FEKETE POLYNOMIALS, QUADRATIC RESIDUES, AND ARITHMETIC

JÁN MINÁČ, TUNG T. NGUYEN, NGUYỄN DUY TÂN

Dedicated to Professor Paulo Ribenboim with gratitude and admiration

ABSTRACT. Fekete polynomials associate with each prime number p a polynomial with coefficients -1 or 1 except the constant term, which is 0. These coefficients reflect the distribution of quadratic residues modulo p. These polynomials were already considered in the 19th century in relation to the studies of Dirichlet L-functions. In our paper, we introduce two closely related polynomials. We then express their special values at several integers in terms of certain class numbers and generalized Bernoulli numbers. Additionally, we study the splitting fields and the Galois group of these polynomials. In particular, we propose two conjectures on the structure of these Galois groups. We also provide some computational evidence toward the validity of these conjectures.

1. INTRODUCTION

Recall that for each prime p the Fekete polynomial $F_p(x)$ is defined by

$$F_p(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^a.$$

Here $\left(\frac{a}{p}\right)$ is the Legendre symbol which is equal to, for $1 \leq a \leq p-1$, the value 1 if a is a quadratic residue modulo p and the value -1 if a is not a quadratic residue modulo p. Because $F_2(x)$ is just x, in our subsequent considerations we assume that p is an odd prime number.

The function $\chi_p(a) = \left(\frac{a}{p}\right)$, $a \in \mathbb{Z}$, is a Dirichlet character. The infinite series

$$L(s, \chi_p) = \sum_{n=1}^{\infty} \frac{\chi_p(n)}{n^s},\ s = \sigma + it, \sigma, t \in \mathbb{R},$$

Date: November 22, 2021.

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

is an absolutely convergent for $\sigma > 1$. It is well-known that $L(s, \chi_p)$ has an analytical continuation to the entire complex plane and this analytical continuation which we also denote as $L(s, \chi_p)$ is a regular function for all complex s (see [3, Chapter 12]). Michael Fekete observed that if $F_p(x)$ has no real zeroes in the interval $0 < x < 1$ then $L(s, \chi_p)$ has no real zero $s > 0$. Therefore, these polynomials $F_p(x)$ are now called the Fekete polynomials. In fact, Fekete conjectured in 1912 that $F_p(x)$ has no real roots between 0 and 1. George Pólya in 1919 showed that this conjecture is false for $p = 67$ and for infinitely many other primes (see [24], [25], [1].) Polya's examples of $f_p(x)$ with negative values on the interval $[0, 1]$ use quadratic reciprocity law and Dirichlet's theorem on primes in arithmetic sequences to establish infinitely many primes p such that

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{11}{p}\right) = \left(\frac{13}{p}\right) = -1.$$

A simple but elegant argument establishes the existence of $x_0 \in (0, 1)$ such that for primes p considered above $f_p(x_0) < 0$. These simple and beautiful considerations were also used in [26, Problem 46 of part 5]. Among some further interesting investigations of behaviors of $f_p(x)$ over the interval $[0, 1]$ and also its roots in the complex plane, we mention just [4],[10]. Our main interest in these polynomials lies in exploring their arithmetic and Galois theoretic properties using the interesting interplay between the distribution of quadratic residues, arithmetic properties of Bernoulli numbers, class number formulas, elementary polynomials, and Galois theoretic considerations. This paper is an outgrowth of our further reflections on the special values of L-functions considered in [22]. Nevertheless, formally our paper is independent of [22].

We refer [20, page 231] for some interesting historical comments on Fekete polynomials. In particular, Fekete polynomials already implicitly showed up in Gauss's sixth proof [13] of the quadratic reciprocity law.

The structure of our article is as follows. In Section 2, we focus on determining the multiplicity of the roots $x = 1$ and $x = -1$ of $F_p(x)$. Using some of the results in Section 2, we define in Section 3 the polynomials $f_p(x)$ where we divide $F_p(x)$ by the factor $x(1-x)$ if $p \equiv 3 \pmod 4$ and by $x(1-x)^2(x+1)$ if $p \equiv 1 \pmod 4$. We observe further that $f_p(x)$ is a reciprocal polynomial of even degree. From this observation, we define another key polynomial $g_p(x)$ which is closely related to $F_p(x)$ and $f_p(x)$. We call this $g_p(x)$ the "reduced Fekete polynomial" associated with p. These reduced Fekete polynomials are interesting as they contain considerable arithmetic information. In particular, we show that their special values $g_p(-2), g_p(-1), g_p(0), g_p(1), g_p(2)$ are

closely related to the class numbers of some some specific quadratic number fields. In Section 4, we investigate some Galois theoretic properties of the splitting fields of $f_p(x)$ and $g_p(x)$ over the rational number field. Based on our results, heuristic considerations, and numerical evidence, we make the Conjecture 4.9 about the Galois group of $g_p(x)$. In Section 5, we investigate some modular properties of $F_p(x), f_p(x), g_p(x)$ modulo p. We conclude our paper with some specific numerical examples of $f_p(x)$ and $g_p(x)$.

2. Roots of $F_p(x)$

We can see that $x = 0$ is a root of $F_p(x)$. Furthermore, we have

$$F_p(1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Therefore, $x = 1$ is also root of $F_p(x)$. Let r_p be the multiplicity of the root $x = 1$. To study r_p, we need the following lemma.

Lemma 2.1. *(a)* $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4 \\ \neq 0 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

(b) $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a^2 \neq 0.$

We first recall that the Bernoulli polynomials $B_n(x)$ and Bernoulli numbers B_n are defined as

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}$$

and

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}.$$

One can define the generalized Bernoulli numbers $B_{n,\chi}$ and Bernoulli polynomials $B_{n,\chi}(x)$ for a Dirichlet character χ with conduction $f = f_\chi$ as

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{(a+x)t}}{e^{ft} - 1}$$

and

$$B_{n,\chi}(x) = \sum_{k=0}^{n} \binom{n}{k} B_{k,\chi} x^{n-k}.$$

(See ([17, pp. 7-9]).)

Proof of Lemma 2.1. Let χ be the quadratic character $\left(\frac{\cdot}{p}\right)$. One has ([17, page 10])

$$B_{n,\chi}(x) = p^{n-1}\sum_{a=1}^{p-1}\chi(a)B_n(\frac{a-p+x}{p}). \tag{1}$$

Substituting $n = 1$ and $x = 0$ in (1), one obtains

$$\begin{aligned} B_{1,\chi} &= \sum_{a=1}^{p-1}\chi(a)B_1\left(\frac{a}{p}-1\right) = \sum_{a=1}^{p-1}\chi(a)\left(\frac{a}{p}-\frac{1}{2}\right) \\ &= \frac{1}{p}\sum_{a=1}^{p-1}\chi(a)a - \frac{1}{2}\sum_{a=1}^{p-1}\chi(a) = \frac{1}{p}\sum_{a=1}^{p-1}\chi(a)a. \end{aligned}$$

Hence

$$\sum_{a=1}^{p-1}\chi(a)a = pB_{1,\chi} = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4 \\ \neq 0 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The last statement follows from [17, pages 12-13, Theorem 2].

Substituting $n = 2$ and $x = 0$ in (1), one obtains

$$\begin{aligned} B_{2,\chi} &= p\sum_{a=1}^{p-1}\chi(a)B_2(\frac{a}{p}-1) \\ &= p\sum_{a=1}^{p-1}\chi(a)\left(\frac{a^2}{p^2}-\frac{a}{p}+\frac{1}{6}\right) \\ &= \frac{1}{p}\sum_{a=1}^{p-1}\chi(a)a^2 - \sum_{a=1}^{p-1}\chi(a)a + \frac{1}{6}\sum_{a=1}^{p-1}\chi(a) \\ &= \frac{1}{p}\sum_{a=1}^{p-1}\chi(a)a^2 - \sum_{a=1}^{p-1}\chi(a)a. \end{aligned}$$

Hence

$$\sum_{a=1}^{p-1}\chi(a)a^2 = pB_{2,\chi} + p\sum_{a=1}^{p-1}\chi(a)a.$$

If $p \equiv 1 \pmod 4$, then $\sum_{a=1}^{p-1}\chi(a)a^2 = pB_{2,\chi} \neq 0$ (by [17, pages 12-13, Theorem 2]). If $p \equiv 3 \pmod 4$, then $\sum_{a=1}^{p-1}\chi(a)a^2 = p\sum_{a=1}^{p-1}\chi(a)a = p^2B_{1,\chi} \neq 0$ (by [17, pages 12-13, Theorem 2]). □

We are now ready to compute r_p explicitly.

Proposition 2.2.

$$r_p = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 4 \\ 2 & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Proof. One has

$$F_p'(1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a.$$

By Lemma 2.1 (a), $r_p = 1$ if $p \equiv 3 \pmod 4$ and $r_p \geq 2$ if $p \equiv 1 \pmod 4$.

Now we suppose that $p \equiv 1 \pmod 4$. By Lemma 2.1, one has

$$\begin{aligned} F_p''(1) &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a(a-1) \\ &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a^2 - \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a \\ &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a^2 \neq 0. \end{aligned}$$

Hence $r_p = 2$. □

Next, let us investigate whether $x = -1$ is a root of $F_p(x)$. We have the following observation.

Proposition 2.3. *Let p be a prime number and $F_p(x)$ is the Fekete polynomial. Then*

(1) If $p \equiv 1 \pmod 4$ then $x = -1$ is a root of $F_p(x)$.
(2) If $p \equiv 3 \pmod 4$ then $x = -1$ is not a root of $F_p(x)$.

Proof. First, let us consider the case $p \equiv 1 \pmod 4$. We have

$$\begin{aligned} F_p(-1) &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (-1)^a \\ &= \sum_{a=1}^{\frac{p-1}{2}} \left[\left(\frac{a}{p}\right) (-1)^a + \left(\frac{p-a}{p}\right) (-1)^{p-a} \right] \\ &= \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) \left[(-1)^a + (-1)^{p-a} \right] = 0. \end{aligned}$$

Note that the in third equality, we use the fact if that $p \equiv 1 \pmod 4$ then

$$\left(\frac{p-a}{p}\right) = \left(\frac{a}{p}\right).$$

Now, let us consider the case $p \equiv 3 \pmod 4$. We have

$$\begin{aligned} F_p(-1) &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)(-1)^a \\ &= \sum_{a=1}^{\frac{p-1}{2}} \left[\left(\frac{2a}{p}\right)(-1)^{2a} + \left(\frac{p-2a}{p}\right)(-1)^{p-2a}\right] \\ &= 2\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{2a}{p}\right) = 2\left(\frac{2}{p}\right)\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right). \end{aligned}$$

By [5, Corollary 3.4], we have

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = \left(2 - \left(\frac{2}{p}\right)\right) h(-p).$$

where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Therefore,

$$F_p(-1) = 2\left(2\left(\frac{2}{p}\right) - 1\right) h(-p).$$

We conclude that $F_p(-1) \neq 0$ if $p \equiv 3 \pmod 4$. □

Remark 2.4. The above proof also shows that if $p \equiv 3 \pmod 4$ then $x = -1$ is not a root of $F_p(x)$ modulo p. In fact, we have

$$0 < \left(2 - \left(\frac{2}{p}\right)\right) h(-p) = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) \leq \frac{p-1}{2}.$$

Hence, we see that $\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) \in \{1, 2, \ldots, \frac{p-1}{2}\}$. In particular, we have

$$p \nmid \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

From this, we can see that $p \nmid F_p(-1)$.

Here is another observation.

Lemma 2.5. *Suppose* $p \equiv 1 \pmod 4$. *Then*

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = 0$$

Proof. We use the same tricks as above. First, we know that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

We have

$$0 = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{a=1}^{\frac{p-1}{2}} \left[\left(\frac{a}{p}\right) + \left(\frac{p-a}{p}\right)\right] = 2\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

Hence

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = 0.$$

□

We have the following proposition.

Proposition 2.6. *If* $p \equiv 1 \pmod 4$ *then* $x = -1$ *is a simple root of* $F_p(x)$.

