_1)a^1 + ... + (a_{n-1} + b_{n-1})a^{n-1}))x^a \\
&= \varphi_p(f + g).
\end{aligned}
$$

(2)

$$
\begin{aligned}
&c\varphi_p(f) \\
&= c\sum_{a\in\mathbb{Z}_n} (a_0a^0 + a_1a^1 + .. + a_{n-1}a^{n-1})x^a \\
&= \sum_{a\in\mathbb{Z}_n} c(a_0a^0 + a_1a^1 + .. + a_{n-1}a^{n-1})x^a \\
&= \varphi_p(cf).
\end{aligned}
$$

□

We now have the following result.

Theorem 2.
With respect to the standard basis $\{1, x, \ldots, x^{p-1}\}$, the map φ_p is given by the matrix

$$
M_p = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 \\
1 & 1 & 1 & \cdots & 1 \\
1 & 2^1 & 2^2 & \cdots & 2^{p-1} \\
1 & 3^1 & 3^2 & \cdots & 3^{p-1} \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
1 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1}
\end{bmatrix}.
$$

Proof: Let $f(x) = a_0x^0 + a_1x^1 + \cdots a_{p-1}x^{p-1}$. We have that $f(0) = a_0$, $f(1) = a_01^0 + a_11^1 + \cdots + a_{p-1}1^1$,.., $f(p-1) = a_0(p-1)^0 + a_1(p-1)1^1 + \cdots a_{p-1}(p-1)^{p-1}$. It gives us, directly, the matrix

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2^1 & 2^2 & \cdots & 2^{p-1} \\ 1 & 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{bmatrix}.$$

$\square$

We will soon move on to our first example. But first, let us state a definition.

Definition 1.
*Let v and w be elements in $\mathbb{Z}_p^p$. We say that v and w belongs to the same **cycle** whenever there exists an i such that $M_p^i v = w$.*

A difficult problem is to classify the cycles that arises. The following example shows the computation of the cycles when $p = 3$, using M_3.

Example 1.
Let $p = 3$. Then

$$M_3 = \begin{bmatrix} 1 & 0 & 0 \\ 1^0 & 1^1 & 1^2 \\ 2^0 & 2^1 & 2^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix}.$$

Every polynomial will now be represented as a vector of size 3. For example, the polynomial $f(x) = 1 + x$ will be represented by

$$v_0 := \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix},$$

since the constant coefficient is 1, the coefficient in front of x equals 1 and the coefficient in front of x^2 is 0.

If we now apply M_3 repeatedly, where the starting vector is v_0, we see that

$$v_1 := M_3 \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$$

$$v_2 := M_3 \cdot \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}$$

$$v_3 := M_3 \cdot \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$v_4 := M_3 \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$v_5 := M_3 \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$v_6 := M_3 \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$$

$$v_7 := M_3 \cdot \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$

$$v_8 = M_3 \cdot \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}.$$

Thus $v_8 = v_0$, so the cycle consists of 8 elements. Namely $v_0, v_1, .., v_7$.

Another cycle with 8 elements is given by

$$v'_i := 2v_i.$$

This gives us the list of vectors

$$v'_0 = \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix}, \quad v'_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \quad v'_2 = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}, \quad v'_3 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}$$

$$v'_4 = \begin{bmatrix} 2 \\ 2 \\ 2 \end{bmatrix}, \quad v'_5 = \begin{bmatrix} 2 \\ 0 \\ 2 \end{bmatrix}, \quad v'_6 = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \quad v'_7 = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}.$$

Let us now choose

$$v''_0 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

This also gives us a cycle consisting of 8 elements. After applying M_3 we see that the cycle consists of the elements

$$v''_0 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad v''_1 = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \quad v''_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \quad v''_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$v''_4 = \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix}, \quad v''_5 = \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}, \quad v''_6 = \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix}, \quad v''_7 = \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}.$$

Since there are $3^3 = 27$ different vectors and we already have $3 \cdot 8 = 24$

of them in any of the three cycles there are only 3 vectors left. But the first component in our vector stays fixed under the transformation.

Fix the first component. Then there are $3^2 = 9$ vectors we can get from it. This mean that we must have one vector with the first component equals 0, one with the first component equals 1 and one with the first component equals 2 left. These vectors are

$$v := \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad u := \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, \quad w := \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}.$$

Hence, we must have that $M_3 v = v$, $M_3 u = u$ and $M_3 w = w$. That is cycles with only 1 element. $\square$

An interesting property this matrix has is that it is invertible. This can be seen by computing the determinant and using that the Vandermonde matrix is invertible. In the next section we will determine the inverse of M_p.

