ALBANIAN JOURNAL OF MATHEMATICS
Volume 17, Number 2, Pages 3–17
ISSN: 1930-1235; (**2023**)

GENERALIZED WALL-SUN-SUN PRIMES AND MONOGENIC POWER-COMPOSITIONAL TRINOMIALS

LENNY JONES

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

Abstract. For positive integers a and b, we let $[U_n]$ be the Lucas sequence of the first kind defined by

$$U_0 = 0, \quad U_1 = 1 \quad \text{and} \quad U_n = aU_{n-1} + bU_{n-2} \quad \text{for } n \geq 2,$$

and let $\pi(m) := \pi_{(a,b)}(m)$ be the period length of $[U_n]$ modulo the integer $m \geq 2$, where $\gcd(b, m) = 1$. We define an (a, b)-*Wall-Sun-Sun prime* to be a prime p such that $\pi(p^2) = \pi(p)$. When $(a, b) = (1, 1)$, such a prime p is referred to simply as a *Wall-Sun-Sun prime*.

We say that a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree N is *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 $f(\theta) = 0$.

Let $f(x) = x^2 - ax - b$, and let s be a positive integer. Then, with certain restrictions on a, b and s, we prove that the monogenicity of

$$f(x^{s^n}) = x^{2s^n} - ax^{s^n} - b$$

is independent of the positive integer n and is determined solely by whether s has a prime divisor that is an (a, b)-Wall-Sun-Sun prime. This result improves and extends previous work of the author in the special case $b = 1$.

MSC 2020: Primary 11R04, 11B39, Secondary 11R09, 12F05
Keywords: Wall-Sun-Sun prime, monogenic, power-compositional

E-mail address: doctorlennyjones@gmail.com.

1. Introduction

Throughout this article, we let $(*)$ denote the set of conditions:

$$(*)\begin{cases} a \text{ and } b \text{ are positive integers} \\ a \not\equiv 0 \pmod 4 \\ b \text{ is squarefree} \\ \mathcal{D} \text{ is squarefree,} \end{cases}$$

where

$$\mathcal{D} := \begin{cases} a^2+4b & \text{if } a \equiv 1 \pmod 2 \\ (a/2)^2+b & \text{if } a \equiv 0 \pmod 2. \end{cases}$$

We also let $[U_n]$ be the Lucas sequence of the first kind defined by

$$U_0 = 0, \quad U_1 = 1 \quad \text{and} \quad U_n = aU_{n-1} + bU_{n-2} \quad \text{for } n \geq 2. \tag{1.1}$$

The sequence $[U_n]$ is well known to be periodic modulo any integer $m \geq 2$, where $\gcd(b,m) = 1$, and we let $\pi(m) := \pi_{(a,b)}(m)$ denote the length of the period of $[U_n]$ modulo m.

Definition 1.1. An (a,b)-*Wall-Sun-Sun prime* is a prime p with $\gcd(b,p) = 1$, such that

$$\pi(p^2) = \pi(p). \tag{1.2}$$

We provide some examples of (a,b)-Wall-Sun-Sun primes in Table 1.

(a,b)	$\{[p,\pi(p^2)]\}$
$(2,1)$	$\{[13,28],[31,30]\}$
$(3,26)$	$\{[71,126]\}$
$(10,41)$	$\{[29,120]\}$
$(11,43)$	$\{[2,3],[5,24]\}$
$(15,14)$	$\{[29,28]\}$
$(23,11)$	$\{[2,3],[3,3],[71,35]\}$
$(25,7)$	$\{[5,8]\}$
$(27,22)$	$\{[13,84]\}$

Table 1. (a,b)-Wall-Sun-Sun primes p and the corresponding period length $\pi(p^2) = \pi(p)$

When $(a,b) = (1,1)$, the sequence $[U_n]$ is the well-known Fibonacci sequence, and the (a,b)-Wall-Sun-Sun primes in this case are known simply as *Wall-Sun-Sun* primes [4, 20]. However, at the time this article was written, no Wall-Sun-Sun primes were known to exist. The existence of Wall-Sun-Sun primes was first investigated by D. D. Wall [17] in 1960, and subsequently studied by the Sun brothers [15], who showed that the first case of Fermat's Last Theorem is false for exponent p only if p is a Wall-Sun-Sun prime.

When $b = 1$, primes satisfying (1.2) are also known simply as a-Wall-Sun-Sun primes [19, 20]. We point out that the definition of an a-Wall-Sun-Sun prime given in [19, 20] is a prime p such that

$$U_{\pi(p)} \equiv 0 \pmod{p^2}. \tag{1.3}$$

In the more general situation of (a,b)-Wall-Sun-Sun primes, it is easily seen that condition (1.2) implies condition (1.3). Although it can be shown that the converse is true when $b=1$ [5], the converse is false in general, as can be seen by the counterexample $(a,b)=(5,2)$ with $p=7$. In this particular example, we have $\pi(7)=48$ and $U_{48}\equiv 0 \pmod{49}$, but $\pi(49)=7\pi(7)=336$. Since Wall was originally concerned with whether there exist any primes p such that (1.2) holds in the case of $(a,b)=(1,1)$, we have chosen to use condition (1.2), instead of condition (1.3), for our definition of the more general (a,b)-Wall-Sun-Sun prime.

Let $\Delta(f)$ and $\Delta(K)$ denote, respectively, the discriminants over $\mathbb{Q}$ of $f(x)\in\mathbb{Z}[x]$ and a number field K. We define $f(x)\in\mathbb{Z}[x]$ to be *monogenic* if $f(x)$ is monic, irreducible over $\mathbb{Q}$ and

$$\Theta=\{1,\theta,\theta^2,\ldots,\theta^{\deg(f)-1}\}$$

is a basis for the ring of integers $\mathbb{Z}_K$ of $K=\mathbb{Q}(\theta)$, where $f(\theta)=0$. If Θ fails to be a basis for $\mathbb{Z}_K$, we say that $f(x)$ is *non-monogenic*. If $f(x)$ is irreducible over $\mathbb{Q}$ with $f(\theta)=0$, then [3]

$$\Delta(f)=\left[\mathbb{Z}_K:\mathbb{Z}[\theta]\right]^2\Delta(K). \tag{1.4}$$

Observe then, from (1.4), that $f(x)$ is monogenic if and only if $\Delta(f)=\Delta(K)$. Thus, if $\Delta(f)$ is squarefree, then $f(x)$ is monogenic from (1.4). However, the converse does not hold in general, and when $\Delta(f)$ is not squarefree, it can be quite difficult to determine whether $f(x)$ is monogenic.

