SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Cycles of certain maps from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_p[x]$

av

Björn Carlsten

2021 - No K8

Cycles of certain maps from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_p[x]$

Björn Carlsten

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Samuel Lundqvist

2021

Abstract

In this essay we investigate cycles of a certain map between polynomials in one variable over finite fields using methods from experimental mathematics. We show that a certain cycle of length 4 exists for all fields of prime characteristic, and that all possible cycles must be of even length. Based on previous results on cycles of length 2, we describe a theory of critical equations that serves as the basis for an automated search program to find more examples of such cycles. The results from that automated search are categorized into a taxonomic hierarchy of cycles of length 2. Finally, we explore the necessary conditions that must hold for cycles of length 2 to occur and propose hypotheses regarding these conditions.

Acknowledgements

I would like to thank my supervisor Samuel Lundqvist for his great patience and helpful guidance over the course of this project. I would also like to thank Tomas Carlsten for his assistance in proof-reading the text.

Contents

1 Introduction

We begin by giving a brief description of experimental mathematics, and then introduce the mathematical topic under investigation.

1.1 Experimental Mathematics

Mathematics as it is presented in journal articles and textbooks follows a familiar practice. Definitions are formulated, from which theorems are proved. What is almost always omitted from this practice are the intuitions and exploratory calculations that lead the mathematician to make guesses that eventually turn into the theorems of the final text. While the Definition-Theorem-Proof model of mathematical presentation is elegant and compact, it gives a false impression of the actual mathematical work that produced the published results. In this section, we will describe an alternative philosophy of mathematical presentation and research that aims to give a more accurate description of the mathematician's process.

Experimental Mathematics is a methodology of conducting mathematical research involving heavy use of computation. Suppose we are interested in investigating a mathematical object or structure. The experimental mathematician begins her inquiry by generating a large number of examples by computation, either by hand or with digital aid. From this wealth of examples, the experimental mathematician searches for patterns and peculiarities. The results of this search motivate the formulation of hypotheses regarding the properties of the mathematical object under consideration. Further computation serves to test these hypotheses, which might yield conclusive falsification if the computation reveals counter-examples. If a hypothesis withstands this computational scrutiny, perhaps a true pattern has been detected, and the experimental mathematician would then proceed to attempt a formal proof.

This process has many similarities to the scientific method. Natural science is empirical and employs inductive reasoning (not to be confused with mathematical induction). The natural scientist makes observations of some phenomena under investigation. These observations lead the scientist to formulate hypotheses, which are tested against experimental data. In modern science, statistical analysis is often employed, so as to more rigourously determine the likelihood that a hypothesis is true, given a set of data. Up to this point, the methodologies of the natural scientist and the experimental mathematician are exactly the same, the only difference being the subject matter; where the natural scientist observes phenomena in nature, the ex-

perimental mathematician observes the behaviour of a mathematical object. The similarities end when the mathematician attempts a formal deductive proof, a method that is unavailable to the natural scientist.

In this essay we explore the behaviour of a mapping between polynomials in one variable over finite fields. In the spirit of experimental mathematics, we approach this problem as a scientist would. Accordingly, the essay is structured as a scientific paper, with methods and results sections. The results then serve as a springboard to further formal analysis with traditional mathematical tools.

1.2 Cycles of Certain Maps from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_p[x]$

Definition 1. We define a map $\Psi : \mathbb{Z}_p[x] \mapsto \mathbb{Z}_p[x]$, such that

$$\Psi : f \mapsto \sum_{a \in Z(f)} x^a$$

where $Z(f)$ is the set $\{a \in \mathbb{Z}_p | f(a) = 0\}$.

This map takes the zero-set of the polynomial equation $f = 0$ over the integers modulo p, and maps it to the polynomial $\Psi(f)$ where the exponents are taken from the zero-set of the previous polynomial.

Remark 1. Since we are working over $\mathbb{Z}_p$, a in $a \in Z(f)$ is treated as a residue class of a modulo p. However, in x^a, a is treated as the integer $0 \leq a < p$ belonging to this residue class. The notation in Definition 1 is therefore ambiguous, but is adopted due to convenience.

Remark 2. The map Ψ can take as its argument any polynomial over $\mathbb{Z}_p$. However, Ψ invariably maps to polynomials where all coefficients are equal to either 1 or 0. Therefore, we only consider polynomials where the coefficients are equal to either 1 or 0.

Remark 3. Consider Fermat's little theorem

$$a^{p-1} = 1$$

where $a \in \mathbb{Z}_p$, and is not equal to zero. Multiplying by a, we obtain

$$a^p = a.$$

Since polynomial functions in $\mathbb{Z}_p[x]$ only take values of x from $\mathbb{Z}_p$, any term with an exponent greater than $p-1$ can be reduced to a smaller exponent, as per Fermat's little theorem above. Therefore, we only consider polynomials of degree at most $p - 1$.

Definition 2. Let Ω_p be the set of all polynomials in $\mathbb{Z}_p[x]$ with coefficients equal to either 0 or 1, with degree at most $p-1$.

With these restrictions on f established, we turn our attention to the special case of Ψ that is this essay's main object of study.

Definition 3. We define a map $\Phi : \Omega_p \mapsto \Omega_p$, such that

$$\Phi : f \mapsto \sum_{a \in Z(f)} x^a$$

where $Z(f)$ is the set $\{a \in \mathbb{Z}_p | f(a) = 0\}$.

Theorem 1. The size of Ω_p for a given prime number p is 2^p.

Proof. Consider the general case of a polynomial f in Ω_p,

$$f(x) = \underbrace{a_0x^0 + a_1x^1 + \ldots + a_{p-1}x^{p-1}}_{p \text{ terms}}$$

where a_n is equal to either 0 or 1. Therefore, for every term, there are two possibilities. Since there are p terms, there are 2^p possible polynomials in Ω_p. $\square$

Let's see how Φ works with an example.

Example 1. Let $p = 7$, and

$$f(x) = 1 + x^3 + x^5 + x^6.$$

Now we want to find for which $x \in \mathbb{Z}_7$, we have $f(x) = 0$. Since $f(2) = 0$ and $f(6) = 0$, the zero-set of f is $Z(f) = \{2, 6\}$. This zero-set is mapped to a new polynomial

$$\Phi(f) = x^2 + x^6.$$

For this new polynomial, $x = 0$ is the only zero, so when we apply Φ again, we have

$$\Phi^2(f) = x^0 = 1.$$

Now, $\Phi^2(f) = 1 = 0$ has no solutions, so its zero-set is empty. Then, applying Φ again,

$$\Phi^3(f) = 0.$$

Note now that $\Phi^3(f)$ is always equal to zero; therefore, its zero-set contains every element of $\mathbb{Z}_7$, so $Z(\Phi^3(f)) = \{0, 1, 2, 3, 4, 5, 6\}$. This zero-set maps to

$$\Phi^4(f) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6.$$

For $\Phi^4(f) = 0$, only $x = 1$ is a solution, which gives us

$$\Phi^5(f) = x.$$

Here, $\Phi^5(f) = 0$ only has $x = 0$ as a solution. But note that $x = 0$ was also the only solution to $\Phi(f) = 0$, so $\Phi^6(f) = \Phi^2(f)$. Therefore, continuing to apply Φ will only repeat the cycle

$$x \mapsto 1 \mapsto 0 \mapsto 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \mapsto x \mapsto \dots$$

Let's look at another example, and see if any interesting patterns emerge.

Example 2. Let $p = 11$, and

$$f(x) = 1 + x^2 + x^6 + x^7 + x^8 + x^{10}.$$

Iterating Φ as in the previous example, we have

$$1 + x^2 + x^6 + x^7 + x^8 + x^{10} \mapsto x^6 + x^9 \mapsto 1 + x^{10} \mapsto$$

$$0 \mapsto 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} \mapsto 1 \mapsto 0 \dots$$

2 A Cycle of Polynomials For All p

Note that in Example 2, we ended up in a similar cycle consisting of four polynomials, as in Example 1. We can represent this cycle as a directed graph (See Figure 1).

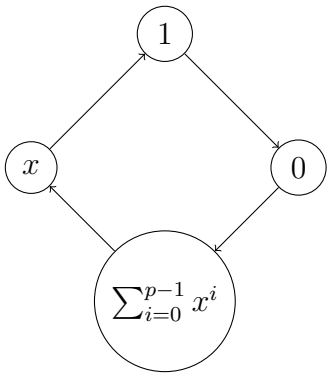

Figure 1: A cycle of polynomials mapped by Φ.

Now we will proceed to prove that these polynomials map to each other under Φ, as indicated by Figure 1.

Theorem 2. When the map Φ acts on polynomials over $\mathbb{Z}_p$, we have the mappings
i) $x \mapsto 1$
ii) $1 \mapsto 0$
iii) $0 \mapsto \sum_{i=0}^{p-1} x^i$
iv) $\sum_{i=0}^{p-1} x^i \mapsto x$.

Proof. Cases i, ii, iii, follow trivially from the definition of Φ. See Example 1 for generalizable special cases. It remains to prove case iv. The mapping in case iv corresponds to the equation $\sum_{i=0}^{p-1} x^i = 0$. Let

$$f(x) = \sum_{i=0}^{p-1} x^i = 1 + x + x^2 + ... + x^{p-1}.$$

We want to prove that the zero-set of f equals $\{1\}$. First, we show that $1 \in Z(f)$.

$$f(1) = \underbrace{1 + 1 + 1 + ... + 1}_{\text{p terms}} = 1 \cdot p = p = 0.$$

So, $1 \in Z(f)$. It remains to demonstrate that there exist no other solutions to $f(x) = 0$.

Consider solutions to the polynomial equation

$$(x-1) \cdot f(x) = (x-1) \sum_{i=0}^{p-1} x^i = 0 \tag{1}$$

where solutions to $f = 0$ are also solutions to 1.

Note that $x = 1$ is clearly a solution. Expanding, we get

$$(x-1)(1 + x + x^2 + ... + x^{p-1})$$

$$x + x^2 + x^3 + ... + x^p - 1 - x - x^2 - ... - x^{p-1}.$$

Note that every term cancels except 1 and x^p, so the polynomial from 1 is reduced to the following, which we call g:

$$g(x) = x^p - 1.$$

We have already established that $x = 1$ solves 1, and therefore also solves $g(x) = 0$. It remains to prove that it is the only solution. Now, evaluate $g(a)$, for some $a \in \mathbb{Z}_p$.

$$g(a) = a^p - 1.$$

By Fermat's little theorem,

$$g(a) = a - 1.$$

Clearly, only $a = 1$ solves $g(a) = 0$. Therefore, $x = 1$ is the only solution to the polynomial equation in 1. $\square$

According to Theorem 2, for all polynomials over $\mathbb{Z}_p$, we have a cycle of four polynomials. If Φ ever maps to any of the polynomials in Theorem 2, we will end up in this cycle.