3 Inverse of φ_p

Our problem is to find a matrix

$$M_p^{-1} = \begin{bmatrix} m'_{11} & m'_{12} & m'_{13} & \cdots & m'_{1(p-2)} & m'_{1(p-1)} \\ m'_{21} & m'_{22} & m'_{23} & \cdots & m'_{2(p-2)} & m'_{2(p-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ m'_{(p-2)1} & m'_{(p-2)2} & m'_{(p-2)3} & \cdots & m'_{(p-2)(p-2)} & m'_{(p-2)(p-1)} \\ m'_{(p-1)1} & m'_{(p-1)2} & m'_{(p-1)3} & \cdots & m'_{(p-1)(p-2)} & m'_{(p-1)(p-1)} \end{bmatrix}$$

such that $M_p M_p^{-1} = M_p^{-1} M_p = I_p$ (where I_p denotes the identity matrix of size p).

We will begin by stating an existence lemma. This lemma ensures us that M_p is invertible.

Lemma 1. *Assume $a_1 \neq 0$ and let*

$$M_p = \left[\begin{array}{c:ccc} a_1 & 0 & \cdots & 0 \\ a_2 & & & \\ \vdots & & & V_p \\ a_n & & & \end{array}\right]$$

where V_p is invertible, then M_p is invertible.

Proof. Since $a_1 \neq 0$ we can use that row to eliminate $a_2, .., a_n$.

$$\left[\begin{array}{c:ccc} a_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & V_p \\ 0 & & & \end{array}\right].$$

Now, the first row is clearly not a linear combination of any of the other rows, since V_p is invertible, the conclusion follows. □

3.1 Defining Vandermonde matrix and investigate some properties

A well-known type of matrix is the Vandermonde matrix. There are well-known facts about these types of matrices. One is that there exist a formula for the inverse matrix.

Definition 2. *A Vandermonde matrix of order n is a square matrix of the form*

$$V_n = \begin{bmatrix} x_1 & x_1^2 & \cdots & x_1^n \\ x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^2 & \cdots & x_n^n \end{bmatrix}.$$

We define our Vandermonde matrix V_p to be the $(p-1) \times (p-1)$

matrix defined by

$$V_p = \begin{bmatrix} 1 & 1^2 & 1^3 & \cdots & 1^{p-2} & 1^{p-1} \\ 2 & 2^2 & 2^3 & \cdots & 2^{p-2} & 2^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (p-1) & (p-1)^2 & (p-1)^3 & \cdots & (p-1)^{p-2} & (p-1)^{p-1} \end{bmatrix}.$$

Our goal is to compute the inverse of V_p. We are now ready to present the general formula for the inverse of a Vandermonde matrix.

Theorem 3. *Let V_n be a Vandermonde matrix of order n. Then its inverse $V_n^{-1} = [v]_n$ can be specified as*

$$v_{ji} = \begin{cases} (-1)^{j-1} \left(\dfrac{\displaystyle\sum_{\substack{1 \le m_1 < \ldots < m_{n-j} \le n \\ m_1, \ldots, m_{n-j} \ne i}} x_{m_1} \cdots x_{m_{n-j}}}{x_i \displaystyle\prod_{\substack{1 \le m \le n \\ m \ne i}} (x_m - x_i)} \right) & : 1 \le j < n \\ \dfrac{1}{x_i \displaystyle\prod_{\substack{1 \le m \le n \\ m \ne i}} (x_i - x_m)} & : j = n \end{cases}$$

Proof: Result can be found in [1]. □

In our case $x_m = m$ and $n = p - 1$. We will see that for V_p, we will arrive at a simpler expression than the form of Theorem 3. To do so, we will start by proving the following useful lemma:

Lemma 2.
Let p be a prime number, then

$$i \prod_{\substack{1 \le m \le p-1 \\ m \ne i}} (m - i) = 1 \qquad \forall i : 1 \le i \le p - 1. \tag{1}$$

Proof: First, notice that $p = 0 \in \mathbb{Z}_p$ and therefore $1p = 2p = 3p = ... = (p-1)p = 0$. This implies that $p - i = ip - i$. In the first step below we will use Wilson's Theorem. Since p is a prime, we have $(p-1)! = (p-1)(p-2)! = p-1$. Hence $(p-2)! = 1$.

$1 = (p-2)! = (p-2)(p-3)\cdots(p-i)\cdots 1 = (p-2)(p-3)\cdots(ip - i)\cdots 1 = i\Big[(p-2)(p-3)\cdots(p-(i+1))(p-1)(p-(i-1))\cdots 1\Big] = i\Big[(-2)(-3)\cdots(-(i+1))(-(i-1))\cdots 1\Big] = i\Big[(-2)(-3)\cdots((p-1)-i)(1-i)\cdots((i+2)-i)((i+1)-i)\Big] = i\Big[(1-i)(2-i)\cdots((i-1)-i)((i+1)-i)((i+2)-i)\cdots((p-1)-i)\Big]$

$$= i \prod_{\substack{1 \le m \le p-1 \\ m \ne i}} (m - i).$$

□

A corollary is the following

Corollary 1.

