FEKETE POLYNOMIALS
OF PRINCIPAL DIRICHLET CHARACTERS

SHIVA CHIDAMBARAM, JÁN MINÁČ, TUNG T. NGUYEN, NGUYỄN DUY TÂN

ABSTRACT. Fekete polynomials have a rich history in mathematics. They first appeared in the work of Michael Fekete in his investigation of Siegel zeros of Dirichlet L-functions. They also played a significant role in Gauss's original sixth proof of the quadratic reciprocity law. In recent works, we introduce and study the arithmetic of generalized Fekete polynomials associated with primitive quadratic Dirichlet characters. We show further that these polynomials possess many interesting and important properties. In this paper, we introduce and study a different incarnation of Fekete polynomials, namely those associated with principal Dirichlet characters. We then determine their cyclotomic and non-cyclotomic factors. Additionally, we investigate their modular properties and special values. Finally, based on both theoretical and numerical data, we propose a precise conjecture on the structure of the Galois group of these Fekete polynomials.

CONTENTS

Date: January 9, 2023.

2020 *Mathematics Subject Classification.* Primary 11C08, 11R09, 11M06, 11Y70.

Key words and phrases. Fekete polynomials, cyclotomic polynomials, separability, irreducibility, Galois groups.

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. He gratefully acknowledges the Western University Faculty of Science Distinguished Professorship 2020-2021. NDT is funded by Vingroup Joint Stock Company and supported by Vingroup Innovation Foundation (VinIF) under the project code VINIF.2021.DA00030.

1. Introduction

Let $\chi : (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$ be a Dirichlet character with modulus $n > 1$. We can attach to χ its L-function which is defined by the following infinite series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

This infinite series is absolutely convergent when $\Re(s) > 1$. It is also known that $L(\chi, s)$ has a meromorphic continuation to the entire complex plane with a possible simple pole at $s = 1$ in the case χ is the principal character. Furthermore, $L(\chi, s)$ has the following integral representation (see [18, Proposition 3.3]. We remark that in this cited article, χ is assumed to be primitive; however, the proof goes through without this assumption.)

$$\Gamma(s)L(\chi, s) = \int_0^1 \frac{(-\log(t))^{s-1}}{t} \frac{F_\chi(t)}{1-t^n} dt, \tag{1.1}$$

where $\Gamma(s)$ is the Gamma function and

$$F_\chi(x) = \sum_{a=0}^{n-1} \chi(a) x^a.$$

When $\chi := \left(\frac{\cdot}{p}\right)$ is the quadratic character with a prime conductor p. Michael Fekete made the observation that if $F_\chi(x)$ has no real zeroes in the interval $0 < x < 1$, then $L(s, \chi)$ has no real zero on $(0, 1)$. In other words, the study of $F_\chi(x)$ could shed some light on the existence of Siegel zeroes near $s = 1$. For this historical reason, we coin the term Fekete polynomials to these $F_\chi(x)$.

Fekete polynomials have a rich history in mathematics. As explained in the previous paragraphs, their first official appearance can be traced to the 19th century in relation to the studies of Dirichlet L-functions through the work of Michael Fekete. These polynomials also played a significant role in Gauss's original sixth proof of the quadratic reciprocity law (see [15, Chapter 10, Section 3]). There are extensive works in the literature studying various aspects of Fekete polynomials such as their extremal properties, their Mahler measure, their connections to oscillations of quadratic L-functions, the distribution of their complex roots, and much more (see [1, 3, 4, 9, 11].)

In recent works, we introduce and study the arithmetic of Fekete polynomials in the case χ is a primitive quadratic Dirichlet character (see [17, 18]). In these works, we determine cyclotomic and non-cyclotomic factors of F_χ. We also show that Fekete polynomials contain interesting arithmetic information such as the class numbers or the orders of certain K-groups of certain quadratic fields. Furthermore, our extensive numerical data suggests that F_χ has exactly one irreducible non-cyclotomic factor which we will denote by f_χ. What is more, the Galois group of f_χ seems to be as large as possible (see [17, Conjecture 4.9, Conjecture 4.13] and [18, Conjecture 11.16]).

In this article, we consider a somewhat orthogonal situation; namely the case $\chi_n : (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$ is the principal Dirichlet character. More concretely, χ_n is defined by the following formula

$$\chi_n(a) = \begin{cases} 0 & \text{if } \gcd(a,n) > 1 \\ 1 & \text{if } \gcd(a,n) = 1. \end{cases}$$

For simplicity, we will denote $F_n(x) = F_{\chi_n}(x)$ for the Fekete polynomial associated with χ_n. By definition, $F_n(x)$ is given by the following formula

$$F_n(x) = \sum_{\substack{1 \le a \le n-1 \\ \gcd(a,n)=1}} x^a.$$

With this article, we aim to lay the foundation for the study of F_n. In particular, we will explain how to determine the cyclotomic and non-cyclotomic factors of F_n with a special focus on the case n is the product of two prime numbers. Quite surprisingly, as we will see later in the article, F_n usually has exactly one irreducible non-cyclotomic factor which we will denote by f_n. Furthermore, like the case of quadratic characters considered in [17, 18], the Galois group of f_n is also often as large as possible. Additionally, we also discover that the coefficients of f_n are relatively small. For example, when $n = 3p$ where p is a prime number, the coefficients of f_{3p} belong to the set $\{-2, -1, 0, 1, 2\}$ (see Proposition 6.2). This property suggests that f_n could potentially have interesting extremal properties which we hope to investigate in the near future. Finally, it is worth noting that we approach this project from a computational perspective; namely many statements in our article are first discovered by producing and analyzing a large amount of data. We refer the readers to the GitHub repository [8] for a collection of those data.

We remark that the theory of Fekete polynomials is closely related to the construction of certain Paley graphs. In the case where χ is a primitive quadratic Dirichlet character, we discuss this connection in [16]. When χ is a principal Dirichlet character, the corresponding Paley graph is called a unitary Caley graph in the literature (see [2, 14]). These types of Paley graphs have found applications in various fields such as coding and cryptography theory (see [12, 13]). It is our hope that the study in this paper would shed some light on further applications of Fekete polynomials and Paley graphs.

The structure of the article is as follows. In the first section, we describe integral representations of certain L-functions using Fekete polynomials F_n. Based on this, we then show a direct relationship between F_n and F_{n_0} where n_0 is the radical of n. In the next section, we compute some special values of F_n and its derivatives. Section 4 deals with the case $n = p$ and $n = 2p$ where we can derive an explicit formula for the factors of F_n. Section 5 studies the case $n = pq$ where $q < p$ are two odd prime numbers. In this section, we determine certain cyclotomic factors of F_n. Using this information, we then define the Fekete polynomial f_n and its trace polynomial g_n. We then proceed to study some arithmetic properties of F_n over $\mathbb{F}_p[x]$. In the next section, we pay special attention to the case $n = 3p$. In this case, using modular methods, we show that f_n is separable. Furthermore, we show that the coefficients of f_n are relatively small; namely, they belong to the set $\{-2, -1, 0, , 1, 2\}$. Section 7 studies the case $n = 5p$. We show again that f_n is separable. It is worth remarking that while the method is similar to the case $n = 3p$, the proof in this section is more involved. In section 8, we discuss some algorithms to study the irreducibility of f_n and g_n. Finally, in the last section, we study the Galois groups of g_n and f_n. Based on our numerical data, we propose precise conjectures on the structure of these Galois groups.

2. Reduction to the squarefree cases

Let n be an integer and n_0 the radical of n which is defined as the product of the distinct prime numbers dividing n. Let χ_n and χ_{n_0} be the principal Dirichlet characters associated with n and n_0 as explained in the introduction. By definition, we see that $L(\chi_n, s) = L(\chi_{n_0}, s)$. By the integral representations of these L-functions 1.1 we conclude that for all $s > 1$

$$\int_0^1 \frac{(-\log(t))^{s-1}}{t} \frac{F_n(t)}{1-t^n} dt = \int_0^1 \frac{(-\log(t))^{s-1}}{t} \frac{F_{n_0}(t)}{1-t^{n_0}} dt.$$

This suggests the following proposition.

Proposition 2.1. *Let n be an integer and n_0 the radical of n. Then we have the following equality*

$$(x^n - 1)F_{n_0}(x) = (x^{n_0} - 1)F_n(x).$$

Proof. It is sufficient to show that

$$\frac{F_{n_0}(x)}{x^{n_0} - 1} = \frac{F_n(x)}{x^n - 1}.$$

In fact, we have

$$\frac{F_{n_0}(x)}{x^{n_0} - 1} = F_{n_0}(x) \sum_{k=0}^{\infty} x^{kn} = \sum_{\substack{1 \le a \\ \gcd(a, n_0) = 1}} x^a.$$

Similarly

$$\frac{F_n(x)}{x^n - 1} = \sum_{\substack{1 \le a \\ \gcd(a, n) = 1}} x^a.$$

We note further that since n_0 is the radical of n, $\gcd(a, n) = 1$ if and only if $\gcd(a, n_0) = 1$. Consequently

$$\sum_{\substack{1 \le a \\ \gcd(a, n_0) = 1}} x^a = \sum_{\substack{1 \le a \\ \gcd(a, n) = 1}} x^a.$$

By the above equality, we conclude that

$$\frac{F_{n_0}(x)}{x^{n_0}-1} = \frac{F_n(x)}{x^n-1}. \qquad \square$$

Corollary 2.2. *Let $f \in \mathbb{Z}[x]$ be a non-cyclotomic irreducible polynomial. Then f is a divisor of F_n if and only if f is a divisor of F_{n_0}.*

Corollary 2.3. *Suppose that n is an odd integer and n_0 is its radical. Then*

$$F_n'(-1) = F_{n_0}'(-1).$$

3. Special values of $F_n(x)$

For a fixed positive integer d, we will denote by $\zeta = \zeta_d$ a fixed primitive d-th root of unity.

Proposition 3.1. *Let n be a positive integer and d a divisor of n. Then*

$$F_n(\zeta_d) = \mu(d)\varphi\left(\frac{n}{d}\right).$$

Proof. We have

$$F_n(\zeta_d) = \varphi\left(\frac{n}{d}\right) \sum_{\substack{1 \le a \le d-1 \\ \gcd(a,d)=1}} \zeta_d^a = \mu(d)\varphi\left(\frac{n}{d}\right).$$

$\square$

Proposition 3.2. *Let p and q be two different primes. Let d be a nontrivial divisor of $p-1$. Suppose that $d \neq q$ then $F_{pq}(\zeta_d) = 0$. Consequently, $\Phi_d(x)$ is a divisor of $F_{pq}(x)$.*

Proof. One has

$$\begin{aligned}
F_{pq}(\zeta) &= \sum_{k=1}^{pq} \zeta^k - \sum_{k=1}^{p-1} \zeta^{qk} - \sum_{k=1}^{q} \zeta^{kp} \\
&= \sum_{k=1}^{q(p-1)} \zeta^k + \sum_{k=1}^{q} \zeta^{q(p-1)+k} - \sum_{k=1}^{p-1} \zeta^{qk} - \sum_{k=1}^{q} \zeta^{kp} \\
&= \sum_{k=1}^{q} (\zeta^k - \zeta^{kp}) - \sum_{k=1}^{p-1} \zeta^{qk} \\
&= -\sum_{k=1}^{p-1} \zeta^{qk} = 0.
\end{aligned}$$

$\square$

Next, we generalize this result for arbitrary n. First, we need the following lemma.