3 Towards Other Types of Cycles

Given the finiteness of Ω_p, from Theorem 1, iterating Φ must inevitably lead to a cycle of some type. If a given polynomial in Ω_p is not eventually mapped by Φ to one of the polynomials from Theorem 2, there must exist at least one other type of cycle.

To explore the possibility of other types of cycles, we will introduce a more compact notation for polynomials mapped by Φ. In Examples 1 and 2, we represented Φ as a map between polynomials. Since Φ exclusively maps to polynomials with coefficients equal to 0 or 1, these polynomials can be represented as sets of exponents. For instance, we would have

$$1 + x^2 + x^6 + x^7 + x^8 + x^{10} = \{0, 2, 6, 7, 8, 10\}$$

$$1 + x^2 + x^6 + x^7 + x^8 + x^{10} \mapsto x^6 + x^9 = \{0, 2, 6, 7, 8, 10\} \mapsto \{6, 9\}.$$

Now if we look at the action of Φ from Example 1, we have

$$\{0, 3, 5, 6\} \mapsto \{2, 6\} \mapsto \{0\} \mapsto \{\} \mapsto \{0, 1, 2, 3, 4, 5, 6\} \mapsto \{1\} \mapsto \{0\} \ldots$$

Observe that we alternate between sets where $x = 0$ is a solution, and sets where $x = 0$ is not a solution. This observation motivates the formulation of a theorem that must hold for any hypothetical cycle.

Theorem 3. Iterating Φ, we will never end up in a cycle of odd length.

Proof. Let f be a polynomial over $\mathbb{Z}_p$. Either $x = 0$ is a solution to $f = 0$, or $x = 0$ is not solution to $f = 0$.

Suppose $x = 0$ is not a solution to $f = 0$. Now there are two possibilities. Either we have an empty or non-empty set of solutions to $f = 0$. If the zero-set is empty, we end up in the cycle of length 4 from Theorem 2. If we assume solutions exist, then f maps to g by Φ as follows.

$$\Phi(f) = g = a_1 x^1 + \cdots + a_{p-1} x^{p-1}$$

where not all a_i are zero.

Since g has no constant term, $x = 0$ clearly is a solution to $g = 0$. Observe that on the assumption that $f = 0$ is not solved by $x = 0$, f is mapped to a polynomial that is solved by $x = 0$ (or ends up in a 4-length cycle).

Suppose instead $x = 0$ is a solution to $f = 0$. Letting Φ act of f, we have

$$\Phi(f) = g = 1 + a_1 x^1 + \cdots + a_{p-1} x^{p-1}.$$

Now g has a constant term, so $x = 0$ is not a solution to $g = 0$. This time, assuming $x = 0$ is a solution, Φ maps to a polynomial where $x = 0$ is not a solution.

Therefore, under Φ, we alternate between polynomials where $x = 0$ is a solution and polynomials where $x = 0$ it is not a solution.

For a cycle to have odd length, it is necessary that there is some f, so that

$$Z(f) = Z(\Phi^k(f))$$

for some odd k.

But this is impossible, since odd iterations of Φ will map to a polynomial where $0 \in Z(\Phi^k(f))$ if $0 \notin Z(f)$, or $0 \notin Z(\Phi^k(f))$ if $0 \in Z(f)$. $\square$

According to Theorem 3, we need only consider hypothetical cycles of even length. This puts a useful constraint on the search space for any automated search algorithm we might want to run.

4 Cycles of Length 2

In this section, we will consider cycles of length 2. Other than the cycle of length 4 from Theorem 2, variations of which exist for all p, cycles of length 2 seem to be the most frequent, as indicated by preliminary results.

4.1 Preliminary Results

An automated computer search, courtesy of Samuel Lundqvist, turned up examples of polynomials, for certain prime numbers p, where $\Phi^2(f) = f$.

These are therefore instances where we have cycles of length 2. See Table 1 for a few examples of these cycles.

p	$\Phi(f)$	f
151	$\{0, 33, 119, 150\}$	$\{69, 150\}$
181	$\{0, 49, 133, 180\}$	$\{111, 180\}$
569	$\{0, 76, 277, 292, 493\}$	$\{160, 220\}$
1021	$\{0, 226, 250, 374, 384, 486, 535, 637, 647, 771, 795\}$	$\{381, 731\}$

Table 1: Examples of cycles of length 2.

Let's look more closely at a few of these cycles.

Example 3. For $p = 151$, we have

$$f(x) = x^{69} + x^{150}$$

which is mapped to

$$\Phi(f) = 1 + x^{33} + x^{119} + x^{150}.$$

Accordingly, the zero-set of $f = 0$ is $Z(f) = \{0, 33, 119, 150\}$. Factoring f, we obtain

$$f(x) = x^{69}(x^{81} + 1).$$

Clearly, $x = 0$ solves $f = 0$, which explains why $0 \in Z(f)$. Observe also that if we sum the remaining three exponents of $\Phi(f)$, we have $33+119+150 = 0$.

Moreover, consider the set

$$S = \{33, 119, 150\}.$$

Taking $33 \in S$ and raising it to odd powers, we have $33^1 = 33$, $33^3 = 150$, $33^5 = 119$. Since $33^3 = 150 = -1$, we have $33^6 = 1$. Therefore, odd powers greater than 5 can be reduced by multiples of 6, and we cycle around. Accordingly, 33 generates S. In a likewise manner, $119 \in S$ also generates S.

Furthermore, from the second factor of f, we have that the equation

$$x^{81} = -1$$

must have exactly three distinct solutions. Finally, note that $gcd(81, 150) = 3$.

Example 4. For $p = 181$, we have

$$f(x) = x^{111} + x^{180} = x^{111}(x^{69} + 1).$$

As in Example 3, the exponents of $\Phi(f)$ sum to zero. Similarly, for the set $S = \{49, 133, 180\}$, $49, 133 \in S$ generate S, and $gcd(69, 180) = 3$.

Remark 4. From Table 1, for all $\Phi(f)$ we observe that the exponents sum to zero. Furthermore, the set whose elements are the exponents in $\Phi(f)$ (excluding 0) are generated from the elements in a similar manner as in Examples 3 and 4. Finally, for the general binomial $f(x) = x^m + x^n$, where $m \leq n$, we obtain a factor $x^{n-m} + 1$, requiring s distinct solutions, where we have $gcd(n - m, p - 1) = s$. For $p = 151$ and $p = 181$, we have $s = 3$, and three solutions (excluding $x = 0$) for $f = 0$; for $p = 569$, $s = 4$, and four solutions; and for $p = 1021$, $s = 10$, and ten solutions.

In the next section, these observations are put on firmer formal ground.

4.2 Critical Equations

Consider a cycle of length 2 as a pair of polynomials $\{f, \Phi(f)\}$ where $f \in \Omega_p$ such that $\Phi^2(f) = f$. We want to understand why f maps to $\Phi(f)$. By Definition 3, the zero-set of f determines how f is mapped by Φ. So the question becomes how the structure of the polynomial f determines its zero-set. In this section, we will explore this question, in the hope that understanding this structure will be helpful in the search for more cycles. To that end, we will work towards and motivate a definition of critical equations, which feature prominently in many different kinds of cycles when we iterate Φ.

Theorem 4. For $p > 2$, Φ is not a bijective map.

Proof. For there to be a bijection between two sets, each element of one set must be paired exactly with one element of the other set, and vice versa, with there being no unpaired elements. For our purposes, the set is the collection of polynomials Ω_p, which maps to itself. It suffices to show that two or more polynomials map onto the same polynomial by Φ to show that Φ is not bijective.

Let p be a prime number greater than 2. For some integers n, m, consider the polynomial

$$f(x) = x^n(x^m + 1).$$

The zero-set of f determines which polynomial it is mapped to by Φ. Solutions to the equations $x^n = 0$ and $x^m = -1$ solve $f = 0$. But if we change

n to some other integer n', the equations $x^n = 0$ and $x^{n'} = 0$ have the same solution: $x = 0$. Meanwhile, the factor $(x^m + 1)$ is unchanged, and therefore its solutions remain the same. But in changing n, we get a new polynomial, but with the same zero-set as the previous polynomial. By the definition of Φ, both these polynomials are mapped to the same polynomial. Therefore there is no one-to-one correspondence and Φ is not bijective. $\square$

This leads us to consider a transformation of f with the interesting feature that the zero-set of f is invariant under the transformation, and therefore the mapping by Φ is also invariant under the transformation.

Theorem 5. For polynomials $f(x) = x^n + 1$ in Ω_p, where $n \neq 0$, $f = 0$ has the same set of solutions as $x^{p-1-n} + 1 = 0$.

Proof. Consider f

$$f(x) = x^n + x^{p-1} = x^n(x^{p-1-n} + 1) \tag{2}$$

where $n \neq 0$.

Here, $x = 0$ is a solution to $f = 0$. Furthermore, if $x^{p-1-n} = -1$ has some set of solutions $x = \{a_1, \ldots, a_k\}$, where $a_i \in \mathbb{Z}_p$, those values for x also solve $f = 0$.

Multiply f with powers of x.

$$x^q f(x) = x^{q+n}(x^{p-1-n} + 1).$$

Observe that this new polynomial retains the set of solutions to $f = 0$. We have that $x = 0$ still solves $x^{q+n} = 0$, and $x = \{a_1, \ldots, a_k\}$ still solves $x^{p-1-n} = -1$. However, suppose we let $a \in \mathbb{Z}_p$ be such that $a^n + 1 = 0$, and let $q = 1$, then we also have, by Fermat's little theorem,

$$af(a) = a^{n+1} + a^p = a^{n+1} + a$$

$$af(a) = a(a^n + 1) = 0.$$

Since $a \neq 0$, it follows that $f(a) = 0$.

Then, from 2, we have

$$f(a) = a^n(a^{p-1-n} + 1) = 0$$

where $a^{p-1-n} + 1 = 0$.

