Journal of Integer Sequences, Vol. 9 (2006),
Article 06.3.3

Sequences of Reducible $\{0,1\}$–Polynomials Modulo a Prime

Judith Canner
Department of Statistics
North Carolina State University
Raleigh, North Carolina 27695-8203
USA
jecanner@ncsu.edu

Lenny Jones and Joseph Purdom
Department of Mathematics
Shippensburg University
Shippensburg, Pennsylvania 17257
USA
lkjone@ship.edu
jp9506@ship.edu

Abstract

Construct a recursive sequence of polynomials, staring with 1, in the following way. Each new term in the sequence is determined by adding the smallest power of x larger than the degree of the previous term, such that the new polynomial is reducible over the rationals. Filaseta, Finch and Nicol have shown that this sequence is finite. In this paper we investigate variations of this problem over a finite field. In particular, we allow the starting polynomial to be any $\{0,1\}$–polynomial with nonzero constant term, and we allow the exponent on the power of x added at each step to be chosen from the set of multiples of a fixed positive integer k. Among our results, we show that these sequences are always infinite. We develop necessary and sufficient conditions on k and the characteristic p of the field, so that the sequence starting with 1 uses every multiple of k as an exponent in its construction. In addition, we prove for $k = 1$ and $p \geq 5$ that there exists a $\{0,1\}$–polynomial f such that the sequence starting with f uses every positive integer larger than the degree of f as an exponent in its construction.

1 Introduction

The following problem [1] provided the motivation for this paper.

> *Define a sequence of $\{0,1\}$–polynomials (polynomials all of whose coefficients are either 0 or 1) in $\mathbb{Q}[x]$ by*
>
> $$f_1 := 1 \quad \text{and} \quad f_i := f_{i-1} + x^n, \quad \text{for} \quad i \geq 2,$$
>
> *where n is the smallest integer larger than the degree of f_{i-1} such that $f_{i-1} + x^n$ is reducible over $\mathbb{Q}$. Is this sequence infinite?*

The first eight terms of this sequence are given below:

$f_1 = 1$
$f_2 = 1 + x^3$
$f_3 = 1 + x^3 + x^{15}$
$f_4 = 1 + x^3 + x^{15} + x^{16}$
$f_5 = 1 + x^3 + x^{15} + x^{16} + x^{32}$
$f_6 = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33}$
$f_7 = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34}$
$f_8 = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}$.

Filaseta, Finch and Nicol [1] have proven the somewhat surprising fact that $f_8 + x^n$ is irreducible over $\mathbb{Q}$ for all $n \geq 36$, so that this sequence is actually finite and terminates at f_8.

In this paper we consider variations of this problem modulo a prime. Specifically, let p be a prime, let $k \geq 1$ be an integer and let $f(x)$ be a polynomial, with $f(0) \not\equiv 0 \pmod{p}$. Define a sequence of polynomials in $\mathbb{F}_p[x]$, denoted (f, k, p), as follows:

$$f_1 := f \quad \text{and} \quad f_i := f_{i-1} + x^{kn}, \quad \text{for} \quad i \geq 2,$$

where kn is the smallest integer multiple of k larger than the degree of f_{i-1}, such that $f_{i-1} + x^{kn}$ is reducible over $\mathbb{F}_p$.

We impose the restriction that $f(0) \not\equiv 0 \pmod{p}$ to avoid the trivial situation, and we do not require that f be reducible or irreducible over $\mathbb{F}_p$.

Although we show that all sequences (f, k, p) are infinite (see Theorem 4.1), this particular attribute is but one item of interest to us here (see Section 2). Also, while our definition of the sequence (f, k, p) does not require that f be a $\{0,1\}$–polynomial, the predominate focus of this paper is on sequences where f is a $\{0,1\}$–polynomial. The main reason for this is that in many situations of interest, even if f is not a $\{0,1\}$–polynomial, there is a corresponding $\{0,1\}$–polynomial g, such that the sequence (g, k, p) has many of the same properties as the sequence (f, k, p) (see Lemma 4.1).

2 Preliminaries

As one might expect, many patterns emerge modulo a prime that are not present in the characteristic zero situation. Because of the existence of these patterns, we are motivated to define the following:

Definition 2.1. Let p be a prime and let $\mathbb{F}_{p^m}$ denote the finite field with p^m elements. Let (f,k,p) be a sequence as defined in Section 1, allowing the possibility that f is not necessarily a $\{0,1\}$–polynomial, but as always, $f(0) \not\equiv 0 \pmod{p}$.

