WIEFERICH PRIMES AND MONOGENIC TRINOMIALS

LENNY JONES

Abstract. A prime p is called a *Wieferich prime* if $2^{p-1} \equiv 1 \pmod{p^2}$. A monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree N is called *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{N-1}\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. In this article, we show that $\mathcal{F}_p(x) := x^{2p} + 2x^p + 2$ is monogenic if and only if p is not a Wieferich prime.

1. Introduction

We say that a prime p is a *Wieferich prime* if $2^{p-1} \equiv 1 \pmod{p^2}$. Currently, the only known Wieferich primes are $p = 1093$ and $p = 3511$.

We say that a monic polynomial $f(x) \in \mathbb{Z}[x]$ is *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{\deg(f)-1}\}$ is a basis for the ring of integers, $\mathbb{Z}_K$, of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. It is well known [1] that

$$\Delta(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \, \Delta(K), \tag{1.1}$$

where $\Delta(f)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $f(x)$ and the number field K. We refer to $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ as the *index* of $f(x)$, and we denote it $\text{index}(f)$. Thus, from (1.1),

$$f(x) \text{ is monogenic if and only if } \Delta(f) = \Delta(K), \text{ or equivalently, } \mathbb{Z}_K = \mathbb{Z}[\theta]. \tag{1.2}$$

In this article, we prove the following theorem:

Theorem 1.1. *Let $p \geq 3$ be a prime, and let*

$$\mathcal{F}_p(x) := x^{2p} + 2x^p + 2.$$

Then $\mathcal{F}_p(x)$ is monogenic if and only if p is not a Wieferich prime.

While analogous theorems exist for k-Wall-Sun-Sun primes [5] (aka Fibonacci-Wieferich primes when $k = 1$) and generalized Wall-Sun-Sun primes [2, 4], these previous results do not pertain to the situation in Theorem 1.1.

Remark 1.2. We point out that Theorem 1.1 is also valid when $p = 2$ since 2 is not a Wieferich prime and it is easy to verify that $x^4 + 2x^2 + 2$ is monogenic.

2. Preliminaries

Throughout this article, we assume that p is an odd prime and that

$$\mathcal{F}_p(x) := x^{2p} + 2x^p + 2. \tag{2.1}$$

Date: May 14, 2026.
2020 *Mathematics Subject Classification.* Primary 11A07, 11R09; Secondary 11A41, 11R04.
Key words and phrases. Wieferich prime, monogenic, trinomial.

Note that $\mathcal{F}_p(x)$ is irreducible over $\mathbb{Q}$ since it is 2-Eisenstein. From a theorem due to Swan [6], we have

$$\Delta(\mathcal{F}_p) = -2^{3p-1}p^{2p}. \tag{2.2}$$

Thus, we see from (1.1) and (1.2) that

$$\mathcal{F}_p(x) \text{ is monogenic if and only if } \gcd(2p, \operatorname{index}(\mathcal{F}_p)) = 1. \tag{2.3}$$

One method that can be used, for any monic irreducible polynomial, to determine explicit conditions (more so than (2.3)) on the prime divisors of the polynomial discriminant to guarantee monogenicity is known as Dedekind's Index Criterion [1]. However, another more-algorithmic method exists that is derived from Dedekind's theorem and designed explicitly for trinomials. This streamlined version of Dedekind's theorem is due to Jakhar, Khanduja and Sangwan [3, Theorem 1.1], and requires that only one out of a list of five conditions be checked for each prime divisor p of the discriminant of the trinomial to determine whether p divides the index of the trinomial. Moreover, a careful analysis of [3, Theorem 1.1] reveals that we only need to apply the fourth condition of that theorem in our situation, which yields the following very succinct result.

Theorem 2.1. *The trinomial $\mathcal{F}_p(x)$ is monogenic if and only if the polynomials*

$$H_1(x) := x^2 + 2x + 2 \quad \text{and} \quad H_2(x) := \frac{2x^p + 2 - (2x+2)^p}{p}$$

are coprime in $\mathbb{F}_p[x]$.

