Czechoslovak Mathematical Journal

Srinivas Kotyada; Subramani Muthukrishnan

Non-Wieferich primes in number fields and abc-conjecture

Czechoslovak Mathematical Journal, Vol. 68 (2018), No. 2, 445–453

Persistent URL: http://dml.cz/dmlcz/147228

Czechoslovak Mathematical Journal, 68 (143) (2018), 445–453

NON-WIEFERICH PRIMES IN NUMBER FIELDS AND abc-CONJECTURE

Srinivas Kotyada, Chennai, Subramani Muthukrishnan, Kelambakkam

Received September 16, 2016. First published January 19, 2018.

Abstract. Let $K/\mathbb{Q}$ be an algebraic number field of class number one and let $\mathcal{O}_K$ be its ring of integers. We show that there are infinitely many non-Wieferich primes with respect to certain units in $\mathcal{O}_K$ under the assumption of the abc-conjecture for number fields.

Keywords: Wieferich prime; non-Wieferich prime; number field; abc-conjecture

MSC 2010: 11A41, 11R04

1. Introduction

An odd rational prime p is called Wieferich prime if

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

Wieferich in [8] proved that if an odd prime p is non-Wieferich prime, i.e., p satisfies

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

then there are no integer solutions to the Fermat equation $x^p + y^p = z^p$, with $p \nmid xyz$. The known Wieferich primes are 1093 and 3511 and according to the PrimeGrid project (see [5]), these are the only Wieferich primes less than $17 \cdot 10^{15}$. One of the unsolved problems in this area of research is to determine whether the number of Wieferich or non-Wieferich primes is finite or infinite. Instead of the base 2 if we take any base a, then p is said to be a Wieferich prime with respect to the base a if

$$a^{p-1} \equiv 1 \pmod{p^2}, \tag{1.2}$$

DOI: 10.21136/CMJ.2018.0485-16

and if the congruence (1.2) does not hold then we say that p is non-Wieferich prime with respect to the base a. Under the famous *abc*-conjecture (defined below), Silverman in [6] proved that given any integer a, there are infinitely many non-Wieferich primes with respect to the base a. He established this result by showing that for any fixed $\alpha \in \mathbb{Q}^{\times}$, $\alpha \neq \pm 1$, and assuming the truth of the *abc* conjecture,

$$\mathrm{card}\{p \leqslant x\colon\ \alpha^{p-1} \not\equiv 1 \pmod{p^2}\} \gg_{\alpha} \log x \quad \text{as } x \to \infty.$$

In [1] Graves and Murty extended this result to primes in an arithmetical progression by showing that for any $a \geqslant 2$ and any fixed $k \geqslant 2$, there are $\gg \log x/\log\log x$ primes $p \leqslant x$ such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$, under the assumption of the *abc* conjecture.

In this paper, we study non-Wieferich primes in algebraic number fields of class number one. More precisely, we prove

Theorem 1.1. *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one and assume that the abc-conjecture holds true in K. Then there are infinitely many non-Wieferich primes in $\mathcal{O}_K$ with respect to the unit ε satisfying $|\varepsilon| > 1$.*

Theorem 1.2. *Let K be any algebraic number field of class number one and assume that the abc-conjecture holds true in K. Let η be a unit in $\mathcal{O}_K$ satisfying $|\eta| > 1$ and $|\eta^{(j)}| < 1$ for all $j \neq 1$, where $\eta^{(j)}$ is the jth conjugate of η. Then there exist infinitely many non-Wieferich primes in K with respect to the base η.*

The plan of this article is as follows. In Section 2, we define the *abc*-conjecture for number fields. In Section 3, a brief introduction to Wieferich/non-Wieferich primes over number fields will be given and in Sections 4 and 5, we prove Theorem 1.1 and Theorem 1.2, respectively.

2. The *abc*-conjecture

The *abc*-conjecture propounded by Oesterlé and Masser (1985) states that given any $\delta > 0$ and positive integers a, b, c such that $a + b = c$ with $(a, b) = 1$, we have

$$c \ll_{\delta} (\mathrm{rad}(abc))^{1+\delta},$$

where $\mathrm{rad}(abc) := \prod_{p \mid abc} p$.

The *abc*-conjecture has several applications, the reader may refer to [7], [2], [3] for details.

