Bull. Aust. Math. Soc. **108** (2023), 373–378
doi:10.1017/S0004972723000138

A NOTE ON GENERALISED WALL–SUN–SUN PRIMES

JOSHUA HARRINGTON and LENNY JONES

(Received 30 November 2022; accepted 16 January 2023; first published online 28 February 2023)

Abstract

Let a and b be positive integers and let $\{U_n\}_{n\geq 0}$ be the Lucas sequence of the first kind defined by

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

We define an (a, b)-*Wall–Sun–Sun prime* to be a prime p such that $\gcd(p, b) = 1$ and $\pi(p^2) = \pi(p)$, where $\pi(p) := \pi_{(a,b)}(p)$ is the length of the period of $\{U_n\}_{n\geq 0}$ modulo p. When $(a, b) = (1, 1)$, such primes are known in the literature simply as *Wall–Sun–Sun primes*. In this note, we provide necessary and sufficient conditions such that a prime p dividing $a^2 + 4b$ is an (a, b)-Wall–Sun–Sun prime.

2020 *Mathematics subject classification*: primary 11B39; secondary 11A41.

Keywords and phrases: Wall–Sun–Sun prime, Fibonacci–Wieferich prime, Lucas sequence.

1. Introduction

Throughout this note, for positive integers a and b, we let $\{U_n\}_{n\geq 0}$ be the Lucas sequence of the first kind [6] 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 $\{U_n\}_{n\geq 0}$ is periodic modulo any prime p with $\gcd(p, b) = 1$, and we denote by $\pi(p) := \pi_{(a,b)}(p)$ the length of the period of $\{U_n\}_{n\geq 0}$ modulo p.

We define an (a, b)-*Wall–Sun–Sun prime* to be a prime p such that

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

An $(a, 1)$-Wall–Sun–Sun prime is also known in the literature as an a-*Wall–Sun–Sun prime* [10] or an a-*Fibonacci–Wieferich prime*. Note that when $(a, b) = (1, 1)$, the sequence $\{U_n\}_{n\geq 0}$ is the well-known Fibonacci sequence. In this case, such primes are referred to simply as *Wall–Sun–Sun primes* [3, 10] or *Fibonacci–Wieferich* primes [11]. However, at the time this note was written, no Wall–Sun–Sun primes were known to exist. The existence of Wall–Sun–Sun primes was first investigated by Wall [9] in 1960, and subsequently studied by the Sun brothers [8], 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.

For an a-Wall–Sun–Sun prime p, it can be shown [4, 5] that the following conditions are equivalent:

(1) $\pi(p^2) = \pi(p)$;
(2) $U_{\pi(p)} \equiv 0 \pmod{p^2}$;
(3) $U_{p-\delta_p} \equiv 0 \pmod{p^2}$, where δ_p is the Legendre symbol $(\frac{a^2+4}{p})$.

Because of this equivalence, various authors have chosen to use either item (2) or item (3) for the definition of an a-Wall–Sun–Sun prime. However, for the more general (a, b)-Wall–Sun–Sun prime p, it turns out that, while item (1) implies the still-equivalent items (2) and (3), the converse is false in general. For example, with $(a, b) = (5, 8)$ and $p = 7$, an easy calculation shows that items (2) and (3) are true, but item (1) is false since $\pi(49) = 42$ and $\pi(7) = 6$. Because of this phenomenon, and the fact that Wall [9] was originally concerned with the impossibility of item (1) in the Wall–Sun–Sun situation, we have chosen to adopt (1.2) as our definition of an (a, b)-Wall–Sun–Sun prime.

This note is motivated in part by recent results of Bouazzaoui [1, 2] which show, under certain restrictions on a, b and p, that an odd prime p is an (a, b)-Wall–Sun–Sun prime if and only if $\mathbb{Q}(\sqrt{a^2 + 4b})$ is not p-rational. We recall that a number field K is *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.

A second motivation for this note is recent work of the second author which, again under certain restrictions on a and p, establishes a connection between $(a, 1)$-Wall–Sun–Sun primes p and the monogenicity of certain power-compositional trinomials [5].