$$\frac{1}{i \displaystyle\prod_{\substack{1 \le m \le p-1 \\ m \ne i}} (i - m)} = p - 1 \qquad \forall i : 1 \le i \le p-1.$$

Proof: Consider

$$\prod_{\substack{1 \le m \le p-1 \\ m \ne i}} (i - m)\,.$$

Since $m \ne i$, there are $p - 1 - 1 = p - 2$ different m's. This is an odd number. This gives us

$$(-1)^{p-2} \prod_{\substack{1 \le m \le p-1 \\ m \ne i}} (m - i) = - \prod_{\substack{1 \le m \le p-1 \\ m \ne i}} (m - i)\,.$$

By the previous lemma we have

$$i \prod_{\substack{1 \leq m \leq p-1 \\ m \neq i}} (m-i) = 1.$$

So

$$\frac{1}{i \displaystyle\prod_{\substack{1 \leq m \leq p-1 \\ m \neq i}} (i-m)} = \frac{1}{-1} = \frac{1}{p-1}.$$

But $(p-1)^{-1} = p-1$. So

$$\frac{1}{i \displaystyle\prod_{\substack{1 \leq m \leq p-1 \\ m \neq i}} (i-m)} = p-1.$$

$\square$

Hence, we are left with

$$v_{ji} = \begin{cases} (-1)^{j-1} \left(\dfrac{\displaystyle\sum_{\substack{1 \leq m_1 < \ldots < m_{(p-1)-j} \leq p-1 \\ m_1, \ldots, m_{(p-1)-j} \neq i}} m_1 \cdots m_{(p-1)-j}}{1} \right) & : 1 \leq j < p-1 \\ p-1 & : j = p-1 \end{cases}$$

The next step is to simplify the sum

$$\sum_{\substack{1 \leq m_1 < \ldots < m_{(p-1)-j} \leq p-1 \\ m_1, \ldots, m_{(p-1)-j} \neq i}} m_1 \cdots m_{(p-1)-j}$$

in the inverse formula.

Lemma 3.
Let p be a prime number, then

$$\frac{x^{p-1}-1}{x-i} = x^{p-2}+i^{-(p-2)}x^{p-3}+\cdots+i^{-2}x^1+i^{-1}x^0 \text{ for all } i \in \mathbb{Z}_p. \quad (2)$$

Proof: We have that

$$\frac{x^{p-1}-1}{x-i} = x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1x + a_0.$$

Multiplying both sides by $x - i$ gives us

$$x^{p-1}-1 = x^{p-1}+a_{p-3}x^{p-2}+\cdots+a_1x^2+a_0x-ix^{p-2}-ia_{p-3}x^{p-3}+\cdots-ia_1x-ia_0.$$

If this equality should hold, we need to have the coefficients of x^{p-1} to be equal each other, the coefficients of x^{p-2} to be equal each other all the way down to x^0. This leaves us with a system of equation to solve

$$\begin{cases} -a_0 = -1 \Leftrightarrow a_0 = i^{-1} \\ a_0 - ia_1 = 0 \Leftrightarrow a_1 = i^{-2} \\ a_1 - ia_2 = 0 \Leftrightarrow a_2 = i^{-3} \\ \qquad\qquad \vdots \\ a_{p-4} - ia_{p-3} = 0 \Leftrightarrow a_{p-3} = i^{-(p-2)}. \end{cases}$$

a_{p-3} should also satisfy the equation $(a_{p-3} - i)x^{p-2} = 0x^{p-2}$. But it is true since $a_{p-3} - i = 0 \Leftrightarrow a_{p-3} = i$. But $a_{p-3} = i^{-(p-2)}$. So $i^{-(p-2)} = i$ since, if we multiply both sides by i^{-1}, we get $i^{-(p-1)} = 1$. We can now conclude that

$$\frac{x^{p-1}-1}{x-i} = x^{p-2} + i^{-(p-2)}x^{p-3} + \cdots + i^{-2}x + i^{-1}.$$

$\square$

The previous result can now be used to prove that

$$\sum_{\substack{1 \leq m_1 < \ldots < m_{(p-1)-j} \leq p-1 \\ m_1, \ldots, m_{(p-1)-j} \neq i}} m_1 \cdots m_{(p-1)-j}$$

has the following form.