In this article, we establish a connection between (a,b)-Wall-Sun-Sun primes and the monogenicity of certain power-compositional trinomials. More precisely, we prove

Theorem 1.2. *Let $f(x)=x^2-ax-b\in\mathbb{Z}[x]$, where a and b satisfy $(*)$. Let $s\geq 1$ be an integer such that $\gcd(b,s)=1$, $\delta_p\neq 1$ for each prime divisor $p\geq 3$ of s and $\delta_3=-1$ if $3\mid s$, where δ_p is the Legendre symbol $\left(\frac{\mathcal{D}}{p}\right)$. For any integer $n\geq 1$, define $\mathcal{F}_n(x):=f(x^{s^n})$. Then $\mathcal{F}_n(x)$ is monogenic if and only if no prime divisor of s is an (a,b)-Wall-Sun-Sun prime.*

Theorem 1.2 improves and extends previous work of the author on the special case of $b=1$ [9], which was, in part, originally motivated by recent results of Bouazzaoui [1,2]. Bouazzaoui showed, under certain conditions on the prime $p\geq 3$, that

$$\mathbb{Q}(\sqrt{d})\quad \text{is } p\text{-rational if and only if}\quad \pi_{(a,b)}(p^2)\neq\pi_{(a,b)}(p),$$

where $d>0$ is a fundamental discriminant [18], $a=\varepsilon+\overline{\varepsilon}$ and $b=-\mathcal{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\varepsilon)$, with ε equal to the fundamental unit of $\mathbb{Q}(\sqrt{d})$. We recall, for a prime $p\geq 3$, that a number field K is said to be *p-rational* if the Galois group of the maximal pro-p-extension of K which is unramified outside p is a free pro-p-group of rank r_2+1, where r_2 is the number of pairs of complex embeddings of K.

2. Preliminaries

The formula for the discriminant of an arbitrary monic trinomial, due to Swan [16], is given in the following theorem.

Theorem 2.1. *Let $f(x)=x^N+Ax^M+B\in\mathbb{Z}[x]$, where $0<M<N$. Let $r=\gcd(N,M)$, $N_1=N/r$ and $M_1=M/r$. Then*

$$\Delta(f)=(-1)^{N(N-1)/2}B^{M-1}D^r,$$

where

$$D := N^{N_1}B^{N_1-M_1} - (-1)^{N_1}M^{M_1}(N-M)^{N_1-M_1}A^{N_1}. \tag{2.1}$$

The next two theorems are due to Capelli [14].

Theorem 2.2. *Let $f(x)$ and $h(x)$ be polynomials in $\mathbb{Q}[x]$ with $f(x)$ irreducible. Suppose that $f(\alpha) = 0$. Then $f(h(x))$ is reducible over $\mathbb{Q}$ if and only if $h(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$.*

Theorem 2.3. *Let $c \in \mathbb{Z}$ with $c \geq 2$, and let $\alpha \in \mathbb{C}$ be algebraic. Then $x^c - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either there is a prime p dividing c such that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ or $4 \mid c$ and $\alpha = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$.*

The next proposition follows from Proposition 1 in [21].

Proposition 2.4. *Let $b = 1$. Then $\alpha = (a + \sqrt{a^2+4})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{\mathcal{D}})$ with $\mathcal{N}(\alpha) = -1$, where $\mathcal{N} := \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}$ denotes the algebraic norm.*

In the sequel, for an integer $m \geq 2$, we let $\mathrm{ord}_m(*)$ denote the order of $*$ modulo m, and we define $(a,b)_m := (a \pmod m, b \pmod m)$. For brevity of notation, we also define

$$\lambda := \mathrm{ord}_p(b^2) \quad \text{and} \quad \delta_p := \left(\frac{\mathcal{D}}{p}\right),$$

where $\left(\frac{\mathcal{D}}{p}\right)$ is the Legendre symbol.

The following theorem is a compilation of results from various sources.

Theorem 2.5. *Let $[U_n]$ be the Lucas sequence as defined in (1.1). Let p be a prime with $b \not\equiv 0 \pmod p$.*

(1) $\pi(p) = 2$ *if and only if* $(a,b)_p = (0,1)$.
(2) *If* $p = 2$, *then*

$$\pi(2) = \begin{cases} 2 & \text{if } (a,b)_4 \in \{(2,1),(2,3)\} \\ 3 & \text{if } (a,b)_4 \in \{(1,1),(1,3),(3,1),(3,3)\} \end{cases}$$

$$\text{and} \quad \pi(4) = \begin{cases} 3 & \text{if } (a,b)_4 = (3,3) \\ 4 & \text{if } (a,b)_4 \in \{(2,1),(2,3)\} \\ 6 & \text{if } (a,b)_4 \in \{(1,1),(1,3),(3,1)\}. \end{cases}$$

(3) *If* $p \geq 3$, *then* $\pi(p^2) \in \{\pi(p), p\pi(p)\}$.
(4) *If* $\delta_p = -1$, *then* $2(p+1)\lambda \equiv 0 \pmod{\pi(p)}$.

Proof. Item (1) is obvious. Item (2) follows easily by direct calculation, recalling that $a \not\equiv 0 \pmod 4$ from conditions $(*)$. Item (3) can be found in [12], while item (4) follows from a theorem in [6]. □

The following theorem, known as *Dedekind's Index Criterion*, or simply *Dedekind's Criterion* if the context is clear, is a standard tool used in determining the monogenicity of a polynomial.

Theorem 2.6 (Dedekind [3])**.** *Let $K = \mathbb{Q}(\theta)$ be a number field, $T(x) \in \mathbb{Z}[x]$ the monic minimal polynomial of θ, and $\mathbb{Z}_K$ the ring of integers of K. Let p be a prime number and let $\overline{*}$ denote reduction of $*$ modulo p (in $\mathbb{Z}$, $\mathbb{Z}[x]$ or $\mathbb{Z}[\theta]$). Let*

$$\overline{T}(x) = \prod_i \overline{\tau_i}(x)^{e_i}$$

be the factorization of $T(x)$ modulo p in $\mathbb{F}_p[x]$, and set

$$g(x) = \prod_i \tau_i(x),$$

where the $\tau_i(x) \in \mathbb{Z}[x]$ are arbitrary monic lifts of the $\overline{\tau_i}(x)$. Let $h(x) \in \mathbb{Z}[x]$ be a monic lift of $\overline{T}(x)/\overline{g}(x)$ and set

$$F(x) = \frac{g(x)h(x) - T(x)}{p} \in \mathbb{Z}[x].$$

Then

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod p \Longleftrightarrow \gcd\left(\overline{F}, \overline{g}, \overline{h}\right) = 1 \text{ in } \mathbb{F}_p[x].$$

The next result is essentially an algorithmic adaptation of Theorem 2.6 specifically for trinomials.