One restriction imposed on p in the work of these motivational articles is that $a^2 + 4b \not\equiv 0 \pmod{p}$. In this note, our focus is on primes p that divide $a^2 + 4b$, and in this case, we provide necessary and sufficient conditions so that p is an (a, b)-Wall–Sun–Sun prime. More precisely, we prove the following result.

THEOREM 1.1. *Let a and b be positive integers and let p be a prime divisor of $a^2 + 4b$ such that* $\gcd(p, b) = 1$. *Let* $(a, b)_m := (a \bmod m, b \bmod m)$. *Then*

- *$p = 2$ is an (a, b)-Wall–Sun–Sun prime if and only if $(a, b)_4 = (0, 1)$;*
- *$p = 3$ is an (a, b)-Wall–Sun–Sun prime if and only if*

$$(a, b)_9 \in \{(1, 8), (2, 5), (4, 2), (5, 2), (7, 5), (8, 8)\};$$

- *$p \geq 5$ is never an (a, b)-Wall–Sun–Sun prime.*

2. Proof of Theorem 1.1

Note that the sequence $\{U_n\}_{n\geq 0}$ from (1.1) is explicitly

$$\{U_n\} = [0, 1, a, a^2 + b, a^3 + 2ab, a^4 + 3a^2 b + b^2, a^5 + 4a^3 b + 3ab^2, \ldots]. \tag{2.1}$$

We let $\{U_n\}_p$ denote the sequence (2.1) modulo the prime p.

https://doi.org/10.1017/S0004972723000138 Published online by Cambridge University Press

We first address the prime $p = 2$. Since $a^2 + 4b \equiv 0 \pmod 2$, it follows that $a \equiv 0 \pmod 2$. Then, since $\gcd(p, b) = 1$, we see from (2.1) that

$$\{U_n\}_2 = [0, 1, 0, 1, \ldots] \quad \text{and} \quad \{U_n\}_4 = [0, 1, a, b, 0, b^2 \ldots].$$

Thus, $\pi(2) = 2$ and $\pi(4) = 2$ if and only if $(a, b)_4 = (0, 1)$, which finishes the case $p = 2$.

Next, let $p = 3$. Since $a^2 + 4b \equiv 0 \pmod 3$, we see that $a^2 \equiv -b \pmod 3$. Since $\gcd(3, b) = 1$, we deduce that $b \equiv 2 \pmod 3$ and $a^2 \equiv 1 \pmod 3$. Hence, from (2.1),

$$\{U_n\}_3 = [0, 1, a, 0, 2a, 2, 0, 1, \ldots],$$

where $a \equiv 1, 2 \pmod 3$. We conclude that

$$\pi(3) = \begin{cases} 6 & \text{if } a \equiv 1 \pmod 3, \\ 3 & \text{if } a \equiv 2 \pmod 3. \end{cases}$$

Observe that $\pi(9) = 3$ if and only if

$$U_3 = a^2 + b \equiv 0 \pmod 9 \quad \text{and} \quad U_4 = aU_3 + bU_2 \equiv ba \equiv 1 \pmod 9.$$

Since $b \bmod 9 \in \{2, 5, 8\}$, it follows that

$$\pi(9) = 3 \quad \text{if and only if } (a, b)_9 \in \{(2, 5), (5, 2), (8, 8)\}.$$

If $\pi(9) = 6$, then

$$U_6 = a^5 + 4a^3b + 3ab^2 = a(a^2 + b)(a^2 + 3b) \equiv 0 \pmod 9,$$

which implies that $a^2 + b \equiv 0 \pmod 9$, since $a^2 + b \equiv 0 \pmod 3$ and $\gcd(3, b) = 1$. Hence, from (2.1), we have that

$$\{U_n\}_9 = [0, 1, a, 0, ab, a^2b, 0, a^2b^2, \ldots],$$

where $a^2b^2 \equiv 1 \pmod 9$. Thus,

$$ab \equiv -1 \pmod 9, \tag{2.2}$$

since we are assuming that $\pi(9) \neq 3$. Consequently,

$$\{U_n\}_9 = [0, 1, a, 0, -1, -a, 0, 1, \ldots].$$

Recall that $b \equiv 2 \pmod 3$. Then, for each $b \bmod 9 \in \{2, 5, 8\}$, solving (2.2) for a yields

$$\pi(9) = 6 \quad \text{if and only if } (a, b)_9 \in \{(1, 8), (4, 2), (7, 5)\},$$

which completes the proof when $p = 3$.