If we instead begin with the assumption that $a \in \mathbb{Z}_p$ is such that $a^{p-1-n} + 1 = 0$, then from 2 we have

$$f(a) = a^n + a^{p-1} = a^n(a^{p-1-n} + 1) = 0.$$

Multiplying the above with a, we obtain

$$af(a) = a^{n+1} + a^p = a + a^{n+1} = a(a^n + 1) = 0.$$

As $a \neq 0$, it then follows that $a^n + 1 = 0$.

Taken together, we have demonstrated that $a^n + 1 = a^{p-1-n} + 1$. Therefore, $x^a = -1$ must have the exact same set of solutions as $x^{p-1-a} = -1$. □

Theorem 5 can be generalized to a slightly larger class of polynomials, which we will be looking at more closely.

Theorem 6. For polynomials in Ω_p, the equation $x^{n-m} = -1$, where $m \neq 0$, has the same set of solutions as $x^{m+q-1} = -1$, where $q = p - n$.

Proof. As Theorem 5, except $f(x) = x^m + x^n$, and multiply x^q with f. □

To see how $x^{n-m} = -1$ and $x^{m+q-1} = -1$ must share the same set of solutions, we can consider factorizations of $n - m$ and $m + q - 1$. If $n - m$ and $m + q - 1$ share factors, there would exist a greatest common factor s, such that $gcd(n-m, m+q-1) = s$. Then we would be able to rewrite $x^{n-m} = -1$ and $x^{m+q-1} = -1$ as

$$x^{n-m} = x^{s \cdot k_1} = (x^s)^{k_1} = -1$$

$$x^{m+q-1} = x^{s \cdot k_2} = (x^s)^{k_2} = -1.$$

Now, if k_1 and k_2 both are odd, and if $x^s = -1$ has solutions, then those solutions would also solve $x^{n-m} = -1$ and $x^{m+q-1} = -1$.

The equation $x^s = -1$ is therefore what ultimately decides how the solutions to $f = 0$ look like, for binomials such as in Theorem 6.

Definition 4. Let $f(x) = x^m + x^n \in \mathbb{Z}_p[x]$, where $m \leq n$. For $q = p - n$, let $s = gcd(n - m, m + q - 1)$. The equation $x^s = -1$ is called the **critical equation** for f.

An interesting result connected to this definition is demonstrated below, using $q = p - n$.

Theorem 7. If $gcd(n - m, m - n + p - 1) = s$, then $s \mid p - 1$.

Lemma 1. For any integer t, $gcd(a, b + ta) = gcd(a, b)$.

Proof of Lemma 1. If $gcd(a, b) = s$, then $a = sk_1$ and $b = sk_2$. Then $b + ta = sk_2 + tsk_1 = s(k_2 + tk_1)$. Therefore, s divides $b + ta$. □

Proof of Theorem 7. By Lemma 1, letting $t = -1$, we have $gcd(n - m, p - 1 - (n - m)) = gcd(n - m, p - 1) = s$. □

According to Theorem 7, if we are looking for cycles where $x^s = -1$ is a critical equation, we need only test our proposed polynomials against prime numbers p where s divides $p - 1$. A corollary of Theorem 7 is that we can formulate a definition equivalent to Definition 4, without the language relating to the transformation.

Theorem 8. For $f(x) = x^m + x^n \in \mathbb{Z}_p[x]$, where $m \leq n$, and let $s = gcd(n - m, p - 1)$, $x^s = -1$ is the critical equation for f.

Remark 5. Recall Example 3 from the previous section, where $f(x) = x^{69} + x^{150} = x^{69}(x^{81} + 1)$, and $gcd(81, 150) = 3$. So, $x^3 = -1$ is the critical equation for f.

4.2.1 Distinct Solutions to Critical Equations

Let's look again at Example 3 from section 4. For $p = 151$, we have

$$f(x) = x^{69} + x^{150} = x^{69}(x^{81} + 1).$$

For f to be mapped to $\Phi(f) = 1 + x^{33} + x^{119} + x^{150}$ (see Table 1), the zero-set of f must be $Z(f) = \{0, 33, 119, 150\}$. The $x = 0$ solution is associated with the x^{69} factor. Therefore, the other three solutions must be associated with the second factor, and the equation

$$x^{81} = -1$$

must have three distinct solutions.

The question becomes why this equation has precisely three distinct solutions. From Theorem 8, the critical equation of f is $x^3 = -1$, since $gcd(81, 150) = 3$. So we must demonstrate the connection between critical equations and the number of distinct solutions.

We are interested in the number of solutions to the equation,

$$x^s = -1$$

for some integer s, over $\mathbb{Z}_p$.

Consider the equation

$$x^{2s} = 1$$

$$(x^s - 1)(x^s + 1) = x^{2s} - 1.$$

By investigating the solutions to $x^s = 1$ and $x^{2s} = 1$, we will gain information about the solutions to $x^s = -1$.

Since we are working over the field $\mathbb{Z}_p$, we have a multiplicative group G_p. If $g \in G$ is an element of G_p, the **order** of g is the smallest positive integer n such that $g^n = 1$.

Theorem 9. For a group G and $g \in G$, where the order of g is n, then

$$g^m = 1$$

is true if and only if m is a multiple of n.

Proof. Let $m = kn$, then

$$g^m = g^{kn} = (g^n)^k = 1^k = 1.$$

Suppose now that $g^m = 1$. Then, by Euclidian division, there exist integers k, r

$$m = kn + r, 0 \leq r < n$$

$$1 = g^m = g^{kn+r} = g^{kn}g^r = (g^n)^k g^r = 1^k g^r = g^r.$$

However, n is per definition the smallest positive integer such that $g^n = 1$ is true. Therefore $r = 0$ and $m = kn$. □

By Theorem 9, if $x = a$ solves $x^s = 1$, then $x = a$ also solves x^{ks}.

$|G|$ denotes the order of G, which is the number of elements in G. If $x \in G$, then a subgroup of G is $\langle x \rangle = \{1, x, x^2, \ldots\}$. G is cyclic if there exists $x \in G$ such that all elements $y \in G$ kan be written as powers of x. So, $G = \{1, x, x^2, \ldots\} = \langle x \rangle$. This can be understood as the group $\langle x \rangle$ is generated by the element x.

Lemma 2. (Lagrange's theorem). [1] If G is a finite group of order n and H is a subgroup of order m, then m divides n.

Lemma 3. [2] The multiplicative group G_p is cyclic.

Note that $G_p = \langle x \rangle = \{1, x, x^2, \ldots x^{p-1}\} = \{1, 2, \ldots, p-1\}$. Therefore the order of G_p is $p - 1$.

Theorem 10. G is a cyclic group of order $n \geq 2 \Rightarrow$ for each divisor d of n the number of elements $x \in G$ which satisfy $x^d = 1$ is d.

Proof (adapted from [1]). Let G be a cyclic group of order n generated by the element $g \in G$. If d is a divisor of n, then $dk = n$ for some integer k. Consider then

$$1, g^k, g^{2k}, \ldots, g^{(d-1)k} \tag{3}$$

which are distinct elements in G. These solve $x^d = 1$ since

$$(g^{ik})^d = (g^{dk})^i = (g^n)^i = 1^i = 1.$$

So d elements of G satisfy $x^d = 1$. It remains to show that there are no other solutions. Let y be an element from G such that $y^d = 1$. Since G is cyclic, it is generated by g, therefore there is some $e \geq 0$ such that $y = g^e$. Then

$$g^{ed} = (g^e)^d = y^d = 1.$$

The order of g is n, so n is the smallest integer for which $g^n = 1$. Therefore ed must be a multiple of n, such as ln for some integer l. Then

$$ed = ln = l(dk).$$

So $e = lk$ and $y = g^e = g^{lk}$, but this is already an element in 3. Therefore these are the only solutions. □

Putting things together, by Lemma 3, G_p is a cyclic group of order $p - 1$. Supposing we have some element $g \in G$ such that $g^s = 1$ and $s \leq p - 1$, then by Lemma 2, s divides $p - 1$. By Theorem 10, then there are s distinct solutions to $x^s = 1$. Further supposing we have $g \in G$ such that $g^{2s} = 1$ and $2s \leq p - 1$, we then have that $x^{2s} = 1$ must have $2s$ distinct solutions. Consequently, $x^s = -1$ must also have s distinct solutions.

Going back to the equation at the beginning of this section, we have for $p = 151$

$$x^{81} = -1.$$

Since $81 = 3^4$ and $gcd(81, 150) = 3$ the equation above has three distinct solutions.

4.2.2 Critical Equations and Roots of Unity

In Example 3, for $p = 151$, if we exclude the $x = 0$ solution from the zero-set of $f = 0$, we have the set $S = \{33, 119, 150\}$. The sum of these elements is zero modulo 151, and we have that this set is generated from the elements $33, 119 \in S$, such that $S = \{33^1, 33^3, 33^5\} = \{119^1, 119^3, 119^5\}$.

This peculiar structure is explicable in light of properties of roots of unity, as will be demonstrated in this section.

Theorem 11. For $s \in \mathbb{Z}_p$, where $2s$ is a proper divisor of $p-1$, supposing $x = \alpha$ is a solution to the equation $x^s = -1$, then solutions take the form $x = \{\alpha, \alpha^3, \ldots, \alpha^{2s-1}\}$, where $\alpha + \alpha^3 + \ldots + \alpha^{2s-1} = 0$.

Proof. Consider the equation

$$x^s = -1.$$

By squaring both sides, we can explore useful features of roots of unity, which are solutions to the equation $x^n = 1$.

$$x^{2s} = 1. \tag{4}$$

By Theorem 10, we have $2s$ distinct solutions to 4, of the form

$$x = \{1, \alpha, \alpha^2, \ldots, \alpha^{2s}\} \tag{5}$$

for some $\alpha \in \mathbb{Z}_p$.

Consider then, from 4,

$$0 = x^{2s} - 1 = (x^s - 1)(x^s + 1). \tag{6}$$

The question becomes which solutions from 5 belong to which factor from 6. We can see immediately that $x = 1$ solves $x^s - 1 = 0$. Supposing $x = \alpha$ solves $x^s = -1$, then

$$\alpha^{2s} = 1,$$

which solves $x^s - 1 = 0$. By similar logic, the solutions to $x^s - 1 = 0$ are $x = \{1, \alpha^2, \alpha^4, \ldots, \alpha^{2s}\}$. These are the even exponents, and there are s distinct solutions. The remaining s distinct solutions, with odd exponents, therefore solve $x^s + 1 = 0$. These solutions are

$$x = \{\alpha, \alpha^3, \ldots, \alpha^{2s-1}\}$$

as desired.