Theorem 2.7. [8] *Let $N \geq 2$ be an integer. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in \mathbb{Z}_K$, the ring of integers of K, having minimal polynomial $f(x) = x^N + Ax^M + B$ over $\mathbb{Q}$, with $\gcd(M, N) = r$, $N_1 = N/r$ and $M_1 = M/r$. Let D be as defined in (2.1). A prime factor p of $\Delta(f)$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if p satisfies one of the following items:*

(1) *when $p \mid A$ and $p \mid B$, then $p^2 \nmid B$;*
(2) *when $p \mid A$ and $p \nmid B$, then*

$$\text{either} \quad p \mid A_2 \text{ and } p \nmid B_1 \quad \text{or} \quad p \nmid A_2\left((-B)^{M_1} A_2^{N_1} - (-B_1)^{N_1}\right),$$

where $A_2 = A/p$ and $B_1 = \frac{B+(-B)^{p^e}}{p}$ with $p^e \parallel N$;
(3) *when $p \nmid A$ and $p \mid B$, then*

$$\text{either} \quad p \mid A_1 \text{ and } p \nmid B_2 \quad \text{or} \quad p \nmid A_1 B_2^{M-1}\left((-A)^{M_1} A_1^{N_1 - M_1} - (-B_2)^{N_1 - M_1}\right),$$

where $A_1 = \frac{A+(-A)^{p^j}}{p}$ with $p^j \parallel (N - M)$, and $B_2 = B/p$;
(4) *when $p \nmid AB$ and $p \mid M$ with $N = up^m$, $M = vp^m$, $p \nmid \gcd(u, v)$, then the polynomials*

$$G(x) := x^{N/p^m} + Ax^{M/p^m} + B \quad \text{and}$$
$$H(x) := \frac{Ax^M + B + \left(-Ax^{M/p^m} - B\right)^{p^m}}{p}$$

are coprime modulo p;
(5) *when $p \nmid ABM$, then $p^2 \nmid D/r^{N_1}$.*

Remark 2.8. We will find both Theorem 2.6 and Theorem 2.7 useful in our investigations.

The next theorem follows from Corollary (2.10) in [11].

Theorem 2.9. *Let K and L be number fields with $K \subset L$. Then*

$$\Delta(K)^{[L:K]} \bigm| \Delta(L).$$

3. The Proof of Theorem 1.2

Throughout this section we let

$$f(x) = x^2 - ax - b \in \mathbb{Z}[x] \quad \text{and} \quad \alpha = \frac{a + \sqrt{a^2 + 4b}}{2},$$

where a and b satisfy $(*)$. We first prove some lemmas.

Lemma 3.1. *Let s be a positive integer. Then $f(x^{s^n})$ is irreducible over $\mathbb{Q}$ for all integers $n \geq 1$.*

Proof. Since $\mathcal{D} > 1$ is squarefree, it follows that $f(x)$ is irreducible over $\mathbb{Q}$, and the trivial case of $s = 1$ is true. So, suppose then that $s \geq 2$. Note that $f(\alpha) = 0$. Let $h(x) = x^{s^n}$ and assume, by way of contradiction, that $f(h(x))$ is reducible. Then, by Theorems 2.2 and 2.3, we have, for some $\beta \in \mathbb{Q}(\alpha)$, that either $\alpha = \beta^p$ for some prime p dividing s, or $\alpha = -4\beta^4$ if $s^n \equiv 0 \pmod 4$.

If $b \geq 2$, then, in either case, we arrive at a contradiction by taking norms, since $\mathcal{N}(\alpha) = -b$ is squarefree but neither $\mathcal{N}(\beta^p) = \mathcal{N}(\beta)^p$ nor $\mathcal{N}(-4\beta^4) = 16\mathcal{N}(\beta)^4$ is squarefree. Suppose then that $b = 1$. If $\alpha = -4\beta^4$, then

$$-1 = \mathcal{N}(\alpha) = \mathcal{N}(-4\beta^4) \equiv 0 \pmod{16},$$

which is impossible. Hence, $\alpha = \beta^p$ for some prime divisor p of s. Then, we see by taking norms that

$$\mathcal{N}(\beta)^p = \mathcal{N}(\alpha) = -1,$$

which implies that $p \geq 3$ and $\mathcal{N}(\beta) = -1$, since $\mathcal{N}(\beta) \in \mathbb{Z}$. Thus, β is a unit, and therefore $\beta = \pm\alpha^j$ for some $j \in \mathbb{Z}$, since α is the fundamental unit of $\mathbb{Q}(\sqrt{\mathcal{D}})$ by Proposition 2.4. Consequently,

$$\alpha = \beta^p = (\pm 1)^p \alpha^{jp},$$

which implies that $(\pm 1)^p \alpha^{jp-1} = 1$, contradicting the fact that α has infinite order in the group of units of the ring of algebraic integers in the real quadratic field $\mathbb{Q}(\sqrt{\mathcal{D}})$. □

Remark 3.2. Although here we are assuming that conditions $(*)$ hold, so that $a \not\equiv 0 \pmod 4$, the argument given in the proof of Lemma 3.1 for the case of $b = 1$ is still valid when $a \equiv 0 \pmod 4$ with the single exception of $a = 4$ [21] since, in that case, $\alpha = 2 + \sqrt{5}$ is not the fundamental unit of $\mathbb{Q}(\sqrt{5})$. However, since $\varepsilon = (1+\sqrt{5})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{5})$, and $\alpha = \varepsilon^3$, Theorem 2.2 and Theorem 2.3 can be used to determine exactly when $f(x^{s^n}) = x^{2s^n} - 4x^{s^n} - 1$ is reducible and how $f(x^{s^n})$ factors.

Lemma 3.3. *The polynomial $f(x)$ is monogenic.*

Proof. By Lemma 3.1, $f(x)$ is irreducible over $\mathbb{Q}$. Let p be a prime divisor of $\Delta(f) = a^2 + 4b$. To examine the monogenicity of $f(x)$, we use Theorem 2.7 with $\theta = \alpha$.

Suppose first that $p \mid a$. Then $p \mid 4b$. If $p \mid b$, then item 1 of Theorem 2.7 applies, and we see that $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] \not\equiv 0 \pmod p$ since b is squarefree. Now suppose that $p \nmid b$, so that item 2 of Theorem 2.7 applies. Note that $p = 2$ since $p \mid 4b$. Hence, $2 \mid a$ and $\mathcal{D} = (a/2)^2 + b \equiv 1 + b \pmod 4$ since $a \not\equiv 0 \pmod 4$. Thus, since $\mathcal{D}$ is squarefree and $2 \nmid b$, it follows that $b \equiv 1 \pmod 4$ and therefore,

$$B_1 = (-b + b^2)/2 = b(b-1)/2 \equiv 0 \pmod 2.$$

Also, $A_2 = -a/2 \equiv 1 \pmod 2$, since $a \not\equiv 0 \pmod 4$. Thus,

$$bA_2^2 - (-B_1)^2 \equiv 1 \pmod 2,$$

from which we conclude that $[[\mathbb{Z}_K : \mathbb{Z}[\alpha]] \not\equiv 0 \pmod 2$.

Next, suppose that $p \nmid a$. Then $p \nmid 4b$ since $p \mid (a^2 + 4b)$, and so item 5 of Theorem 2.7 applies. Since $\mathcal{D}$ is squarefree and $p \neq 2$, we deduce that $p^2 \nmid (a^2 + 4b)$ and consequently, $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] \not\equiv 0 \pmod p$, which completes the proof. □

Lemma 3.4. *Let p be a prime, with $b \not\equiv 0 \pmod p$.*

1. *The prime $p = 2$ is an (a, b)-Wall-Sun-Sun prime if and only if $(a, b)_4 = (3, 3)$.*
2. *If $p \geq 3$ and $a \equiv 0 \pmod p$, then p is an (a, b)-Wall-Sun-Sun prime if and only if $\operatorname{ord}_{p^2}(b) = \operatorname{ord}_p(b)$ and $a \equiv 0 \pmod{p^2}$.*
3. *If $p \geq 5$ and $\delta_p = 0$, then p is not an (a, b)-Wall-Sun-Sun prime.*

Proof. We see that item 1 follows from item 2 of Theorem 2.5.