To state the analogue of the *abc*-conjecture for number fields, we need some preparations, which we do below. The interested reader may refer to [7], [2] for more details.

Let K be an algebraic number field and let V_K denote the set of primes on K, that is, any v in V_K is an equivalence class of the norm on K (finite or infinite). Let $\|x\|_v := N_{K/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$ if v is a prime defined by the prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ in K and $v_{\mathfrak{p}}$ is the corresponding valuation, where $N_{K/\mathbb{Q}}$ is the absolute value norm. Let $\|x\|_v := |g(x)|^e$ for all non-conjugate embeddings $g\colon K \to \mathbb{C}$ with $e = 1$ if g is real and $e = 2$ if g is complex. Define the height of any triple $a, b, c \in K^{\times}$ 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) by

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

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 all primes $\mathfrak{p}$ of $\mathcal{O}_K$ for which $\|a\|_v$, $\|b\|_v$, $\|c\|_v$ are not equal.

The abc conjecture for algebraic number fields is stated as follows: For any $\delta > 0$, we have

$$H_K(a,b,c) \ll_{\delta,K} (\mathrm{rad}_K(a,b,c))^{1+\delta} \tag{2.1}$$

for all $a, b, c \in K^{\times}$ satisfying $a+b+c = 0$, the implied constant depends on K and δ.

3. Wieferich/non-Wieferich primes in number fields

Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. A prime $\pi \in \mathcal{O}_K$ is called a Wieferich prime with respect to the base $\varepsilon \in \mathcal{O}_K^*$ if

$$\varepsilon^{N(\pi)-1} \equiv 1 \pmod{\pi^2}, \tag{3.1}$$

where $N(\cdot)$ is the absolute value norm. If the congruence (3.1) does not hold for a prime $\pi \in \mathcal{O}_K$, then π is called a non-Wieferich prime to the base ε.

Notation: In what follows, ε will denote a unit in $\mathcal{O}_K$ and we will write $\varepsilon^n - 1 = u_n v_n$, where u_n is the square free part and v_n is the squarefull part, i.e., if $\pi \mid v_n$ then $\pi^2 \mid v_n$. We will denote the absolute value norm on K by N.

4. Proof of theorem 1.1

Let $K = \mathbb{Q}(\sqrt{m})$, $m > 0$, be a real quadratic field and $\mathcal{O}_K$ its ring of integers. Let $\varepsilon \in \mathcal{O}_K^*$ be a unit with $|\varepsilon| > 1$. The results of Silverman in [6], Murty and Hester in [1] elucidated in the introduction the use of a key lemma of Silverman (see [6], Lemma 3). We derive an analogue of Silverman's lemma for number fields which will play a fundamental role in the proof of the main theorems.

Lemma 4.1. *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one. Let $\varepsilon \in \mathcal{O}_K^*$ be a unit. If $\varepsilon^n - 1 = u_n v_n$, then every prime divisor π of u_n is a non-Wieferich prime with respect to the base ε.*

Proof. The assumption that K has class number one allows us to write the element $\varepsilon^n - 1 \in \mathcal{O}_K$ as a product of primes uniquely. Accordingly, we will write

$$\varepsilon^n - 1 = u_n v_n$$

for $n \in \mathbb{N}$. Then

$$\varepsilon^n = 1 + \pi w \tag{4.1}$$

with $\pi \mid u_n$ and π and w are coprime. As π is a prime, we have $N(\pi) = p$ or p^2, where p is a rational prime.

Case 1: Suppose $N(\pi) = p$.

From equation (4.1), we get

$$\varepsilon^{n(p-1)} \equiv 1 + (p-1)\pi w \not\equiv 1 \pmod{\pi^2}.$$

Case 2: Suppose $N(\pi) = p^2$.