Finally, suppose that $p \geq 5$. Since

$$\pi(p^2) = \pi(p) \quad \text{implies } U_{\pi(p^2)} = U_{\pi(p)} \equiv 0 \pmod{p^2},$$

we show that $U_{\pi(p)} \not\equiv 0 \pmod{p^2}$ to establish that p is not an (a, b)-Wall–Sun–Sun prime.

https://doi.org/10.1017/S0004972723000138 Published online by Cambridge University Press

We claim that, for $n \geq 0$,

$$U_n \equiv \begin{cases} \dfrac{(-1)^{n/2} ab^{(n-4)/2} n(a^2(n^2-4)+4b(n^2-10))}{48} \pmod{p^2} & \text{if } n \text{ is even,} \\ \dfrac{(-1)^{(n+1)/2} b^{(n-3)/2} n(a^2(n^2-1)+4b(n^2-7))}{24} \pmod{p^2} & \text{if } n \text{ is odd.} \end{cases} \tag{2.3}$$

The proof is by induction on n. The claim is easily verified when $n \in \{0, 1, 2\}$. Since p divides $a^2 + 4b$, we see that p^2 divides $(a^2 + 4b)^2 = a^4 + 8a^2b + 16b^2$. It follows that

$$a^4 \equiv -8a^2b - 16b^2 \pmod{p^2}. \tag{2.4}$$

Suppose that the claim holds for all $n \leq t$ for some even integer t. Then, modulo p^2,

$$\begin{aligned} U_{t+1} &\equiv aU_t + bU_{t-1} \\ &\equiv a\frac{(-1)^{t/2} ab^{(t-4)/2} t(a^2(t^2-4)+4b(t^2-10))}{48} \\ &\quad + b\frac{(-1)^{t/2} b^{(t-4)/2} (t-1)(a^2(t^2-2t)+4b(t^2-2t-6))}{24} \\ &\equiv (-1)^{t/2} b^{(t-4)/2} \frac{a^4(t^3-4t)+6(t+2)(t-3)tba^2+8(t-1)(t^2-2t-6)b^2}{48} \\ &\equiv \frac{(-1)^{(t+2)/2} b^{(t-2)/2} (t+1)(a^2t(t+2)+4b(t^2+2t-6))}{24} \quad \text{(by (2.4))} \\ &\equiv \frac{(-1)^{((t+1)+1)/2} b^{((t+1)-3)/2} (t+1)(a^2((t+1)^2-1)+4b((t+1)^2-7))}{24} \end{aligned}$$

and

$$\begin{aligned} U_{t+2} &\equiv aU_{t+1} + bU_t \\ &\equiv a\frac{(-1)^{((t+1)+1)/2} b^{((t+1)-3)/2} (t+1)(a^2((t+1)^2-1)+4b((t+1)^2-7))}{24} \\ &\quad + b\frac{(-1)^{t/2} ab^{(t-4)/2} t(a^2(t^2-4)+4b(t^2-10))}{48} \\ &\equiv (-1)^{t/2} \frac{-ab^{(t-2)/2}(a^2(t+2)(t^2+4t)+4b(t+2)(t^2+t-6))}{48} \\ &\equiv \frac{(-1)^{(t+2)/2} ab^{((t+2)-4)/2} (t+2)(a^2((t+2)^2-4)+4b((t+2)^2-10))}{48}, \end{aligned}$$

which establishes the claim.

For brevity of notation, we let λ denote the order of $2^{-1}a$ modulo p. Then, since $\gcd(p, b) = 1$, it follows that $\pi(p) = p\lambda$ [7, Theorem 3(c)]. Since λ divides $p - 1$, it follows that $\gcd(p, \lambda) = 1$. To finish the proof, we must show that $U_{\pi(p)} \not\equiv 0 \pmod{p^2}$. We use (2.3).

https://doi.org/10.1017/S0004972723000138 Published online by Cambridge University Press

