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 have introduced and studied the arithmetic of generalized Fekete polynomials associated with primitive quadratic Dirichlet characters. We have shown further that these polynomials possess many interesting and important arithmetic and Galois-theoretic properties. In this paper, we introduce and study a different incarnation of Fekete polynomials, namely those associated with principal Dirichlet characters. We then investigate their cyclotomic and non-cyclotomic factors as well as their multiplicities. Additionally, we study their modular properties and special values. Finally, by combining both theoretical and numerical data, we propose precise questions on the structure of the Galois group of these Fekete polynomials.

CONTENTS

1. Introduction 2
2. Reduction to the squarefree cases 4
3. Zeros on the unit circle 5
4. Cyclotomic factors of F_n and their multiplicity 6
4.1. Cyclotomic factors of F_n 6
4.2. Multiplity of cyclotomic factors 13
4.3. The cases $n = p$ and $n = 2p$ 17
4.4. Cyclotomic factors of F_n with small degree 18
5. The case $n = pq$ 20
5.1. Further properties of the resultant $R_q(y)$ 26
6. The case $n = 3p$ 28
7. The case $n = 5p$ 33

Date: June 23, 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.

8. Irreducibity test for f_n 36
9. Galois theory for f_n and g_n 38
9.1. The Galois group of g_n 38
9.2. The Galois group of f_n 40
Code availability 42
Acknowledgments 42
References 42

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 [20, 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 mathematical history. As mentioned earlier, Michael Fekete introduced them in the 19th century through his studies of Dirichlet L-functions. Additionally, these polynomials played a vital role in Gauss's original sixth proof of the quadratic reciprocity law (see [18, Chapter 10, Section 3]). Many studies in the literature have explored various aspects of Fekete polynomials, including their extremal properties, Mahler measure, connections to oscillations of quadratic L-functions, distribution of their complex roots, and more (see [1, 3, 4, 9, 11]).

In recent works, we have introduced and analyzed the arithmetic properties of Fekete polynomials when χ is a primitive quadratic Dirichlet character (see [20, 21]). Our research has determined both cyclotomic and non-cyclotomic factors of F_χ. Additionally, we have shown that Fekete polynomials contain valuable arithmetic information, such as the class numbers or the orders of certain K-groups of certain quadratic fields. Furthermore, our extensive numerical data support the statement that, apart from x, F_χ has only one monic irreducible non-cyclotomic factor, which we denoted by f_χ. They also suggest that the Galois group of f_χ is as large as possible, as stated in [21, Conjecture 4.9, Conjecture 4.13] and [20, 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

$$F_n(x) = \sum_{\substack{1 \le a \le n-1 \\ \gcd(a,n)=1}} x^a. \tag{1.2}$$

Observe that since $\gcd(n-1, n) = 1$, the degree of F_n is $n-1$. 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.

Surprisingly, as we will demonstrate later in this article, $F_n(x)/x$ usually has only one monic irreducible non-cyclotomic factor, which we denote as f_n. Similar to the case of quadratic characters investigated in [20, 21], the Galois group of f_n is also often as large as possible. In addition, we have found that the coefficients of f_n are relatively small. For instance, 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 characteristic suggests that f_n may have noteworthy extremal properties that we intend to explore in the future. It is important to note that we approach this project from a computational standpoint, meaning that many of the statements in our article were discovered through the analysis of a large dataset. Interested readers can find our data collection at the GitHub repository [8].

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 [19]. When χ is a principal Dirichlet character, the corresponding Paley graph is called a unitary Caley graph in the literature (see [2, 17]). These types of Paley graphs have found applications in various fields such as coding

and cryptography theory (see [13, 16]). It is our hope that the study in this paper would shed some light on further applications of Fekete polynomials and Paley graphs.

The article is structured as follows. In Section 2, we describe integral representations of certain L-functions using Fekete polynomials F_n. Using this, we show a direct relationship between F_n and F_{n_0}, where n_0 is the radical of n. In Section 3, we study the number of zeroes of F_n on the unit circle using the intermediate value theorem. In Section 4, we present our main results concerning the factors of F_n. We describe various cyclotomic factors of F_n and their respective multiplicities. Additionally, we provide explicit conditions to determine if Φ_d is a factor of F_n for $d \in \{2, 3, 4, 6\}$. Section 5 is devoted to the case where $n = pq$ with $q < p$ being odd primes. We conjecturally determine all cyclotomic factors of F_n in this special case. Based on this, we introduce the Fekete polynomial f_n and its trace polynomial g_n. We then study some arithmetic properties of F_n over $\mathbb{F}_p[x]$ with the goal of showing that f_n is separable. In Section 6, we focus on the case $n = 3p$. Here, we use modular methods and the results in Section 5 to show that f_n is separable. We show further that its coefficients are small, belonging to the set $\{-2, -1, 0, 1, 2\}$. Section 7 considers the case where n is of the form $5p$. We once again establish the separability of f_n, although the proof is more involved compared to Section 6. In Section 8, we discuss algorithms for studying the irreducibility of f_n and g_n. Finally, in Section 9, we investigate the Galois groups of g_n and f_n, and propose questions on their structure which are motivated by our extensive numerical data.

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 divisors of n. Let χ_n and χ_{n_0} be the principal Dirichlet characters associated with n and n_0 as explained in the introduction. For an integer a, we know that $\gcd(a, n) = 1$ if and only if $\gcd(a, n_0) = 1$. Therefore, 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

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

Similarly

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

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

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

By the above equality, we conclude that

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

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 $F_n(-1) = F_{n_0}(-1) = 0$ and*

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

3. Zeros on the unit circle

The complex zeros of classical Fekete polynomials $f_p(x) = \sum_{a=0}^{p-1} \chi(a)x^a$ for quadratic Dirichlet characters $\chi = \left(\frac{\cdot}{p}\right)$ of prime conductor p were studied in [9]. It was shown in [9] that at least half of the zeros of f_p lie on the unit circle, and further that there exists a constant $1/2 < k_0 < 1$ such that the fraction of zeros of f_p lying on the unit circle converges to k_0 as p goes to infinity. In this section, we use the approach of [9] to analyze complex zeros of the Fekete polynomials F_n corresponding to principal Dirichlet characters. We remark that since the coefficients of F_n are either 0 or 1, the Erdos-Turan theorem implies that the roots of this polynomial are almost all clustered around the unit circle and equidistributed in angle (see [12, Theorem 1] and [14, Theorem 1.3]). We thank Professor Kannan Soundararajan for explaining this fact to us.

Let $H_n : \mathbb{C}\setminus(0,\infty) \to \mathbb{C}$ be the function defined by $H_n(z) = z^{-n/2}F_n(z)$ where we make a choice of the square root $z^{1/2}$. If $z = e^{2\pi it}$ we have

$$\begin{aligned} H_n(z) &= z^{-n/2} \sum_{\substack{1\le a\le n-1\\ \gcd(a,n)=1}} z^a = \sum_{\substack{1\le a\le (n-1)/2\\ \gcd(a,n)=1}} (x^{a-n/2} + x^{n/2-a}) \\ &= \sum_{\substack{1\le a\le (n-1)/2\\ \gcd(a,n)=1}} 2\cos\left(\pi t(2a-n)\right). \end{aligned}$$

Let $\mathbb{C}_1 = \{z \in \mathbb{C} : |z| = 1\}$ denote the unit circle in $\mathbb{C}$. Thus H_n defines a continuous real valued function on $\mathbb{C}_1 \setminus \{1\}$. For $k \in \mathbb{Z}$, let d_k denote $n/\gcd(n,k)$. By Proposition 4.1, if $0 < k < n$ and $\zeta_n = e^{2\pi i/n}$, we have

$$H_n(\zeta_n^k) = \zeta_n^{-nk/2}F_n(\zeta_n^k) = \frac{(-1)^k\mu(d_k)\phi(n)}{\phi(d_k)} \tag{3.1}$$

If k is such that $\gcd(n,k) = \gcd(n,k+1) = 1$, then H_n changes sign on the arc from ζ_n^k to ζ_n^{k+1}. Therefore, H_n and hence F_n must have a zero on this arc.

Let $\phi_1(n)$ denote the cardinality of the set $\{0 \le a < n | \gcd(n,a) = \gcd(n,a+1) = 1\}$. Then $\phi_1 : \mathbb{N} \to \mathbb{N}$ is a multiplicative function by Chinese Remainder theorem, and $\phi_1(p^k) = p^k(1-2p^{-1})$. Thus we have the formula $\phi_1(n) = n\prod_{p|n}\left(1-\frac{2}{p}\right)$. In summary, we have just proved the following.