Since

$$\begin{aligned} H_2(x) &= \frac{2x^p + 2 - 2^p(x+1)^p}{p} \\ &= \left(\frac{2-2^p}{p}\right)x^p + \frac{2-2^p}{p} - 2^p \sum_{j=1}^{p-1} \frac{\binom{p}{j}}{p} x^j, \end{aligned} \tag{2.4}$$

we see indeed that $H_2(x) \in \mathbb{Z}[x]$, by Fermat's Little Theorem and the fact that $\binom{p}{j} \equiv 0 \pmod{p}$ for all j with $1 \le j \le p-1$,

3. The Proof of Theorem 1.1

Proof. From Theorem 2.1, we must determine exactly when $H_1(x)$ and $H_2(x)$ are coprime in $\mathbb{F}_p[x]$. Observe from (2.4) that

$$\deg(H_2) \ge p - 1 \ge 2 = \deg(H_1).$$

in $\mathbb{F}_p[x]$. Thus, our general strategy is to determine the conditions under which $pH_2(\theta) \equiv 0 \pmod{p^2}$ for the zeros θ of $H_1(x)$, which will tell us precisely when $H_1(x)$ and $H_2(x)$ are not coprime in $\mathbb{F}_p[x]$, and consequently, not monogenic by Theorem 2.1. We split the proof into the two cases $p \equiv \pm 1 \pmod 4$.

Suppose first that $p \equiv 3 \pmod 4$. Then $H_1(x)$ is irreducible in $\mathbb{F}_p[x]$ since -1 is not a square in $\mathbb{F}_p$. Hence, if $H_1(x)$ and $H_2(x)$ are not coprime in $\mathbb{F}_p[x]$, it must be that $H_1(x)$ is an irreducible factor of $H_2(x)$, so that every zero of $H_1(x)$ is a zero of $H_2(x)$. Therefore, it is enough to examine $pH_2(\theta)$ modulo p^2 for any zero θ of $H_1(x)$. Observe that $\alpha := -1 + i$ is a zero of $H_1(x)$, where $i \notin \mathbb{F}_p$ with $i^2 = -1$. Thus, to establish the theorem in this case, we show that

$$pH_2(\alpha) \equiv 0 \pmod{p^2} \quad \text{if and only if} \quad 2^{p-1} \equiv 1 \pmod{p^2}. \tag{3.1}$$

Since $(\alpha+1)^p = i^p = -i$, we have from the definition of $H_2(x)$, that

$$pH_2(\alpha) = 2\alpha^p + 2 - 2^p(\alpha+1)^p = 2\alpha^p + 2 + 2^p i. \tag{3.2}$$

A straightforward induction argument shows that

$$\alpha^j = (-1)^{\frac{j-3}{4}} 2^{\frac{j-1}{2}}(1+i) \quad \text{if } j \equiv 3 \pmod 4.$$

Thus,

$$\alpha^p = (-1)^{\frac{p-3}{4}} 2^{\frac{p-1}{2}}(1+i),$$

which yields the following rearrangement of $pH_2(\alpha)$ from (3.2):

$$\begin{aligned} pH_2(\alpha) &= 2\left((-1)^{\frac{p-3}{4}} 2^{\frac{p-1}{2}}(1+i)\right) + 2 + 2^p i \\ &= 2 + (-1)^{\frac{p-3}{4}} 2^{\frac{p+1}{2}} + \left(2^p + (-1)^{\frac{p-3}{4}} 2^{\frac{p+1}{2}}\right) i. \end{aligned} \tag{3.3}$$

Consequently, from (3.3), it follows that $pH_2(\alpha) \equiv 0 \pmod{p^2}$ if and only if

$$2 + (-1)^{\frac{p-3}{4}} 2^{\frac{p+1}{2}} \equiv 0 \pmod{p^2} \quad \text{and} \quad 2^p + (-1)^{\frac{p-3}{4}} 2^{\frac{p+1}{2}} \equiv 0 \pmod{p^2}. \tag{3.4}$$

To prove (3.1), suppose first that $pH_2(\alpha) \equiv 0 \pmod{p^2}$. From the first congruence in (3.4) we see that

$$(-1)^{\frac{p-3}{4}} 2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}. \tag{3.5}$$

Squaring both sides of (3.5) yields $2^{p-1} \equiv 1 \pmod{p^2}$.