Proof. We already show that $F_p(-1) = 0$. To show that $x = -1$ is a simple root of $F_p(x)$, we need to show $F_p'(1) \neq 0$. We have

$$F_p'(-1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a(-1)^{a-1} = -\sum_{a=1}^{p-1} (-1)^a \left(\frac{a}{p}\right) a.$$

Therefore, it is enough to show that $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a(-1)^a \neq 0$. We have

$$\begin{aligned}\sum_{a=1}^{p-1} (-1)^a \left(\frac{a}{p}\right) a &= \sum_{a=1}^{\frac{p-1}{2}} \left[(-1)^{2a} \left(\frac{2a}{p}\right)(2a) + (-1)^{p-2a}\left(\left(\frac{p-2a}{p}\right)(p-2a)\right]\right. \\ &= \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{2a}{p}\right)(4a) - p\left(\frac{2}{p}\right)\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = 4\left(\frac{2}{p}\right)\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) a.\end{aligned}$$

By [5, Corollary 13.2], we have

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) a < 0.$$

Consequently,

$$\left(\frac{2}{p}\right)\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)(-1)^a a < 0.$$

In particular, $F_p'(-1) \neq 0$. We conclude that $x = -1$ is a simple root of $F_p(x)$. □

We discuss the necessary and sufficient condition for $x = -1$ to be a multiple root of $F_p(x)$ modulo p when $p \equiv 1 \pmod 4$. First, we express this condition in term of the classical Bernoulli numbers.

Proposition 2.7. *Let $p \equiv 1 \pmod 4$ and $p > 5$. Then $x = -1$ is a multiple root of $F_p(x)$ modulo p if and only if $p \mid B_{(p+3)/2}$.*

Proof. As shown above, $x = -1$ is a multiple root of $F_p(x)$ modulo p if and only if

$$p \mid \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)(-1)^a a.$$

By the computation in the proof of Proposition 2.6, this is equivalent to

$$p \mid \sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a.$$

By Euler's criterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, and hence

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a \equiv \sum_{a=1}^{\frac{p-1}{2}} a^{\frac{p-1}{2}}a \equiv \sum_{a=1}^{\frac{p-1}{2}} a^{\frac{p+1}{2}} \pmod p.$$

On the other hand, by [19, formula (10), page 352], one has

$$\sum_{a=1}^{\frac{p-1}{2}}(p-2a)^{2k-1} \equiv (2^{2k}-1)\frac{B_{2k}}{2k} \pmod p,$$

for k with $2k \not\equiv 2 \pmod{p-1}$. We choose the integer k such that $2k - 1 = \dfrac{p+1}{2}$. In this case, $2^{2k} - 1 = 4 \cdot 2^{\frac{p-1}{2}} - 1 \equiv 4\left(\dfrac{2}{p}\right) - 1 \pmod p$. Hence one has

$$\left(4\left(\frac{2}{p}\right)-1\right)\frac{B_{\frac{p+3}{2}}}{\frac{p+3}{2}} \equiv (-2)^{\frac{p+1}{2}}\sum_{a=1}^{\frac{p-1}{2}} a^{\frac{p+1}{2}} \equiv (-2)^{\frac{p+1}{2}}\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a \pmod p.$$

Therefore, for $p > 5$, $p \mid \sum\limits_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a$ if and only if $p \mid B_{\frac{p+3}{2}}$. □

We have a similar statement using generalized Bernoulli numbers.

Proposition 2.8. *Let $p \equiv 1 \pmod 4$ and $p > 5$. Then $x = -1$ is a multiple root of $F_p(x)$ modulo p if and only if $p|B_{2,\chi_p}$ where B_{2,χ_p} is the generalized Bernoulli number associated with χ_p (see* [17]*).*

Proof. As shown above, $x = -1$ is a multiple root of $F_p(x)$ modulo p if and only if

$$p|\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)(-1)^a a.$$

By the computation in the proof of Proposition 2.6, this is equivalent to

$$p|\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a.$$

By [5, Theorem 13.1] applied to χ_p, we have

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a = -\frac{p\sqrt{p}}{\pi^2}(1-\frac{\chi_p(2)}{4})L(2,\chi_p).$$

Furthermore, by the formula in [17, Page 12] we have

$$L(2,\chi_p) = \frac{\sqrt{p}}{2}\left(\frac{2\pi}{p}\right)^2 B_{2,\chi_p}.$$

Combining the above equality, we see that

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a = -\left(1-\frac{\chi_p(2)}{4}\right)B_{2,\chi_p}.$$

Therefore $p|\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a$ if and only if $p|\left(1-\frac{\chi_p(2)}{4}\right)B_{2,\chi_p}$. For $p > 5$, this is equivalent to $p|B_{2,\chi_p}$.

□

Remark 2.9. We have expressed the necessary and sufficient condition for $x = -1$ to be a multiple root of $F_p(x)$ modulo p using $B_{\frac{p+3}{2}}$ and B_{2,χ_p}. Using the Leopoldt-Kubota p-adic L-function, we can show that

$$\frac{B_{2,\chi_p}}{2} \equiv 2\frac{B_{\frac{p+3}{2}}}{p+3} \pmod p.$$

From this relation, we can see that the two conditions $p|B_{\frac{p+3}{2}}$ and $p|B_{2,\chi_p}$ are equivalent.

Remark 2.10. The condition $p|B_{\frac{p+3}{2}}$ implies that p is an irregular prime. In the list of all irregular primes less than 2^{31} computed by the authors of [16], $p = 89209$ is the only prime number that satisfies the condition $p|B_{\frac{p+3}{2}}$.

Remark 2.11. The question of whether $p|B_{2,\chi_p}$ is quite interesting. Let $F = \mathbb{Q}(\sqrt{p})$. By the consequence of the Iwasawa main conjecture proved by Wiles (see [18, Remark 1.4]) we have

$$\text{ord}_p\#H^2(\mathcal{O}_F[1/p], \mathbb{Z}_p(2)) = \text{ord}_p(\zeta_F(-1)) + \text{ord}_p\#H^1(\mathcal{O}_F[1/p], \mathbb{Z}_p(2)). \tag{1}$$

By the Quillen-Lichtenbaum's conjecture (now a theorem, see [9, Theorem 5.6.8]) we have

$$H^2(\mathcal{O}_F[1/p], \mathbb{Z}_p(2)) \cong K_2(\mathcal{O}_F) \otimes \mathbb{Z}_p, H^1(\mathcal{O}_F[1/p], \mathbb{Z}_p(2)) \cong K_3(\mathcal{O}_F) \otimes \mathbb{Z}_p.$$

Furthermore, the Galois group $\text{Gal}(F/\mathbb{Q}) = \{1, c\}$, with c being the complex conjugation, acts on all relevant groups. Because p is odd, we have a canonical decomposition

$$K_r(\mathcal{O}_F) \otimes \mathbb{Z}_p = (K_r(\mathcal{O}_F)^+ \otimes \mathbb{Z}_p) \bigoplus (K_r(\mathcal{O}_F)^- \otimes \mathbb{Z}_p) = (K_r(\mathbb{Z}) \otimes \mathbb{Z}_p) \bigoplus (K_r(\mathcal{O}_F)^- \otimes \mathbb{Z}_p).$$

On the L-function side we also have $\zeta_F(s) = \zeta_{\mathbb{Q}}(s)L(s, \chi_p)$. In particular, at $s = -1$, we have

$$\zeta_F(-1) = \zeta_{\mathbb{Q}}(-1)L(-1, \chi_p).$$

Finally, we have (see [17, Theorem 1])

$$L(-1, \chi_p) = -\frac{B_{2,\chi_p}}{-2}.$$

By the computation in [29, Table 10.1.1], we have $K_2(\mathbb{Z}) \otimes \mathbb{Z}_p = K_3(\mathbb{Z}) \otimes \mathbb{Z}_p = K_3(\mathcal{O}_F) \otimes \mathbb{Z}_p = 0$ for $p \geq 5$. So in summary, we have

$$\text{ord}_p(|K_2(\mathcal{O}_F)|) = \text{ord}_p(|K_2(\mathcal{O}_F)^-|) = \text{ord}_p(B_{2,\chi_p}). \tag{2}$$

Consequently, if $x = -1$ is a multiple root of $F_p(x)$ modulo p, the second K-group $K_2(\mathcal{O}_F)$ would be non-trivial.

In the proof of Proposition 2.6, the sum

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (-1)^a,$$

appears quite naturally. Following Berndt's article [5], we are interested in the following half-sum

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) (-1)^a.$$

Through numerical experiments, we found the following result.

Proposition 2.12. *Let p be an odd prime. Then*

(1) If $p \equiv \pm 1 \pmod 8$ then

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) (-1)^a > 0.$$

(2) If $p \equiv \pm 5 \pmod 8$ then

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) (-1)^a < 0.$$

Equivalently, we can summarize both of these statements into a single statement

$$\left(\frac{2}{p}\right) \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) (-1)^a > 0.$$

Proof. We first provide a proof for this speculation when $p \equiv 3 \pmod 4$. First of all, we have the following equality in the case $p \equiv 3 \pmod 4$.

$$\begin{aligned}
\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (-1)^a &= \sum_{a=1}^{\frac{p-1}{2}} \left[\left(\frac{a}{p}\right) (-1)^a + \left(\frac{p-a}{p}\right) (-1)^{p-a} \right] \\
&= \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) \left[(-1)^a - (-1)^{p-a} \right] \\
&= 2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) (-1)^a.
\end{aligned}$$

Second of all, by the proof of Proposition 2.3 we have

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (-1)^a = F_p(-1) = 2 \left(2 \left(\frac{2}{p}\right) - 1\right) h(-p).$$

Hence, we have

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)(-1)^a = \left(2\left(\frac{2}{p}\right) - 1\right) h(-p).$$

Therefore

$$\left(\frac{2}{p}\right) \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)(-1)^a = \left(2 - \left(\frac{2}{p}\right)\right) h(-p) > 0.$$

Let us now consider the case $p \equiv 1 \pmod 4$. In this case, we have

$$\begin{aligned}
\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)(-1)^a &= \sum_{\substack{1\le a\le \frac{p-1}{2} \\ a\equiv 0 \mod 2}} \left(\frac{a}{p}\right) + \sum_{\substack{1\le a\le \frac{p-1}{2} \\ a\equiv 1 \mod 2}} \left(\frac{a}{p}\right) \\
&= \sum_{a=1}^{\frac{p-1}{4}} \left(\frac{2a}{p}\right) - \sum_{\substack{1\le a\le \frac{p-1}{2} \\ a\equiv 1 \mod 2}} \left(\frac{p-a}{p}\right) \\
&= \left(\frac{2}{p}\right) \sum_{a=1}^{\frac{p-1}{4}} \left(\frac{a}{p}\right) - \sum_{\substack{1\le a\le \frac{p-1}{2} \\ a\equiv 1 \mod 2}} \left(\frac{p-a}{p}\right).
\end{aligned}$$

Note that if a is odd then $p-a$ is even. Let $2u = p-a$ in the second term. Then $\frac{p+1}{4} \le u \le \frac{p-1}{2}$. Because $p \equiv 1 \pmod 4$, we also have $\frac{p+3}{4} \le u \le \frac{p-1}{2}$. Therefore, we have

$$\sum_{\substack{1\le a\le \frac{p-1}{2} \\ a\equiv 1 \mod 2}} \left(\frac{p-a}{p}\right) = \sum_{u=\frac{p+3}{4}}^{\frac{p-1}{2}} \left(\frac{2u}{p}\right) = \left(\frac{2}{p}\right) \sum_{a=\frac{p+3}{4}}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

By Lemma 2.5, we have

$$\sum_{a=\frac{p+3}{4}}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = -\sum_{a=1}^{\frac{p-1}{4}} \left(\frac{a}{p}\right).$$

By the above equations, we see that

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)(-1)^a = 2\left(\frac{2}{p}\right) \sum_{a=1}^{\frac{p-1}{4}} \left(\frac{a}{p}\right).$$

By [5, Inequality 1.2], we have

$$\sum_{a=1}^{\frac{p-1}{4}} \left(\frac{a}{p}\right) > 0.$$

Therefore, we have

$$\left(\frac{2}{p}\right) \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) (-1)^a > 0.$$

□

3. The polynomials $f_p(x)$ and $g_p(x)$

Let us define

$$f_p(x) = \begin{cases} \dfrac{F_p(x)}{x(1-x)} & \text{if } p \equiv 3 \pmod 4 \\ \dfrac{F_p(x)}{x(1-x)^2(x+1)} & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

By the results from the previous section, we know that $f_p(x) \in \mathbb{Z}[x]$. In this section, we investigate some arithmetical properties of $f_p(x)$.

