Functiones et Approximatio
60.2 (2019), 167–175
doi: 10.7169/facm/1709

LUCAS NON-WIEFERICH PRIMES IN ARITHMETIC PROGRESSIONS

Sudhansu Sekhar Rout

Abstract: In this note, we define the Lucas Wieferich primes which are an analogue of the famous Wieferich primes. Conditionally there are infinitely many non-Wieferich primes. We prove under the assumption of the *abc* conjecture for the number field $\mathbb{Q}(\sqrt{\Delta})$ that for fixed positive integer M there are at least $O((\log x/\log\log x)(\log\log\log x)^M)$ many Lucas non-Wieferich primes $p \equiv 1 (\bmod\ k)$ for any fixed integer $k \geqslant 2$.

Keywords: Lucas–Wieferich primes, arithmetic progressions, *abc* conjecture.

1. Introduction

The first case of Fermat's last theorem (FLTI) is the statement that, for any odd prime p, the equation $x^p + y^p = z^p$ does not have integer solutions with $p \nmid xyz$. In 1909, Arthur Wieferich [21] showed that if FLTI fails for an odd prime exponent, then that prime must satisfy the congruence

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{1.1}$$

Subsequently, this result was extended to other primes. Specifically, Granville and Monagan [8] proved that if FLTI fails for prime p then p^2 divides $q^p - q$ for each successive prime q up to 89. A prime satisfying (1.1) is called Wieferich prime for base 2. Until now, we know of only two Wieferich primes for the base 2, that are 1093 and 3511 found respectively by Meissner in 1913 and Beegner in 1922. For any integer $a \geqslant 2$ and any prime p, if

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

then p is said to be Wieferich prime for base a. Otherwise, p is said to be non-Wieferich prime for base a. It is unknown whether there are finitely many or infinitely many Wieferich primes. It is not even known if there are infinitely many non-Wieferich primes. In 1986, Granville [7] proved the infinitude of non-Wieferich

2010 Mathematics Subject Classification: primary: 11B39, 11B25, 11A41

primes for the base 2 under the assumption of a conjecture of Mollin and Walsh on triples of powerful numbers. Silverman [16] proved under the assumption of the *abc* conjecture, that given any integer a, there are infinitely many non-Wieferich primes to the base a. In fact he proved this result by showing that for any fixed $a \in \mathbb{Q}^{\times},\ a \neq \pm 1$ and assuming *abc* conjecture,

$$\#\{\text{primes } p \leqslant x :\ a^{p-1} \not\equiv 1 \pmod{p^2}\} \gg_a \log x \qquad \text{as} \quad x \to \infty.$$

Dekoninck and Doyon in [5] proved the same result under a weaker assumption. Graves and Ram Murty [9] extended this result to primes in arithmetical progression by showing that for any $a \geqslant 2$ and any fixed $k \geqslant 2$, and assuming *abc* conjecture,

$$\#\{\text{primes } p \leqslant x :\ p \equiv 1 \pmod{k}, a^{p-1} \not\equiv 1 \pmod{p^2}\} \gg \frac{\log x}{\log\log x} \quad \text{as} \quad x \to \infty.$$

Recently Chen and Ding [3] studied the same question and improved the lower bound. In particular, they proved under the assumption of the *abc* conjecture, that for any positive integer M,

$$\#\{\text{primes } p \leqslant x :\ p \equiv 1 \pmod{k}, a^{p-1} \not\equiv 1 \pmod{p^2}\} \\ \gg \frac{\log x(\log\log\log x)^M}{\log\log x} \qquad \text{as} \quad x \to \infty.$$

For any integer $n > 1$, define the powerful part of n to be the product

$$\kappa(n) := \prod_{p : p^2 | n} p^{\mathrm{ord}_p(n)}.$$

The quotient $n/\kappa(n)$ is called the powerfree part of n.