To establish item 2, we let $[U_n]_m$ denote the sequence (1.1) reduced modulo the integer $m \in \{p, p^2\}$. Since $a \equiv 0 \pmod p$, we can write $a = pk$, for some positive integer k. Then,

$$[U_n]_p = [0, 1, 0, b, 0, b^2, 0, b^3, 0, b^4, 0, b^5, \dots]$$

and

$$[U_n]_{p^2} = [0, 1, pk, b, 2pkb, b^2, 3pkb^2, b^3, \dots, \operatorname{ord}_p(b)pkb^{\operatorname{ord}_p(b)-1}, b^{\operatorname{ord}_p(b)}, \dots].$$

Thus, it follows that p is an (a, b)-Wall-Sun-Sun prime if and only if

$$\begin{aligned}\pi(p^2) = \pi(p) = 2\operatorname{ord}_p(b) &\iff \operatorname{ord}_{p^2}(b) = \operatorname{ord}_p(b) \quad \text{and} \\ &\qquad \operatorname{ord}_p(b)pkb^{\operatorname{ord}_p(b)-1} \equiv 0 \pmod{p^2} \\ &\iff \operatorname{ord}_{p^2}(b) = \operatorname{ord}_p(b) \quad \text{and} \quad a \equiv 0 \pmod{p^2},\end{aligned}$$

since $b \not\equiv 0 \pmod p$ and $\operatorname{ord}_p(b) \leq p - 1 \not\equiv 0 \pmod p$.

The proof of item 3 can be found in [10]. □

Lemma 3.5. *Let $\overline{\alpha} = (a - \sqrt{a^2 + 4b})/2$, and let $p \geq 3$ be a prime such that $\delta_p = -1$. Then*

1. *$\operatorname{ord}_m(\alpha) = \operatorname{ord}_m(\overline{\alpha}) = \pi(m)$ for $m \in \{p, p^2\}$ and*
2. *$\alpha^{p+1} \equiv -b \pmod p$.*

Proof. Note that $b \not\equiv 0 \pmod p$ since $\delta_p = -1$. It follows from [13] that the order, modulo an integer $m \geq 3$ with $\gcd(m, b) = 1$, of the companion matrix $\mathcal{C}$ for the characteristic polynomial of $[U_n]$ is $\pi(m)$. The characteristic polynomial of $[U_n]$ is $f(x)$, so that

$$\mathcal{C} = \begin{bmatrix} 0 & b \\ 1 & a \end{bmatrix}.$$

Since the eigenvalues of $\mathcal{C}$ are α and $\overline{\alpha}$, we conclude that

$$\operatorname{ord}_m\left(\begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}\right) = \operatorname{ord}_m(\mathcal{C}) = \pi(m), \quad \text{for } m \in \{p, p^2\}.$$

Let $z \geq 1$ be an integer, and suppose that $\alpha^z = c + d\sqrt{\mathcal{D}} \in \mathbb{Q}(\sqrt{\mathcal{D}})$. Then $\mathcal{N}(\alpha^z) = c^2 - \mathcal{D}d^2$. But $\mathcal{N}(\alpha^z) = \mathcal{N}(\alpha)^z = (-b)^z$, so that $c^2 - \mathcal{D}d^2 = (-b)^z$. Thus,

$$\overline{\alpha}^z = (-b/\alpha)^z = (-b)^z/(c + d\sqrt{\mathcal{D}}) = (-b)^z(c - d\sqrt{\mathcal{D}})/(c^2 - \mathcal{D}d^2) = c - d\sqrt{\mathcal{D}}.$$

Hence, since $\delta_p = -1$, it follows that

$$\alpha^z \equiv 1 \pmod{m} \quad \text{if and only if} \quad \overline{\alpha}^z \equiv 1 \pmod{m}$$

for $m \in \{p, p^2\}$, which establishes item 1.

By Euler's criterion,

$$\left(\sqrt{a^2+4b}\right)^{p+1} = (a^2+4b)^{(p-1)/2}(a^2+4b) \equiv \delta_p(a^2+4b) \equiv -(a^2+4b) \pmod{p},$$

which implies

$$\left(\sqrt{a^2+4b}\right)^{p} \equiv -\sqrt{a^2+4b} \pmod{p}.$$

Hence,

$$\begin{aligned}
\alpha^{p+1} &= \left(\frac{a+\sqrt{a^2+4b}}{2}\right)\left(\frac{a+\sqrt{a^2+4b}}{2}\right)^p \\
&= \left(\frac{a+\sqrt{a^2+4b}}{2}\right)\sum_{j=0}^{p}\binom{p}{j}\left(\frac{a}{2}\right)^j\left(\frac{\sqrt{a^2+4b}}{2}\right)^{p-j} \\
&\equiv \left(\frac{a+\sqrt{a^2+4b}}{2}\right)\left(\left(\frac{a}{2}\right)^p + \left(\frac{\sqrt{a^2+4b}}{2}\right)^p\right) \pmod{p} \\
&\equiv \left(\frac{a+\sqrt{a^2+4b}}{2}\right)\left(\frac{a-\sqrt{a^2+4b}}{2}\right) \pmod{p} \\
&\equiv -b \pmod{p},
\end{aligned}$$

which completes the proof of the lemma. □

Lemma 3.6. *Let $p \geq 3$ be a prime such that $\delta_p = -1$. Then the following conditions are equivalent:*

(1) p is an (a,b)-Wall-Sun-Sun prime,
(2) $f(\alpha^{p^m}) \equiv 0 \pmod{p^2}$ for all integers $m \geq 1$,
(3) $f(\alpha^{p^m}) \equiv 0 \pmod{p^2}$ for some integer $m \geq 1$.

Proof. First, observe that 2 clearly implies 3.