By the factor theorem, we have

$$x^s + 1 = (x - \alpha)(x - \alpha^3) \cdots (x - \alpha^{2s-1}) = \prod_{s=1}^{s} (x - \alpha^{2s-1}). \tag{7}$$

Expanding and looking only at the coefficient for the x^{s-1} term, we have

$$(-\alpha - \alpha^3 - \ldots - \alpha^{2s-1})x^{s-1}.$$

Comparing this x^{s-1} term with the left-hand side of 7, we see that this coefficient must be equal to zero. Therefore, solutions to $x^s = -1$ sum to zero, and solutions take the form $x = \{\alpha, \alpha^3, \ldots, \alpha^{2s-1}\}$. □

Theorem 12. For a polynomial $f = x^m + x^n$, where $gcd(n-m, p-1) = s$ such that $2s$ is a proper divisor of $p-1$, and an odd integer k that does not divide $p-1$, f is mapped by Φ to one of two polynomials

$$\Phi(f) = 1 + x^{\alpha} + x^{\alpha^3} + ... + x^{\alpha^{2s-1}} \tag{8}$$

$$\Phi(f) = x^{\alpha} + x^{\alpha^3} + ... + x^{\alpha^{2s-1}}. \tag{9}$$

Proof. Factorizing, we obtain $f(x) = x^m + x^n = x^m(x^{n-m} + 1)$. By assumption, we have that $n - m = sk$ for some integers s and k. Supposing $x = \alpha$ is a solution to $x^s = -1$, then $f(\alpha) = \alpha^m((\alpha^s)^k + 1) = \alpha^m((-1)^k + 1)$. Since k is odd, $x = \alpha$ solves $f = 0$. Since k does not divide $p-1$, we can be assured that no new solutions are introduced. With the factor x^m accounting for the constant term in 8, the solutions take the form from Theorem 11, with f mapped to 8 if $m \neq 0$, or f is mapped to 9 if $m = 0$. □

Remark 6. With Theorem 12, we have established a connection between the critical equation of a binomial f and the zero-set of that binomial, and therefore how f is mapped by Φ. However, recalling that the primary motivation for critical equations stated in the beginning of Section 4.2 was to understand the mapping $f \mapsto \Phi(f)$, an expanded definition of critical equations suggests itself, not limited to binomials. Simply, for $f \in \Omega_p$ and s such that $2s$ is a proper divisor of $p-1$, if we have either $\Phi(x + x^{s+1}) = \Phi(f)$ or $\Phi(x^s + 1) = \Phi(f)$, then $x^s = -1$ is a critical equation for f.

4.2.3 Methods: Critical Equations and the Search for More Cycles

Since critical equations feature in all previous examples of cycles of length 2, we can restrict our search for more cycles to polynomials associated with specific critical equations, and thereby further constrain our search space. Using the concept of critical equations from Remark 6, we can generate polynomials of the form $\Phi(f)$ as candidates for a cycle of length 2. See Appendix 1 for a Mathematica program designed to search for cycles of length 2, based on the mathematics of critical equations.

4.3 Results

In this section, we analyze the results of the automated search for cycles of length 2. See Appendix *A* for the Mathematica code for this this search program, and Appendix *B* for all cycles discovered by this search.

4.3.1 A Taxonomy of Cycles of Length 2

In this section, we propose a taxonomy of cycles of length 2, motivated by their salient features.

Definition 5. A taxonomy is a nested set, forming a hierarchy where sets of lower rank are subsets of sets of higher rank.

Remark 7. Throughout this section, cycles of length 2 are described as consisting of two polynomials $\{f, \Phi(f)\}$ that map to each other under Φ. Here $\Phi(f)$ refers to polynomials generated from critical equations, as in Remark 6. The polynomial f is described simply as the the polynomial that maps to $\Phi(f)$.

Remark 8. As we go through examples in this section, we will build up to a definition of our taxonomic hierarchy, summarized in Figure 2.

Example 5. In Table 2, the polynomials $\Phi(f)$, represented as sets of of exponents, were generated from the critical equation $x^s = -1$, for some integer s. And as can be seen from the tally of cycles in Appendix B, examples of cycles of length 2 have been found for all $s \leq 23$.

p	$\Phi(f)$	f	s
3169	{0, 1325, 1844}	{1110, 1252}	2
3271	{0, 843, 2429, 3270}	{1443, 3270}	3
7793	{0, 2501, 3578, 3609, 3789, 4004, 4184, 4215, 5292}	{4473, 5825}	8
17579	{0, 2602, 6197, 7306, 7550, 7948, 8222, 9787, 10266, 12928, 15090, 17578}	{6806, 8599}	11

Table 2: Examples of cycles of length 2, for some prime p and critical equation $x^s = -1$.

Since all polynomials comprising the cycles in Table 2 and Appendix B were generated from solutions to the critical equation $x^s = -1$, the first and highest rank of taxonomic classification sort cycles of length 2 according to the value of s for which we have $\Phi(x^s + 1) = \Phi(f)$ or $\Phi(x + x^{s+1}) = \Phi(f)$, such that $\Phi^2(f) = f$.

Remark 9. As indicated by Appendix B, the first examples of cycles associated with large values of s tend to occur at larger prime numbers in comparison to cycles associated with smaller values of s. Moreover, the search for cycles for large primes and large values of s becomes progressively more

computationally demanding, requiring longer time to search through shorter intervals of prime numbers.

Example 6. Consider the cycles in Table 3.

p	$\Phi(f)$	f
151	{0, 33, 119, 150}	{69, 150}
151	{33, 119, 150}	{0, 111}
2341	{0, 1107, 1235, 2340}	{1101, 2340}
2341	{1107, 1235, 2340}	{0, 2199}

Table 3: Examples of cycles of length 2, comprising polynomials the zero-set of which either includes $x = 0$ or not.

For these specific prime numbers, there are two versions of each cycle: one version where $x = 0$ belongs to the zero-set of f, and one version where $x = 0$ does not belong to the zero-set of f. This corresponds to the two different polynomials from Theorem 12.

The second rank of taxonomic classification comprises cycles consisting of polynomials the zero-set of which either includes or excludes $x = 0$.

Remark 10. As can be seen from the examples in Tables 2 and 3, as well as in Appendix *B*, for the vast majority of all cycles of length 2, the polynomial f that maps to $\Phi(f)$ is a binomial.

Example 7. Consider the cycles in Table 4.

p	$\Phi(f)$	f
3307	{0, 58, 3250, 3306}	{914, 992, 2315, 2393}
3463	{0, 368, 3096, 3462}	{1676, 1718, 1745, 1787}
3517	{384, 596, 980, 2537, 2921, 3133}	{0, 1650, 2658, 3516}
7237	{0, 1831, 5407, 7236}	{369, 5094, 6765, 7236}

Table 4: Exceptional cycles of length 2, where the polynomial f is not a binomial.

We see exceptions to the general observation in Remark 10. Accordingly, the third rank of taxonomic classification comprises cycles where the polynomial f that maps to $\Phi(f)$ either is a binomial or is not a binomial.

Remark 11. From Table 4, observe that for $p = \{3307, 3463, 7237\}$, the elements of f sum to zero. However, for $p = 3517$, the elements of f do not

sum to zero. From Appendix B, more examples of either situation can be found.

The fourth and final rank of taxonomic classification comprises cycles where the exponents of the polynomial f either sum to zero or do not sum to zero.

The taxonomic scheme is summarized in Definition 6 and illustrated as a polytree graph in Figure 2.

Definition 6. Let T be the set of all unorderd pairs of polynomials $\{f, \Phi(f)\}$ where $f \in \Omega_p$ such that $\Phi^2(f) = f$.
i) Let $T_1 \subseteq T$ be the first taxonomic rank, where $T_1 = \cup_{s \geq 2, 2s|(p-1)} T_{1,s}$, and where $T_{1,s} = \{\{f, \Phi(f)\} \in T_1 | \Phi(x^s + 1) \in \{f, \Phi(f)\} \vee \Phi(x^{s+1} + x) \in \{f, \Phi(f)\}\}$.
ii) Let $T_2 \subseteq T_1$ be the second taxonomic rank, where $T_2 = T_{2,0} \cup T_{2,!0}$, and where $T_{2,0}$ are of pairs of polynomials where 0 belongs to the zero-set of f and $T_{2,!0}$ are pairs of polynomials where 0 does not belong to the zero-set of f.
iii) Let $T_3 \subseteq T_2$ be the third taxonomic rank, where $T_3 = T_{3,b} \cup T_{3,!b}$, and where $T_{3,b}$ are pairs of polynomials where f is a binomial and $T_{3,!b}$ are pairs of polynomials where f is not a binomial.
iv) Let $T_4 \subseteq T_3$ be the fourth taxonomic rank, where $T_4 = T_{4,0} \cup T_{4,!0}$, and where $T_{4,0}$ are pairs of polynomials where the exponents of f sum to zero and $T_{4,!0}$ are pairs of polynomials where the exponents of f do not sum to zero.

Let's categorize a cycle of length 2 according to this taxonomy.

Example 8. For $p = 3517$, we have the cycle

$$C = \{\{0, 1650, 2658, 3516\}, \{384, 596, 980, 2537, 2921, 3133\}\} = \{f, \Phi(f)\}.$$

We know that $\Phi(f)$ is generated from $s = 6$, so $C \in T_{1,6}$; the zero-set of $\Phi(f)$ includes $x = 0$, so $C \in T_{2,0}$; f is not a binomial, so $C \in T_{3,!b}$; and the exponents of f do not sum to zero, so $C \in T_{4,!0}$.