2. Lucas–Wieferich primes

Let P and Q be the nonzero fixed integers with $\Delta := P^2 - 4Q \neq 0$ and $\gcd(P, Q) = 1$. Let α and β be the roots of the polynomial $x^2 - Px + Q$ with the convention that $|\alpha| > |\beta|$. The Lucas sequences of first and second kind for the roots α and β are given by

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n(P,Q) = \alpha^n + \beta^n, \qquad \text{for all} \ \ n = 0, 1, \ldots \quad (2.1)$$

respectively. When P and Q are implicitly understood, we are referring the terms of the Lucas sequence of first kind $U_n(P,Q)$ as U_n and second kind $V_n(P,Q)$ as V_n. The sequence $\{U_n\}$ is called non-degenerate, if α/β is not a root of unity. Further, non-degeneracy implies that $\mathbb{Q}(\alpha)$ is totally real. Throughout this paper, we assume that $\{U_n\}_{n\geqslant 0}$ and $\{V_n\}_{n\geqslant 0}$ are non-degenerate, and $\sqrt{\Delta} = (\alpha - \beta) > 0$. Let $\mu(p)$ denote the Legendre symbol $\left(\frac{\Delta}{p}\right)$. Recall that for $p \nmid \Delta$, the Legendre symbol $\left(\frac{\Delta}{p}\right) = 1$ if Δ is a quadratic residue modulo p and -1 otherwise. Given $m \in \mathbb{Z}$, let ρ be the least positive integer, if it exists, such that $m \mid U_\rho$. This value is called the *rank of apparition* of m, denoted by $\rho(m)$. For fixed prime p, we simply write ρ and μ to denote $\rho(p)$ and $\mu(p)$ respectively.

Fibonacci sequence $\{F_n\}_{n\geqslant 0}$ is an example of Lucas sequence of first kind for $(P,Q) = (1,-1)$ with initial conditions $F_0 = 0$ and $F_1 = 1$. The Lucas sequence of second kind for $(P,Q) = (1,-1)$, is also known as sequence of Lucas numbers and is denoted by $\{L_n\}_{n\geqslant 0}$ with initial conditions $L_0 = 2$ and $L_1 = 1$.

It is well-known (see [4, pp. 393-395]) that $F_{p-\left(\frac{5}{p}\right)}$ is divisible by p, where p is prime and $\left(\frac{5}{p}\right)$ denotes the Legendre symbol. If $F_{p-\left(\frac{5}{p}\right)}$ is divisible by p^2, then we call p a *Fibonacci–Wieferich prime* (these primes are sometimes called Wall–Sun–Sun primes). Sun and Sun [19] proved that if the first case of Fermat's last theorem fails for an odd prime p, then $F_{p-\left(\frac{5}{p}\right)} \equiv 0 \pmod{p^2}$.

Returning to the general Lucas Sequences $\{U_n\}$ and $\{V_n\}$, it is known that $U_{p-\mu}$ is divisible by p whenever p is a prime not dividing $2Q$ (see [2, Theorem XII], [17, Proposition 1(viii)]). A prime p is called a *Lucas–Wieferich prime* associated to the pair (P,Q) if

$$U_{p-\mu} \equiv 0 \pmod{p^2}. \tag{2.2}$$

Every Wieferich prime is a Lucas Wieferich prime associated to the pair $(3,2)$ [12]. Ribenboim [14] proved under the hypothesis of the *abc* conjecture that there are infinitely many Lucas non-Wieferich primes.

The objective of this paper is to show that, for fixed P,Q and for fixed integer $k \geqslant 2$, there are infinitely many Lucas non-Wieferich primes p with $p \equiv 1 \pmod{k}$ under the assumption of *abc* conjecture for the number field $\mathbb{Q}(\sqrt{\Delta})$. Our proof closely follow the papers of Chen and Ding [3] and Graves and Ram Murty [9].

