TAIWANESE JOURNAL OF MATHEMATICS
Vol. 28, No. 1, pp. 17–28, February 2024
DOI: 10.11650/tjm/231003

A New Condition for k-Wall–Sun–Sun Primes

Lenny Jones

Abstract. Let $k \geq 1$ be an integer, and let (U_n) be the Lucas sequence of the first kind defined by

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

It is well known that (U_n) is periodic modulo any integer $m \geq 2$, and we let $\pi(m)$ denote the length of this period. A prime p is called a *k-Wall–Sun–Sun prime* if $\pi(p^2) = \pi(p)$.

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree N that is irreducible over $\mathbb{Q}$. We say $f(x)$ is *monogenic* if $\Theta = \{1, \theta, \theta^2, \ldots, \theta^{N-1}\}$ is a basis for the ring of integers $\mathbb{Z}_K$ of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. If Θ is not a basis for $\mathbb{Z}_K$, we say that $f(x)$ is *non-monogenic*.

Suppose that $k \not\equiv 0 \pmod 4$ and that $\mathcal{D} := (k^2 + 4)/\gcd(2,k)^2$ is squarefree. We prove that p is a k-Wall–Sun–Sun prime if and only if $\mathcal{F}_p(x) = x^{2p} - kx^p - 1$ is non-monogenic. Furthermore, if p is a prime divisor of k^2+4, then $\mathcal{F}_p(x)$ is monogenic.

1. Introduction

Let $k \geq 1$ be an integer, and let $(U_n) := (U_n(k,-1))$ be the Lucas sequence of the first kind defined by

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

It is well known that (U_n) is periodic modulo any integer $m \geq 2$, and we let $\pi(m) := \pi_k(m)$ denote the length of this period. A prime p is called a *k-Wall–Sun–Sun prime* if

$$\pi(p^2) = \pi(p). \tag{1.1}$$

Note that (U_n) is the Fibonacci sequence when $k = 1$, and in this case, primes satisfying (1.1) are simply called *Wall–Sun–Sun primes*. For the Fibonacci sequence, D. D. Wall [15] first asked in 1960 about the existence of primes satisfying (1.1). In 1992, the Sun brothers [13] showed that the first case of Fermat's Last Theorem for exponent p fails only if p satisfies (1.1). The question of whether any Wall–Sun–Sun primes exist is still

Received July 15, 2023; Accepted October 23, 2023.
Communicated by Ming-Lun Hsieh.
2020 *Mathematics Subject Classification*. Primary: 11R04; Secondary: 11B39, 11R09, 12F05.
Key words and phrases. k-Wall–Sun–Sun prime, monogenic.

unresolved, and as of December 2022, if p is a Wall–Sun–Sun prime, then $p > 2^{64}$ [4,16]. However, the situation is quite different when $k \geq 2$ [16].

Several conditions are known to be equivalent to (1.1). For example, it is easy to see that $U_{\pi(p)} \equiv 0 \pmod{p^2}$ is one such condition. Another, less obvious, equivalent condition is $U_{p-\delta_p} \equiv 0 \pmod{p^2}$, where δ_p is the Legendre symbol $\left(\frac{k^2+4}{p}\right)$. For more information and proofs, see [1,2,8,16].

It is the goal of this article to present a new condition equivalent to (1.1) that is quite unlike any previously known condition. This new condition involves the concept of the monogenicity of a certain polynomial, which we now describe. Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial that is irreducible over $\mathbb{Q}$. Let $\mathbb{Z}_K$ be the ring of integers of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. Then [3]

$$\Delta(f) = \left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right]^2 \Delta(K), \tag{1.2}$$

where $\Delta(f)$ and $\Delta(K)$ denote, respectively, the discriminants over $\mathbb{Q}$ of $f(x)$ and the number field K. We define $f(x)$ to be *monogenic* if $\Theta = \left\{1, \theta, \theta^2, \ldots, \theta^{\deg(f)-1}\right\}$ is a basis for $\mathbb{Z}_K$. If Θ fails to be a basis for $\mathbb{Z}_K$, we say that $f(x)$ is *non-monogenic.* Observe then, from (1.2), that $f(x)$ is monogenic if and only if $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] = 1$ or, equivalently, $\Delta(f) = \Delta(K)$.