Proposition 3.1. *F_n has at least $\phi_1(n)$ roots on the unit circle where*

$$\phi_1(n) = n\prod_{p|n}\left(1-\frac{2}{p}\right).$$

If $n = p$ or $n = 2p$ where p is a prime number then all factors of F_n, except x, are cyclotomic polynomials as explained in Section 4.3. The case where n has exactly two odd prime factors is more interesting. Specifically, let us consider the following special case: we fix an odd prime q and consider $n = pq$ for varying primes p. Then $\phi_1(n) \sim \left(1-\frac{2}{q}\right)n$ as $p \to \infty$. Therefore, the number of complex zeros of F_n on the unit circle grows at least as fast as $k_0 n$ in this limit, with $k_0 = 1-\frac{2}{q}$. It would be interesting to study this topic for general n.

4. Cyclotomic factors of F_n and their multiplicity

4.1. **Cyclotomic factors of F_n.** Let n be a squarefree number. Using Sagemath, we have verified numerically that for $n < 10000$, the Fekete polynomial $F_n(x)$ as defined in Eq. (1.2) has several cyclotomic factors. Even more surprisingly, if $n \notin \{p, 2p\}$ where p is a prime number, we observe further that F_n has exactly one irreducible non-cyclotomic factor. Guided by this numerical data, we plan to make an extensive study on cyclotomic factors of F_n.

First, we remark that Φ_d is not a factor of F_n if $d|n$ where Φ_d is the d-th cyclotomic polynomial This is a direct consequence of the theory of Ramanujan sums which is partially summarized in the following proposition (we refer the readers to [15] for some further discussions).

Proposition 4.1. *Let n be a positive integer and d a divisor of n. Let k be a field such that d is invertible in k. Suppose ζ_d is a primitive d-th root of unity in k. Then*

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

Here μ denotes the Mobius function and we consider $F_n[x]$ as a polynomial over $k[x]$ under the canonical map $\mathbb{Z}[x] \to k[x]$.

Proof. If $\mathrm{char}(k) = 0$, by embedding the subfield $\mathbb{Q}(\zeta_d) \subseteq k$ in $\mathbf{C}$, we have

$$F_n(\zeta_d) = \sum_{\substack{1\le a\le n\\ \gcd(a,n)=1}} \exp\left(\frac{2\pi i a}{d}\right),$$

which is a Ramanujan sum (see [15, Section 5.6]). Hence by [15, Theorem 272], we have $F_n(\zeta_d) = \frac{\mu(d)\varphi(n)}{\varphi(d)}$.

To deal with positive characteristics, we first note that the statement is entirely algebraic with all objects defined over the ring of integers $\mathcal{O}_F = Z[\zeta_d]$ of the cyclotomic field $F = \mathbb{Q}(\zeta_d)$. Indeed, we have

$$F_n(x) \in \mathbb{Z}[x], \quad \zeta_d \in \mathcal{O}_F, \quad \mu(d) = \sum_{\substack{1\le a\le n\\ \gcd(a,n)=1}} \zeta_d^a \in \mathcal{O}_F, \quad \phi(n) = \sum_{\substack{1\le a\le n\\ \gcd(a,n)=1}} 1 \in \mathbb{Z}.$$

If $\mathrm{char}(k) = p$, by considering reduction modulo a prime ideal of $\mathcal{O}_F$ above p, we see that the same formula should hold over k. □

Corollary 4.2. *If $d|n$ then $F_n(\zeta_d) \neq 0$. In other words, Φ_d is not a factor of F_n.*

We will now focus on the case where $d \nmid n$. We first have the following observation.

Lemma 4.3. *Let n be a squarefree number that is not prime. Let $d > 1$ be an integer, and let $d_1 = \gcd(d, n)$. In what follow, we will identify $\mathbb{Z}/d = [d] = \{0, 1, \ldots, d-1\}$. Let $S \subset [d]$ be the preimage of $(\mathbb{Z}/d_1)^\times$ under the canonical map $\mathbb{Z}/d \to \mathbb{Z}/d_1$. Then the d-th cyclotomic polynomial $\Phi_d(x)$ divides $F_n(x)$ if $d \neq d_1$ and the elements of $\{1 \le a \le n | \gcd(a, n) = 1\}$ when reduced modulo d, equidistribute among the elements of S.*

This statement follows from the following lemma.

Lemma 4.4. *Let d be a positive integer and d_1 is a divisor of d. Suppose further that $d_1 \neq d$ and d_1 is a squarefree number. Let $S \subset [d]$ be the preimage of $(\mathbb{Z}/d_1)^\times$ under the map $\mathbb{Z}/d \to \mathbb{Z}/d_1$ as described above. Then*

$$\sum_{i\in S} \zeta_d^i = 0.$$

Proof. Let $\zeta = \zeta_d$ and

$$F_S(x) = \sum_{s \in S} x^s.$$

Then we have

$$\frac{F_S(x)}{x^d - 1} = \sum_{s \in S, k \geq 0} x^{s+kd} = \sum_{m \geq 0, \gcd(m, d_1) = 1} x^m = \frac{F_{d_1}(x)}{x^{d_1} - 1}.$$

Consequently

$$F_S(x) = \frac{1 - x^d}{1 - x^{d_1}} F_{d_1}(x).$$

In particular

$$\sum_{i \in S} \zeta^s = F_S(\zeta) = \frac{\zeta^d - 1}{\zeta^{d_1} - 1} F_{d_1}(\zeta) = 0.$$

□

A direct corollary of the above proof is the following.

Corollary 4.5. *Let S be as above and $F_S(x)$ the polynomial*

$$F_S(x) = \sum_{s \in S} x^s.$$

Let $m|d$ be a positive integer. Let $\zeta = \zeta_m$ be a primitive m-root of unity. Then

$$F_S(\zeta) = \begin{cases} 0 & \text{if } m \nmid d_1 \\ \frac{d}{d_1} \frac{\mu(m)\varphi(d_1)}{\varphi(m)} & \text{if } m | d_1. \end{cases}$$

Proof. The first case follows directly from the formula

$$F_S(x) = \frac{1 - x^d}{1 - x^{d_1}} F_{d_1}(x).$$

The second case follows from this formula and Proposition 4.1. □

Remark 4.6. It is interesting to ask for the converse of the statement in Lemma 4.3. In the coming discussions, we will give a partial answer to this question. Specifically, we will show that all Φ_d that we discover by our techniques satisfy the equidistribution condition mentioned in Lemma 4.3.

We remark that if $d = p$ is a prime number such that $p \nmid n$ then the converse of Lemma 4.3 holds. This is a consequence of the following statement about a the field extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Proposition 4.7. *Let p be a prime number and $\zeta = \zeta_p$ is a primitive p-root of unity. Let $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Q}$ such that*

$$\sum_{i=0}^{p-1} a_i \zeta^i = 0.$$

Then $a_1 = a_2 = \ldots = a_{p-1}$.

Proof. First, we have $\sum_{i=0}^{p-1} \zeta^i = 0$. Using this formula, we see that

$$\sum_{i=0}^{p-2} (a_i - a_{p-1})\zeta^i = 0.$$

Since $\{\zeta^i\}_{i=0}^{p-2}$ is a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$, we must have $a_i = a_{p-1}$ for all $0 \leq i \leq p-2$. We conclude that $a_1 = a_2 = \ldots = a_{p-1}$. □

From the equidistribution property, we conclude that.

Corollary 4.8. *Let p be a prime number such that $p \nmid n$. If Φ_p is a factor of F_n then $p|\varphi(n)$. Equivalently, there exists a prime divisor r of n such that $p|r-1$.*

As we will see soon, the converse of this corollary is true as well. To do so, we now start our determination on various cyclotomic factors of F_n and their multiplicity. A crucial ingredient is the following description of F_n.

Lemma 4.9. *Let $n > 1$ be a square-free integer. We have*

$$F_n(x) = (1-x^n) \sum_{m|n} \mu(m) \frac{x^m}{1-x^m}.$$

Another simple algebraic equality that we will use is the following if $xy = 1$ then

$$\frac{x}{1-x} + \frac{y}{1-y} = -1.$$

Below, we describe some rather straightforward consequences of Lemma 4.9.