Theorem 2.1. *Let $K = \mathbb{Q}(\sqrt{\Delta})$ be a real quadratic field and assume that abc conjecture holds in K. Let $k \geqslant 2$ be any fixed integer. Then for any positive integer M, we have*

$$\#\{\text{primes } p \leqslant x : p \equiv 1 \ (mod\ k), U_{p-\mu} \not\equiv 0 \ (mod\ p^2)\} \gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

3. Preliminaries

In this section, we briefly reproduce some notations related to Lucas sequences and some related results. Firstly, we list some known identities for Lucas sequences which we use later.

Lemma 3.1 ([18]). *For the sequences $\{U_n\}_{n\geqslant 0}$ and $\{V_n\}_{n\geqslant 0}$, we have the following:*

1. $V_n^2 - \Delta U_n^2 = 4Q^n$ *for all* $n \geqslant 0$,
2. $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$ *for all* $n \geqslant 1$,
3. $\gcd(U_n, U_m) = U_{\gcd(n,m)}$ *for all* $n, m \geqslant 0$,

Lemma 3.2. *Let $\{U_n\}_{n\geqslant 0}$ be a Lucas sequence of first kind and ρ be the rank of apparition of p. Then*

1. *for $n \in \mathbb{N}$,*
$$p \mid U_n \Leftrightarrow \rho \mid n.$$
2. *Moreover, if $p \mid U_n$ then*
$$v_p(U_n) = v_p\left(\frac{n}{\rho}\right) + v_p(U_\rho). \tag{3.1}$$

Proof. For the proof of first statement (see [1, Corollary 2.2]) and second relation follows from Proposition 2.1 in [1]. ∎

Corollary 3.3. *Let p be a prime coprime to $2Q$. Suppose $U_n \equiv 0 \pmod p$ and $U_n \not\equiv 0 \pmod{p^2}$. Then $U_{p-\mu} \equiv 0 \pmod p$ and $U_{p-\mu} \not\equiv 0 \pmod{p^2}$.*

Proof. Since $p \| U_n$, we have $v_p(U_n) = 1$ and $v_p(U_\rho) \geqslant 1$. This implies $v_p\left(\frac{n}{\rho}\right) = 0$ and $v_p(U_\rho) = 1$. Now from (3.1), we have
$$v_p(U_{p-\mu}) = v_p\left(\frac{p-\mu}{\rho}\right) + v_p(U_\rho) = 1.$$
∎

Lemma 3.4. *For sufficiently large n, we have*
$$|\alpha|^{n/2} < |U_n| \leqslant 2|\alpha|^n.$$

Proof. From (2.1), we have
$$|U_n| = \left|\frac{\alpha^n - \beta^n}{\alpha - \beta}\right| \leqslant \frac{|\alpha|^n + |\beta|^n}{|\alpha - \beta|} < 2|\alpha|^n.$$
For the proof of lower bound refer [6, Theorem 2.3]. ∎

3.1. *abc* conjecture for number field [10, 20]

At first we define the radical then relate this to the number field radical. For relatively prime nonzero integers a, b, c, define the radical
$$\mathrm{rad}(a, b, c) = \mathrm{rad}(abc)$$
where $\mathrm{rad}(m)$ is the product of all distinct prime divisors of m. Now we consider all triples $r, s, t \in \mathbb{Q} \setminus \{0\}$ satisfying $r + s = t$. Every such triple is proportional to a triple of the form $(q, 1-q, 1)$ where $q \in \mathbb{Q} \setminus \{0, 1\}$ and to a triple (a, b, c) of nonzero relatively prime integers such that $a + b = c$. We define the radical of a single rational number $q \in \mathbb{Q} \setminus \{0, 1\}$ by $\mathrm{rad}(q) := \mathrm{rad}(a, b, c)$. Equivalently, $\mathrm{rad}(q)$ is the product of all prime numbers p satisfying $v_p(q(1-q)) \neq 0$.