The main theorem of this article is as follows:

Theorem 1.1. *Let p be a prime. Let $k \geq 1$ be an integer such that $k \not\equiv 0 \pmod 4$ and $\mathcal{D}$ is squarefree, where*

$$\mathcal{D} := \frac{k^2+4}{\gcd(2,k)^2}. \tag{1.3}$$

Then p is a k-Wall–Sun–Sun prime if and only if

$$\text{the polynomial } \mathcal{F}_p(x) := x^{2p} - kx^p - 1 \text{ is non-monogenic.}$$

Furthermore, if p is a prime divisor of k^2+4, then $\mathcal{F}_p(x)$ is monogenic.

At first glance, Theorem 1.1 might appear to be just a special case of Theorem 1.2 in [8] or Theorem 1.2 in [9]. However, upon closer inspection, we see that certain restrictions on the prime p and the quadratic character of $\mathcal{D}$ modulo p are necessary in both [8] and [9]. Therefore, Theorem 1.1 represents an improvement over both [8] and [9], in the particular situation of k-Wall–Sun–Sun primes, since no such restrictions are required here. Moreover, Theorem 1.1 provides explicit conditions under which $\mathcal{F}_p(x)$ is monogenic. Since the particular situation of Theorem 1.1 might be more appealing to a broader audience than the generality found in [9], and regardless of the fact that many of the same methods are employed in [9], we give here a self-contained presentation with full details.

2. Preliminaries

Throughout this article, we assume that k is a positive integer such that $4 \nmid k$ and $\mathcal{D}$ is squarefree, where $\mathcal{D}$ is as defined in (1.3). We also let

- p and q denote primes,
- $\alpha = \frac{k+\sqrt{k^2+4}}{2}$ and $\beta = \frac{k-\sqrt{k^2+4}}{2}$,
- $f(x) := x^2 - kx - 1$ (the characteristic polynomial of the sequence (U_n)),
- $\mathcal{F}_p(x) := x^{2p} - kx^p - 1$,
- $\mathrm{ord}_m(*)$ denote the order of $*$ modulo the integer $m \geq 2$,
- δ_p denote the Legendre symbol $\left(\frac{k^2+4}{p}\right)$.

The first result gives some known facts concerning $\pi(p^2)$ and $\pi(p)$.

Theorem 2.1. [5, 10]

(a) $\pi(p^2) \in \{\pi(p), p\pi(p)\}$.

(b) *If* $\delta_p = 1$, *then* $p - 1 \equiv 0 \pmod{\pi(p)}$.

(c) *If* $\delta_p = -1$, *then* $2(p+1) \equiv 0 \pmod{\pi(p)}$.

The following lemma is a special case of [6, Theorem 1.1].

Lemma 2.2. *Suppose that* p *is a divisor of* k^2+4. *If* $p = 2$, *then* p *is a* k*-Wall–Sun–Sun prime if and only if* $k \equiv 0 \pmod 4$. *If* $p \geq 3$, *then* p *is not a* k*-Wall–Sun–Sun prime.*

The next two theorems are due to Capelli [12].

Theorem 2.3. *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 2.4. *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* $\alpha = \gamma^p$ *for some* $\gamma \in \mathbb{Q}(\alpha)$ *or* $4 \mid c$ *and* $\alpha = -4\gamma^4$ *for some* $\gamma \in \mathbb{Q}(\alpha)$.

The discriminant of $\mathcal{F}_p(x)$ given in the next proposition follows from the formula for the discriminant of an arbitrary monic trinomial [14].

Proposition 2.5. $\Delta(\mathcal{F}_p) = (-1)^{(p+1)(2p-1)} p^{2p} (k^2+4)^p$.

