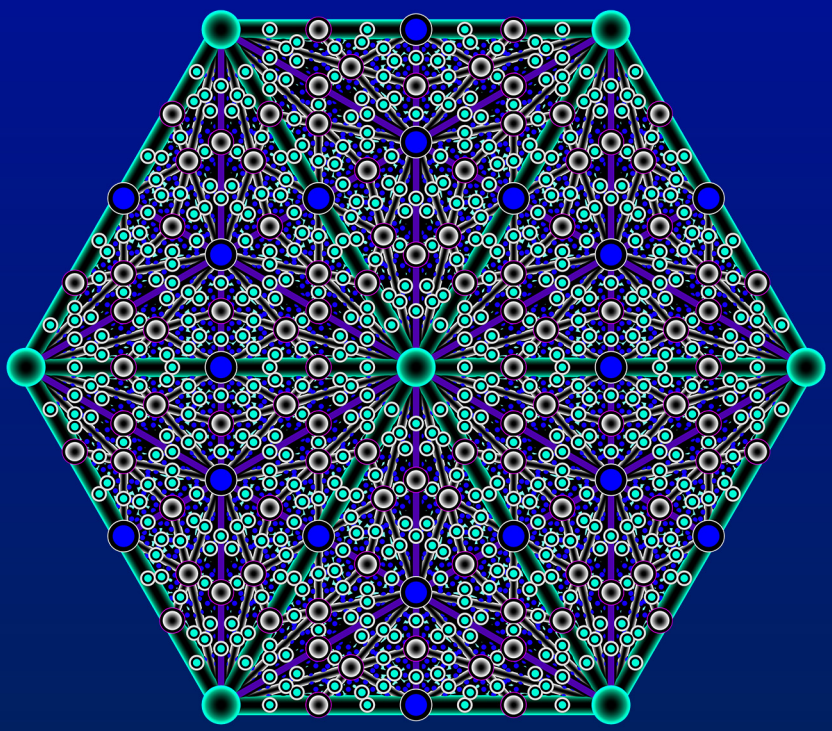
JOURNAL OF EXPERIMENTAL MATHEMATICS



ASSOCIATION FOR MATHEMATICAL RESEARCH

VOLUME 1 ISSUE 1

2025

JOURNAL OF EXPERIMENTAL MATHEMATICS

PUBLISHED BY

Association for Mathematical Research, amathr.org,
Davis, CA; Jenkintown PA.

JOURNAL OF EXPERIMENTAL MATHEMATICS, 1(1):51–93, 2025
jexpmath.org

Fekete polynomials of principal Dirichlet characters

Shiva Chidambaram [*] Ján Mináč [†]
Tung T. Nguyen [‡] Nguyễn Duy Tân [§]

Received 5 Dec 2023; Revised 24 Jan 2024; Accepted 1 Feb 2024

Abstract:

Fekete polynomials associated to quadratic Dirichlet characters have interesting arithmetic properties, and have been studied in many works. In this paper, we study a seemingly simpler yet rich variant: the Fekete polynomial $F_n(x) = \sum_{a=1}^{n} \chi_n(a)x^a$ associated to a principal Dirichlet character χ_n of modulus n. We investigate the cyclotomic factors of F_n and conjecturally describe all of them. One interesting observation from our computations is that the non-cyclotomic part f_n of $F_n(x)/x$ seems to be always irreducible. We study this factor closely in the special case that n is a product of two odd primes, proving separability in specific cases, and studying its coefficients and special values. Combining these theoretical results with computational evidence lets us identify the Galois group of f_n for small n, and raises precise questions in general.

[*]SC was supported by Simons Foundation grant 550033

[†]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.

[‡]JM and TN acknowledge the support of the Western Academy for Advanced Research.

[§]NDT is funded by Vingroup Joint Stock Company and supported by Vingroup Innovation Foundation (VinIF) under the project code VINIF.2021.DA00030.

DOI: 10.56994/JXM.001.001.004

Key words and phrases:
Fekete Polynomials; Cyclotomic Polynomials; Separability; Irreducibility; Galois Groups

1 Introduction

Let $\chi\colon (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$ be a Dirichlet character with modulus $n > 1$. Associated to χ is the Dirichlet L-function defined by

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

This infinite series is absolutely convergent when $\Re(s) > 1$. The function $L(\chi,s)$ has a meromorphic continuation to the entire complex plane, with a simple pole at $s = 1$ in the case χ is a principal character. Furthermore, $L(\chi,s)$ has the following integral representation (see [MNT24, Proposition 3.3]. The character χ is assumed to be primitive in [MNT24], but it is not necessary and 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

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

While studying quadratic characters $\chi = \left(\frac{\cdot}{p}\right)$ of prime conductor p, 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 zeroes on $(0,\infty)$. In this sense, the study of $F_\chi(x)$ could shed light on the existence of Siegel zeroes near $s = 1$. For this historical reason, the $F_\chi(x)$ are called Fekete polynomials.

Fekete polynomials have a rich mathematical history. They appear in Gauss's sixth proof of the quadratic reciprocity law (see [Lem21, Chapter 10, Section 3]). Various aspects of Fekete polynomials have been studied over the years, including their extremal properties (see [Bor02, BCY01]), Mahler measure (see [Erd18, KLM23]), connections to oscillations of quadratic L-functions (see [BM90]), and distribution of their complex roots ([CGPS00]).

In recent works ([MNT24, MNT23]), the last named three authors have analyzed the arithmetic properties of Fekete polynomials when χ is a primitive quadratic Dirichlet character. These works have shown that Fekete polynomials contain valuable arithmetic information, such as class number and orders of K-groups of certain quadratic fields. Furthermore, extensive computational evidence suggests that $F_\chi(x)/x$ has exactly one irreducible non-cyclotomic factor f_χ, and that the Galois group of f_χ is as large as possible, as stated in [MNT23, Conjecture 4.9, Conjecture 4.13] and [MNT24, Conjecture 11.16].

In this article, we consider the story for principal Dirichlet characters. Already in this seemingly simple situation, we notice some interesting phenomena akin to the primitive quadratic case discussed above. Concretely, we consider $\chi_n\colon \mathbb{Z} \to \mathbb{C}^\times$ defined by

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

and let $F_n(x)$ denote the associated Fekete polynomial $F_{\chi_n}(x)$. That is,

$$F_n(x) = \sum_{\substack{0 \le a \le n-1 \\ \gcd(a,n)=1}} x^a. \tag{1.2}$$

Since $\gcd(n-1,n) = 1$, the degree of F_n is $n-1$. In this article, we begin the study of F_n, focusing in particular on the determination and arithmetic of the factors of F_n, both cyclotomic and non-cyclotomic.

We observe that the non-cyclotomic part of $F_n(x)/x$, which we denote by f_n, seems to be always irreducible. Similar to the case of quadratic characters investigated in [MNT24, MNT23], the Galois group of f_n is as large as possible subject to a condition on the discriminant. We also notice that the coefficients of f_n are relatively small. When $n = 3p$ for a prime $p > 3$, we prove in Theorem 4.2 that the coefficients of f_{3p} belong to the set $\{-2,-1,0,1,2\}$. This 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 we discovered many results in our article by computing and analyzing a large dataset. The codes and data are available in the GitHub repository [CMNT23].

We remark that the theory of Fekete polynomials is closely related to the construction of certain Paley graphs. When χ is a primitive quadratic Dirichlet character, this connection is discussed in [MMNT24]. When χ is a principal Dirichlet character, the corresponding Paley graph is called a unitary Caley graph (see [BI15, KS07]). These types of Paley graphs have found applications in various fields such as coding and cryptography theory (see [GK11, Jav14]). We hope that this work sheds more light on further applications of Fekete polynomials and Paley graphs.

The article is structured as follows. In Section 2, we present our main results concerning the factors of F_n. Firstly in Section 2.1, we show that restricting to squarefree n does not miss any interesting phenomena. We then proceed to describe in Theorem 2.19 a large source of cyclotomic factors of F_n and prove in Theorem 2.29 that all cyclotomic factors are simple factors, with the exception of the 4-th cyclotomic polynomial $\Phi_4(x) = x^2+1$ which occurs with multiplicity 2 when n is even. We also make a conjecture relating to the full description of cyclotomic factors of F_n (see Conjecture 2.11). Section 3 is devoted to the case where $n = pq$ for distinct odd primes p,q. We conjecturally determine all cyclotomic

factors of F_n in this special case (see Theorem 3.2). Based on this, we define the Fekete polynomial f_n and its trace polynomial g_n. We then study some arithmetic properties of F_n in characteristic p with the goal of showing that f_n is separable. In Section 4, we focus on the case $n = 3p$. We show in Theorem 4.2 that the coefficients of f_{3p} lie in the set $\{-2,-1,0,1,2\}$. We also prove that f_{3p} is separable, by first proving it in characteristic p. In Section 5 we consider the case $n = 5p$, once again establishing separability of f_n, although the proof is more involved. The last two sections discuss computational techniques and results. Section 6 discusses algorithms for checking irreducibility of f_n and g_n, and Section 7 investigates their Galois groups. Finally Appendix A discusses a tangential question of an analytic flavor, about the proportion of complex zeroes of F_n on the unit circle, using the approach of [CGPS00].

2 Cyclotomic factors of F_n and their multiplicity

2.1 Reduction to the squarefree case

Let n be a positive 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 Eq. (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*

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

Proof. Since n_0 is the radical of n, we have $\gcd(a,n) = 1$ if and only if $\gcd(a,n_0) = 1$. Therefore, we have

$$\frac{F_{n_0}(x)}{1-x^{n_0}} = F_{n_0}(x)\sum_{k=0}^{\infty} x^{kn_0} = \sum_{\substack{1\le a \\ \gcd(a,n_0)=1}} x^a = \sum_{\substack{1\le a \\ \gcd(a,n)=1}} x^a = \frac{F_n(x)}{1-x^n}. \qquad \square$$

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

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

2.2 Cyclotomic factors of F_n

We let n be a positive squarefree integer here onwards, thanks to Proposition 2.1. To get started we calculate the Fekete polynomial $F_n(x)$ in a few simple situations.

Example 2.4. Let p be a prime number. Then we have the factorisation of $F_p(x)$.

$$F_p(x) = x + x^2 + \cdots + x^{p-1} = x\frac{1-x^{p-1}}{x-1} = x\prod_{\substack{d\mid p-1\\ d>1}} \Phi_d(x). \tag{2.1}$$

Example 2.5. Let p be an odd prime. Then we have the following factorisation of $F_{2p}(x)$.

$$\begin{aligned} F_{2p}(x) &= (x + x^3 + \cdots + x^{p-2}) + (x^{p+2} + x^{p+4} + \cdots + x^{2p-1}) \\ &= x(1 + x^2 + \cdots + x^{p-3})(1 + x^{p+1}) = x\frac{x^{p-1}-1}{x^2-1}\frac{x^{2(p+1)}-1}{x^{p+1}-1} \\ &= x\prod_{2<d\mid(p-1)} \Phi_d(x) \prod_{\substack{d\mid 2(p+1)\\ d\nmid p+1}} \Phi_d(x). \end{aligned} \tag{2.2}$$

While we were able to completely describe the cyclotomic factors of F_n in the two examples above, this is quite delicate in general. Moreover, these examples are unrepresentative of the general situation where non-cyclotomic factors also show up. Using SageMath we computed the factorisation of the Fekete polynomial F_n as defined in Eq. (1.2) for all $n < 10^4$. When $n \neq p$ or $2p$ for any prime p, we observe that $F_n(x)/x$ has many cyclotomic factors and *exactly one* irreducible non-cyclotomic factor. This striking observation leads us to the study of the cyclotomic factors of F_n.