First, we introduce the following general notations. Let A be a commutative ring with identity. Recall that given a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

of degree n with coefficients from A, its reciprocal or reflected polynomial, denoted by f^* or f^R, is the polynomial

$$f^*(x) = x^n f\left(\frac{1}{x}\right).$$

The coefficients of f^* are the coefficients of f in reverse order. Polynomial f is called reciprocal or palindromic if $f = f^*$, that means $a_k = a_{n-k}$ for all k.

We also recall that the Dickson polynomial $D_n(x, a)$ of the first kind of degree $n \geq 1$ in the intermediate x and with parameter $a \in A$ is defined as

$$D_n(x, a) = \sum_{k=0}^{\lceil n/2 \rceil} \frac{n}{n-k} \binom{n-k}{k} (-a)^k x^{n-2k}.$$

The term $\frac{n}{n-k}\binom{n-k}{k}$ is an integer. Dickson polynomials $D_n(x, a)$ have following two basic properties:

(1) $D_n\left(x + \dfrac{1}{x}, a\right) = x^n + \dfrac{a^n}{x^n}.$

(2) $D_1(x,a) = x$, $D_2(x,a) = x^2 - 2a$, and

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x).$$

For simplicity we will write $D_n(x)$ for $D_n(x,1)$ so that $D_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$.

Now suppose that $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ is a reciprocal polynomial of even degree n. Write $n = 2s$ and set

$$g(x) = \sum_{k=0}^{s-1} a_k D_{n-k}(x) + a_s \in A[x].$$

Then $f(x) = x^s g(x + \frac{1}{x})$.

We have the following proposition.

Proposition 3.1. *$f_p(x)$ is a reciprocal polynomial of even degree.*

Proof. Let us consider the case $p \equiv 3 \pmod 4$. In this case, we have

$$f_p(x) = \frac{F_p(x)}{x(1-x)}.$$

Let us first consider the Fekete polynomial $F_p(x)$, we have

$$\begin{aligned} x^p F_p\left(\frac{1}{x}\right) &= x^p \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\left(\frac{1}{x}\right)^a = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^{p-a} \\ &= \sum_{u=1}^{p-1} \left(\frac{p-u}{p}\right) x^u = -\sum_{u=1}^{p-1} \left(\frac{u}{p}\right) x^u = -F_p(x). \end{aligned}$$

We then have

$$\begin{aligned} x^{p-3} f_p\left(\frac{1}{x}\right) &= x^{p-3} \frac{F_p\left(\frac{1}{x}\right)}{\frac{1}{x}\left(1 - \frac{1}{x}\right)} = \frac{-x^p F_p(1/x)}{x(1-x)} \\ &= \frac{F_p(x)}{x(1-x)} = f_p(x). \end{aligned}$$

Note that the degree of f_p is $\dfrac{p-3}{2}$ which is even. Therefore $f_p(x)$ is a reciprocal polynomial of even degree.

Next, let us consider the case $p \equiv 1 \pmod 4$. As the previous case, let us consider

$$x^p F_p\left(\frac{1}{x}\right) = x^p \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\left(\frac{1}{x}\right)^a = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)x^{p-a}$$
$$= \sum_{u=1}^{p-1}\left(\frac{p-u}{p}\right)x^u = \sum_{u=1}^{p-1}\left(\frac{u}{p}\right)x^u = F_p(x).$$

We then have

$$x^{p-5} f_p\left(\frac{1}{x}\right) = x^{p-3}\frac{F_p\left(\frac{1}{x}\right)}{\frac{1}{x}\left(\frac{1}{x}+1\right)\left(\frac{1}{x}-1\right)^2}$$
$$= \frac{x^p F_p(1/x)}{x(1+x)(x-1)^2} = \frac{F_p(x)}{x(1+x)(x-1)^2} = f_p(x).$$

Note that the degree of $f_p(x)$ is $\frac{p-5}{2}$ which is even. We conclude that $f_p(x)$ is a reciprocal polynomial of even degree. □

It is natural to define the following related polynomial.

Definition 3.2. Let $g_p(x) \in \mathbb{Z}[x]$ be the polynomial such that

$$f_p(x) = x^{\frac{\deg(f_p)}{2}} g_p\left(x + \frac{1}{x}\right).$$

We will call $g_p(x)$ the reduced Fekete polynomial associated with p.

We provide the explicit formulas for $f_p(x)$ and $g_p(x)$ for $p \leq 23$. Here are some explicit formulas for f_p.

$$f_7 = x^4 + 2x^3 + x^2 + 2x + 1.$$
$$f_{11} = x^8 + x^6 + 2x^5 + 3x^4 + 2x^3 + x^2 + 1$$
$$f_{13}(x) = x^8 + 2x^6 + 2x^5 + 3x^4 + 2x^3 + 2x^2 + 1.$$
$$f_{17} = x^{12} + 2x^{11} + 2x^{10} + 4x^9 + 3x^8 + 4x^7 + 2x^6 + 4x^5 + 3x^4 + 4x^3 + 2x^2 + 2x + 1.$$
$$f_{19} = x^{16} - x^{14} + x^{12} + 2x^{11} + 3x^{10} + 2x^9 + 3x^8 + 2x^7 + 3x^6 + 2x^5 + x^4 - x^2 + 1.$$

$$f_{23}(x) = x^{20} + 2x^{19} + 3x^{18} + 4x^{17} + 3x^{16} + 4x^{15} + 3x^{14} + 4x^{13} + 5x^{12} + 4x^{11}$$
$$+ 3x^{10} + 4x^9 + 5x^8 + 4x^7 + 3x^6 + 4x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1$$

Here are some explicit formulas for $g_p(u)$.

$$g_7(u) = u^2 + 2u - 1.$$

$$g_{11}(u) = u^4 - 3u^2 + 2u + 3.$$

$$g_{13}(u) = u^4 - 2u^2 + 2u + 1.$$

$$g_{17}(u) = u^6 + 2u^5 - 4u^4 - 6u^3 + 4u^2 + 2u - 2.$$

$$g_{19}(u) = u^8 - 9u^6 + 27u^4 + 2u^3 - 26u^2 - 4u + 3.$$

$$g_{23}(u) = u^{10} + 2u^9 - 7u^8 - 14u^7 + 14u^6 + 30u^5 - 5u^4 - 20u^3 - 3u^2 + 2u - 3.$$

It turns out that the special values of $g_p(x)$ contains lots of arithmetic information. We will demonstrate this observation by several propositions. For $p = 3$ or $p = 5$, $g_p(x) = 1$ so these are the trivial cases. From now on, we assume that $p \geq 7$. Let us recall that for a quadratic extension $\mathbb{Q}(\sqrt{s})$ ($s \in \mathbb{Q}^\times$) of $\mathbb{Q}$, we denote by $h(s)$ its class number.

Proposition 3.3. *If* $p \equiv 3 \pmod 4$ *then*

$$g_p(2) = f_p(1) = ph(-p).$$

If $p \equiv 1 \pmod 4$ *then*

$$g_p(2) = f_p(1) = \frac{pB_{2,\chi_p}}{4}.$$

Proof. Let us first consider the case $p \equiv 3 \pmod 4$. In this case $\dfrac{p-3}{2}$ is even, we have

$$g_p(2) = f_p(1).$$

We also have

$$xf_p(x) = \frac{F_p(x)}{1-x}.$$

Taking the limit when $x \to 1$, we have

$$f_p(1) = F_p'(1) = -\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r.$$

The right hand side is a classical sum. More precisely we have the following class number formula (see [14, Equation 3])

$$\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r = -ph(-p).$$

Hence, we see that

$$g_p(2) = f_p(1) = ph(-p).$$

Next, let us consider the case $p \equiv 1 \pmod 4$. As above, we have

$$g_p(2) = f_p(1).$$

Let us now compute $f_p(1)$. We have

$$x(x+1)f_p(x) = \frac{F_p(x)}{(x-1)^2}.$$

Taking the limit of both sides when $x \to 1$ we have

$$2f_p(1) = \frac{F_p''(1)}{2}.$$

By the proof of Lemma 2.1, we have

$$F_p''(1) = pB_{2,\chi_p}.$$

Therefore

$$f_p(1) = \frac{pB_{2,\chi_p}}{4}.$$

□

Proposition 3.4. *If $p \equiv 3 \pmod 4$ then*

$$g_p(-2) = f_p(-1) = -\left(2\left(\frac{2}{p}\right) - 1\right)h(-p).$$

On the other hand, if $p \equiv 1 \pmod 4$ then

$$f_p(-1) = g_p(-2) = -\frac{1}{4}\left(4\left(\frac{2}{p}\right) - 1\right)B_{2,\chi_p}.$$

Here B_{2,χ_p} is the generalized Bernoulli number associated with the character χ_p that was introduced in the second section.

Proof. Let us consider the case $p \equiv 3 \pmod 4$. By cause $\frac{p-3}{2}$ is even, we have

$$g_p(-2) = f_p(-1).$$

Furthermore, we have

$$f_p(-1) = \frac{F_p(-1)}{(-1)(1+1)} = -\frac{F_p(-1)}{2}.$$

By the proof of Proposition 2.3, we have

$$F_p(-1) = 2\left(2\left(\frac{2}{p}\right) - 1\right)h(-p).$$

From these equations, we conclude that

$$g_p(-2) = f_p(-1) = -\left(2\left(\frac{2}{p}\right) - 1\right)h(-p).$$

Next, let us consider the case $p \equiv 1 \pmod 4$. In this case $\dfrac{p-5}{2}$ is even and we have

$$g_p(-2) = f_p(-1).$$

By definition, we have

$$x(x-1)^2 f_p(x) = \frac{F_p(x)}{x+1}.$$

Taking the limit when $x \to -1$ we get

$$-4f_p(-1) = (-1)(-2)^2 f_p(-1) = F_p^{'}(-1).$$

By the computation done in the proof of Proposition 2.6 we have

$$F_p^{'}(-1) = -4\left(\frac{2}{p}\right)\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a.$$

By the proof of Proposition 2.8 we have

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a = -\left(1 - \frac{\chi(2)}{4}\right)B_{2,\chi_p}.$$

In summary, we have

$$g_p(-2) = f_p(-1) = -\frac{1}{4}\left(4\left(\frac{2}{p}\right) - 1\right)B_{2,\chi_p}.$$

□

Next, we compute the values of $g_p(x)$ at 0.

Proposition 3.5. *Let $p \equiv 3 \pmod 4$. Then*

$$g_p(0) = g_p(-2) = -\left(2\left(\frac{2}{p}\right) - 1\right)h(-p).$$

Proof. The statement for $g_p(-2)$ is a direct consequence of the previous proposition. Let us focus on the case $g_p(0)$. First, we recall that

$$f_p(x) = x^{\frac{p-3}{2}} g_p\left(x + \frac{1}{x}\right).$$

Plugging $x = i = \sqrt{-1}$ into this equation gives

$$f_p(i) = i^{\frac{p-3}{2}} g_p(0) = -\left(\frac{2}{p}\right) g_p(0).$$

Now, let us compute $f_p(i)$. We have

$$f_p(i) = -\frac{F_p(i)}{i(i-1)} = \frac{F_p(i)}{i+1}.$$

By the above equality we have

$$g_p(0) = -\frac{\left(\frac{2}{p}\right) F_p(i)}{i+1}.$$

We then have

$$\begin{aligned} F_p(i) &= \sum_{i=1}^{p-1} \left(\frac{a}{p}\right)(-1)^a \\ &= \sum_{a=1}^{\frac{p-1}{2}} \left[\left(\frac{2a}{p}\right) i^{2a} + \left(\frac{p-2a}{p}\right) i^{p-2a}\right] \\ &= (1+i) \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{2a}{p}\right) i^{2a} = (1+i)\left(\frac{2}{p}\right) \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)(-1)^a. \end{aligned}$$

Note that by the proofs of Proposition 2.12 and Proposition 2.3, we have

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)(-1)^a = \frac{1}{2} F_p(-1) = \left(2\left(\frac{2}{p}\right) - 1\right) h(-p).$$