The next theorem is essentially an algorithmic adaptation, specifically for trinomials, of Dedekind's Index Criterion [3], which is a standard tool used to determine the monogenicity of an irreducible monic polynomial.

Theorem 2.6. [7] *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*

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

A prime factor q of $\Delta(f)$ does not divide $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right]$ if and only if q satisfies one of the following items:

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

(b) *when $q \mid A$ and $q \nmid B$, then*

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

where $A_2 = A/q$ and $B_1 = \frac{B + (-B)^{q^e}}{q}$ with $q^e \mid\mid N$;

(c) *when $q \nmid A$ and $q \mid B$, then*

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

where $A_1 = \frac{A + (-A)^{q^j}}{q}$ with $q^j \mid\mid (N - M)$, and $B_2 = B/q$;

(d) *when $q \nmid AB$ and $q \mid M$ with $N = uq^m$, $M = vq^m$, $q \nmid \gcd(u, v)$, then the polynomials*

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

are coprime modulo q;

(e) *when $q \nmid ABM$, then $q^2 \nmid D/r^{N_1}$.*

3. Proof of Theorem 1.1

We first prove some lemmas.

Lemma 3.1. *The polynomial $\mathcal{F}_p(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Clearly, $f(x)$ is irreducible over $\mathbb{Q}$ since $\mathcal{D}$ is squarefree. Note that $f(\alpha) = 0$. Let $h(x) = x^p$ so that $\mathcal{F}_p(x) = f(h(x))$. Assume, by way of contradiction, that $f(h(x))$ is reducible. Then, by Theorems 2.3 and 2.4, we have that $\alpha = \gamma^p$ for some $\gamma \in \mathbb{Q}(\alpha)$. Then, we see by taking norms that

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

which implies that $p \geq 3$ and $\mathcal{N}(\gamma) = -1$, since $\mathcal{N}(\gamma) \in \mathbb{Z}$. Thus, γ is a unit, and therefore $\gamma = \pm\alpha^j$ for some $j \in \mathbb{Z}$, since, in light of the fact that $k \neq 4$, α is the fundamental unit of $\mathbb{Q}(\sqrt{\mathcal{D}})$ [17]. Consequently,

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

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 $\mathbb{Q}(\sqrt{\mathcal{D}})$. $\square$

Lemma 3.2. *Suppose that $p \geq 3$. Then*

(a) $\mathrm{ord}_m(\alpha) = \pi(m)$ *for* $m \in \{p, p^2\}$,

(b) $\alpha^{p-1} \equiv 1 \pmod{p}$ *if* $\delta_p = 1$,

(c) $\alpha^{p+1} \equiv -1 \pmod{p}$ *if* $\delta_p = -1$.

Proof. It follows from [11] that the order, modulo an integer $m \geq 3$, of the companion matrix

$$\mathcal{C} = \begin{bmatrix} 0 & 1 \\ 1 & k \end{bmatrix}$$

for the characteristic polynomial $f(x)$ of (U_n) is $\pi(m)$. Since the eigenvalues of $\mathcal{C}$ are α and β, we conclude that

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

It follows that at least one of α and β has order $\pi(m)$, and we can assume without loss of generality, that $\mathrm{ord}_m(\alpha) = \pi(m)$, which establishes (a).

For (b) and (c), we have by Euler's criterion that

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

which implies that $\left(\sqrt{k^2+4}\right)^p \equiv \delta_p\sqrt{k^2+4} \pmod{p}$. Hence,

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

$$\equiv \left(\frac{k+\sqrt{k^2+4}}{2}\right)\left(\left(\frac{k}{2}\right)^p+\left(\frac{\sqrt{k^2+4}}{2}\right)^p\right) \pmod p$$
$$\equiv \left(\frac{k+\sqrt{k^2+4}}{2}\right)\left(\frac{k+\delta_p\sqrt{k^2+4}}{2}\right) \pmod p$$
$$\equiv \begin{cases} \alpha^2 \pmod p & \text{if } \delta_p=1, \\ -1 \pmod p & \text{if } \delta_p=-1. \end{cases}$$