- We say (f,k,p) has the *root pattern* $[r_1, r_2, \ldots, r_t]$ in $\mathbb{F}_{p^m}$ if $r_i \in \mathbb{F}_{p^m}$ and $f_{N+b}(r_i) \equiv 0 \pmod{p}$ for some positive integer N and all positive integers $b \equiv i \pmod{t}$.
- We define $\mathcal{M}$ to be the set of all positive integer multiples of k greater than the degree of f which are not the degree of any term of (f,k,p).
- We say (f,k,p) has the *factor pattern* $[g_1, g_2, \ldots, g_t]$ in $\mathbb{F}_p[x]$ if the polynomial g_i is a proper divisor of f_{N+b} in $\mathbb{F}_p[x]$ for some positive integer N and all positive integers $b \equiv i \pmod{t}$.
- If the sequence (f,k,p) has the root pattern $[r_1, r_2, \ldots, r_j]$ (respectively, factor pattern $[g_1, g_2, \ldots, g_j]$), then we say the root pattern (respectively, factor pattern) has *period* t, if t is the smallest integer such that $r_i = r_{t+i}$ (respectively, $g_i = g_{t+i}$) for all $i = 1, 2, \ldots, t$. Throughout the remainder of this paper, we indicate all root and factor patterns as $[r_1, r_2, \ldots, r_t]$ or $[g_1, g_2, \ldots, g_t]$, where t is the period of the pattern.

We consider the root patterns $[r_i, r_{i+1}, \ldots, r_t, r_1, \ldots, r_{i-1}]$, for any $2 \le i \le t$, to be equivalent to the root pattern $[r_1, r_2, \ldots, r_t]$. In the event of the occurrence of multiple roots, a sequence (f,k,p) can sometimes have more than one root pattern (see Example 3.4).

Factor patterns and root patterns are related in the following way. Suppose that (f,k,p) has a factor pattern $[g_1, g_2, \ldots, g_t]$ in $\mathbb{F}_p[x]$, with δ_i the degree of g_i, and $m=\mathrm{lcm}(\delta_1, \delta_2, \ldots, \delta_t)$. Let g be a polynomial of degree m which is irreducible over $\mathbb{F}_p$. Then (f,k,p) has a root pattern in $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^m}$, where $g(\alpha) \equiv 0 \pmod{p}$. (see Example 3.6). Conversely, if (f,k,p) has a root pattern in $\mathbb{F}_{p^m}$, then (f,k,p) has a factor pattern in $\mathbb{F}_{p^h}[x]$ for all h with $1 \le h \le m$.

Although the proofs of some of our results use arguments which involve both root patterns and factor patterns, we choose to state our results only in terms of root patterns. Because of the connection between root patterns and factor patterns, analogous statements can be made in terms of factor patterns. While it seems plausible that when the sequence (f,k,p) has a root pattern in $\mathbb{F}_p$, or a factor pattern in $\mathbb{F}_p[x]$, then $\mathcal{M}$ is not infinite (Question 5.1), the converse is false (see Example 3.1 and Theorem 4.3).

When $\mathcal{M}$ is finite for a sequence (f,k,p), we can use $\mathcal{M}$ to construct a polynomial $\hat{f}$ such that $\mathcal{M}$ is empty for the sequence $(\hat{f},k,p)$. Explicitly, if $\mathcal{M} = \{km_1, km_2, \ldots, km_s\}$ for the sequence (f,k,p), where the degree of f is kd, then let $\hat{f}(x) = f(x) + \sum_{j=d+1}^{m_s+1} a_j x^{kj}$ be the polynomial of degree $k(m_s+1)$ such that $a_j = 0$ when $kj \in \mathcal{M}$, and $a_j = 1$ otherwise. Then $\mathcal{M}$ is empty for the sequence $(\hat{f},k,p)$, since this sequence starts by adding powers of

x whose exponents are larger than the elements of $\mathcal{M}$. A similar technique is used in the proofs of Lemma 4.1 and Theorem 4.5. See also Example 4.6.

The first main result of this article is Theorem 4.1, where we see that the situation over $\mathbb{F}_p$ is quite different than it is over $\mathbb{Q}$, in that no sequence (f, k, p) is ever finite. Next, Theorem 4.2 shows that no root patterns exist in $\mathbb{F}_p$ for the sequences $(f, k, 2)$ and $(f, k, 3)$. Then, for the sequences $(1, k, p)$, we establish in Theorem 4.3, necessary and sufficient conditions on k and p so that $\mathcal{M}$ is empty, and in these situations we show that no root patterns exist in $\mathbb{F}_{p^m}$ for any m. Finally, for $p \geq 5$, we prove in Theorem 4.5 that there exists a $\{0,1\}$–polynomial f such that the sequence $(f, 1, p)$ has a root pattern in $\mathbb{F}_p$ with $\mathcal{M}$ empty.

Throughout this paper we let $|a|_{p^m}$ denote the order of a in $(\mathbb{F}_{p^m})^*$, the multiplicative group of $\mathbb{F}_{p^m}$, and we let $\Phi_n := \Phi_n(x)$ denote the n-th cyclotomic polynomial.

Lemma 2.1, Lemma 2.2 and Lemma 2.3 are stated without proof since they contain information which is well-known.

Lemma 2.1.

- *There exists a primitive root modulo m if and only if $m = 2,\ 4,\ q^a$, or $2q^a$, where q is an odd prime and $a \geq 1$ is an integer.*
- *Let q be an odd prime. If α is a primitive root modulo q^a for some $a \geq 2$, then α is a primitive root modulo q^a for all $a \geq 1$.*

Lemma 2.2.