If $\lambda \equiv 0 \pmod 2$, then modulo p^2,

$$\begin{aligned}
U_{p\lambda} &\equiv \frac{(-1)^{p\lambda/2}ab^{(p\lambda-4)/2}p\lambda(a^2((p\lambda)^2-4)+4b((p\lambda)^2-10))}{48}\\
&\equiv \frac{(-1)^{p\lambda/2}ab^{(p\lambda-4)/2}p\lambda(a^2(-4)+4b(-10))}{48}\\
&\equiv \frac{(-1)^{\lambda(p+2)/2}4ab^{(p\lambda-4)/2}p\lambda(a^2+10b)}{48}.
\end{aligned}$$

Since $p \notin \{2,3\}$ and does not divide a, b or λ, if $U_{p\lambda} \equiv 0 \pmod{p^2}$, then p divides a^2+10b. However, since p divides a^2+4b, it follows that

$$a^2+10b \equiv 6b \not\equiv 0 \pmod p,$$

completing the proof in this case.

Suppose now that $\lambda \equiv 1 \pmod 2$. Then, modulo p^2,

$$\begin{aligned}
U_{p\lambda} &\equiv \frac{(-1)^{(p\lambda+1)/2}b^{(p\lambda-3)/2}p\lambda(a^2((p\lambda)^2-1)+4b((p\lambda)^2-7))}{24}\\
&\equiv \frac{(-1)^{(p\lambda+1)/2}b^{(p\lambda-3)/2}p\lambda(a^2(-1)+4b(-7))}{24}\\
&\equiv \frac{(-1)^{(p\lambda+3)/2}b^{(p\lambda-3)/2}p\lambda(a^2+28b)}{24}.
\end{aligned}$$

Reasoning as in the previous case, we see that $U_{p\lambda} \equiv 0 \pmod{p^2}$ if and only if $a^2+28b \equiv 0 \pmod p$. However, since $a^2+4b \equiv 0 \pmod p$, it follows that

$$a^2+28b \equiv 24b \not\equiv 0 \pmod p,$$

which completes the proof of the theorem.

Acknowledgement

The authors thank the anonymous referee for the suggestions that helped to improve the paper.

References

[1] Z. Bouazzaoui, 'Fibonacci numbers and real quadratic p-rational fields', *Period. Math. Hungar.* **81**(1) (2020), 123–133.

[2] Z. Bouazzaoui, 'On periods of Fibonacci sequences and real quadratic p-rational fields', *Fibonacci Quart.* **58**(5) (2020), 103–110.

[3] R. Crandall, K. Dilcher and C. Pomerance, 'A search for Wieferich and Wilson primes', *Math. Comp.* **66**(217) (1997), 433–449.

[4] A.-S. Elsenhans and J. Jahnel, 'The Fibonacci sequence modulo p^2—An investigation by computer for $p < 10^{14}$', Preprint, 2010, arXiv:1006.0824v1.

[5] L. Jones, 'A connection between the monogenicity of certain power-compositional trinomials and k-Wall–Sun–Sun primes', Preprint, 2022, arXiv:2211.14834.

[6] Lucas sequence, https://en.wikipedia.org/wiki/Lucas sequence, Wikipedia, 2023.

[7] M. Renault, 'The period, rank, and order of the (a, b)-Fibonacci sequence mod m', *Math. Mag.* **86**(5) (2013), 372–380.
[8] Z. H. Sun and Z. W. Sun, 'Fibonacci numbers and Fermat's last theorem', *Acta Arith.* **60**(4) (1992), 371–388.
[9] D. D. Wall, 'Fibonacci series modulo m', *Amer. Math. Monthly* **67** (1960), 525–532.
[10] Wall–Sun–Sun Prime, https://en.wikipedia.org/wiki/Wall–Sun–Sun prime, Wikipedia, 2022.
[11] Wieferich Prime, https://en.wikipedia.org/wiki/Wieferich prime, Wikipedia, 2023.

JOSHUA HARRINGTON, Department of Mathematics,
Cedar Crest College, Allentown, Pennsylvania, USA
e-mail: Joshua.Harrington@cedarcrest.edu

LENNY JONES, Professor Emeritus of Mathematics,
Department of Mathematics, Shippensburg University,
Shippensburg, PA 17257, USA
e-mail: doctorlennyjones@gmail.com

https://doi.org/10.1017/S0004972723000138 Published online by Cambridge University Press