Lemma 3.3. *Let n be a positive integer and let p be a prime divisor of n. Let d be a nontrivial divisor of $p-1$. Let ζ is a primitive dth root of unity. Then*

$$\sum_{k=1}^{n} \zeta^k = \sum_{k=1}^{n/p} \zeta^k$$

Proof. Write $n = pa$, for some positive integer a. We have

$$\sum_{k=1}^{n} \zeta^k = \sum_{k=1}^{(p-1)a} \zeta^k + \sum_{k=1}^{a} \zeta^{(p-1)a+k} = \sum_{k=1}^{a} \zeta^k. \qquad \square$$

Proposition 3.4. *Let n be a square-free positive integer and p a prime divisor of n. If d is a nontrivial divisor of $p-1$ such that $d \nmid n/p$ then $\Phi_d(x)$ is a divisor of $F_n(x)$.*

Proof. Suppose that $n = p_1 \cdots p_r$ be the prime factorization of n, where $p_1 = p, p_2, \ldots, p_r$ are distinct primes. For each i, $1 \le i \le r$, we set $A(i)$ to be the set of integers k such that $1 \le k \le n$ and $p_i \mid k$. Let s be an integer with $1 \le s \le r$. We consider an s-tuple $(i_1, \ldots, i_s)$ of integers such that $1 \le i_1 < \cdots < i_s \le r$. Then for each $k \in A(i_1) \cap \cdots \cap A(i_s)$, one can write $k = p_{i_1} \cdots p_{i_s} l$ for some l with $1 \le l \le \frac{n}{p_{i_1} \cdots p_{i_s}}$. If $i_1 = 1$ then

$$\sum_{k \in A(i_1) \cap \cdots \cap A(i_s)} \zeta^k = \sum_{k=1}^{\frac{n}{pp_{i_2} \cdots p_{i_s}}} (\zeta^{pp_{i_2} \cdots p_{i_s}})^k = \sum_{k=1}^{\frac{n}{pp_{i_2} \cdots p_{i_s}}} (\zeta^{p_{i_2} \cdots p_{i_s}})^k.$$

(Here we note that $pp_{i_2} \cdots p_{i_s} \equiv p_{i_2} \cdots p_{i_s} \pmod{d}$.) If $i_1 > 1$ then by the previous lemma,

$$\sum_{k \in A(i_1) \cap \cdots \cap A(i_s)} \zeta^k = \sum_{k=1}^{\frac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}}} (\zeta^{p_{i_1} p_{i_2} \cdots p_{i_s}})^k = \sum_{k=1}^{\frac{n}{pp_{i_1} p_{i_2} \cdots p_{i_s}}} (\zeta^{p_{i_1} p_{i_2} \cdots p_{i_s}})^k$$

(Here we note that $\zeta^{p_{i_1} p_{i_2} \cdots p_{i_s}}$ is a primitive eth root of unity, for some e with $e \mid d \mid p-1$ and $e > 1$.)

From the above discussions, we have

$$(-1)^s \sum_{1 \le i_1 < i_2 < \cdots < i_s} \sum_{k \in A(i_1) \cap \cdots \cap A(i_s)} \zeta^k = (-1)^s \sum_{2 \le i_2 < \cdots < i_s} \sum_{k=1}^{\frac{n}{pp_{i_2} \cdots p_{i_s}}} (\zeta^{p_{i_2} \cdots p_{i_s}})^k$$
$$+ (-1)^s \sum_{2 \le i_1 < i_2 < \cdots < i_s} \sum_{k=1}^{\frac{n}{pp_{i_1} p_{i_2} \cdots p_{i_s}}} (\zeta^{p_{i_1} p_{i_2} \cdots p_{i_s}})^k.$$

Thus,

$$\begin{aligned}
F_n(\zeta) &= \sum_{k=1}^{n} \zeta^k + \sum_{s=1}^{r-1} (-1)^s \sum_{1 \le i_1 < i_2 < \cdots < i_s} \sum_{k \in A(i_1) \cap \cdots \cap A(i_s)} \zeta^k + (-1)^r \zeta^n \\
&= \sum_{k=1}^{n} \zeta^k + \sum_{s=1}^{r-1} (-1)^s \sum_{2 \le i_2 < \cdots < i_s} \sum_{k=1}^{\frac{n}{pp_{i_2}\cdots p_{i_s}}} (\zeta^{p_{i_2}\cdots p_{i_s}})^k \\
&+ \sum_{s=1}^{r-1} (-1)^s \sum_{2 \le i_1 < i_2 < \cdots < i_s} \sum_{k=1}^{\frac{n}{pp_{i_1}p_{i_2}\cdots p_{i_s}}} (\zeta^{p_{i_1}p_{i_2}\cdots p_{i_s}})^k + (-1)^r \zeta^n \\
&= \sum_{k=1}^{n} \zeta^k - \sum_{k=1}^{n/p} \zeta^k + (-1)^{r-1} \zeta^{p_{i_1}p_{i_2}\cdots p_{i_s}} + (-1)^r \zeta^n \\
&= 0.
\end{aligned}$$

□

We have the following lemma.

Lemma 3.5. *Let n be a natural number.*

$$\sum_{1 \le i \le n-1} (-1)^{i-1} i = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{-(n-1)}{2} & \text{if } n \text{ is odd .} \end{cases}$$

Proof. Let us consider

$$M_n(x) = \sum_{i=1}^{n-1} x^i = \frac{x^n - x}{x-1}.$$

We then derive the above formula by observing that it is equal to $M_n'(-1)$. □

Proposition 3.6. *Let n be a positive integer and n_0 its radical. Then*

$$F_n'(-1) = \sum_{1 \le i \le n, \gcd(i,n)=1} (-1)^{i-1} i = \begin{cases} \dfrac{n\varphi(n)}{2} & \text{if } n \text{ is even} \\ \dfrac{\mu(n_0)\varphi(n_0)}{2} & \text{if } n \text{ is odd .} \end{cases}$$

Here $\mu(n)$ is the Möbius function.

Proof. Suppose that n is even. One has

$$\begin{aligned}
F_n'(-1) &= \sum_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} (-1)^{i-1} i = \sum_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} i = \frac{1}{2} \left(\sum_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} i + \sum_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} (n-i) \right) \\
&= \frac{n\varphi(n)}{2}.
\end{aligned}$$

Now we suppose that n is odd. By Corollary 2.3, we may suppose that n is square-free. By Lemma 3.5, we have

$$\sum_{1\le i\le m-1}(-1)^{i-1}i=-\frac{m-1}{2}.$$

Let $n=p_1\cdots p_r$ be the prime factorization of n, where $p_1,\ldots,p_r$ are distinct primes. For each i, $1\le i\le r$, we set $A(i)$ to be the set of integers k such that $1\le k\le n-1$ and $p_i\mid k$. Let s be an integer with $1\le s\le r-1$. We consider an s-tuple $(i_1,\ldots,i_s)$ of integers such that $1\le i_1<\cdots<i_s\le r$. Then for each $k\in A(i_1)\cap\cdots\cap A(i_s)$, one can write $k=p_{i_1}\cdots p_{i_s}l$ for some l with $1\le l\le \frac{n}{p_{i_1}\cdots p_{i_s}}-1$. Note that $(-1)^{k-1}k=p_{i_1}\cdots p_{i_s}(-1)^{l-1}l$. Hence

$$\begin{aligned}\sum_{k\in A(i_1)\cap\cdots\cap A(i_s)}(-1)^{k-1}k&=p_{i_1}\cdots p_{i_s}\sum_{1\le l\le\frac{n}{p_{i_1}\cdots p_{i_s}}-1}(-1)^{l-1}l=-p_{i_1}\cdots p_{i_s}\frac{\frac{n}{p_{i_1}\cdots p_{i_s}}-1}{2}\\&=-\frac{n-p_{i_1}\cdots p_{i_s}}{2}.\end{aligned}$$

Therefore

$$\begin{aligned}&\sum_{\substack{1\le k\le n\\ \gcd(k,n)=1}}(-1)^{k-1}k=\sum_{1\le k\le n-1}(-1)^{k-1}k-\sum_{1\le i\le r}\sum_{k\in A(i)}(-1)^{k-1}k+\sum_{1\le i<j\le r}\sum_{k\in A(i)\cap A(j)}(-1)^{k-1}k\\&-\cdots+(-1)^{r-1}\sum_{1\le i_1<\cdots<i_{r-1}\le r}\ \sum_{k\in A(i_1)\cap\cdots\cap A(i_{r-1})}(-1)^{k-1}k\\&=-\frac{n-1}{2}+\sum_{1\le i_1\le r}\frac{n-p_{i_1}}{2}-\sum_{1\le i_1<i_2\le r}\frac{n-p_{i_1}p_{i_2}}{2}+\cdots+(-1)^r\sum_{1\le i_1<\cdots<i_{r-1}\le r}\frac{n-p_{i_1}\cdots p_{i_{r-1}}}{2}\\&=-\frac{1}{2}n\left(1-\binom{r}{1}+\binom{r}{2}-\cdots+(-1)^{r-1}\binom{r}{r-1}\right)+\frac{1}{2}\\&-\frac{1}{2}\left(\sum_{1\le i_1\le r}p_{i_1}-\sum_{1\le i_1<i_2\le r}p_{i_1}p_{i_2}-\cdots+(-1)^r\sum_{1\le i_1<\cdots<i_{r-1}\le r}p_{i_1}\cdots p_{i_{r-1}}\right)\\&=\frac{1}{2}(-1)^r\left(n-\sum_{1\le i_1<\cdots<i_{r-1}\le r}p_{i_1}\cdots p_{i_{r-1}}+\cdots+(-1)^{r-1}\sum_{1\le i_1\le r}p_{i_1}+(-1)^r\right)\\&=\frac{1}{2}(-1)^r(p_1-1)\cdots(p_r-1)=\frac{\mu(n)\varphi(n)}{2}.\end{aligned}$$

□

Corollary 3.7. *Let n be an odd positive integer and n_0 its radical. Then -1 is a simple root of $F_n(x)$.*

4. THE CASES $n=p$ AND $n=2p$

We first consider the case that $n=p$ is a prime number.

Proposition 4.1. *We have*

$$F_p(x) = x \prod_{\substack{d|p-1 \\ d>1}} \Phi_d(x).$$

Proof.

$$F_p(x) = x + x^2 + \ldots + x^{p-1} = x\frac{1-x^{p-1}}{x-1} = x \prod_{\substack{d|p-1 \\ d>1}} \Phi_d(x).$$

□

Corollary 4.2. *Let p be a prime number. For $n \geq 2$*

$$F_{p^n}(x) = F_p(x) \prod_{i=2}^{n} \Phi_{p^i}(x) = x\frac{x^{p-1}-1}{x-1} \prod_{i=2}^{n} \Phi_{p^i}(x)$$

Proposition 4.3. *Let p be an odd prime. Then $F_{2p}(x)/x$ is a product of cyclotomic polynomials. More precisely*

$$F_{2p}(x) = x \prod_{2<d|(p-1)} \Phi_d(x) \prod_{\substack{d|2(p+1) \\ d\nmid p+1}} \Phi_d(x).$$

Proof. One has

$$\begin{aligned} F_{2p}(x) &= (x + x^3 + \cdots + x^{p-2}) + (x^{p+2} + x^{p+} \cdots + x^{2p-1}) \\ &= x(1 + x^2 + \cdots + x^{p-3})(1 + x^{p+1}) = x\frac{x^{p-1}-1}{x^2-1}\frac{x^{2(p+1)}-1}{x^{p+1}-1} \\ &= x \prod_{2<d|(p-1)} \Phi_d(x) \prod_{\substack{d|2(p+1) \\ d\nmid p+1}} \Phi_d(x). \end{aligned}$$

□

5. THE CASE $n = pq$

In this section, we study the case $n = pq$ where $q < p$ are two odd prime numbers.

Proposition 5.1. *The d-th cyclotomic polynomial $\Phi_d(x)$ divides $F_n(x)$ if $d > 1$ and one of the following holds*

(a) d divides $q-1$.
(b) d divides $p-1$ and $d \neq q$.
(c) d divides $\gcd(qp+1, p+q)$.