Proposition 4.10. *Let p be a prime number such that $\gcd(p,n) = 1$. Then we have the following recursive formula*

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

Proof. By Lemma 4.9 and the inclusion-exclusion principle we have

$$\begin{aligned} F_{np}(x) &= (1-x^{np}) \sum_{m|np} \mu(m) \frac{x^m}{1-x^m} \\ &= (1-x^{np}) \sum_{m|n} \mu(m) \frac{x^m}{1-x^m} + (1-x^{np}) \sum_{pm|np} \mu(pm) \frac{x^{pm}}{1-x^{pm}} \\ &= \frac{1-x^{np}}{1-x^n} F_n(x) - F_n(x^p). \end{aligned}$$

□

Corollary 4.11. *Let $n > 1$ be a square-free integer and d a positive integer not dividing n. If Φ_d is a factor of F_n then Φ_d is also a factor of F_{np} for every prime number p with $\gcd(d,p) = 1$.*

Proof. By Proposition 4.10 we have

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

Let ζ be a primitive dth root of unity. Then ζ^p is a primitive d- root of unity and hence $F_n(\zeta) = F_n(\zeta^p) = 0$. Therefore, the above formula implies $F_{np}(\zeta) = 0$ as well. □

By a similar argument, we have the following.

Corollary 4.12. *Let $n > 1$ be a square-free integer and d a positive integer not dividing n. Let p, q be two primes such that $\gcd(d, p) = 1$ and $p \equiv q \pmod{d}$. Then Φ_d is a factor of F_{np} if and only if it is a factor of F_{nq}.*

We now utilize Lemma 4.9 and the inclusion-exclusion principle to catch a big net of cyclotomic factors for F_n.

Theorem 4.13. *Let $d > 1$ be a positive integer which is not a divisor of a squarefree positive integer n. Suppose one of the following conditions is satisfied.*

(1) There is a prime divisor p of n such that $p \equiv 1 \pmod{d}$.
(2) There are two distinct prime divisors p_1, p_2 of n such that $p_1 p_2 + 1 \equiv 0 \pmod{d}$, $p_1 + p_2 \equiv 0 \pmod{d}$.
(3) There are three distinct prime divisors p_1, p_2, p_3 of n such that $p_1 p_2 p_3 - 1 \equiv 0 \pmod{d}$, $p_1 p_2 - p_3 \equiv 0 \pmod{d}$, $p_2 p_3 - p_1 \equiv 0 \pmod{d}$, $p_1 p_3 - p_2 \equiv 0 \pmod{d}$.
(4) There are three distinct prime divisors p_1, p_2, p_3 of n such that $p_1 p_2 + 1 \equiv 0 \pmod{d}$, $p_2 p_3 - p_1 \equiv 0 \pmod{d}$, $p_1 p_3 - p_2 \equiv 0 \pmod{d}$.
(5) There are three distinct prime divisors p_1, p_2, p_3 of n such that $p_1 p_2 p_3 - 1 \equiv 0 \pmod{d}$, $p_1 + p_2 \equiv 0 \pmod{d}$, $p_1 p_2 - p_3 \equiv 0 \pmod{d}$.

Then Φ_d is a factor of F_n.

Proof. (1) We have

$$\begin{aligned}\sum_{m|n} \mu(m) \frac{\zeta^m}{1-\zeta^m} &= \sum_{pm|n} \mu(pm) \frac{\zeta^{pm}}{1-\zeta^{pm}} + \sum_{m|(n/p)} \mu(m) \frac{\zeta^m}{1-\zeta^m} \\ &= \sum_{m|(n/p)} (-1)\mu(m) \frac{\zeta^m}{1-\zeta^m} + \sum_{m|(n/p)} \mu(m) \frac{\zeta^m}{1-\zeta^m} = 0.\end{aligned}$$

Here we note that $pm \equiv m \pmod{m}$, hence $\zeta^{pm} = \zeta^m$.

(2) We have

$$\begin{aligned}
&\sum_{m|n} \mu(m) \frac{\zeta^m}{1-\zeta^m} \\
&= \sum_{p_1p_2m|n} \mu(p_1p_2m) \frac{\zeta^{p_1p_2m}}{1-\zeta^{p_1p_2m}} + \sum_{p_1m|(n/p_2)} \mu(p_1m) \frac{\zeta^{p_1m}}{1-\zeta^{p_1m}} + \sum_{p_2m|(n/p_1)} \mu(p_2m) \frac{\zeta^{p_2m}}{1-\zeta^{p_2m}} \\
&+ \sum_{m|(n/p_1p_2)} \mu(m) \frac{\zeta^m}{1-\zeta^m} \\
&= \sum_{m|(n/(p_1p_2))} \mu(m) \left(\frac{\zeta^{p_1p_2m}}{1-\zeta^{p_1p_2m}} + \frac{\zeta^m}{1-\zeta^m} \right) + \sum_{m|(n/(p_1p_2))} (-1)\mu(m) \left(\frac{\zeta^{p_1m}}{1-\zeta^{p_1m}} + \frac{\zeta^{p_2m}}{1-\zeta^{p_2m}} \right) \\
&= \sum_{m|(n/(p_1p_2))} \mu(m)(-1) + \sum_{m|(n/(p_1p_2))} (-1)\mu(m)(-1) \\
&= 0.
\end{aligned}$$

For parts (3)-(5), we have

$$\begin{aligned}
\sum_{m|n} \mu(m) \frac{\zeta^m}{1-\zeta^m} &= \sum_{p_1p_2p_3m|n} \mu(p_1p_2p_3m) \frac{\zeta^{p_1p_2p_3m}}{1-\zeta^{p_1p_2p_3m}} + \sum_{p_2p_3m|(n/p_1)} \mu(p_2p_3m) \frac{\zeta^{p_2p_3m}}{1-\zeta^{p_2p_3m}} \\
&+ \sum_{p_1p_3m|(n/p_2)} \mu(p_1p_3m) \frac{\zeta^{p_1p_3m}}{1-\zeta^{p_1p_3m}} + \sum_{p_1p_2m|(n/p_3)} \mu(p_1p_2m) \frac{\zeta^{p_1p_2m}}{1-\zeta^{p_1p_2m}} \\
&+ \sum_{p_1m|(n/p_2p_3)} \mu(p_1m) \frac{\zeta^{p_1m}}{1-\zeta^{p_1m}} + \sum_{p_2m|(n/p_1p_3)} \mu(p_2m) \frac{\zeta^{p_2m}}{1-\zeta^{p_2m}} + \sum_{p_3m|(n/p_1p_2)} \mu(p_3m) \frac{\zeta^{p_3m}}{1-\zeta^{p_3m}} \\
&+ \sum_{m|(n/p_1p_2p_3)} \mu(m) \frac{\zeta^m}{1-\zeta^m}
\end{aligned}$$

In part (3), we have

$$\begin{aligned}
\mu(p_1p_2p_3m) \frac{\zeta^{p_1p_2p_3m}}{1-\zeta^{p_1p_2p_3m}} + \mu(m) \frac{\zeta^m}{1-\zeta^m} &= 0, \\
\mu(p_2p_3m) \frac{\zeta^{p_2p_3m}}{1-\zeta^{p_2p_3m}} + \mu(p_1m) \frac{\zeta^{p_1m}}{1-\zeta^{p_1m}} &= 0, \\
\mu(p_1p_3m) \frac{\zeta^{p_1p_3m}}{1-\zeta^{p_1p_3m}} + \mu(p_2) \frac{\zeta^{p_2m}}{1-\zeta^{p_2m}} &= 0, \\
\mu(p_1p_2m) \frac{\zeta^{p_1p_2m}}{1-\zeta^{p_1p_2m}} + \mu(p_3m) \frac{\zeta^{p_3m}}{1-\zeta^{p_3m}} &= 0.
\end{aligned}$$

Hence $\sum_{m|n} \mu(m) \frac{\zeta^m}{1-\zeta^m} = 0$.

In part (4), we have

$$\begin{aligned}
\mu(p_1p_2p_3m)\frac{\zeta^{p_1p_2p_3m}}{1-\zeta^{p_1p_2p_3m}}+\mu(p_3m)\frac{\zeta^{p_3m}}{1-\zeta^{p_3m}}&=\mu(m),\\
\mu(p_2p_3m)\frac{\zeta^{p_2p_3m}}{1-\zeta^{p_2p_3m}}+\mu(p_1m)\frac{\zeta^{p_1m}}{1-\zeta^{p_1m}}&=0,\\
\mu(p_1p_3m)\frac{\zeta^{p_1p_3m}}{1-\zeta^{p_1p_3m}}+\mu(p_2)\frac{\zeta^{p_2m}}{1-\zeta^{p_2m}}&=0,\\
\mu(p_1p_2m)\frac{\zeta^{p_1p_2m}}{1-\zeta^{p_1p_2m}}+\mu(m)\frac{\zeta^{m}}{1-\zeta^{m}}&=-\mu(m).
\end{aligned}$$

Hence $\sum_{m|n}\mu(m)\frac{\zeta^m}{1-\zeta^m}=0$.