Let K be an algebraic number field and $\mathcal{O}_K$ be its ring of integers. Let V_K be the set of places on K, that is $v \in V_K$ is an equivalence class of non-trivial norms on K (finite or infinite). For $v \in V_K$, we choose an absolute value $\|\cdot\|_v$ in the following way: if v is finite place corresponding to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, then we put $\|x\|_v = N_{K/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$ for $x \in K \setminus \{0\}$ and $\|0\|_v = 0$ where $v_{\mathfrak{p}}$ is the corresponding valuation; if v is infinite and corresponds to $\sigma : K \to \mathbb{C}$, then we put $\|x\|_v = |\sigma(x)|^e$ for $x \in K$ where $e = 1$ if $\sigma(K) \subset \mathbb{R}$ and $e = 2$ otherwise. Then *height* of any triple $(a, b, c) \in (K^*)^3$ is defined as

$$H_K(a,b,c) = \prod_{v \in V_K} \max(\|a\|_v, \|b\|_v, \|c\|_v),$$

and the *radical* of (a, b, c) as

$$\mathrm{rad}_K(a,b,c) = \prod_{\mathfrak{p} \in I_K(a,b,c)} N_{K/\mathbb{Q}}(\mathfrak{p})^{v_{\mathfrak{p}}(p)},$$

where p is a rational prime with $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ and $I_K(a, b, c)$ is the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ for which $\|a\|_v, \|b\|_v, \|c\|_v$ are not equal. Now one can easily verify that $\mathrm{rad}_K(a, b, c) = \mathrm{rad}(a, b, c)$ if $K = \mathbb{Q}$. Finally, the statement of *abc* conjecture for number field is as follows:

Conjecture 3.5. *For any $\epsilon > 0$, there exists a positive constant $C_{K,\epsilon}$ depending on K, ϵ, such that for all $a, b, c \in K^*$ satisfying $a + b + c = 0$, we have*

$$H_K(a,b,c) \leqslant C_{K,\epsilon}(rad_K(a,b,c))^{1+\epsilon}. \tag{3.2}$$

For $K = \mathbb{Q}$, this reduces to the Oesterlé–Masser conjecture.

Definition 3.6. For any integer $m \geqslant 1$, the m-th cyclotomic polynomial can be defined as

$$\Phi_m(x) = \prod_{\substack{(d,m)=1 \\ 0<d<m}} (X - \zeta_m^d), \tag{3.3}$$

where ζ_m is a primitive m-th root of unity. We have

$$X^m - 1 = \prod_{d|m} \Phi_d(X). \tag{3.4}$$

Lemma 3.7 ([13, p.233]). *If $p \mid \Phi_n(b)$, then either $p \mid n$ or $p \equiv 1 \pmod{n}$.*

Lemma 3.8 ([15, Proposition 2.4]). *For any real number b with $|b| > 1$, there exists $C > 0$ such that*

$$|\Phi_n(b)| \geqslant C \cdot |b|^{\phi(n)},$$

where $\phi(n)$ is Euler's totient function.

Lemma 3.9 ([11, Theorem 437]). *Let $\pi_m(x)$ denote the number of squarefree integers which do not exceed x and have exactly m prime factors. Then*

$$\pi_m(x) \sim \frac{x(\log\log x)^m}{(m-1)!\log x}.$$

We write $U_n = X_n Y_n$ where X_n is the squarefree part of U_n and Y_n is the powerful part of U_n. By Corollary 3.3, p is a *Lucas non-Wieferich prime* if $p \mid X_n$ for some n. Define

$$X_n' = \gcd(X_n, \Phi_n(\alpha/\beta)) \qquad \text{and} \qquad Y_n' = \gcd(Y_n, \Phi_n(\alpha/\beta)).$$

One can easily show that $X_n' Y_n' = \Phi_n(\alpha/\beta) = \Phi_n(\alpha^2/Q)$. Let p_i be the ith prime. For $n \geqslant 2$, let

$$\delta_n := \prod_{p|n}\left(1 - \frac{1}{p}\right) \qquad \text{and} \qquad \widetilde{\delta}_n := \prod_{i=1}^{n}\left(1 - \frac{1}{p_i}\right).$$