- *If p is a prime that divides n, then $\Phi_n(x^p) = \Phi_{pn}(x)$.*
- *$\Phi_n(x^k)$ is irreducible over $\mathbb{Q}$ if and only if every prime divisor of k divides n.*
- *Let n and k be relatively prime. Then $\Phi_n(x^k) = \prod_{d|k} \Phi_{dn}(x)$.*

Lemma 2.3. *Let p be a prime, and let $g(x)$ be a polynomial over $\mathbb{F}_p$. If $g(x)$ is irreducible modulo p, then $g(x)$ divides $x^{p^m} - x$, where m is any multiple of the degree of $g(x)$.*

In the investigation of the reducibility over $\mathbb{Q}$ of certain polynomials, it is sometimes fruitful, and more efficient, to first test for divisibility by cyclotomic polynomials [2]. Cyclotomic polynomials also play a role here in determining the reducibility of certain $\{0,1\}$–polynomials over $\mathbb{F}_p$. A slight adjustment is required since cyclotomic polynomials do not always remain irreducible modulo a prime. Theorem 2.2 describes explicitly the factorization of cyclotomic polynomials in $\mathbb{F}_p[x]$.

Theorem 2.2. [3] *Let p be a prime, and let $n = p^a m$ be a positive integer, where p does not divide m. Let b be the smallest positive integer such that $p^b \equiv 1 \pmod{m}$. Then $\Phi_n(x)$ factors as the product of $\dfrac{\phi(m)}{b}$ incongruent irreducible monic polynomials modulo p, each of degree b, and each raised to the $\phi(p^a)$ power.*

We also make use of the following immediate corollary of Theorem 2.2 in the proof of Theorem 4.3.

Corollary 2.1. *Let p be a prime, and let $n = p^a m$ be a positive integer, where p does not divide m. Then $\Phi_n(x)$ is irreducible modulo p if and only if p is a primitive root modulo m, and either $a = 0$, or $p = 2$ with $a = 1$.*

Although straightforward, Lemma 2.4 provides insight into the basic understanding of root patterns for the sequences (f, k, p).

Lemma 2.4. *Let p be a prime, and let $r \in \mathbb{F}_{p^m}$, with $|r|_{p^m} = s \neq 1$. Let $k \geq 1$ be an integer, and let $a = \gcd(s, k)$. For any polynomial $g(x)$ and any $n \geq 0$, define the polynomial $h(x) := g(x) + x^{k(n+1)} + x^{k(n+2)} + \cdots + x^{k(n+b)}$, where $b = p$ if $a = s$, and $b = s/a$ otherwise. Then $g(r) \equiv 0 \pmod{p}$ if and only if $h(r) \equiv 0 \pmod{p}$.*

Proof. If $a = s$, then clearly $h(r) \equiv g(r) \pmod{p}$. Otherwise, we have

$$
\begin{aligned}
h(r) &= g(r) + r^{k(n+1)} + r^{k(n+2)} + \cdots + r^{k(n+b)} \\
&= g(r) + r^{k(n+1)}(1 + r^k + (r^k)^2 + \cdots + (r^k)^{b-1}) \\
&= g(r) + r^{k(n+1)} \left(\frac{(r^k)^b - 1}{r^k - 1} \right) \\
&= g(r) + r^{k(n+1)} \left(\frac{(r^s)^{k/a} - 1}{r^k - 1} \right) \\
&\equiv g(r) \pmod{p},
\end{aligned}
$$

and the lemma follows. □

Before we present our main results, we give some examples of sequences (f, k, p).

3 Examples of Sequences (f, k, p)

In the following examples, a computer was used to determine likely candidates for $\mathcal{M}$, and, with the exception of Example 3.1, Lemma 2.4 was used to verify this evidence by establishing the existence of any root or factor patterns.

Example 3.1. $(1, 4, 3)$

Although this example is a special case of Theorem 4.3(3), we nevertheless provide a separate analysis here to give the reader an introduction to some of the techniques used in this paper.

We claim that $f_n = 1 + x^4 + x^8 + \cdots + x^{4(n-1)}$, for $n \geq 2$. First note that $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$ over $\mathbb{F}_3$ so that $f_2 = 1 + x^4$. When $n \equiv 0, 1, 3, 5 \pmod{6}$, there exists an odd prime q that divides n, and it is easy to show then that Φ_q is a proper divisor of $1+x^4+x^8+\cdots+x^{4(n-1)}$. Similarly, when $n \equiv 2,4 \pmod 6$, with $n>2$, we have that Φ_8 is a proper divisor of $1+x^4+x^8+\cdots+x^{4(n-1)}$, establishing the claim, and proving that $\mathcal{M}$ is empty. The observation that f_n has a zero modulo 3 if and only if $n \equiv 0 \pmod 3$ proves that $(1,4,3)$ has no root pattern in $\mathbb{F}_3$.

Example 3.2. $(1+x,1,5)$

First note that $1+x+x^2$ and $1+x+x^3$ are irreducible over $\mathbb{F}_5$. But $f_2=1+x+x^4$, $f_3=1+x+x^4+x^5$, $f_4=1+x+x^4+x^5+x^6$ and $f_5=1+x+x^4+x^5+x^6+x^7$, since, modulo 5, they have the respective zeros: 3,4,2,4. Thus, by Lemma 2.4, $(1+x,1,5)$ has the root pattern $[3,4,2,4]$ in $\mathbb{F}_5$, and $\mathcal{M}=\{2,3\}$.