In part (5), we have

$$\begin{aligned}
\mu(p_1p_2p_3m)\frac{\zeta^{p_1p_2p_3m}}{1-\zeta^{p_1p_2p_3m}}+\mu(m)\frac{\zeta^{m}}{1-\zeta^{m}}&=0,\\
\mu(p_2p_3m)\frac{\zeta^{p_2p_3m}}{1-\zeta^{p_2p_3m}}+\mu(p_1p_3m)\frac{\zeta^{p_1p_3m}}{1-\zeta^{p_1p_3m}}&=-\mu(m),\\
\mu(p_1p_2m)\frac{\zeta^{p_1p_2m}}{1-\zeta^{p_1p_2m}}+\mu(p_3m)\frac{\zeta^{p_3m}}{1-\zeta^{p_3m}}&=0,\\
\mu(p_1m)\frac{\zeta^{p_1m}}{1-\zeta^{p_1m}}+\mu(p_2m)\frac{\zeta^{p_2m}}{1-\zeta^{p_2m}}&=\mu(m).
\end{aligned}$$

Hence $\sum_{m|n}\mu(m)\frac{\zeta^m}{1-\zeta^m}=0$. □

Combining part (1) of Theorem 4.13 and Corollary 4.8, we have the following.

Corollary 4.14. *Let p be a prime number. Then Φ_p is a factor of n if and only if $p\nmid n$ and there exists a divisor r of n such that $p|r-1$.*

We observe that all d described above satisfy the equidistribution condition mentioned in Lemma 4.3

Proposition 4.15. *Let $d>1$ be a positive integer that is not a divisor of a squarefree positive integer n. Suppose one of the four conditions in Theorem 4.13 is satisfied. Then the elements of $\{1\le a\le n \mid \gcd(a,n)=1\}$ when reduced modulo d, equidistribute among the elements of $S\subset \mathbb{Z}/d\mathbb{Z}$ where S is the preimage of $(\mathbb{Z}/d_1)^\times$ under the canonical map $\mathbb{Z}/d\to\mathbb{Z}/d_1$.*

Proof. Let $F_S(x)$ be the polynomial defined in Corollary 4.5, namely

$$F_S(x)=\sum_{s\in S}x^s.$$

Let us consider the following polynomial

$$G_S(x)=F_n(x)-\frac{\varphi(n)d_1}{d\varphi(d_1)}F_S(x).$$

We claim that $G_S(\zeta)=0$ if ζ is a d-root of unity (not necessarily primitive). In fact, let $m|d$ and ζ_m a primitive m-root of unity. If $m\nmid d_1$ then $m\nmid n$. Consequently, m also satisfies

one of the four conditions in Theorem 4.13. Therefore, we know that $F_n(\zeta_m) = 0$. By Corollary 4.5, we also know that $F_S(\zeta_m) = 0$. We conclude that in this case $G_S(\zeta_m) = 0$. Let us consider the case $m|d_1$. We know that $m|n$ as well. By Proposition 4.1, we have

$$F_n(\zeta_m) = \frac{\mu(m)\varphi(n)}{\varphi(m)}.$$

By Corollary 4.5 we also know that

$$F_S(\zeta_m) = \frac{d}{d_1}\frac{\mu(m)\varphi(d_1)}{\varphi(m)}.$$

We then see that $G_S(\zeta_m) = 0$. Since this is true for all $m|d$, we conclude that $G_S(\zeta) = 0$ if ζ is a d-root of unity. As a result, $G_S(x) = (x^d - 1)K_S(x)$ where K_S is a polynomial. We can then write

$$F_n(x) = F_S(x) + (x^d - 1)K_S(x).$$

Our proposition follows easily from this recursive formula. □

4.2. **Multiplity of cyclotomic factors.** In this section, we determine the multiplicity of cyclotomic factors in F_n. To do so, we will investigate the value $F_n'(\zeta_d)$. By Lemma 4.9 we have

$$F_n'(x) = nx^{n-1}\sum_{m|n}\mu(m)\frac{x^m}{x^m-1} + (x^n-1)\sum_{m|n}\mu(m)\frac{-mx^{m-1}}{(x^m-1)^2}. \tag{4.1}$$

Remark 4.16. We remark that by Corollary 4.2, ζ_d is not a factor of F_n if $d|n$. Therefore, we can safely assume that $d \nmid n$ in our investigation. When this condition is satisfied, there is no danger in evaluating $F_n'(x)$ at $x = \zeta_d$ as $\zeta_d^m - 1 \neq 0$ for all $m|n$.

Based on Equation 4.1, we introduce the following polynomial.

$$G_n(x) = (x^n-1)^2\sum_{m|n}\mu(m)\frac{mx^m}{(x^m-1)^2}.$$

Equivalently, we have

$$x(x^n-1)F_n'(x) = nx^nF_n(x) - G_n(x), \tag{4.2}$$

and

$$G_n(x) = nx^nF_n(x) - (x^{n+1}-x)F_n'(x) = xF_n'(x) + \sum_{1\le a\le n,\gcd(a,n)=1}(n-a)x^{n+a}. \tag{4.3}$$

By explicit calculations, we have

$$G_n(x) = \sum_{1\le a\le n,\gcd(a,n)=1}(n-a)[x^{n+a}+x^{n-a}] = x^n\sum_{1\le a\le n,\gcd(a,n)=1}(n-a)[x^a+\frac{1}{x^a}]. \tag{4.4}$$

Utilizing Equation 4.4 we have the following.

Lemma 4.17. *Let d be a positive integer and n a positive squarefree integer. Let $\zeta = \zeta_d$ be a primitive d-root of unity. Then*

(1) If n is even then ζ_4 is a (simple) root of G_n.
(2) If $d \geq 2n$ then $G_n(\zeta) \neq 0$ unless $n = 2$ and $d = 4$.

Proof. Let us first show the first part. We remark that if a is odd then

$$\zeta_4^a + \frac{1}{\zeta_4^a} = 0.$$

If n is even and $\gcd(a, n) = 1$ then it must be the case that n is odd. Consequently

$$G_n(\zeta_4) = \zeta_4^n \sum_{1 \leq a \leq n, \gcd(a,n)=1} (n-a)[\zeta_4^a + \frac{1}{\zeta_4^a}] = 0.$$

Let us now prove the second part. We can rewrite $G_n(x)$ as follow

$$\begin{aligned} x^{-n} G_n(x) &= \sum_{1 \leq a \leq \frac{n}{2}, \gcd(a,n)=1} \left[(n-a)(x^a + x^{-a}) + a(x^{n-a} + x^{a-n})\right] \\ &= \sum_{1 \leq a \leq \frac{n}{2}, \gcd(a,n)=1} (n-2a)[x^a + x^{-a}] + \sum_{1 \leq a \leq \frac{n}{2}, \gcd(a,n)=1} a[x^a + x^{-a} + x^{n-a} + x^{a-n}]. \end{aligned}$$

Let $\zeta_d = e^{\frac{2\pi i}{d}}$, then by Euler formula we have

$$\zeta_d^{-n} G_n(\zeta_d) = 2 \sum_{1 \leq a \leq \frac{n}{2}, \gcd(a,n)=1} (n-2a) \cos(\frac{2\pi a}{d}) + 2 \sum_{1 \leq a \leq \frac{n}{2}, \gcd(a,n)=1} \sin(\frac{\pi n}{d}) \cos(\frac{(n-2a)\pi}{d}).$$

Since $d \geq 2n$ and $1 \leq a \leq \frac{n}{2}$ we have

$$0 \leq \frac{2\pi a}{d} \leq \frac{\pi}{2}, \quad 0 \leq \frac{(n-2a)\pi}{d} \leq \frac{\pi}{2}, \quad 0 < \frac{\pi n}{d} \leq \frac{\pi}{4}.$$

Consequently, we see that

$$\zeta_d^{-n} G_n(\zeta_d) \geq 0.$$

Furthermore, if $G_n(\zeta_d) = 0$ then $\cos(\frac{2\pi}{d}) = 0$. This implies that $d = 4$ and hence $n = 2$. □

We remark that by Equation 4.2, we know that $\zeta = \zeta_d$ is simple root of F_n if and only if $F_n(\zeta) = 0$ and $G_n(\zeta) \neq 0$ (we recall Remark 4.16 that when we evaluate G_n at ζ_d, we implicitly assume that d is not a divisor of n.) Furthermore, by the recursive formula for F_n described in Proposition 4.10, we also see that if $p \nmid n$, then

$$G_{np}(x) = \left(\frac{1 - x^{np}}{1 - x^n}\right)^2 G_n(x) - pG_n(x^p).$$

In order to study the multiplicity of Φ_d in F_n, we introduce the following abstract nonsense proposition.