Again from equation (4.1), we obtain

$$\varepsilon^{n(p^2-1)} = \varepsilon^{n(N(\pi)-1)} = (1 + \pi w)^{(p^2-1)} \equiv 1 + \pi w(p^2 - 1) \not\equiv 1 \pmod{\pi^2}.$$

Thus in either case,

$$\varepsilon^{(N(\pi)-1)} \not\equiv 1 \pmod{\pi^2},$$

and hence π is a non-Wieferich prime to the base ε. □

The above lemma shows that whenever a prime π divides u_n for some positive integer n, then π is a non-Wieferich prime with respect to the base ε. Thus, if we can show that the set $\{N(u_n)\colon n \in \mathbb{N}\}$ is unbounded, then this will imply that the set $\{\pi\colon \pi \mid u_n, n \in \mathbb{N}\}$ is an infinite set. Consequently, this establishes the fact that there are infinitely many non-Wieferich primes in every real quadratic field of class number one with respect to the unit ε, with $|\varepsilon| > 1$. Therefore, we need only to show

Lemma 4.2. *Let $\mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one. Let $\varepsilon \in \mathcal{O}_K^*$ be a unit with $|\varepsilon| > 1$. Then under the abc-conjecture for number fields, the set $\{N(u_n)\colon n \in \mathbb{N}\}$ is unbounded.*

Proof. Invoking the *abc*-conjecture (2.1) to the equation

$$\varepsilon^n = 1 + u_n v_n \tag{4.2}$$

yields

$$|\varepsilon^n| \ll \Big(\prod_{\mathfrak{p}|u_n v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)}\Big)^{1+\delta} = \Big(\prod_{\mathfrak{p}|u_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)}\Big)^{1+\delta} \tag{4.3}$$

for some $\delta > 0$. Here the implied constant depends on K and δ.

As $v_{\mathfrak{p}}(p) \leqslant 2$ for any prime ideal $\mathfrak{p}$ lying above the rational prime p, we have

$$\prod_{\mathfrak{p}|u_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leqslant N(u_n)^2. \tag{4.4}$$

For a prime ideal $\mathfrak{p} \mid v_n$, let $e_{\mathfrak{p}}$ be the largest exponent of $\mathfrak{p}$ dividing v_n, i.e., $\mathfrak{p}^{e_{\mathfrak{p}}} \parallel v_n$. As v_n is the square-full part of $\varepsilon^n - 1$, we have $e_{\mathfrak{p}} \geqslant 2$. Hence,

(1) $N(\mathfrak{p})^{2v_{\mathfrak{p}}(p)} \leqslant N(\mathfrak{p})^{2+e_{\mathfrak{p}}}$ for all prime ideals $\mathfrak{p}$ with $v_{\mathfrak{p}}(p) = 2$;

(2) $N(\mathfrak{p})^{2v_{\mathfrak{p}}(p)} \leqslant N(\mathfrak{p})^{e_{\mathfrak{p}}}$ for all prime ideals $\mathfrak{p}$ with $v_{\mathfrak{p}}(p) = 1$.

Thus,

$$\begin{aligned}
\prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{2v_{\mathfrak{p}}(p)} &\leqslant \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{2+e_{\mathfrak{p}}} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=1}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \\
&\leqslant \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{2} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=1}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \\
&\leqslant {\prod_{\mathfrak{p}}}' N(\mathfrak{p})^{2} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=1}} N(\mathfrak{p})^{e_{\mathfrak{p}}},
\end{aligned}$$

where '$'$' indicates that the product is over all primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(p) = 2$. As it is well known that there are only finitely many ramified primes in a number field, it follows that the product is bounded by a constant A (say). Thus, we have

$$\prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leqslant \sqrt{AN(v_n)}. \tag{4.5}$$

Combining equations (4.3), (4.4) and (4.5), we get

$$|\varepsilon^n| \ll \left(N(u_n)^2\sqrt{N(v_n)}\right)^{1+\delta}. \tag{4.6}$$

Now, as $|\varepsilon| > 1$,

$$N(u_n)N(v_n) = N(\varepsilon^n - 1) \leqslant 2|\varepsilon^n - 1| < 2|\varepsilon|^n,$$

i.e.,

$$N(v_n) < \frac{2|\varepsilon|^n}{N(u_n)}.$$

Substituting the above expression into (4.6), we obtain

$$|\varepsilon^n| \ll \left(N(u_n)^2\frac{|\varepsilon|^{n/2}}{\sqrt{N(u_n)}}\right)^{1+\delta}.$$

Thus,

$$(N(u_n))^{3(1+\delta)/2} \gg |\varepsilon|^{n(1-\delta)/2}.$$

Thus, for a fixed δ, $N(u_n) \to \infty$ as $n \to \infty$. This proves the lemma and hence completes the proof of the theorem. □

5. Non-Wieferich primes in algebraic number fields

In this section we generalize the arguments of the previous section to arbitrary number fields. From now onwards, K will always denote an algebraic number field of degree $[K:\mathbb{Q}] = l$ over $\mathbb{Q}$ of class number one. Let r_1 and r_2 be the number of real and non-conjugate complex embeddings of K into $\mathbb{C}$, respectively, so that $l = r_1 + 2r_2$. We begin with an analogue of Lemma (4.1).