Example 3.3. $(1,1,5)$

While this sequence has the same root pattern $[3,4,2,4]$ in $\mathbb{F}_5$ as the sequence $(1+x,1,5)$ in Example 3.2, we see that the pattern does not emerge as soon in this sequence since here $\mathcal{M}=\{1,3,12,25,36,37,49,323,1985,4054,5885,6648\}$.

Example 3.4. $(1,1,7)$

There are, in fact, two root patterns for this sequence in $\mathbb{F}_7$: $[4,2,3,4,2,6]$ and $[4,6,3,6,2,6]$. Here, $\mathcal{M}=\{1,2,4,17,36,41\}$.

Example 3.5. $(1+x,1,17)$

This sequence has the root pattern $[8,16,9,4,2,16,15,4]$ in $\mathbb{F}_{17}$, and $\mathcal{M}=\{2,5,8,11,24\}$.

Example 3.6. $(1+x+x^2+x^5+x^6+x^8+x^{10},1,3)$

This sequence has the root pattern $[2,\alpha,2,\alpha+1,2,\alpha,2,\alpha+2]$ in $\mathbb{F}_9$, where $\alpha^2+1=0$. The corresponding factor pattern in $\mathbb{F}_3$ is given by $[g_1,g_2,\ldots,g_8]$, where

$$\begin{aligned} g_1 &= g_3 = g_5 = g_7 = x-2 \\ g_2 &= g_6 = x^2+1 \\ g_4 &= x^2+x+2 \quad \text{and} \\ g_8 &= x^2+2x+2. \end{aligned}$$

Here, $\mathcal{M}$ is empty.

4 Main Results

Theorem 4.1. *Every sequence (f,k,p) is infinite.*

Proof. For any prime p, positive integer k, and polynomial $h(x)\in\mathbb{F}_p[x]$, we claim that there exists a positive integer t, with t divisible by k and larger than the degree of $h(x)$, such that $h(x)+x^t$ is reducible modulo p.

Suppose that p^s is the exact power of p that divides k, and let $L=k/p^s$. Let $a=p^{sv}(k-1)$, where $v=1$ if $L=1$, and v is the order of p^s modulo L, otherwise. Let $g(x)$ be an irreducible factor of $h(x)+x^{a+1}$, and let $m>s$ be a multiple of the degree of $g(x)$ with p^m+a larger than the degree of $h(x)$, such that L divides p^m-1. Note that p^s divides p^m+a since $m>s$

and $v \geq 1$. Also, L divides $p^m + a$ by the choices of m and v. Hence, k divides $p^m + a$. By Lemma 2.3, $g(x)$ divides $x^{p^m} - x$. Since $g(x)$ divides $h(x) + x^{a+1}$, it follows that $g(x)$ divides

$$h(x) + x^{a+1} + x^a \left(x^{p^m} - x\right) = h(x) + x^{p^m + a},$$

establishing the claim with $t = p^m + a$, and completing the proof of the theorem. □

Theorem 4.2. *Let $p = 2$ or 3. Then the sequence (f, k, p) does not have a root pattern in $\mathbb{F}_p$.*

Proof. The only possible root patterns are [1], if $p = 2$, and [1], [2] and [1, 2] if $p = 3$. Since the arguments are similar for each of these cases, we show only that the root pattern [1, 2] is impossible when $p = 3$. If [1, 2] is the root pattern for the sequence $(f, k, 3)$, then, for some index i, it follows that

$$0 \equiv f_i(1) \equiv f_{i+2}(1) = f_i(1) + 1 + 1 \equiv 2 \pmod 3,$$

which is impossible. □

Theorem 4.3.

1. *If $k = 1$, then $\mathcal{M}$ is never empty for the sequence $(1, k, p)$ for any prime p.*
2. *If $k = 2$, then $\mathcal{M}$ is empty for the sequence $(1, k, p)$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*
3. *If $k \geq 3$, then $\mathcal{M}$ is empty for the sequence $(1, k, p)$ if and only if $k \neq q^a$, where $a \geq 1$, and $q \geq 3$ is a prime such that p is a primitive root modulo q^2.*

Moreover, in each case that $\mathcal{M}$ is empty, the sequence $(1, k, p)$ has no root pattern in $\mathbb{F}_{p^m}$ for any m.

Proof. We first establish parts (1), (2) and (3) of the theorem, and then show that when $\mathcal{M}$ is empty, the sequence $(1, k, p)$ has no root pattern in $\mathbb{F}_{p^m}$ for any m. Throughout the proof, for $n \geq 2$, we let $g_n := g_n(x) = 1 + x^k + x^{2k} + \cdots + x^{(n-1)k}$.

When $k = 1$, we have that $1 \in \mathcal{M}$, since $1 + x$ is irreducible for all primes p. So, statement (1) of the theorem is obvious.