Proposition 4.18. *Let $G(x) = \frac{P(x)}{Q(x)}$ where $P(x), Q(x)$ are polynomials with rational coefficients. Let $G_p(x)$ be the following rational function*

$$G_p(x) = G(x) - pG(x^p).$$

Let d be a positive number and $\zeta = \zeta_d$ a primitive d-root of unity such that $Q(\zeta) \neq 0$. Let m be a prime number such that $p \nmid d$. Then

$$\text{mult}_{\zeta_d}(G) = \text{mult}_{\zeta_d}(G_p).$$

Proof. By induction, we can see that for each $k \geq 0$

$$G_p^{(k)}(x) = G^{(k)}(x) - p^{k+1}x^{k(p-1)}G^{(k)}(x^p) + \sum_{0 \leq h \leq k-1} M_{k,h}(x)G^{(h)}(x^p), \tag{4.5}$$

where $M_{k,h} \in \mathbb{Q}[x]$. In order to prove the above statement, we will show that for all k

$$G(\zeta) = \dots G^{(k)}(\zeta) = 0$$

if and only if

$$G_p(\zeta) = \dots G_p^{(k)}(\zeta) = 0$$

Let us consider the base case $k = 0$. Suppose that $G(\zeta) = 0$. Since ζ and ζ^p are Galois-conjugate and G is a rational function with rational coefficients, $G(\zeta^p) = 0$ as well. We conclude that $G_p(\zeta) = 0$. Conversely, suppose that $G_p(\zeta) = 0$. Then

$$G(\zeta) = pG(\zeta^p).$$

Let $N : \mathbb{Q}(\zeta) \to \mathbb{Q}$ be the norm map with respect to the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Since $p \nmid d$, ζ and ζ^p are conjugate. Consequently, $G(\zeta)$ and $G(\zeta^p)$ are conjugate as well. We then have

$$N(G(\zeta^p)) = N(G(\zeta)) = p^{\varphi(d)}N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(G_n(\zeta^p)).$$

This implies that $N(G(\zeta^p)) = N(G(\zeta)) = 0$. We conclude that $G(\zeta) = 0$. Assume that the above statement holds for $k-1$. Let us show that it is true for k as well. First, suppose that

$$G(\zeta) = \dots G^{(k)}(\zeta) = 0$$

By the induction hypothesis, we already know that

$$G_p(\zeta) = \dots G_p^{(k-1)}(\zeta) = 0$$

We will show that $G_p^{(k)}(\zeta) = 0$ as well. In fact, since ζ and ζ^p are conjugate, we know that $G^{(h)}(\zeta^p) = 0$ for $0 \leq h \leq k$ as well. By Equation 4.5, we conclude that $G_p^{(k)}(\zeta) = 0$. Conversely, assume that

$$G_p(\zeta) = \dots G_p^{(k)}(\zeta) = 0$$

By the induction hypothesis, we know that

$$G(\zeta) = \dots G^{(k-1)}(\zeta) = 0.$$

Let us show that $G^{(k)}(\zeta) = 0$. By the same conjugacy argument, we know that

$$G(\zeta^p) = \dots G^{(k-1)}(\zeta^p) = 0.$$

Additionally, since $G_p^{(k)}(\zeta) = 0$, Equation 4.5 tells us that

$$G^{(k)}(\zeta) = p^{k+1}x^{k(p-1)}G^{(k)}(\zeta^p).$$

Using the norm argument as above, we conclude that $G^{(k)}(\zeta) = 0$.

□

Corollary 4.19. *Suppose that $p \nmid nd$ and $d \nmid n$. Let $\zeta = \zeta_d$ be a primitive d-root of unity. Then*

$$\text{mult}_\zeta(G_n) = \text{mult}_\zeta(G_{np}).$$

Proof. Let us introduce the following slight modification of G_n

$$\tilde{G}_n = \frac{G_n}{(1-x^n)^2}.$$

Then we have

$$\tilde{G}_{np}(x) = \tilde{G}_n(x) - p\tilde{G}(x^p).$$

Since $d \nmid n$, ζ is not a root of ζ_d is not a root of $x^n - 1$. The above statement follows directly from Proposition 4.18. □

When $n = q$ is a prime number, we have

$$G_q(x) = \frac{x}{(1-x)^2} - \frac{qx^q}{(1-x^q)^2} = \frac{xH_q(x)}{(1-x^q)^2},$$

where

$$H_q(x) = \left(\frac{1-x^q}{1-x}\right)^2 - qx^{q-1}.$$

Note that $H_2(x) = x^2 + 1 = \Phi_4(x)$.

Lemma 4.20. *$H_q(x+1)$ is an Eisenstein polynomial at the prime q. Consequently, $H_q(x)$ is irreducible. Furthermore, if q is odd then for all d, ζ_d is not a root of H_q and for all $d \notin \{1, q\}$, ζ_d is not a root of G_q.*

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

$$H_q(x) \equiv (1-x)^{2(q-1)}.$$

Additionally

$$H_q(1) = q^2 - q.$$

By definition, $H_q(x+1)$ is an Eisenstein polynomial at the prime q.

Suppose that ζ_d is a root of H_q. Since $\Phi_d(x)$ and $H_q(x)$ are both irreducible, we must have $\Phi_d = H_q$. In particular

$$q^2 - q = H_q(1) = \Phi_d(1).$$

If $d = p^k$ is a prime power ($k \geq 1$) then $\Phi_d(1) = p$. In this case, we have $p = q^2 - q$. In this case, $q|p$ and hence $q = p = 2$. If d is not a prime power then $\Phi_d(1) = 1$. This implies that $q^2 - q = 1$ which is impossible. □

With these preparations, we are now able to describe the multiplicity of Φ_d in F_n for all d.

Theorem 4.21. *Let $n > 1$ be a squarefree integer. Let d be a positive integer and $\zeta = \zeta_d$ a primitive d-root of unity such that $F_n(\zeta) = 0$. Then we have the following*

(1) If $d \neq 4$, then ζ_d is a simple roof of F_n.
(2) If $d = 4$ and n is odd, Then ζ_d is a simple roof of F_n.
(3) If $d = 4$ and n is even, Then ζ_d is a double root of F_n.

Proof. Let us prove the first and the second part of the statement. Suppose that $\zeta = \zeta_d$ is a repeated root of F_n. Then we know that $d \nmid n$ and that $F_n(\zeta) = G_n(\zeta) = 0$. Let $d_1 = \gcd(n, d)$. Let us write $n = d_1 n_1$ where $\gcd(n_1, d) = 1$. Since n is a squarefree integer, this also implies that $\gcd(n_1, d_1 d) = 1$. Since $G_n(\zeta) = G_{d_1 n_1}(\zeta) = 0$, Corollary 4.19 implies that $G_{d_1}(\zeta) = 0$ as well. Since $d \geq 2d_1$, Lemma 4.17 implies that $d = 4$ and $d_1 = 2$. This contradicts our assumption that $d \neq 4$ (for the first statement) or n is odd (for the second statement.)

Let us now prove the last statement when $d = 4$ and n is even. By Corollary 4.19, we know that

$$\mathrm{mult}_{\zeta_4}(G_n) = \mathrm{mult}_{\zeta_4}(G_2) = 1.$$

Equation 4.5 then shows that $F_n(\zeta_4) = F_n'(\zeta_4) = 0$ but $F_n''(\zeta_4) \neq 0$. This shows that ζ_4 is a double root of F_n.

□

Remark 4.22. We note that the above statement does not say that $\mathrm{mult}_{\zeta_4}(F_n) = 2$ if n is even. This is only true if $F_n(\zeta_4) = 0$. For example, Proposition 4.25 below shows that if $p \equiv 3 \pmod 4$, then $F_{2p}(\zeta_4) \neq 0$. We can in fact classify all n such that ζ_4 is a factor of F_n. We will do this in the next section.

4.3. **The cases $n = p$ and $n = 2p$.** We first consider the case that $n = p$ is a prime number.

Proposition 4.23. *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 4.24. *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 4.25. *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

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

□

4.4. **Cyclotomic factors of F_n with small degree.** In this section, we give an explicit condition for which Φ_d is a factor of F_n with $d \in \{2,3,4,6\}$. The case $d = 2$ and the case $d = 3$ follow directly from Corollary **??**, Theorem 4.13, and Corollary 4.2. More precisely, we have

Proposition 4.26.

(1) Φ_2 is a factor of F_n if and only if n is odd.

(2) Φ_3 is a factor of F_n if $3 \nmid n$ and there exists a prime divisor p of n such that $p \equiv 1 \pmod 3$.