Since $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$ when $\delta_p = 1$, we note that (b) also follows from Fermat's Little Theorem. $\square$

Lemma 3.3. *Suppose that $p \geq 3$. Then*

$$\mathcal{F}_p(\beta) \equiv 0 \pmod{p^2} \iff \mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}.$$

Proof. Note that if $\mathcal{F}_p(\beta) = \beta^{2p} - k\beta^p - 1 \equiv 0 \pmod{p^2}$, then

$$\beta^p - k - \beta^{-p} \equiv 0 \pmod{p^2}. \tag{3.1}$$

Since $\alpha\beta \equiv -1 \pmod p$, we have that $(\alpha\beta)^p \equiv (-1)^p \equiv -1 \pmod{p^2}$. Thus, since $\alpha^p \not\equiv k \pmod p$ from Lemma 3.2, we have

$$\begin{aligned}
\mathcal{F}_p(\beta) \equiv 0 \pmod{p^2} &\iff \beta^p(\beta^p - k) \equiv 1 \pmod{p^2} \\
&\iff \alpha^p\beta^p(\beta^p - k) \equiv \alpha^p \pmod{p^2} \\
&\iff -(\beta^p - k) \equiv \alpha^p \pmod{p^2} \\
&\iff -(\alpha^p - k)(\beta^p - k) \equiv \alpha^p(\alpha^p - k) \pmod{p^2} \\
&\iff -(\alpha^p\beta^p - k\alpha^p - k\beta^p + k^2) \equiv \alpha^p(\alpha^p - k) \pmod{p^2} \\
&\iff 1 + k(\alpha^p + \beta^p) - k^2 \equiv \alpha^p(\alpha^p - 1) \pmod{p^2} \\
&\iff 1 + k(-\beta^{-p} + \beta^p) - k^2 \equiv \alpha^p(\alpha^p - 1) \pmod{p^2} \\
&\iff 1 \equiv \alpha^p(\alpha^p - 1) \pmod{p^2} \quad \text{(from (3.1))} \\
&\iff \mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}.
\end{aligned}$$
$\square$

Lemma 3.4. *Suppose that $p \geq 3$. Let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathcal{F}_p(\theta) = 0$. Then*

$$\mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2} \iff \left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod p.$$

Proof. Since $f(\alpha) = \alpha^2 - k\alpha - 1 = 0$, we note that $\alpha^2 \equiv k\alpha + 1 \pmod p$, which implies that

$$\alpha^{2p} \equiv (k\alpha + 1)^p \pmod{p^2}. \tag{3.2}$$

Suppose first that $\mathcal{F}_p(\alpha) = \alpha^{2p} - k\alpha^p - 1 \equiv 0 \pmod{p^2}$. Observe then that

$$-k\alpha^p - 1 \equiv -\alpha^{2p} \pmod{p^2}. \tag{3.3}$$

Let

$$G(x) = f(x) = x^2 - kx - 1 \quad \text{and} \quad H(x) = \frac{-kx^p - 1 + (kx+1)^p}{p}.$$

Hence, $G(\alpha) \equiv 0 \pmod{p}$ and

$$\begin{aligned} pH(\alpha) &= -k\alpha^p - 1 + (k\alpha+1)^p \\ &\equiv -\alpha^{2p} + (k\alpha+1)^p \pmod{p^2} \quad \text{(from (3.3))} \\ &\equiv -\alpha^{2p} + \alpha^{2p} \pmod{p^2} \quad \text{(from (3.2))} \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

Thus, $G(x)$ and $H(x)$ are not coprime modulo p so that $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod{p}$ by Theorem 2.6(d).