Combining the above equations we have

$$F_p(i) = (i+1)\left(2 - \left(\frac{2}{p}\right)\right) h(-p).$$

Therefore, we have

$$g_p(0) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p).$$

□

By the same method, we can also compute $g_p(-1)$. Here we note that if ζ_3 is the cubic root of 1, namely $\zeta_3 = \exp(\frac{2\pi i}{3}) = \dfrac{-1+\sqrt{-3}}{2}$ then

$$\zeta_3 + \frac{1}{\zeta_3} = -1.$$

We then have

$$g_p(-1) = g_p\left(\zeta_3 + \frac{1}{\zeta_3}\right) = -\frac{F_p(\zeta_3)}{\zeta_3^{\frac{p-1}{2}}(\zeta_3 - 1)}. \tag{3}$$

Now, let us compute $F_p(\zeta_3)$. By definition

$$F_p(\zeta_3) = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_3^a.$$

We can break this sum into three sums according to $a \pmod 3$. More precisely

$$\begin{aligned}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_3^a &= \sum_{0<3a<p}\left(\frac{3a}{p}\right)\zeta_3^{3a} + \sum_{0<3a+1<p}\left(\frac{3a+1}{p}\right)\zeta_3^{3a+1} + \sum_{0<3a+2<p}\left(\frac{3a+2}{p}\right)\zeta_3^{3a+2}\\ &= \sum_{0<a\le\frac{p-1}{3}}\left(\frac{3a}{p}\right) + \zeta_3\sum_{0<3a+1<p}\left(\frac{3a+1}{p}\right) + \zeta_3^2\sum_{0<3a+2<p}\left(\frac{3a+2}{p}\right)\end{aligned}$$

First, let us consider the case $p \equiv 1 \pmod 3$. In this case, the two sets $\{3a\}$ and $\{p-3a-1\}$ are the same. Similarly, the two sets $\{3a+2\}$ and $\{p-3a-2\}$ are the same. Additionally, because $p \equiv 3 \pmod 4$, we have

$$\sum_{0<3a+1<p}\left(\frac{3a+1}{p}\right) = -\sum_{0<3a+1<p}\left(\frac{p-3a-1}{p}\right) = -\sum_{0<3a<p}\left(\frac{3a}{p}\right).$$

Simillarly

$$\sum_{0<3a+2<p}\left(\frac{3a+2}{p}\right) = -\sum_{0<3a+2<p}\left(\frac{p-3a-2}{p}\right) = -\sum_{0<3a+2<p}\left(\frac{3a+2}{p}\right).$$

Consequently,

$$\sum_{0<3a+2<p}\left(\frac{3a+2}{p}\right) = 0.$$

In summary, we have

$$F_p(\zeta_3) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_3^a = (1-\zeta_3) \sum_{0<3a<p} \left(\frac{3a}{p}\right) = (1-\zeta_3)\left(\frac{3}{p}\right) \sum_{0<a<p/3} \left(\frac{a}{p}\right).$$

By [5, Corollary 4.3] we have

$$\sum_{0<a<p/3} \left(\frac{a}{p}\right) = \frac{1}{2}\left(3 - \left(\frac{3}{p}\right)\right) h(-p).$$

We then have

$$F_p(\zeta_3) = \frac{1}{2}(1-\zeta_3)\left(3\left(\frac{3}{p}\right) - 1\right) h(-p).$$

From Equation 3 and the fact that $p \equiv 1 \pmod 3$, we have

$$g_p(-1) = -\frac{F_p(\zeta_3)}{\zeta_3^{\frac{p-1}{2}}(\zeta_3 - 1)} = \frac{1}{2}\left(3\left(\frac{3}{p}\right) - 1\right) h(-p).$$

Now, let us consider the case $p \equiv 2 \pmod 3$. By the same method, we can see that in this case

$$\begin{aligned} \sum_{0<3a+2<p} \left(\frac{3a+2}{p}\right) &= -\sum_{0<3a+2<p} \left(\frac{p-3a-2}{p}\right) \\ &= -\sum_{0<3a<p} \left(\frac{3a}{p}\right) \end{aligned}$$

Additionally

$$\sum_{0<3a+1<p} \left(\frac{3a+1}{p}\right) = 0.$$

Therefore

$$F_p(\zeta_3) = (1-\zeta_3^2)\left(\frac{3}{p}\right) \sum_{0<a<p/3} \left(\frac{a}{p}\right).$$

By [5, Corollary 4.3] we have

$$\sum_{0<a<p/3} \left(\frac{a}{p}\right) = \frac{1}{2}\left(3 - \left(\frac{3}{p}\right)\right) h(-p).$$

We then have

$$F_p(\zeta_3) = \frac{1}{2}(1-\zeta_3^2)\left(3\left(\frac{3}{p}\right) - 1\right) h(-p).$$

We note that when $p \equiv 2 \pmod 3$ we have $\zeta_3^{\frac{p-1}{2}} = \zeta_3^2$. Therefore

$$\zeta_3^{\frac{p-1}{2}}(\zeta_3 - 1) = \zeta_3^2(\zeta_3 - 1) = 1 - \zeta_3^2.$$

We conclude that in this case we have

$$g_p(-1) = -\frac{F_p(\zeta_3)}{\zeta_3^{\frac{p-1}{2}}(\zeta_3 - 1)} = -\frac{1}{2}\left(3\left(\frac{3}{p}\right) - 1\right)h(-p).$$

In summary we have the following proposition.

Proposition 3.6. *Let $p \equiv 3 \pmod 4$ then*

$$g_p(-1) = \begin{cases} \frac{1}{2}\left(3\left(\frac{3}{p}\right) - 1\right)h(-p) & \text{if } p \equiv 1 \pmod 3 \\ -\frac{1}{2}\left(3\left(\frac{3}{p}\right) - 1\right)h(-p) & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

In other words, we have

$$g_p(-1) = -\frac{1}{2}\left(\left(\frac{p}{3}\right) + 3\right)h(-p).$$

Let us go further to compute $g_p(1)$. To do so, we use the 6-primitive root of unity, namely $x = \zeta_6 = \exp(\frac{2\pi i}{6})$. We first note that

$$1 = \zeta_6 + \frac{1}{\zeta_6}.$$

As before, we have

$$g_p(1) = -\frac{F_p(\zeta_6)}{\zeta_6^{\frac{p-1}{2}}(\zeta_6 - 1)}.$$

We have

$$F_p(\zeta_6) = \sum_{i=0}^{5} \zeta_6^i \left[\sum_{0<6n+i<p} \left(\frac{6n+i}{p}\right)\right].$$

To compute this sum, we use the same technique as before. First, we note that when $p \equiv 1 \pmod 3$, the following sets are the same

$$\{6n+1\} = \{p - 6n\}, \{6n+4\} = \{p - (6n+3)\}, \{6n+5\} = \{p - (6n+2)\}.$$

From this observation we have the following identities

$$\sum_{0<6n+1<p} \left(\frac{6n+1}{p}\right) = -\sum_{0<6n<p} \left(\frac{6n}{p}\right),$$

$$\sum_{0<6n+4<p} \left(\frac{6n+4}{p}\right) = -\sum_{0<6n+3<p} \left(\frac{6n+3}{p}\right),$$

$$\sum_{0<6n+5<p}\left(\frac{6n+5}{p}\right)=-\sum_{0<6n+2<p}\left(\frac{6n+2}{p}\right).$$

Therefore, we see that

$$F_p(\zeta_6)=(1-\zeta_6)\sum_{0<6n<p}\left(\frac{6n}{p}\right)+(\zeta_6^2-\zeta_6^5)\sum_{0<6n+2<p}\left(\frac{6n+2}{p}\right)+(\zeta_6^3-\zeta_6^4)\sum_{0<6n+3<p}\left(\frac{6n+3}{p}\right).$$

Now, let us simplify the second and the third sums. We have

$$\begin{aligned}\sum_{0<6n+2<p}\left(\frac{6n+2}{p}\right)&=\left(\frac{2}{p}\right)\sum_{0<3n+1<p/2}\left(\frac{3n+1}{p}\right)\\&=-\left(\frac{2}{p}\right)\sum_{0<3n+1<p/2}\left(\frac{p-(3n+1)}{p}\right).\end{aligned}$$

Let $3u=p-(3n+1)$. Then $u\in\mathbb{Z}$ and $p/6<u<p/3$. Therefore, the above identity can be rewritten as

$$\sum_{0<6n+2<p}\left(\frac{6n+2}{p}\right)=-\left(\frac{6}{p}\right)\sum_{p/6<u<p/3}\left(\frac{u}{p}\right)=-\left(\frac{6}{p}\right)S_{26}.$$

Here we use the notations S_{ij} as introduced in [5, Page 265]. By a similar computation, we can see that

$$\sum_{0<6n+3<p}\left(\frac{6n+3}{p}\right)=-\left(\frac{6}{p}\right)\sum_{p/3<u<p/2}\left(\frac{u}{p}\right)=-\left(\frac{6}{p}\right)S_{36}.$$

Finally, we have

$$\sum_{0<6n<p}\left(\frac{6n+2}{p}\right)=\left(\frac{6}{p}\right)S_{16}.$$

In summary, we have

$$\begin{aligned}F_p(\zeta_6)&=\left(\frac{6}{p}\right)\left[(1-\zeta_6)S_{16}-(\zeta_6^2-\zeta_6^5)S_{26}-(\zeta_6^3-\zeta_6^4)S_{36}\right]\\&=-\zeta_6^2\left(\frac{6}{p}\right)\left[S_{16}+2S_{26}+S_{36}\right].\end{aligned}$$

Here we use the following identities

$$1-\zeta_6=-\zeta_6^2,\zeta_6^2-\zeta_6^5=2\zeta_6^2,\zeta_6^3-\zeta_6^4=\zeta_6^2.$$

By [5, Theorem 6.1], we have

$$S_{16}=\frac{h(-p)}{2}\left[1+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)-\left(\frac{6}{p}\right)\right],$$

$$S_{26} = \frac{h(-p)}{2}\left[2 - 2\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right],$$

$$S_{36} = \frac{h(-p)}{2}\left[1 - 2\left(\frac{2}{p}\right) + \left(\frac{3}{p}\right)\right],$$

By some simple algebraic calculations, we have

$$S_{16} + 2S_{26} + S_{36} = 6 - 3\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right).$$

Using these equations, we conclude that

$$F_p(\zeta_6) = -\zeta_6^2 \times \frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6 - 3\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right].$$

Note that when $p \equiv 1 \pmod 3$ we have $\zeta_6^{\frac{p-1}{2}} = -1$. Additionally, we note that $\zeta_6 - 1 = \zeta_6^2$. Consequently, we have

$$g_p(1) = -\frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6 - 3\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right].$$

Now, let us consider the case $p \equiv 2 \pmod 3$. In this case, we observe that the following sets are the same

$$\{6n+5\} = \{p - 6n\}, \{6n+4\} = \{p - (6n+1)\}, \{6n+2\} = \{p - (6n+3)\}.$$

Therefore

$$F_p(\zeta_6) = (1 - \zeta_6^5)\sum_{0<6n<p}\left(\frac{6n}{p}\right) + (\zeta_6^4 - \zeta)\sum_{0<6n+4<p}\left(\frac{6n+2}{p}\right) + (\zeta_6^3 - \zeta_6^2)\sum_{0<6n+3<p}\left(\frac{6n+3}{p}\right).$$

By the same arguments in in the case $p \equiv 1 \pmod 3$, we have

$$\sum_{0<6n+2<p}\left(\frac{6n+2}{p}\right) = -\left(\frac{6}{p}\right)\sum_{p/6<u<p/3}\left(\frac{u}{p}\right) = -\left(\frac{6}{p}\right)S_{26},$$

and

$$\sum_{0<6n+3<p}\left(\frac{6n+3}{p}\right) = -\left(\frac{6}{p}\right)\sum_{p/3<u<p/2}\left(\frac{u}{p}\right) = -\left(\frac{6}{p}\right)S_{36}.$$

By [5, Theorem 6.1], we have

$$\begin{aligned} F_p(\zeta_6) &= \left(\frac{6}{p}\right)\left[(1-\zeta_6^5)S_{16} - (\zeta_6^4-\zeta_6)S_{26} - (\zeta_6^3-\zeta_6^2)S_{36}\right] \\ &= \zeta_6\left(\frac{6}{p}\right)[S_{16}+2S_{26}+S_{36}] \\ &= \zeta_6\frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6-3\left(\frac{2}{p}\right)-2\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)\right]. \end{aligned}$$

When $p \equiv 2 \pmod 3$, we also have

$$\zeta_6^{\frac{p-1}{2}}(\zeta_6-1) = \zeta_6.$$

Hence

$$g_p(1) = -\frac{F_p(\zeta_6)}{\zeta_6^{\frac{p-1}{2}}(\zeta_6-1)} = -\frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6-3\left(\frac{2}{p}\right)-2\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)\right].$$

In summary, we have just showed that.