Lemma 4.
Let p be a prime number. Then

$$\sum_{\substack{1 \leq m_1 < \ldots < m_{(p-1)-j} \leq (p-1) \\ m_1, \ldots, m_{(p-1)-j} \neq i}} m_1 \cdots m_{(p-1)-j} = (-1)^j i^{-j}.$$

Proof: We have that

$$\frac{x^{p-1}-1}{x-i} = (x-1)(x-2)\cdots(x-(i-1))(x-(i+1))\cdots(x-(p-1)).$$

It equals to $x^{p-2} + i^{-(p-2)}x^{p-3} + \cdots + i^{-2}x + i^{-1}$ by Lemma 3. Now

$$\begin{aligned} &x^{p-2} + i^{-(p-2)}x^{p-3} + \cdots + i^{-2}x + i^{-1} \\ &= (x-1)(x-2)\cdots(x-(i-1))(x-(i+1))\cdots(x-(p-1)). \end{aligned}$$

If we now carry out the multiplication of the right hand side we get $x^{p-2} - (1+2+3+\cdots+(p-1))x^{p-3} + \cdots + (1 \cdot 2 \cdots (p-1))$.

So we now have

$$\begin{aligned} &x^{p-2} + i^{-(p-2)}x^{p-3} + \cdots + i^{-2}x + i^{-1} = \\ &x^{p-2} - (1+2+\cdots+(i-1)+(i+1)+\cdots+p-1)x^{p-3} \\ &+\cdots - 1 \cdot 2 \cdots (i-1)(i+1)\cdots(p-1). \end{aligned}$$

This tells us exactly that $i^{-(p-2)} = -(1+2+3\cdots+(p-1))$,.., $i^{-2} = 1\cdots(i-1)(i+1)\cdots(p-2)+...+2\cdots(i-1)(i+1)\cdots(p-1)$

and
$i^{-1} = -1 \cdots (i-1)(i+1) \cdots (p-1)$. This sum is alternating between $-$ and $+$. It is $-$ when j is odd and $+$ when j is even. Hence,

$$\sum_{\substack{1 \leq m_1 < \ldots < m_{(p-1)-j} \leq p-1 \\ m_1, \ldots, m_{(p-1)-j} \neq i}} m_1 \cdots m_{(p-1)-j} = (-1)^j i^{-j}.$$

□

So we have now reduced the formula

$$v_{ji} = (-1)^{j+1}(-1)^j i^{-j} = -i^{-j}.$$

This is the inverse of V_p.

Theorem 4.

Let

$$V_p = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 2^1 & 2^2 & \cdots & 2^{p-1} \\ 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \cdots & \vdots \\ (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{bmatrix}$$

then

$$V_p^{-1} = \begin{bmatrix} -1^{-1} & -2^{-1} & \cdots & -(p-1)^{-1} \\ -1^{-2} & -2^{-2} & \cdots & -(p-1)^{-2} \\ \vdots & \vdots & \cdots & \vdots \\ -1^{-(p-2)} & -2^{-(p-2)} & \cdots & -(p-1)^{-(p-2)} \\ -1^{-(p-1)} & -2^{-(p-1)} & \cdots & -(p-1)^{-(p-1)} \end{bmatrix}.$$

Proof: Follows from the formula we just derived. So $v_{ji} = -i^{-j}$. □

Here is an alternative proof of the inverse of the Vandermonde matrix V_p:

Proof: We are going to show that

$$V_p V_p^{-1} = I_{p-1}.$$

To see that the diagonal consists of 1's; Pick an arbitrary row, call it i, from V_p and pick column i of V_{p-1}^{-1}. Then we will have

$$-\sum_{k=0}^{p-1} i^{k-k} = -\sum_{k=0}^{p-1} 1 = -(p-1) = 1.$$

Consider now row i, column j (where $i \neq j$). This gives us

$$i^1 j^{-1} + i^2 j^{-2} + ... + i^{p-1} j^{-(p-1)} = (i^1 j^{-1})^1 + (i^1 j^{-1})^2 + ... + (i^1 j^{-1})^{p-1}.$$

Since the inverse is unique, and $i \neq j$, $i^1 j^{-1} \neq 1$. Hence, we can apply Lemma 3, which shows that the sum equals 0. So $V_p V_p^{-1} = I_{p-1}$. $\square$

We are soon ready to present the inverse to M_p. But before we do that, we will present another lemma which will come in handy.

Lemma 5. *If* $p-1 \not| k$ *then* $1^k + 2^k + \cdots + (p-1)^k = 0$.

Proof: Proof is given in [2]. $\square$

Theorem 5.

$$M_p^{-1} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1^{-1} & -2^{-1} & \cdots & -(p-1)^{-1} \\ 0 & -1^{-2} & -2^{-2} & \cdots & -(p-1)^{-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & -1^{-(p-2)} & -2^{-(p-2)} & \cdots & -(p-1)^{-(p-2)} \\ p-1 & -1^{-(p-1)} & -2^{-(p-1)} & \cdots & -(p-1)^{-(p-1)} \end{bmatrix}.$$