We show next that 1 implies 2. Because p is an (a,b)-Wall-Sun-Sun prime, we define

$$\pi := \pi(p^2) = \pi(p).$$

Since $\delta_p = -1$, we see from item 4 of Theorem 2.5 that

$$2(p+1)\lambda \equiv 0 \pmod{\pi}.$$

The squares modulo p form a subgroup, of order $(p-1)/2$, of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Thus, $(p-1)/2 \equiv 0 \pmod{\lambda}$, so that

$$2(p+1)(p-1)/2 = p^2 - 1 \equiv 0 \pmod{\pi}.$$

Consequently, $\alpha^{p^2-1} \equiv 1 \pmod{p^2}$ by item 1 of Lemma 3.5, from which it follows that

$$\alpha^{p^{2k}} \equiv \alpha \pmod{p^2} \quad \text{and} \quad \alpha^{p^{2k+1}} \equiv \alpha^p \pmod{p^2},$$

for every integer $k \ge 1$. Hence,

$$f(\alpha^{p^m}) \equiv \begin{cases} \alpha^2 - a\alpha - b \pmod{p^2} & \text{if } m \equiv 0 \pmod 2, \\ \alpha^{2p} - a\alpha^p - b \pmod{p^2} & \text{if } m \equiv 1 \pmod 2. \end{cases}$$

Thus, $f(\alpha^{p^m}) \equiv 0 \pmod{p^2}$ when $m \equiv 0 \pmod 2$, since $\alpha^2 - a\alpha - b = 0$. Suppose then that $m \equiv 1 \pmod 2$. Let $\overline{\alpha} = (a - \sqrt{a^2+4b})/2$. Since p is an (a,b)-Wall-Sun-Sun prime, and the fact that $\overline{\alpha} = -b/\alpha$, we deduce from the Binet-representation formula for U_π that

$$U_\pi = \frac{\alpha^\pi - \overline{\alpha}^\pi}{\alpha - \overline{\alpha}} = \frac{\alpha^{2\pi} - (-b)^\pi}{\alpha^\pi(\alpha - \overline{\alpha})} \equiv 0 \pmod{p^2}. \tag{3.1}$$

Hence, since $\alpha^\pi \equiv 1 \pmod{p^2}$ from item 1 of Lemma 3.5, we conclude from (3.1) that $(-b)^\pi \equiv 1 \pmod{p^2}$, which implies that

$$b^{2(p+1)\lambda} \equiv 1 \pmod{p^2}, \tag{3.2}$$

by item 4 of Theorem 2.5. Thus, from (3.2), it follows that

$$b^{2(p+1)\lambda} - 1 \equiv (b^{2\lambda} - 1)B \equiv 0 \pmod{p^2}, \tag{3.3}$$

where

$$B = (b^{2\lambda})^p + (b^{2\lambda})^{p-1} + \cdots + b^{2\lambda} + 1.$$

Since $b^{2\lambda} \equiv (b^2)^\lambda \equiv 1 \pmod p$, we see that $B \equiv p+1 \equiv 1 \pmod p$. Therefore,

$$b^{2\lambda} - 1 \equiv 0 \pmod{p^2}, \tag{3.4}$$

from (3.3). Also, since $\delta_p = -1$ and $\alpha^\pi \equiv 1 \pmod{p^2}$, we have from item 4 of Theorem 2.5 that

$$\alpha^{2(p+1)\lambda} - 1 \equiv 0 \pmod{p^2}. \tag{3.5}$$

Combining (3.4) and (3.5) yields

$$\alpha^{2(p+1)\lambda} - b^{2\lambda} \equiv \left(\alpha^{p+1} - b\right)\left(\alpha^{p+1} + b\right)C \equiv 0 \pmod{p^2}, \tag{3.6}$$

where

$$\begin{aligned} C &= \left(\alpha^{2(p+1)}\right)^{\lambda-1} + \left(\alpha^{2(p+1)}\right)^{\lambda-2} b^2 + \cdots + \alpha^{2(p+1)}(b^2)^{\lambda-2} + (b^2)^{\lambda-1} \\ &\equiv \lambda b^{2\lambda+2} \pmod p, \end{aligned}$$

since $\alpha^{2(p+1)} \equiv b^2 \pmod p$ from item 2 of Lemma 3.5. Thus, from (3.4) and the fact that $(p-1)/2 \equiv 0 \pmod \lambda$, we deduce that $C \equiv \lambda b^2 \not\equiv 0 \pmod p$. Note that $\alpha^{p+1} - b \not\equiv 0 \pmod p$ since $\alpha^{p+1} + b \equiv 0 \pmod p$ and $b \not\equiv 0 \pmod p$. Therefore, it follows from (3.6) that $\alpha^{p+1} \equiv -b \pmod{p^2}$. Hence, $\alpha^p \equiv -b\alpha^{-1} \pmod{p^2}$, and consequently,

$$\begin{aligned} f(\alpha^{p^m}) &\equiv \alpha^{2p} - a\alpha^p - b \pmod{p^2} \\ &\equiv \left(-b\alpha^{-1}\right)^2 - a\left(-b\alpha^{-1}\right) - b \pmod{p^2} \\ &\equiv -b\alpha^{-2}(\alpha^2 - a\alpha - b) \pmod{p^2} \\ &\equiv 0 \pmod{p^2} \end{aligned}$$

since $\alpha^2 - a\alpha - b = 0$, which completes the proof that 1 implies 2.

Finally, to establish that 3 implies 1, we first note that $\pi(p^2) \in \{\pi(p), p\pi(p)\}$ by item 3 of Theorem 2.5. Then, in either case, we have that $\alpha^{p\pi(p)} \equiv 1 \pmod{p^2}$, and we conclude from item 4 of Theorem 2.5 that $\alpha^{2p(p+1)\lambda} \equiv 1 \pmod{p^2}$. Since $(p-1)/2 \equiv 0 \pmod{\lambda}$, we deduce

$$\alpha^{2p(p+1)(p-1)/2} \equiv \alpha^{p^3-p} \equiv 1 \pmod{p^2},$$

so that $\alpha^{p^3} \equiv \alpha^p \pmod{p^2}$. It then follows easily that

$$\alpha^{p^{2k}} \equiv \alpha^{p^2} \pmod{p^2} \quad \text{and} \quad \alpha^{p^{2k+1}} \equiv \alpha^p \pmod{p^2}, \tag{3.7}$$

for all integers $k \geq 1$. Hence, from (3.7), we have that

$$f(\alpha^{p^m}) \equiv \begin{cases} \alpha^{2p^2} - a\alpha^{p^2} - b \pmod{p^2} & \text{if } m \equiv 0 \pmod{2}, \\ \alpha^{2p} - a\alpha^p - b \pmod{p^2} & \text{if } m \equiv 1 \pmod{2}. \end{cases} \tag{3.8}$$

Since $\delta_p = -1$, we have that $f(x)$ is irreducible modulo p. Consequently, the only zeros of $f(x)$ in $(\mathbb{Z}/p^2\mathbb{Z})[\sqrt{5}]$ are α and $\overline{\alpha} = -b\alpha^{-1}$. Suppose that $f(\alpha^{p^m}) \equiv 0 \pmod{p^2}$ for some integer $m \equiv 1 \pmod{2}$. Then, we see from (3.8) that

$$\text{either} \quad \alpha^p \equiv \alpha \pmod{p^2} \quad \text{or} \quad \alpha^p \equiv \overline{\alpha} \pmod{p^2}.$$