Proposition 3.7. *Let $p \equiv 3 \pmod 4$. Then*

$$g_p(1) = -\frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6-3\left(\frac{2}{p}\right)-2\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)\right].$$

Next, let us compute $g_p(0)$, $g_p(1)$ and $g_p(-1)$ when $p \equiv 1 \pmod 4$. First, let us compute $g_p(-1)$. We have

$$g_p(0) = \frac{F_p(i)}{i^{\frac{p-3}{2}}(1+i)(i-1)^2} = \frac{F_p(i)}{-2(i+1)i^{\frac{p-1}{2}}}.$$

We have

$$F_p(i) = \sum_{i=1}^{p-1}\left(\frac{n}{p}\right)i^n = \sum_{i=0}^{3} i^a\left[\sum_{0<4n+i<p}\left(\frac{4n+i}{p}\right)\right].$$

The following sets are the same

$$\{4n\} = \{p-(4n+1)\}, \{4a+3\} = \{p-(4n+3)\}.$$

Therefore we have

$$\sum_{0<4n+1<p}\left(\frac{4a+1}{p}\right) = \sum_{0<4n+1<p}\left(\frac{p-(4n+1)}{p}\right) = \sum_{0<4n<p}\left(\frac{4n}{p}\right) = S_{14}.$$

Similarly, we have

$$\sum_{0<4n+3<p}\left(\frac{4n+3}{p}\right)=\sum_{0<4n+3<p}\left(\frac{p-(4n+3)}{p}\right)=\sum_{0<4n+2<p}\left(\frac{4n+2}{p}\right).$$

We have

$$\begin{aligned}\sum_{0<4n+2<p}\left(\frac{4n+2}{p}\right)&=\left(\frac{2}{p}\right)\sum_{0<2n+1<p/2}\left(\frac{2n+1}{p}\right)\\&=\left(\frac{2}{p}\right)\sum_{0<2n+1<p/2}\left(\frac{p-(2n+1)}{p}\right)\\&=\left(\frac{2}{p}\right)\sum_{p/4<u<p/2}\left(\frac{2u}{p}\right)=\sum_{p/4<u<p/2}\left(\frac{u}{p}\right).\end{aligned}$$

By the proof of Proposition 2.12, we have

$$\sum_{p/4<u<p/2}\left(\frac{u}{p}\right)=-\sum_{0<u<p/4}\left(\frac{u}{p}\right)=-S_{14}.$$

We then deduce that

$$F_p(\zeta_4)=(1+i)S_{14}-(i^2+i^3)S_{14}=2(i+1)S_{14}.$$

Hence

$$g_p(-1)=\frac{F_p(\zeta_4)}{-2(i+1)i^{\frac{p-1}{2}}}=\frac{2(i+1)S_{14}}{-2(i+1)i^{\frac{p-1}{2}}}=-\frac{S_{14}}{(-1)^{\frac{p-1}{4}}}=-\left(\frac{2}{p}\right)S_{14}.$$

By [5, Corollary 3.9], we have $S_{14}=\frac{1}{2}h(-4p)$. Therefore, we have

Proposition 3.8. *Let* $p\equiv 1 \pmod 4$, *then*

$$g_p(0)=-\frac{1}{2}\left(\frac{2}{p}\right)h(-4p).$$

Next, we will use ζ_6 to compute this $g_p(1)$. We have

$$g_p(1)=\frac{F_p(\zeta_6)}{\zeta_6^{\frac{p-3}{2}}(1+\zeta_6)(\zeta_6-1)^2}=-\frac{F_p(\zeta_6)}{\zeta_6^{\frac{p-1}{2}}(1+\zeta_6)}.$$

Let us consider the case $p \equiv 1 \pmod 3$. By the same argument as in the case $p \equiv 3 \pmod 4$ we have

$$\begin{aligned} F_p(\zeta_6) &= \left(\frac{6}{p}\right)\left[(1+\zeta_6)S_{16} + (\zeta_6^2+\zeta_6^5)S_{26} + (\zeta_6^3+\zeta_6^4)S_{36}\right] \\ &= (1+\zeta_6)\left(\frac{6}{p}\right)[S_{16}-S_{36}] \end{aligned}$$

We then have

$$g_p(1) = -\left(\frac{6}{p}\right)\frac{S_{16}-S_{36}}{\zeta_6^{\frac{p-1}{2}}} = -\left(\frac{6}{p}\right)[S_{16}-S_{36}].$$

By [5, Theorem 6.1] we have

$$S_{16} = \frac{1}{2}\left(1+\left(\frac{2}{p}\right)\right)h(-3p),$$

and

$$S_{36} = -\frac{1}{2}h(-3p).$$

Hence

$$\begin{aligned} g_p(1) &= -\frac{1}{2}\left(\frac{6}{p}\right)\left(2+\left(\frac{2}{p}\right)\right)h(-3p) \\ &= -\frac{1}{2}\left(\frac{p}{3}\right)\left(\frac{6}{p}\right)\left(2+\left(\frac{2}{p}\right)\right)h(-3p) \\ &= -\frac{1}{2}\left(\frac{p}{3}\right)\left(\frac{3}{p}\right)\left(\frac{2}{p}\right)\left(2+\left(\frac{2}{p}\right)\right)h(-3p) \\ &= -\frac{1}{2}\left(2\left(\frac{2}{p}\right)+1\right)h(-3p) \end{aligned}$$

Note that, in the third equality, we use the quadratic reciprocity law

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = 1,$$

as in our case $p \equiv 1 \pmod 4$. Now, let us consider the case $p \equiv 2 \pmod 3$. Then we have

$$\begin{aligned} F_p(\zeta_6) &= \left(\frac{6}{p}\right)\left[(1+\zeta_6^5)S_{16} + (\zeta_6^4+\zeta_6)S_{26} + (\zeta_6^3+\zeta_6^2)S_{36}\right] \\ &= (1-\zeta_6^2)\left(\frac{6}{p}\right)[S_{16}-S_{36}]. \end{aligned}$$

Therefore

$$g_p(1) = -\frac{F_p(\zeta_6)}{\zeta_6^{\frac{p-1}{2}}(1+\zeta_6)} = \left(\frac{6}{p}\right)[S_{16} - S_{36}] = \frac{1}{2}\left(\frac{6}{p}\right)\left(2 + \left(\frac{2}{p}\right)\right)h(-3p).$$

By the same calculation as in the case $p \equiv 1 \pmod 3$, the above sum can be simplify to

$$g_p(1) = -\frac{1}{2}\left(2\left(\frac{2}{p}\right) + 1\right)h(-3p).$$

We conclude that

Proposition 3.9. *Let $p \equiv 1 \pmod 4$, then*

$$g_p(1) = -\frac{1}{2}\left(2\left(\frac{2}{p}\right) + 1\right)h(-3p).$$

Finally, let us compute $g_p(-1)$. We have

$$g_p(-1) = \frac{F_p(\zeta_6)}{\zeta_3^{\frac{p-3}{2}}(1+\zeta_3)(\zeta_3-1)^2} = \frac{F_p(\zeta_3)}{3\zeta_3^{\frac{p-3}{2}}}.$$

Let us consider the case $p \equiv 1 \pmod 3$. By the same argument as above we have

$$\begin{aligned} F_p(\zeta_3) &= \left(\frac{6}{p}\right)\left[(1+\zeta_3)S_{16} + (\zeta_3^2 + \zeta_3^5)S_{26} + (\zeta_3^3 + \zeta_2^4)S_{36}\right] \\ &= -\zeta_3^2\left(\frac{6}{p}\right)[S_{16} - 2S_{26} + S_{36}] \\ &= 3\zeta_3^2\left(\frac{6}{p}\right)S_{26}. \end{aligned}$$

For the last equality, we use the fact that when $p \equiv 1 \pmod 4$

$$S_{16} + S_{26} + S_{36} = \sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right) = 0.$$

We conclude that

$$g_p(-1) = \left(\frac{6}{p}\right)S_{26}.$$

By [5, Theorem 6.1], we have

$$S_{26} = -\frac{1}{2}\left(\frac{2}{p}\right)h(-3p).$$

Therefore

$$g_p(-1) = -\frac{1}{2}\left(\frac{3}{p}\right)h(-3p).$$

Let us consider the case $p \equiv 2 \pmod 3$. Then we have

$$\begin{aligned} F_p(\zeta_3) &= \left(\frac{6}{p}\right)\left[(1+\zeta_3^5)S_{16} + (\zeta_3^4+\zeta_3)S_{26} + (\zeta_3^3+\zeta_3^2)S_{36}\right] \\ &= -\zeta_3\left(\frac{6}{p}\right)[S_{16} - S_{36}] \\ &= 3\zeta_3\left(\frac{6}{p}\right)S_{26}. \end{aligned}$$

By the same argument as above we see that

$$g_p(-1) = -\frac{1}{2}\left(\frac{3}{p}\right)h(-3p).$$

In summary, we have the following proposition.

Proposition 3.10. *Let $p \equiv 1 \pmod 4$, then*

$$g_p(-1) = -\frac{1}{2}\left(\frac{3}{p}\right)h(-3p).$$

Here is a table for the special values of these $g_p(u)$, for $p \leq 23$, at $u = -2, -1, 0, 1, 2$.

p	$g_p(-2)$	$g_p(-1)$	$g_p(0)$	$g_p(1)$	$g_p(2)$
7	-1	-2	-1	2	7
11	3	-1	3	3	11
13	5	-2	1	2	13
17	-6	1	-2	-3	34
19	3	-2	3	-6	19
23	-3	-3	-3	-3	69

4. Galois theory for f_p and $g_p(x)$

In this section, we study Galois theory for f_p and g_p for prime $p \geq 7$. The following lemma is the direct consequence of our previous computations for $g_p(2)$ and $g_p(-2)$.

Lemma 4.1. *Let $s_p = f_p(1)f_p(-1) = g_p(2)g_p(-2)$. Then*

$$s_p = \begin{cases} (1-4\left(\frac{2}{p}\right))p\left(\frac{B_{2,\chi_p}}{4}\right)^2 & \text{if } p \equiv 1 \pmod 4 \\ -(2\left(\frac{2}{p}\right)-1)ph(-p)^2 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Corollary 4.2. *The polynomial f_p is irreducible over $\mathbb{Q}$ if and only if g_p is irreducible over $\mathbb{Q}$*

Proof. It is clear that if g_p is reducible over $\mathbb{Q}$ then f_p is reducible over $\mathbb{Q}$. Now we suppose that g_p is irreducible over $\mathbb{Q}$. By the above lemma, we see that $|s_p| = |f_p(1)| \cdot |f_p(-1)|$ is never a square in $\mathbb{Q}$. Hence $|f_p(1)|$ or $|f_p(-1)|$ are not perfect squares. By [6, Theorem 11] we conclude that f_p is irreducible. □

We have the following proposition.

Proposition 4.3. *$\sqrt{s_p}$ belongs the splitting field of f_p.*

We provide two proofs for this proposition. The first proof uses the following observation which is interesting on its own. We are grateful to Professor Arturas Dubickas for alerting us that the result was already known. See the following interesting references [2, page 127], [12, page 85] and [8, page 51], where the statement was observed and proved.

Proposition 4.4. *Let f be a reciprocal polynomial of even degree $2n$ over a field of characteristics different from 2. Let g be the polynomial of degree n such that*

$$f(x) = x^n g(u),$$

where $u = x + \dfrac{1}{x}$. Let $s = (-1)^n f(1)f(-1)$. Then

$$\Delta(f) = s \times \Delta(g)^2,$$

where $\Delta(f)$ is the discriminant of a monic polynomial f. Recall that $\Delta(f)$ is defined to be

$$\Delta(f) = \prod_{i<j}(z_i - z_j)^2,$$

with z_i are all the roots of f. In particular, $\sqrt{s}$ belongs to the splitting field of f.