Proof: Let

$$N_p^{-1} = \begin{bmatrix} m_{11} & m_{12} & m_{13} & \cdots & m_{1(p-1)} \\ m_{21} & -1^{-1} & -2^{-1} & \cdots & -(p-1)^{-1} \\ m_{31} & -1^{-2} & -2^{-2} & \cdots & -(p-1)^{-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ m_{(p-2)1} & -1^{-(p-2)} & -2^{-(p-2)} & \cdots & -(p-1)^{-(p-1)} \\ m_{(p-1)1} & -1^{-(p-1)} & -2^{-(p-1)} & \cdots & -(p-1)^{-(p-1)} \end{bmatrix}.$$

Hence, we have to find the first row and first column. If all the elements in the first row, except the first one, should equal 0 then we must have $m_{12} = m_{13} = ... = m_{1(p-1)} = 0$. This can be seen since the first row of M_p is $(1\ 0\ 0\ \cdots\ 0)$. Multiplying this row with any of $p-2$ last column gives us $m_{1j} + 0 + 0... + 0 = 0 \Leftrightarrow m_{1j} = 0$.

Multiplying all the rows of M_p with the first column of N_p^{-1} gives us

$$\begin{cases} m_{11} = 1 \\ m_{11} + 1^1 m_{21} + ... + 1^{p-1} m_{(p-1)1} = 0 \\ m_{11} + 2^1 m_{21} + ... + 2^{p-1} m_{(p-1)1} = 0 \\ \qquad\qquad\qquad \vdots \\ m_{11} + (p-1)^1 m_{21} + ... + (p-1)^{p-1} m_{(p-1)1} = 0. \end{cases}$$

Since $m_{11} = 1$ and Vandermonde matrices are invertible, we have that

$$\begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} + V_p \begin{bmatrix} m_{21} \\ m_{31} \\ \vdots \\ m_{(p-1)1} \end{bmatrix} = \vec{0}$$

$$\Longleftrightarrow \begin{bmatrix} m_{21} \\ m_{31} \\ \vdots \\ m_{(p-1)1} \end{bmatrix} = V_p^{-1} \begin{bmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{bmatrix}.$$

Hence, we want to compute

$$\begin{bmatrix} -1^{-1} & -2^{-1} & \cdots & -(p-1)^{-1} \\ -1^{-2} & -2^{-2} & \cdots & -(p-1)^{-2} \\ \vdots & \vdots & \cdots & \vdots \\ -1^{-(p-2)} & -2^{-(p-2)} & \cdots & -(p-1)^{-(p-1)} \\ -1^{-(p-1)} & -2^{-(p-1)} & \cdots & -(p-1)^{-(p-1)} \end{bmatrix} \begin{bmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{bmatrix}.$$

Choose row k of V_p^{-1}, where k is not the last row, and multiply it with the vector. This gives us

$$1^{-k} + 2^{-k} + \cdots + (p-1)^{-k}.$$

Let $k' = -k$. Then we have

$$1^{k'} + 2^{k'} + \cdots + (p-1)^{k'}.$$

Since k is not the last row, we have that $k' < p-1$ and hence $p-1 \not| k'$ which means that the hypothesis in Lemma 5 is satisfied. This means that $m_{21} = m_{31} = \cdots = m_{(p-2)1} = 0$. For the last element we have

$$1^{-(p-1)}+2^{-(p-1)}+\cdots+(p-1)^{-(p-1)} = 1+1+1+\cdots+1 = (p-1)\cdot 1 = p-1.$$

Hence the last element is $p-1$ by Fermat's little theorem. We can now conclude the inverse is given by

$$M_p^{-1} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1^{-1} & -2^{-1} & \cdots & -(p-1)^{-1} \\ 0 & -1^{-2} & -2^{-2} & \cdots & -(p-1)^{-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & -1^{-(p-2)} & -2^{-(p-2)} & \cdots & -(p-1)^{-(p-2)} \\ p-1 & -1^{-(p-1)} & -2^{-(p-1)} & \cdots & -(p-1)^{-(p-1)} \end{bmatrix}.$$

□

We would like not to have inverses inside the inverse matrix, e.g elements such as -2^{-1} and $-3^{-(p-3)}$, so we will apply the following lemma.

Lemma 6. *If $0 \neq a \in \mathbb{Z}_p$ then $a^{p-i-1} = a^{-i}$.*

Proof: Let $a \in \mathbb{Z}_p$ where $a \neq 0$. We now have

$$\begin{aligned} a^{p-i-1} &= a^{-i} \Leftrightarrow \\ a^i \cdot a^{p-i-1} &= 1 \Leftrightarrow \\ a^{i+p-i-1} &= 1 \Leftrightarrow \\ a^{p-1} &= 1. \end{aligned} \tag{3}$$

where the last equality is true by Fermat's little theorem. Since all of the expressions are equivalent, we can conclude that $a^{p-i-1} = a^{-i}$.

□

Corollary 2.
Let p be a prime. The inverse to M_p is given by

$$M_p^{-1} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1^{p-2} & -2^{p-2} & \cdots & -(p-1)^{p-2} \\ 0 & -1^{p-3} & -2^{p-3} & \cdots & -(p-1)^{p-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & -1^{1} & -2^{1} & \cdots & -(p-1)^{1} \\ p-1 & p-1 & p-1 & \cdots & p-1 \end{bmatrix}.$$

□

Here is an example how the inverse can be used to go backward in the cycles.