Lemma 3.10. *Suppose the abc conjecture for number field $\mathbb{Q}(\sqrt{\Delta})$ holds. Then for any $\epsilon > 0$,*

$$|Q|^{\phi(n)} X_n' \gg |U_n|^{2(\delta_n - \epsilon)}.$$

Proof. From (2.1) we have,

$$\sqrt{\Delta} U_n - \alpha^n + \beta^n = 0.$$

Then we use *abc* conjecture for $K = \mathbb{Q}(\sqrt{\Delta})$. By (3.2), for any $\epsilon > 0$, there exists a constant C_ϵ such that

$$H(\sqrt{\Delta}U_n, -\alpha^n, \beta^n) \leqslant C_\epsilon (\mathrm{rad}(\sqrt{\Delta}U_n, -\alpha^n, \beta^n))^{1+\epsilon}. \tag{3.5}$$

Now from the definition of the height, we have

$$\begin{aligned} H(\sqrt{\Delta}U_n, -\alpha^n, \beta^n) &\geqslant \max\{|\sqrt{\Delta}U_n|, |-\alpha^n|, |\beta^n|\} \cdot \max\{|-\sqrt{\Delta}U_n|, |-\beta^n|, |\alpha^n|\} \\ &\geqslant |\sqrt{\Delta}U_n| \cdot |-\sqrt{\Delta}U_n| = \Delta U_n^2 = \Delta X_n^2 Y_n^2. \end{aligned} \tag{3.6}$$

We shall now estimate $\mathrm{rad}(\sqrt{\Delta}U_n, -\alpha^n, \beta^n)$ in the right hand side of (3.5). Since $\alpha\beta = Q, \mathrm{rad}(Y_n) \leqslant \mathrm{rad}(\sqrt{Y_n})$ and $v_{\mathfrak{p}}(p) \leqslant 2$ for any prime ideal $\mathfrak{p}$ lying above the rational prime p, we have

$$\mathrm{rad}(\sqrt{\Delta}U_n, -\alpha^n, \beta^n) = \prod_{\mathfrak{p}|Q\sqrt{\Delta}U_n} N_{K/\mathbb{Q}}(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leqslant Q^2 \Delta X_n^2 Y_n. \tag{3.7}$$

Thus from (3.5), (3.6) and (3.7), we obtain

$$\Delta(X_n Y_n)^2 \leqslant C_\epsilon (Q^2 \Delta X_n^2 Y_n)^{1+\epsilon}$$

and hence

$$Y_n \ll_{\epsilon,\Delta} U_n^{2\epsilon}. \tag{3.8}$$

From Lemma 3.8,

$$|X_n' Y_n'| = |\Phi_n(\alpha^2/Q)| \geqslant C \left|\frac{\alpha^2}{Q}\right|^{\phi(n)}.$$

Using the Lemma 3.4,

$$|X'_n Y'_n| \geqslant C \left|\frac{\alpha^2}{Q}\right|^{\phi(n)} = C \left|\frac{\alpha^2}{Q}\right|^{n\delta_n} \geqslant C_1 \cdot |U_n|^{2\delta_n} \cdot \left(\frac{1}{|Q|}\right)^{\phi(n)}. \tag{3.9}$$

Thus, from (3.8) and (3.9),

$$|X'_n U_n^{2\epsilon}| \geqslant |X'_n Y'_n| \geqslant C_1 \cdot |U_n|^{2\delta_n} \cdot \left(\frac{1}{|Q|}\right)^{\phi(n)},$$

which will further simplify to

$$|X'_n| \gg |U_n|^{2(\delta_n - \epsilon)} \left(\frac{1}{|Q|}\right)^{\phi(n)}. \qquad \blacksquare$$

The following lemma is very essential to prove our theorem.

Lemma 3.11. *If* $m < n$, *then* $\gcd(X'_m, X'_n) = 1$.