Proof. We have

$$\begin{aligned} (x^q - 1)F_n(x) &= \sum_{\substack{1\leq k\leq qp \\ \gcd(k,qp)=1}} x^{k+q} - \sum_{\substack{1\leq k\leq qp \\ \gcd(k,qp)=1}} x^k \\ &= \sum_{1\leq i\leq q-1} \left(x^{qp+i} + x^{ip} - x^i - x^{ip+q}\right). \end{aligned}$$

If d divides $q-1$, or $d \neq q$ divides $p-1$, then $\Phi_d(x)$ divides $F_n(x)$ by Proposition 3.4. Now suppose $d > 1$ divides $\gcd(pq+1, p+q)$. Let ζ_d be a primitive d-th root of unity. Since $qp + i = i - 1 \pmod{d}$ and $ip + q = (i-1)p \pmod{d}$, we get

$$\begin{aligned}(\zeta_d^q - 1)F_n(\zeta_d) &= \sum_{1 \le i \le q-1} \left(\zeta_d^{i-1} + \zeta_d^{ip} - \zeta_d^i - \zeta_d^{(i-1)p}\right) \\ &= 1 + \zeta_d^{(q-1)p} - \zeta_d^{q-1} - 1 = 0.\end{aligned}$$

Since $d \nmid q$, this shows that $F_n(\zeta_d) = 0$ and hence $\Phi_d(x)$ divides $F_n(x)$. $\square$

Let S_n be the set of integers d described in 5.1, namely

(5.1)
$$S_n = \{d > 1, d \neq q, d \mid p-1\} \cup \{d > 1, d \mid q-1\} \cup \{d > 1, d \mid \gcd(qp+1, p+q)\}.$$

Definition 5.2. Suppose $n = pq$ for odd primes p, q such that $q < p$. Let S_n be as above. We define the Fekete polynomial $f_n(x) \in \mathbb{Z}[x]$ to be the polynomial such that

$$F_n(x) = f_n(x) \cdot x \cdot \prod_{d \in S_n} \Phi_d(x)$$

Proposition 5.3. *Suppose $n = pq$ for odd primes p, q such that $q < p$. Let f_n denote the Fekete polynomial defined above. Let $D_1 = \gcd(p-1, q-1)$, $D_2 = \gcd(pq+1, p+q)$, $D_3 = \gcd(pq+1, p+q, p-1) = \gcd(p-1, q+1)$, $D_4 = \gcd(pq+1, p+q, q-1) = \gcd(p+1, q-1)$. Then f_n is a reciprocal polynomial of even degree. More precisely,*

$$\deg(f_n) = \begin{cases} pq - p - q - 1 + D_1 + D_3 + D_4 - D_2 & \text{if } p \neq 1 \pmod{q} \\ pq - p - 2 + D_1 + D_3 + D_4 - D_2 & \text{if } p = 1 \pmod{q}. \end{cases}$$

Furthermore, we have

$$f_n(1) = \begin{cases} \dfrac{D_1 D_3 D_4}{2D_2} & \text{if } p \neq 1 \pmod{q} \\ \dfrac{q D_1 D_3 D_4}{2D_2} & \text{if } p = 1 \pmod{q} \end{cases},$$
$$f_n(-1) = \frac{-D_1 D_3 D_4}{2D_2}.$$

Proof. Let

$$f(x) = \prod_{\substack{d \mid q-1 \\ d \neq 1}} \Phi_d(x), \quad g(x) = \prod_{\substack{d \mid p-1 \\ d \neq q \\ d \nmid q-1}} \Phi_d(x), \quad h(x) = \prod_{\substack{d \mid \gcd(pq+1, p+q) \\ d \nmid q-1, d \nmid p-1}} \Phi_d(x).$$

Then we have $F_n(x) = xf(x)g(x)h(x)f_n(x)$. Using the inclusion-exclusion principle, we get the following description of the cyclotomic factors in this decomposition:

$$f(x) = \frac{1-x^{q-1}}{1-x} = \frac{F_q(x)}{x}, \quad g(x) = \begin{cases} \frac{1-x^{p-1}}{1-x^{D_1}} & \text{if } p \neq 1 \pmod{q} \\ \frac{(1-x^{p-1})(1-x)}{(1-x^{D_1})(1-x^q)} & \text{if } p = 1 \pmod{q} \end{cases}$$

$$h(x) = \frac{(1-x^{D_2})(1-x^2)}{(1-x^{D_3})(1-x^{D_4})}.$$

This gives the formula for $\deg(f_n)$.

It is also clear from this description that

$$f(1) = q-1, \quad g(1) = \begin{cases} \frac{p-1}{D_1} & \text{if } p \neq 1 \pmod{q} \\ \frac{p-1}{qD_1} & \text{if } p = 1 \pmod{q} \end{cases}$$

$$h(1) = \frac{2D_2}{D_3 D_4}.$$

Since $F_n(1) = (p-1)(q-1)$, we infer the value of $f_n(1)$.

Note that D_i is even for $1 \leq i \leq 4$, and hence $g(-1), h(-1) \neq 0$ whereas $F_n(-1) = f(-1) = 0$. Thus, we calculate $F_n'(-1)$ and $f'(-1)$ using Proposition 3.6, and $g(-1)$ and $h(-1)$ using calculus to infer the value of $f_n(-1)$.

$$F_n'(-1) = \frac{(p-1)(q-1)}{2}, \quad f'(-1) = -F_q'(-1) = \frac{q-1}{2}$$

$$g(-1) = \frac{p-1}{D_1}, \quad h(-1) = \frac{2D_2}{D_3 D_4}$$

□

Definition 5.4. We define g_n to be the trace polynomial of f_n, i.e., it is the unique polynomial such that $g_n\left(x + \frac{1}{x}\right) = x^{-\deg(f_n)/2} f_n(x)$.

Proposition 5.5. *Suppose $n = pq$ for odd primes p, q such that $q < p$. Let f_n denote the Fekete polynomial defined above. Assume* $\operatorname{disc}(g_n)$ *(or equivalently* $\operatorname{disc}(f_n)$*) is nonzero.*
If $p \neq 1 \pmod{q}$, then up to squares, we have

$$\operatorname{disc}(f_n) = \begin{cases} -1 & \textit{if } p, q = 1 \pmod{4} \\ 1 & \textit{otherwise} \end{cases}$$

If $p = 1 \pmod{q}$, then up to squares, we have

$$\operatorname{disc}(f_n) = \begin{cases} q & \textit{if } p = 3 \pmod{4} \textit{ and } q = 1 \pmod{4} \\ -q & \textit{otherwise} \end{cases}$$

Proof. Since f_n is a reciprocal polynomial,

$$\operatorname{disc}(f_n) = (-1)^{\deg(f_n)/2} f_n(1) f_n(-1) \operatorname{disc}(g_n)^2.$$

Therefore Proposition 5.3 tells us that up to squares, we have

$$\operatorname{disc}(f_n) = \begin{cases} (-1)^{\deg(f_n)/2}(-1) & \text{if } p \neq 1 \pmod q \\ (-1)^{\deg(f_n)/2}(-q) & \text{if } p = 1 \pmod q \end{cases}$$

Calculating $\deg(f_n)$ modulo 4, using the formula in Proposition 5.3, we obtain the stated result. ☐

Here is a direct corollary of this proposition.

Corollary 5.6. *$f_{pq}(x)$ is not a product of cyclotomic polynomials. In particular, $f_{pq}(x)$ is not a cyclotomic polynomial.*

Proof. Suppose that

$$f_{pq}(x) = \prod_{i=1}^{r} \Phi_{m_i}(x),$$

where $1 \leq m_1 \leq m_2 \cdots \leq m_r$ are positive integers. Since $f_{pq}(1)f_{pq}(-1) \neq 0$, we can assume that $m_1 > 2$. By [6, Lemma 7], we have $\Phi_{m_i}(-1) > 0$ for all $1 \leq i \leq r$. Consequently $f_{pq}(-1) > 0$. This contradicts the above determination of $f_{pq}(-1)$. ☐

We now investigate the roots of the Fekete polynomials F_{pq} in $\overline{\mathbb{F}}_p$. Before we do so, we recall the following definition.

Definition 5.7. Let f, g be two polynomials. The Wronskian $W(f,g)$ of f and g is defined by the following formula

$$W(f,g) = f'g - g'f.$$

We then introduce the following polynomial

$$u_q(x) = W(s(x), F_q(x)) = s_q'(x)F_q(x) - F_q'(x)s_q(x),$$

where $F_q(x) = x + x^2 + \ldots + x^{q-1}$ and $s_q(x) = x^q - 1$. We can check that $u_q(x)$ has the following explicit formula.

$$u_q(x) = \sum_{1 \leq i \leq q-1} (q-i)x^{q-1+i} + \sum_{1 \leq i \leq q-1} ix^{i-1}$$

Proposition 5.8. *The polynomial $u_q(x)$ is irreducible.*

Proof. We have

$$F_q(x) = x\frac{x^{q-1}-1}{x-1} = \frac{x^q - x}{x-1}.$$

Therefore

$$F_q'(x) = \frac{(qx^{q-1}-1)(x-1) - (x^q - x)}{(x-1)^2}.$$

Over $\mathbb{F}_q[x]$ we have

$$F_q'(x) = \frac{1-x^q}{(x-1)^2} = -(x-1)^{q-2}.$$

Additionally, over $\mathbb{F}_q[x]$, we have $s_q(x) = (x-1)^q$ and $s'_q(x) = 0$. Therefore, over $\mathbb{F}_q[x]$, we have $u_q(x) = (x-1)^{2q-2} \pmod{q}$. Let $v_q(x) = u_q(x+1)$. Then $v_q(x) \equiv x^{2q-2} \pmod{q}$ and $v_q(0) = u_q(1) = q(q-1)$. By Eisenstein's criterion for irreducibility, we conclude that $v_q(x)$ (and hence $u_q(x)$) is irreducible. $\square$

Proposition 5.9. *Suppose $n = pq$ for odd primes p, q such that $q < p$.*

(a) Let $x_0 \in \overline{\mathbb{F}}_p$ be a zero of $F_n(x)$. Then $\operatorname{mult}_{x_0}(F_n) - 1 = \operatorname{mult}_{x_0}(u_q)$.

(b) Let $x_0 \in \overline{\mathbb{F}}_p$ be a zero of $F_n(x)$. If p is sufficiently large compared to q, then $\operatorname{mult}_{x_0}(F_n) \leq 2$.

(c) Let $x_0 \in \mathbb{F}_p$. Then $\operatorname{mult}_{x_0}(F_n) - 1 = \operatorname{mult}_{x_0}(u_q) = \operatorname{mult}_{x_0}(f_n)$.

Proof. As in the proof of Proposition 5.1, we have

$$\begin{aligned}(x^q-1)F_n(x) &= \sum_{1\leq i\leq q-1}\left(x^{qp+i}-x^i\right) + \sum_{1\leq i\leq q-1}(x^{ip}-x^{ip+q}) \\ &= (x^{qp}-1)F_q(x) - (x^q-1)F_q(x^p)\end{aligned}$$

and hence

$$\begin{aligned}F_n(x) &= (x^q-1)^{p-1}F_q(x) - F_q(x)^p \pmod{p} \\ F'_n(x) &\equiv F'_q(x)(x^q-1)^{p-1} - qx^{q-1}F_q(x)(x^q-1)^{p-2} \pmod{p} \\ &= -(x^q-1)^{p-2}u_q(x) \pmod{p}.\end{aligned}$$

(a) Proposition 3.1 says that $F_n(\zeta_q) = -\varphi(p) \equiv 1 \pmod{p}$, and $F_n(1) = \varphi(n) = (q-1)(p-1) \equiv 1-q \not\equiv 0 \pmod{p}$. Therefore, if $x_0 \in \overline{\mathbb{F}}_p$ is a zero of $F_n(x)$, then it is not a zero of $x^q - 1$. Hence, the relation of F'_n and u_q obtained above shows that $\operatorname{mult}_{x_0}(F_n) - 1 = \operatorname{mult}_{x_0}(u_q)$.