If $\alpha^p \equiv \alpha \pmod{p^2}$, then, from item 2 of Lemma 3.5, we have that

$$\frac{a^2 + 4b + a\sqrt{a^2+4b}}{2} = \alpha^2 + b \equiv \alpha^{p+1} + b \equiv 0 \pmod{p},$$

which implies that $a^2 + 4b \equiv 0 \pmod{p}$, contradicting the fact that $\delta_p = -1$. Hence,

$$\alpha^p \equiv \overline{\alpha} \equiv -b\alpha^{-1} \pmod{p^2} \quad \text{or equivalently,} \quad \alpha^{p+1} \equiv -b \pmod{p^2}. \tag{3.9}$$

Since $\alpha^{2p} - a\alpha^p - b \equiv 0 \pmod{p^2}$, then $\overline{\alpha}^{2p} - a\overline{\alpha}^p - b \equiv 0 \pmod{p^2}$ so that

$$\text{either} \quad \overline{\alpha}^p \equiv \alpha \pmod{p^2} \quad \text{or} \quad \overline{\alpha}^p \equiv \overline{\alpha} \pmod{p^2}.$$

From (3.9), we have that

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

If $\overline{\alpha}^p \equiv \overline{\alpha} \pmod{p^2}$, then we see from (3.10) that $\overline{\alpha}^2 \equiv (-b)^p \pmod{p^2}$, so that $\overline{\alpha}^2 + b \equiv 0 \pmod{p}$. That is,

$$\left(\frac{a - \sqrt{a^2+4b}}{2}\right)^2 + b = \frac{a^2 + 4b - a\sqrt{a^2+4b}}{2} \equiv 0 \pmod{p},$$

which implies that $a^2 + 4b \equiv 0 \pmod{p}$, again contradicting the fact that $\delta_p = -1$. Therefore, $\overline{\alpha}^p \equiv \alpha \pmod{p^2}$, and we see from (3.9) and (3.10) that

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

Consequently,

$$(-b)^{p-1} \equiv 1 \pmod{p^2}. \tag{3.11}$$

Combining (3.9) and (3.11) yields

$$\alpha^{p^2-1} \equiv (\alpha^{p+1})^{p-1} \equiv (-b)^{p-1} \equiv 1 \pmod{p^2}. \tag{3.12}$$

Recall that $\pi(p^2) \in \{\pi(p), p\pi(p)\}$ by item 3 of Theorem 2.5. If $\pi(p^2) = p\pi(p)$, then we have by item 1 of Lemma 3.5 and (3.12) that $p^2 - 1 \equiv 0 \pmod{p}$, which is impossible. Thus, we must have $\pi(p^2) = \pi(p)$, which completes the proof that 3 implies 1 when $m \equiv 1 \pmod{2}$.

Suppose now that $f(\alpha^{p^m}) \equiv 0 \pmod{p^2}$ for some integer $m \equiv 0 \pmod 2$. Then, we see from (3.8) that

$$\text{either} \quad \alpha^{p^2} \equiv \alpha \pmod{p^2} \quad \text{or} \quad \alpha^{p^2} \equiv \overline{\alpha} \equiv -b\alpha^{-1} \pmod{p^2}. \tag{3.13}$$

If $\alpha^{p^2} \equiv -b\alpha^{-1} \pmod{p^2}$, then $\alpha^{p^2+1} \equiv -b \pmod{p^2}$. Note that $p \nmid b$ since $\delta_p = -1$. Hence, using item 2 of Lemma 3.5, we have that

$$\begin{aligned}
\alpha^{p^2+1} \equiv -b \pmod p &\Longrightarrow \left(-b\alpha^{-1}\right)^p \alpha \equiv -b \pmod p \\
&\Longrightarrow (-b)^p(\alpha^p)^{-1}\alpha \equiv -b \pmod p \\
&\Longrightarrow \alpha \equiv \alpha^p \pmod p \\
&\Longrightarrow \alpha \equiv \overline{\alpha}, \pmod p
\end{aligned}$$

which yields the contradiction $a^2 + 4b \equiv 0 \pmod p$. Thus, $\alpha^{p^2} \equiv \alpha \pmod{p^2}$ from (3.13), which implies that $\alpha^{p^2-1} \equiv 1 \pmod{p^2}$. Therefore, the conclusion of the proof in this case is identical to the conclusion of the case $m \equiv 1 \pmod 2$ following (3.12). $\square$

Lemma 3.7. *Let $s \geq 3$ and $n \geq 1$ be integers. Let $p \geq 3$ be a prime such that $p^m \parallel s^n$ with $m \geq 1$. Suppose that $\mathcal{F}_n(x) := f(x^{s^n})$ and $K = \mathbb{Q}(\theta)$, with $\mathbb{Z}_K$ the ring of integers of K, where $\mathcal{F}_n(\theta) = 0$.*

(1) If $\delta_p \neq 1$, then

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \equiv 0 \pmod p \quad \textit{if and only if} \quad \alpha^{2p^m} - a\alpha^{p^m} - b \equiv 0 \pmod{p^2}.$$

(2) Furthermore, if $\delta_p = 0$, then $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod p$.

Proof. For item 1, we apply Theorem 2.6 to $T(x) := \mathcal{F}_n(x)$ using the prime p. Let

$$\tau(x) = x^{2s^n/p^m} - ax^{s^n/p^m} - b = f\left(x^{s^n/p^m}\right), \tag{3.14}$$

and $\overline{\tau}(x) = \prod_i \overline{\tau_i}(x)^{e_i}$, where the $\overline{\tau_i}(x)$ are irreducible in $\mathbb{F}_p[x]$. Then $\overline{T}(x) = \prod_i \overline{\tau_i}(x)^{p^m e_i}$. Thus, we can let

$$g(x) = \prod_i \tau_i(x) \quad \text{and} \quad h(x) = \prod_i \tau_i(x)^{p^m e_i - 1},$$

where the $\tau_i(x)$ are monic lifts of the $\overline{\tau_i}(x)$. Note also that

$$g(x)h(x) = \prod_i \tau_i(x)^{p^m e_i} = \tau(x) + pw(x),$$

for some $w(x) \in \mathbb{Z}[x]$. Then, in Theorem 2.6, we have that

$$\begin{aligned}
pF(x) &= g(x)h(x) - T(x) \\
&= (\tau(x) + pw(x))^{p^m} - T(x) \\
&= \sum_{j=1}^{p^m-1} \binom{p^m}{j} \tau(x)^j (pw(x))^{p^m-j} + (pw(x))^{p^m} + \tau(x)^{p^m} - T(x) \qquad (3.15)\\
&\equiv \tau(x)^{p^m} - T(x) \pmod{p^2}.
\end{aligned}$$

Suppose that $\tau(\gamma) = 0$. Then, we see from (3.14) that

$$\tau(\gamma) = f(\gamma^{s^n/p^m}) = 0.$$

If $\delta_p = -1$, then $f(x)$ is irreducible modulo p, while if $\delta_p = 0$, then $f(x) \equiv (x-\alpha)^2 \pmod{p}$, where $\alpha = 2^{-1}a \pmod{p}$. In either case, without loss of generality, we can assume $\gamma^{s^n/p^m} = \alpha$ so that $\gamma^{s^n} = \alpha^{p^m}$. Hence, from (3.15), it follows that

$$\begin{aligned} pF(\gamma) &\equiv -T(\gamma) \pmod{p^2} \\ &\equiv -\left(\gamma^{2s^n} - a\gamma^{s^n} - b\right) \pmod{p^2} \\ &\equiv -\left(\alpha^{2p^m} - a\alpha^{p^m} - b\right) \pmod{p^2}, \end{aligned}$$

which completes the proof of item 1.