Conversely, suppose that $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod{p}$. Then, we have by Theorem 2.6(d) that $G(x)$ and $H(x)$ are not coprime modulo p. In light of Lemma 3.3, we assume then, without loss of generality, that

$$pH(\alpha) = -k\alpha^p - 1 + (k\alpha+1)^p \equiv 0 \pmod{p^2}. \tag{3.4}$$

Hence,

$$\begin{aligned} \mathcal{F}_p(\alpha) &= \alpha^{2p} - k\alpha^p - 1 \\ &\equiv (k\alpha+1)^p - k\alpha^p - 1 \quad \text{(from (3.2))} \\ &\equiv (k\alpha^p+1) - k\alpha^p - 1 \pmod{p^2} \quad \text{(from (3.4))} \\ &\equiv 0 \pmod{p^2}, \end{aligned}$$

which completes the proof. □

Lemma 3.5. *Suppose that $p \geq 3$. Then*

$$p \textit{ is a } k\textit{-Wall–Sun–Sun prime} \iff \mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}.$$

Proof. We consider the three cases: $\delta_p \in \{0, -1, 1\}$.

Suppose first that $\delta_p = 0$. Then $k^2 + 4 \equiv 0 \pmod{p}$, so that $\alpha \equiv k/2 \pmod{p}$ and $(k/2)^2 \equiv -1 \pmod{p}$. Hence, $(k/2)^{2p} \equiv -1 \pmod{p^2}$ or, equivalently,

$$k^{2p} \equiv -2^{2p} \pmod{p^2}. \tag{3.5}$$

By Lemma 2.2, we have that p is not a k-Wall–Sun–Sun prime. We must show that $\mathcal{F}_p(\alpha) \not\equiv 0 \pmod{p^2}$. Assume, by way of contradiction, that

$$\mathcal{F}_p(\alpha) \equiv (k/2)^{2p} - k(k/2)^p - 1 \equiv -1 - k(k/2)^p - 1 \equiv 0 \pmod{p^2}.$$

Thus,

$$k^{p+1} \equiv -2^{p+1} \pmod{p^2}. \tag{3.6}$$

Squaring both sides of (3.6) yields

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

Note that $p \nmid k$ since $p \geq 3$. Therefore, $k^2 + 4 \equiv 0 \pmod{p^2}$ from (3.5) and (3.7), which contradicts the fact that $\mathcal{D}$ is squarefree, and completes the proof when $\delta_p = 0$.

Suppose next that $\delta_p = -1$. Assume first that p is a k-Wall–Sun–Sun prime. Then, since $\pi(p^2) = \pi(p)$, we conclude from Theorem 2.1(c), and Lemma 3.2(a)(c) that

$$(\alpha^{p+1} - 1)(\alpha^{p+1} + 1) \equiv \alpha^{2(p+1)} - 1 \equiv 0 \pmod{p^2}. \tag{3.8}$$

Note that $\alpha^{p+1} - 1 \not\equiv 0 \pmod{p}$ since $\alpha^{p+1} + 1 \equiv 0 \pmod{p}$ from Lemma 3.2(c). Therefore, we see from (3.8) that $\alpha^{p+1} + 1 \equiv 0 \pmod{p^2}$, or equivalently, that $\alpha^p \equiv -\alpha^{-1} \pmod{p^2}$. Hence,

$$\mathcal{F}_p(\alpha) = \alpha^{2p} - k\alpha^p - 1 \equiv \alpha^{-2} + k\alpha^{-1} - 1 \equiv -\frac{\alpha^2 - k\alpha - 1}{\alpha^2} \equiv 0 \pmod{p^2}.$$

Conversely, assume that $\mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}$. Since $\delta_p = -1$, we have that $f(x)$ is irreducible modulo p. Consequently, the only zeros of $f(x)$ in $(\mathbb{Z}/p^2\mathbb{Z})[\sqrt{\mathcal{D}}]$ are α and $\beta = -\alpha^{-1}$. Hence,