Conversely, suppose that $2^{p-1} \equiv 1 \pmod{p^2}$. Then

$$2^{p-1} - 1 \equiv (2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p^2}. \tag{3.6}$$

From (3.6) we conclude that

$$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p^2},$$

since p divides one and only one of the factors in the factorization (3.6). We claim that

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \pmod{p^2}. \tag{3.7}$$

Suppose first that $2^{\frac{p-1}{2}} \equiv 1 \pmod{p^2}$, so that $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. By Euler's criterion and the quadratic character of 2, we have that

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Since $p \equiv 3 \pmod 4$, it follows that $p \equiv 7 \pmod 8$ and thus,

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p+1}{4}} = 1.$$

Similarly, if $2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}$, then $p \equiv 3 \pmod 8$, so that

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p+1}{4}} = -1.$$

Therefore, the claim (3.7) is estabished. Therefore, since $2^p \equiv 2 \pmod{p^2}$ and $p \equiv 3 \pmod 4$, we have from (3.3) and (3.7) that

$$\begin{aligned} pH_2(\alpha) &\equiv 2\left(1+(-1)^{\frac{p-3}{4}}2^{\frac{p-1}{2}}\right)(1+i) \\ &\equiv 2\left(1+(-1)^{\frac{p-3}{4}}(-1)^{\frac{p+1}{4}}\right)(1+i) \\ &\equiv 2\left(1+(-1)^{\frac{p-1}{2}}\right)(1+i) \\ &\equiv 0 \pmod{p^2}, \end{aligned}$$

which finishes the proof of (3.1), and completes the proof of the theorem when $p \equiv 3 \pmod 4$.

Suppose next that $p \equiv 1 \pmod 4$. Then $H_1(x)$ is reducible in $\mathbb{F}_p[x]$ since -1 is a square in $\mathbb{F}_p$. Let $\alpha = -1+i \in \mathbb{F}_p$ be a zero of $H_2(x)$, where i and α are such that $1 \le \alpha \le p-3$ and $2 \le i \le p-2$ with $i^2 \equiv -1 \pmod p$. Then, $\beta = p-1-i \in \mathbb{F}_p[x]$ is the other zero of $H_1(x)$, where $1 \le \beta \le p-3$. The strategy here, as in the previous case, is to determine conditions under which $pH_2(\theta) \equiv 0 \pmod{p^2}$, where $\theta \in \{\alpha, \beta\}$. It is conceivable that exactly one of the two zeros θ, and not the other, could satisfy the congruence $pH_2(\theta) \equiv 0 \pmod{p^2}$. However, it turns out that

$$pH_2(\alpha) \equiv 0 \pmod{p^2} \quad \text{if and only if} \quad pH_2(\beta) \equiv 0 \pmod{p^2}, \tag{3.8}$$

which shows that considering the single zero α will suffice. We postpone the proof of (3.8) to focus first on α, and show that

$$pH_2(\alpha) \equiv 0 \pmod{p^2} \quad \text{if and only if} \quad 2^{p-1} \equiv 1 \pmod{p^2}. \tag{3.9}$$

Since $H_1(\alpha) \equiv 0 \pmod p$, we see that $\alpha^2 \equiv -2(\alpha+1) \pmod p$, which implies

$$\alpha^{2p} \equiv -2^p(\alpha+1)^p \equiv -2^p i^p \pmod{p^2}. \tag{3.10}$$

Therefore, from the definition of $H_2(x)$, (2.1) and (3.10), it follows that

$$\begin{aligned} pH_2(\alpha) &= 2\alpha^p + 2 - 2^p(\alpha+1)^p \\ &= 2\alpha^p + 2 - 2^p i^p \\ &\equiv 2\alpha^p + 2 + \alpha^{2p} \pmod{p^2} \\ &\equiv \mathcal{F}_p(\alpha) \pmod{p^2}. \end{aligned} \tag{3.11}$$

To prove (3.9), suppose that $pH_2(\alpha) \equiv 0 \pmod{p^2}$. Then $\mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}$ from (3.11), and hence

$$\alpha^p \equiv -\frac{\alpha^{2p}+2}{2} \pmod{p^2}. \tag{3.12}$$

Squaring both sides of (3.12) yields

$$\alpha^{2p} \equiv \frac{(\alpha^{2p}+2)^2}{4} \pmod{p^2}. \tag{3.13}$$

Thus, from (3.10) and (3.13), we have

$$-2^{p+2}i^p \equiv 2^{2p}i^{2p} - 2^{p+2}i^p + 4 \pmod{p^2},$$

or equivalently,

$$2^{2p}i^{2p} + 4 \equiv 0 \pmod{p^2}. \tag{3.14}$$

Since $i^2 \equiv -1 \pmod{p}$, we have

$$i^{2p} \equiv (-1)^p \equiv -1 \pmod{p^2}. \tag{3.15}$$

Consequently, from (3.14) and (3.15), we deduce that

$$(2^p - 2)(2^p + 2) \equiv 0 \pmod{p^2}. \tag{3.16}$$

Since $2^p \equiv 2 \pmod{p}$, we have that $2^p + 2 \not\equiv 0 \pmod{p}$ since $p \geq 3$. Thus, it follows from (3.16) that $2^p - 2 \equiv 0 \pmod{p^2}$ and, therefore, $2^{p-1} \equiv 1 \pmod{p^2}$.