Exempel 2.

We will now go back to Example 1. Then we have

$$M_3^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1^1 & -2^1 \\ 2 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{bmatrix}$$

Now, consider the element v_7 from Example 1. If we now do the same kind of iteration as we did in the previous example, we see that

$$M_3^{-1}\begin{bmatrix}1\\2\\1\end{bmatrix}=\begin{bmatrix}1\\2\\2\end{bmatrix}=v_6$$
$$M_3^{-1}\begin{bmatrix}1\\2\\2\end{bmatrix}=\begin{bmatrix}1\\0\\1\end{bmatrix}=v_5$$
$$M_3^{-1}\begin{bmatrix}1\\0\\1\end{bmatrix}=\begin{bmatrix}1\\1\\1\end{bmatrix}=v_4$$
$$M_3^{-1}\begin{bmatrix}1\\1\\1\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix}=v_3$$
$$M_3^{-1}\begin{bmatrix}1\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\2\end{bmatrix}=v_2$$
$$M_3^{-1}\begin{bmatrix}1\\0\\2\end{bmatrix}=\begin{bmatrix}1\\2\\0\end{bmatrix}=v_1$$
$$M_3^{-1}\begin{bmatrix}1\\2\\0\end{bmatrix}=\begin{bmatrix}1\\1\\0\end{bmatrix}=v_0.$$

This shows us that if we apply M_3^{-1} on the vectors, compare to Example 1, we have a rule that makes it possible to see which element is the previous element in a cycle. We end this example by applying M_3^{-1} on the remaining vectors.

Choose v'_7 from Example 1, then

$$
\begin{aligned}
M_3^{-1}v'_7 &= v'_6\\
M_3^{-1}v'_6 &= v'_5\\
M_3^{-1}v'_5 &= v'_4\\
M_3^{-1}v'_4 &= v'_3\\
M_3^{-1}v'_3 &= v'_2\\
M_3^{-1}v'_2 &= v'_1\\
M_3^{-1}v'_1 &= v'_0.
\end{aligned}
$$

and we can also see, by doing the same computation for the third 8-cycle with starting vector v''_7, that

$$
\begin{aligned}
M_3^{-1}v''_7 &= v''_6\\
M_3^{-1}v''_6 &= v''_5\\
M_3^{-1}v''_5 &= v''_4\\
M_3^{-1}v''_4 &= v''_3\\
M_3^{-1}v''_3 &= v''_2\\
M_3^{-1}v''_2 &= v''_1\\
M_3^{-1}v''_1 &= v''_0.
\end{aligned}
$$

By applying M_3^{-1} to the vectors belonging to cycles with only 1 elements clearly gives us back the same vector. This is because

$$M_p^{-1}v = v \iff v = M_p^{-1}v.$$

4 Eigenvalues and Eigenvectors

Take a polynomial $f \in \mathcal{A}_p$, apply φ_p on f to get a new polynomial f_1; $\varphi_p(f) = f_1$. Do the same on f_1 to get $\varphi_p \circ \varphi_p(f) = \varphi_p(f_1) = f_2$. How many times do we have to apply φ_p before we end up at the same polynomial, f, again? To investigate this problem we will define what we mean by the order of φ_p.

Definition 3. *The* ***order*** *of* φ_p *is the least* i *such that*

$$\varphi_p^i = id \iff M_p^i = I_p.$$

We will now walk through an example where we find the order of M_3. This will show us that we could never have gotten any larger cycle than the 8-cycles we got in Example 1.

Example 3.

Consider M_3. Then

$$M_3^{(2)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix}$$

$$M_3^{(3)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix}$$

$$M_3^{(4)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}$$

$$M_3^{(5)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 2 \\ 0 & 1 & 2 \end{bmatrix}$$

$$M_3^{(6)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 2 \\ 0 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 0 \end{bmatrix}$$

$$M_3^{(7)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{bmatrix}$$

$$M_3^{(8)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

By definition, the order is 8. $\square$

We will now prove that $\lambda = 1$ is always an eigenvalue.

Proposition 1. *Let p be a prime, then 1 is an eigenvalue to M_p.*

Proof: Let $\lambda \in \mathbb{Z}_p$. Now;

$$|M - \lambda I| = \begin{vmatrix} 1-\lambda & 0 & 0 & \cdots & 0 \\ 1 & 1-\lambda & 1 & \cdots & 1 \\ 1 & 2^1 & 2^2-\lambda & \cdots & 2^{p-1} \\ 1 & 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1}-\lambda \end{vmatrix}$$

$$= (1-\lambda) \begin{vmatrix} 1-\lambda & 1 & \cdots & 1 \\ 2^1 & 2^2-\lambda & \cdots & 2^{p-1} \\ 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \cdots & \vdots \\ (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1}-\lambda \end{vmatrix} = 0.$$

From the first factor we find that $1 - \lambda = 0 \iff \lambda = 1$. Hence 1 is always an eigenvalue. $\square$

That 1 is an eigenvalue is the same as saying that if we apply M_p to a vector we fix that vector. Here is an example where we use eigenvectors to classify some of the cycles in M_5.