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

If $\alpha^p \equiv \alpha \pmod{p^2}$, then, from Lemma 3.2(c), we have that

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

which implies that $k^2 + 2 \equiv 0 \pmod{p}$, and either $p \mid k$ or $k^2 + 4 \equiv 0 \pmod{p}$. In either case, we arrive at the contradiction that $p = 2$. Hence,

$$\alpha^p \equiv \beta \equiv -\alpha^{-1} \pmod{p^2} \quad \text{or equivalently,} \quad \alpha^{p+1} \equiv -1 \pmod{p^2}.$$

Thus, $\alpha^{2(p+1)} \equiv 1 \pmod{p^2}$ so that

$$2(p+1) \equiv 0 \pmod{\operatorname{ord}_{p^2}(\alpha)}.$$

By Lemma 3.2(a) and Theorem 2.1(a), we have that

$$\mathrm{ord}_{p^2}(\alpha) = \pi(p^2) \in \{\pi(p), p\pi(p)\}.$$

Therefore, we see that $\pi(p^2) = p\pi(p)$ is impossible since $p^2-1 \not\equiv 0 \pmod{p}$. Consequently, $\pi(p^2) = \pi(p)$, which implies that p is a k-Wall–Sun–Sun prime.

Finally, suppose that $\delta_p = 1$. Assume first that p is a k-Wall–Sun–Sun prime. Since $\pi(p^2) = \pi(p)$, it follows from Theorem 2.1(b), and Lemma 3.2(a)(b) that

$$\alpha^{p-1} \equiv 1 \pmod{p^2} \quad \text{or equivalently,} \quad \alpha^p \equiv \alpha \pmod{p^2}.$$

Thus, since $f(\alpha) = \alpha^2 - k\alpha - 1 = 0$, we have that

$$\mathcal{F}_p(\alpha) = \alpha^{2p} - k\alpha^p - 1 \equiv \alpha^2 - k\alpha - 1 \equiv 0 \pmod{p^2}.$$

Conversely, assume that $\mathcal{F}_p(\alpha) \equiv 0 \pmod{p^2}$. Since $f(\alpha) = \alpha^2 - k\alpha - 1 = 0$, we have that

$$\alpha + \frac{1}{\alpha} = 2\alpha - k. \tag{3.9}$$

Additionally, note that

$$\widehat{\alpha} = \alpha - \frac{f(\alpha)}{f'(\alpha)} = \alpha - \frac{\alpha^2 - k\alpha - 1}{2\alpha - k} = \frac{\alpha^2 + 1}{2\alpha - k}$$

is the Hensel lift modulo p^2 of α, so that $f(\widehat{\alpha}) \equiv 0 \pmod{p^2}$. Then, since

$$\mathcal{F}_p(\alpha) = (\alpha^p)^2 - k(\alpha^p) - 1 \equiv 0 \pmod{p^2},$$

it follows that

$$\alpha^p \equiv \frac{\alpha^2 + 1}{2\alpha - k} \pmod{p^2},$$

which implies that

$$\alpha^{p-1} \equiv \frac{\alpha + 1/\alpha}{2\alpha - k} \equiv 1 \pmod{p^2}$$

from (3.9). Hence, $p - 1 \equiv 0 \pmod{\mathrm{ord}_{p^2}(\alpha)}$. By Lemma 3.2(a) and Theorem 2.1(a), we have that

$$\mathrm{ord}_{p^2}(\alpha) = \pi(p^2) \in \{\pi(p), p\pi(p)\}.$$

Therefore, we see that $\pi(p^2) = p\pi(p)$ is impossible since $p-1 \not\equiv 0 \pmod{p}$. Consequently, $\pi(p^2) = \pi(p)$, which implies that p is a k-Wall–Sun–Sun prime. □

Combining Lemmas 3.4 and 3.5 yields the following.

Lemma 3.6. *Suppose that $p \geq 3$. Let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathcal{F}_p(\theta) = 0$. Then*

$$p \text{ is a } k\text{-Wall–Sun–Sun prime} \quad \Longleftrightarrow \quad \left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod{p}.$$

We are now in a position to provide a proof of the main result.