(b) Since the polynomial u_q is irreducible in $\mathbb{Z}[x]$, in particular, it is separable and thus $\operatorname{disc}(u_q) \neq 0$. If p is sufficiently large compared to q, we can then assume that $\operatorname{disc}(u_q) \neq 0 \pmod{p}$. Therefore the reduction of u_q modulo p is also separable. Hence $\operatorname{mult}_{x_0}(u_q) \leq 1$ for all $x_0 \in \overline{\mathbb{F}}_p$. Part (a) then implies that $\operatorname{mult}_{x_0}(F_n) \leq 2$.

(c) If $x_0 \in \mathbb{F}_p$, then by Fermat's little theorem, we have $F_q(x_0) = F_q(x_0)^p$ and $(x_0^q - 1)^{p-1} = 1$ and hence $F_n(x_0) = 0$. Part (a) then implies that $\operatorname{mult}_{x_0}(F_n) - 1 = \operatorname{mult}_{x_0}(u_q)$. Since $x_0 \in \mathbb{F}_p$, it is a $(p-1)^{th}$ root of unity. Since x_0 is a zero of F_n, we know as in Part (a) that it is not a q^{th} root of unity. So there exists some d dividing $p-1$, $d \neq q$, such that x_0 is a root of the d^{th} cyclotomic polynomial Φ_d. Therefore by Proposition 5.1 we get that $\operatorname{mult}_{x_0}(F_n) - 1 = \operatorname{mult}_{x_0}(f_n)$. $\square$

To further study the separability of $F_n(x)$ over $\mathbb{F}_p[x]$, we introduce the following auxiliary polynomial. Let $\operatorname{Res}_q(y)$ be the resultant of $u_q(x)$ and the following polynomial both considered as polynomials over $\mathbb{Z}[x]$

$$a(x,y) = s_q(x) - yt_q(x),$$

where

$$s_q(x) = x^q - 1, t_q(x) = \sum_{i=1}^{q-1} x^i.$$

The following proposition provides a direct link between the separability of $F_n(x)$ and the arithmetic of $\mathrm{Res}_q(y)$.

Proposition 5.10. *Suppose that $F_n(x)$ has a repeated root $x_0 \in \overline{\mathbb{F}}_p$. Then $\mathrm{Res}_q(y)$ has a root $\mu \in \mathbb{F}_p$.*

Proof. By Proposition 5.9 Part (a), $\mathrm{mult}_{x_0}(u_q) = \mathrm{mult}_{x_0}(F_n) \geq 1$, i.e., x_0 is a root of $u_q(x)$ modulo p. We claim that x_0 is not a root of $F_q(x) = x\dfrac{x^{q-1}-1}{x-1}$ modulo p. In fact, let us assume that x_0 is a root of $F_q(x)$ modulo p. Then x_0 is a simple root of $F_q(x)$ modulo p, because $(x-1)F_1(x) = x(x^{q-1}-1)$ is separable mod p. Since x_0 is a repeated root of $F_n(x) = (x^q - 1)F_q(x) - F_q(x)^q$ modulo p, we imply that x_0 has to be a root of $x^q - 1$ modulo p. On the other hand, $x_0 \neq 0$, hence x_0 is a root of $x^{q-1} - 1$ modulo p. This forces $x_0 - 1 = x_0^q - 1 - x_0(x_0^{q-1} - 1) = 0$. Hence $x_0 = 1$, but this is a contradiction since $F_n(1) = \varphi(n) = (p-1)(q-1) \neq 0 \pmod p$.

Now $0 = F_n(x_0) = (x_0^q - 1)^{p-1}F_q(x_0) - F_q(x_0)^q \pmod p$ implies that $(x_0^q - 1)^{p-1} = F_q(x_0)^{p-1}$. Hence $x_0^q - 1 = \mu F_q(x_0)$, for some $\mu \in \mathbb{F}_p^\times$. Thus, x_0 is a root of the polynomial $a(x,\mu) := x^q - 1 - \mu F_q(x) \in \mathbb{F}_p[x]$. In particular, $a(x,\mu)$ and $u_q(x)$ has a common zero. Therefore

$$\mathrm{resultant}(a(x,\mu), u(x)) = \mathrm{Res}_q(\mu) = 0.$$

□

5.1. **Further properties of the resultant $\mathrm{Res}_q(y)$.** We find through numerical data that $\mathrm{Res}_q(y)$ has some interesting properties on its own which might be of independent interest. In this section, we discuss some of them. First, we have the following lemma.

Lemma 5.11. *We have the following*

a) $\mathrm{Res}(s_q(x), s_q'(x)) = q^q$.
b) $\mathrm{Res}(t_q(x), t_q'(x)) = -(q-1)^{q-3}$.
c) $\mathrm{Res}(t_q(x), s_q(x)) = q - 1$.

Proof. a) Let ξ_k, $k = 1, \ldots, q$ be the qth root of unity. Then

$$\mathrm{Res}(s_q(x), s_q'(x)) = \prod_{k=1}^{n} s_q'(\xi_k) = q^q \left(\prod_{k=1}^{n} \xi_k\right)^{q-1} = q^q.$$

b) From $(x-1)t_q(x) = x^q - x$, we have

$$\mathrm{disc}(x^q - x) = \mathrm{disc}(x-1)\mathrm{disc}(t_q(x))\,\mathrm{Res}(x-1, t_q(x))^2.$$

Let ξ_k, $k = 1, \ldots, q-1$, be the $(q-1)$th root of unity. Then

$$\begin{aligned}\operatorname{disc}(x^q - x) &= (-1)^{q(q-1)/2} \operatorname{Res}(x^q - x, qx^{q-1} - 1) = (-1)^{q(q-1)/2} \cdot (-1) \cdot \prod_{k=1}^{q-1} (q\xi_k^{q-1} - 1) \\ &= -(-1)^{q(q-1)/2} (q-1)^{q-1}.\end{aligned}$$

Also, we have $\operatorname{Res}(x-1, t_q(x))^2 = t_q(1)^2 = (q-1)^2$. Hence

$$\operatorname{disc}(t_q(x)) = -(-1)^{q(q-1)/2} (q-1)^{q-3},$$

and thus

$$\operatorname{Res}(t_q(x), t_q'(x)) = (-1)^{(q-1)(q-2)/2} \operatorname{disc}(t_q(x)) = -(q-1)^{q-3}.$$

c) Let ξ_k, $k = 1, \ldots, q$ be the qth root of unity, where $\xi_q = 1$. Then

$$\operatorname{Res}(s_q(x), t_q(x)) = \prod_{k=1}^{n} t_q(\xi_k) = (q-1) \prod_{k=1}^{q-1} \frac{\xi_k^q - \xi_k}{\xi_k - 1} = (q-1) \prod_{k=1}^{q-1} \frac{1 - \xi_k}{\xi_k - 1} = q - 1.$$

□

Proposition 5.12. *Over $\mathbb{F}_q[y]$, $\operatorname{Res}_q(y)$ factors as follow*

$$\operatorname{Res}_q(y) = y^{2q-2}.$$

Proof. Using the property that $\operatorname{Res}(AB, C) = \operatorname{Res}(A, C) \operatorname{Res}(B, C)$ and the fact that $u_q(x) = (x-1)^{2q-2}$ over $\mathbb{F}_q[x]$ we have

$$\begin{aligned}\operatorname{Res}(a(x,y), u_q(x)) &= \operatorname{Res}(a(x,y), (x-1)^{2q-2}) = [\operatorname{Res}(a(x,y), x-1))]^{2q-2} \\ &= a(1,y)^{2q-2} = (q-1)^{2q-2} y^{2q-2} = y^{2q-2}.\end{aligned}$$

□

Proposition 5.13. $\operatorname{Res}_q(y)$ *is an even polynomial of degree $2q-2$. Its leading coefficient is $-(q-1)^{q-2}$ and its constant coefficient is $(q-1)q^q$.*

Proof. We observe that

$$\begin{aligned}a\left(\frac{1}{x}, y\right) &= \left[s_q\left(\frac{1}{x}\right) - y t_q\left(\frac{1}{x}\right)\right] \\ &= -\frac{1}{x^q}\left[s_q(x) + y t_q(x)\right].\end{aligned}$$

Consequently

$$a\left(\frac{1}{x}, y\right) a(x,y) = \frac{1}{x^q}(y^2 t_q(x)^2 - s_q(x)^2).$$

Let $z_1, z_2, \ldots, z_{2q-2}$ be the roots $u_q(x)$. Since $u_q(x)$ is a reciprocal polynomial of degree $2q-2$, we can assume further that $z_i z_{2q-1-i} = 1$. We have

$$\begin{aligned}\mathrm{Res}_q(y) &= \prod_{i=1}^{2q-2} a(z_i, y) = \prod_{i=1}^{q-1}\left[a(z_i,y)a\left(\frac{1}{z_i}, y\right)\right] \\ &= \prod_{i=1}^{q-1}\frac{1}{z_i^q}(y^2t_q(z_i)^2 - s_q(z_i)^2) = \left[\prod_{i=1}^{q-1}\frac{1}{z_i^q}\right]\prod_{i=1}^{q-1}(y^2t_q(z_i)^2 - s_q(z_i)^2).\end{aligned}$$

This shows that $\mathrm{Res}_q(y)$ is an even polynomial. We note also that

$$\mathrm{Res}_q(y) = \prod_{i=1}^{2q-2}(s_q(z_i) - yt_q(z_i)).$$

From this formula, we see that the leading coefficient of $\mathrm{Res}_q(y)$ is exactly $\prod_{i=1}^{2q-2} = t_q(z_i) = \mathrm{Res}(t_q(x), u_q(x))$. Similarly, the constant coefficient of $\mathrm{Res}_q(y)$ is $\prod_{i=1}^{2q-2} s_q(z_i) = \mathrm{Res}(s_q(x), u_q(x))$. To compute the leading coefficient, we note that

$$\begin{aligned}\mathrm{Res}(t_q(x), u_q(x)) &= \mathrm{Res}(t_q(x), s_q'(x)t_q(x) - s_q(x)t_q'(x)) = \mathrm{Res}(t_q(x), -s_q(x)t_q'(x)) \\ &= \mathrm{Res}(t_q(x), s_q(x))\,\mathrm{Res}(t_q(x), t_q'(x)) = -(q-1)^{q-2}.\end{aligned}$$

Similarly, the constant coefficient of $\mathrm{Res}_q(y)$ is $(q-1)q^q$. $\square$

It seems that $\mathrm{Res}_q(y)$ has further interesting properties. Based on the numerical data that we produced for various values of q, we propose the following conjectures/questions.

Conjecture 5.14. There exists $h_1, h_2 \in \mathbb{Z}[x]$ such that

$$\mathrm{Res}_q(y) = h_1(y^2)^2 - qh_2(y^2)^2.$$

Conjecture 5.15. $\mathrm{Res}_q(\sqrt{q}y) = q^{q-1}c(y)$ where $c(y)$ is an Eisenstein polynomial with respect to the prime q.

6. The case $n = 3p$

In this section, we focus on a special case, namely $n = 3p$. We can see that the set S_{3p} described in Equation 5.1 can be rewritten in the following form.