To establish item 2, we show that

$$S(x) := x^{2p^m} - ax^{p^m} - b$$

has no zeros modulo p^2 for any integer $m \geq 1$. Observe that

$$S(x) \equiv f(x)^{p^m} \equiv (x-\alpha)^{2p^m} \pmod{p},$$

where $\alpha = 2^{-1}a \pmod{p}$. Since $S'(\alpha) \equiv 0 \pmod{p}$, we deduce from Hensel that either $S(x)$ has no zeros modulo p^2, or has the p zeros:

$$\alpha, \quad \alpha+p, \quad \alpha+2p, \quad \dots, \quad \alpha+(p-1)p \quad \text{modulo } p^2.$$

Suppose then, by way of contradiction, that

$$S(\alpha) = \alpha^{2p^m} - a\alpha^{p^m} - b \equiv 0 \pmod{p^2}. \tag{3.16}$$

Since $\delta_p = 0$, then $\alpha^2 \equiv 2^{-2}a^2 \equiv -b \pmod{p}$, and therefore,

$$\alpha^{2p^m} \equiv (-b)^{p^m} \pmod{p^2}. \tag{3.17}$$

Hence, from (3.16) and (3.17), we have that

$$a\alpha^{p^m} \equiv (-b)^{p^m} - b \pmod{p^2}. \tag{3.18}$$

Then, squaring both sides of (3.18) and using (3.17) again gives

$$a^2(-b)^{p^m} \equiv \left((-b)^{p^m} - b\right)^2 \pmod{p^2}, \tag{3.19}$$

which in turn yields

$$\begin{aligned} &\Longrightarrow a^2(-b)^{p^m-2} \equiv \left((-b)^{p^m-1}+1\right)^2 \pmod{p^2} \\ &\Longrightarrow a^2(-b)^{p^m-2} - 4(-b)^{p^m-1} \equiv \left((-b)^{p^m-1}+1\right)^2 - 4(-b)^{p^m-1} \pmod{p^2} \end{aligned}$$

$$\Longrightarrow \left(a^2+4b\right)(-b)^{p^m-2} \equiv \left((-b)^{p^m-1}-1\right)^2 \equiv 0 \pmod{p^2}, \tag{3.20}$$

since $(-b)^{p^m-1} - 1 \equiv 0 \pmod{p}$. Thus, since $p \nmid b$, we conclude from (3.20) that

$$a^2 + 4b \equiv 0 \pmod{p^2},$$

which contradicts the fact that $\mathcal{D}$ is squarefree, and completes the proof of the lemma. □

Remark 3.8. In the context of Lemma 3.7, item 2 shows that a prime p with $\delta_p = 0$ cannot "cause" $\mathcal{F}_n(x)$ to be non-monogenic.

Proof of Theorem 1.2. Note that $\mathcal{F}_0(x) = f(x)$. We have that $\mathcal{F}_n(x)$ is irreducible for all $n \geq 0$ by Lemma 3.1. By Theorem 2.1,

$$\Delta(\mathcal{F}_n) = (-b)^{s^n-1} s^{2ns^n} (a^2+4b)^{s^n}. \tag{3.21}$$

($\Rightarrow$) We prove the contrapositive. Assume that s has a prime divisor p that is an (a,b)-Wall-Sun-Sun prime, and that $p^m \parallel s^n$, with $m \geq 1$.

Suppose first that $p = 2$, and write $s^n = 2^m v$, with $2 \nmid v$. Then $2 \nmid a$ since $(a,b) = (3,3)_4$ by item 1 of Lemma 3.4. Applying item 4 of Theorem 2.7 to $\mathcal{F}_n(x)$ we see that

$$\begin{aligned}
G(x) &= x^{2s^n/2^m} - ax^{s^n/2^m} - b\\
&= x^{2v} - ax^v - b\\
&\equiv x^{2v} + x^v + 1 \pmod 2 \quad \text{and}\\
H(x) &= \frac{-ax^{2^m v} - b + (ax^v+b)^{2^m}}{2}\\
&= \left(\frac{a^{2^m}-a}{2}\right)x^{2^m v} + \sum_{j=1}^{2^m-1} \frac{\binom{2^m}{j}}{2}(ax^v)^j b^{2^m-j} + \frac{b^{2^m}-b}{2} \qquad (3.22)\\
&\equiv \left(x^{2v}+x^v+1\right)^{2^{m-1}} \pmod 2,
\end{aligned}$$

since $a^{2^m} - a \equiv b^{2^m} - b \equiv 2 \pmod 4$ and [7]

$$\binom{2^m}{j} \equiv \begin{cases} 0 \pmod 4 & \text{if } j \neq 2^{m-1}\\ 2 \pmod 4 & \text{if } j = 2^{m-1}. \end{cases} \tag{3.23}$$

Thus, $G(x)$ and $H(x)$ are not coprime in $\mathbb{F}_2[x]$, and therefore, $\mathcal{F}_n(x)$ is not monogenic.

Suppose next that $p \geq 3$. Recall that if $p = 3$, then $\delta_3 = -1$ by hypothesis. If $p \geq 5$, then, since p is an (a,b)-Wall-Sun-Sun prime and $\delta_p \neq 1$, we conclude that $\delta_p = -1$, from item 3 of Lemma 3.4. Thus, $\mathcal{F}_n(x)$ is non-monogenic by Lemma 3.6 and item 1 of Lemma 3.7, which completes the proof in this direction.

($\Leftarrow$) Note that when $s = 1$, we have that $\mathcal{F}_n(x) = f(x)$ for all $n \geq 0$, and so $\mathcal{F}_n(x)$ is monogenic by Lemma 3.3. So, assume that $s \geq 2$, and suppose that no prime divisor of s is an (a,b)-Wall-Sun-Sun prime.