We now consider the case $d = 4$. In order to simplify our calculations, we introduce the following modification of F_n

$$\tilde{F}_n(x) = \frac{1}{1-x^n}F_n(x) = \sum_{m|n}\frac{\mu(m)x^m}{1-x^m}.$$

We remark that as long as $d \nmid n$, $F_n(\zeta_d)$ is well-defined. Furthermore, $F_n(\zeta_d) = 0$ if and only if $\tilde{F}_n(\zeta_d) = 0$. Furthermore, if $p \nmid n$ then by Proposition 4.10 we have the following recursive formula

$$\tilde{F}_{np}(x) = \tilde{F}_n(x) - \tilde{F}_n(x^p).$$

By Theorem 4.13, we know that if n has a prime factor p such that $p \equiv 1 \pmod 4$ then $F_n(\zeta_4) = 0$. It turns out that the converse is true as well. This follows from the following proposition.

Proposition 4.27. *Suppose that $n = 2^s p_1 p_2 \ldots, p_r$ where $s \in \{0, 1\}$ and $p_1, \ldots, p_r$ are distint odd primes of the form $4k + 3$. Then*

$$\tilde{F}_n(\zeta_4) = 2^{r-1}\zeta_4.$$

In particular, $F_n(\zeta_4) \neq 0$.

Proof. Let us write $\zeta = \zeta_4$ for simplicity. First, we remark that if $s = 1$ and $m = p_1 p_2 \ldots p_r$ then

$$\tilde{F}_n(\zeta) = \tilde{F}_m(\zeta) - \tilde{F}_m(\zeta^2) = \tilde{F}_m(\zeta) - \tilde{F}_m(-1).$$

By Theorem 4.13, we know that $F_m(-1) = 0$. Therefore $\tilde{F}_n(\zeta) = \tilde{F}_m(\zeta)$. For this reason, it is sufficient to prove the above statement when n is odd. We will prove this by induction. If $n = p_1$ is a prime of the form $4k + 3$ then we have

$$\tilde{F}_n(\zeta) = \frac{\zeta}{1 - \zeta^p} \frac{1 - \zeta^{p-1}}{1 - \zeta} = \zeta.$$

Suppose the required formula is true if n has r odd prime factors. Let us now suppose that $n = p_1 p_2 \ldots p_{r+1}$. Let $m = p_2 \ldots p_{r+1}$. We already know that $\tilde{F}_m(\zeta) = 2^{r-1}\zeta_4$. By taking conjugation, we see that $\tilde{F}_m(\zeta^3) = 2^{r-1}\zeta^3 = -2^{r-1}\zeta$ as well. Therefore, we have

$$\tilde{F}_n(\zeta) = \tilde{F}_m(\zeta) - \tilde{F}_m(\zeta^{p_1}) = \tilde{F}_m(\zeta) - \tilde{F}_m(\zeta^3) = 2^r\zeta.$$

By the induction principle, we conclude that $\tilde{F}_n(\zeta_4) = 2^{r-1}\zeta_4$. □

By a similar method, we can give another proof for the classification of all n such that $F_n(\zeta_3) = 0$ as well. In fact, we have the following proposition.

Proposition 4.28. *$F_n(\zeta_3) = 0$ if and only if $3 \nmid n$ and there exists a prime divisor p of n such that $p \equiv 1 \pmod 3$.*

Proof. By 4.13, we know that the if part is true. Let us prove the "only if" part. Suppose to the contrary that $n = p_1 p_2 \ldots p_r$ where p_i are primes of the form $3k + 2$. We will show by induction that

$$\tilde{F}_n(\zeta_3) = 2^{r-1}\frac{1}{\sqrt{3}}i.$$

In fact, when $r = 1$, we know that

$$\tilde{F}_{p_1}(x) = \frac{1}{1 - x^{p_1}} \frac{x(1 - x^{p_1 - 1})}{1 - x}.$$

By direct calculations, we can see that $F_{p_1}(\zeta_3) = \frac{1}{\sqrt{3}}i$. For the general case, we use the recursive formula

$$\tilde{F}_n(\zeta_3) = \tilde{F}_{mp_1}(\zeta_3) = \tilde{F}_m(\zeta_3) - \tilde{F}_m(\zeta_3^{p_1}),$$

where $m = p_2 \ldots p_r$. Using the fact that $p_1 \equiv 2 \pmod 3$, we know that $\zeta_3^{p_1} = \zeta_3^2 = \overline{\zeta_3}$. Consequently $\tilde{F}_m(\zeta_3^{p_1}) = \overline{\tilde{F}_n(\zeta_3)}$ and hence

$$\tilde{F}_n(\zeta_3) = \tilde{F}_{mp_1}(\zeta_3) - \overline{\tilde{F}_{mp_1}(\zeta_3)} = 2\Im(\tilde{F}_m(\zeta_3)).$$

The required formula is obtained from the above recursive formula by induction. □

By a similar argument, we can also deal with the case $d = 6$.

Proposition 4.29. *$F_n(\zeta_6) = 0$ if and only if $6 \nmid n$ and there exists a prime divisor p of n such that $p \equiv 1 \pmod 6$.*

Proof. The if part follows from Theorem 4.13. Let's focus on the "only if" part of the proposition. Suppose that $n = p_1 \dots p_r$ where $p_i \not\equiv 1 \pmod 6$. We can assume that $n > 6$. Then, for a prime divisor p of n, either $p = 2$, $p = 3$ or $p \equiv 5 \pmod 6$. First, let us suppose that $\gcd(n, 6) = 1$. Then all prime divisors of n are of the form $6k + 5$. By induction, we see that

$$\tilde{F}_n(\zeta_6) = 2^{r-1}\sqrt{3}i.$$

Let us consider the case that $2|n$ but $3 \nmid n$. Let $n = 2m$. We have

$$\begin{aligned}\tilde{F}_n(\zeta_6) &= \tilde{F}_m(\zeta_6) - \tilde{F}_m(\zeta_6^2) = \tilde{F}_m(\zeta_6) - \tilde{F}_m(\overline{\zeta_3}) = \tilde{F}_m(\zeta_6) - \overline{\tilde{F}_m(\zeta_3)} \\ &= 2^{r-2}\sqrt{3}i + 2^{r-2}\frac{1}{\sqrt{3}}i = 2^{r-2}[\sqrt{3} + \frac{1}{\sqrt{3}}]i.\end{aligned}$$

We remark that the second to last equality follows from our inductive formula for $\tilde{F}_m(\zeta_6)$ and the formula for $\tilde{F}_m(\zeta_3)$ that we derived in the proof of Proposition 4.28. Finally, let us consider the case $3|n$ but $2 \nmid n$. Let us write $n = 3m$. Then

$$\begin{aligned}\tilde{F}_n(\zeta_6) &= \tilde{F}_m(\zeta_6) - \tilde{F}_m(\zeta_6^3) = \tilde{F}_m(\zeta_6) - \tilde{F}_m(-1) \\ &= 2^{r-2}\sqrt{3}i - 0 = 2^{r-2}\sqrt{3}i.\end{aligned}$$

We conclude that in all cases $\tilde{F}_n(\zeta_6) \neq 0$. This completes the proof.

□

5. The case $n = pq$

In this section, we study the case $n = pq$ where $q < p$ are two odd prime numbers. The following proposition is a direct consequence of Theorem 4.13

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 $\gcd(qp + 1, p + q)$.

If we assume the converse of Lemma 4.3 holds, the above proposition will capture all possible cyclotomic factors of F_{pq}. More precisely, we have the following.

Proposition 5.2. *Assume that the converse of Lemma 4.3 is true. Then Proposition 5.1 is a complete characterization of all cyclotomic factors of $F_n(x)$, when $n = pq$ is a product of two primes $p > q > 2$.*

Proof. We have

$$
\begin{aligned}
(x^p-1)(x^q-1)F_n(x) &= (x^p-1)\sum_{1\le i\le q-1}\left(x^{qp+i}+x^{ip}-x^i-x^{ip+q}\right)\\
&= x^{qp}-x^p-x^{qp+q}+x^{p+q}+\\
&\qquad \sum_{1\le i\le q-1}\left(x^{(q+1)p+i}-x^{qp+i}-x^{p+i}+x^i\right). \qquad (5.1)
\end{aligned}
$$