Lemma 5.1. *Let ε be a unit in $\mathcal{O}_K$. If $\varepsilon^n - 1 = u_n v_n$, then every prime divisor π of u_n is a non-Wieferich prime with respect to the base ε.*

Proof. Let $N(\pi) = p^k$, where p is a rational prime and k is a positive integer. Then

$$\varepsilon^{n(N(\pi)-1)} = \varepsilon^{n(p^k-1)} = (1 + w\pi)^{(p^k-1)} \equiv 1 + (p^k - 1)w\pi \not\equiv 1 \pmod{\pi^2}.$$

This implies $\varepsilon^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}$.

Thus, the lemma shows that π is a non-Wieferich prime to the base ε whenever the hypothesis of the lemma is met. Now, under the *abc*-conjecture for number fields, we show below the existence of infinitely many non-Wieferich primes. □

Lemma 5.2. *The set* $\{N(u_n)\colon\, n \in \mathbb{N}\}$ *is unbounded, where* u_n*'s are as defined in Lemma* 5.1.

Proof. By the hypothesis of the lemma, we have $\varepsilon^n = 1 + u_n v_n$, where $\varepsilon^n, 1, u_n v_n \in K^\times$. Applying the *abc*-conjecture for number fields to the above equation, we obtain

$$\prod_{v \in V_K} \max(|u_n v_n|_v, |1|_v, |\varepsilon^n|_v) \ll \Bigl(\prod_{\mathfrak{p} \mid u_n v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)}\Bigr)^{1+\delta} \tag{5.1}$$

for some $\delta > 0$.

Note that for the absolute value $|\cdot|$ in V_K we have

$$|\varepsilon^n| \leqslant \prod_{v \in V_K} \max(|u_n v_n|_v, |1|_v, |\varepsilon^n|_v). \tag{5.2}$$

As $v_{\mathfrak{p}}(p) \leqslant l$ for any prime ideal $\mathfrak{p}$ lying above the rational prime p, we have

$$\prod_{\mathfrak{p} \mid u_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leqslant N(u_n)^l. \tag{5.3}$$

As before, we denote by $e_{\mathfrak{p}}$ the largest exponent of $\mathfrak{p}$ which divides v_n, i.e., $\mathfrak{p}^{e_{\mathfrak{p}}} \parallel v_n$. Clearly $e_{\mathfrak{p}} \geqslant 2$. Then

$$\begin{aligned}
\prod_{\mathfrak{p} \mid v_n} N(\mathfrak{p})^{2 v_{\mathfrak{p}}(p)} &\leqslant \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) \geqslant 2}} N(\mathfrak{p})^{2l + e_{\mathfrak{p}}} \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) = 1}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \\
&\leqslant \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) \geqslant 2}} N(\mathfrak{p})^{2l} \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) \geqslant 2}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) = 1}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \\
&\leqslant {\prod_{\mathfrak{p}}}' N(\mathfrak{p})^{2l} \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) \geqslant 2}} N(\mathfrak{p})^{e_{\mathfrak{p}}} \prod_{\substack{\mathfrak{p} \mid v_n \\ v_{\mathfrak{p}}(p) = 1}} N(\mathfrak{p})^{e_{\mathfrak{p}}},
\end{aligned}$$

where '$'$' indicates that the product is over all primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(p) \geqslant 2$. As there are only finitely many ramified primes in a number field, it is bounded by a constant B (say). Thus, we have

$$\prod_{\mathfrak{p} \mid v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leqslant \sqrt{B N(v_n)}. \tag{5.4}$$

Therefore, the equations (5.1)–(5.4) yield

$$|\varepsilon^n| \ll (N(u_n)^l \sqrt{N(v_n)})^{1+\delta}. \tag{5.5}$$

Note that in the case of real quadratic fields, the unit ε satisfies $|\varepsilon| > 1$ and this information was crucial in proving Theorem 1.1. However, in the case of general number fields, the following result (see [4], Lemma 8.1.5) comes to our rescue. We state this result as