Let

$$S_{3p} = \begin{cases} \{d \in \mathbb{N} \mid d > 1, d \neq 3, d \mid p-1\} \cup \{8\} & \text{if } p \equiv 1 \mod 12 \\ \{d \in \mathbb{N} \mid d > 1, d \mid p-1\} \cup \{8\} & \text{if } p \equiv 5 \mod 12 \\ \{d \in \mathbb{N} \mid d > 1, d \neq 3, d \mid p-1\} & \text{if } p \equiv 7 \mod 12 \\ \{d \in \mathbb{N} \mid d > 1, d \mid p-1\} & \text{if } p \equiv 11 \mod 12. \end{cases}$$

Furthermore, the Fekete polynomial $f_{3p}(x)$ has the following description

$$F_{3p}(x) = f_{3p}(x) \cdot x \cdot \prod_{d \in C(3p)} \Phi_d(x)$$
$$= \begin{cases} f_{3p}(x) x \dfrac{x^{p-1}-1}{(x-1)\Phi_3(x)} & \text{if } p \equiv 1,7,19 \pmod{24} \\ f_{3p}(x) x \dfrac{x^{p-1}-1}{(x-1)\Phi_3(x)} \Phi_8(x) & \text{if } p \equiv 13 \pmod{24} \\ f_{3p}(x) x \dfrac{x^{p-1}-1}{(x-1)} \Phi_8(x) & \text{if } p \equiv 5 \pmod{24} \\ f_{3p}(x) x \dfrac{x^{p-1}-1}{(x-1)} & \text{if } p \equiv 11,17,23 \pmod{24} \end{cases}$$

We then have the following explicit formula for $f_{3p}(x)$.

Proposition 6.1. *In particular $f_{3p}(x)$ is a reciprocal polynomial of even degree. More precisely,*

$$f_{3p}(x) = \begin{cases} x^{2p+2} + x^{2p+1} + x^{p+2} + x^p + x + 1 & \textit{if } p \equiv 1,7,19 \pmod{24} \\ \dfrac{x^{2p+2} + x^{2p+1} + x^{p+2} + x^p + x + 1}{x^4+1} & \textit{if } p \equiv 13 \pmod{24} \\ \dfrac{x^{2p+2} + x^{2p+1} + x^{p+2} + x^p + x + 1}{(x^2+x+1)(x^4+1)} & \textit{if } p \equiv 5 \pmod{24} \\ \dfrac{x^{2p+2} + x^{2p+1} + x^{p+2} + x^p + x + 1}{x^2+x+1} & \textit{if } p \equiv 11,17,23 \pmod{24} \end{cases}$$

and

$$\deg f_{3p} = \begin{cases} 2p+2 & \textit{if } p \equiv 1,7,19 \pmod{24} \\ 2p-2 & \textit{if } p \equiv 13 \pmod{24} \\ 2p-4 & \textit{if } p \equiv 5 \pmod{24} \\ 2p & \textit{if } p \equiv 11,17,23 \pmod{24} \end{cases}$$

As before, let g_{3p} be the trace polynomial of f_{3p}, namely it is the polynomial such that

$$f_{3p}(x) = x^{\frac{\deg(f_{3p})}{2}} g_{3p}\left(x + \frac{1}{x}\right).$$

There is a classical theorem that the coefficients of $\Phi_{pq}(x)$ are in $\{0, -1, 1\}$ (see [5]). The first example of $\Phi_n(x)$ whose coefficients are not contained in $\{0, -1, 1\}$ is $n = 105$. Motivated by this, we observe that the coefficients of f_{3p} are quite small. In fact, for $p < 1200$, we use Sagemath and verify that the coefficients of f_{3p} are in the set $\{-2, -1, 0, 1, 2\}$. This leads us to the following proposition.

Proposition 6.2. *The coefficients of f_{3p} are in the set $\{-2, -1, 0, 1, 2\}$.*

Proof. The statement is clearly true if $p \equiv 1, 7, 19 \pmod{24}$.

Now we suppose $p \equiv 13 \pmod{24}$. Write $p = 13 + 24a$, for some $a \in \mathbb{N}$. Then

$$x^{2p+2} + 1 = (x^4)^{7+12a} + 1 = (x^4+1) \sum_{k=0}^{6+12a} (-1)^k x^{4k}$$

$$x^{2p+1} + x^{p+2} = x^{p+2}[(x^4)^{3+6a} + 1] = (x^4+1) \sum_{k=0}^{2+6a} (-1)^k x^{4k+15+24a}$$

$$x^p + x = x[(x^4)^{3+6a} + 1] = (x^4+1) \sum_{k=0}^{2+6a} (-1)^k x^{4k+1}.$$

Hence

$$f_{3p}(x) = \sum_{k=0}^{6+12a} (-1)^k x^{4k} + \sum_{k=0}^{2+6a} (-1)^k x^{4k+15+24a} + \sum_{k=0}^{2+6a} (-1)^k x^{4k+1}$$

Thus, all of the coefficients of f_3p are in $\{-1, 0, 1\}$.

Now we suppose that $p \equiv 2 \pmod 3$. Write $p = 2 + 3a$, for some $a \in \mathbb{N}$. Let

$$g(x) = \sum_{k=a+1}^{2a+1} x^{3k+1} - \sum_{k=a+1}^{2a} x^{3k+2} + \sum_{k=1}^{a} x^{3k} - \sum_{k=0}^{a-1} x^{3k+2} + 1.$$

It is straightforward to check that

$$\begin{aligned}(x^2+x+1)g(x) &= x^{6a+6} + x^{6a+5} + x^{3a+4} + x^{3a+2} + x + 1 \\ &= x^{2p+2} + x^{2p+1} + x^{p+2} + x^p + x + 1.\end{aligned}$$

Hence if $p \equiv 11, 17, 23 \pmod{24}$ then $f_{3p}(x) = g(x)$ whose coefficients are in $\{-1, 0, 1\}$.

Now we suppose further that $p \equiv 5 \pmod{24}$. Write $g(x) = \sum_{k=0}^{2p} b_k x^k$, then

$$b_k = \begin{cases} 1 & \text{if } k \equiv 1 \pmod 3 \text{ and } p+2 \le k \le 2p \\ -1 & \text{if } k \equiv 2 \pmod 3 \text{ and } k \neq p \\ 1 & \text{if } k \equiv 0 \pmod 3 \text{ and } 0 \le k \le p-2 \\ 0 & \text{otherwise} \end{cases}$$

In particular, $b_k = b_{k'}$ if $k \equiv k \pmod 3$ and $0 \le k, k' \le p-1$. We write $f_{3p}(x) = \sum_{k=0}^{2p-4} a_k x^k$. From $f_{3p}(x)(x^4+1) = g(x)$, we see that

$$a_k = b_k \qquad \text{if } k \in \{0, 1, 2, 3, 2p-7, 2p-6, 2p-5, 2p-4\}$$

$$a_k + a_{4+k} = b_{4+k} \qquad \text{if } 0 \le k \le 2p-8.$$

We claim that if $0 \le k \le p-25$ then $a_k = a_{k+24}$. In fact, we have

$$\begin{aligned}a_k - a_{k+24} &= (b_{4+k} + b_{12+k} + b_{20+k}) - (b_{8+k} + b_{16+k} + b_{24+k}) \\ &= (b_{4+k} - b_{16+k}) + (b_{12+k} - b_{24+k}) + (b_{20+k} - b_{8+k}) = 0.\end{aligned}$$

In particular the sequence $a_0, a_1, \ldots, a_{p-1}$ is periodic with a period 24. It is straightforward to check that the sequence $a_0, a_1, \ldots, a_{23}$ is

$$1, 0, -1, 1, -1, -1, 2, -1, 0, 2, -2, 0, 1, -2, 1, 1, -1, 1, 0, -1, 0, 0, 0, 0.$$

Hence $a_k \in \{-2, -1, 0, 1, 2\}$ for $0 \le k \le p-1$. Since $f_{3p}(x)$ is reciprocal, $a_k = a_{2p-4-k}$ is also in $\{-2, -1, 0, 1, 2\}$ if $p \le k \le 2p-4$.

$\square$

Corollary 6.3. *Let $a_{\frac{\deg f_{3p}}{2}}$ be the middle coefficient of f_{3p}. Then*

$$a_{\frac{\deg f_{3p}}{2}} = \begin{cases} 0 & \text{if } p \equiv 1, 7, 11, 17, 19, 23 \pmod{24} \\ 1 & \text{if } p \equiv 5 \pmod{24} \\ -1 & \text{if } p \equiv 13 \pmod{24}. \end{cases}$$

Next, we study some modular properties of f_{3p}. We start with the following proposition which is a stronger version of Proposition 5.9.

Theorem 6.4. *Let $p > 3$ is a prime. Let $x_0 \in \overline{\mathbb{F}}_p$ be a zero of $F_{3p}(x)$ modulo p.*

(1) The multiplicity of x_0 is at most 2.

(2) The multiplicity of x_0 is 2 if and only $x_0 \in \mathbb{F}_p$ and x_0 is a root of

$$u_3(x) = x^4 + 2x^3 + 2x + 1.$$

Proof. Let us first discuss the first statement. We have

$$\operatorname{disc}(u_3) = -1728 = -2^6 \times 3^3 \neq 0 \pmod{p}.$$

Since $\operatorname{disc}(u_3) \neq 0$, it must be the case that $u_3(x)$ is separable. In particular, all of its roots are simple. Hence the first statement follows from Proposition 5.9 Part (a).

The first part of the second statement follows from Proposition 5.9 Part (c). Now we discuss the second part of the second statement. We suppose that the multiplicity of $x_0 \in \overline{\mathbb{F}}_p$ is 2. By Proposition 5.10, there exists $\mu \in \mathbb{F}_p$ such that

$$\operatorname{resultant}(a(x, \mu), u_3(x)) = -2\mu^4 + 36\mu^2 + 54 = 0.$$

This implies that $108 = (\mu^2 - 9)^2$ and hence 3 is a square modulo p. Write $3 = c^2$ for some $c \in \mathbb{F}_p$. We have

$$u_3(x) = (x^2 + x + 1)^2 - 3x^2 = (x^2 + (1 + c)x + 1)(x^2 + (1 - c)x + 1) \in \mathbb{F}_p[x].$$

Let $b(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of x_0 over $\mathbb{F}_p$. Then $b(x)$ is an irreducible factor of both $u(x)$ and $a_\mu(x)$. In particular $\deg b(x) = 1$ or 2.

If $\deg b(x) = 2$, then $b(x) = x^2 + (1 + c)x + 1$ or $b(x) = x^2 + (1 - c)x + 1$. In either case, $b(x)$ is reciprocal. Hence the zeroes of $b(x)$ are α and $1/\alpha$ for some $\alpha \in \overline{\mathbb{F}}_p$. Thus, the zeroes of $a(x, \mu) = x^3 - \mu x^2 - \mu x - 1$ are $\alpha, 1/\alpha$ and β, for some $\beta \in \overline{\mathbb{F}}_p$. By Vieta's formula, $\alpha \cdot (1/\alpha)\beta = 1$. Hence $\beta = 1$ and $0 = a(1, \mu 1) = -2\mu$, a contradiction since $x_0^3 - 1 \neq 0$ as explained above.

The above arguments show that $\deg b(x) = 1$ and $x_0 \in \mathbb{F}_p$. $\square$

Corollary 6.5. *Let $p > 3$ be a prime. Then $\operatorname{disc}(F_{3p}) = 0 \pmod{p}$ if and only if $u(x) = x^4 + 2x^3 + 2x + 1$ has a zero modulo p. In particular,*

a) *if $p \equiv \pm 5 \pmod{12}$ then $p \nmid \operatorname{disc}(F_{3p})$,*
b) *if $p \equiv 11 \pmod{12}$ then $p \mid \operatorname{disc}(F_{3p})$,*
c) *if $p \equiv 1 \pmod{12}$ then $p \mid \operatorname{disc}(F_{3p})$ if and only if 12 is a quartic residue mod p.*

Proof. The first statement follows immediately from Theorem 6.4. In particular if $p \equiv \pm 5 \pmod{12}$ then $\left(\dfrac{3}{p}\right) = -1$ and hence $u_3(x) = (x^2 + x + 1)^2 - 3x^2$ has no zeros in $\mathbb{F}_p$. Therefore $\operatorname{disc}(F_{3p}) \neq 0 \pmod{p}$.