To evaluate at a primitive d-th root of unity ζ_d, it is enough to consider the monomial exponents modulo d. Lemma 4.3 says that we only need to consider the following cases.
Case 1: Suppose $d = pd_1$ with $1 < d_1$ dividing $\phi(q)$. We can without loss of generality consider the monomial exponents in Eq. (5.1) modulo $p(q-1)$. Thus we get

$$
\sum_{1\le i\le q-1}\left(x^{2p+i}-2x^{p+i}+x^i\right) = (x^p-1)^2\sum_{1\le i\le q-1}x^i = (x^p-1)^2\frac{x(x^{q-1}-1)}{x-1},
$$

whose value at ζ_d is clearly non-zero.
Case 2: Suppose $d = qd_1$ with $1 < d_1$ dividing $\phi(p)$. Considering the monomial exponents in Eq. (5.1) modulo $q(p-1)$, we get

$$
\begin{aligned}
\sum_{1\le i\le q}\left(x^{p+q-1+i}-x^{q+i}-x^{p-1+i}+x^i\right) &= (x^{p+q-1}-x^q-x^{p-1}+1)\frac{x(x^q-1)}{x-1}\\
&= (x^{p-1}-1)(x^q-1)\frac{x(x^q-1)}{x-1},
\end{aligned}
$$

whose value at ζ_d is clearly non-zero.
Case 3: Suppose $1 < d$ divides $\phi(n)$. Considering the monomial exponents in Eq. (5.1) modulo $\phi(n)$, we get

$$
\begin{aligned}
&x^{p+q-1}-x^p-x^{p+2q-1}+x^{p+q}+\sum_{1\le i\le q-1}\left(x^{2p+q+i-1}-x^{p+q+i-1}-x^{p+i}+x^i\right)\\
&=\sum_{i\in S_1}x^i-\sum_{i\in S_2}x^i,
\end{aligned}
$$

where $S_1 = \{1\le i\le q-1\}\cup\{p+q-1, p+q\}\cup\{2p+q\le i\le 2p+2q-2\}$ and $S_2 = \{p\le i\le p+2q-1\}$. Note that S_2 is a sequence of $2q$ consecutive integers. Therefore, this polynomial evaluated at ζ_d is zero if and only if S_1 modulo d is equal to the same set of consecutive residues modulo d. This happens if and only if d divides $p-1$, $q-1$, or $p+q$. If d divides $p+q$, then d also divides $pq+1$ because $pq+1 = \phi(n)+(p+q)$. □

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

$$
S_n = \{d>1, d\neq q, d\mid p-1\}\cup\{d>1, d\mid q-1\}\cup\{d>1, d\mid \gcd(qp+1, p+q)\}. \qquad (5.2)
$$

Definition 5.3. 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 5.4. *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,*

$$\deg(f_n) = \begin{cases} pq - p - q - 1 + D_1 + D_3 + D_4 - D_2 & \text{if } p \not\equiv 1 \pmod{q} \\ pq - p - 2 + D_1 + D_3 + D_4 - D_2 & \text{if } p \equiv 1 \pmod{q}. \end{cases}$$

Furthermore, we have

$$f_n(1) = \begin{cases} \dfrac{D_1 D_3 D_4}{2D_2} & \text{if } p \not\equiv 1 \pmod{q} \\ \dfrac{q D_1 D_3 D_4}{2D_2} & \text{if } p \equiv 1 \pmod{q}, \end{cases}$$

$$f_n(-1) = \frac{-D_1 D_3 D_4}{2D_2}.$$

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

$$f(x) = \frac{1 - x^{q-1}}{1 - x} = \frac{F_q(x)}{x}, \quad g(x) = \begin{cases} \frac{1-x^{p-1}}{1-x^{D_1}} & \text{if } p \not\equiv 1 \pmod{q} \\ \frac{(1-x^{p-1})(1-x)}{(1-x^{D_1})(1-x^q)} & \text{if } p \equiv 1 \pmod{q}, \end{cases}$$

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

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

It is also clear from this description that

$$f(1) = q - 1, \quad g(1) = \begin{cases} \frac{p-1}{D_1} & \text{if } p \not\equiv 1 \pmod{q} \\ \frac{p-1}{qD_1} & \text{if } p \equiv 1 \pmod{q}, \end{cases}$$

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

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 $F_n(-1) = f(-1) = 0$. Hence

$$F_n'(-1) = (-1)f'(-1)g(-1)h(-1)f_n(-1).$$

Thus, we calculate $F_n'(-1)$ and $f'(-1)$ using Proposition **??**, and $g(-1)$ and $h(-1)$ using calculus to infer the value of $f_n(-1)$:

$$F_n'(-1) = \frac{(p-1)(q-1)}{2}, \quad f'(-1) = -F_q'(-1) = \frac{q-1}{2},$$
$$g(-1) = \frac{p-1}{D_1}, \quad h(-1) = \frac{2D_2}{D_3D_4}.$$

□

Here is a direct corollary of this proposition.

Corollary 5.5. *$f_{pq}(x)$ 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 $f_{pq}(-1)$. □

Definition 5.6. 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 5.7. *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 $p \not\equiv 1 \pmod{q}$, then up to squares, we have

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

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

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

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 5.4 tells us that up to squares, we have

$$\operatorname{disc}(f_n) = \begin{cases} (-1)^{\deg(f_n)/2}(-1) & \text{if } p \not\equiv 1 \pmod{q} \\ (-1)^{\deg(f_n)/2}(-q) & \text{if } p \equiv 1 \pmod{q}. \end{cases}$$

Calculating $\deg(f_n)$ modulo 4, using the formula in Proposition 5.4, we obtain the stated result. □

We now investigate the roots of the Fekete polynomials F_{pq} in $\overline{\mathbb{F}}_p$. The ultimate goal of this study is to show that f_n is separable over $\mathbb{Z}$. We will see later that, in some special cases, this can be done by showing that f_n is separable over $\mathbb{F}_p$. Before we do so, we recall the following definition.

Definition 5.8. 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

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

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

$$u_q(x) = \sum_{1 \le i \le q-1} (q-i)x^{q-1+i} + \sum_{1 \le i \le q-1} ix^{i-1}. \tag{5.3}$$

Lemma 5.9. *Over $\mathbb{F}_q[x]$, we have $u_q(x) = (x-1)^{2q-2} \pmod{q}$.*

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 $s_q'(x) = 0$. Hence

$$u_q(x) = s_q'(x)F_q(x) - F_q'(x)s_q(x) = (x-1)^{2q-2} \pmod{q}.$$ □

Corollary 5.10. *The polynomial $u_q(x)$ is irreducible.*

Proof. 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. □

Proposition 5.11. *Suppose $n = pq$ for odd primes p, q such that $q < p$. Let $x_0 \in \overline{\mathbb{F}}_p$ be a zero of $F_n(x)$. Then*

(a) $\text{mult}_{x_0}(F_n) - 1 = \text{mult}_{x_0}(u_q)$.

(b) If $\text{disc}(u_q) \neq 0 \mod p$, *then* $\text{mult}_{x_0}(F_n) \leq 2$.

(c) Suppose $x_0 \in \mathbb{F}_p$. *Then* $\text{mult}_{x_0}(F_n) - 1 = \text{mult}_{x_0}(f_n)$.

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

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

(a) Proposition 4.1 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 $\text{mult}_{x_0}(u_q) = \text{mult}_{x_0}(F_n) - 1$.

(b) This is a straight-forward consequence of part (a). If $\text{disc}(u_q) \neq 0 \mod p$, then the reduction of u_q modulo p is separable. Hence $\text{mult}_{x_0}(u_q) \leq 1$ and $\text{mult}_{x_0}(F_n) \leq 2$.

(c) 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 $\text{mult}_{x_0}(F_n) - 1 = \text{mult}_{x_0}(f_n)$. □

Remark 5.12. We note that the irreducibility of the polynomial $u_q \in \mathbb{Z}[x]$, implies in particular that $\text{disc}(u_q) \neq 0$. Therefore for primes p sufficiently large compared to q, we have $\text{disc}(u_q) \neq 0 \pmod{p}$ and hence $\text{mult}_{x_0}(F_{pq}) \leq 2$.

To further study the separability of $F_n(x)$ over $\mathbb{F}_p[x]$, we introduce the following auxiliary polynomial. Let

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

where

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

Let $R_q(y)$ be the resultant of $u_q(x)$ and $a(x, y)$ with respect to the variable x.

The following proposition provides a direct link between the separability of $F_n(x)$ and the arithmetic of $R_q(y)$.