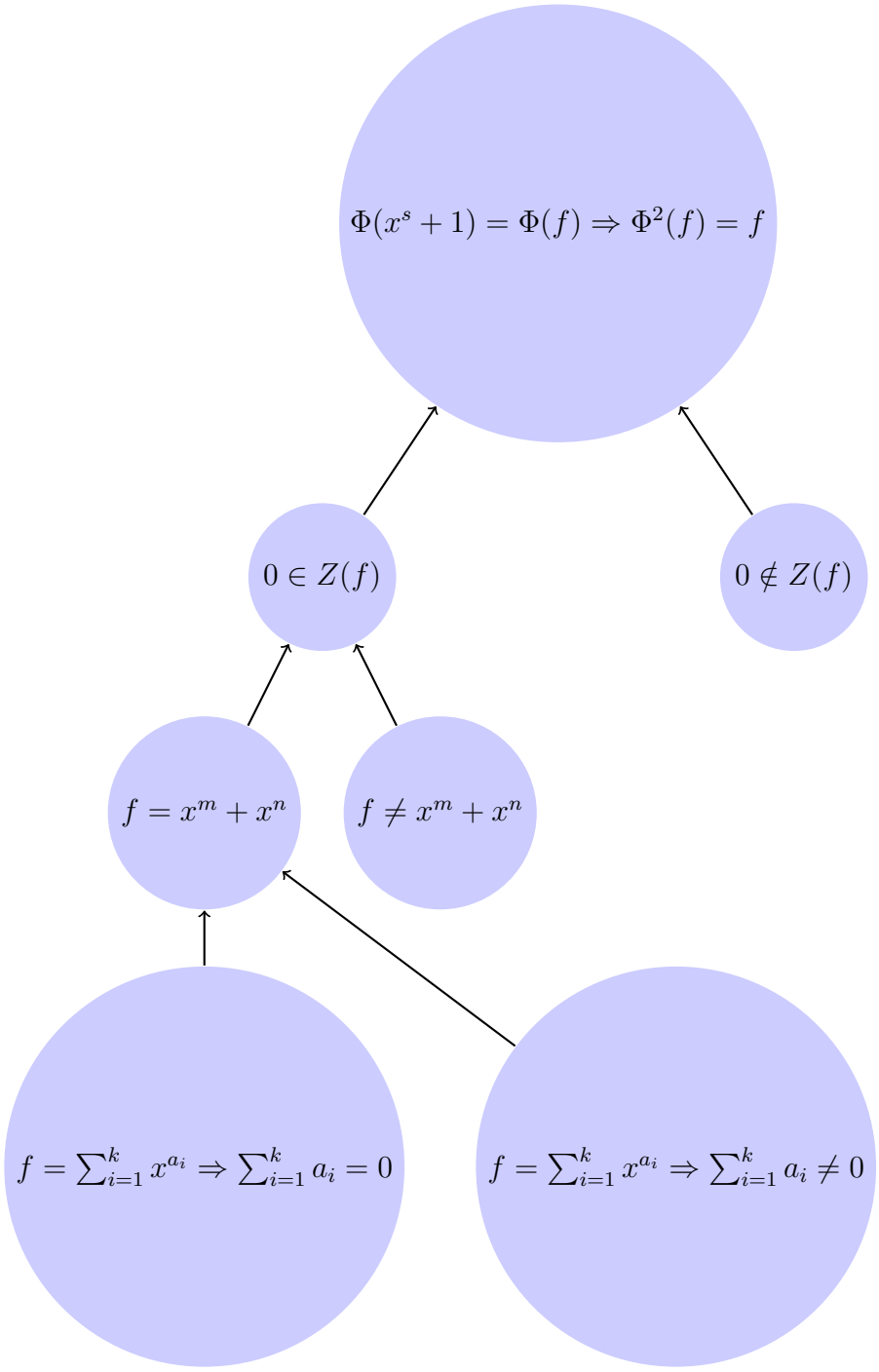

Figure 2: A taxonomy of cycles of length 2, descending from the first rank. For reasons of image formatting, this figure excludes the tree connected to the right node at the second rank, which is identical to the tree connected to the left node at the same rank. Also for reasons of image formatting, the complete criterion for the first rank is not included. See Definition 6 for the complete criterion.

4.3.2 Prerequisites for Cycles of Length 2

In previous sections, we have used f to denote a polynomial that maps to the polynomial $\Phi(f)$. A cycle of length 2 occurs when $\Phi^2(f) = f$. The question becomes if there are any restrictions on f and $\Phi(f)$ that determine whether a cycle of length 2 occurs for a given prime number p.

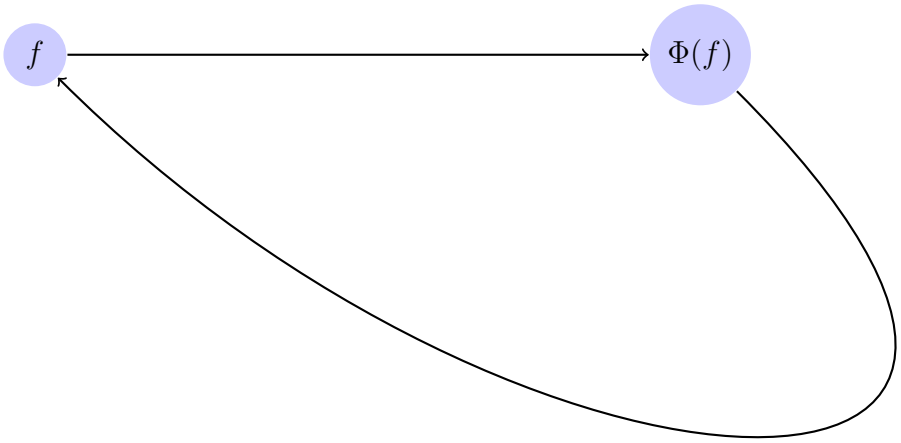

Figure 3: A cycle of length 2.

First a brief note on the automated search program used to discover the cycles of length 2 tallied in Appendix *B* and discussed in section 6.1.

Remark 12. For some s and p, the polynomial $x^s + 1$ over the integers modulo p has a zero-set. The automated search program in Appendix *A* uses this zero-set to create a polynomial, as in Section 4.2.3. Call this polynomial $\Phi(f)$. Then the program maps $\Phi(f)$ to a new polynomial f under Φ. Finally, the program checks whether $\Phi^2(f) = f$; if this is true, a cycle of length 2 exists for this s and p.

From Remark 12, it is clear that for a given s and p, $\Phi(f)$ is fixed. There is one zero-set, mapped to one polynomial $\Phi(f)$. For this reason, all polynomials $\Phi(f)$ from Tables 2, 3 and 4 exhibit a similar structure, as described in Section 4.2.2. However, as discussed in the previous section, the polynomials f exhibit greater variety. One reason for this is that several different polynomials map to $\Phi(f)$.

Example 9. For $p = 7793$, and $f \mapsto \Phi(f)$, consider the following cycle.

$$\{4473, 5825\} \mapsto \{0, 2501, 3578, 3609, 3789, 4004, 4184, 4215, 5292\}.$$

Here, $\Phi(f)$ is generated from $x^8 = -1$. We can see why $f \mapsto \Phi(f)$ by factorizing the polynomial f.

$$f(x) = x^{4473} + x^{5825} = x^{4473}(x^{1352} + 1)$$

where $gcd(1352, 7792) = 8$. From Theorem 8, we know that $x^8 = -1$ is the critical equation for f, which by Theorem 12 detemines how f is mapped by Φ. However f is not the only polynomial mapped to $\Phi(f)$. Consider

$$\hat{f}(x) = x + x^9$$

where $\hat{f}(x) = 0$ has the exact same zero-set as $f(x) = 0$, and therefore $\Phi(\hat{f}) = \Phi(f)$. This observation is generalized in the following corollary to Theorem 12.

Theorem 13. Working over $\mathbb{Z}_p$, supposing $2s$ is a proper divisor of $p - 1$, let $f(x) = x^n + x^{s+2ks+n}$, for some integer k. Then, if and only if $2k+1$ does not divide $p - 1$, f is mapped by Φ to

$$\Phi(f) = 1 + x^{\alpha} + x^{\alpha^3} + \ldots + x^{\alpha^{2s-1}}. \tag{10}$$

Proof. Factorize f.

$$f(x) = x^n(x^{s+2ks} + 1).$$

The factor x^n is zero when $x = 0$, which accounts for the constant term in 10. For the rest of the terms in 10, we require that the solution set of f, excepting the $x = 0$ solution, is the same the solution set as $x^s = -1$. Suppose $x = \alpha$ is a solution to $x^s = -1$. Add even multiples of s to the exponent in x^s, giving

$$x^{s+2ks} = x^{s(2k+1)} = (x^s)^{(2k+1)} \Rightarrow (\alpha^s)^{2k+1} = (-1)^{2k+1} = -1.$$

So, solutions to $x^s = -1$ are also solutions to $x^{s+2ks} = -1$; therefore f maps to 10, with one exception. From the assumption in the theorem, we have that $p - 1 = 2sq$, for some factors s and q, where q may be composite or equal to 1. Now, if $2k + 1 = q \neq 1$, then $2(2k + 1)$ is a proper divisor of $p - 1$, and by Theorem 11, for such values of k, $x^{s+2ks} = -1$ has a different solution set than $x^s = -1$, and f is not mapped to 10. $\square$

Example 10. For $p = 733$, and $f \mapsto \Phi(f)$, consider the following cycle.

$$\{338, 347, 386, 395\} \mapsto \{0, 308, 426, 732\}.$$

From the automated search, we know that $\Phi(f)$ is generated from $x^3 = -1$, which gives a clue why f maps to $\Phi(f)$. For f, divide the exponents by 3, and rewrite them as quotient and remainder.

$$f(x) = x^{338} + x^{347} + x^{386} + x^{395}$$

$$f(x) = (x^3)^{112}x^2 + (x^3)^{115}x^2 + (x^3)^{128}x^2 + (x^3)^{131}x^2.$$

Supposing $\alpha^3 = -1$, then

$$f(\alpha) = (-1)^{112}\alpha^2 + (-1)^{115}\alpha^2 + (-1)^{128}\alpha^2 + (-1)^{131}\alpha^2.$$

$$f(\alpha) = \alpha^2 - \alpha^2 + \alpha^2 - \alpha^2 = 0.$$

Observe the pairwise cancellation of terms, suggesting another class of polynomials that also map to 10.

Theorem 14. Working over $\mathbb{Z}_p$, supposing $2s$ is a proper divisor of $p - 1$, then

$$f(x) = x^{sq_{1.1}+r_1} + x^{sq_{1.2}+r_1} + x^{sq_{2.1}+r_2} + x^{sq_{2.2}+r_2} + \ldots + x^{sq_{n.1}+r_n} + x^{sq_{n.2}+r_n}$$

maps to 10 from Theorem 13 if the parity of $q_{k.1}$ and $q_{k.2}$ is not the same.