Now we suppose that $p \equiv \pm 1 \pmod{12}$ then $\left(\dfrac{3}{p}\right) = 1$. Therefore $3 = c^2$ for some $c \in \mathbb{F}_p$ and

$$u_3(x) = (x^2 + x + 1)^2 - 3x^2 = (x^2 + (1 + c)x + 1)(x^2 + (1 - c)x + 1).$$

The discriminant of $x^2 + (1 + c)x + 1$ is equal to $(1 + c)^2 - 4 = 2c$, and the discriminant of $x^2 + (1 - c)x + 1$ is equal to $(1 - c)^2 = -2c$. If $p \equiv 11 \pmod{12}$ then $\left(\dfrac{-1}{p}\right) = -1$, hence either $2c$ or $-2c$ is a square in $\mathbb{F}_p$. Therefore, either $x^2 + (1 + c)x + 1$ or $x^2 + (1 - c)x + 1$ has a zero in $\mathbb{F}_p$, and $p \mid \operatorname{disc}(F_{3p})$.

Suppose that $p \equiv 1 \pmod{12}$. In this case, $\left(\dfrac{2c}{p}\right) = \left(\dfrac{-2c}{p}\right)$. Then $p \mid \operatorname{disc}(F_{3p})$ if and only if there exists $a \in \mathbb{F}_p$ such that $a^2 = 2c$ if and only if there exists $a \in \mathbb{F}_p$ such that $a^4 = 12$ if and only if 12 is a quartic residue mod p. $\square$

Corollary 6.6. *Let $x_0 \in \mathbb{F}_p$. Then x_0 is a root of the Fekete polynomial $f_{3p}(x)$ if and only if it is a root of $u_3(x) = x^4 + 2x^3 + 2x + 1$.*

Corollary 6.7. *The polynomial $f_{3p}(x) \mod p$ is separable, in particular $f_{3p}(x)$ is separable. Consequently, $g_{3p}(x)$ is separable as well.*

Regarding the values of f_{3p} at 1 and -1, we have the following statement which is a direct corollary of Proposition 5.3.

Lemma 6.8. *We have*

$$f_{3p}(1) = \begin{cases} 6 & \text{if } p \equiv 1, 7, 19 \pmod{24} \\ 3 & \text{if } p \equiv 13 \pmod{24} \\ 1 & \text{if } p \equiv 5 \pmod{24} \\ 2 & \text{if } p \equiv 11, 17, 23 \pmod{24} \end{cases}$$

and

$$f_{3p}(-1) = \begin{cases} -2 & \text{if } p \equiv 1,7,11,17,19,23 \pmod{24} \\ -1 & \text{if } p \equiv 5,13 \pmod{24} \end{cases}.$$

Using this lemma where can prove the following proposition which was first discovered by experimental data.

Proposition 6.9. *The following statements are true.*

(1) *If* $p \equiv 1 \pmod 3$ *then* $\operatorname{disc}(f_{3p}) < 0$.
(2) *If* $p \equiv 2 \pmod 3$ *then* $\operatorname{disc}(f_{3p})$ *is a nonzero perfect square.*

Proof. This follows from the fact that

$$\operatorname{disc}(f_{3p}) = (-1)^{\frac{\deg(f_{3p})}{2}} f_{3p}(-1) f_{3p}(1) \operatorname{disc}(g_{3p})^2.$$

More precisely,

$$\operatorname{disc}(f_{3p}) = \begin{cases} (-1)^{p+1} \cdot (-2) \cdot 6 \cdot \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 1,7,19 \pmod{24} \\ (-1)^{p-1} \cdot (-1) \cdot 3 \cdot \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 13 \pmod{24} \\ (-1)^{p-2} \cdot (-1) \cdot 1 \cdot \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 5 \pmod{24} \\ (-1)^{p} \cdot (-2) \cdot 2 \cdot \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 11,17,23 \pmod{24} \end{cases}$$

$$= \begin{cases} -12 \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 1,7,19 \pmod{24} \\ -3 \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 13 \pmod{24} \\ \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 5 \pmod{24} \\ 4 \operatorname{disc}(g_{3p})^2 & \text{if } p \equiv 11,17,23 \pmod{24} \end{cases}$$

□

Regarding the 3-adic property of $\operatorname{disc}(f_{3p})$ we have the following

Corollary 6.10. *The following statements hold*

(1) *If* $p \equiv 2 \pmod 3$ *then* $\operatorname{disc}(f_{3p}) \equiv 1 \pmod 3$.
(2) *If* $p \equiv 1 \pmod 3$ *then* $\operatorname{disc}(f_{3p}) \equiv 0 \pmod 3$.

7. THE CASE $n = 5p$

In this section, we provide some partial results for the case $n = 5p$ where $p > 5$. The goal is to prove the following theorem which is a direct analog of Theorem 6.4.

Theorem 7.1. *Let* $p > 5$ *is a prime. Let* $x_0 \in \overline{\mathbb{F}}_p$ *be a zero of* $F_{5p}(x)$ *modulo* p.

(1) *The multiplicity of* x_0 *is at most* 2.
(2) *The multiplicity of* x_0 *is* 2 *if and only* $x_0 \in \mathbb{F}_p$ *and* x_0 *is a root of*

$$u_5(x) = x^8 + 2x^7 + 3x^6 + 4x^5 + x^3 + 3x^2 + 2x + 1.$$

Proof of Theorem 7.1 part (1). Suppose that $x_0 \in \overline{\mathbb{F}}_p$ is a multiple root of $F_{5p}(x)$. Similar to the proof of Theorem 6.4, x_0 is a common root of the following polynomials

$$a(x,\mu) = (x^5 - 1) - \mu(x + x^2 + x^3 + x^4),$$

and

$$u_5(x) = W(x^5 - 1, x + x^2 + x^3 + x^4) = x^8 + 2x^7 + 3x^6 + 4x^5 + x^3 + 3x^2 + 2x + 1,$$

where $\mu \in \mathbb{F}_p$. We can check that the discriminant of $u_5(x)$ has the following factorization

$$\mathrm{disc}(u_5(x)) = -1 * 2^{12} * 5^7 * 11^2.$$

Consequently, if $p \notin \{2, 5, 11\}$ then $u_5(x)$ has no repeated root over $\overline{\mathbb{F}}_p$. Consequently, for $p \neq 11$, all zeroes of $F_{5p}(x)$ has multiplicity at most 2. When $p = 11$, we can check directly that $F_{pq}(x)$ has no repeated roots. Thus, we have proved the first part of Theorem 7.1. □

Using Sagemath, we see that the resultant of $a_\mu(x)$ and $u_5(x)$ is given by

$$\mathrm{Res}_5(\mu) = \mathrm{Res}(a(x,\mu), u_5(x)) = 64\mu^8 - 400\mu^6 - 500\mu^4 - 25000\mu^2 - 12500.$$

Because $a_\mu(x)$ and $u_5(x)$ have a common roots, their resultant must be 0. In other words, we know that $\mu \in \mathbb{F}_p$ is a root of $\mathrm{Res}_5(y)$. Using Sagemath, we can see that we can rewrite $\mathrm{Res}_5(y)$ in the following form

$$\mathrm{Res}_5(y) = (8y^4 - 25y^2 + 125)^2 - 5(25y^2 + 75)^2.$$

Lemma 7.2. *Suppose that $F_{5p}(x)$ has a repeated root $x_0 \in \overline{\mathbb{F}}_p$, then $\left(\frac{5}{p}\right) = 1$.*

Proof. As explained above, the existence of a repeated root $x_0 \in \overline{\mathbb{F}}_p$ implies that $\mathrm{Res}_5(y)$ has a root $\mu \in \mathbb{F}_p$ where

$$\mathrm{Res}_5(y) = (8y^4 - 25y^2 + 125)^2 - 5(25y^2 + 75)^2.$$

If $25\mu^2 + 75 \neq 0$, then we conclude that $\left(\frac{5}{p}\right) = 1$. Otherwise, we must have $\mu^2 + 3 = 0$. Consequently

$$0 = \mathrm{Res}_5(\mu) = (8\mu^4 - 25\mu^2 + 125)^2 = 2^4 \times 17.$$

Since $p > 5$, we conclude that $p = 17$. This is impossible because $\left(\frac{-3}{17}\right) = -1$, and hence the equation $\mu^2 + 3 = 0$ has no solution in $\mathbb{F}_p$. □

Corollary 7.3. *If $\left(\frac{5}{p}\right) = -1$ then $F_{5p}(x)$ is separable over $\overline{\mathbb{F}}_p[x]$.*

We now complete the proof of Theorem 7.1.

Proof of Theorem 7.1 Part(2). By Proposition 5.9 Part (c), if $x_0 \in \mathbb{F}_p$ is a root of $u_5(x)$ then $\mathrm{mult}_{x_0}(F_{5p}) \geq 2$. Combining with Theorem 7.1 Part(1), we conclude that $\mathrm{mult}_{x_0}(F_{5p}) = 2$.

Now we suppose that $x_0 \in \overline{\mathbb{F}}_p$ is a multiple root of $F_{5p}(x)$. By Lemma 7.2, one has $\left(\frac{5}{p}\right) = 1$. Let $c \in \mathbb{F}_p$ be such that $c^2 = 5$. Then we have

$$u_5(x) = (1+x+x^2+x^3+x^4)^2 - 5x^2 = (1+x+x^2+x^3+x^4-cx^2)(1+x+x^2+x^3+x^4+cx^2).$$

Let $b(x)$ be the minimal polynomial of x_0. Then $b(x)$ is a common divisor of $u_5(x)$ and $a_\mu(x)$. Up to a choice of c, we can assume that $b(x)$ is a divisor of

$$v(x) = 1 + x + x^2 + x^3 + x^4 - cx^2.$$

Since x_0 is a common root of $v(x) = 1 + x + x^2 + x^3 + x^4 - cx^2$ and $a_\mu(x) = (x^5 - 1) - \mu(x + x^2 + x^3 + x^4)$, one has

$$x_0^5 - 1 = \mu(x_0 + x_0^2 + x_0^3 + x_0^4) = \mu(cx_0^2 - 1).$$

Also,

$$x_0^5 - 1 = (1 + x_0 + x_0^2 + x_0^3 + x_0^4)(x_0 - 1) = cx_0^2(x_0 - 1) = cx_0^3 - cx_0^2.$$

Hence $cx_0^3 - cx_0^2 = \mu(cx_0^2 - 1)$ and x_0 is a root of $w(x) := cx^3 - (c + c\mu)x^2 + \mu$.

Let $m(x)$ be the minimal polynomial of x_0 over $\mathbb{F}_p$. Then $m(x)$ is a common divisor of $v(x)$ and $w(x)$. Hence $\deg m \leq 2$. Suppose that $\deg m = 2$ and $m(x) = x^2 + ax + b$, for some $a, b \in \mathbb{F}_p$.

Case 1: $b = 1$, i.e., $m(x)$ is reciprocal. In this case, the roots of $m(x)$ are x_0 and $1/x_0$. This implies that $1/x_0$ is also a root of $a_\mu(x)$. Hence

$$0 = x_0^5 a_\mu(x_0) = (1 - x_0^5) - \mu x_0(1 + x_0 + x_0^2 + x_0^3 + x_0^4) = (1 - x_0^5) - \mu x_0(x_0^5 - 1).$$

Clearly $x_0^5 \neq 1$. Otherwise we would have $cx_0^2(x_0 - 1) = x_0^5 - 1 = 0$ and $x_0 = 0$ or 1, a contradiction. Thus $x_0 = -1/\mu$ is an element in $\mathbb{F}_p$, a contradiction.