Proof. As above, let $\{u_1, \ldots, u_n\}$ are the roots of g. For each u_i, the is a corresponding quadratic equation

$$u_i = x + \frac{1}{x}.$$

The above equation can be rewritten as

$$x^2 - u_i x + 1 = 0.$$

Let x_{i1}, x_{i2} be the two roots of this equation. Then, the set $\{x_{i1}, x_{i2}\}_{i=1}^n$ is the set of all roots of $f(x)$. We will order this set using the lexicographical order on the product $\{1, 2, \ldots, n\} \times \{1, 2\}$. We have the following identities

$$x_{i1} + x_{i2} = u_i, x_{i1}x_{i2} = 1, \forall 1 \leq i \leq n.$$

Let $1 \leq i < j \leq n$, then there are four roots associated with these two indices namely $\{x_{i1}, x_{i2}, x_{j1}, x_{j2}\}$. The term appeared in the discriminant of f associated with these four roots is

$$\begin{aligned}(x_{j1} - x_{i1})^2(x_{j1} - x_{i2})^2(x_{j2} - x_{i1})^2(x_{j2} - x_{i2})^2 &= [(x_{j1} - x_{i1})(x_{j1} - x_{i2})]^2[(x_{j2} - x_{i1})^2(x_{j2} - x_{i2})]^2 \\ &= \Big[(x_{j1}^2 - u_i x_{j1} + 1)(x_{j2}^2 - u_i x_{j2} + 1)\Big]^2.\end{aligned}$$

Using the property that $x_{j1}x_{j2} = 1$ and $x_{j1} + x_{j2} = u_j$, we can see that

$$\begin{aligned}(x_{j1}^2 - u_i x_{j1} + 1)(x_{j2}^2 - u_i x_{j2} + 1) &= 2 - 2u_i(x_{j1} + x_{j2}) + x_{j1}^2 + x_{j2}^2 + u_j^2 \\ &= 2 - 2u_i uj + (u_i^2 - 2) + u_j^2 \\ &= (u_i - u_j)^2.\end{aligned}$$

Therefore, we have

$$(x_{j1} - x_{i1})^2(x_{j1} - x_{i2})^2(x_{j2} - x_{i1})^2(x_{j2} - x_{i2})^2 = (u_i - u_j)^4.$$

Note that when $i = j$, we also have the term

$$(x_{i2} - x_{i1})^2 = u_i^2 - 4.$$

In particular, we have

$$\begin{aligned}\prod_{i=1}^{n}(x_{i2} - x_{i1})^2 = \prod_{i=1}^{n}(u_i^2 - 4) &= \prod_{i-1}^{n}(2 - u_i)(-2 - u_i) \\ &= \prod_{i=1}^{n}(2 - u_i) \times \prod_{i=1}^{n}(-2 - u_i) \\ &= g(2)g(-2) = (-1)^n f(1)f(-1) = s.\end{aligned}$$

From these computations, we conclude that

$$\Delta(f) = s \times \Delta(g)^2.$$

Finally note that $\sqrt{\Delta(f)}$ belongs to the splitting field of f. By the above relation, we can conclude that $\sqrt{s}$ belongs to the splitting field of f as well.

□

The second proof is quite similar to the first proof. We actually found the second proof first through some numerical computations with small prime p. For the sake of completeness, we include it here. The proof will be almost identical for the two cases

$p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 4$. Therefore, we only provide our proof in the case $p \equiv 3 \pmod 4$.

Proof. Let $\{u_i\}_{i=1}^{\frac{p-5}{2}}$ be the roots of $g_p(x)$. By definition of u, we know that for all $1 \leq i \leq \frac{p-5}{2}$, we have $u_i \in \mathbb{Q}(f_p)$. Furthermore, for each $1 \leq i \leq \frac{p-5}{2}$, the roots of the following equation are also in $\mathbb{Q}(f_p)$

$$u_i = x + \frac{1}{x}.$$

The above equation can be rewritten as

$$x^2 - u_i x + 1 = 0.$$

By the quadratic formula, the two roots of this quadratic equation are given by

$$x_{1,\pm} = \frac{u_i \pm \sqrt{u_i^2 - 4}}{2}.$$

A direct consequence of this calculation is that $\sqrt{u_i^2 - 4} \in \mathbb{Q}(f_p)$. In particular, $\sqrt{s} \in \mathbb{Q}(f_p)$ where

$$s_p = \prod_{i=1}^{\frac{p-5}{2}} (u_i^2 - 4)$$

Let us compute s_p. We notice that

$$s_p = \prod_{i=1}^{\frac{p-5}{2}} (u_i^2 - 4) = \prod_{i=1}^{\frac{p-5}{2}} (2 - u_i) \times \prod_{i=1}^{\frac{p-5}{2}} (-2 - u_i) = g_p(2) g_p(-2) = f_p(1) f_p(-1).$$

This completes the proof.

□

We have the following immediate corollaries.

Corollary 4.5. *Let $p \equiv 3 \pmod 4$. Let $h = -(2\left(\frac{2}{p}\right) - 1)p$. Then $\sqrt{h}$ belongs to the splitting field of f_p.*

Corollary 4.6. *Let $p \equiv 1 \pmod 4$. Let $h = (1 - 4\left(\frac{2}{p}\right))p$. Then $\sqrt{h}$ belongs to the splitting field of f_p.*

Let us keep the same notations in Proposition 4.4 and its proof. Furthermore, let $\mathbb{Q}(f)$, $\mathbb{Q}(g)$ be the splitting fields of f and g respectively. Then we have

$$\mathbb{Q}(g) = \mathbb{Q}(u_1, \ldots, u_n),$$

and

$$\mathbb{Q}(f) = \mathbb{Q}(g)[x_{i1}, x_{i2} | 1 \leq i \leq n].$$

Note that x_{i1}, x_{i2} are roots of a quadratic equation with coefficients in $\mathbb{Q}(g)$, namely

$$x^2 - u_i x + 1 = 0.$$

We therefore can see that

$$[\mathbb{Q}(g)[x_{i1}, x_{i2}] : \mathbb{Q}(g)] \leq 2.$$

Consequently

$$[\mathbb{Q}(f) : \mathbb{Q}(g)] = [\mathbb{Q}(g)[x_{i1}, x_{i2} | 1 \leq i \leq n] : \mathbb{Q}(g)] \leq \prod_{i=1}^{n} [\mathbb{Q}(g)[x_{i1}, x_{i2}] : \mathbb{Q}(g)] \leq 2^n.$$

The following is an immediate consequence of the above estimate and the fact that $\deg(g) = n$.

Corollary 4.7. *Let f, g be as in Proposition 4.4, then*

$$n! \geq [\mathbb{Q}(g) : \mathbb{Q}] \geq \frac{[\mathbb{Q}(f) : \mathbb{Q}]}{2^n}.$$

In particular, if $n! = \dfrac{[\mathbb{Q}(f) : \mathbb{Q}]}{2^n}$ then $\mathbb{Q}(g)/\mathbb{Q}$ is a Galois extension with Galois group S_n. Additionally, $\mathbb{Q}(f)/\mathbb{Q}$ is a Galois extension of degree $2^n n!$.

Using the computer program PARI, we found that for $p \leq 43$, it is always the case that

$$[\mathbb{Q}(f_p) : \mathbb{Q}] = 2^{h_p}(h_p)!,$$

with $h_p = \dfrac{\deg(f_p)}{2} = \deg(g_p)$. By Corollary 4.7, we conclude that

Proposition 4.8. *Let p be a prime number such that $p \leq 43$. Then $\mathbb{Q}(g_p)/\mathbb{Q})$ is a Galois extension with Galois group S_{h_p} where $h_p = \deg(g_p)$. Additionally, $\mathbb{Q}(f_p)/\mathbb{Q}$ is a Galois extension of degree $2^{h_p}(h_p)!$*

By this proposition, it is reasonable to make the following conjecture.

Conjecture 4.9. *$\mathbb{Q}(g_p)/\mathbb{Q}$ is a Galois extension with Galois group S_{h_p} where $h_p = \deg(g_p)$.*

We provide some further evidence for Conjecture 4.9. Since it is computationally challenging to compute the degree of $\mathbb{Q}(g_p)$ in general, we develop another strategy to show that $\mathbb{Q}(g_p)/\mathbb{Q} \cong S_{h_p}$ where $h_p = \deg(g_p)$. This strategy is based on the following observation.

Proposition 4.10. *Let $f(x)$ be a monic polynomial with integer coefficients of degree n. Assume that there exists a triple of prime numbers (q_1, q_2, q_3) such that*

(1) $f(x)$ is irreducible in $\mathbb{F}_{q_1}[x]$.

(2) $f(x)$ has the following factorization in $\mathbb{F}_{q_2}[x]$

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

where $c \in \mathbb{F}_{q_2}$ and $h(x)$ is an irreducible polynomial of degree $n - 1$.

(3) $f(x)$ has the following factorization in $\mathbb{F}_{q_3}[x]$

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

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

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

A proof for this proposition can be read off from [21, Example 4.33] where a particular example of (q_1, q_2, q_3) is discussed. For the sake of completeness, we provide a proof of the this proposition as stated above.

Proof. Let $G_f = \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ which is naturally a subgroup of S_n. The first condition implies that $f(x)$ is irreducible over $\mathbb{Z}$, hence over $\mathbb{Q}$. By [21, Proposition 4.4], G_f is a transitive subgroup of S_n. The second condition implies that G_f contains an $(n-1)$ cycle. The third condition implies that G_f contains a transposition. By [21, Lemma 4.32], we must have $G_f = S_n$.

□

Example 4.11. Let us discuss a concrete example with $p = 11$. In this case, we have

$$g_{11}(x) = x^4 - 3x^2 + 2x + 3.$$

Let $(q_1, q_2, q_3) = (5, 7, 53)$. Then $g_{11}(x)$ is irreducible in $\mathbb{F}_5[x]$. In $\mathbb{F}_7[x]$, $g_{11}(x)$ has the following factorization

$$g_{11}(x) = (x + 4)(x^3 + 3x^2 + 6x + 6).$$

In $\mathbb{F}_{53}[x]$, $g_{11}(x)$ has the following factorization

$$g_{11}(x) = (x + 26)(x + 30)(x^2 + 50x + 21).$$

We see that the triple (q_1, q_2, q_3) satisfies the conditions given in Proposition 4.10. Therefore the Galois group of $g_{11}(x)$ must be S_4.

Example 4.12. Let us consider the case $p = 13$. In this case, we have

$$g_{13}(x) = x^4 - 2x^2 + 2x + 1.$$

Let $(q_1, q_2, q_3) = (3, 5, 61)$. Then $g_{13}(x)$ is irreducible in $\mathbb{F}_3[x]$. In $\mathbb{F}_5[x]$, it has the following factorization

$$g_{13}(x) = (x + 2)(x^3 + 3x^2 + 2x + 3).$$

In $\mathbb{F}_{61}[x]$, it has the following factorization

$$g_{13}(x) = (x + 51)(x + 54)(x^2 + 17x + 34).$$

We see that (q_1, q_2, q_3) satisfies the conditions given in Proposition 4.10. We conclude that the Galois group of $g_{13}(x)$ is S_4.

We wrote some SageMath codes to test the above strategy (see [23]). We found that for $p \leq 1600$, the triple (q_1, q_2, q_3) always exists. We provide below the smallest triple (q_1, q_2, q_3) for $p < 1000$. We then show the running time for each p in the range $[1000, 1100]$ (Table 3). Finally, we provide the running time when we search for the triple (q_1, q_2, q_3) for several p. As indicated in Table 4, this is a computationally challenging problem.