Proof. On the contrary suppose $p \mid X'_m$ and $p \mid X'_n$ for $m < n$ and suppose $\gcd(m,n) = d$. Then $p \mid \Phi_m(\alpha/\beta)$ and $p \mid \Phi_n(\alpha/\beta)$. Thus, $p \mid U_m$ and $p \mid U_n$. Since $\gcd(U_m, U_n) = U_{\gcd(m,n)} = U_d$, we have $p \mid U_d$. Also,

$$\frac{U_n}{U_d} = \beta^{n-d} \frac{(\alpha/\beta)^n - 1}{(\alpha/\beta)^d - 1}, \tag{3.10}$$

and it follows that $\Phi_n(\alpha/\beta) | (U_n/U_d)$, hence $p \mid (U_n/U_d)$. By writing $U_n = (U_n/U_d)U_d$, we conclude that $p^2 \mid U_n$. This is a contradiction as $p \mid X'_n$. Thus $\gcd(X'_m, X'_n) = 1$. $\blacksquare$

In the following, we fix integers k, M with $k \geqslant 2$ and $M \geqslant 1$. Let T_M be the set of all squarefree integers with exactly M prime factors.

Lemma 3.12. *Suppose that abc conjecture for number field* $\mathbb{Q}(\sqrt{\Delta})$ *is true and* $n \in T_M$. *Then there exists an integer* c_0 *depending only on* α, k, M *such that for* $n \geqslant c_0$, *we have* $|Q|^{\phi(nk)}|X'_{nk}| > nk$.

Proof. Suppose $\epsilon = \widetilde{\delta}_M \phi(k)/3k$. From Lemma 3.10, we have

$$|Q|^{\phi(nk)}|X'_{nk}| \gg |U_{nk}|^{2(\delta_{nk} - \epsilon)}. \tag{3.11}$$

Since $\phi(nk) = \phi(n)\phi(k)\frac{g}{\phi(g)}$, where $g = \gcd(k,n)$ we have $\phi(nk) \geqslant \phi(n)\phi(k)$. By Lemma 3.4,

$$|U_{nk}|^{2(\delta_{nk} - \epsilon)} > |\alpha|^{nk(\delta_{nk} - \epsilon)} \geqslant |\alpha|^{(n\widetilde{\delta}_M \phi(k) - nk\epsilon)} = |\alpha|^{2nk\epsilon} \tag{3.12}$$

as $n \in T_M$. Thus,

$$|Q|^{\phi(nk)}|X'_{nk}| \gg |\alpha|^{2nk\epsilon} \gg |\alpha|^{2nk\epsilon - \log(nk)/\log|\alpha|} nk. \tag{3.13}$$

Therefore, there exists an integer c_0 depending only on α, k, M such that, if $n \in T_M$ with $n \geqslant c_0$, then $|Q|^{\phi(nk)}|X'_{nk}| > nk$. $\blacksquare$

4. The proof of Theorem 2.1

First we show that there exists a prime p_n such that

$$p_n \mid X'_{nk}, \qquad p_n \equiv 1 \pmod{nk}, \qquad U_{p-\mu} \not\equiv 0 \pmod{p_n^2}. \tag{4.1}$$

Let c_0 be as in Lemma 3.12 and $n \in T_M$ with $n \geqslant c_0$. By Lemma 3.1(2) and 3.12, and X'_{nk} being squarefree, there is a prime p_n such that $p_n \mid X'_{nk}$ and $p_n \nmid nk$. Since $X'_{nk} \mid \Phi_{nk}(\alpha/\beta)$, it follows from Lemma 3.7 that $p_n \equiv 1 \pmod{nk}$. Since $p_n \mid X'_{nk}$, $X'_{nk} \mid X_{nk}$ by Corollary 3.3, we have $U_{p-\mu} \not\equiv 0 \pmod{p_n^2}$. From Lemma 3.11, primes p_n are distinct when $n \in T_M$ and $n \geqslant c_0$. By Lemma 3.4, we have $|\alpha|^{nk/2} \leqslant |U_{nk}|$ for $n \geqslant c_1$ where c_1 is a positive integer. Thus $|U_{nk}| \leqslant x$ if and only if