Proof. For f to map to 10, we require that $f(x) = 0$ has the same zero-set as $x^s = -1$. Rewrite the exponents for each pair of terms as

$$(x^s)^{q_{k.1}}x^{r_k} + (x^s)^{q_{k.2}}x^{r_k}.$$

Supposing $\alpha^s = -1$, then we have

$$(\alpha^s)^{q_{k.1}}\alpha^{r_k} + (\alpha^s)^{q_{k.2}}\alpha^{r_k} = (-1)^{q_{k.1}}\alpha^{r_k} + (-1)^{q_{k.2}}\alpha^{r_k}.$$

By assumption, the parity of $q_{k.1}$ and $q_{k.2}$ is not the same, which results in pairwise cancellation. Therefore solutions to $x^s = -1$ also solve $f(x) = 0$. □

Remark 13. As can be seen from Theorem 14, critical equations apply to a larger class of polynomials, not necessarily binomials, as discussed in Remark 6.

From Theorems 13 and 14, we see that several polynomials map to $\Phi(f)$. Together with $\Phi(f)$, these polynomials can be seen as candidate polynomials for a cycle of length 2. A cycle occurs if $\Phi(f)$ is mapped back to f.

The situation is summarized in Figure 4, where for a given s and p, we have a fixed point represented by the polynomial $\Phi(f)$, and several polynomials that all map to $\Phi(f)$.

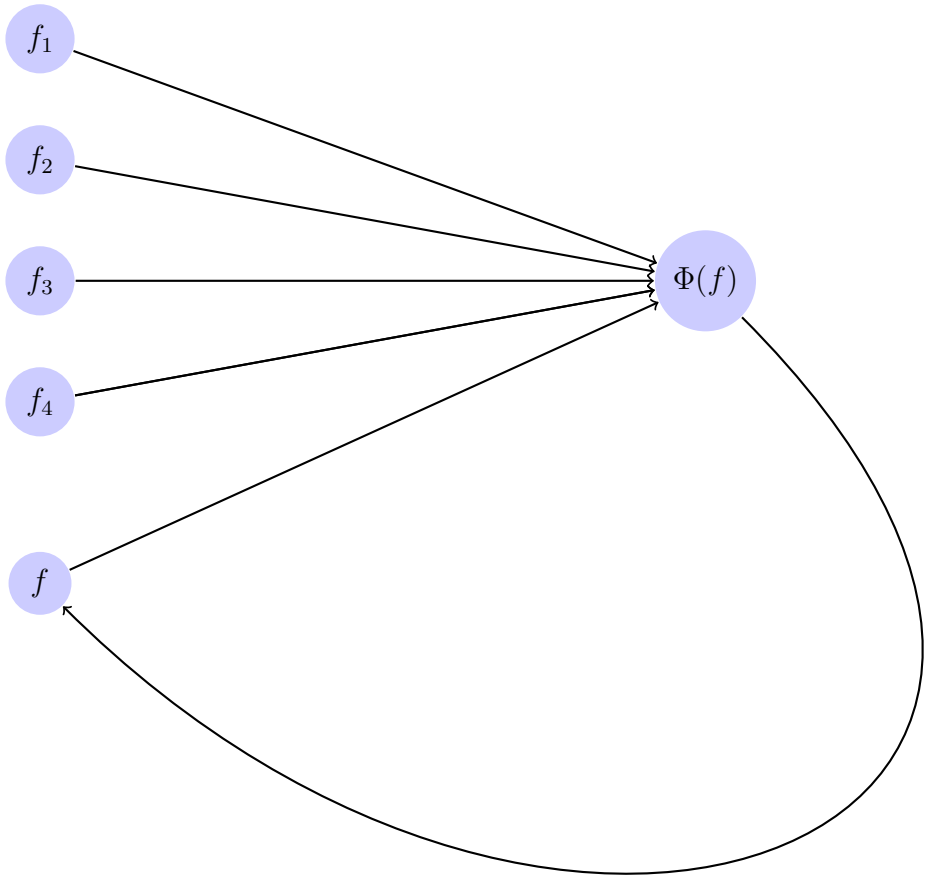

Figure 4: A cycle of length 2 along with candidate polynomials.

We conclude by formulating two hypotheses regarding cycles of length 2.

Remark 14. By design, from Remark 12, all polynomials found by the automated search exhibit the structure in $\Phi(f)$ from Theorems 13 and 14. Moreover, all examples from the previous search, by Samuel Lundqvist, also exhibit this same structure. This constitutes weak heuristic motivation for the following hypothesis.

Hypothesis 1. All cycles of length 2 exhibit the structure in $\Phi(f)$ from Theorem 12. Explicitly, for cycles of length 2 of the form $\{f, \Phi(f)\}$, where $f \in \Omega_p$, the exponents of the polynomial $\Phi(f)$ are determined by the roots of unity of the equation $x^{2s} = 1$ and the critical equation $x^s = -1$, from Theorem 11.

Remark 15. As can be seen in Appendix *B*, examples have been found of cycles of length 2 up to $s = 23$. Since the search became progressively more computationally demanding for higher values of s and p, the search was terminated at $s = 23$. However, there are no prima facie reasons to believe there exist no cycles of length 2 for higher values of s.

Hypothesis 2. For each $s \in \mathbb{Z}$, there is at least one prime number p for which there exists a cycle of length 2 where $x^s = -1$ is a critical equation.

A Appendix A: A Mathematica Program to Search for Cycles of Length 2

In this appendix, we include the Mathematica code for the automated search algorithm that searches for cycles of length 2 where $x^s = -1$ is a critical equation.

```
f[p_, s_] := Union[Solve[x^s == -1, x, Modulus -> p]];

haslengtheq9[l_, s_] := Length[l[[2]]] == s;

g[n_, s_] :=
  Select[Transpose[{Map[Prime, Range[1, 3000]],
       Map[f[#, s] &, Map[Prime, Range[1, 3000]]]}],
     haslengtheq9[#, s] &][[n]][[2]];

h[n_, s_] :=
  Select[Transpose[{Map[Prime, Range[1, 3000]],
       Map[f[#, s] &, Map[Prime, Range[1, 3000]]]}],
     haslengtheq9[#, s] &][[n]][[1]];

i[n_, s_] := Piecewise[{
    {0, g[n, s] == {}},
    {Total[y^x /. g[n, s]] + 1 /. y -> x, True}
    }];

j[n_, s_] := Union[Solve[i[n, s] == 0, x, Modulus -> h[n, s]]];

xi[n_, s_] := Map[First[#][[2]] &, j[n, s]];

Regel[l_] := Map[{x -> #} &, l];

qhi[l_, p_] :=
  Map[First[#][[2]] &,
   Union[Solve[(Total[y^x /. Regel[l]] /. y -> x) == 0, x,
     Modulus -> p]]];

phi[l_, p_] := If[l == {}, Range[0, p - 1], qhi[l, p]];

nphi[l_, p_, k_] := Nest[phi[#, p] &, l, k];

check2orbit[n_, s_] := nphi[xi[n, s], h[n, s], 2] == xi[n, s];

Search[a_, b_, s_] :=
  Select[Transpose[{Map[h[#, s] &, Range[a, b]],
     Map[check2orbit[#, s] &, Range[a, b]]}], MemberQ[#, True] &];
```

B Appendix B: Cycles of Length 2

p	$\Phi(f)$	f	p	$\Phi(f)$	f
409	{0, 143, 266}	{41, 331}	3457	{0, 708, 2749}	{557, 2523}
449	{0, 67, 382}	{197, 223}	5333	{0, 2630, 2703}	{1621, 1619}
1373	{0, 668, 705}	{266, 272}	5441	{0, 2452, 2989}	{608, 4354}
1889	{0, 331, 1158}	{1158, 1812}	6089	{0, 455, 5634}	{2266, 3444}
2473	{0, 567, 1906}	{1047, 1649}	6217	{0, 2372, 3845}	{2694, 5656}
3169	{0, 1325, 1844}	{1110, 1252}	6521	{0, 2364, 4157}	{2488, 4530}