For $n \geq 0$, define

$$\alpha_n := \alpha^{1/s^n} \quad \text{and} \quad K_n := \mathbb{Q}(\alpha_n).$$

Then $\alpha_0 = \alpha$ and, since $\mathcal{F}_0(x) = f(x)$ is monogenic, we have that $\Delta(\mathcal{F}_0) = \Delta(K_0)$. Additionally, for all $n \geq 1$, we have that

$$\mathcal{F}_n(\alpha_n) = 0 \quad \text{and} \quad [K_n : K_{n-1}] = s,$$

by Lemma 3.1. We assume that $\mathcal{F}_{n-1}(x)$ is monogenic, so that $\Delta(\mathcal{F}_{n-1}) = \Delta(K_{n-1})$, and we proceed by induction on n to show that $\mathcal{F}_n(x)$ is monogenic. Let $\mathbb{Z}_{K_n}$ denote the ring of integers of K_n. Consequently, by Theorem 2.9, it follows that

$$\Delta(\mathcal{F}_{n-1})^s \text{ divides } \Delta(K_n) = \frac{\Delta(\mathcal{F}_n)}{[\mathbb{Z}_{K_n} : \mathbb{Z}[\alpha_n]]^2},$$

which implies that

$$[\mathbb{Z}_{K_n} : \mathbb{Z}[\alpha_n]]^2 \text{ divides } \frac{\Delta(\mathcal{F}_n)}{\Delta(\mathcal{F}_{n-1})^s}.$$

We see from (3.21) that

$$|\Delta(\mathcal{F}_{n-1})^s| = (-b)^{s^n-s}s^{2(n-1)s^n}(a^2+4b)^{s^n} \quad \text{and}$$
$$|\Delta(\mathcal{F}_n)| = (-b)^{s^n-1}s^{2ns^n}(a^2+4b)^{s^n}.$$

Hence,

$$\left|\frac{\Delta(\mathcal{F}_n)}{\Delta(\mathcal{F}_{n-1})^s}\right| = (-b)^{s-1}s^{2s^n}.$$

Thus, it is enough to show that $\gcd(bs, [\mathbb{Z}_{K_n} : \mathbb{Z}[\alpha_n]]) = 1$. Recall that $\gcd(b, s) = 1$ by hypothesis.

Suppose first that p is a prime divisor of b. If $p \mid a$, then it follows that

$$[\mathbb{Z}_{K_n} : \mathbb{Z}[\alpha_n]] \not\equiv 0 \pmod p \tag{3.24}$$

by item 1 of Theorem 2.7 since b is squarefree. So, assume that $p \nmid a$. In this case, we apply item 3 of Theorem 2.7 to $\mathcal{F}_n(x)$. Observe that $A_1 = 0$ since $p \nmid s$, and $B_2 = -b/p \not\equiv 0 \pmod p$ since b is squarefree. Thus, the first condition of item 3 holds, and therefore once again we have (3.24).

Suppose next that p is a prime divisor of s with $s^n = p^m v$, where $m \geq 1$ and $p \nmid v$. Note that $p \nmid b$.

We first address the prime $p = 2$. If $2 \mid a$, then we apply item 2 of Theorem 2.7 to $\mathcal{F}_n(x)$. Observe from conditions $(*)$ that in this case, $2 \parallel a$ and $b \equiv 1 \pmod 4$ since respectively, $a \not\equiv 0 \pmod 4$ and $\mathcal{D} = (a/2)^2 + b$ is squarefree. Thus,

$$A_2 = -\frac{a}{2} \not\equiv 0 \pmod 2 \quad \text{and} \quad B_1 = \frac{-b + b^{2^{m+1}}}{2} \equiv 0 \pmod 2,$$

from which we conclude that the second condition of item 2 of Theorem 2.7 holds. Therefore, in this case, we have (3.24). If $2 \nmid a$, we apply item 4 of Theorem 2.7 to $\mathcal{F}_n(x)$. Since 2 is not an (a, b)-Wall-Sun-Sun prime, we have that

$$(a, b)_4 \in \{(1,1), (1,3), (3,1)\}$$

from item 2 of Theorem 2.5. Since

$$c^{2^m} - c \equiv \begin{cases} 0 \pmod 4 & \text{if } c \equiv 1 \pmod 4 \\ 2 \pmod 4 & \text{if } c \equiv 3 \pmod 4, \end{cases}$$

for an integer c and and an integer $m \geq 1$, it follows from (3.22) and (3.23) that

$$\overline{G}(x) = x^{2v} + x^v + 1 \quad \text{and}$$

$$\overline{H}(x) = \begin{cases} x^{2^{m-1}v} & \text{if } (a,b)_4 = (1,1) \\ (x^v+1)^{2^{m-1}} & \text{if } (a,b)_4 = (1,3) \\ x^{2^{m-1}v}(x^v+1)^{2^{m-1}} & \text{if } (a,b)_4 = (3,1). \end{cases}$$

Hence, for every zero ρ of $\overline{H}(x)$, we see that $\overline{G}(\rho) = 1$. Thus, $G(x)$ and $H(x)$ are coprime modulo 2, so that (3.24) holds with $p = 2$.

Now suppose that $p \geq 3$. If $\delta_p = -1$, then (3.24) follows from Lemma 3.6 and item 1 of Lemma 3.7, since p is not an (a, b)-Wall-Sun-Sun prime. Recall that $\delta_3 = -1$ by hypothesis. Then, finally, if $p \geq 5$ with $\delta_p = 0$, it follows from item 2 of Lemma 3.7 that (3.24) holds, completing the proof of the theorem. □

REFERENCES

[1] Z. Bouazzaoui, *Fibonacci numbers and real quadratic p-rational fields*, Period. Math. Hungar. **81** (2020), no. 1, 123–133.

[2] Z. Bouazzaoui, *On periods of Fibonacci sequences and real quadratic p-rational fields*, Fibonacci Quart. **58** (2020), no. 5, 103–110.

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

[4] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), no. 217, 433–449.

[5] A.-S. Elsenhans and J. Jahnel, *The Fibonacci sequence modulo* p^2*-An investigation by computer for* $p < 1014$, arXiv:1006.0824v1.

[6] S. Gupta, P. Rockstroh and F. E. Su, *Splitting fields and periods of Fibonacci sequences modulo primes*, Math. Mag. **85** (2012), no. 2, 130–135.

[7] P. Haggard and J. Kiltinen, *Binomial expansions modulo prime powers*, Internat. J. Math. Math. Sci. **3** (1980), no. 2, 397–400.

[8] 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.

[9] L. Jones, *A Connection Between the Monogenicity of Certain Power-Compositional Trinomials and* k*-Wall-Sun-Sun Primes*, http://arxiv.org/abs/2211.14834.

[10] J. Harrington and L. Jones, *A note on generalized Wall-Sun-Sun primes*, Bull. Aust. Math. Soc. (to appear).

[11] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[12] M. Renault, *The period, rank, and order of the* (a,b)*-Fibonacci sequence mod* m, Math. Mag. **86** (2013), no. 5, 372–380.

[13] D. W. Robinson, *A note on linear recurrent sequences modulo* m, Amer. Math. Monthly **73** (1966), 619–621.

[14] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, **77**, Cambridge University Press, Cambridge, 2000.

[15] Zhi Hong Sun and Zhi Wei Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), no. 4, 371–388.

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

[17] D. D. Wall, *Fibonacci series modulo* m, Amer. Math. Monthly **67** (1960), 525–532.

[18] *Fundamental Discriminant* https://en.wikipedia.org/wiki/Fundamental_discriminant

[19] *Wieferich Prime* https://en.wikipedia.org/wiki/Wieferich_prime

[20] *Wall-Sun-Sun Prime*
https://en.wikipedia.org/wiki/Wall%E2%80%93Sun%E2%80%93Sun_prime

[21] H. Yokoi, *On real quadratic fields containing units with norm* -1, Nagoya Math. J. **33** (1968), 139–152.