Case 2: $b \neq 1$, i.e., $m(x)$ is not reciprocal. In this case, since $v(x)$ is reciprocal of degree 4, one has

$$v(x) = \frac{1}{b}(x^2 + ax + b)(1 + ax + bx^2).$$

By comparing the corresponding coefficients, we obtain $\dfrac{a + ab}{b} = 1$ and $\dfrac{a^2 + b^2}{b} = 1 - c$. Hence

$$a + ab = b \text{ and } a^2 + b^2 = b - bc.$$

Also, since $m(x) = x^2 + ax + b$ is a divisor of $w(x) = cx^3 - (c + c\mu)x^2 + \mu$, one can write

$$cx^3 - (c + c\mu)x^2 + \mu = (x^2 + ax + b)(cx - d) = cx^3 + (ac - d)x^2 + (bc - ad)x - bd,$$

for some $d \in \mathbb{F}_p$. By comparing the corresponding coefficients, we obtain that

$$ac - d = -c - c\mu, \quad bc - ad = 0, \quad \text{and } -bd = \mu.$$

Hence

$$bc = ad = a(ac + c + c\mu) = a^2c + ac + ac\mu.$$

Thus $b = a^2 + a + a\mu$. Also, we have

$$a\mu = -abd = -b^2c.$$

Hence

$$b = a^2 + a - b^2c.$$

In summary, we obtain the following three relations

$$a + ab = b \ (1), \quad a^2 + b^2 = b - bc \ (2), \quad b = a^2 + a - b^2c \ (3).$$

From (2) we get $a^2b + b^3 = b^2 - b^2c$. Combining with (1) and (3), we get

$$(a + ab) - (a^2b + b^3) = b - (a^2b + b^3) = (a^2 + a - b^2c) - (b^2 - b^2c) = a^2 + a - b^2.$$

Thus, we get

$$ab - a^2b - b^3 = a^2 - b^2 = (a - b)(a + b) = -ab(a + b)$$

(For the last equality, we use (1).) Therefore $ab - b^3 = -ab^2$ hence $a + ab = b^2$ (since $b \neq 0$). Combining with (1), we obtain $b^2 = b$. This implies that $b = 1$ which is a contradiction. □

Corollary 7.4. *The polynomial $f_{5p}(x) \mod p$ is separable, in particular $f_{5p}(x)$ is separable. Consequently, $g_{5p}(x)$ is separable as well.*

Remark 7.5. Interested readers may wonder whether a similar statement like Theorem 7.1 happens for general $n = pq$. It turns out that the answer is no. Below, we provide some concrete counterexamples.

(1) When $q = 7, p = 101$ we can check that over $\mathbb{F}_p[x]$, $x^2 + 42x + 10$ is an irreducible factor of $F_{pq}(x)$ (and $f_{pq}(x)$) with multiplicity equal to 2.
(2) When $q = 11, p = 13$ we can check that over $\mathbb{F}_p[x]$, $x^2 + 9x + 10$ is an irreducible factor of $F_{pq}(x)$ (and $f_{pq}(x)$) with multiplicity equal to 2.
(3) When $q = 11, p = 61$ we can check that over $\mathbb{F}_p[x]$, $x^2 + 16x + 14$ is an irreducible factor of $F_{pq}(x)$ (and $f_{pq}(x)$) with multiplicity equal to 2.

It would be quite interesting to investigate this problem further. For example, we wonder whether we can get some upper bounds on the degree of a repeated root $x_0 \in \overline{\mathbb{F}}_p$ of $F_n(x)$.

8. IRREDUCIBITY TEST FOR f_n

In this section, we discuss some methods to verify the irreducibility of f_n over $\mathbb{Z}[x]$. Generally speaking, there are some built-in functions to test whether a given polynomial $f \in \mathbb{Z}[x]$ is irreducible or not. While these built-in functions work quite well for polynomials of small degrees, it becomes computationally expensive when we work with polynomials of large degrees. For our problem, we exploit the fact that f_n is a reciprocal polynomial. In some cases, the irreducibility of f_n is equivalent to the irreducibility of g_n. The advantage of working with g_n is that its degree is only half of the degree of f_n. Furthermore, some modular methods apply to g_n but not to f_n (for example, when the discriminant of f_n is a perfect square, f_n is reducible over $\mathbb{F}_q[x]$ for all prime q, see e.g. [18, Remark 11.3]). We start with the following proposition.

Proposition 8.1. *(See* [7, Theorem 11]*) Let f be a monic reciprocal polynomial of degree $2n$. Let g be the trace polynomial of f. Suppose that g is irreducible. Then f is also irreducible if at least one of the following conditions holds.*

(1) $|f(1)|$ and $|f(-1)|$ are not perfect squares.
(2) $f(1)$ and the middle coefficient of f have different signs.
(3) The middle coefficient of f is 0 or ± 1.

In what follows, we propose some modifications to this proposition. First, we introduce the following definition.

Definition 8.2. (see [7]) Let h be a polynomial of degree n. We define the reversal polynomial of h by $h_{\text{rev}} = x^n h(1/x)$.

Lemma 8.3. *Let f be a monic reciprocal polynomial of degree $2n$. Let g be the trace polynomial of f. Suppose that g is irreducible. If f is reducible, then there exists $a \in \{-1, 1\}$ and a monic polynomial $h(x) \in \mathbb{Z}[x]$ such that*

$$f(x) = ah(x)h_{rev}(x).$$

Furthermore, if $f(1) > 0$ then $a = 1$.

Proof. This follows from the proof of [7, Theorem 11]. □

Proposition 8.4. *Let f be a monic reciprocal polynomial of degree $4n$. Let g be the trace polynomial of f. Suppose that g is irreducible and that $f(1)f(-1) < 0$. Then f is irreducible.*

Proof. Suppose that f is reducible. Then 8.3, $f(x) = ax^{2n}h(x)h(\frac{1}{x})$ where $h \in \mathbb{Z}[x]$ and $a \in \{1, -1\}$. We have $f(1) = ah(1)^2$ and $f(-1) = ah(-1)^2$. Consequently

$$f(1)f(-1) = a^2h(1)^2h(-1)^2.$$

This is impossible because $f(1)f(-1) < 0$. □

We can apply this proposition to our f_{pq} because $f_{pq}(1) > 0$ and $f_{pq}(-1) < 0$ provided that the degree of f_{pq} is divisible by 4 (see Proposition 5.3).

Proposition 8.5. *Let $f = \sum_{k=0}^{2n} a_k x^k$ be a monic reciprocal polynomial of degree $2n$ such that $f(1)f(-1) \neq 0$. Let g be the trace polynomial of f. Suppose that g is irreducible. Suppose that the middle coefficient $|a_n| \leq 2$. Then f is irreducible.*

Proof. Suppose that f is reducible. Without loss of generality, we can assume that $f(1) > 0$. Then we can find a monic $h(x) \in \mathbb{Z}[x]$ such that $f(x) = h(x)h_{\text{rev}}(x)$. Let $h(x) = \sum_{k=0}^{n} c_k x^k$. By definition $c_n = 1$. Furthermore, by comparing the leading coefficients of both sides, we must have $c_0 = 1$ as well. Additionally, by comparing the middle coefficients of both sides we have

$$a_n = \sum_{k=0}^{n} c_k^2.$$

Since $c_n = c_0 = 1$, we conclude that $c_k = 0$ for $1 \leq k \leq n$. In other words, $h(x) = x^n + 1$. If n is odd then $h(-1) = 0$ and so $f(-1) = 0$ which is a contradiction. If n is even then $h(x)$ and $h_{\text{rev}}(x)$ are both reciprocal polynomials. This forces $g(x)$ to be reducible which is also a contradiction. We conclude that $f(x)$ must be irreducible. □

Remark 8.6. I checked that for $q = 5$ and $p \leq 1000$, the middle coefficients of $f_{5p} \in \{-2, -1, 0, 1, 2\}$. This is unforuntunately not true for $q = 7$ (the middle coefficient of $f_{7\times 601}$ is 3.)

Proposition 8.7. *Let f be a monic reciprocal polynomial of degree $2n$. Let g be the trace polynomial of f. Suppose that g is irreducible. Suppose that there exists a prime number q_1 and a number m that the number of irreducible factors of degree m of f modulo q_1 is an odd number. Then f is irreducible.*

Proof. As before, if f is reducible then $f(x) = \pm h(x)h_{rev}(x)$. If $a(x)$ is an irreducible factor of $h(x)$ modulo q then so is $a_{\text{rev}}(x)$. Therefore, the degree $\deg(a(x))$ must appear an even number of time. This contradicts the assumption, hence f must be irreducible. □

Algorithm 8.8. To apply the criterion mentioned in Proposition 8.7 to f_{pq}, we do the following two steps.

- Step 1: Show that g_{pq} is irreducible. This can be achieved by finding a prime number q_2 such that g_{pq} is irreducible modulo q_2.
- Step 2: Find a prime number q_1 that satisfies the condition of Proposition 8.7.

Example 8.9. We demonstrate this method with a concrete example. Let us take $f_{15}(x) = x^6 - x^4 + x^3 - x^2 + 1$. We have

$$g_{15}(x) = x^3 - 4x + 1.$$

We can check that $g_{15}(x)$ is irreducible over $\mathbb{F}_3(x)$, so it is irreducible over $\mathbb{Z}[x]$ as well. Furthermore, over $\mathbb{F}_2(x)$, $f(x)$ factors as follow

$$f_{15}(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

We see that the degree 2 factors appear only one time. Therefore, by Proposition 8.7 $f_{15}(x)$ must be irreducible.

Conjecture 8.10. Let $n = pq$ be a product of two distinct odd primes. Then f_n and g_n are both irreducible.

Remark 8.11. Using the strategy described in Algorithm 8.8, we have verified that Conjecture 8.10 holds for $n \leq 10000$. It is interesting to remark that while the values of q_2 vary with respect to the size of n, the values q_1 are often small.

9. Galois theory for f_n and g_n

For a polynomial $f \in \mathbb{Q}[x]$, we let $\mathbb{Q}(f)$ be the splitting field of f. For $n = pq$, we let f_n and (respectively g_n) be the Fekete polynomial associated with n (respectively its trace polynomial). In this section, we investigate the Galois group of f_n and g_n.

9.1. **Galois group of g_n.** Let m be the degree of g_n. Then the Galois group of g_n is a naturally a subgroup of S_m since S_m permutes the roots of g_n. In our investigation, it turns out that the Galois group of g_n is always S_m for the cases that we consider. In order to verify this fact, we use the following proposition.

Proposition 9.1. ([17, Proposition 4.10]) *Let $g(x)$ be a monic polynomial with integer coefficients of degree m. Assume that there exists a triple of prime numbers (q_1, q_2, q_3) such that*

(1) $g(x)$ is irreducible in $\mathbb{F}_{q_1}[x]$.
(2) $g(x)$ has the following factorization in $\mathbb{F}_{q_2}[x]$

$$g(x) = (x + c)h(x),$$

where $c \in \mathbb{F}_{q_2}$ and $h(x)$ is an irreducible polynomial of degree $m - 1$.
(3) $g(x)$ has the following factorization in $\mathbb{F}_{q_3}[x]$

$$g(x) = m_1(x)m_2(x),$$

where $m_1(x)$ is an irreducible polynomial of degree 2 and $m_2(x)$ is a product of distinct irreducible polynomials of odd degrees.

Then the Galois group of $\mathbb{Q}(g)/\mathbb{Q}$ is S_m.

We demonstrate the usage of Proposition 9.1 by a concrete example.