Table 5: Cycles of length 2, with $x^2 = -1$ as a critical equation

p	$\Phi(f)$	f	p	$\Phi(f)$	f
151	{0, 33, 119, 150}	{69, 150}	8161	{0, 2904, 5258, 8160}	{2675, 5486}
151	{0, 111}	{33, 119, 150}	8233	{2613, 5621, 8232}	{0, 2865}
181	{0, 49, 133, 180}	{111, 180}	8233	{0, 2613, 5621, 8232}	{6303, 8232}
367	{0, 84, 284, 366}	{26, 341}	8293	{2051, 6243, 8292}	{0, 579}
373	{0, 89, 285, 372}	{81, 372}	8329	{1053, 7277, 8328}	{0, 177}
751	{0, 73, 679, 750}	{219, 750}	8353	{1737, 6617, 8352}	{0, 4569}
769	{0, 361, 409, 768}	{363, 768}	8353	{0, 1737, 6617, 8352}	{7095, 8352}
937	{0, 323, 615, 936}	{501, 936}	8539	{0, 2553, 5987, 8538}	{4599, 8538}
1021	{0, 369, 653, 1020}	{549, 1020}	8581	{425, 8157, 8580}	{0, 489}
1831	{0, 673, 1159, 1830}	{63, 1830}	8641	{0, 3573, 5069, 8640}	{699, 8640}
1867	{0, 835, 1033, 1866}	{303, 1866}	8923	{0, 3848, 5076, 8922}	{953, 7970}
1879	{0, 489, 1391, 1878}	{525, 1878}	9883	{0, 2537, 7347, 9882}	{483, 9882}
2341	{0, 1107, 1235, 2340}	{1101, 2340}	10111	{0, 4282, 5830, 10110}	{2114, 7997}
2341	{0, 2199}	{1107, 1235, 2340}	10159	{0, 4594, 5566, 10158}	{4040, 6119}
3067	{0, 974, 2094, 3066}	{18, 346, 2721, 3049}	10531	{0, 5081, 5451, 10530}	{831, 10530}
3217	{0, 1707}	{205, 3013, 3216}	10723	{0, 1256, 9468, 10722}	{5237, 5486}
3271	{0, 843, 2429, 3270}	{1443, 3270}	10753	{0, 5151, 5603, 10752}	{7953, 10752}
3307	{0, 58, 3250, 3306}	{914, 992, 2315, 2393}	10993	{1545, 9449, 10992}	{0, 8253}
3463	{0, 368, 3096, 3462}	{1676, 1718, 1745, 1787}	11083	{0, 4378, 6706, 11082}	{1078, 5173, 5910, 10005}
3691	{0, 475, 3217, 3690}	{3351, 3690}	11551	{0, 3980, 7572, 11550}	{4937, 6614}
3697	{0, 520, 3178, 3696}	{362, 3335}	12289	{6049, 6241, 12288}	{0, 6141}
3733	{0, 949, 2785, 3732}	{519, 3732}	12517	{0, 6111, 6407, 12516}	{8433, 12516}
3847	{0, 639}	{1893, 1955, 3846}	12553	{0, 5158, 7396, 12552}	{1763, 10790}
4021	{0, 2607}	{1813, 2209, 4020}	12577	{0, 2068, 2863, 6345}	{4815, 7763, 12576}
4057	{0, 1409, 2649, 4056}	{1425, 4056}	12739	{0, 5586, 7154, 12738}	{704, 1787, 10952, 12035}
4261	{0, 1648, 2614, 4260}	{1625, 2636}	12967	{0, 5718, 7250, 12966}	{4070, 8897}
4273	{0, 1611, 2663, 4272}	{3435, 4272}	13003	{0, 1688, 11316, 13002}	{4635, 5862, 7141, 8368}
4423	{0, 67, 4357, 4422}	{3939, 4422}	13999	{0, 4212, 9788, 13998}	{3173, 10826}
4483	{0, 506, 3978, 4482}	{110, 4373}	14143	{0, 5172, 8972, 14142}	{3401, 10742}
4567	{0, 3663}	{1113, 3455, 4566}	14503	{0, 4174, 10330, 14502}	{2185, 3069, 11434, 12318}
5077	{0, 1630, 3448, 5076}	{1388, 3689}	14551	{0, 3836, 10716, 14550}	{7112, 7439}
5749	{0, 2019}	{331, 5419, 5748}	14557	{0, 6222, 8336, 14556}	{6416, 8141}
5827	{0, 3963}	{1351, 4477, 5826}	14683	{0, 3299, 11385, 14682}	{10965, 14682}
5923	{0, 429, 5495, 5922}	{3201, 5922}	15241	{0, 6388, 8854, 15240}	{566, 14675}
6367	{0, 770, 5598, 6366}	{674, 5693}	15277	{0, 811, 14467, 15276}	{11559, 15276}
6547	{0, 2333, 4215, 6546}	{5757, 6546}	15349	{0, 6548, 8802, 15348}	{1442, 13907}
6547	{0, 1119}	{2333, 4215, 6546}	15559	{0, 3635, 11925, 15558}	{14397, 15558}
6823	{0, 2686, 4138, 6822}	{485, 6338}	16087	{0, 5620, 10468, 16086}	{6722, 9365}
6967	{0, 5331}	{383, 6585, 6966}	16249	{0, 7517, 8733, 16248}	{2349, 16248}
7069	{0, 267}	{2041, 5029, 7068}	16333	{0, 1550, 14784, 16332}	{1676, 14657}
7177	{0, 2039, 5139, 7176}	{3561, 7176}	16411	{0, 2757, 13655, 16410}	{2253, 16410}
7237	{0, 1831, 5407, 7236}	{369, 5094, 6765, 7236}	16651	{0, 224, 16428, 16650}	{8201, 8450}
7393	{0, 1718, 5676, 7392}	{143, 7250}	17041	{0, 2698, 14344, 17040}	{4862, 12179}
7537	{0, 1963, 5575, 7536}	{5115, 7536}	17107	{0, 6798, 10310, 17106}	{6134, 10973}
7621	{0, 1683}	{3125,4497,7620}	17203	{0, 4388, 12816, 17202}	{3686, 13517}
			17467	{0, 6892, 10576, 17466}	{4220, 13247}

Table 6: Cycles of length 2, with $x^3 = -1$ as a critical equation

p	$\Phi(f)$	f
569	{0, 76, 277, 292, 493}	{190, 220}
1153	{0, 75, 123, 1030, 1078}	{190, 378}
2417	{0, 345, 1205, 1212, 2072}	{1172, 1992}
6833	{0, 428, 910, 5923, 6405}	{1622, 3314}

Table 7: Cycles of length 2, with $x^4 = -1$ as a critical equation

p	$\Phi(f)$	f	p	$\Phi(f)$	f
421	{44, 67, 142, 169, 420}	{0, 325}	13151	{0, 3719, 3891, 8622, 10071, 13150}	{965, 13150}
431	{26, 186, 315, 336, 430}	{0, 385}	15451	{325, 1141, 2532, 11454, 15450}	{0, 8405}
3631	{0, 523, 1529, 2427, 2784, 3630}	{3605, 3630}	17191	{748, 7799, 11288, 14548, 17190}	{0, 10585}
5591	{0, 137, 2367, 3595, 5084, 5590}	{145, 5590}	18541	{1393, 2103, 6356, 8690, 18540}	{0, 6755}
6991	{0, 1085, 3183, 4254, 5461, 6990}	{4795, 6990}	19081	{5464, 6469, 10477, 15753, 19080}	{0, 515}
7321	{1925, 1960, 4636, 6122, 7320}	{0, 4525}	19211	{2524, 7476, 13434, 14989, 19210}	{0, 3205}
7331	{458, 2835, 4882, 6488, 7330}	{0, 1055}	19751	{8286, 16128, 16431, 18409, 19750}	{0, 19095}
8461	{193, 5056, 5668, 6006, 8460}	{0, 245}	20981	{1844, 5772, 14780, 19567, 20980}	{0, 3685}
8951	{0, 3608, 6041, 8497, 8708, 8950}	{8516, 8761}	21341	{1627, 8991, 11569, 20496, 21340}	{0, 1195}
9041	{18, 3516, 5832, 8717, 9040}	{0, 3995}	23131	{0, 721, 12172, 13768, 19602, 23130}	{9356, 11101}
11681	{569, 3307, 8848, 10639, 11680}	{0, 3125}	25601	{0, 2404, 6610, 7781, 8807, 25600}	{3860, 11265}
12071	{0, 5108, 5838, 6260, 6937, 12070}	{3305, 6630}	26821	{581, 7340, 7789, 11112, 26820}	{0, 19055}
12941	{1267, 3016, 9264, 12336, 12940}	{0, 11105}	26321	{0, 1048, 5262, 7178, 12834, 26320}	{1308, 25013}
12941	{0, 1267, 3016, 9264, 12336, 12940}	{2789, 8674}	27011	{9728, 12560, 14084, 17651, 27010}	{0, 2105}

Table 8: Cycles of length 2, with $x^5 = -1$ as a critical equation

p	$\Phi(f)$	f
1693	{0, 92, 704, 796, 897, 989, 1601}	{638, 968}
2713	{0, 191, 696, 887, 1826, 2017, 2522}	{651, 2325}
3517	{384, 596, 980, 2537, 2921, 3133}	{0, 1650, 2658, 3516}
5281	{0, 1153, 1673, 2455, 2826, 3608, 4128}	{2097, 2619}
5953	{0, 1107, 1296, 2403, 3550, 4657, 4846}	{496, 1678}
7057	{0, 84, 1850, 1934, 5123, 5207, 6973}	{1549, 4639}
8089	{0, 1387, 2293, 3680, 4409, 5796, 6702}	{312, 4554}
10321	{0, 2528, 3151, 4642, 5679, 7170, 7793}	{5190, 7908}
10729	{0, 495, 3970, 4465, 6264, 6759, 10234}	{7186, 9352}
12517	{0, 902, 3740, 4642, 7875, 8777, 11615}	{1980, 2754}
12541	{0, 1141, 1253, 2394, 10147, 11288, 11400}	{678, 2640}
12577	{0, 793, 5113, 5906, 6671, 7464, 11784}	{2395, 11377}
15289	{2134, 4966, 7100, 8189, 10323, 13155}	{0, 2166, 13122, 15288}
15973	{0, 1982, 4844, 6826, 9147, 11129, 13991}	{6308, 7838}
21577	{749, 6703, 7452, 14125, 14874, 20828}	{0, 6894, 14682, 21576}
22381	{0, 4921, 8275, 9185, 13196, 14106, 17460}	{6704, 15158}
22453	{1289, 4306, 5595, 16858, 18147, 21164}	{0, 4542, 17910, 22452}
24517	{3804, 7868, 11672, 12845, 16649, 20713}	{0, 9414, 19686, 24516}
24781	{0, 352, 5683, 6035, 18746, 19098, 24429}	{4658, 24284}
25321	{6347, 9148, 9826, 15495, 16173, 18974}	{0, 1302, 24018, 25320}
25873	{0, 894, 7322, 8216, 17657, 18551, 24979}	{6082, 22936}
26881	{0, 676, 12212, 12888, 13993, 14669, 26205}	{19238, 23036}

Table 9: Cycles of length 2, with $x^6 = -1$ as a critical equation

p	$\Phi(f)$	f
71	{0, 63}	{23, 26, 34, 39, 41, 51, 70 }
421	{0, 7}	{36, 51, 174, 269, 346, 388, 420}
1163	{469, 1162}	{0, 185, 253, 390, 665, 878, 1119, 1162}
2591	{2219, 2590}	{0, 211, 741, 1449, 1556, 1700, 2117, 2590}
3697	{0, 1519}	{441, 1400, 1460, 1569, 3107, 3115, 3696}
5419	{0, 4781}	{8, 254, 512, 1323, 3387, 5355, 5418}
7127	{0, 6489}	{1412, 1528, 1816, 1945, 2872, 4682, 7126}
7253	{5327, 7252}	{0, 961, 3264, 3845, 3985, 4842, 4863, 7252}
8289	{1340, 1529}	{0, 846, 2006, 3274, 4257, 6719, 7556, 8218}
9227	{7077, 9226}	{0, 1340, 2287, 3665, 5488, 6891, 8011, 9226}
9857	{0, 1421}	{292, 1798, 3449, 7262, 8163, 8608, 9856}
11173	{0, 1883}	{962, 1315, 1915, 2590, 6873, 8692, 11172}
13217	{10638, 10785}	{0, 1938, 3346, 4999, 6068, 11001, 12300, 13216}
17627	{0, 17367}	{2848, 5405, 5587, 11541, 12558, 14943, 17626}
18341	{0, 16247}	{1469, 4610, 5119, 5128, 6277, 14080, 18340}
20231	{0, 14091}	{6032, 10545, 12782, 12963, 19055, 19548, 20230}
21799	{0, 12887}	{10602, 11101, 14903, 15039, 16207, 19345, 21798}
24697	{0, 16163}	{15651, 15742, 19810, 23831, 23927, 24525, 24696}
26153	{24339, 26152}	{0, 4239, 5686, 10112, 13615, 20665, 24143, 26152}