Proof of Theorem 1.1. We first investigate the monogenicity of $\mathcal{F}_p(x)$. Let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathcal{F}_p(\theta) = 0$. Recall from Proposition 2.5 that

$$\Delta(\mathcal{F}_p) = (-1)^{(p+1)(2p-1)} p^{2p} (k^2 + 4)^p.$$

Let $q \neq p$ be a prime divisor of $\Delta(\mathcal{F}_p)$. Then $k^2 + 4 \equiv 0 \pmod{q}$. Suppose first that $q \geq 3$. Then $q \nmid kp$, and we use Theorem 2.6(e) to address q. Since $\mathcal{D}$ is squarefree, we deduce that $q^2 \nmid D/p^2$, and therefore, $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{q}$. Suppose next that $q = 2$. Then $2 \mid k$, and we use Theorem 2.6(b) to address q. Since $B_1 = 0$, the first condition fails. However, since $4 \nmid k$, we see that $2 \nmid A_2$, and so the second condition is satisfied. Hence, $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{2}$.

Thus, we have shown that the monogenicity of $\mathcal{F}_p(x)$ is completely determined by the prime p. More explicitly, we have that

$$\mathcal{F}_p(x) \text{ is monogenic} \quad \Longleftrightarrow \quad \left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{p}.$$

Consequently, if $p \geq 3$, then the theorem follows from Lemma 3.6.

We now address the case $p = 2$. Recall that $4 \nmid k$. We examine the two subcases: $k \equiv 2 \pmod{4}$ and $k \equiv 1 \pmod{2}$.

If $k \equiv 2 \pmod{4}$, then $k^2 + 4 \equiv 0 \pmod{2}$ and $p = 2$ is not a k-Wall–Sun–Sun prime by Lemma 2.2. Since $2 \mid k$, we apply Theorem 2.6(b), and use the same argument as used above, to deduce that $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{2}$. Therefore, the theorem is established when $p = 2$ and $k \equiv 2 \pmod{4}$.

If $k \equiv 1 \pmod{2}$, then straightforward computations reveal that $\pi(4) = 6$ and $\pi(2) = 3$. Hence, $p = 2$ is not a k-Wall–Sun–Sun prime in this subcase as well, and we must show that $\mathcal{F}_2(x)$ is monogenic. We use Theorem 2.6(d) with $q = p = 2$ to see that

$$G(x) = x^2 - kx - 1 \quad \text{and} \quad H(x) = \frac{-kx^2 - 1 + (kx+1)^2}{2} = kx\left(\frac{k-1}{2}x + 1\right).$$

Since $G(x)$ is irreducible in $\mathbb{F}_2[x]$, it follows that $G(x)$ and $H(x)$ are coprime in $\mathbb{F}_2[x]$. Hence, $\mathcal{F}_2(x)$ is monogenic in this case, which completes the proof of the main statement of the theorem.

Furthermore, it then follows immediately from Lemma 2.2 that $\mathcal{F}_p(x)$ is monogenic if p is a prime divisor of $k^2 + 4$. $\square$

References

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

[2] ———, *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*, Grad. Texts in Math. **138**, Springer-Verlag, Berlin, 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] 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.

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

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

[8] L. Jones, *A connection between the monogenicity of certain power-compositional trinomials and k-Wall–Sun–Sun primes*, arXiv:2211.14834.

[9] ———, *Generalized Wall–Sun–Sun primes and monogenic power-compositional trinomials*, Albanian J. Math. **17** (2023), no. 2, 3–17.

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

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

[12] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia Math. Appl. **77**, Cambridge University Press, Cambridge, 2000.

[13] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), no. 4, 371–388.

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

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

[16] *Wall–Sun–Sun prime*, https://en.wikipedia.org/wiki/Wall–Sun–Sun_prime.

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

Lenny Jones
Professor Emeritus, Department of Mathematics, Shippensburg University,
Shippensburg, Pennsylvania 17257, USA
E-mail address: doctorlennyjones@gmail.com