Lemma 5.3. *Let $E = \{k \in \mathbb{Z}\colon 1 \leqslant k \leqslant r_1 + r_2\}$. Let $E = A \cup B$ be a proper partition of E. There exists a unit $\eta \in \mathcal{O}_K$ with $|\eta^{(k)}| < 1$ for $k \in A$, and $|\eta^{(k)}| > 1$ for $k \in B$.*

Taking $A = \{k\colon 1 < k \leqslant r_1 + r_2\}$ and $B = \{1\}$, Lemma 5.3 produces a unit $\eta \in \mathcal{O}_K^*$ such that $|\eta| > 1$ and $|\eta^{(k)}| < 1$, where $\eta^{(k)}$ denotes the kth conjugate of $\eta, k \neq 1$. Since every unit satisfies (5.5), replacing ε with η in (5.5) we obtain

$$|\eta^n| \ll (N(u_n)^l \sqrt{N(v_n)})^{1+\delta}, \tag{5.6}$$

where, by abuse of notation, we will denote $\eta^n - 1 = u_n v_n$, with u_n and v_n denoting the same quantities as defined earlier.

Now,

$$N(u_n)N(v_n) = N(\eta^n - 1) = (\eta^n - 1)(\eta^{(2)n} - 1)(\eta^{(3)n} - 1)\ldots(\eta^{(l)n} - 1).$$

By Lemma 5.3, $|\eta^{(j)n} - 1| < 2$ for all j, $2 \leqslant j \leqslant l$.

Thus,

$$N(u_n)N(v_n) < C|\eta^n| \quad \text{or} \quad N(v_n) < \frac{C|\eta^n|}{N(u_n)}.$$

Now, (5.6) can be written as

$$(N(u_n))^{(2l-1)(1+\delta)/2} \gg |\eta|^{n(1-\delta)/2}. \tag{5.7}$$

For a fixed δ, the right hand side of (5.7) tends to ∞ as $n \to \infty$. Therefore the set $\{N(u_n)\colon n \in \mathbb{N}\}$ is unbounded. This shows that there are infinitely many non-Wieferich primes in K with respect to the base η. □

Acknowledgement. We express our indebtedness to Prof. M. Ram Murty for initiating us into this project and for having many fruitful discussions. The second author would like to thank Prof. T. R. Ramadas for encouragement and also acknowledges him with thanks for the financial support extended by DST through his J. C. Bose Fellowship. Our sincere thanks to the referee for pointing out some errors and suggesting some changes in an earlier version of this paper. This work is part of the PhD thesis of the second author.

References

[1] *H. Graves, M. R. Murty*: The *abc* conjecture and non-Wieferich primes in arithmetic progressions. J. Number Theory *133* (2013), 1809–1813. zbl MR doi

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

[3] *M. R. Murty*: The *ABC* conjecture and exponents of class groups of quadratic fields. Number Theory. Proc. Int. Conf. On Discrete Mathematics and Number Theory, Tiruchirapalli, India, 1996 (V. K. Murty et al., eds.). Contemp. Math. 210. AMS, Providence, 1998, pp. 85–95. zbl MR doi

[4] *M. R. Murty, J. Esmonde*: Problems in Algebraic Number Theory. Graduate Texts in Mathematics 190, Springer, Berlin, 2005. zbl MR doi

[5] PrimeGrid Project. Available at `http://www.primegrid.com/`.

[6] *J. H. Silverman*: Wieferich's criterion and the *abc*-conjecture. J. Number Theory *30* (1988), 226–237. zbl MR doi

[7] *P. Vojta*: Diophantine Approximations and Value Distribution Theory. Lecture Notes in Mathematics 1239, Springer, Berlin, 1987. zbl MR doi

[8] *A. Wieferich*: Zum letzten Fermatschen Theorem. J. Reine Angew. Math. *136* (1909), 293–302. (In German.) zbl MR doi

Authors' addresses: Srinivas Kotyada, Institute of Mathematical Sciences, Homi Bhabha National Institute, IV Cross Road, CIT Campus, Taramani, Chennai 600113, Tamil Nadu, India, e-mail: `srini@imsc.res.in`; Subramani Muthukrishnan, Chennai Mathematical Institute, H1, SIPCOT IT Park, Siruseri, Kelambakkam 603103, India, e-mail: `subramani@cmi.ac.in`.