Making use of the fact that $\Phi_n(x^k)$ divides $g_n(x)$, we prove statements (2) and (3) of the theorem by determining exactly when $f_n = g_n$ for all $n \geq 2$, or equivalently, when $g_n(x)$ is reducible over $\mathbb{F}_p$ for all $n \geq 2$. First note that

$$\deg\left(\Phi_n\left(x^k\right)\right) = \phi(n)k \leq (n-1)k = \deg\left(g_n\left(x\right)\right).$$

Therefore, since $\Phi_n(x^k)$ divides $g_n(x)$ for all $n \geq 2$, it follows that $g_n(x)$ is reducible over $\mathbb{Q}$, and hence over $\mathbb{F}_p$, except possibly when n is a prime q. Also, by Lemma 2.2, $\Phi_q\left(x^k\right)$ is reducible over $\mathbb{Q}$, and hence over $\mathbb{F}_p$, if there exists a prime divisor r of k with $r \neq q$. Thus, for $k \geq 2$, we have that $\mathcal{M}$ is empty when $k \neq q^a$, for some prime q with $a \geq 1$. Consequently, our focus is narrowed to the examination of when $\Phi_q\left(x^{q^a}\right) = \Phi_{q^{a+1}}\left(x\right)$, with $a \geq 1$, is reducible over $\mathbb{F}_p$.

If $k = q = 2$, then $a = 1$, and $\Phi_{q^{a+1}}(x) = \Phi_4(x) = x^2 + 1$, which is easily seen to be reducible over $\mathbb{F}_p$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Combining this fact with the above discussion completes the proof of statement (2) of the theorem.

When $k = 2^a$, with $a \geq 2$, we have immediately, from Lemma 2.1 and Corollary 2.1, that $\Phi_{2^{a+1}}(x)$ is reducible over $\mathbb{F}_p$ for all primes p. When $k = q^a$, for some prime $q \geq 3$, with $a \geq 1$, we appeal again to Lemma 2.1 and Corollary 2.1 to conclude that $\Phi_{q^{a+1}}(x)$ is irreducible over $\mathbb{F}_p$ if and only if p is a primitive root modulo q^2. Therefore, statement (3) of the theorem has been established.

We now show that when $\mathcal{M}$ is empty, the sequence $(1, k, p)$ has no root pattern in $\mathbb{F}_{p^m}$ for all m. We do this by showing that $(1, k, p)$ has no factor pattern in $\mathbb{F}_p[x]$. Note that under the assumption that $\mathcal{M}$ is empty, we have that $f_n = g_n$ for all $n \geq 2$, so we use the notation g_n. Let $q > p$ be prime. For any divisor d of k, we can write $dq = p^a q m_d$, where p does not divide m_d. Let b be the smallest positive integer such that $p^b \equiv 1 \pmod{qm_d}$. Since

$$p^b > p^b - 1 \geq q m_d \geq q,$$

we have that $b > \log(q)/\log(p)$. Therefore, from Theorem 2.2, each irreducible factor of $\Phi_{dk}(x)$ modulo p has degree larger than $\log(q)/\log(p)$, and this is independent of the divisor d. Since

$$g_q(x) = \Phi_q\left(x^k\right) = \prod_{d|k} \Phi_{dq}(x),$$

it follows that, as q approaches infinity, the minimum degree of an irreducible factor of g_q also approaches infinity, proving the impossibility of the existence of a factor pattern for $(1, k, p)$ in $\mathbb{F}_p[x]$. $\square$

The following lemma, which is needed for the proof of Theorem 4.5, indicates in certain situations how a sequence whose terms are not all $\{0,1\}$–polynomials can be used to construct a sequence where all terms are $\{0,1\}$–polynomials, and such that the two sequences share particular properties.

Lemma 4.1. *Let p be a prime and let $g(x) = 1 + \sum_{i=1}^{d} a_i x^i$ be a polynomial of degree $d \leq p-1$ that is not a $\{0,1\}$–polynomial in $\mathbb{F}_p[x]$. Suppose that the sequence $(g, 1, p)$ has a root pattern in $\mathbb{F}_p$ and that $\mathcal{M}$ is empty. Then there exists a $\{0,1\}$–polynomial $f(x)$ of degree at most $p^2 - 3p + d + 3$, such that the sequence $(f, 1, p)$ has a root pattern equivalent to $(g, 1, p)$ in $\mathbb{F}_p$, and $\mathcal{M}$ is empty.*

Proof. The following two-step algorithm, which incorporates Fermat's Little Theorem, is used to construct $f(x)$.

1. Replace every non-constant term $a_i x^i$ of $g(x)$ with $\sum_{j=0}^{a_i - 1} x^{i+j(p-1)}$. Since $1 \leq i \leq p-1$, we have that no two exponents of the resulting polynomial are the same. That is, this step produces a $\{0,1\}$–polynomial $g_1(x)$ such that $g_1(x) \equiv g(x) \pmod p$ for all $x \in \mathbb{F}_p$, and the degree of $g_1(x)$ is $d_1 = \max\limits_{1 \leq i \leq d} \{i + (a_i - 1)(p-1)\}$.