Example 4.
Consider

$$M_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 & 1 \\ 1 & 4 & 1 & 4 & 1 \end{bmatrix}.$$

We want to find vectors v satisfying

$$M_5 v = \lambda v \iff M_5 v - \lambda v = 0 \iff (M_5 - \lambda I_5)v = 0.$$

Let

$$M_5^*(\lambda) = M_5 - \lambda I_5.$$

To find the eigenvalues we will compute the characteristic polynomial

$$|M_5^*(\lambda)| = (\lambda + 1)(\lambda + 4)(\lambda^3 + \lambda^2 + 4\lambda + 3) = 0.$$

The solutions to this equation is given by $\lambda = 4$ and $\lambda = 1$. We now want to solve

$$M_5^*(4)v = 0.$$

Reduction of $M_5^*(4)$ gives us a parametrization

$$\begin{aligned} x_1 &= 0 \\ x_2 &= 4t \\ x_3 &= 4t \\ x_4 &= 2t \\ x_5 &:= t. \end{aligned}$$

Thus, the eigenspace corresponding to the eigenvalue 4 is spanned by

$$v = \begin{bmatrix} 0 \\ 4 \\ 4 \\ 2 \\ 1 \end{bmatrix}.$$

v belongs to a cycle with length 2, since $4 = 2^2$ and

$$M_5 M_5 v = M_5 2^2 v = 2^2 M_5 v = 2^2 \cdot 2^2 v = 2^4 v = v.$$

Where the last equality is due to Fermat's little theorem.

We now want to find the eigenvectors for $\lambda = 1$,

$$M_5^*(1)v = 0.$$

By reducing $M_5^*(1)$ we find the parametrization

$$\begin{aligned} x_1' &= 3s \\ x_2' &= 4s \\ x_3' &= s \\ x_4' &= 0 \\ x_5' &:= s. \end{aligned}$$

And from this we find that the eigenspace corresponding to the eigenvalue 1 is spanned by

$$v' = \begin{bmatrix} 3 \\ 4 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Since this vector, v', corresponds to the eigenvalue 1, it satisfies

$$M_5 v = v.$$

This example shows us that, for example, the polynomial $3 + 4x + x^2 + x^4$ stays fixed under φ_5. $\square$

Due to that 1 is an eigenvalue; a problem we are interested investigating is to find the eigenspace

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2^1 & 2^2 & \cdots & 2^{p-1} \\ 1 & 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}.$$

Here is a theorem which tells us how a_1 relates to a_{p-1}.

Theorem 6. *If*

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2^1 & 2^2 & \cdots & 2^{p-1} \\ 1 & 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}$$

then $a_1 = -a_{p-1}$.

Proof: Consider

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2^1 & 2^2 & \cdots & 2^{p-1} \\ 1 & 3^1 & 3^2 & \cdots & 3^{p-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}.$$

By multiplying the matrix with the vector on the left hand side we find that

$$\begin{aligned} a_0 &= a_0 \\ a_0 + a_1 + ... + a_{p-1} &= a_1 \\ 2^0 a_0 + 2^1 a_1 + ... + 2^{p-1} a_{p-1} &= a_2 \\ &\vdots \\ (p-1)^0 a_0 + (p-1)^1 a_1 + ... + (p-1)^{p-1} a_{p-1} &= a_{p-1}. \end{aligned} \tag{4}$$

Let $a_0 = 1$. Adding all the rows gives us an expression of the form $(*) \quad (1 + 1... + 1) + (1^1 + 2^1 + ... + (p-1)^1)a_1 + (1^2 + 2^2 + ... + (p-1)^2)a_2 + ... + (1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1})a_{p-1} = a_1 + a_2 + ... + a_{p-1}$. But from the second equation we have that

$$a_1 + a_2 + ... + a_{p-1} = a_1 - 1.$$

So we can substitute that expression in to the right hand side of $(*)$ $(1 + 1... + 1) + (1^1 + 2^1 + ... + (p-1)^1)a_1 + (1^2 + 2^2 + ... + (p-1)^2)a_2 + ... + (1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1})a_{p-1} = a_1 - 1$.