Proposition 5.13. *Suppose that $F_n(x)$ has a repeated root $x_0 \in \overline{\mathbb{F}}_p$. Then $R_q(y)$ has a root $\mu \in \mathbb{F}_p$.*

Proof. By Proposition 5.11 Part (a), $\mathrm{mult}_{x_0}(u_q) = \mathrm{mult}_{x_0}(F_n) - 1 \geq 1$, 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 $(x-1)F_q(x) = x(x^{q-1}-1)$ 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

$$\mathrm{resultant}(u_q(x), a(x,\mu)) = R_q(\mu) = 0. \qquad \square$$

5.1. **Further properties of the resultant $R_q(y)$.** We find through numerical data that $R_q(y)$ 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 5.14. *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 ζ_k, $k = 1, \ldots, q$, be the qth root of unity. Then

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

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

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

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

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

and thus

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

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

$$\mathrm{Res}(s_q(x), t_q(x)) = \prod_{k=1}^{n} t_q(\zeta_k) = (q-1)\prod_{k=1}^{q-1}\frac{\zeta_k^q - \zeta_k}{\zeta_k - 1} = (q-1)\prod_{k=1}^{q-1}\frac{1-\zeta_k}{\zeta_k - 1} = q-1. \quad \square$$

Proposition 5.15. *Over $\mathbb{F}_q[y]$, $R_q(y)$ factors as follow*

$$R_q(y) = y^{2q-2}.$$

Proof. Using the property that $\mathrm{Res}(AB, C) = \mathrm{Res}(A, C)\,\mathrm{Res}(B, C)$ and the fact that $u_q(x) = (x-1)^{2q-2}$ over $\mathbb{F}_q[x]$ (Lemma 5.9) we have

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

Proposition 5.16. *$R_q(y)$ 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

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

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

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

This shows that $R_q(y)$ is an even polynomial. We note also that

$$R_q(y) = \prod_{i=1}^{2q-2}(s_q(z_i) - y t_q(z_i)).$$

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

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

Conjecture 5.17. There exists $h_1, h_2 \in \mathbb{Z}[x]$ such that

$$R_q(y) = h_1(y^2)^2 - qh_2(y^2)^2.$$

Conjecture 5.18. $R_q(\sqrt{q}y) = q^{q-1}c(y)$ 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 5.2 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

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

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,*

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

and

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

Proof. We have

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

The statement then follows. □

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

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

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

$$\begin{aligned} a_k &= b_k \qquad \text{if } k \in \{0, 1, 2, 3, 2p-7, 2p-6, 2p-5, 2p-4\} \\ a_k + a_{4+k} &= b_{4+k} \qquad \text{if } 0 \le k \le 2p-8. \end{aligned}$$

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 $p \le k \le 2p-4$. □

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 5.11.

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 5.11 Part (a).

The 'if' part of the second statement also follows from Proposition 5.11 Part (a). Now we discuss the 'only if' part. We suppose that the multiplicity of $x_0 \in \overline{\mathbb{F}}_p$ is 2. By Proposition 5.13, 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 $x_0 \in \mathbb{F}_p$. □

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 $\left(\frac{3}{p}\right) = -1$ 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 $\left(\frac{3}{p}\right) = 1$. 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 $\left(\frac{-1}{p}\right) = -1$, 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, $\left(\frac{2c}{p}\right) = \left(\frac{-2c}{p}\right)$. 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. □

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 5.4.

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

(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* $u_5(x_0) = 0$.

Proof of Theorem 7.1 part (1). Following the proof of Proposition 5.11, if the discriminant of u_5 is not zero modulo p, we get the desired result. We compute that

$$\operatorname{disc}(u_5) = -1 \cdot 2^{12} \cdot 5^7 \cdot 11^2.$$

When $p = 11$, we check directly that $F_{5p}(x)$ has no repeated root in $\overline{\mathbb{F}}_p$. Proof of Theorem 7.1 part (2) will be provided below. □

In this section, we use $a_\mu(x)$ for $a(x, \mu) = (x^5 - 1) - \mu(x + x^2 + x^3 + x^4)$. Using Sagemath, we see that the resultant of $a_\mu(x)$ and $u_5(x)$ is given by

$$R_5(\mu) = \operatorname{Res}(a_\mu(x), u_5(x)) = 64\mu^8 - 400\mu^6 - 500\mu^4 - 25000\mu^2 - 12500.$$

Because $a_\mu(x)$ and $u_5(x)$ have a common root, their resultant must be 0. In other words, we know that $\mu \in \mathbb{F}_p$ is a root of $R_5(y)$. Using Sagemath, we can see that we can rewrite $R_5(y)$ in the following form

$$R_5(y) = (8y^4 - 25y^2 + 125)^2 - 5(25y^2 + 75)^2.$$

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 $R_5(y)$ has a root $\mu \in \mathbb{F}_p$ where

$$R_5(y) = (8y^4 - 25y^2 + 125)^2 - 5(25y^2 + 75)^2.$$

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

$$0 = R_5(\mu) = (8\mu^4 - 25\mu^2 + 125)^2 = 2^4 \times 17.$$

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

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

$$\begin{aligned} u_5(x) &= (1 + x + x^2 + x^3 + x^4)^2 - 5x^2 \\ &= (1 + x + x^2 + x^3 + x^4 - cx^2)(1 + x + x^2 + x^3 + x^4 + cx^2). \end{aligned}$$

Let $m(x)$ be the minimal polynomial of x_0 over $\mathbb{F}_p$. Then $m(x)$ is a common divisor of $u_5(x)$ and $a_\mu(x)$. Up to a choice of c, we can assume that $m(x)$ is a divisor of

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

By polynomial division, we see that $a_\mu(x) = (x - \mu - 1)v(x) + w(x)$, where $w(x) = cx^3 - (c + c\mu)x^2 + \mu$. Since x_0 is a common root of $v(x)$ and $a_\mu(x)$, we get that x_0 is a common root 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

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

From $a_\mu(x_0) = 0$, we see that $x_0^5 - 1 = \mu(x_0 + x_0^2 + x_0^3 + x_0^4) = 1 - x_0^5$. Hence $x_0^5 - 1 = 0$. Thus $0 = (x_0^5 - 1) = (1 + x_0 + x_0^2 + x_0^3 + x_0^4)(x_0 - 1) = cx_0^2(x_0 - 1)$. This implies that $x_0 = 0$ or 1, 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

$$\frac{a + ab}{b} = 1 \quad \text{and} \quad \frac{1 + a^2 + b^2}{b} = 1 - c.$$

Hence

$$a + ab = b \text{ and } 1 + a^2 + b^2 = b - bc.$$

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

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

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

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

From (2) and (3) we get

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

Hence

$$b^2 - b^3 = a^2 + a^2b + a = ab + a = b.$$

(For the second and last equality, we use (1).) Since $b \neq 0$, we obtain that $b^2 - b + 1 = 0$.

Now from (2), we have $-bc = 1 + a^2 + b^2 - b = a^2$. Hence $a^4 = b^2c^2 = 5b^2$. From (1), we obtain $b = a(1 + b)$. Hence $b^4 = a^4(1 + b)^4 = 5b^2(1 + b)^4$. Thus

$$b^2 = 5(1 + b)^4 = 5(1 + 2b + b^2)^2 = 5(3b)^2 = 45b^2.$$

We obtain that $p \mid 44$. Hence $p = 11$. But we can check directly that $F_{5\cdot 11}(x)$ has no repeated root in $\overline{\mathbb{F}}_p$, a contradiction. $\square$

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. [20, 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 5.4).

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. By Proposition 6.2, the middle coefficient of $f_{3p} \in \{-2, -1, 0, 1, 2\}$. We checked that for $q = 5$ and $p \leq 1000$, this is still true. However, this is unfortunately 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 $n = pq$ with $13 \leq q < p$ and $n \leq 6000$ as of January 2023 (the case $q < 13$ will be studied in more detail in the next section). 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. We refer the readers to the GitHub repository [8] for the data regarding this issue.

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 groups of f_n and g_n.

9.1. The 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 permuting 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. *(*[21, 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 propose the following question.

Question 9.3. Let $n = pq$ be a product of two distinct odd prime numbers. Is it true that 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. *The answer for Question 9.3 is affirmative 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. **The 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 [20, Lemma 11.1].)

Lemma 9.5.

$$\begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z})^m \rtimes S_m & \hookrightarrow & S_{2m} \\ & \searrow^{\Sigma} & \downarrow{\scriptstyle sgn} \\ & & \mathbb{Z}/2 \end{array}$$

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. *(*[20, 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* [20, 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 5.7, 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 5.7, 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 ask the following question.

Question 9.10. Let $n = pq$ as before and $2m = \deg(f_n)$. Is it true that the following statements 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 one of 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. *The answer to Question 9.10 is affirmative 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* $11 < p < 300$.

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. *Acta Arithmetica*, 184(3):215–230, 2018.

[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. *Annales de l'institut Fourier*, 50(3):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] P. Erdos and P. Turán. On the distribution of roots of polynomials. *Annals of mathematics*, pages 105–119, 1950.

[13] 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.

[14] A. Granville. The distribution of roots of a polynomial. In *Equidistribution in number theory, an introduction*, pages 93–102. Springer, 2007.

[15] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford university press, 1979.

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

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

[18] F. Lemmermeyer. *Quadratic number fields*. Springer Undergraduate Mathematics Series. Springer, 2021.

[19] 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.

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

[21] J. Mináč, T. T. Nguyen, and N. D. Tân. Fekete polynomials, quadratic residues, and arithmetic. *Journal of Number Theory*, 242:532–575, 2023.

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