2. Define $f(x)$ to be $g_1(x)+x^{d+1+c(p-1)}$, where c is the smallest positive integer such that $d+1+c(p-1)>d_1$.

Then, if the root pattern for the sequence $(g,1,p)$ is $[r_1,r_2,\ldots,r_t]$, this definition of $f(x)$ guarantees that the sequence $(f,1,p)$ has the equivalent root pattern $[r_2,r_3,\ldots,r_t,r_1]$, and that $\mathcal{M}$ is empty. Since $d_1\le d+(p-2)(p-1)$, it follows that the degree of $f(x)$ is at most $d+1+(p-2)(p-1)=p^2-3p+d+3$. □

We give an example to illustrate Lemma 4.1.

Example 4.4. Let $p=7$, $k=1$ and $g(x)=6x^4+4x^3+6x^2+2x+1$. Then $(g,1,7)$ has the root pattern $[2,6,4,6,3,6]$ in $\mathbb{F}_7$, which begins with the addition of x^5. Using Lemma 4.1, we get $f(x)=x^{35}+x^{34}+x^{32}+x^{28}+x^{26}+x^{22}+x^{21}+x^{20}+x^{16}+x^{15}+x^{14}+x^{10}+x^9+x^8+x^7+x^4+x^3+x^2+x+1$. The sequence $(f,1,7)$, with the equivalent root pattern $[6,4,6,3,6,2]$ in $\mathbb{F}_7$, has $\mathcal{M}$ empty, and is constructed by adding consecutively x^{36}, x^{35}, …, instead of, respectively x^5, x^6, …, for the sequence $(g,1,7)$. Note that the sequence $(f-x^{35},1,7)$ has $\mathcal{M}$ empty, and has the exact same root pattern as $(g,1,7)$, beginning with the addition of x^{35}.

Theorem 4.5. *For any prime $p\ge 5$, there exists a $\{0,1\}$–polynomial $f(x)$, with $f(0)=1$, such that the sequence $(f,1,p)$ has a root pattern in $\mathbb{F}_p$, and $\mathcal{M}$ is empty. Moreover, if $p\equiv 3 \pmod 4$, then f can be found whose degree is at most $p^2-3p+q+5$, where q is the smallest odd prime factor of $p-1$, and the period of the root pattern is $2q$; while if $p\equiv 1 \pmod 4$, then f can be found such that the degree of f is at most $2p-6$, and the period of the root pattern is 4.*

Remark. The proof of Theorem 4.5 is constructive, and although the technique we use to construct f when $p\equiv 3 \pmod 4$ can be modified slightly to construct f when $p\equiv 1 \pmod 4$, we use a different approach in the latter case since the alternative approach has two distinct advantages. The first advantage is that the construction of the polynomial f requires fewer computations, while the second advantage is that the upper bound on the degree of f is significantly less.

Proof. Suppose first that $p\equiv 3 \pmod 4$, and let q be the smallest odd prime factor of $p-1$. Let $\beta\in\mathbb{F}_p$ with $|\beta|_p=2q$. Then

$$|\beta^2|_p=|\beta^4|_p=\cdots=|\beta^{2q-2}|_p=q \quad\text{and}\quad |\beta^q|_p=2.$$

If we can demonstrate the existence of a polynomial $g(x)=1+\sum_{i=1}^{q+1}a_ix^i$, with $a_{q+1}\not\equiv 0 \pmod p$, satisfying all of the following conditions:

$$
\begin{aligned}
g(\beta^q) + (\beta^q)^{q+2} &\equiv 0 \pmod p \\
g(\beta^2) + (\beta^2)^{q+2} + (\beta^2)^{q+3} &\equiv 0 \pmod p \\
g(\beta^4) + (\beta^4)^{q+2} + (\beta^4)^{q+3} + (\beta^4)^{q+4} + (\beta^4)^{q+5} &\equiv 0 \pmod p \\
\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad &\vdots \\
g(\beta^{2q-2}) + (\beta^{2q-2})^{q+2} + \cdots + (\beta^{2q-2})^{3q-1} &\equiv 0 \pmod p \\
g(\beta) + \beta^{q+2} + \beta^{q+3} + \cdots + \beta^{3q+1} &\equiv 0 \pmod p,
\end{aligned} \tag{1}
$$

then $g(x)$ has the root pattern $[\beta^q, \beta^2, \beta^q, \beta^4, \ldots, \beta^q, \beta^{2q-2}, \beta^q, \beta]$ by Lemma 2.4, clearly $\mathcal{M}$ is empty since $a_{q+1} \not\equiv 0 \pmod p$, and using Lemma 4.1, we can construct the desired polynomial $f(x)$.