We can also apply Lemma 5 on all the coefficients for $a_1, a_2, .., a_{p-2}$ on the left hand side, since no of them are divisible by $p-1$. Hence they must be 0. So we are now left with $(p-1) + (p-1)a_{p-1} = -1 - a_{p-1} = a_1 - 1 \iff -a_{p-1} = a_1$. Where we have used Fermat's little Theorem for a_{p-1}. $\square$

5 Experiments

Down below are three tables. The first one shows the order of the matrix for a particular p and the factorization of the characteristic polynomial. The second shows the degree of every factor of the characteristic polynomial for M_p. The last table present the corresponding eigenspace for the eigenvalue 1.

p	Order	Characteristic polynomial
2	2	$(x+1)^2$
3	8	$2(x+2)(x^2+x+2)$
5	124	$4(x+1)(x+4)(x^3+x^2+4x+3)$
7	1368	$6(5+x)(6+x)(1+3x+x^2)(4+2x+x^2+x^3)$
11	X	$10(10+x)(1+x+x^2)(7+x+x^3)(8+4x+7x^4+x^5)$

Table 1

p	Degree of factors
13	$1, 12$
17	$1, 1, 6, 9$
19	$1, 1, 3, 3, 5, 6$
23	$1, 3, 7, 12$
29	$1, 1, 2, 12, 13$
31	$1, 2, 3, 3, 6, 6, 7$
37	$1, 1, 1, 2, 13, 19$
41	$1, 1, 2, 4, 9, 10, 14$
43	$1, 1, 4, 37$
47	$1, 1, 2, 5, 6, 6, 26$
53	$1, 3, 9, 17, 23$
59	$1, 1, 3, 9, 13, 32$
61	$1, 1, 10, 15, 34$
67	$1, 1, 2, 3, 7, 23, 30$
71	$1, 1, 2, 3, 3, 6, 7, 12, 36$
73	$1, 2, 7, 63$
79	$1, 1, 1, 1, 1, 3, 7, 14, 50$
83	$1, 2, 6, 11, 18, 21, 24$
89	$1, 1, 16, 27, 44$
97	$1, 3, 14, 34, 45$
101	$1, 5, 9, 9, 23, 54$
103	$1, 1, 1, 4, 14, 23, 28, 31$
107	$1, 1, 2, 5, 30, 68$
109	$1, 1, 107$
113	$1, 1, 3, 4, 5, 99$
127	$1, 1, 3, 4, 9, 19, 35, 55$

Table 2

p	Eigenspace corresponding to 1 generated by
2	$(0, 1)$
3	$(2, 2, 1)$
5	$(3, 4, 1, 0, 1)$
7	$(3, 6, 3, 6, 0, 1, 1)$
11	$(10, 10, 9, 2, 3, 8, 7, 6, 3, 6, 1)$

Table 3

By inspecting Table 1, we see that the order of M_p is given by the sequence $2, 8, 124, 1368, ...$ I haven't been able to find any pattern in this sequence. I have also entered the sequence into the online encyclopedia of integer sequences [3], but with no positive result.

6 Appendix/Code

Representation of the matrix

```
m[p_] := Mod[Insert[Map[Prepend[#, 1] &,
Table[x^y, {x, p - 1}, {y, p - 1}]],
    Prepend[0^Range[p - 1], 1], 1], p]
```

Computing the order of M_p

```
ComputeOrder[p_] := Block[
m[p_] := Mod[
   Insert[Map[Prepend[#, 1] &, Table[x^y, {x, p - 1},
    {y, p - 1}]], Prepend[0^Range[p - 1], 1], 1], p]
TMatrix = Mod[MatrixPower[m[11], 1], 11];
mp = m[p];
Idp = IdentityMatrix[p];
j = 1;
While[TMatrix != Idp, TMatrix = Mod[TMatrix.mp, p];
   Print[j]; j++]
   ]
```

Computing the order of M_{11}

```
m[p_] := Mod[
   Insert[Map[Prepend[#, 1] &, Table[x^y, {x, p - 1},
    {y, p - 1}]], Prepend[0^Range[p - 1], 1], 1], p]
TMatrix = Mod[MatrixPower[m[11], 1], 11];
m11 = m[11];
Id11 = IdentityMatrix[11];
j = 1;
While[TMatrix != Id11, TMatrix = Mod[TMatrix.m11, 11];
   Print[j]; j++]
```

Computing eigenvalues to M_p

```
ModCharacteristicPolynomial[p_] :=
```

```
Factor[PolynomialMod[CharacteristicPolynomial[m[p],
  \[Lambda]], p], Modulus -> p]
```

Computes eigenvectors, where eigenvalue equals 1*, to* M_p

References

[1] Donald Ervin Knuth, The Art of Computer Programming, *ADDISON–WESLEY*, (1968).

[2] Kieren MacMillan and Jonathan Sondow, "Proofs of Power Sum and Binomial Coefficient Congruences Via Pascal's Identity" , *Transactions of the American Math. Society*, to appear, *arXiv preprint at* `arXiv:1011.0076` (2010).

[3] https://oeis.org/