Conversely, if $2^{p-1} \equiv 1 \pmod{p^2}$, then $2^p - 2 \equiv 0 \pmod{p^2}$, and the steps of the proof in the other direction can be reversed from (3.16) back to (3.13) to give us

$$\left(\alpha^{2p} + 2 - 2\alpha^p\right)\left(\alpha^{2p} + 2 + 2\alpha^p\right) \equiv 0 \pmod{p^2}. \tag{3.17}$$

Suppose that

$$\alpha^{2p} + 2 - 2\alpha^p \equiv \left(\alpha^2 + 2 - 2\alpha\right)^p \equiv 0 \pmod{p}.$$

Then, since $H_1(\alpha) = \alpha^2 + 2\alpha + 2 \equiv 0 \pmod{p}$, we arrive at the contradiction

$$H_1(\alpha) - \left(\alpha^2 + 2 - 2\alpha\right) = 4\alpha \equiv 0 \pmod{p}.$$

Therefore, we conclude from (3.17) and (3.11) that

$$pH_2(\alpha) \equiv \mathcal{F}_p(\alpha) \equiv \alpha^{2p} + 2 + 2\alpha^p \equiv 0 \pmod{p^2},$$

which completes the proof in this direction for the zero α.

To show that we do not need to consider the zero β, we now provide a proof of (3.8). Since $\alpha\beta \equiv 2 \pmod{p}$, it follows that

$$\alpha^p \beta^p \equiv 2^p \pmod{p^2}. \tag{3.18}$$

Since $H_1(\beta) \equiv 0 \pmod{p}$, we see that $\beta^2 \equiv -2(\beta + 1) \pmod{p}$, which implies

$$\beta^{2p} \equiv -2^p(\beta + 1)^p \equiv -2^p(p - i)^p \equiv 2^p i^p \pmod{p^2}. \tag{3.19}$$

Therefore, from the definition of $H_2(x)$, (2.1) and (3.19), it follows that

$$\begin{aligned} pH_2(\beta) &= 2\beta^p + 2 - 2^p(\beta + 1)^p \\ &= 2\beta^p + 2 - 2^p(p - i)^p \\ &= 2\beta^p + 2 + 2^p i^p \pmod{p^2} \\ &\equiv 2\beta^p + 2 + \beta^{2p} \pmod{p^2} \\ &\equiv \mathcal{F}_p(\beta) \pmod{p^2}. \end{aligned} \tag{3.20}$$

To establish (3.8), suppose that $pH_2(\alpha) \equiv 0 \pmod{p^2}$. Then $\mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}$ from (3.11), and therefore, $2^p \equiv 2 \pmod{p^2}$ from the argument following (3.16).

Hence, from (3.18), it follows that

$$\begin{aligned}\mathcal{F}_p(\beta) &= \beta^{2p} + 2\beta^p + 2 \\ &\equiv \left(\frac{2^p}{\alpha^p}\right)^2 + 2\left(\frac{2^p}{\alpha^p}\right) + 2 \pmod{p^2} \\ &\equiv \frac{2\left(\alpha^{2p} + 2\alpha^p + 2\right)}{\alpha^{2p}} \pmod{p^2} \\ &\equiv \frac{2\mathcal{F}_p(\alpha)}{\alpha^{2p}} \pmod{p^2} \\ &\equiv 0 \pmod{p^2}.\end{aligned}$$

Thus, $pH_2(\beta) \equiv 0 \pmod{p^2}$ from (3.20). The converse is similar and we omit the details. □

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 2000.

[2] J. Harrington and L. Jones, *A note on generalised Wall-Sun-Sun primes*, Bull. Aust. Math. Soc. **108**, No. 3, 373–378 (2023).

[3] A. Jakhar, S. Khanduja and N. Sangwan, *Characterization of primes dividing the index of a trinomial*, Int. J. Number Theory **13** (2017), no. 10, 2505–2514.

[4] L. Jones, *Generalized Wall-Sun-Sun primes and monogenic power compositional trinomials*, Albanian J. Math. **17**, No. 2, 3–17 (2023).

[5] L. Jones, *A new condition for k-Wall-Sun-Sun primes*, Taiwanese J. Math. **28**, No. 1, 17–28 (2024).

[6] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

Professor Emeritus, Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania 17257, USA

Email address, Lenny Jones: doctorlennyjones@gmail.com