The conditions imposed on $g(x)$ in (1) give a system of $q+1$ linear equations in the $q+1$ variables $a_1, a_2, \ldots, a_{q+1}$. Thus, to show the existence of a polynomial $g(x) \in \mathbb{F}_p[x]$ satisfying (1), it suffices to show that the coefficient matrix

$$
A = \begin{bmatrix}
\beta^q & (\beta^q)^2 & (\beta^q)^3 & \ldots & (\beta^q)^{q+1} \\
\beta^2 & (\beta^2)^2 & (\beta^2)^3 & \ldots & (\beta^2)^{q+1} \\
\beta^4 & (\beta^4)^2 & (\beta^4)^3 & \ldots & (\beta^4)^{q+1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\beta^{2q-2} & (\beta^{2q-2})^2 & (\beta^{2q-2})^3 & \ldots & (\beta^{2q-2})^{q+1} \\
\beta & \beta^2 & \beta^3 & \ldots & \beta^{q+1}
\end{bmatrix}
$$

is invertible modulo p. To do this, we show that p does not divide $\det(A)$. Factor out the power of β in each row that appears in the first column of A to get that $\det(A) = \beta^{q^2+1} \det(V)$, where

$$
V = \begin{bmatrix}
1 & \beta^q & (\beta^q)^2 & \ldots & (\beta^q)^q \\
1 & \beta^2 & (\beta^2)^2 & \ldots & (\beta^2)^q \\
1 & \beta^4 & (\beta^4)^2 & \ldots & (\beta^4)^q \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \beta^{2q-2} & (\beta^{2q-2})^2 & \ldots & (\beta^{2q-2})^q \\
1 & \beta & \beta^2 & \ldots & \beta^q
\end{bmatrix}.
$$

Now, V is a Vandermonde matrix, and its determinant is well-known. Labelling the entries of the second column of V as

$$
x_1 = \beta^q, \qquad x_i = \beta^{2i-2}, \quad \text{for} \quad i = 2, 3, \ldots, q, \qquad \text{and} \qquad x_{q+1} = \beta,
$$

we have that $\det(V) = \prod_{i>j}(x_i - x_j)$. Since $|\beta|_p = 2q$, the x_i are distinct powers of β in $\mathbb{F}_p$, so that $\det(V) \not\equiv 0 \pmod{p}$, which proves the existence of a polynomial $g(x)$ satisfying (1). There is no guarantee, however, that the polynomial $g(x)$ produced here is such that $a_{q+1} \not\equiv 0 \pmod{p}$, and so it could be that $\mathcal{M}$ is not empty for the sequence $(g, 1, p)$. If, in fact, $a_{q+1} \not\equiv 0 \pmod{p}$, then, since $q+1 < p-1$, we can invoke Lemma 4.1 on $g(x)$ to produce a polynomial $f(x)$ of degree at most $p^2 - 3p + q + 4$ such that the sequence $(f, 1, p)$ has the root pattern $[\beta^2, \beta^q, \beta^4, \ldots, \beta^q, \beta^{2q-2}, \beta^q, \beta, \beta^q]$ with $\mathcal{M}$ empty. On the other hand, if $a_{q+1} \equiv 0 \pmod{p}$, we let $h(x) = g(x) + x^{q+2}$. Then the sequence $(h, 1, p)$ has the root pattern $[\beta^2, \beta^q, \beta^4, \ldots, \beta^q, \beta^{2q-2}, \beta^q, \beta, \beta^q]$ with $\mathcal{M}$ empty. Since $q+2 < p-1$, Lemma 4.1 can be applied to $h(x)$ which yields a polynomial $f(x)$ of degree at most $p^2 - 3p + q + 5$, such that the sequence $(f, 1, p)$ has the root pattern $[\beta^q, \beta^4, \ldots, \beta^q, \beta^{2q-2}, \beta^q, \beta, \beta^q, \beta^2,]$ with $\mathcal{M}$ empty, completing the proof of the theorem when $p \equiv 3 \pmod{4}$.

Now suppose that $p \equiv 1 \pmod{4}$. Let $r \in \mathbb{F}_p$ with $|r|_p = 4$. Since $r \not\equiv -1 \pmod{p}$, there exists a with $2 \le a \le p-1$ such that $a(r+1) \equiv 1 \pmod{p}$. Then the following facts are easily derived, and we make use of them in the remainder of the proof:

$$\begin{aligned} |r^3|_p = 4, \quad r^2 &\equiv (r^3)^2 \equiv -1 \pmod{p}, \\ r^3 &\equiv r^{-1} \equiv -r \equiv a(r^3+1) \pmod{p}. \end{aligned} \tag{2}$$

Define the polynomial f of degree $4a-4$ as

$$f := f(x) = x^{4a-4} + (x+1)\sum_{k=0}^{a-2} x^{4k}.$$

Then, using (2) together with the fact that $|r|_p = 4$, we have that $f(r) \equiv 1 - r \pmod{p}$, $f(r^2) \equiv 1 \pmod{p}$, $f(r^3) \equiv 0 \pmod{p}$, and consequently,

$$f(r^2) + (r^2)^{4a-3} \equiv 1 + (-1)^{4a-3} \equiv 0 \pmod{p},$$

$$f(r) + r^{4a-3} + r^{4a-2} \equiv (1-r) + (r)^{-3} + (r)^{-2} \equiv (1-r) + r + (-1) \equiv 0 \pmod{p} \quad \text{and}$$

$$\begin{aligned} f(r^3) + (r^3)^{4a-3} + (r^3)^{4a-2} + (r^3)^{4a-1} + (r^3)^{4a} &\equiv 0 + (-r)^{4a-3} + (-r)^{4a-2} + (-r)^{4a-1} + 1 \\ &\equiv -r^{-3} + r^{-2} - r^{-1} + 1 \equiv -r + (-1) - (-r) + 1 \equiv 0 \pmod{p}. \end{aligned}$$

Hence, $(f, 1, p)$ has the root pattern $[r^2, r, r^2, r^3] = [p-1, r, p-1, p-r]$ by Lemma 2.4, and $\mathcal{M}$ is empty.