$$n \leqslant \frac{2\log x}{k \log |\alpha|}.$$

Now $|U_{nk}| \leqslant x$ and $n \in T_M$ if and only if

$$n \leqslant \frac{2\log x}{k \log |\alpha|}, \qquad n \in T_M.$$

From Lemma 3.9 the number of integers n with $|U_{nk}| \leqslant x, n \in T_M$ and $n \geqslant c_2 := \max(c_0, c_1)$ is

$$\gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

Therefore,

$$\#\{\text{primes } p \leqslant x : p \equiv 1 \pmod{k}, U_{p-\mu} \not\equiv 0 \pmod{p^2}\} \gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

This completes the proof of Theorem 2.1.

Acknowledgment. The author is grateful to the anonymous referee for his/her valuable suggestions which improved the quality of this manuscript and also the author thank Professor Shanta Laishram for his useful suggestions during the preparation of this manuscript.

References

[1] Y. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte*, J. Reine Angew. Math. **539** (2001), 75–122.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **15**(1–4) (1913/14), 30–70.

[3] Y. Chen and Y. Ding, *Non-Wieferich primes in arithmetic progressions*, Proc. Amer. Math. Soc. **145** (2017), 1833–1836.

[4] L. E. Dickson, *The History of the Theory of Numbers*, vol. 1, reprinted: Chelsea Publishing Company, New York, 1966.

[5] J. M. Dekonick and N. Doyon, *On the set of Wieferich primes and its complement*, Anna. Univ. Sci. Budapest, Sect. Comput. **27** (2007), 3–13.

[6] G. Everest, A. van der Poorten, I. E. Shparlinski and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, Volume 104, American Mathematical Society, Providence, RI, 2003.

[7] A. Granville, *Powerful numbers and Fermat's last theorem*, C. R. Math. Rep. Acad. Sc. Canada **8** (1986), 215–218.

[8] A. Granville and M. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714, 591, 416, 091, 389, Trans. Amer. Math. Soc. **306** (1988), 329–359.

[9] H. Graves and M. R. Murty, *The abc conjecture and non-Wieferic primes in arithmetic progressions*, *J. Number Theory* **133** (2013), 1809–1813.

[10] K. Győry, *On the abc conjecture in algebraic number fields*, Acta. Arith. **133** (2008), 281–295.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, The Clarendon Press, Oxford University Press, New York, 1979.

[12] R. J. McIntosh and E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087–2094.

[13] M. R. Murty, *Problems in Analytic Number Theory*, second edition, Grad. Texts. in Math., Springer, 2008.

[14] P. Ribenboim, *On square factors of terms of binary recurring sequences and the abc conjecture*, Publ. Math. Debrecen **59** (2001), 459–469.

[15] S. S. Rout, *Balancing non-Wieferich primes in arithmetic progression and abc conjecture*, Proc. Japan Acad. Ser. A Math. Sci. **92**(9) (2016), 112–116.

[16] J. Silverman, *Wieferich's criterion and the abc conjecture*, J. Number Theory **30** (1988), 226–237.

[17] L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, in Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), pages 515–525, Kluwer Acad. Publ., Dordrecht, 1993.

[18] C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. **35** (1977), 425–447.

[19] Z.-H. Sun and Z.-W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta. Arith. **60** (1992), 371–388.

[20] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, Springer-Verlag, 1980.

[21] A. Wieferich, *Zum letzten Fermatschen Theorem (German)*, J. Reine Angew. Math **136** (1909), 293–302.

Address: Sudhansu Sekhar Rout: Institute of Mathematics & Applications, Andharua, Bhubaneswar, Odisha-751 029, India.

E-mail: lbs.sudhansu@gmail.com

Received: 11 October 2017; **revised:** 28 August 2018