Our starting point in this endeavor is the result that if $d|n$ then the d-th cyclotomic polynomial Φ_d is *not* a factor of F_n. This is a direct consequence of the theory of Ramanujan sums (see [HW79] for a detailed treatment) which is partially summarized in the following proposition.

Proposition 2.6. *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 [HW79, Section 5.6]). Hence by [HW79, Theorem 272], we have $F_n(\zeta_d) = \dfrac{\mu(d)\varphi(n)}{\varphi(d)}$.

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

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

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

Hereafter we assume that $d \nmid n$. Let $d_1 = \gcd(d,n)$ so that $d_1 \neq d$, and let S be the set $\{0 \le a < d | \gcd(a,d_1) = 1\}$. Note that if we identify the integer residues modulo d with the set $[d] = \{0,1,\ldots,d-1\}$, then $S \subset [d]$ is the preimage of the set $(\mathbb{Z}/d_1)^\times$ under the reduction map $\mathbb{Z}/d \to \mathbb{Z}/d_1$. Thus we have $\#S = \frac{\varphi(d_1)d}{d_1}$. Consider the polynomial $F_S(x) = \sum_{s\in S} x^s$. The following lemma gives some useful information about F_S.

Lemma 2.8. *With notation as above, we have $F_S(x) = \dfrac{1-x^d}{1-x^{d_1}} F_{d_1}(x)$. Let $m|d$ be a positive integer, and $\zeta = \zeta_m$ be a primitive m-th root of unity. Then*

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

Proof. Noting that the expression $(1-x^{d_1})F_S(x)$ is a telescopic sum, we get

$$(1-x^{d_1})F_S(x) = (1-x^{d_1}) \sum_{0\le j<d/d_1} \sum_{\substack{1\le i\le d_1\\ (i,d_1)=1}} x^{jd_1+i} = (1-x^d)F_{d_1}(x).$$

Since $m|d$ we have $1-\zeta^d = 0$. If $m \nmid d_1$, then $1-\zeta^{d_1} \neq 0$. So $F_S(\zeta) = 0$. If $m|d_1$, then the value of $\frac{1-x^d}{1-x^{d_1}}$ at $x = \zeta$ is $\frac{d}{d_1}$. Further Proposition 2.6 gives $F_{d_1}(\zeta) = \frac{\mu(m)\varphi(d_1)}{\varphi(m)}$. □

We can now state a sufficient condition for the d-th cyclotomic polynomial Φ_d to be a factor of F_n. Note that, in order to determine whether $F_n(\zeta_d)$ is zero or not, it is sufficient to consider $F_n(x) \pmod{x^d-1}$.

Proposition 2.9. *Let n be a positive squarefree integer. Let $d > 1$ be an integer not dividing n. Let $d_1 = \gcd(d,n)$ and $S = \{1 \le a \le d | \gcd(a,d_1) = 1\}$. If the elements of $\{1 \le a \le n | \gcd(a,n) = 1\}$ when reduced modulo d, equidistribute among the elements of S, then the d-th cyclotomic polynomial Φ_d divides F_n.*

Proof. Let $F_S(x) = \sum_{s \in S} x^s$ be the polynomial introduced earlier. If the equidistribution condition holds, then by reducing modulo d the exponents of monomials in F_n, we see that $F_n(x) \equiv cF_S(x) \pmod{x^d - 1}$ for some constant c. To be precise, $c = c_{n,d} = \frac{\varphi(n)}{\#S} = \frac{\varphi(n)d_1}{\varphi(d_1)d}$. So it is enough to show that $F_S(\zeta_d) = 0$, which we get from Lemma 2.8 since $d > d_1$. □

Remark 2.10. In the proof above, we saw that the equidistribution property implies $F_n \equiv cF_S \pmod{x^d - 1}$. In fact they are equivalent. If $F_n = cF_S + (x^d - 1)G$ for some $G \in \mathbb{Q}[x]$, then for each $s \in S$, we can sum the coefficients of the monomials x^a with $a \equiv s \pmod{d}$ occuring on each side. This gives us that $\#\{1 \le a \le n | \gcd(a,n) = 1, a \equiv s \pmod{d}\} = c$ independent of s, yielding equidistribution.

It is interesting to ask if the converse of Proposition 2.9 is true. In all cases we have computed, the converse holds. See Theorem 2.24 for the cases where the converse is proven to be true. This prompts us to make the conjecture.

Conjecture 2.11. Let n, d, d_1, S be as in Proposition 2.9. Then Φ_d divides F_n if and only if the elements of $\{1 \le a \le n | \gcd(a,n) = 1\}$ when reduced modulo d, equidistribute in S. Equivalently, Φ_d divides F_n if and only if $x^d - 1$ divides $F_n(x) - \frac{\varphi(n)d_1}{\varphi(d_1)d} F_S(x)$.

Remark 2.12. In Section 3 we give a complete description of the cyclotomic factors of F_n when $n = pq$ is a product of two odd primes, contingent on Conjecture 2.11.

Remark 2.13. If $d = p$ is a prime not dividing n, then it is straightforward to see that Conjecture 2.11 holds. This is because the only linear relation among $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ is that they sum to 0.

We now write down a recursive formula for F_n. This will be useful in obtaining a neater description of F_n in Proposition 2.17, which will be crucial in describing certain explicit cyclotomic factors of F_n (Theorem 2.19) and their multiplicites (Theorem 2.29).

Proposition 2.14. *Let p be a prime number such that $\gcd(p,n) = 1$. Then we have the following recursive formula*

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

Proof. We have

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

□

Corollary 2.15. *Let $n>1$ be a squarefree 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. If ζ is a primitive d-th root of unity, ζ^p is also a primitive d-th root of unity. Hence $F_n(\zeta) = F_n(\zeta^p) = 0$. Therefore, Proposition 2.14 implies $F_{np}(\zeta) = 0$ as well. □

Corollary 2.16. *Let $n>1$ be a squarefree integer and d a positive integer not dividing n. Let p,q be two distinct primes such that $p \equiv q \pmod{d}$. Then Φ_d is a factor of F_{np} if and only if it is a factor of F_{nq}.*

Proof. Since $p \neq q$ and $p \equiv q \pmod{d}$, we get that $p \nmid d$. So $d \nmid np$ and we can evaluate the formula in Proposition 2.14 at ζ_d. Since $\zeta_d^p = \zeta_d^q$, we deduce that $F_{np}(\zeta_d) = F_{nq}(\zeta_d)$. □

Using this recursive formula of Proposition 2.14, we get the following description for F_n as a sum over divisors of n. This will used crucially in what follows.

Proposition 2.17. *Let $n>1$ be a squarefree integer. Then*

$$\frac{F_n(x)}{1-x^n} = \sum_{m|n} \mu(m) \frac{x^m}{1-x^m}. \tag{2.3}$$

Proof. We prove by induction on the number of prime factors of n. If $n=q$ is prime then

$$\frac{F_q(x)}{1-x^q} = \frac{x+x^2+\cdots+x^q-x^q}{1-x^q} = \frac{x}{1-x} - \frac{x^q}{1-x^q} = \sum_{m|q} \frac{\mu(m)x^m}{1-x^m}.$$

Now suppose that the statement is true for a squarefree integer n. Let p be a prime number such that $\gcd(p,n)=1$. We show that the statement holds true for np. Indeed, by Proposition 2.14 and the induction hypothesis we have

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

□

One consequence of Proposition 2.17 is a formula for $F_n'(-1)$. This will be useful later in Section 3 to describe the value of the reduced Fekete polynomial $f_n(x)$ at $x=-1$.

Proposition 2.18. *Let $n>1$ be an integer and n_0 its radical. Then*

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

Proof. Suppose n is even. Then

$$F_n'(-1)=\sum_{\substack{1\le k\le n\\ \gcd(k,n)=1}}(-1)^{k-1}k=\sum_{\substack{1\le k\le n\\ \gcd(k,n)=1}}k=\sum_{\substack{1\le k\le n/2\\ \gcd(k,n)=1}}(k\quad+\quad n-k)=\frac{n\varphi(n)}{2}.$$

Now suppose n is odd. By Corollary 2.3, we may assume that n is squarefree. Differentiating Eq. (2.3), we get

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

Hence

$$F_n'(-1)=\frac{n}{2}\sum_{m|n}\mu(m)+\frac{1}{2}\sum_{m|n}\mu(m)m=\frac{1}{2}\mu(n)\sum_{m|n}\mu(n/m)m=\frac{1}{2}\mu(n)\varphi(n).$$ □

We now utilize Proposition 2.17 and the inclusion-exclusion principle to catch a big chunk of cyclotomic factors of F_n.

Theorem 2.19. *Let n be a positive squarefree integer. Suppose $N>1$ is a divisor of n and T is a partition of the set of all divisors of N into two-element subsets $\{a_1,b_1\},\{a_2,b_2\},\dots,\{a_l,b_l\}$. Let $D=\gcd_i(a_i+\mu(a_i)\mu(b_i)b_i)$. Then Φ_d divides F_n for every $d|D$ such that $d\nmid n$.*

Proof. Let ζ be a primitive d-th root of unity. Since $d\nmid n$, we can evaluate Eq. (2.3) at ζ.

$$\frac{F_n(\zeta)}{1-\zeta^n}=\sum_{m|n}\frac{\mu(m)\zeta^m}{1-\zeta^m}=\sum_{m|(n/N)}\sum_{i=1}^{l}\left\{\frac{\mu(a_im)\zeta^{a_im}}{1-\zeta^{a_im}}+\frac{\mu(b_im)\zeta^{b_im}}{1-\zeta^{b_im}}\right\}.$$

Let l_0 be the number of i's in $\{1,2,\dots,l\}$ such that $\mu(a_i)=\mu(b_i)$. In the case that $l_0>0$, without loss of generality, suppose that $\mu(a_i)=\mu(b_i)$ for $1\le i\le l_0$ and $\mu(a_i)=-\mu(b_i)$ for $i>l_0$. Note that this means

$$2\sum_{i=1}^{l_0}\mu(a_i)=\sum_{i=1}^{l_0}(\mu(a_i)+\mu(b_i))=\sum_{i=1}^{l}(\mu(a_i)+\mu(b_i))=\sum_{k|N}\mu(k)=0.$$

For $i > l_0$, since $d|(a_i - b_i)$ we have $\zeta^{a_i} = \zeta^{b_i}$ and hence

$$\frac{\mu(a_i m)\zeta^{a_i m}}{1-\zeta^{a_i m}} + \frac{\mu(b_i m)\zeta^{b_i m}}{1-\zeta^{b_i m}} = 0.$$

For $i \leq l_0$, since $d|(a_i + b_i)$ we have $\zeta^{a_i} = \zeta^{-b_i}$ and hence

$$\frac{\mu(a_i m)\zeta^{a_i m}}{1-\zeta^{a_i m}} + \frac{\mu(b_i m)\zeta^{b_i m}}{1-\zeta^{b_i m}} = -\mu(a_i m).$$

Putting things together, we get that

$$\frac{F_n(\zeta)}{1-\zeta^n} = \sum_{m|n} \frac{\mu(m)\zeta^m}{1-\zeta^m} = \sum_{m|(n/N)} \sum_{i=1}^{l_0} -\mu(a_i m) = -\sum_{m|(n/N)} \mu(m) \sum_{i=1}^{l_0} \mu(a_i) = 0.$$

This proves that $F_n(\zeta) = 0$, and hence Φ_d divides F_n. □

Remark 2.20. Theorem 2.19 does not describe all cyclotomic factors of F_N. For instance, when $N = 105$, the cyclotomic polynomial $\Phi_{24}(x) = x^8 - x^4 + 1$ divides F_N, but this cannot be seen through Theorem 2.19.