We now show that f can be found with degree at most $2p - 6$. Since $r \not\equiv 1 \pmod{p}$, there exists b, with $2 \le b \le p-1$, such that $b(-r+1) \equiv 1 \pmod{p}$. Then $b(r+1) \equiv r \pmod{p}$ from (2). Since $a(r+1) \equiv 1 \pmod{p}$, we have $a(-r+1) \equiv -r \pmod{p}$ from (2), and thus

$$-r + 1 \equiv a(-r+1) + 1 \equiv a(-r+1) + a(r+1) \equiv 2a \pmod{p}. \tag{3}$$

Similarly,

$$r + 1 \equiv b(r+1) + 1 \equiv b(r+1) + b(-r+1) \equiv 2b \pmod{p}. \tag{4}$$

Combining (3) and (4), we have

$$a + b \equiv 1 \pmod{p}. \tag{5}$$

Also, from either (3) or (4), we have

$$2ab \equiv (-r+1)b \equiv 1 \pmod{p}. \tag{6}$$

Since $2 \leq a, b \leq p-1$, if both a and b are greater than or equal to $\dfrac{p+1}{2}$, then (5) implies that $a = b = \dfrac{p+1}{2}$. But then, from (6), we have $1 \equiv 2ab \equiv 2\left(\dfrac{p+1}{2}\right)^2 \pmod{p}$, so that $2 \equiv 1 \pmod{p}$, which is impossible. Hence, at least one of a and b is smaller than $\dfrac{p+1}{2}$. Therefore, we can choose r such that $a \leq \dfrac{p-1}{2}$. Then the degree of f is $4a-4 \leq 4\left(\dfrac{p-1}{2}\right)-4 = 2p-6$, which completes the proof of the theorem. □

We give two examples which illustrate Theorem 4.5.

Example 4.6. When $p = 7$, letting $\beta = 3$, the proof of the first part of Theorem 4.5 yields the polynomial $g(x) = 4x^4 + 3x^3 + 5x^2 + 6x + 1$, which in turn produces $f(x) = x^{31} + x^{26} + x^{25} + x^{22} + x^{20} + x^{19} + x^{16} + x^{15} + x^{14} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$, and $(f, 1, 7)$ has the root pattern $[6, 2, 6, 4, 6, 3]$ in $\mathbb{F}_7$. Observe that this polynomial is quite different from the polynomial in Example 4.4, and the polynomial $\hat{f}(x) = x^{42} + x^{40} + x^{39} + x^{38} + x^{37} + x^{35} + \cdots + x^{18} + x^{16} + \ldots x^5 + x^3 + 1$ constructed from Example 3.4 using the technique described in Section 2. However, for all three of these polynomials, $\mathcal{M}$ is empty, and their root patterns are equivalent.

Example 4.7. When $p = 13$, the proof of the second part of Theorem 4.5 produces the polynomial $f(x) = x^8 + x^5 + x^4 + x + 1$, and $(f, 1, 13)$ has the root pattern $[12, 8, 12, 5]$ in $\mathbb{F}_{13}$.

5 Some Open Questions

Computer evidence has led us to pose the following questions.

Question 5.1. *If the sequence (f, k, p) has a root pattern in $\mathbb{F}_{p^m}$ for some m, then must $\mathcal{M}$ be finite or empty?*

Question 5.2. *Which of the sequences $(1, 1, p)$ have $\mathcal{M}$ finite?*

Question 5.3. *If we fix any one or two of the parameters f, k and p, can we always find infinitely many values for the other parameter(s) such that the sequence (f, k, p) has $\mathcal{M}$ nonempty and finite?*

6 Acknowledgments

The authors thank Michael Filaseta for suggesting the approach used in the proof of Theorem 4.1. The authors also thank the referee for the valuable suggestions.

References

[1] Michael Filaseta, Carrie Finch and Charles Nicol, On three questions concerning $\{0,1\}$–polynomials, *J. Théorie Nombres Bordeaux*, to appear.

[2] M. Filaseta and A. Schinzel, On testing the divisibility of lacunary polynomials by cyclotomic polynomials, *Math. Comp.* **73** (2004), 957–965.

[3] W. J. Guerrier, The factorization of the cyclotomic polynomials mod p, *Amer. Math. Monthly* **75** (1968) 46.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford University Press, 1979.

[5] Ramanujachary Kumanduri and Cristina Romero, *Number Theory with Computer Applications*, Prentice Hall, 1998.

[6] Melvyn B. Nathanson, *Elementary Methods in Number Theory*, Springer-Verlag, New York, 2000.

2000 *Mathematics Subject Classification*: Primary 11R09, 11A07; Secondary 11T06, 11C08, 11B50, 11B83.
Keywords: polynomials; reducible; finite field.

Received December 19 2005; revised version received July 19 2006. Published in *Journal of Integer Sequences*, July 19 2006 .

Return to Journal of Integer Sequences home page.