TABLE 1. Smallest triples (q_1, q_2, q_3) for primes $7 < p < 500$

p	(q_1, q_2, q_3)
11	$(5, 7, 53)$
13	$(3, 5, 61)$
17	$(19, 3, 11)$
19	$(5, 31, 43)$
23	$(7, 13, 101)$
29	$(53, 5, 83)$
31	$(61, 13, 17)$
37	$(7, 13, 31)$
41	$(11, 103, 43)$
43	$(5, 31, 23)$
47	$(107, 7, 53)$
53	$(11, 59, 17)$
59	$(211, 257, 41)$
61	$(197, 5, 41)$
67	$(113, 41, 29)$
71	$(31, 37, 5)$
73	$(97, 149, 47)$
79	$(73, 113, 53)$
83	$(617, 61, 101)$
89	$(127, 151, 103)$
97	$(53, 61, 41)$
101	$(547, 149, 89)$
103	$(457, 277, 127)$
107	$(17, 193, 53)$
109	$(127, 293, 157)$
113	$(23, 491, 101)$
127	$(223, 197, 41)$
131	$(499, 1193, 19)$
137	$(839, 523, 59)$
139	$(673, 103, 157)$
149	$(107, 43, 179)$

p	(q_1, q_2, q_3)
151	$(1217, 37, 67)$
157	$(229, 67, 191)$
163	$(23, 239, 103)$
167	$(199, 379, 73)$
173	$(127, 139, 29)$
179	$(131, 211, 101)$
181	$(569, 347, 613)$
191	$(509, 281, 101)$
193	$(13, 307, 107)$
197	$(2141, 257, 17)$
199	$(547, 787, 17)$
211	$(47, 311, 23)$
223	$(1481, 179, 103)$
227	$(317, 439, 223)$
229	$(631, 719, 89)$
233	$(1559, 977, 29)$
239	$(199, 17, 59)$
241	$(2857, 1231, 83)$
251	$(41, 73, 277)$
257	$(1129, 919, 227)$
263	$(1571, 239, 17)$
269	$(929, 97, 43)$
271	$(821, 3343, 239)$
277	$(317, 2693, 59)$
281	$(283, 131, 71)$
283	$(89, 953, 199)$
293	$(523, 691, 11)$
307	$(137, 487, 197)$
311	$(1291, 2029, 83)$
313	$(197, 661, 31)$
317	$(1583, 59, 193)$

p	(q_1, q_2, q_3)
331	$(53, 1733, 337)$
337	$(3257, 599, 79)$
347	$(2113, 173, 197)$
349	$(53, 421, 11)$
353	$(1301, 2689, 653)$
359	$(1069, 443, 463)$
367	$(1459, 677, 269)$
373	$(647, 151, 347)$
379	$(2003, 9421, 337)$
383	$(47, 59, 71)$
389	$(167, 1423, 401)$
397	$(701, 5741, 23)$
401	$(1117, 823, 83)$
409	$(59, 157, 107)$
419	$(659, 2939, 149)$
421	$(1093, 31, 11)$
431	$(163, 2447, 251)$
433	$(811, 809, 149)$
439	$(3187, 2143, 593)$
443	$(5879, 4973, 149)$
449	$(241, 131, 293)$
457	$(79, 2393, 233)$
461	$(1531, 3691, 173)$
463	$(2753, 2999, 97)$
467	$(463, 593, 113)$
479	$(5527, 1187, 509)$
487	$(991, 3323, 179)$
491	$(89, 3347, 103)$
499	$(947, 887, 59)$

TABLE 2. Smallest triples (q_1, q_2, q_3) for primes p: $500 < p < 1000$

p	(q_1, q_2, q_3)
503	(89, 1913, 19)
509	(2729, 617, 71)
521	(701, 1069, 277)
523	(541, 3557, 151)
541	(787, 1553, 109)
547	(241, 1049, 73)
557	(2027, 271, 131)
563	(593, 929, 107)
569	(4153, 197, 487)
571	(79, 683, 71)
577	(223, 1759, 229)
587	(7457, 2099, 13)
593	(43, 1367, 439)
599	(13, 3709, 811)
601	(1697, 2459, 103)
607	(599, 7207, 211)
613	(401, 7559, 331)
617	(659, 641, 47)
619	(31, 1553, 197)
631	(457, 463, 61)
641	(751, 6577, 53)
643	(5623, 1499, 307)
647	(1879, 41, 13)
653	(9781, 2711, 19)
659	(1543, 5743, 677)

p	(q_1, q_2, q_3)
661	(149, 3469, 233)
673	(59, 127, 37)
677	(3187, 1451, 97)
683	(4603, 3307, 83)
691	(239, 947, 83)
701	(3023, 1231, 29)
709	(1217, 997, 263)
719	(73, 7213, 53)
727	(5443, 4111, 43)
733	(1367, 3581, 97)
739	(4451, 97, 349)
743	(359, 13, 37)
751	(19, 13267, 601)
757	(6421, 491, 97)
761	(523, 5281, 5)
769	(2099, 2671, 109)
773	(10369, 3511, 1061)
787	(2861, 251, 443)
797	(283, 6091, 7)
809	(1009, 5417, 1693)
811	(709, 103, 109)
821	(2677, 4957, 67)
823	(443, 8167, 13)
827	(9769, 199, 13)

p	(q_1, q_2, q_3)
829	(2017, 2129, 457)
839	(41, 1867, 5)
853	(8017, 4691, 13)
857	(919, 3461, 199)
859	(1129, 3359, 251)
863	(4493, 331, 1151)
877	(4999, 1297, 31)
881	(1213, 2693, 331)
883	(1621, 1889, 97)
887	(743, 6547, 29)
907	(997, 14767, 277)
911	(3931, 4027, 59)
919	(839, 9547, 733)
929	(4583, 9103, 29)
937	(4871, 15467, 3851)
941	(3313, 359, 1093)
947	(17669, 5641, 223)
953	(1973, 4013, 79)
967	(859, 4759, 821)
971	(1973, 1291, 557)
977	(2617, 2153, 17)
983	(3637, 947, 89)
991	(239, 3037, 173)
997	(4583, 1907, 191)

We provide some further examples and the running times of our codes.

p	(q_1, q_2, q_3)	Wall time
1009	$(5393, 4211, 593)$	5min 35s
1013	$(499, 3049, 43)$	2 min 2s
1019	$(2687, 1373, 193)$	2min 28s
1021	$(11171, 48187, 79)$	26min 18s
1031	$(983, 547, 1747)$	2min
1033	$(6131, 1789, 79)$	4min 18s
1039	$(4231, 1367, 383)$	3min 43s
1049	$(683, 3407, 17)$	2min 18s
1051	$(859, 1093, 1087)$	2min 6s
1061	$(2027, 3727, 313)$	3min 40s
1063	$(2179, 3259, 179)$	3min 18s
1069	$(1973, 211, 433)$	1min 43s
1087	$(3863, 1289, 313)$	3min 25s
1091	$(211, 6301, 311)$	3min 58s
1093	$(41, 10103, 283)$	5min 56s
1097	$(1103, 1607, 173)$	2min 1s

TABLE 3. Smallest triples (q_1, q_2, q_3) for primes $1000 < p < 1100$ and the running times

Finally, we show the running time when we test several p simultaneously. Here we look for triples (q_1, q_2, q_3) such that $\max\{q_1, q_2, q_3\} < 10^6$.

Interval	# primes	Existence of (q_1, q_2, q_3)	Wall time
$(1000, 1100)$	16	YES	1h 20min 41s
$(1100, 1200)$	11	YES	1h 6min 53s
$(1200, 1300)$	15	YES	2h 51min 41s
$(1300, 1400)$	11	YES	1h 16min 13s
$(1400, 1500)$	17	YES	3h 29min 46s
$(1500, 1600)$	12	YES	2h 45min 41s

TABLE 4. Existence of (q_1, q_2, q_3) for primes $1000 < p < 1600$ and the running times.

Conjecture 4.13. *$\mathbb{Q}(f_p)/\mathbb{Q}$ is a Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^{h_p} \rtimes S_{h_p}$ where $h_p = \deg(g_p)$ and the symmetric group S_{h_p} acts naturally as the group of permutations on $(\mathbb{Z}/2\mathbb{Z})^{h_p}$.*

Note that Conjecture 4.13 implies Conjecture 4.9. We will provide some numerical evidence for Conjecture 4.13. Since it is computationally difficult to compute the degree of $\mathbb{Q}(f_p)/\mathbb{Q}$ explicitly, we adapt a similar approach as before to show that the Galois group of $\mathbb{Q}(f_p)/\mathbb{Q}$ is $(\mathbb{Z}/2\mathbb{Z})^{h_p} \rtimes S_{h_p}$ where $2h_p = \deg(f_p)$. This approach is based on the following proposition.

Proposition 4.14. *Let $f(x)$ be a monic reciprocal polynomial with integer coefficients of even degree $2n$. Assume that there exists a quadruple of prime numbers (q_1, q_2, q_3, q_4) such that*

(1) $f(x)$ is irreducible in $\mathbb{F}_{q_1}[x]$.

(2) $f(x)$ has the following factorization in $\mathbb{F}_{q_2}[x]$

$$f(x) = (x + c_1)(x + c_2)h(x),$$

where c_1, c_2 are distinct elements in $\mathbb{F}_{q_2}$ and $h(x)$ is an irreducible polynomial of degree $2n - 2$.

(3) $f(x)$ has the following factorization in $\mathbb{F}_{q_3}[x]$

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

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

(4) $f(x)$ has the following factorization in $\mathbb{F}_{q_4}[x]$

$$f(x) = p_1(x)p_2(x),$$

where $p_1(x)$ is irreducible polynomial of degree 4 and $p_2(x)$ is a product of distinct irreducible polynomials of odd degrees.

Then the Galois group of $\mathbb{Q}(f)/\mathbb{Q}$ is $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$

Proof. The above conditions shows that the Galois group $\mathbb{Q}(f)/\mathbb{Q}$ contains an $2n$-cycle, an $(2n-2)$-cycle, a 4-cycle, and a 2-cycle. By [11, Lemma 2], the Galois group of $\mathbb{Q}(f)/\mathbb{Q}$ is $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$. □

Below we provide a table for the existence for (q_1, q_2, q_3, q_4) for $p < 600$.

TABLE 5. Quadruple (q_1, q_2, q_3, q_4)

p	(q_1, q_2, q_3, q_4)	p	(q_1, q_2, q_3, q_4)	p	(q_1, q_2, q_3, q_4)
11	(5, 23, 7, 73)	173	(503, 409, 191, 3121)	383	(47, 6217, 59, 2551)
13	(3, 19, 31, 103)	179	(421, 2069, 211, 1103)	389	(857, 16249, 1423, 3221)
17	(37, 541, 31, 367)	181	(569, 347, 727, 773)	397	(3323, 5741, 7459, 3061)
19	(5, 307, 31, 503)	191	(509, 2909, 127, 101)	401	(2729, 8269, 823, 11287)
23	(7, 97, 181, 241)	193	(13, 307, 673, 4027)	409	(2969, 4229, 157, 3559)
29	(53, 541, 19, 787)	197	(5113, 617, 149, 31)	419	(659, 8537, 3307, 7369)
31	(61, 263, 13, 821)	199	(547, 787, 8581, 499)	421	(3637, 431, 6983, 59)
37	(7, 19, 109, 53)	211	(47, 947, 311, 1439)	431	(1579, 2447, 2621, 601)
41	(107, 743, 173, 467)	223	(2333, 3449, 449, 541)	433	(811, 2347, 5087, 2311)
43	(7, 751, 1237, 23)	227	(317, 3271, 4157, 9001)	439	(3187, 2143, 1997, 4129)
47	(107, 419, 421, 409)	229	(5519, 719, 1801, 2767)	443	(5879, 4973, 10597, 7487)
53	(293, 631, 191, 41)	233	(1559, 9601, 2069, 29)	449	(241, 5419, 43, 3217)
59	(211, 1907, 53, 41)	239	(199, 809, 233, 179)	457	(10859, 13009, 47, 3229)
61	(197, 89, 487, 2161)	241	(2857, 1231, 773, 617)	461	(1531, 3691, 269, 211)
67	(257, 227, 167, 337)	251	(41, 433, 443, 277)	463	(2753, 5119, 2087, 3347)
71	(31, 97, 461, 601)	257	(1129, 5779, 919, 15233)	467	(463, 12853, 1493, 9661)
73	(827, 149, 229, 919)	263	(4463, 239, 3769, 11171)	479	(5527, 5471, 1187, 3307)
79	(691, 173, 113, 71)	269	(929, 6067, 97, 4129)	487	(991, 14051, 7477, 2837)
83	(617, 367, 541, 331)	271	(3067, 3343, 4363, 3931)	491	(461, 12721, 3347, 1867)
89	(127, 449, 151, 1129)	281	(3919, 23623, 2089, 1741)	499	(4397, 14653, 4937, 6197)
97	(53, 757, 157, 773)	283	(89, 8629, 3251, 6691)	499	(4397, 14653, 4937, 6197)
101	(1061, 1213, 149, 89)	293	(3373, 1823, 677, 883)	503	(89, 1913, 307, 19)
103	(457, 1013, 211, 4937)	307	(353, 487, 661, 557)	509	(2729, 5483, 4201, 337)
107	(797, 211, 139, 3307)	311	(1523, 8317, 1531, 2347)	521	(701, 1069, 1747, 19379)
109	(373, 467, 293, 797)	313	(197, 5849, 263, 947)	523	(541, 5113, 2657, 12893)
113	(397, 631, 1217, 1549)	317	(3769, 1499, 383, 673)	541	(4463, 1871, 367, 6761)
127	(223, 1811, 97, 53)	331	(53, 1861, 2833, 2081)	547	(241, 1861, 1049, 3967)
131	(499, 7549, 1319, 223)	337	(3257, 599, 4793, 3833)	557	(4409, 271, 977, 5519)
137	(839, 9619, 617, 2633)	347	(8081, 173, 503, 197)	563	(593, 10181, 953, 15053)
139	(839, 3607, 103, 1801)	349	(6823, 421, 3329, 2377)	569	(7673, 5839, 197, 6803)
149	(107, 827, 1823, 5827)	353	(1301, 4271, 3121, 1831)	571	(79, 1567, 1873, 2333)
151	(1249, 359, 283, 1879)	359	(1069, 9973, 443, 3881)	577	(421, 1759, 11177, 947)
157	(229, 67, 2251, 2609)	367	(1459, 677, 2113, 2399)	587	(7457, 17921, 17029, 13)
163	(1879, 13337, 991, 3163)	373	(5147, 3229, 151, 39113)	593	(43, 2767, 16193, 12689)
167	(347, 379, 109, 79)	379	(3061, 9421, 9719, 27043)	599	(1597, 3709, 7829, 23743)