We will use the following special case of this theorem the most.

Corollary 2.21. *Let r be a prime factor of n and suppose d is an integer dividing $r-1$ such that $d \nmid n$. Then Φ_d divides F_n.* □

For a prime number p, we also have a necessary condition for Φ_p to divide F_n.

Proposition 2.22. *Let p be a prime number such that $p \nmid n$. If Φ_p is a factor of F_n then $p|\varphi(n)$, i.e., there exists a prime divisor r of n such that $p|r-1$.*

Proof. If Φ_p is a factor of F_n then $F_n = \Phi_p Q$ for some $Q \in \mathbb{Z}[x]$. Hence $\varphi(n) = F_n(1) = \Phi_p(1)Q(1) = pQ(1)$ and thus $p \mid \varphi(n)$.
Alternatively, by Remark 2.13, we know that Conjecture 2.11 holds in this case. So the elements of $\{1 \leq a \leq n | \gcd(a,n) = 1\}$ when reduced modulo p, equidistribute in $S = \{0, 1, \ldots, p-1\}$. Therefore $p = \#S$ divides $\varphi(n)$. □

Combining Corollary 2.21 and Proposition 2.22, we have the following.

Corollary 2.23. *Let p be a prime number. Then Φ_p is a factor of F_n if and only if $p \nmid n$ and there exists a prime divisor r of n such that $p|r-1$.* □

We observe that all cyclotomic factors described by Theorem 2.19 satisfy the equidistribution condition mentioned in Proposition 2.9.

Theorem 2.24. *Let n,N,D be as in Theorem 2.19. Suppose $D \nmid n$. Let $d = D$ and $d_1 = \gcd(d,n)$. Then the elements of $\{1 \le a \le n \mid \gcd(a,n) = 1\}$ when reduced modulo d, equidistribute in $S = \{1 \le a \le d \mid \gcd(a,d_1) = 1\}$. Equivalently, we have that $x^d - 1$ divides $F_n - cF_S = F_n - c\sum_{s\in S} x^s$ for some constant c.*

Proof. Let $c = \frac{\varphi(n)d_1}{d\varphi(d_1)}$ and consider the polynomial $W(x) = F_n(x) - cF_S(x)$. By Remark 2.10 it is enough to show that $x^d - 1$ divides $W(x)$.

Let m be any integer dividing d, and ζ_m be a primitive m-th root of unity. If $m \nmid n$ then we know $F_n(\zeta_m) = 0$ by Theorem 2.19 and $F_S(\zeta_m) = 0$ by Lemma 2.8. Hence $W(\zeta_m) = 0$. If $m|n$ then $m|d_1 = \gcd(d,n)$, and we again deduce that $W(\zeta_m) = 0$ by Proposition 2.6 and Lemma 2.8. □

2.3 Multiplicity of cyclotomic factors

In this section, we determine the multiplicity of cyclotomic factors of F_n. To do so, we need to investigate the value $F_n'(\zeta_d)$ whenever $F_n(\zeta_d) = 0$. By Corollary 2.7, ζ_d is not a root of F_n if $d|n$. Therefore, we can assume that $d \nmid n$ in our investigation. By Proposition 2.17 we have

$$F_n'(x) = nx^{n-1}\sum_{m|n}\mu(m)\frac{x^m}{x^m-1} + (x^n-1)\sum_{m|n}\mu(m)\frac{-mx^{m-1}}{(x^m-1)^2}. \tag{2.4}$$

We introduce the following polynomial

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

so that Eq. (2.4) becomes

$$x(x^n-1)F_n'(x) = nx^nF_n(x) - G_n(x). \tag{2.5}$$

Expanding this out using the definition of F_n, we have the following explicit formula

$$\begin{aligned} G_n(x) = nx^nF_n(x) - (x^{n+1}-x)F_n'(x) &= \sum_{\substack{1\le a\le n\\ \gcd(a,n)=1}} \left(ax^a + (n-a)x^{n+a}\right) \\ &= \sum_{\substack{1\le a\le n\\ \gcd(a,n)=1}} (n-a)[x^{n+a}+x^{n-a}] = x^n \sum_{\substack{1\le a\le n\\ \gcd(a,n)=1}} (n-a)[x^a + x^{-a}]. \end{aligned} \tag{2.6}$$

Lemma 2.25. *Let d be a positive integer and n a positive squarefree integer. Let $\zeta = \zeta_d$ be a primitive d-th root of unity.*

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

Proof. The first part follows immediately from Eq. (2.6) and the fact that $\zeta_4^a + \zeta_4^{-a} = 0$ for odd integers a. For the second part we first rewrite Eq. (2.6) as follows

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

Working over $\mathbb{C}$, if we let $\zeta_d = e^{\frac{2\pi i}{d}}$, then by Euler formula we have

$$\zeta_d^{-n}G_n(\zeta_d) = 2\sum_{\substack{1\le a\le \frac{n}{2}\\ \gcd(a,n)=1}} (n-2a)\cos\left(\frac{2\pi a}{d}\right) + 4\sum_{\substack{1\le a\le \frac{n}{2}\\ \gcd(a,n)=1}} a\cos\left(\frac{\pi n}{d}\right)\cos\left(\frac{(n-2a)\pi}{d}\right).$$

Since $d \ge 2n$ and $1 \le a \le \frac{n}{2}$, each term in the sum is non-negative and we get $\zeta_d^{-n}G_n(\zeta_d) \ge 0$. Further, if $G_n(\zeta_d) = 0$ then it must be the case that $(n-2)\cos\left(\frac{2\pi}{d}\right) = 0$ and $\cos\left(\frac{n\pi}{d}\right)\cos\left(\frac{(n-2)\pi}{d}\right) = 0$. This implies that $d = 4$ and $n = 2$. □

We remark that by Eq. (2.5), $\zeta = \zeta_d$ is simple root of F_n if and only if $F_n(\zeta) = 0$ and $G_n(\zeta) \neq 0$. Using the definition of G_n, we also get the following recursive formula for G_n analogous to the one for F_n described in Proposition 2.14. If $p \nmid n$, then

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

To study the multiplicity of Φ_d as a factor of G_n, we will use a general proposition.

Proposition 2.26. *Let $G(x) = \frac{P(x)}{Q(x)}$ where $P(x), Q(x)$ are polynomials with rational coefficients. Let d be a positive number and $\zeta = \zeta_d$ a primitive d-th root of unity such that $Q(\zeta) \neq 0$. Let p be a prime number such that $p \nmid d$. Let $G_p(x)$ be the following rational function*

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

Then

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

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

$$G_p^{(k)}(x) = G^{(k)}(x) - p^{k+1}x^{k(p-1)}G^{(k)}(x^p) + \sum_{0\le h\le k-1} M_{k,h}(x)G^{(h)}(x^p), \tag{2.7}$$

where $M_{k,h} \in \mathbb{Q}[x]$. In order to prove the above statement, we will show that for all $k \geq 0$, $G(\zeta) = \cdots = G^{(k)}(\zeta) = 0$ if and only if $G_p(\zeta) = \cdots = G_p^{(k)}(\zeta) = 0$.

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 $G_p(\zeta) = 0$, i.e., $G(\zeta) = pG(\zeta^p)$. Since $G_p \in \mathbb{Q}(x)$, we have this equality for any primitive d-th root of unity. In particular $G(\zeta) = pG(\zeta^p) = p^2 G(\zeta^{p^2}) = \ldots = p^{\varphi(d)} G(\zeta)$. This means that $G(\zeta) = 0$.

Assume that the statement holds for $k-1$. Let us show that it is true for k as well. First, suppose that $G(\zeta) = \cdots = G^{(k)}(\zeta) = 0$. By the induction hypothesis, we already know that $G_p(\zeta) = \cdots = G_p^{(k-1)}(\zeta) = 0$. Since ζ and ζ^p are Galois conjugate over $\mathbb{Q}$, we know that $G^{(h)}(\zeta^p) = 0$ for $0 \leq h \leq k$ as well. By Eq. (2.7), we conclude that $G_p^{(k)}(\zeta) = 0$. Conversely, assume that $G_p(\zeta) = \cdots = G_p^{(k)}(\zeta) = 0$. By the induction hypothesis, we know that $G(\zeta) = \cdots = G^{(k-1)}(\zeta) = 0$. Let us show that $G^{(k)}(\zeta) = 0$. Because of Galois conjugacy we again know that $G(\zeta^p) = \cdots = G^{(k-1)}(\zeta^p) = 0$. Additionally, since $G_p^{(k)}(\zeta) = 0$, Eq. (2.7) tells us that

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

Since this equality holds for any primitive d-th root of unity, a similar argument as in the base case lets us conclude that $G^{(k)}(\zeta) = 0$. □

Corollary 2.27. *Suppose that $p \nmid nd$ and $d \nmid n$. Let $\zeta = \zeta_d$ be a primitive d-th root of unity. Then* $\mathrm{mult}_\zeta(G_n) = \mathrm{mult}_\zeta(G_{np})$.

Proof. Consider the slightly modified function

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

Since $d \nmid np$, $\zeta = \zeta_d$ is not a root of $x^{np} - 1$. So $\mathrm{mult}_\zeta(G_n) = \mathrm{mult}_\zeta(\tilde{G}_n)$ and $\mathrm{mult}_\zeta(G_{np}) = \mathrm{mult}_\zeta(\tilde{G}_{np})$. Furthermore we have $\tilde{G}_{np}(x) = \tilde{G}_n(x) - p\tilde{G}(x^p)$. Applying Proposition 2.26 to $\tilde{G}_n$ gives the desired statement. □

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

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

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 2.28. *The polynomial $H_q(x+1)$ is an Eisenstein polynomial at the prime q. Consequently, $H_q(x)$ is irreducible. Moreover, if q is odd, then ζ_d is not a root of H_q for any d, and hence ζ_d is not a root of G_q.*

Proof. Over $\mathbb{F}_q$ we have $H_q(x) = (1-x)^{2(q-1)}$. Additionally $H_q(1) = q^2 - q$. This shows that $H_q(x+1)$ is an Eisenstein polynomial at the prime q.

Suppose on the contrary 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 $p = q^2 - q$, which implies that $q|p$ and hence $q = p = 2$. If d is not a prime power then $\Phi_d(1) = 1$. But there is no prime q such that $q^2 - q = 1$. □

With these preparations, we can now describe the multiplicity of any cyclotomic factor Φ_d of F_n.

Theorem 2.29. *Let $n > 1$ be a squarefree integer. Let d be a positive integer and $\zeta = \zeta_d$ a primitive d-th 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 root of F_n.*
2. *If $d = 4$ and n is odd, then ζ_d is a simple root of F_n.*
3. *If $d = 4$ and n is even, then ζ_d is a double root of F_n.*

Proof. We will prove the first and second statements by showing the contrapositive. 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 2.27 implies that $G_{d_1}(\zeta) = 0$ as well. Since $d \geq 2d_1$ we conclude by Lemma 2.25 that $d = 4$ and $d_1 = 2$ meaning that n is even.

When $d = 4$ and n is even, we know by Corollary 2.27 that $\mathrm{mult}_{\zeta_4}(G_n) = \mathrm{mult}_{\zeta_4}(G_2) = 1$. Eq. (2.5) then shows that $F_n(\zeta_4) = F_n'(\zeta_4) = 0$ but $F_n''(\zeta_4) \neq 0$. This proves that ζ_4 is a double root of F_n. □

Remark 2.30. It is not true that $\mathrm{mult}_{\zeta_4}(F_n) = 2$ for all even squarefree integers n. For instance, Example 2.5 says that for odd primes p, $F_{2p}(\zeta_4) = 0$ if and only if $p \equiv 1 \pmod 4$. Theorem 2.29 only asserts $\mathrm{mult}_{\zeta_4}(F_n) = 2$ on the condition that ζ_4 is a root of F_n. In the next section we will classify all n such that ζ_4 is a root of F_n.

2.4 Cyclotomic factors of F_n with small degree

In this section, we give explicit descriptions of the squarefree integers n such that Φ_d is a factor of F_n, for each $d \leq 7$. The cases $d = 2,3,5,7$ are already dealt with by Corollary 2.23. We will show that the same statement also holds for $d = 4,6$.

Remark 2.31. This statement fails for $d = 8$, with the smallest example coming from $n = 15$. By Theorem 2.19, we know that Φ_8 is a factor of F_n, but n has no prime factor congruent to $1 \pmod 8$.

In order to simplify our calculations, we consider the modified function $\tilde{F}_n(x) = \frac{F_n(x)}{1-x^n}$. The value $\tilde{F}_n(\zeta_d)$ is well-defined as long as $d \nmid n$, and furthermore it is zero if and only if $F_n(\zeta_d) = 0$. We also recall the recursive formula $\tilde{F}_{np}(x) = \tilde{F}_n(x) - \tilde{F}_n(x^p)$ for $p \nmid n$ from Proposition 2.14, which will be used repeatedly in this section.

We now consider the case $d = 4$. By Corollary 2.21, if n has a prime factor $p \equiv 1 \pmod 4$ then $F_n(\zeta_4) = 0$. It turns out that the converse is true as well.

Proposition 2.32. *Suppose that $n = 2^s p_1 p_2 \dots p_r$ where $s \in \{0,1\}$ and $p_1, \dots, p_r$ 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. If $s = 1$ and $m = p_1 p_2 \dots p_r$ we get using the recursive formula that

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

since $F_m(-1) = 0$ by Corollary 2.21. So it is sufficient to prove the statement for odd n. We will do this by induction on the number of prime factors of n.

When $n = p$ is a prime of the form $4k+3$, we have $\tilde{F}_n(\zeta) = \frac{1}{1-\zeta^p}\frac{\zeta(1-\zeta^{p-1})}{1-\zeta} = \zeta$. Suppose that the formula is true when n is a product of r primes of the form $4k+3$. Let us now suppose that $n = p_1 p_2 \dots p_{r+1}$. Let $m = p_2 \dots p_{r+1}$. By the induction hypothesis, we know that $\tilde{F}_m(\zeta) = 2^{r-1}\zeta$. By Galois conjugation, we get that $\tilde{F}_m(\zeta^3) = 2^{r-1}\zeta^3 = -2^{r-1}\zeta$. Now applying the recursive formula gives us the desired statement.

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

This finishes the proof by induction. □

For $d = 6$, Corollary 2.21 tells us that if $6 \nmid n$ and n has a prime factor $p \equiv 1 \pmod 6$, then $F_n(\zeta_6) = 0$. It again turns out that the converse is true. We first need a lemma.

Lemma 2.33. *Suppose that $n = p_1 p_2 \dots p_r$ for distinct primes $p_1, \dots, p_r$ of the form $3k+2$. Then $\tilde{F}_n(\zeta_3) = 2^{r-1}(1+2\zeta_3)/3$.*

Proof. When $r = 1$, direct calculation gives $\tilde{F}_{p_1}(\zeta_3) = \frac{1}{1-\zeta_3^{p_1}} \frac{\zeta_3(1-\zeta_3^{p_1-1})}{1-\zeta_3} = (1+2\zeta_3)/3$. In the general case, we let $m = p_2 \dots p_r$ and use the recursive formula

$$\tilde{F}_n(\zeta_3) = \tilde{F}_{mp_1}(\zeta_3) = \tilde{F}_m(\zeta_3) - \tilde{F}_m(\zeta_3^{p_1}) = \tilde{F}_m(\zeta_3) - \tilde{F}_m(\zeta_3^2).$$

Now the induction hypothesis $\tilde{F}_m(\zeta_3) = 2^{r-2}(1+2\zeta_3)/3$ and Galois conjugacy implies that $\tilde{F}_n(\zeta_3) = \frac{2^{r-2}}{3}\left((1+2\zeta_3) - (1+2\zeta_3^2)\right) = 2^{r-1}(1+2\zeta_3)/3$. □

Proposition 2.34. *$F_n(\zeta_6) = 0$ 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 Corollary 2.21. So we focus on the "only if" part. By Corollary 2.7 we know that if $6 \mid n$ then $F_n(\zeta_6) \neq 0$. So let us assume that $6 \nmid n$. Suppose that n has no prime factor $p \equiv 1 \pmod 6$. We consider three cases according to whether $\gcd(n,6) = 1$, 2 or 3.

In the first case, $n = p_1 p_2 \dots p_r$ for distinct primes $p_i \equiv 5 \pmod 6$, and we can show by induction that $\tilde{F}_n(\zeta_6) = 2^{r-1}(2\zeta_6 - 1) \neq 0$.

In the second case, we write $n = 2m = 2p_1 p_2 \dots p_r$ for distinct primes $p_i \equiv 5 \pmod 6$. The recursive formula then tells us that

$$\tilde{F}_n(\zeta_6) = \tilde{F}_m(\zeta_6) - \tilde{F}_m(\zeta_6^2) = 2^{r-1}(2\zeta_6 - 1) - 2^{r-1}\frac{1+2\zeta_6^2}{3} \neq 0,$$

where we have used the formula from the first case, and Lemma 2.33.

In the last case, we write $n = 3m = 3p_1 p_2 \dots p_r$ for distinct primes $p_i \equiv 5 \pmod 6$ and get

$$\tilde{F}_n(\zeta_6) = \tilde{F}_m(\zeta_6) - \tilde{F}_m(\zeta_6^3) = \tilde{F}_m(\zeta_6) - \tilde{F}_m(-1) = \tilde{F}_m(\zeta_6) = 2^{r-1}(2\zeta_6 - 1) \neq 0.$$

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

3 The case $n = pq$

In this section, we study more closely the case where n is a product of two odd primes $p > q$. The following proposition is a direct consequence of Theorem 2.19. If we assume that Conjecture 2.11 holds, this proposition in fact captures *all* cyclotomic factors of F_{pq}.

Proposition 3.1. *Let n be a product of two odd primes $p > q$. Suppose $d > 1$ and one of the following holds:*

(a) d divides $q - 1$;

(b) d divides $p-1$ and $d \neq q$;

(c) d divides $\gcd(qp+1, p+q)$. □

Then the d-th cyclotomic polynomial Φ_d divides F_n.

Theorem 3.2. *Assume Conjecture 2.11 is true. Then Proposition 3.1 is a complete characterization of all cyclotomic factors of F_n, when $n = pq$ is a product of two odd primes $p > q$.*

Proof. We have

$$\begin{aligned}(x^p-1)(x^q-1)F_n(x) &= (x^p-1)\sum_{1\le i\le q-1}\left(x^{qp+i}+x^{ip}-x^i-x^{ip+q}\right)\\ &= x^{qp}-x^p-x^{qp+q}+x^{p+q}+\sum_{1\le i\le q-1}\left(x^{(q+1)p+i}-x^{qp+i}-x^{p+i}+x^i\right).\end{aligned} \tag{3.1}$$

To evaluate a polynomial at a primitive d-th root of unity ζ_d, it is enough to consider its reduction modulo x^d-1. In particular, we may reduce the monomial exponents modulo d.

By Corollary 2.7 we know that $d \nmid n$. Suppose $d = d_1e_1$ with $d_1 = \gcd(d,n)$ and $e_1 > 1$. We have the following cases depending on whether d_1 is p, q or 1.

Case 1: Suppose $d_1 = p$. The equidistribution from Conjecture 2.11 implies that $\#S = \varphi(d_1)e_1 = \varphi(p)e_1$ divides $\varphi(n) = \varphi(p)\varphi(q)$. Hence $e_1|\varphi(q)$ and $d|p\varphi(q)$. Reducing Eq. (3.1) modulo $x^{p\varphi(q)}-1$ without loss of generality, 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 $d_1 = q$. Conjecture 2.11 implies that $\#S = \varphi(d_1)e_1$ divides $\varphi(n)$. Hence $e_1|\varphi(p)$ and $d|q\varphi(p)$. Reducing Eq. (3.1) modulo $x^{q\varphi(p)}-1$, we get

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

whose value at ζ_d is zero if and only $d|p-1$ and $d \neq q$.

Case 3: Suppose $d_1 = 1$. Conjecture 2.11 implies that $\#S = e_1 = d$ divides $\varphi(n)$. Reducing Eq. (3.1) modulo $x^{\varphi(n)}-1$, 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 $pq+1 = \varphi(n)+(p+q)$. □

Let S_n be the set of integers d described in Proposition 3.1, namely

$$S_n = \{d > 1, d \neq q, d \mid p-1\} \cup \{d > 1, d \mid q-1\} \cup \{d > 1, d \mid \gcd(pq+1, p+q)\}. \tag{3.2}$$

Definition 3.3. Suppose $n = pq$ for odd primes $p > q$. 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 3.4. *Suppose $n = pq$ for odd primes $p > q$. Let f_n be the Fekete polynomial as in Definition 3.3. 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

$$f_n(1) = \begin{cases} \dfrac{D_1 D_3 D_4}{2D_2} & \text{if } p \not\equiv 1 \pmod{q} \\ \dfrac{qD_1 D_3 D_4}{2D_2} & \text{if } p \equiv 1 \pmod{q}, \end{cases}$$
$$f_n(-1) = \frac{-D_1 D_3 D_4}{2D_2}.$$

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 $F_n(x) = xf(x)g(x)h(x)f_n(x)$. Using the inclusion-exclusion principle, we get the following formulas for f, g, h in this decomposition:

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

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

Since each of the polynomials $F_n(x)/x$, f, g, h are reciprocal, we deduce that f_n is also a reciprocal polynomial. The formula for $\deg(f_n)$ can also be deduced easily from the explicit descriptions of f, g, h given above.

It is also clear from this description that

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

$$h(1) = \frac{2D_2}{D_3D_4}.$$

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

Note that D_i is even for $1 \le i \le 4$, 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 2.18, and $g(-1)$ and $h(-1)$ using calculus, to infer the value of $f_n(-1)$:

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

□

Corollary 3.5. *$f_{pq}(x)$ is not a product of cyclotomic polynomials. In particular, $f_{pq}(x)$ is not a cyclotomic polynomial.*

Proof. Suppose on the contrary that $f_{pq}(x) = \prod_{i=1}^{r} \Phi_{m_i}(x)$, where $1 \le m_1 \le m_2 \cdots \le m_r$ are positive integers. Since $f_{pq}(1)f_{pq}(-1) \neq 0$, we can assume that $m_1 > 2$. By [BHPM18, Lemma 7], we have $\Phi_{m_i}(-1) > 0$ for all $1 \le i \le r$. Consequently $f_{pq}(-1) > 0$. This contradicts the above determination of $f_{pq}(-1)$. □

Definition 3.6. 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 3.7. *Suppose $n = pq$ for odd primes $p > q$. Let f_n be the Fekete polynomial as in Definition 3.3, and g_n its trace polynomial as in Definition 3.6. 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 3.4 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, again using Proposition 3.4, we obtain the stated result. □

We now investigate roots of the Fekete polynomial F_{pq} in $\overline{\mathbb{F}}_p$. The objective of this study is to prove that f_n is separable over $\mathbb{Z}$. We will see later that, in some special cases, this can be done by proving separability over $\mathbb{F}_p$. We first recall the following definition.

Definition 3.8. Let f, g be two polynomials. The Wronskian $W(f,g)$ of f and g is defined by the formula $W(f,g) = f'g - g'f$.

Let q be a prime. We now introduce the polynomial $u_q(x) = W(s_q(x), F_q(x)) \in \mathbb{Z}[x]$ where $s_q(x) = x^q - 1$ and $F_q(x) = \sum_{i=1}^{q-1} x^i$. Then u_q has the following explicit formula

$$u_q(x) = \sum_{1 \le i \le q-1} (q-i)x^{q-1+i} + \sum_{1 \le i \le q-1} i x^{i-1} = \Phi_q(x)^2 - q x^{q-1}. \tag{3.3}$$

Lemma 3.9. *Over $\mathbb{F}_q$, we have $u_q(x) = (x-1)^{2q-2} \pmod q$.*

Proof. We have

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

Over $\mathbb{F}_q$ this becomes

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

We also have that $s_q(x) = (x-1)^q$ and $s_q'(x) = 0$ over $\mathbb{F}_q$. Hence

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

Corollary 3.10. *The polynomial u_q 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 (and hence u_q) is irreducible. $\square$

Proposition 3.11. *Suppose $n = pq$ for odd primes $p > q$. Let $x_0 \in \overline{\mathbb{F}}_p$ be a root of F_n. Then*

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

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

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

Proof. Using the recursive formula from Proposition 2.14, we have

$$F_n(x) = \frac{x^{qp}-1}{x^q-1}F_q(x) - F_q(x^p),$$

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 2.6 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, then it is not a zero of $x^q - 1$. Hence the relation of F_n' and u_q obtained above shows that $\mathrm{mult}_{x_0}(u_q) = \mathrm{mult}_{x_0}(F_n) - 1$.

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

(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 Definition 3.3 we get that $\mathrm{mult}_{x_0}(F_n) - 1 = \mathrm{mult}_{x_0}(f_n)$.

□

Remark 3.12. We note that irreducibility of the polynomial $u_q \in \mathbb{Z}[x]$ implies in particular that $\mathrm{disc}(u_q) \neq 0$. Therefore for primes p sufficiently large compared to q, we have $\mathrm{disc}(u_q) \neq 0 \pmod{p}$ and hence $\mathrm{mult}_{x_0}(F_{pq}) \leq 2$.

To further study separability of F_n over $\mathbb{F}_p$, we introduce the following auxiliary polynomials. Let

$$a(x,y) = s_q(x) - yF_q(x) \text{ where } s_q(x) = x^q - 1, F_q(x) = \sum_{i=1}^{q-1} x^i,$$

and let $R_q(y)$ be the resultant of $u_q(x)$ and $a(x,y)$ with respect to the variable x. There is a direct link between separability of F_n and the arithmetic of R_q.

Proposition 3.13. *Suppose that F_n has a repeated root $x_0 \in \overline{\mathbb{F}}_p$. Then R_q has a root $\mu \in \mathbb{F}_p$.*

Proof. By Proposition 3.11 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. We claim that x_0 is not a root of F_q. Suppose on the contrary that it is a root of F_q. Then firstly it is a simple root because $(x-1)F_q(x) = x(x^{q-1}-1)$ is separable over $\mathbb{F}_p$. Since x_0 is a repeated root of $F_n(x) = (x^q-1)^{p-1}F_q(x) - F_q(x)^p$, and only a simple root of $F_q(x)$, we deduce that x_0 must be a root of $x^q - 1$. On the other hand, since $x_0 \neq 0$ and $x_0(x_0^{q-1}-1) = (x_0-1)F_q(x_0) = 0$, we get that $x_0^{q-1} - 1$. This forces $x_0 = x_0^q - 1 - x_0(x_0^{q-1}-1) + 1 = 1$. But this is a contradiction because $F_n(1) = \varphi(n) = (p-1)(q-1) \neq 0 \pmod{p}$.

Now $0 = F_n(x_0) = (x_0^q-1)^{p-1}F_q(x_0) - F_q(x_0)^p$ 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 $u_q(x)$ have a common root. Therefore

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

□

3.1 Further properties of the resultant $R_q(y)$

We record in this section a few interesting properties of the resultant polynomial $R_q(y)$. We need the following lemma.

Lemma 3.14. *Let q be an odd prime, and $s_q(x) = x^q - 1$ and $F_q(x) = \sum_{i=1}^{q-1} x^i$. Then*

(a) $\mathrm{Res}(s_q(x), s_q'(x)) = q^q$.

(b) $\mathrm{Res}(F_q(x), F_q'(x)) = -(q-1)^{q-3}$.

(c) $\mathrm{Res}(F_q(x), s_q(x)) = q-1$.

Proof. (a) Let ζ_k, $k = 1, \ldots, q$, be all the q-th roots of unity. Then

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

(b) Since $(x-1)F_q(x) = x^q - x$, we have

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

Let ζ_k, $k = 1, \ldots, q-1$, be all the $(q-1)$-th roots 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 $\mathrm{Res}(x-1, F_q(x))^2 = F_q(1)^2 = (q-1)^2$. Hence

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

and thus

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

(c) Let ζ_k, $k = 1, \ldots, q$, be all the q-th roots of unity, where $\zeta_q = 1$. Then

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

Proposition 3.15. *Over $\mathbb{F}_q$, the polynomial $R_q(y)$ factors as $R_q(y) = y^{2q-2}$.*

Proof. Using the property that $\mathrm{Res}(AB, C) = \mathrm{Res}(A, C)\,\mathrm{Res}(B, C)$ and using Lemma 3.9 which says that $u_q(x) = (x-1)^{2q-2}$ over $\mathbb{F}_q$, we have

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

Proposition 3.16. *The polynomial $R_q(y)$ is an even polynomial of degree $2q-2$, i.e., it is a polynomial in y^2. It has leading coefficient $-(q-1)^{q-2}$ and constant coefficient $(q-1)q^q$.*

Proof. We first note that

$$a(1/x,y) = s_q(1/x) - yF_q(1/x) = -x^{-q}(s_q(x) + yF_q(x)).$$

and hence $x^q a(1/x,y)\,a(x,y) = (y^2F_q(x)^2 - s_q(x)^2)$ is a polynomial in the variables x, y^2. Let $z_1, z_2, \ldots, z_{2q-2}$ be the roots of u_q. Since u_q is a reciprocal polynomial, we can assume further that $z_i z_{2q-1-i} = 1$. Thus we have

$$R_q(y) = \mathrm{Res}(a(x,y), u_q(x)) = \prod_{i=1}^{2q-2} a(z_i,y) = \prod_{i=1}^{q-1} (a(z_i,y)a(1/z_i,y))$$

which shows that R_q is an even polynomial. The formula

$$R_q(y) = \prod_{i=1}^{2q-2} a(z_i,y) = \prod_{i=1}^{2q-2} (s_q(z_i) - yF_q(z_i))$$

also shows that the leading coefficient of R_q is $\prod_{i=1}^{2q-2} F_q(z_i) = \mathrm{Res}(F_q(x), u_q(x))$, and the constant coefficient of R_q is $\prod_{i=1}^{2q-2} s_q(z_i) = \mathrm{Res}(s_q(x), u_q(x))$. We can compute them using Lemma 3.14. We compute the leading coefficient as follows

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

Similarly, the constant coefficient of R_q is $(q-1)q^q$. □

4 The case $n = 3p$

In this section, we focus on the special case $n = 3p$ for some prime $p > 3$. We note that the set S_{3p} described in Eq. (3.2) can be rewritten explicity.

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

Accordingly, we have the explicit description

$$\begin{aligned} F_{3p}(x) &= f_{3p}(x)\cdot x\cdot \prod_{d\in S_{3p}} \Phi_d(x) \\ &= \begin{cases} f_{3p}(x)x\dfrac{x^{p-1}-1}{x^3-1} & \text{if } p\equiv 1,7,19 \pmod{24} \\ f_{3p}(x)x\dfrac{x^{p-1}-1}{x^3-1}\Phi_8(x) & \text{if } p\equiv 13 \pmod{24} \\ f_{3p}(x)x\dfrac{x^{p-1}-1}{x-1}\Phi_8(x) & \text{if } p\equiv 5 \pmod{24} \\ f_{3p}(x)x\dfrac{x^{p-1}-1}{x-1} & \text{if } p\equiv 11,17,23 \pmod{24}. \end{cases} \end{aligned} \tag{4.1}$$

Proposition 4.1. *Let $p>3$ be a prime. Then the polynomial f_{3p} has the explicit formula*

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

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. The statements follow from noting that

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

□

It is a classical theorem that for any distinct odd primes p,q, the coefficients of the cyclotomic polynomial Φ_{pq} are in $\{0,-1,1\}$ (see [Bro16]). The smallest integer n such that Φ_n has a coefficient not contained in $\{0,-1,1\}$ is $n=105$. Along these lines, we observe that the coefficients of f_{3p} are quite small. In fact, for $p<1200$, we verify using SageMath that the coefficients of f_{3p} are in the set $\{-2,-1,0,1,2\}$. In fact this is true for all p as the next theorem shows.

Theorem 4.2. *Let $p > 3$ be a prime. The coefficients of f_{3p} are in the set $\{-2,-1,0,1,2\}$.*

Proof. Suppose that $p \equiv 1 \pmod 3$. If $p \equiv 1,7,19 \pmod{24}$, the statement is clear from Proposition 4.1. If $p \equiv 13 \pmod{24}$, say $p = 13+24a$ 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

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

which shows that all the coefficients of f_{3p} are in $\{-1,0,1\}$.

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

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

It is straightforward to check that

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

Now if $p \equiv 11,17,23 \pmod{24}$, then Proposition 4.1 says that $f_{3p}(x) = g(x)$, and so all the coefficients of f_{3p} are in $\{-1,0,1\}$. The last remaining case is $p \equiv 5 \pmod{24}$. If we write $g(x) = \sum_{k=0}^{2p} b_k x^k$, then the coefficients b_k are given by

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

In particular we have $b_k = b_{k'}$ whenever $k \equiv k' \pmod 3$ and $0 \le k,k' \le p-1$. Proposition 4.1 says that in this case we have $f_{3p}(x)(x^4+1) = g(x)$. If we write $f_{3p}(x) = \sum_{k=0}^{2p-4} a_k x^k$, then we get that the coefficients

of g and f_{3p} are related by

$$b_k = \begin{cases} a_k & \text{if} \quad 0 \le k \le 3 \\ a_k + a_{k-4} & \text{if} \quad 4 \le k \le 2p-4 \\ a_{k-4} & \text{if} \quad 2p-3 \le k \le 2p. \end{cases}$$

For $24 \le k \le p-1$, using the recursive formula $b_k = a_k + a_{k-4}$ repeatedly, we have

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

showing that 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} is reciprocal, we know that $a_k = a_{2p-4-k}$ and so $a_k \in \{-2,-1,0,1,2\}$ for all $0 \le k \le 2p-4$. □

Corollary 4.3. *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 more properties of f_{3p} in characteristic p. We start with the following theorem which is an improved version of Proposition 3.11 in the special case $n = 3p$.

Theorem 4.4. *Let $p > 3$ be a prime. Let $x_0 \in \overline{\mathbb{F}}_p$ be a root of F_{3p}.*

1. *The multiplicity of x_0 as a root of F_{3p} is at most 2.*
2. *The multiplicity of x_0 as a root of F_{3p} is 2 if and only if $x_0 \in \mathbb{F}_p$ and x_0 is a root of $u_3(x) = x^4 + 2x^3 + 2x + 1$.*

Proof. We have $\operatorname{disc}(u_3) = -1728 = -2^6 \times 3^3 \neq 0 \pmod{p}$. So the first statement follows from Proposition 3.11 Part (b).

The 'if' part of the second statement follows from Proposition 3.11 Part (a). Now we discuss the 'only if' part. Suppose that the multiplicity of x_0 as a root of F_{3p} is 2. Proposition 3.11 Part (a) immediately implies that x_0 is a root of u_3. So the only thing left to show is that $x_0 \in \mathbb{F}_p$.

As described in the proof of Proposition 3.13, there exists $\mu \in \mathbb{F}_p$ such that

$$a_3(x_0,\mu) = 0, \quad \text{and} \quad R_3(\mu) = \text{resultant}(a_3(x,\mu), u_3(x)) = -2\mu^4 + 36\mu^2 + 54 = 0.$$

The latter equation 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 $u_3(x)$ and $a_3(x,\mu)$. In particular $\deg b(x) = 1$ or 2.

If $\deg b(x) = 2$, then $b(x) = x^2 + (1 \pm c)x + 1$ is reciprocal. Hence the zeroes of $b(x)$ are x_0 and $1/x_0$. Since $b(x)$ divides $a_3(x,\mu) = x^3 - \mu x^2 - \mu x - 1$, the zeroes of $a_3(x,\mu)$ are $x_0, 1/x_0$ and β, for some $\beta \in \overline{\mathbb{F}}_p$. By Vieta's formula, $\beta = x_0 \cdot (1/x_0) \cdot \beta = 1$. Hence $0 = a_3(1,\mu) = -2\mu$, a contradiction since $R_3(0) = 54 \neq 0 \in \mathbb{F}_p$.

The above argument shows that $\deg b(x) = 1$ and hence $x_0 \in \mathbb{F}_p$. □

Corollary 4.5. *Let $p > 3$ be a prime. Then $\text{disc}(F_{3p}) = 0 \pmod p$ if and only if $u(x) = x^4 + 2x^3 + 2x + 1$ has a root modulo p. In particular,*

(a) if $p \equiv \pm 5 \pmod{12}$ then $p \nmid \text{disc}(F_{3p})$,

(b) if $p \equiv 11 \pmod{12}$ then $p \mid \text{disc}(F_{3p})$,

(c) if $p \equiv 1 \pmod{12}$ then $p \mid \text{disc}(F_{3p})$ if and only if 12 is a quartic residue mod p.

Proof. The first statement follows immediately from Theorem 4.4. 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 root in $\mathbb{F}_p$. Therefore $\text{disc}(F_{3p}) \neq 0 \pmod p$.

Now suppose $p \equiv \pm 1 \pmod{12}$. Then $\left(\frac{3}{p}\right) = 1$. Let $c \in \mathbb{F}_p$ such that $3 = c^2$.

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

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 $(1-c)^2 - 4 = -2c$.

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 root in $\mathbb{F}_p$. So Theorem 4.4 implies that F_{3p} has a double root in $\mathbb{F}_p$, and so $p \mid \operatorname{disc}(F_{3p})$.

If $p \equiv 1 \pmod{12}$ then $\left(\frac{2c}{p}\right) = \left(\frac{-2c}{p}\right)$. By Theorem 4.4, we get that $p \mid \operatorname{disc}(F_{3p})$ if and only if there exists $a \in \mathbb{F}_p$ such that $a^2 = 2c$. Since $c^2 = 3$, this is true if and only if there exists $a \in \mathbb{F}_p$ such that $a^4 = 12$, i.e., 12 is a quartic residue mod p. □

Corollary 4.6. *Let $x_0 \in \mathbb{F}_p$. Then x_0 is a root of the Fekete polynomial f_{3p} if and only if it is a root of $u_3(x) = x^4+2x^3+2x+1$.*

Proof. Suppose $x_0 \in \mathbb{F}_p$ is a root of $u_3(x)$. Then Theorem 4.4 says that x_0 is a double root of F_{3p}. By the explicit description of the cyclotomic factors of F_{3p} given in Eq. (4.1), it is clear that $x \prod_{d \in S_{3p}} \Phi_d(x)$ is separable over $\mathbb{F}_p$. So we can deduce that x_0 is a root of f_{3p}.

Conversely, suppose $x_0 \in \mathbb{F}_p$ is a root of f_{3p}. So it is also a root of F_{3p}. We know by Proposition 2.6 that $F_{3p}(1) = 2(p-1) = -2 \neq 0 \in \mathbb{F}_p$ and $F_{3p}(\zeta_3) = -(p-1) = 1 \neq 0 \in \mathbb{F}_p$. This means that $x_0^3 \neq 1$. On the other hand, since $x_0 \in \mathbb{F}_p$, we know that $x_0^{p-1} = 1$. Therefore by Eq. (4.1), we see that x_0 has multiplicity at least 2 as a root of F_{3p}. Theorem 4.4 then gives us that x_0 is a root of $u_3(x)$. □

Corollary 4.7. *The polynomial f_{3p} is separable over $\mathbb{F}_p$, and hence also separable over $\mathbb{Z}$. Consequently, g_{3p} is separable as well.*

Proof. Suppose on the contrary that f_{3p} is not separable over $\mathbb{F}_p$. Let $x_0 \in \overline{\mathbb{F}}_p$ be a root of f_{3p} with $\operatorname{mult}_{x_0}(f_{3p}) \geq 2$. Then $\operatorname{mult}_{x_0}(F_{3p}) \geq 2$ and Theorem 4.4 says that $\operatorname{mult}_{x_0}(F_{3p}) = 2$ and $x_0 \in \mathbb{F}_p$. This is absurd because x_0 is also a root of $x \prod_{d \in S_{3p}} \Phi_d(x)$ by Eq. (4.1), but that makes $\operatorname{mult}_{x_0}(F_{3p}) \geq 3$. □

We now write down explicitly the values $f_{3p}(1)$ and $f_{3p}(-1)$. These can be obtained directly from Proposition 3.4, or computed using the explicit formula for f_{3p} in Proposition 4.1. We then use this information to prove a fact about $\operatorname{disc}(f_{3p})$ that was first discovered by experimental data. Note that $\operatorname{disc}(f_{3p}) \neq 0$ since f_{3p} is separable.

Lemma 4.8. *Let $p > 3$ be a prime. Then*

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

Proposition 4.9. *Let $p > 3$ be a prime. If $p \equiv 1 \pmod 3$ then $\operatorname{disc}(f_{3p}) < 0$. If $p \equiv 2 \pmod 3$ then $\operatorname{disc}(f_{3p})$ is a nonzero perfect square.*

Proof. Since f_{3p} is a reciprocal polynomial with g_{3p} its trace polynomial, we have

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

Calculating using Lemma 4.8 and Proposition 4.1, we get

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

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

□

5 The case $n = 5p$

In this section, we provide some partial results for the case $n = 5p$ where p is a prime greater than 5. The goal is to prove the following analog of Theorem 4.4.

Theorem 5.1. *Let $p > 5$ be a prime. Let $x_0 \in \overline{\mathbb{F}}_p$ be a root of F_{5p}.*

(a) The multiplicity of x_0 as a root of F_{5p} is at most 2.

(b) The multiplicity of x_0 as a root of F_{5p} is 2 if and only $x_0 \in \mathbb{F}_p$ and $u_5(x_0) = 0$.

Proof of Theorem 5.1 Part (a). By Proposition 3.11 Part (b), if the discriminant of u_5 is not zero modulo p, we get the desired result. We compute that

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

When $p = 11$, we check directly that $F_{5p} = F_{55}$ has no repeated root in $\overline{\mathbb{F}}_{11}$. □

In this section, we use $a_\mu(x)$ for $a_5(x,\mu) = (x^5-1) - \mu(x+x^2+x^3+x^4)$. Using SageMath, we see that the resultant of $a_\mu(x)$ and $u_5(x)$ is given by

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

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 5.2. *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 5.3. *If $\left(\frac{5}{p}\right) = -1$ then F_{5p} is separable over $\mathbb{F}_p$.* □

We now complete the proof of Theorem 5.1.

Proof of Theorem 5.1 Part(2). Suppose $x_0 \in \mathbb{F}_p$ is a root of $u_5(x)$. By Eq. (3.3), since we know that $u_5(1) = q(q-1) \neq 0 \in \mathbb{F}_p$ and $u_5(\zeta_5) = -5\zeta_5^4 \neq 0 \in \overline{\mathbb{F}}_p$ for any primitive 5-th root of unity $\zeta_5 \in \overline{\mathbb{F}}_p$, we get that $x_0^5 \neq 0$. On the other hand $x_0^{p-1} = 1$. Hence $F_{5p}(x_0) = 0$. So Proposition 3.11 Part (a) says that $\mathrm{mult}_{x_0}(F_{5p}) \geq 2$. Combining with Theorem 5.1 Part(a), we conclude that $\mathrm{mult}_{x_0}(F_{5p}) = 2$.

Conversely suppose that $x_0 \in \overline{\mathbb{F}}_p$ is a double root of F_{5p}. By Lemma 5.2, 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

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

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. □

Corollary 5.4. *The polynomial f_{5p} is separable over $\mathbb{F}_p$, and hence also separable over $\mathbb{Z}$. Consequently, g_{5p} is separable as well.*

Remark 5.5. One may wonder if a similar statement as Theorem 5.1 holds for general $n=pq$. It turns out that the answer is no. We provide some concrete counterexamples.

1. When $q=7, p=101$, the polynomial $x^2+42x+10$ is an irreducible factor of F_{pq} (and f_{pq}) over $\mathbb{F}_p$, with multiplicity equal to 2.

2. When $q=11, p=13$, the polynomial $x^2+9x+10$ is an irreducible factor of F_{pq} (and f_{pq}) over $\mathbb{F}_p$, with multiplicity equal to 2.

3. When $q=11, p=61$, the polynomial $x^2+16x+14$ is an irreducible factor of F_{pq} (and f_{pq}) over $\mathbb{F}_p$, with multiplicity equal to 2.

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

6 Irreducibility of f_n

Checking irreducibility of a polynomial $f(x) \in \mathbb{Z}[x]$ is computationally expensive when $\deg(f)$ is large. A natural way to show irreducibility is by finding a prime $p \nmid \operatorname{disc}(f)$ such that the reduction $\overline{f}(x)$ mod p is irreducible over $\mathbb{F}_p$. This strategy fails if $\deg(f) = 2n$ is even and $\operatorname{disc}(f)$ is a perfect square: For every $p \nmid \operatorname{disc}(f)$, there is a Frobenius element Frob_p in the symmetric group S_{2n} determining the Galois orbit decomposition of the roots of $\overline{f}$. If $\operatorname{disc}(f)$ is a perfect square, Frob_p is an even permutation and hence cannot be a $2n$-cycle.

In this section, we will discuss some methods to computationally verify irreducibility of the Fekete polynomial $f_n \in \mathbb{Z}[x]$ by exploiting the fact that it is reciprocal. These are slight improvements of the criteria described in [CC17], and they all depend on irreducibility of the trace polynomial g_n, for which we turn to the method mentioned above.

We first make the following definition and state a key lemma from [CC17].

Definition 6.1. For a polynomial h of degree n, its reversal polynomial is defined by $h_{\mathrm{rev}}(x) = x^n h(1/x)$.

Lemma 6.2. *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 monic irreducible polynomial $h \in \mathbb{Z}[x]$ such that $f(x) = \pm h(x)h_{rev}(x)$. Furthermore, if $f(1) > 0$ then $f(x) = h(x)h_{rev}(x)$.*

Proof. See [CC17, Corollary 6] and the remark after it. □

Our first irreducibility criterion is Proposition 6.3. Together with Proposition 3.4, this shows that whenever the degree of the Fekete polynomial f_{pq} is divisible by 4, it is irreducible if and only if its trace polynomial g_{pq} is irreducible.

Proposition 6.3. *Let f be a monic reciprocal polynomial of degree $4n$. Let g be the trace polynomial of f. Suppose that g is irreducible and $f(1)f(-1) < 0$. Then f is irreducible.*

Proof. Suppose f is reducible. Then by Lemma 6.2, $f(x) = \pm x^{2n} h(x)h(\frac{1}{x})$ for some $h \in \mathbb{Z}[x]$. Consequently $f(1)f(-1) = h(1)^2 h(-1)^2 \geq 0$ which contradicts the hypothesis. □

Our second irreducibility criterion is Proposition 6.4. Together with Theorem 4.2, this proves that for all primes $p > 3$, the Fekete polynomial f_{3p} is irreducible if and only if its trace polynomial g_{3p} is irreducible.

Proposition 6.4. *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 and the middle coefficient of f satisfies $|a_n| \leq 2$. Then f is irreducible.*

Proof. Suppose that f is reducible. Without loss of generality, we can assume $f(1) > 0$ and hence by Lemma 6.2, $f(x) = h(x)h_{\text{rev}}(x)$ for some monic irreducible polynomial $h \in \mathbb{Z}[x]$. Let $h(x) = \sum_{k=0}^{n} c_k x^k$ with $c_n = 1$. Since f is monic, by comparing leading coefficients, we deduce that $c_0 = 1$ as well. Further, we get the following expression for the middle coefficient of f:

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

Since $|a_n| \leq 2$ and $c_n = c_0 = 1$, we conclude that $c_k = 0$ for $1 \leq k \leq n-1$ and thus $h(x) = x^n + 1$. Since $f(-1) \neq 0$, we deduce that n is even. So $f = hh_{\text{rev}}$ is a factorisation into reciprocal polynomials of even degree, which yields a non-trivial factorisation of g (see [CC17, Proposition 8]). This contradicts the hypothesis that g is irreducible. □

Remark 6.5. For $p \leq 1000$, we have also checked that the middle coefficient of f_{5p} lies in the set $\{-2,-1,0,1,2\}$. However the middle coefficient of $f_{7\times 73}$ is -3.

Our last irreducibility criterion is Proposition 6.6. This forms the basis of Algorithm 6.7.

Proposition 6.6. *Let f be a monic reciprocal polynomial of degree $2n$. Let g be the trace polynomial of f. Suppose that g is irreducible. Suppose also that there exists a prime number q and a positive integer m such that the number of irreducible factors of degree m of the reduction $\overline{f} \in \mathbb{F}_q[x]$, counted with multiplicity, is an odd number. Then f is irreducible.*

Proof. By Lemma 6.2, if f is reducible then $f(x) = \pm h(x)h_{\text{rev}}(x)$. So any irreducible factor $a(x)$ of $\overline{f}(x)$ divides either $\overline{h}(x)$ or $\overline{h}_{\text{rev}}(x)$, and thus $a_{\text{rev}}(x)$ is another irreducible factor of $\overline{f}(x)$. Therefore, the degree of any irreducible factor of $\overline{f}(x)$ must arise an even number of times. This contradicts the given hypothesis. So f must be irreducible. □

Algorithm 6.7 (Verifying irreducibility of a reciprocal polynomial $f(x)$ of even degree)**.**

Step 1. Compute the trace polynomial $g(x)$.

Step 2. Find a prime number q_1 such that the reduction $\overline{g}(x) \in \mathbb{F}_{q_1}[x]$ is irreducible.

Step 3. Find a prime number q_2 such that the factorisation of $\overline{f}(x) \in \mathbb{F}_{q_2}[x]$ has an odd number of irreducible factors of some degree m (when counted with multiplicity) i.e. satisfying the hypothesis of Proposition 6.6.

Step 4. If Steps 2 and 3 terminate, return `True`.

Example 6.8. We give a concrete example to demonstrate this method. Let us consider the Fekete polynomial $f_{15}(x) = x^6 - x^4 + x^3 - x^2 + 1$. Its trace polynomial is $g_{15}(x) = x^3 - 4x + 1$. We can check that the reduction $\overline{g}_{15}(x) \in \mathbb{F}_3[x]$ is irreducible, so $g_{15}(x)$ is irreducible over $\mathbb{Z}$. Furthermore, the reduction $\overline{f}_{15}(x) \in \mathbb{F}_2[x]$ factors as:

$$\overline{f}_{15}(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Since the degree 2 (and 4) irreducible factor appears only once in the factorisation, by Proposition 6.6, the Fekete polynomial $f_{15}(x)$ is irreducible.

Using Algorithm 6.7, we have verified irreducibility of the Fekete polynomial $f_n(x)$ when $n < 10^4$ is a product of two distinct odd primes. For each n, our GitHub repository [CMNT23] lists the corresponding prime pairs (q_1, q_2). We are tempted to make the conjecture:

Conjecture 6.9. Let $n = pq$ be a product of two distinct odd primes. Then the Fekete polynomial f_n from Definition 3.3 is irreducible.

The polynomials $1 - x + x^k - x^{2k-1} + x^{2k}$ associated to certain symmetric numerical semigroups were studied in [HPM21]. In particular, besides determining the cyclotomic factors, [HPM21, Conjecture 6.6] predicts that these polynomials have a unique irreducible non-cyclotomic factor. We observe that the Fekete polynomials F_{pq} considered in this paper do not come from numerical semigroups, but their factorisation exhibits an analogous picture, as described in Theorem 3.2, Definition 3.3 and Conjecture 6.9.

7 Galois groups of f_n and g_n

Let f be a polynomial over $\mathbb{Q}$ of degree m. The Galois group of f is the Galois group of its splitting field, denoted $\mathbb{Q}(f)$, as an extension of $\mathbb{Q}$. Using the permutation action on the roots of f, it is naturally a subgroup of the symmetric group S_m. If f is irreducible, then it is a transitive subgroup of S_m. We recall the well-known result that a transitive subgroup of S_m containing a 2-cycle (transposition) and an $(m-1)$-cycle is all of S_m. Using this result, we have a criterion to verify that the Galois group of a polynomial of degree m is the full symmetric group S_m. See [MNT23, Propisition 4.10].

7.1 The Galois group of g_n

It is known that the Galois group of a polynomial of degree m is generically the full symmetric group S_m. This also seems to be the case for the special family g_n from Definition 3.6. We use the technique mentioned above to verify this for a range of values of n. We first demonstrate this technique using an example.

Example 7.1. Let $n = 3 \times 7 = 21$. Then

$$g_n(x) = x^8 + x^7 - 8x^6 - 7x^5 + 20x^4 + 14x^3 - 16x^2 - 6x + 2,$$

is a polynomial of degree $m = 8$. Let $G = \mathrm{Gal}(\mathbb{Q}(g_n)|\mathbb{Q})$. Using SageMath, we see that g_n is irreducible over $\mathbb{F}_5$. This shows that G is a transitive subgroup of S_m. Over $\mathbb{F}_{19}$, g_n factors as the product of a linear factor and an irreducible factor of degree $m-1$:

$$g_n(x) = (x+8)(x^7 + 12x^6 + 10x^5 + 8x^4 + 13x^3 + 5x^2 + x + 5) \pmod{19}.$$

This shows that G contains an $(m-1)$-cycle. Finally, over $\mathbb{F}_7$, we have the factorisation

$$g_n(x) = (x^2 + x + 4)(x^3 + 4)(x^3 + 2x + 1) \pmod{7},$$

which contains exactly one irreducible factor of degree 2, and no other irreducible factor of even degree. This shows that G contains a transposition. Therefore $G = S_8$.

Question 7.2. Let $n = pq$ be a product of two distinct odd primes, g_n be the polynomial from Definition 3.6, and $m = \deg(g_n)$. Is the Galois group of g_n isomorphic to S_m?

While this question seems hard to tackle, we find extensive computational evidence.

Proposition 7.3. *The answer to Question 7.2 is affirmative for all $n < 10^4$ such that n is a product of two distinct odd primes p, q.*

Proof. For each n, our GitHub repository [CMNT23] lists prime triples (q_1, q_2, q_3), such that the reduction of g_n modulo q_i has the desired factorization type as in Example 7.1. □

7.2 The Galois group of f_n

Recall that the Fekete polynomials f_n from Definition 3.3 are reciprocal polynomials whose trace polynomial is g_n (Definition 3.6). Let m denote the degree of g_n. Then we have the following commutative diagram where the vertical maps are natural inclusions coming from the permutation action on roots.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(f_n)|\mathbb{Q}(g_n)) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(f_n)/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(g_n)/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \subseteq} & & \downarrow{\scriptstyle \subseteq} & & \downarrow{\scriptstyle \subseteq} & & \\ 1 & \longrightarrow & (\mathbb{Z}/2)^m & \longrightarrow & (\mathbb{Z}/2) \wr S_m & \longrightarrow & S_m & \longrightarrow & 1 \end{array} \tag{7.1}$$

Thus the Galois group of f_n is naturally a subgroup of the wreath product $(\mathbb{Z}/2) \wr S_m$. Note that this wreath product is the semidirect product $(\mathbb{Z}/2)^m \rtimes S_m$, where S_m acts by permuting the coordinates. It

can be seen as a subgroup of S_{2m} by [DDS98, Section 2]. We utilize [MNT24, Propositions 11.8, 11.11] to determine the Galois group of f_n for a range of values of n. We first demonstrate their use with a couple of examples.

Example 7.4. Let $n = 3 \times 7 = 21$. In Example 7.1, we showed that the Galois group of g_n is S_8. By Proposition 3.7, the discriminant of f_n is not a perfect square. Further

$$\begin{aligned} f_n(x) = (x^2+12x+1) \times (x^7+78x^6+173x^5+18x^4+119x^3+129x^2+107x+9) \\ \times (x^7+138x^6+90x^5+215x^4+2x^3+221x^2+160x+101) \pmod{227}. \end{aligned}$$

This factorisation over $\mathbb{F}_{227}$ contains exactly one irreducible factor of degree 2, and no other irreducible factor of even degree. By [MNT24, Proposition 11.11], we conclude that the Galois group of f_n is $(\mathbb{Z}/2)^8 \rtimes S_8$.

Example 7.5. Let $n = 5 \times 7 = 35$. Then g_n is a polynomial of degree 11

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

As in Example 7.1, the factorization of g_n over $\mathbb{F}_{q_i}$ with $(q_1, q_2, q_3) = (29, 47, 31)$ yields that the Galois group of g_n is S_{11}. Over $\mathbb{F}_{433}$, the polynomial f_n factors as

$$\begin{aligned} f_n(x) =& (x+97) \times (x+125) \times (x^2+41x+1) \times (x^4+124x^3+295x^2+124x+1) \\ & \times (x^7+190x^6+62x^5+191x^4+406x^3+37x^2+393x+313) \\ & \times (x^7+289x^6+393x^5+76x^4+168x^3+50x^2+251x+350) \pmod{433}, \end{aligned}$$

with a unique irreducible factor each of degrees 2 and 4, and no other irreducible factor of even degree. Remembering that now $\operatorname{disc}(f_n)$ is a perfect square by Proposition 3.7, and using [MNT24, Proposition 11.8], we conclude that the Galois group of f_n is $\ker(\Sigma) \rtimes S_{11}$ where $\Sigma\colon (\mathbb{Z}/2)^{11} \to \mathbb{Z}/2$ is the summation map.

Thus we raise the following question, supported by extensive numerical evidence.

Question 7.6. Let $n = pq$ be a product of two distinct odd primes, f_n be the Fekete polynomial from Definition 3.3, and $2m = \deg(f_n)$. Are the following statements true?

1. Suppose $p \equiv 1 \pmod{q}$, or $p \not\equiv 1 \pmod{q}$ and $p, q \equiv 1 \pmod{4}$. Then the Galois group of f_n is $(\mathbb{Z}/2)^m \rtimes S_m$.

2. Suppose we are in the remaining case, i.e., $p \not\equiv 1 \pmod{q}$ and at least one of p or q is not congruent to $1 \pmod 4$. Then the Galois group of f_n is $\ker(\Sigma) \rtimes S_m$ where $\Sigma\colon (\mathbb{Z}/2)^m \to \mathbb{Z}/2$ is the summation map.

Proposition 7.7. *The answer to Question 7.6 is affirmative for all $n < 10^4$ such that n is a product of two distinct odd primes p, q.*

Proof. By Proposition 7.3, the trace polynomial g_n has Galois group isomorphic to S_n. For each n, our GitHub repository [CMNT23] lists another prime q_4, such that the factorisation of f_n modulo q_4 yields the desired conclusion, using [MNT24, Propositions 11.8, 11.11]. □

Code availability

An open-source code repository for this work is available on GitHub [CMNT23].

A 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 [CGPS00]. It was shown in [CGPS00] 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 [CGPS00] 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 [ET50, Theorem 1] and [Gra07, Theorem 1.3]). We thank Professor Kannan Soundararajan for pointing this out to us.

Let $H_n\colon \mathbb{C}\setminus(0,\infty) \to \mathbb{C}$ 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

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

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 2.6, if $0 < k < n$ and $\zeta_n = e^{2\pi i/n}$, we

have

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

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 A.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 Examples 2.4 and 2.5. 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 question for general n.

Acknowledgments

We thank Oleksiy Klurman, Andrew Granville, Bjorn Poonen and Kannan Soundararajan for helpful discussions and correspondence. The third named author would like to thank William Stein for his help with the platform Cocalc where our computations are based. We are also grateful to the referee for his/her comments and valuable suggestions which we have used to improve our exposition.

References

[BCY01] Peter Borwein, Kwok-Kwong Choi, and Soroosh Yazdani. An extremal property of Fekete polynomials. *Proceedings of the American Mathematical Society*, 129(1):19–27, 2001. 52

[BHPM18] Bartlomiej Bzdega, Andrés Herrera-Poyatos, and Pieter Moree. Cyclotomic polynomials at roots of unity. *Acta Arithmetica*, 184(3):215–230, 2018. 69

[BI15] Milan Bašić and Aleksandar Ilić. Polynomials of unitary Cayley graphs. *Filomat*, 29(9):2079–2086, 2015. 53

[BM90] RC Baker and Hugh L Montgomery. Oscillations of quadratic L-functions. In *Analytic Number Theory*, pages 23–40. Springer, 1990. 52

[Bor02] Peter Borwein. *Computational excursions in analysis and number theory*. Springer Science & Business Media, 2002. 52

[Bro16] Gary Brookfield. The coefficients of cyclotomic polynomials. *Mathematics Magazine*, 89(3):179–188, 2016. 75

[CC17] Antonio Cafure and Eda Cesaratto. Irreducibility criteria for reciprocal polynomials and applications. *The American Mathematical Monthly*, 124(1):37–53, 2017. 84, 85

[CGPS00] Brian Conrey, Andrew Granville, Bjorn Poonen, and K Soundararajan. Zeros of Fekete polynomials. *Annales de l'institut Fourier*, 50(3):865–889, 2000. 52, 54, 89

[CMNT23] Shiva Chidambaram, Ján Mináč, Tung T Nguyen, and Nguyễn Duy Tân. Fekete polynomials of principal Dirichlet characters. https://github.com/tungprime/fekete_polynomials_principal_characters, 2023. 53, 86, 87, 89

[DDS98] S Davis, W Duke, and X Sun. Probabilistic Galois theory of reciprocal polynomials. *Expositiones Mathematicae*, 16:263–270, 1998. 88

[Erd18] Tamás Erdélyi. Improved lower bound for the Mahler measure of the Fekete polynomials. *Constructive Approximation*, 48(2):283–299, 2018. 52

[ET50] Paul Erdos and Pál Turán. On the distribution of roots of polynomials. *Annals of mathematics*, pages 105–119, 1950. 89

[GK11] Dina Ghinelli and Jennifer D Key. Codes from incidence matrices and line graphs of Paley graphs. *Advances in Mathematics of Communications*, 5(1):93, 2011. 53

[Gra07] Andrew Granville. The distribution of roots of a polynomial. In *Equidistribution in number theory, an introduction*, pages 93–102. Springer, 2007. 89

[HPM21] Andrés Herrera-Poyatos and Pieter Moree. Coefficients and higher order derivatives of cyclotomic polynomials: old and new. *Expo. Math.*, 39(3):309–343, 2021. 86

[HW79] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Oxford university press, 1979. 55, 56

[Jav14] Jérôme Javelle. *Cryptographie Quantique: Protocoles et Graphes*. PhD thesis, Université de Grenoble, 2014. 53

[KLM23] Oleksiy Klurman, Youness Lamzouri, and Marc Munsch. *l_q* norms and Mahler measure of Fekete polynomials. *arXiv preprint arXiv:2306.07156*, 2023. 52

[KS07] Walter Klotz and Torsten Sander. Some properties of unitary Cayley graphs. *The electronic journal of combinatorics*, pages R45–R45, 2007. 53

[Lem21] F. Lemmermeyer. *Quadratic number fields*. Springer Undergraduate Mathematics Series. Springer, 2021. 52

[MMNT24] Ján Mináč, Lyle Muller, Tung T. Nguyen, and Nguyễn Duy Tân. On the Paley graph of a quadratic character. *Math. Slovaca*, 74(3):527–542, 2024. 53

[MNT23] Ján Mináč, Tung T Nguyen, and Nguyễn Duy Tân. Fekete polynomials, quadratic residues, and arithmetic. *Journal of Number Theory*, 242:532–575, 2023. 52, 53, 86

[MNT24] Ján Mináč, Tung T. Nguyen, and Nguyễn Duy Tân. On the arithmetic of generalized Fekete polynomials. *Exp. Math.*, 33(4):723–754, 2024. 52, 53, 88, 89

AUTHORS

Shiva Chidambaram

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

shivac@mit.edu
https://math.mit.edu/~shivac/

Ján Mináč

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

minac@uwo.ca
https://www.math.uwo.ca/faculty/minac/index.html

Tung T. Nguyen

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

tungnt@uchicago.edu
https://tungprime.github.io/

Nguyễn Duy Tân

Faculty of Mathematics and Informatics
Hanoi University of Science and Technology
1 Dai Co Viet Road
Hanoi, Vietnam

tan.nguyenduy@hust.edu.vn
https://fami.hust.edu.vn/giang-vien/?name=tannd