Example 9.2. Let $n = 3 \times 7$. In this case, $g_n(x)$ is the following degree 8 polynomial

$$g_n(x) = x^8 + x^7 + 2x^6 + 3x^5 + 4x^3 + 4x^2 + 4x + 2.$$

Using Sagemath, we see that $g_n(x)$ is irreducible over $\mathbb{F}_5[x]$. Over $\mathbb{F}_{19}[x]$, $g(x)$ factors as

$$g_n(x) = (x+8)(x^7 + 12x^6 + 10x^5 + 8x^4 + 13x^3 + 5x^2 + x + 5).$$

Finally, over $\mathbb{F}_7(x)$, g_n factors as

$$g_n(x) = (x^2 + x + 4)(x^3 + 4)(x^3 + 2x + 1).$$

By Proposition 9.1, we conclude that the Galois group of g_n is S_8.

Based on the extensive numerical data that we produced, it seems reasonable to make the following conjecture.

Conjecture 9.3. Let $n = pq$ be a product of two distinct odd prime numbers. Then the Galois group of g_n is maximal; namely, it is S_m where $m = \deg(g_n)$.

Using Proposition 9.1, we have verified the following.

Proposition 9.4. *Conjecture 9.3 holds for the following values of n*

(1) $n = 3p$ *with* $3 < p < 1000$.
(2) $n = 5p$ *with* $5 < p < 1000$.
(3) $n = 7p$ *with* $p < 600$.
(4) $n = 11p$ *with* $p < 500$.

Proof. The data for the required triple (q_1, q_2, q_3) described in Proposition 9.1 is contained in the GitHub repository [8]. □

9.2. **Galois group of f_n.** By definition of g_n and f_n, we know that there is an exact sequence of Galois groups

$$1 \to \mathrm{Gal}(\mathbb{Q}(f_n)/\mathbb{Q}(g_n)) \to \mathrm{Gal}(\mathbb{Q}(f_n)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(g_n)/\mathbb{Q}) \to 1.$$

As explained in the previous section, the Galois group $\mathrm{Gal}(\mathbb{Q}(g_n)/\mathbb{Q})$ is naturally a subgroup of S_m. Additionally, the Galois group $\mathrm{Gal}(\mathbb{Q}(f_n)/\mathbb{Q}(g_n))$ is naturally a subgroup of $(\mathbb{Z}/2)^m$. The symmetric group S_m acts naturally on $(\mathbb{Z}/2)^m$ by permutation. From the above exact sequence, we conclude that $\mathrm{Gal}(\mathbb{Q}(f_n)/\mathbb{Q})$ is a subgroup of $(\mathbb{Z}/2)^m \rtimes S_m$. We note that we can also consider $(\mathbb{Z}/2)^m \rtimes S_m$ as a subgroup of S_{2m} (see [10, Section 2]). Furthermore, we have the following commutative diagram (see [18, Lemma 11.1].)

Lemma 9.5.

$$\begin{tikzcd}
(\mathbb{Z}/2\mathbb{Z})^m \rtimes S_m \arrow[r, hook] \arrow[dr, "\Sigma"'] & S_{2m} \arrow[d, "sgn"] \\
& \mathbb{Z}/2
\end{tikzcd}$$

Here sgn is the signature map and Σ is the following summation map

$$\Sigma(a_1, a_2, \ldots, a_m, \sigma) = \prod_{i=1}^{m} a_i.$$

From this diagram and some arguments with group theory, we have the following criteria to detect the Galois group of f_n.

Proposition 9.6. *(*[18, Proposition 11.11]*) Let $f(x)$ be a monic reciprocal polynomial with integer coefficients of even degree $2m$. Let g be the trace polynomial of f. Assume that*

(1) The Galois group of g is S_m.
(2) There exists a prime number q such that $f(x)$ has the following factorization in $\mathbb{F}_q(x)$

$$f(x) = p_2(x)h(x),$$

where $p_2(x)$ is an irreducible polynomial of degree 2, and $h(x)$ is a product of distinct irreducible polynomials of odd degrees.

Then the Galois group of f is $(\mathbb{Z}/2)^m \rtimes S_m$.

Proposition 9.7. *(See* [18, Proposition 11.8]*) Let $f(x)$ be a monic reciprocal polynomial with integer coefficients of even degree $2m$. Let g be the trace polynomial of f. Assume that*

(1) The Galois group of g is S_m.
(2) The discriminant of f, or equivalently $(-1)^m f(1)f(-1)$, is a perfect square.
(3) There exists a prime number q such that $f(x)$ has the following factorization in $\mathbb{F}_q(x)$

$$f(x) = p_2(x)p_4(x)h(x),$$

where $p_2(x)$ is an irreducible polynomial of degree 2, $p_4(x)$ is an irreducible polynomial of degree 4, and $h(x)$ is a product of distinct irreducible polynomials of odd degrees.

Then the Galois group of f is $\ker(\Sigma') \rtimes S_n$ where Σ' is the summation map

$$\Sigma'(a_1, a_2, \ldots, a_m) = \prod_{i=1}^{m} a_i.$$

We demonstrate the usage of these criteria with some concrete examples.

Example 9.8. Let us consider the case $n = 3 \times 7$. As demonstrated in Example 9.2, we know that the Galois group of g_n is S_8. By Proposition 5.5, the discriminant of f_n is not a perfect square. Furthermore, over $\mathbb{F}_{227}[x]$, f_n factors as follow

$$\begin{aligned} f_n(x) = &(x^2 + 12x + 1)(x^7 + 78x^6 + 173x^5 + 18x^4 + 119x^3 + 129x^2 + 107x + 9) \\ &\times (x^7 + 138x^6 + 90x^5 + 215x^4 + 2x^3 + 221x^2 + 160x + 101). \end{aligned}$$

By Proposition 9.6, we conclude that the Galois group of f_n is $(\mathbb{Z}/2)^8 \rtimes S_8$.

Example 9.9. Let us consider the case $n = 5 \times 7$. In this case, we can check that $g_n(x)$ is a polynomial of degree 11

$$g_n(x) = x^{11} - 11x^9 + 43x^7 + x^6 - 71x^5 - 5x^4 + 46x^3 + 4x^2 - 8x + 2.$$

We can check that the triple $(q_1, q_2, q_3) = (29, 47, 31)$ satisfies the conditions of Proposition 9.1. We conclude that the Galois group of g_n is S_{11}. By Proposition 5.5, we know that the discriminant of f_n is a perfect square. We can check that over $\mathbb{F}_{433}[x]$, f_n factors as

$$\begin{aligned}
&(x+97)(x+125)(x^2+41x+1)(x^4+124x^3+295x^2+124x+1) \\
&\times (x^7+190x^6+62x^5+191x^4+406x^3+37x^2+393x+313) \\
&\times (x^7+289x^6+393x^5+76x^4+168x^3+50x^2+251x+350).
\end{aligned}$$

By Proposition 9.7, we conclude that the Galois group of f_n is $\ker(\Sigma') \rtimes S_{11}$ where Σ' is the summation map

$$\Sigma' : (\mathbb{Z}/2)^{11} \to \mathbb{Z}/2.$$

Based on the extensive numerical data that we found, it seems reasonable to make the following conjecture.

Conjecture 9.10. Let $n = pq$ as before and $2m = \deg(f_n)$. Then the following hold

(1) If $p \equiv 1 \pmod q$ then the Galois group of f_n is $(\mathbb{Z}/2)^m \rtimes S_m$.
(2) If $p \not\equiv 1 \pmod q$ and $p, q \equiv 1 \pmod 4$, then the Galois group of f_n is $(\mathbb{Z}/2)^m \rtimes S_m$.
(3) In the remaining case, namely $p \not\equiv 1 \pmod q$ and at least p or q is not of the form $4k+1$, then the Galois group of f_n is $\ker(\Sigma') \rtimes S_m$ where Σ' is the summation map

$$\Sigma' : (\mathbb{Z}/2)^m \to \mathbb{Z}/2.$$

Using Proposition 9.6 and Proposition 9.7 we have verified the following.

Proposition 9.11. *Conjecture 9.10 holds for the following values of n*

(1) $n = 3p$ *with* $3 < p < 1000$.
(2) $n = 5p$ *with* $5 < p < 500$.
(3) $n = 7p$ *with* $7 < p < 500$.
(4) $n = 11p$ *with* $11 < p < 500$.

Code availability

An open-source code repository for this work is available on GitHub [8].

Acknowledgments

The third named author would like to thank William Stein for his help with the platform Cocalc where our computations are based.

References

[1] R. Baker and H. L. Montgomery. Oscillations of quadratic L-functions. In *Analytic Number Theory*, pages 23–40. Springer, 1990.

[2] M. Bašić and A. Ilić. Polynomials of unitary cayley graphs. *Filomat*, 29(9):2079–2086, 2015.

[3] P. Borwein. *Computational excursions in analysis and number theory*. Springer Science & Business Media, 2002.

[4] P. Borwein, K.-K. Choi, and S. Yazdani. An extremal property of Fekete polynomials. *Proceedings of the American Mathematical Society*, 129(1):19–27, 2001.

[5] G. Brookfield. The coefficients of cyclotomic polynomials. *Mathematics Magazine*, 89(3):179–188, 2016.

[6] B. Bzdega, A. Herrera-Poyatos, and P. Moree. Cyclotomic polynomials at roots of unity. *arXiv preprint arXiv:1611.06783*, 2016.

[7] A. Cafure and E. Cesaratto. Irreducibility criteria for reciprocal polynomials and applications. *The American Mathematical Monthly*, 124(1):37–53, 2017.

[8] S. Chidambaram, J. Mináč, T. T. Nguyen, and N. D. Tân. Fekete polynomials of principal Dirichlet characters. `https://github.com/tungprime/fekete_polynomials_principal_characters`, 2023.

[9] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan. Zeros of Fekete polynomials. In *Annales de l'institut Fourier*, volume 50, pages 865–889, 2000.

[10] S. Davis, W. Duke, and X. Sun. Probabilistic Galois theory of reciprocal polynomials. *Expositiones Mathematicae*, 16:263–270, 1998.

[11] T. Erdélyi. Improved lower bound for the Mahler measure of the Fekete polynomials. *Constructive Approximation*, 48(2):283–299, 2018.

[12] D. Ghinelli and J. D. Key. Codes from incidence matrices and line graphs of Paley graphs. *Advances in Mathematics of Communications*, 5(1):93, 2011.

[13] J. Javelle. *Cryptographie Quantique: Protocoles et Graphes*. PhD thesis, Université de Grenoble, 2014.

[14] W. Klotz and T. Sander. Some properties of unitary cayley graphs. *The electronic journal of combinatorics*, pages R45–R45, 2007.

[15] F. Lemmermeyer. *Quadratic number fields*. Springer, 2021.

[16] J. Mináč, L. Muller, T. T. Nguyen, and N. D. Tân. On the paley graph of a quadratic character. *arXiv preprint arXiv:2212.02005*, 2022.

[17] J. Mináč, T. T. Nguyen, and N. D. Tân. Fekete polynomials, quadratic residues, and arithmetic. *Journal of Number Theory*, 2022.

[18] J. Mináč, T. T. Nguyen, and N. D. Tân. On the arithmetic of generalized Fekete polynomials. *arXiv preprint arXiv:2206.11778*, 2022.

Department of Mathematics, Massachusetts Institute of Technology, Massachusetts Avenue Cambridge, MA 02139-4307

Email address: shivac@mit.edu

Department of Mathematics, Western University, London, Ontario, Canada N6A 5B7

Email address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
Email address: tungnt@uchicago.edu

SCHOOL OF APPLIED MATHEMATICS AND INFORMATICS, HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY, 1 DAI CO VIET ROAD, HANOI, VIETNAM
Email address: tan.nguyenduy@hust.edu.vn