Finally, we provide the running times for some larger primes p.

p	(q_1, q_2, q_3, q_4)	Wall time
601	$(9181, 4691, 499, 12409)$	15min 8s
607	$(599, 7207, 7541, 9463)$	15min 8s
613	$(401, 27901, 1109, 7853)$	24min 4s
617	$(7307, 53731, 10597, 11171)$	54min 37s
619	$(2039, 1553, 1051, 6221)$	6min 9s
631	$(57329, 463, 359, 10847)$	47min 3s

TABLE 6. Smallest triples (q_1, q_2, q_3, q_4) for primes $600 < p < 632$ and the running times

5. MODULAR PROPERTIES OF $f_p(x)$ AND $g_p(x)$

First, we study the reduction of $F_p(x)$ modulo p.

Proposition 5.1. *The reduction modulo p of $F_p(x)$ has the following factorization in $\mathbb{F}_p[x]$*

$$F_p(x) = (x-1)^{\frac{p-1}{2}} h(x),$$

where $h(x)$ is a polynomial in $\mathbb{F}_p[x]$ and $h(1) \neq 0$.

Proof. Because the degree of $F_p(x)$ is less than p, the above statement is equivalent to the following conditions (these equations are taken in $\mathbb{F}_p[x]$).

(1) For $r < \frac{p-1}{2}$, $F_p^{(r)}(1) = 0$ where $F_p^{(r)}(x)$ is the r-th derivative of $F_p(x)$.
(2) $F_p^{(\frac{p-1}{2})}(1) \neq 0$.

By definition, the r-the derivative of $F_p(x)$ is given by

$$F_p^{(r)}(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a(a-1)\dots(a-r+1)x^{a-r}.$$

For example when $r = 1$

$$F_p^{(r)}(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a x^{a-1}.$$

The leading term of $a(a-1)\cdots(a-r+1)$ is a^r. We can see that the above two conditions are equivalent to the following two conditions.

(1) For $r < \frac{p-1}{2}$

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a^r \equiv 0 \pmod{p}.$$

(2) For $r = \frac{p-1}{2}$

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a^r \not\equiv 0 \pmod{p}.$$

We can prove (1) and (2) as follows: By Euler's criterion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, for $1 \leq a \leq p-1$. By considering modulo p, one has

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a^r \equiv \sum_{a=1}^{p-1} a^{\frac{p-1}{2}+r} \equiv \begin{cases} 0 & \text{if } r < \frac{p-1}{2} \\ -1 & \text{if } r = \frac{p-1}{2}. \end{cases}$$

□

Then by Proposition 5.1, we have the following corollary.

Corollary 5.2. *$f_p(x)$ has the following factorization in $\mathbb{F}_p[x]$*

$$f_p(x) = (x-1)^{\frac{p-1}{2}-r_p} g(x),$$

where $g(1) \neq 0$.

If $p \geq 7$ then $\frac{p-1}{2} - r_p \geq 2$. Therefore, if $p \geq 7$ then $x = 1$ is a multiple root of $f_p(x)$. We have the following immediate corollary.

Corollary 5.3. *If $p \geq 7$ then $p \mid D(f_p)$ where $D(f_p)$ is the discriminant of f_p.*

In fact, the following stronger statement holds.

Corollary 5.4. *For all primes p we have*

$$v_p(D(f_p)) \geq \frac{p-3}{2} - r_p.$$

Proof. By Corollary 5.2, the degree of the greatest common divisor of the reductions of f_p and f_p' modulo p is at least $\frac{p-3}{2} - r_p$. Now the statement follows from [15, Theorem]. □

We also have the following estimation at the prime $q = 2$.

Proposition 5.5. *One has $v_2(D(f_p)) \geq \deg f_p$.*

Proof. Let $f(x) = \sum\limits_{k=0}^{p-3} a_k x^k = \dfrac{F_p(x)}{x(1-x)}$. Then by using the relation

$$(1-x)\sum_{k=0}^{p-3} a_k x^k = \sum_{a=1}^{p-2} \left(\frac{a}{p}\right) x^{a-1},$$

one has, for $k = 0, \ldots, p-3$,

$$a_k = \sum_{a=1}^{k+1} \left(\frac{a}{p}\right).$$

Thus, if k is odd then $a_k \equiv \sum_{a=1}^{k+1} 1 \equiv 0 \pmod 2$. This implies that $f'(x) \equiv 0 \pmod 2$. Suppose further that $p \equiv 1 \pmod 4$. In this case $f(x) = (1-x)(x+1)f_p(x)$. Thus

$$f'(x) = -(x+1)f_p(x) + (1-x)f_p(x) + (1-x)(1+x)f_p'(x) \equiv (x+1)^2 f_p'(x) \pmod 2$$

This implies that $f_p'(x) \equiv 0 \pmod 2$. Therefore for any prime number p, one always has $f_p'(x) \equiv 0 \pmod 2$ and hence and $f_p'(x) = 2h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Now, one has

$$D(f_p) = (\pm)R(f_p, f_p') = (\pm)R(f_p, 2h) = (\pm)2^{\deg f_p} R(f_p, h).$$

This implies that $v_2(D(f_p)) \geq \deg f_p$. □

Remark 5.6. The inequality in the above proposition could be strict. For example, for $p = 19$, $v_2(D(f_{19})) = 18 > 16 = \deg f_{19}$.

ACKNOWLEDGMENTS

The first-named author would like to thank Professor Paulo Ribenboim for many discussions concerning class numbers of algebraic number fields and properties of Bernoulli numbers. The second-named author would like to thank Professor Kazuya Kato on some helpful discussions on p-adic L-functions. He is also thankful to Professor David Harvey for his help with the numerical computations of irregular primes. The third-named author gratefully acknowledges the Vietnam Institute for Advanced Study in Mathematics (VIASM) for hospitality and support during a visit in 2021. We would like to thank Professor Arturas Dubickas for his interest in our paper and for sending us references on Proposition 4.3, which was proved earlier. We thank Professor Franz Lemmermeyer for his nice comments on our paper after we posted it on arXiv and for sending us interesting references. We also thank Professor Danny Neftin for his encouragement. We thank Professor William Duke who kindly sent to us a copy of the paper [11] which we used in Proposition 4.14. Last but not least, we would like to thank

the Editor of the Journal of Number theory for his kind encouragement and valuable suggestions about adding further numerical evidence towards our conjectures on the Galois groups of Fekete polynomials.

REFERENCES

[1] G. L. Alexanderson, The random walks of George Pólya. MAA Spectrum, Mathematical Association of America, Washington, DC, 2000, 213–215, Appendix 3, written by P. H. Lehmer.

[2] O. Ahmadi, G. Vega, On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields, Finite Fields Appl. 14 (2008), no. 1, 124–131.

[3] M. Apostol, Introduction to analytic number theory, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[4] P. T. Bateman, G. B. Purdy, S. S. Wagstaff, Some numerical results on Fekete polynomials, Mathematics of Computation 29 (1975), 7–23.

[5] B. Berndt, Classical theorems on quadratic residues, Enseign. Math. 22 (1976), 261–304.

[6] A. Cafure, E. Cesaratto, Irreducibility criteria for reciprocal polynomials and applications, Amer. Math. Monthly 124 (2017), no. 1, 37–53.

[7] L. Carlitz. Some sums connected with quadratic residues, Proc. Amer. Math. Soc. 4 (1953), 12–15.

[8] C. Christopoulos, J. McKee, Galois theory of Salem polynomials, Math. Proc. Cambridge Philos. Soc. 148 (2010), 47–54.

[9] J. Coates, A. Raghuram, A. Saikia, R. Sujatha (eds.), The Bloch-Kato conjecture for the Riemann zeta function, London Mathematical Society Lecture Note Series 418, Cambridge University Press, Cambridge, 2015.

[10] B. Conrey, A. Granville, B. Poonen, K. Soundararajan, Zeros of Fekete polynomials, Annales de l'institut Fourier 50 (2000), no. 3, 865–889.

[11] S. Davis, W. Duke, X. Sun, Probabilistic Galois theory of reciprocal polynomials, Exposition. Math. 16 (1998), 263–270.

[12] A. Dubickas, Salem numbers as Mahler measures of nonreciprocal units, Acta Arith. 176 (2016), no. 1, 81–88.

[13] C. F. Gauss, Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae, 1818; Werke II, 47–64.

[14] K. Girstmair, A popular class number formula, Amer. Math. Monthly 101 (1994), no. 10, 997–1001.

[15] D. Gomez, J. Gutierrez, A. Ibeas, D. Sevilla, Common factors of resultants modulo p, Bull. Aust. Math. Soc. 79 (2009), no. 2, 299–302.

[16] W. Hart, D. Harvey, W. Ong, Irregular primes to two billion, Math. Comp. 86 (2017), no. 308, 3031–3049.

[17] K. Iwasawa, Lectures on p-adic L-functions, Annals of Mathematics Studies 74, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972.

[18] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, Compositio Math. 81 (1992), no. 2, 223–236.

[19] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. (2) 39 (1938), no. 2, 350–360.
[20] F. Lemmermeyer, Quadratic number fields, Springer Undergraduate Mathematics Series, Springer, 2021.
[21] J. Milne, Fields and Galois theory, (2020), https://www.jmilne.org/math/CourseNotes/ft.html
[22] Ján Mináč, Tung T. Nguyen, Nguyễn Duy Tân, Further insight into mysteries of values of zeta functions at integers, preprint, available at https://arxiv.org/abs/2108.08171
[23] Ján Mináč, Tung T. Nguyen, Nguyễn Duy Tân, Github repository for the codes, https://github.com/tungprime/Fekete-polynomials-Calculations
[24] G. Pólya, George Collected papers. Vol. II: Location of zeros, edited by R. P. Boas, Mathematicians of Our Time, vol. 8, the MIT Press, Cambridge, Mass.-London, 1974, 1–26.
[25] G. Pólya, Verschiedene Bemerkung zur Zahlentheorie, Jber. deutsch Math. Verein 28 (1919), 31–40.
[26] G. Pólya and G. Szego, Problems and theorems in analysis, v. 2: Theory of functions, zeros, polynomials, determinants, number theory, geometry, revised and enlarged translation of the 4th German edition, Grundlehren Math. Wiss 216.
[27] G. Shimura, Elementary Dirichlet series and modular forms, Springer Monographs in Mathematics. Springer, New York, 2007.
[28] G. Shimura, The critical values of generalizations of the Hurwitz zeta function, Doc. Math. 15 (2010), 489-–506.
[29] C. Weibel, An introduction to algebraic *K*-theory, Graduate Studies in Mathematics 145, American Mathematical Society, Providence, RI, 2013.

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
Email address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF CHICAGO, CHICAGO, ILLINOIS, USA.
Email address: tungnt@uchicago.edu

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