Table 10: Cycles of length 2, with $x^7 = -1$ as a critical equation

p	$\Phi(f)$	f
7793	{0, 2501, 3578, 3609, 3789, 4004, 4184, 4215, 5292}	{4473, 5825}
10529	{0, 543, 967, 2831, 4192, 6337, 7698, 9562, 9986}	{1445, 1469}
18257	{0, 2541, 6151, 7545, 8507, 9750, 10712, 12106, 15716}	{5429, 9581}

Table 11: Cycles of length 2, with $x^8 = -1$ as a critical equation

p	$\Phi(f)$	f
397	{35, 85, 93, 111, 201, 318, 363, 383, 396}	{0, 81}
1999	{0, 461, 674, 809, 864, 1130, 1191, 1372, 1496, 1998}	{13, 490}
2953	{0, 407, 653, 770, 801, 1776, 2153, 2581, 2672, 2952}	{2907, 2952}
5563	{0, 712, 1004, 1780, 2510, 2779, 4166, 4450, 4852, 5562}	{4413, 5448}
7489	{1613, 2468, 2612, 3151, 3264, 4403, 5022, 7424, 7488}	{0, 4509}
13159	{0, 304, 1447, 3947, 4194, 7518, 10740, 11631, 12856, 13158}	{6986, 12737}
13249	{0, 3209, 3252, 4544, 5453, 7255, 8796, 10041, 10447, 13248}	{5751, 13248}
14779	{6689, 6874, 7411, 8091, 10622, 10781, 11366, 12062, 14778}	{0, 5049}
16741	{0, 4821, 5200, 6180, 6720, 8818, 10562, 11208, 13456, 16740}	{625, 15916}
20089	{0, 3661, 5934, 8166, 11924, 16531, 16795, 17713, 19722, 20088}	{3263, 16826}
20431	{5207, 5927, 8792, 9297, 9352, 11640, 11991, 19519, 20430}	{0, 13491}
22159	{0, 3520, 7105, 7143, 7911, 9728, 15254, 18640, 19336, 22158}	{922, 3595}
27361	{287, 2429, 9935, 10669, 14263, 21560, 23227, 27075, 27360}	{0, 27351}

Table 12: Cycles of length 2, with $x^9 = -1$ as a critical equation

p	$\Phi(f)$	f
1021	{0, 226, 250, 374, 384, 486, 535, 637, 647, 771, 795}	{381, 731}
7561	{0, 1151, 2923, 3071, 3186, 3602, 3959, 4375, 4490, 4638, 6410}	{1390, 6540}
26681	{0, 231, 2199, 2915, 8833, 12503, 14178, 17848, 23766, 24482, 26450}	{13634, 24004}

Table 13: Cycles of length 2, with $x^{10} = -1$ as a critical equation

p	$\Phi(f)$	f
2311	{41, 592, 630, 808, 1149, 1422, 1537, 1691, 1784, 1902, 2310}	{0, 517}
17579	{0, 2602, 6197, 7306, 7550, 7948, 8222, 9787, 10266, 12928, 15090, 17578}	{6806, 8599}

Table 14: Cycles of length 2, with $x^{11} = -1$ as a critical equation

p	$\Phi(f)$	f
3217	{452, 633, 762, 1032, 1085, 1423, 1794, 2132, 2185, 2455, 2584, 2765}	{0, 204, 3012, 3216}
9049	{0, 413, 747, 1468, 2215, 3513, 3926, 5123, 5536, 6834, 7581, 8302, 8636 }	{2817, 8373}
10993	{0, 395, 831, 2286, 3117, 5265, 5333, 5660, 5728, 7876, 8707, 10162, 10598}	{884, 10952}
25153	{0, 47, 583, 2628, 3211, 5044, 5091, 20062, 20109, 21942, 22525, 24570, 25106}	{164, 10712}

Table 15: Cycles of length 2, with $x^{12} = -1$ as a critical equation

p	$\Phi(f)$	f
6761	{592, 1108, 1534, 2838, 3393, 4100, 4607, 4868, 5091, 6122, 6433, 6642, 6760}	{0, 247}
7333	{1774, 1856, 2316, 2638, 3752, 3868, 3900, 5229, 5975, 6114, 6604, 7306, 7332}	{0, 559}
7411	{188, 1711, 2720, 3444, 3875, 4416, 4696, 5189, 5853, 6079, 6472, 7235, 7410}	{0, 1963}
14821	{0, 664, 2092, 3734, 3805, 4086, 5469, 7871, 8506, 10552, 13638, 13960, 14550, 14820}	{265, 11978}
20749	{208, 515, 576, 4512, 4686, 14343, 14595, 15462, 15958, 17283, 17374, 18983, 20748}	{0, 12493}

Table 16: Cycles of length 2, with $x^{13} = -1$ as a critical equation

p	$\Phi(f)$	f
78877	{0, 628, 9860, 16176, 21994, 23352, 26295, 34597, 44280, 52582, 55525, 56883, 62701, 69017, 78249}	{16105, 27375}

Table 17: Cycles of length 2, with $x^{14} = -1$ as a critical equation

p	$\Phi(f)$	f
23071	{0, 1449, 2238, 3471, 6829, 9814, 10149, 11473, 12771, 13397, 13529, 14321, 18292, 20834, 22931, 23070}	{2900, 21305}

Table 18: Cycles of length 2, with $x^{15} = -1$ as a critical equation

p	$\Phi(f)$	f
15329	{0, 631, 1494, 1525, 2719, 4463, 4640, 6453, 6744, 8585, 8876, 10689, 10866, 12610, 13804, 13835, 14698}	{2208, 14640}

Table 19: Cycles of length 2, with $x^{16} = -1$ as a critical equation

p	$\Phi(f)$	f
9181	{0, 347, 585, 635, 739, 2103, 2633, 4449, 4739, 4946, 5021, 6653, 7786, 8125, 8147, 8168, 8373, 9180}	{3673, 8960}
14723	{0, 191, 1817, 2303, 3031, 3892, 4181, 6305, 7501, 7688, 9999, 10163, 11186, 11194, 11504, 13032, 13798, 14722}	{2975, 14722}

Table 20: Cycles of length 2, with $x^{17} = -1$ as a critical equation

p	$\Phi(f)$	f
7669	{379, 746, 943, 2292, 2642, 2671, 2751, 3497, 3585, 4084, 4172, 4918, 4998, 5027, 5377, 6726, 6923, 7290}	{0, 2070, 5598, 7668}
16417	{713, 870, 1453, 3846, 4559, 6180, 6341, 7050, 7794, 8623, 9367, 10076, 10237, 11858, 12571, 14964, 15547, 15704}	{0, 558, 15858, 16416}
19477	{0, 2660, 3452, 4542, 4834, 5909, 7562, 7994, 8734, 9255, 10222, 10743, 11483, 11915, 13568, 14643, 14935, 16025, 16817}	{11719, 15517}

Table 21: Cycles of length 2, with $x^{18} = -1$ as a critical equation

p	$\Phi(f)$	f
85159	{0, 863, 9617, 10123, 21662, 23002, 25591, 32848, 35228, 40674, 46111, 56307, 58585, 58588, 59985, 60619, 69005, 76480, 81144, 85158}	{14611, 85158}

Table 22: Cycles of length 2, with $x^{19} = -1$ as a critical equation

p	$\Phi(f)$	f
20641	{0, 1453, 3803, 3821, 3864, 4295, 6672, 7633, 8353, 9900, 10073, 10568, 10741, 12288, 13008, 13969, 16346, 16777, 16820, 16838, 19188}	{14768, 20028}

Table 23: Cycles of length 2, with $x^{20} = -1$ as a critical equation

p	$\Phi(f)$	f
883	{0, 27, 45, 75, 125, 134, 151, 154, 157, 176, 257, 269, 338, 546, 551, 556, 587, 624, 684, 797, 812, 882}	{777, 882}
8317	{0, 1032, 1287, 1578, 1636, 2536, 2703, 4434, 4749, 4901, 4979, 5016, 6062, 6717, 6779, 6986, 7031, 7221, 7869, 8012, 8277, 8316}	{3885, 8316}
14449	{4, 64, 903, 1024, 1935, 2062, 4094, 6201, 6709, 7708, 7736, 8184, 10353, 10611, 10837, 12403, 12515, 12522, 14193, 14433, 14448}	{0, 2625}

Table 24: Cycles of length 2, with $x^{21} = -1$ as a critical equation

p	$\Phi(f)$	f
67189	{0, 3362, 4911, 8073, 10784, 12119, 16486, 17127, 18290, 26123, 27122, 32878, 34311, 40067, 41066, 48899, 50062, 50703, 55070, 56405, 59116, 62278, 63827}	{36783, 44857}

Table 25: Cycles of length 2, with $x^{22} = -1$ as a critical equation

p	$\Phi(f)$	f
63803	{3453, 6827, 7165, 7952, 8049, 14819, 16043, 21446, 22245, 24190, 24911, 31401, 32064, 33479, 37447, 40837, 45016, 47663, 48328, 52564, 53860, 58272, 63802}	{0, 42205}
68449	{2404, 2434, 4836, 5470, 5956, 6556, 6603, 10586, 13813, 14284, 22662, 30707, 33575, 35278, 36843, 38949, 51095, 55520, 56066, 59762, 60777, 61866, 68448}	{0, 63365}
71347	{0, 5016, 6830, 12038, 12698, 16413, 16596, 19302, 19703, 23030, 25235, 30612, 38097, 43551, 44061, 48301, 51496, 56694, 58627, 60299, 62165, 63660, 70394, 71346}	{976, 60569}

Table 26: Cycles of length 2, with $x^{23} = -1$ as a critical equation

References

[1] Norman L. Biggs. *Discrete Mathematics*. Oxford University Press, Second Edition, 2009.

[2] Keith Conrad. *Cyclicity of* $(Z/(p))^x$.
`https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf`