On The index of the number field defined by $x^8+ax+b$

Ben Yakkou Hamid (✉ beyakouhamid@gmail.com)
Faculty of Sciences Dhar El Mahraz, P.O. Box 1874 Atlas-Fes, Sidi Mohamed ben Abdellah University, Morocco
https://orcid.org/0000-0002-1374-6333

Brahim Boudine (✉ brahimboudine.bb@gmail.com)
Faculty of Sciences Dhar El Mahraz, P.O. Box 1874 Atlas-Fes, Sidi Mohamed ben Abdellah University, Morocco

Research Article

Keywords:

DOI: https://doi.org/10.21203/rs.3.rs-2675695/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License
ON THE INDEX OF THE OCTIC NUMBER FIELD DEFINED BY
\[ x^8 + ax + b \]

HAMID BEN YAKKOU AND BRAHIM BOUDINE

Abstract. Let \( K \) be an octic number field generated by a complex root \( \theta \) of a monic irreducible trinomial \( F(x) = x^8 + ax + b \in \mathbb{Z}[x] \), where \( a \) and \( b \) are two non-zero rational integers. Let \( i(K) \) be the index of \( K \). In this paper, we show that \( i(K) \) is either 1 or a power of 2. Further, we give necessary and sufficient conditions depending only on \( a \) and \( b \) so that 2 is a prime common index divisor of \( K \). In particular, we provide sufficient conditions for which \( K \) is non-monogenic. In such a way our results extend a result proved in [H. Ben Yakkou, On monogenicity of certain number fields defined by trinomial of type \( x^8 + ax + b \), Acta Math. Hungar. 166 (2022), 614-623], when some sufficient conditions of the divisibility of \( i(K) \) by 2 are provided.

1. Introduction

Let \( K \) be a number field generated by \( \theta \); a root of a monic irreducible polynomial \( F(x) \in \mathbb{Z}[x] \) of degree \( n \), and \( \mathbb{Z}_K \) its ring of integers. It is well known that the ring \( \mathbb{Z}_K \) is a free \( \mathbb{Z} \)-module of rank \( n \) (see [9] Theorem 4.42). Thus, the abelian group \( \mathbb{Z}_K/\mathbb{Z}[\theta] \) is finite, its cardinal order is called the index of \( \mathbb{Z}[\theta] \) and denoted \( (\mathbb{Z}_K : \mathbb{Z}[\theta]) \). We say that \( \mathbb{Z}_K \) have a power integral basis if it admits a \( \mathbb{Z} \)-basis \( (1, \eta, \ldots, \eta^{n-1}) \), for some \( \eta \in \mathbb{Z}_K \); namely, we have either \( \mathbb{Z}_K = \mathbb{Z}[\eta] \) or \( \mathbb{Z}_K \) is mono-generated as a ring with a single generator \( \eta \). In such a case, the field \( K \) is said to be monogenic. Otherwise, \( K \) is not monogenic. In this paper, \( i(K) \) will denote the index of the field \( K \) defined as follows:

\[ i(K) = \gcd \{(\mathbb{Z}_K : \mathbb{Z}[\eta]) \mid \eta \in \mathbb{Z}_K \text{ and } K = \mathbb{Q}(\eta)\}. \tag{1.1} \]

A rational prime \( p \) dividing \( i(K) \) is called a prime common index divisor of \( K \). Notice that if \( K \) is monogenic, then \( i(K) = 1 \). Thus, a field possessing a prime common index divisor is not monogenic. The problem of studying indices and the monogenity in number fields has been intensively studied (cf. [2], [6], [8], [13], [16], [17], [20], [23], [26], [28], [29]). Győry provided the first general algorithms for deciding whether \( K \) is monogenic or not and for determining all power integral bases in \( \mathbb{Z}_K \). In [20], Gaál, Pethő and Pohst studied the monogenity of quartic number fields. In [19], Gaál and Győry described an algorithm to solve index form equations in quintic number fields and they computed all generators of power integral bases in some totally real quintic number fields with Galois group \( S_5 \). In [8], Bilu, Gaál and Győry studied the monogenity of some totally real sextic number fields with Galois group \( S_6 \). In [33], Pethő and Ziegler gave an efficient criterion to decide whether the maximal order of a biquadratic field has a unit power integral basis or not. In [22], Gaál and Remete gave deep results regarding the monogenity of pure number

2010 Mathematics Subject Classification. 11R04, 11R16, 11R21.

Key words and phrases. Monogenity, Power integral basis, Theorem of Ore, prime ideal factorization, common index divisor.
fields $\mathbb{Q}(\sqrt{m})$, where $3 \leq n \leq 9$ and $m$ is square-free. In [2, 3], Ahmed et al. studied the monogenity of sextic pure number fields $\mathbb{Q}(\sqrt{m})$, where $m \neq \pm 1$ is a square-free rational integer. We refer also to the papers: [21] by Gaàl and Remete, [37] by Pethô and Pohst, and to the books [10, 17], which give detailed surveys on the discriminant, the index form theory and its applications, including related Diophantine equations and monogenity of number fields. The question of monogenity in the relative case has been profoundly studied by Györy in [27] and [28], see also [16].

Recently, the study of indices and the monogenity in number fields defined by trinomials of type $x^n + ax^m + b$ interests several researchers. In 2021, Gaàl [18] started a nice attempt at the monogenity of number fields defined by $x^6 + ax^3 + b$. Many other cases have been studied following the values of $n$ and $m$: Davis and Spearman [11] for $(n, m) = (4, 1)$, Jakhar, Kaur and Kumar [30] for $(n, m) = (5, 1)$, Ben Yakkou [4] for $(n, m) = (5, 3)$, Gaàl [18] and El Fadil [12] for $(n, m) = (3, 6)$, El Fadil and Kehit [13] for $(n, m) = (7, 3)$. In [31], Jakhar, Khanduja and Sangwan solved completely the problem of the integral closedness of $\mathbb{Z}[\theta]$. In [32], Jones and White gave classes of monogenic trinomials with non square-free discriminant. Also, in [33], Jones and Phillips constructed infinite families of monogenic trinomials.

The goal of this paper, is to investigate the index of the octic number field generated by a root of a monic irreducible trinomial of type $F(x) = x^8 + ax + b$. Recall that in [7], Ben Yakkou and El Fadil studied the non-monogenity of number fields defined by $x^n + ax + b$. More precisely, they gave sufficient conditions for which $i(K)$ has an odd prime divisor. Moreover, they studied the cases $n = 5$ and $n = 6$. These results are generalized in [34] by Ben Yakkou, for number fields defined by $x^n + ax^m + b$. Also, in [6], Ben Yakkou studied the monogenity of the number field defined by $x^8 + ax + b$. In particular, he provided four sufficient conditions on $a$ and $b$ for which $2$ divides $i(K)$. However, the above mentioned results cannot completely characterise the divisors of $i(K)$. The results of the present paper give the desired complete answer in all possible cases. These results combined with the ones found in [6, 34] deeply investigate the monogenity of octic number fields defined by such trinomials.

2. Main Results

In what follows, let $K$ be a number field generated by $\theta$; a root of a monic irreducible trinomial $F(x) = x^8 + ax + b \in \mathbb{Z}[x]$, where $ab \neq 0$ and $\mathbb{Z}_K$ is its ring of integers. For every rational prime $p$ and any non-zero $p$-adic integer $m$, $\nu_p(m)$ will denote the $p$-adic valuation of $m$; the highest power of $p$ dividing $m$, $m_p := \frac{m}{p^{\nu_p(m)}}$, and $\mathbb{F}_p$ the finite field with $p$ elements. Without loss of generality, for every prime $p$, we assume that

$$
\nu_p(a) < 7 \text{ or } \nu_p(b) < 8. \tag{2.1}
$$

For simplicity, if $p\mathbb{Z}_K = p^{e_1} \cdots p^{e_g}$ is the factorization of $p\mathbb{Z}_K$ into a product of powers of prime ideals in $\mathbb{Z}_K$ with residue degrees $f(p_i/p) = [\mathbb{Z}_K/p_i : \mathbb{F}_p] = f_i$, then we write $p\mathbb{Z}_K = [f_1^{e_1}, \ldots, f_g^{e_g}]$. We recall, by the Fundamental Equality (see [9] Theorem 4.8.5]), that

$$
\sum_{i=1}^{g} e_if_i = 8 = \text{deg}(K). \tag{2.2}
$$
For any integers $a, b, c, d$, by the notation $(a, b) = (c, d) \pmod{p}$, we mean $a \equiv c \pmod{p}$ and $b \equiv c \pmod{p}$. Further, $(a, b) \in S \pmod{p}$ means that $(a, b)$ equal some element of $S$ modulo $p$.

Now, we state our first main result.

**Theorem 2.1.** Let $a$ and $b$ be two non-zero rational integers such that $F(x) = x^8 + ax + b \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, and $K$ the number field generated by a complex root $\theta$ of $F(x)$. If $p$ is an odd rational prime, then $p$ does not divide the index $i(K)$.

**Remark 2.2.** From Theorem 2.1 we have either $i(K) = 1$ or $i(K)$ is a power of 2. The following theorem gives the complete answer.

**Theorem 2.3.** Let $K$ be a number field generated by a complex root $\theta$ of a monic irreducible trinomial $F(x) = x^8 + ax + b \in \mathbb{Z}[x]$. Assume that $(a, b) \not\in (32 + 64\mathbb{Z}) \times (16 + 64\mathbb{Z})$ and $(a, b) \not\in (64\mathbb{Z}) \times (112 + 128\mathbb{Z})$. When $a \equiv 8 \pmod{16}$ and $b \equiv 7 \pmod{16}$, let

$$
\begin{align*}
\omega &= \nu_2(b^7 - 7^7 a_8^2), \\
A_{1,2} &= b(b^7 - 7^7 a_8^2) + 7a_2(7^7 a_8^2 - b^7 + b^6 a_2), \\
A_{2} &= b(7^7 a_8^2 - b^7 + b^6 a_2), \\
B_{a,b} &= (b^7 - 7^7 a_8^2) + 7^3 \cdot a_8^3 \cdot b^6.
\end{align*}
$$

Then, the form of the factorization of the ideal $2\mathbb{Z}_K$ into a product of powers of prime ideals of $\mathbb{Z}_K$ is given in Table 2 below. In particular, $2$ divides $i(K)$ if and only if one of the conditions $C12, C15, C16, C17, C19, C20, C22$ hold. Otherwise, $i(K) = 1$.

**Remarks 2.4.**

1. Theorem 2.1 implies Theorem 2.3 of [6].
2. Note that in the case of the octic field $K$, the prime 2 is a common index divisor of $K$ if and only if there are three prime ideals of $\mathbb{Z}_K$ of residue degree 1 each, or two prime ideals of residue degree 2 each lying above $2\mathbb{Z}_K$ (see [5], Theorems 4.33 and 4.34) and Equality (2.2).
3. Notice that if $a \equiv 8 \pmod{16}$ and $b \equiv -9 \pmod{32}$, then $\omega = 4$, and if $a \equiv 8 \pmod{16}$ and $b \equiv 7 \pmod{32}$, then $\omega = \nu_2(1 - a_8^2)$ is greater than 5.

**Corollary 2.5.** Under the assumptions of Theorem 2.3 if one of the conditions $C12, C15, C16, C17, C19, C20, C22$ holds, then $K$ cannot be monogenic; namely, $\mathbb{Z}_K$ has no power integral basis.

**Corollary 2.6.** Under the assumptions of Theorem 2.3. If $a \equiv 8 \pmod{16}$, $b \equiv 7 \pmod{32}$, and $a_2 \in \{5, 11, 21, 32, 37, 43, 53, 59, 69, 75, 85, 91, 101, 107, 117, 123\} \pmod{128}$, then $w = 5$. By Case $C16$ of Theorem 2.3 2 divides $i(K)$. So, the field $K$ cannot be monogenic.

**Remarks 2.7.**

1. Note that the important work of Śliwa [11] concerning the computation of $\nu_p(i(K))$ is about the unramified primes of $K$. But in the case of the octic number field defined by $x^8 + ax + b$, the prime 2 is ramified in all cases. So, we cannot apply Śliwa’s results to compute $\nu_2(i(K))$ when $i(K) \geq 2$. 
<table>
<thead>
<tr>
<th>Case</th>
<th>Conditions</th>
<th>Factorization of $2\mathbb{Z}_K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>$ab \equiv 1 \pmod{2}$</td>
<td>$[2^1, 6^1]$</td>
</tr>
<tr>
<td>C2</td>
<td>$a \equiv 1 \pmod{2}$ and $b \equiv 0 \pmod{2}$</td>
<td>$[1^1, 1^1, 3^1, 3^1]$</td>
</tr>
<tr>
<td>C3</td>
<td>$1 \leq \nu_2(a) \leq 6$ and $8\nu_2(a) &lt; 7\nu_2(b)$</td>
<td>$[1^1, 1^1]$</td>
</tr>
<tr>
<td>C4</td>
<td>$\nu_2(b) \in {1, 3, 5, 7}$ and $8\nu_2(a) &gt; 7\nu_2(b)$</td>
<td>$[2^1]$</td>
</tr>
<tr>
<td>C5</td>
<td>$\nu_2(b) \in {2, 6}$ and $8\nu_2(a) &gt; 7\nu_2(b)$</td>
<td>$[1^8], [1^1, 1^1]$ or $[2^1]$</td>
</tr>
<tr>
<td>C6</td>
<td>$a \equiv 16 \pmod{32}$ and $b \equiv 16 \pmod{32}$</td>
<td>$[1^3]$</td>
</tr>
<tr>
<td>C7</td>
<td>$a \equiv 32 \pmod{64}$ and $b \equiv 48 \pmod{64}$</td>
<td>$[1^3]$</td>
</tr>
<tr>
<td>C8</td>
<td>$a \equiv 0 \pmod{64}$ and $b \equiv 48 \pmod{128}$</td>
<td>$[2^1]$</td>
</tr>
<tr>
<td>C9</td>
<td>$(a, b) \in {(0, 1), (2, 3)} \pmod{4}$</td>
<td>$[1^3]$</td>
</tr>
<tr>
<td>C10</td>
<td>$a \equiv 2 \pmod{4}$ and $b \equiv 1 \pmod{4}$</td>
<td>$[1, 1^1]$</td>
</tr>
<tr>
<td>C11</td>
<td>$(a, b) \in {(0, 4), (4, 7)} \pmod{8}$</td>
<td>$[2^1]$</td>
</tr>
<tr>
<td>C12</td>
<td>$a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$</td>
<td>$[1, 2^1, 1^1]$</td>
</tr>
<tr>
<td>C13</td>
<td>$(a, b) \in {(0, 7), (8, 15)} \pmod{16}$</td>
<td>$[2^1, 1^1]$</td>
</tr>
<tr>
<td>C14</td>
<td>$(a, b) \in {(0, 15), (16, 31)} \pmod{32}$</td>
<td>$[2, 1^2, 1^1]$</td>
</tr>
<tr>
<td>C15</td>
<td>$(a, b) \in {(0, 31), (16, 15)} \pmod{32}$</td>
<td>$[1, 1, 2^1, 1^1]$</td>
</tr>
<tr>
<td>C16</td>
<td>$a \equiv 8 \pmod{16}, b \equiv 7 \pmod{32}$ and $\omega$ is odd</td>
<td>$[1^2, 2^1, 1^1]$</td>
</tr>
<tr>
<td>C17</td>
<td>$a \equiv 8 \pmod{16}, b \equiv 9 \pmod{32}$ and $A_{a,b}^1 \equiv 0 \pmod{4}$</td>
<td>$[1^2, 2^1, 1^1]$</td>
</tr>
<tr>
<td>C18</td>
<td>$a \equiv 8 \pmod{16}, b \equiv 9 \pmod{32}$, $A_{a,b}^1 \equiv 2 \pmod{4}$ and $A_{a,b}^2 \equiv 2 \pmod{4}$</td>
<td>$[2, 1^2, 1^1]$</td>
</tr>
<tr>
<td>C19</td>
<td>$a \equiv 8 \pmod{16}, b \equiv 9 \pmod{32}$, $A_{a,b}^1 \equiv 2 \pmod{4}$ and $A_{a,b}^2 \equiv 0 \pmod{4}$</td>
<td>$[1, 1, 2^1, 1^1]$</td>
</tr>
<tr>
<td>C20</td>
<td>$\omega \geq 6$ is even and $B_{a,b} \equiv 2 \pmod{4}$</td>
<td>$[1^2, 1^2, 1^1]$</td>
</tr>
<tr>
<td>C21</td>
<td>$\omega \geq 6$ is even and $B_{a,b} \equiv 4 \pmod{8}$</td>
<td>$[2, 1^2, 1^1]$</td>
</tr>
<tr>
<td>C22</td>
<td>$\omega \geq 6$ is even and $B_{a,b} \equiv 0 \pmod{8}$</td>
<td>$[1, 1, 2^1, 1^1]$</td>
</tr>
</tbody>
</table>

Table 1. The factorization of $2\mathbb{Z}_K$

(2) Notice that the condition $i(K) = 1$ is not sufficient for the monogenity of $K$. The pure cubic number field $K = \mathbb{Q}(\sqrt[3]{755})$ is a simple counter example, since $i(K) = 1$, but $K$ is not monogenic as its index form equals $5x^3 - 7y^3$ and never assumes the values $\pm 1$ (see [1] Example 7.4.4]).

(3) Note that the fundamental method to test whether a number field is monogenic or not is to solve the index form equation, which is very complicated for higher degree number fields. In the case of octic number fields, the index form equation $I_2(x_2, x_3, \ldots, x_8) = \pm 1$ is a Diophantine equation of degree 28 with 7 variables. However, to decide the monogenity of $K$, we need to solve this equation which is not easy to achieve. Indeed, one must use advanced techniques and methods in addition to computations using powerful computers and algorithms (cf. [3] [11] [16] [17] [18] [19] [20] [22] [26] [27] [37] and the references therein). Actually, we do not have any general practical procedure to solve the corresponding index form equations in octic number fields. Here, we prefer the prime ideal factorization method as our approach. We determine the prime ideals factorization by using
Newton polygon techniques. This method is efficient to investigate indices and monogenity of number fields defined by trinomials.

Now, we propose three numerical examples to illustrate our results.

**Example 2.8.** Let $K = \mathbb{Q}(\theta)$, where $\theta$ is a root of $F(x) = x^8 + 463424804x + 123$. Since $F(x)$ is a 41-Eisenstein polynomial, it is irreducible over $\mathbb{Q}$. By Case C12 of Theorem 2.3, 2 divides $i(K)$. Hence, $K$ is not monogenic. More generally, if $F(x) = x^8 + 4p^s x + 3p$, where $p$ is a rational prime congruent to 1 modulo 8 and $s$ is a natural integer, then $F(x)$ is irreducible over $\mathbb{Q}$, and the octic number fields generated by the roots of $F(x)$ are not monogenic.

**Example 2.9.** Let $K = \mathbb{Q}(\theta)$, where $\theta$ is a root of $F(x) = x^8 + 922 + 1023$. Then $K$ is not monogenic by Case C15 of Theorem 2.3.

**Example 2.10.** Let $K = \mathbb{Q}(\theta)$, where $\theta$ is a root of $F(x) = x^8 + p^s(1 + 2h)x + p(1 + 2k)$, where $p$ is an odd rational prime, $s$ is a natural integer, $k$ and $h$ are two rational integers, with $2k \neq -1 \pmod{p}$. Then $i(K) = 1$ by Case C1 of Theorem 2.3.

3. Preliminary Results

Let $K$ be a number field generated by $\theta$, a root of a monic irreducible trinomial $F(x) = x^8 + ax + b \in \mathbb{Z}[x]$ and $\mathbb{Z}_K$ its ring of integers. Let $p$ be a rational prime. We start by stating the following Lemma which gives a necessary and sufficient condition for a rational prime $p$ to be a prime common index divisor of $K$. This Lemma will play an essential role in the proof of our results. It is a consequence of Dedekind’s Theorem on the factorization of primes in number fields (see [35, Theorems 4.33 and 4.34] and [10]).

**Lemma 3.1.** Let $p$ be a rational prime and $K$ be a number field. For every positive integer $f$, let $L_p(f)$ be the number of distinct prime ideals of $\mathbb{Z}_K$ lying above $p$ with residue degree $f$, and $N_p(f)$ the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree $f$. Then $p$ is a common index divisor of $K$ if and only if $L_p(f) > N_p(f)$, for some positive integer $f$.

Since the given condition in Lemma 3.1 for a prime $p$ to divide $i(K)$ depends upon the factorization of $p$ in $\mathbb{Z}_K$, we need to determine the number of distinct prime ideals of $\mathbb{Z}_K$ lying above $p$. We will use Newton polygon techniques. This method was introduced by Ore [36] and developed profoundly by Guàrdia, Montes and Nart [14, 23, 24, 34]. So, let us briefly recall some fundamental notions and results of this method. The reader can see also [8, pages 617-618]. Let $p$ be a rational prime and $\nu_p$ the discrete valuation of $\mathbb{Q}_p(x)$ defined on $\mathbb{Z}_p[x]$ by

$$
\nu_p \left( \sum_{i=0}^{m} a_i x^i \right) = \min \{ \nu_p(a_i), 0 \leq i \leq m \}.
$$

Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo $p$ is irreducible. Upon the Euclidean division by successive powers of $\phi(x)$, the polynomial $F(x) \in \mathbb{Z}[x]$ admits a unique $\phi$-adic development

$$
F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^n,
$$

where $a_i(x)$ are polynomials in $\mathbb{Z}[x]$. The polynomial $F(x)$ is said to be $\phi$-monic if $a_0(x)$ is monic.
where \( a_i(x) \in \mathbb{Z}_p[x] \) and \( \deg(a_i(x)) < \deg(\phi(x)) \). For every \( 0 \leq i \leq n \), let \( u_i = \nu_p(a_i(x)) \).

The \( \phi \)-Newton polygon of \( F(x) \) with respect to \( p \) is the lower convex hull of the points

\[
\{(i, u_i) \mid 0 \leq i \leq n, a_i(x) \neq 0\}
\]

in the Euclidean plane, which we denote by \( N_\phi(F) \). The polygon \( N_\phi(F) \) is the union of different adjacent sides \( S_1, S_2, \ldots, S_g \) with increasing slopes \( \lambda_1, \lambda_2, \ldots, \lambda_g \). We shall write \( N_\phi(F) = S_1 + S_2 + \cdots + S_g \). The polygon determined by the sides of negative slopes of \( N_\phi(F) \) is called the \( \phi \)-principal Newton polygon of \( F(x) \) with respect to \( p \) and will be denoted by \( N_\phi^+(F) \). The length of \( N_\phi^+(F) \) is \( l(N_\phi^+(F)) = \nu_p(F(x)) \); the highest power of \( \phi \) dividing \( F(x) \) modulo \( p \).

Let \( \mathbb{F}_p \) be the finite field \( \mathbb{Z}[x]/(p, \phi(x)) \simeq \mathbb{F}_p[x]/(\overline{\phi(x)}) \). We attach to any abscissa \( 0 \leq i \leq l(N_\phi^+(F)) \) the following residue coefficient \( c_i \in \mathbb{F}_p^* : \)

\[
c_i = \begin{cases} 
0, & \text{if } (i, u_i) \text{ lies strictly above } N_\phi^+(F), \\
\frac{a_i(x)}{p^{u_i}} \pmod{(p, \phi(x))}, & \text{if } (i, u_i) \text{ lies on } N_\phi^+(F).
\end{cases}
\]

Let \( S \) be one of the sides of \( N_\phi^+(F) \). Then the length of \( S \), denoted \( l(S) \), is the length of its projection to the horizontal axis and its height, denoted \( b(S) \), is the length of its projection to the vertical axis. Let \( \lambda = -\frac{b(S)}{l(S)} = -\frac{h}{e} \) be its slope, where \( e \) and \( h \) are two positive coprime integers. The degree of \( S \) is \( d(S) = \gcd(b(S), l(S)) = \frac{l(S)}{e} \), it is equal to the number of segments into which the integral lattice divides \( S \). More precisely, if \( (s, u_s) \) is the initial point of \( S \), then the points with integer coordinates lying in \( S \) are exactly

\[
(s, u_s), \ (s + e, u_s - h), \ldots, (s + de, u_s - dh).
\]

The natural integer \( e = \frac{l(S)}{d(S)} \) is called the ramification index of the side \( S \) and denoted by \( e(S) \). We attach to \( S \) the following residual polynomial:

\[
R_\lambda(F)(y) = c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in \mathbb{F}_p[y].
\]

The \( \phi \)-index of \( F(x) \), denoted by \( ind_\phi(F) \), is \( \deg(\phi) \) multiplied by the number of points with natural integer coordinates that lie below or on the polygon \( N_\phi^+(F) \), strictly above the horizontal axis and strictly below the vertical axis (see [13], Def. 1.3).

Now, let \( \overline{F(x)} = \prod_{i=1}^r \phi_i(x)^{t_i} \) be the factorization of \( \overline{F(x)} \) into a product of powers of distinct monic irreducible polynomials in \( \mathbb{F}_p[x] \). For every \( i = 1, \ldots, t \), let \( N_\phi(F) = S_{i1} + \cdots + S_{ir} \) and for every \( j = 1, \ldots, r_i \), let \( R_{\lambda_{ij}}(F)(y) = \prod_{s=1}^{t_{ij}} \psi^{n_{ij}^s}(y) \) be the factorization of \( R_{\lambda_{ij}}(F)(y) \) into a product of powers of distinct irreducible polynomials in \( \mathbb{F}_p[y] \). The polynomial \( F(x) \) is said to be \( \phi \)-regular with respect to \( p \) if, for each side \( S_{ij} \) of \( N_\phi^+(F) \), the residual polynomial \( R_{\lambda_{ij}}(F)(y) \) is separable in \( \mathbb{F}_p[y] \) (that means that \( n_{ij}^s = 1 \), for all \( s = 1, \ldots, s_{ij} \)). The polynomial \( F(x) \) is said to be \( p \)-regular if it is \( \phi \)-regular, for every \( 1 \leq i \leq t \). By the corresponding statements of the product, the polygon and the residual polynomial (see [28], Theorems 1.13, 1.15 and 1.19), we have the following theorem of Ore, which will be often used in the proofs of our theorems (see [14], Theorem 1.7 and Theorem 1.9, [33] and [36]).
Theorem 3.2. (Ore’s Theorem)
Under the above notations, we have:

\[ \nu_p((\mathbb{Z}_K : \mathbb{Z}[\theta]]) \geq \sum_{i=1}^{t} \text{ind}_{\phi_i}(F). \]

Moreover, the equality holds if \( F(x) \) is \( p \)-regular.

(2) If \( F(x) \) is \( p \)-regular, then the factorization of the ideal \( p\mathbb{Z}_K \) into a product of powers of prime ideals of \( \mathbb{Z}_K \) is

\[ p\mathbb{Z}_K = \prod_{i=1}^{t} \prod_{j=1}^{r_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ij}^{e_{ij}}, \]

where \( e_{ij} \) is the ramification index of the side \( S_{ij} \) and \( f(\mathfrak{p}_{ij}/p) = \deg(\phi_i) \times \deg(\psi_{ij}) \) is the residue degree of \( \mathfrak{p}_{ij} \) over \( p \) for every \( (i,j,s) \).

The following result is an immediate consequence of the above theorem.

Corollary 3.3. Under the above hypotheses, the following statements hold:

(1) If \( l_i = 1 \) for some \( i = 1, \ldots, r \), then the factor \( \phi_i(x) \) of \( F(x) \) modulo \( p \) provides a unique prime ideal of \( \mathbb{Z}_K \) lying above \( p \), of residue degree equals \( \deg(\phi_i(x)) \) and ramification index 1.

(2) If \( N^+_\phi(F) = S_{11} \) has only one side of degree 1 for some \( i = 1, \ldots, r \), then the factor \( \phi_i(x) \) of \( F(x) \) modulo \( p \) provides a unique prime ideal of \( \mathbb{Z}_K \) lying above \( p \), of residue degree equals \( \deg(\phi_i(x)) \) and ramification index \( l_i \).

We recall the following example when we apply Ore’s Theorem (see [6, Example 3.2]).

Example 3.4.
Consider the monic irreducible polynomial \( F(x) = x^6 + 24x + 15 \in \mathbb{Z}[x] \), which factors in \( \mathbb{F}_2[x] \) into \( F(x) = (\phi_1(x) \cdot \phi_2(x))^2 \), where \( \phi_1(x) = x - 1 \) and \( \phi_2(x) = x^2 + x + 1 \). The \( \phi_1 \)-adic development of \( F(x) \) is

\[ F(x) = \phi_1(x)^6 + 6 \phi_1(x)^5 + 15 \phi_1(x)^4 + 20 \phi_1(x)^3 + 15 \phi_1(x)^2 + 30 \phi_1(x) + 40. \]

Thus \( N^+_\phi(F) = S_{11} + S_{12} \) has two sides of degree 1 each joining the points \( (0, 3), (1, 1) \) and \( (2, 0) \). Their attached residual polynomials are \( R_{\lambda_{11}}(F)(y) = R_{\lambda_{12}}(F)(y) = 1 + y \), which are irreducible polynomials in \( \mathbb{F}_{\phi_1}[y] \simeq \mathbb{F}_2[y] \) as they are of degree 1. Thus, \( F(x) \) is \( \phi_1 \)-regular. The \( \phi_2 \)-adic development of \( F(x) \) is

\[ F(x) = \phi_2(x)^3 - 3x\phi_2(x)^2 + (2x - 2)\phi_2(x) + 24x + 16. \]

Since \( \nu_2(24x + 16) = \min(\nu_2(24), \nu_2(16)) \geq 3 \), we have \( N^+_\phi(F) = S_{21} + S_{22} \) has two sides of degree 1 each (see FIGURE 1). Thus \( R_{\lambda_{2k}}(F)(y) \) is irreducible over \( \mathbb{F}_{\phi_2} \) for \( k = 1, 2 \). Then \( F(x) \) is \( \phi_2 \)-regular. Hence, \( F(x) \) is 2-regular. By Theorem 3.2, one gets:

\[ \nu_2(\text{ind}(F)) = \nu_2((\mathbb{Z}_K : \mathbb{Z}[\theta]]) = \text{ind}_{\phi_1}(F) + \text{ind}_{\phi_2}(F) = 1 + 1 = 2, \]

and

\[ 2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{211}\mathfrak{p}_{221}, \]

with residue degrees \( f(\mathfrak{p}_{111}/2) = f(\mathfrak{p}_{121}/2) = 1 \) and \( f(\mathfrak{p}_{211}/2) = f(\mathfrak{p}_{221}/2) = 2 \).
When the polynomial $F(x)$ is not $p$-regular, that is some factors of $F(x)$ provided by Hensel’s factorization and refined by residual polynomials $R_{\lambda_1}(F)(y)$ are not irreducible in $\mathbb{Q}_p(x)$, then Guàrdia, Montes, and Nart, introduced an efficient algorithm to complete the factorization of the principal ideal $p\mathbb{Z}_K$ (see [23, 24]). They defined the Newton polygon of order $r$ and they proved an extension of the theorem of the product, theorem of the polygon, theorem of the residual polynomial, and theorem of the index in order $r$. As we will use this algorithm in second order; $r = 2$, we shortly recall those concepts that we use throughout. Let $\phi(x)$ be a monic irreducible factor of $F(x)$ modulo $p$. Let $S$ be a side of $N_1 = N_\phi(F)$, with slope $\lambda = -\frac{h}{e}$, where $h$ and $e$ are two coprime positive integers. Assume that $R_\lambda(F)(y)$ is not separable in $\mathbb{F}_p[y]$ and has an irreducible factor $\psi(y)$ of degree $f$. A type of order 2 associated to $\lambda, \phi(x)$ and $\psi(y)$ is a data:

$$T = (\phi(x); \lambda, \Phi_2(x)),$$

where $\Phi_2(x)$ is a monic irreducible polynomial in $\mathbb{Z}_p[x]$ of degree $m_2 = e \cdot f \cdot \deg(\phi)$ such that

1. $N_1(\Phi_2)$ is one-sided with slope $\lambda$.
2. The residual polynomial of $\Phi_2$ in first order, $R_\lambda(\Phi_2)(y) = \psi_1(y)$ in $\mathbb{F}_p[y]$ (up to multiply by a nonzero element of $\mathbb{F}_p$).

The polynomial $\Phi_2$ induces a valuation $\nu_p^{(2)}$ on $\mathbb{Q}_p(x)$, called the augmented valuation of $\nu_p$ of second order with respect to $\lambda, \phi(x)$ and $\psi(y)$. Moreover, by [23] Proposition 2.7, if $P(x) \in \mathbb{Z}_p[x]$ such that $P(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_t(x)\phi(x)^t$, then

$$\nu_p^{(2)}(P(x)) = e \times \min_{0 \leq j \leq l} \{\nu_p(a_i(x)) + i|\lambda|\}.$$

Let $F(x) = A_0(x) + A_1(x)\Phi_2(x) + \cdots + A_t(x)\Phi_2(x)^t$ be the $\Phi_2$-adic development of $F(x)$ and let $\mu_i^{(2)} = \nu_p^{(2)}(a_i(x)\Phi_2(x)^i) = \nu_p^{(2)}(a_i(x)) + i\nu_p^{(2)}(\Phi_2(x))$, for every $0 \leq i \leq t$. The $\Phi_2$-Newton polygon of $F(x)$ of second order with respect to $T$ is the lower boundary of the convex envelope of the set of points $\{(i, \mu_i^{(2)}), 0 \leq i \leq t\}$ in the Euclidean plane, which we denote by $N_2(F)$. We will use the theorem of the polygon and the theorem of the residual polynomial in second order ([23 Theorems 3.1 and 3.4]). For more details, we refer to the paper [23] by Guàrdia, Montes and Nart.
4. PROOFS OF MAIN RESULTS

Let $\overline{F(x)} = \prod_{i=1}^{r} \phi_i(x)^{d_i}$ be the factorization of $\overline{F(x)}$ into a product of powers of distinct monic irreducible polynomials in $\mathbb{F}_p[x]$. If $\deg(\phi_i(x)) = d_i$, then we write $F = [d_1, \ldots, d_r]$. Now, we prove our first main theorem.

**Proof of Theorem 2.1.** By Żyliński’s condition, if $p$ divides $i(K)$, then $p < 8$ (see [33, 40]). Therefore, the candidate odd prime integers to be a common index divisor of $K$ are 3, 5, and 7. So, it is sufficient to show that $3 \mid i(K)$, $5 \mid i(K)$ and $7 \mid i(K)$. Also, by [33, Proposition 2.13], for any $\eta \in \mathbb{Z}_K$, we have the following index formula:

$$\nu_p(D(\eta)) = 2\nu_p(\langle \mathbb{Z}_K : \mathbb{Z}[\eta] \rangle) + \nu_p(D_K),$$

(4.1)

where $D(\eta)$ is the discriminant of the minimal polynomial of $\eta$ and $D_K$ is the discriminant of $K$. By the definition (1.1) of $i(K)$ and the above equation, if $p$ divides $i(K)$, then $p^2$ divides $\Delta(F)$. Recall that

$$\Delta(F) = 2^{24}b^7 - 7^7a^8.$$  

(4.2)

(1)– Let us show that $3$ does not divide $i(K)$. If $3$ divides $i(K)$, then by (4.1) and (4.2), we see that $(a, b) \in \{(0, 0), (1, 1), (-1, 1)\}$ (mod 3). We need to distinguish three cases:

(a) If $a \equiv 1 \pmod{3}$ and $b \equiv 1 \pmod{3}$, then $\overline{F(x)} = \phi_1(x)^2 \phi_2(x)$ in $\mathbb{F}_3[x]$, where $\phi_1(x) = x - 1$ and $\phi_2(x) = x^6 - x^5 + x^3 - x^2 + 1$. By Corollary 3.3(2), the factor $\phi_2(x)$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 of residue degree 6. By the Fundamental Equality, we see that $3\mathbb{Z}_K \in \{[1, 1, 6], [1^2, 6], [2, 6]\}$. Thus, by Lemma 3.1, 3 does not divide $i(K)$.

(b) The case when $a \equiv -1 \pmod{3}$ and $b \equiv 1 \pmod{3}$ is similar to the above case.

(c) If $3$ divides both $a$ and $b$, then $\overline{F(x)} = \phi_1(x)^3$ in $\mathbb{F}_3[x]$, where $\phi_1(x) = x$. By the hypothesis (2.1), we discuss four cases:

- If $8\nu_3(a) > 7\nu_3(b)$ and $\nu_3(b) \in \{1, 3, 5, 7\}$, then $N_{\phi_1}^+(F) = S_{11}$ has only one side of degree 1 joining $(0, \nu_3(b))$ and $(8, 0)$ with ramification index equals 8. By Corollary 3.3(2), $3\mathbb{Z}_K = p_{11}^3$ with $f(p_{11}/3) = 1$. By Lemma 3.1, 3 does not divide $i(K)$.

- If $8\nu_3(a) > 7\nu_3(b)$ and $\nu_3(b) \in \{2, 6\}$, then $N_{\phi_1}(F) = S_{11}$ has only one side of degree 2 with ramification index $e_{11} = 4$. Its attached residual polynomial is $R_{\lambda_1}(y) = a_3 + y^2$. If $a_3 \equiv 1 \pmod{3}$, then $R_{\lambda_1}(y)$ is irreducible in $\mathbb{F}_3[y]$. By Theorem 3.2(2), $3\mathbb{Z}_K = p_{11}^3$, where $p_{11}$ is a prime ideal of $\mathbb{Z}_K$ of residue degree 2. If $a_3 \equiv -1 \pmod{3}$, then $R_{\lambda_1}(y) = y^2 - 1 = (y - 1)(y + 1)$ which is separable. By Theorem 3.2(2), $3\mathbb{Z}_K = p_{11}^3 \cdot p_{12}^3$, where $p_{11}$ and $p_{12}$ are two prime ideals of $\mathbb{Z}_K$ of residue degree 1 each. By Lemma 3.1, 3 does not divide $i(K)$.

- If $8\nu_3(a) > 7\nu_3(b)$ and $\nu_3(b) = 4$, then $N_{\phi_1}^+(F) = S_{11}$ has only one side of degree 4 with ramification index $e_{11} = 2$. Further, $R_{\lambda_1}(F)(y) = a_3 + y^2$. If $a_3 \equiv 1 \pmod{3}$, then $R_{\lambda_1}(y) = y^4 + 1 = (y^2 + y - 1)(y^2 - y - 1) \in \mathbb{F}_{\phi_1}[y]$. So, $F(x)$ is 3-regular. Applying Theorem 3.2(2), we see that $2\mathbb{Z}_K = p_{11}^3 \cdot p_{12}^3$, where $p_{11}$ and $p_{12}$ are two prime ideals of $\mathbb{Z}_K$ of residue degree 2 each. If $a_3 \equiv -1 \pmod{3}$, then $R_{\lambda_1}(y) = y^4 - 1 = (y - 1)(y + 1)(y^2 + 1)$ which is separable over $\mathbb{F}_{\phi_1}$. Therefore, the form of the factorization of $3\mathbb{Z}_K$ is $[1^2, 1^2, 2^2]$. Hence, by Lemma 3.1, 3 does not divide $i(K)$.

- If $8\nu_3(a) > 7\nu_3(b)$ and $\nu_3(b) = 1$, then $N_{\phi_1}(F) = S_{11}$ has only one side of degree 1 joining $(0, \nu_3(b))$ and $(8, 0)$ with ramification index equals 8. By Corollary 3.3(2), $3\mathbb{Z}_K = p_{11}^3$ with $f(p_{11}/3) = 1$. By Lemma 3.1, 3 does not divide $i(K)$.


• If \(8
\nu_3(a) < 7\nu_3(b)\) and \(\nu_3(a) \leq 6\), then \(N_{\mathbb{Q}}^+(F) = S_{11} + S_{12}\) has two sides of degree 1 each joining \((0, \nu_3(b)), (1, \nu_3(a))\) and \((8, 0)\) with respective ramification indices equal 1 and 7. Thus, the residual polynomials \(R_{\lambda_{11}}(F)(y)\) and \(R_{\lambda_{12}}(F)(y)\) are separable as they are of degree 1. By Theorem 3.2 we see that \(3\mathbb{Z}_K = p_{111} \cdot p_{211}\) where \(p_{111}\) and \(p_{211}\) are two prime ideals of \(\mathbb{Z}_K\) of residue degree 1 each. By Lemma 3.1, 2 does not divide \(i(K)\).

We conclude that in each case, 3 does not divide \(i(K)\).

(2)– Let us prove that 5 does not divide \(i(K)\). According to (4.1) and (4.2), if 5 divides \(i(K)\), then \((a, b) \in \{(0, 0), (1, 2), (2, 2), (-2, 2), (-1, 2)\}\) \(\pmod{5}\). Reducing \(F(x)\) modulo 5 and determining the corresponding Newton’s polygon, then by applying Theorem 3.2 and using the Fundamental Equality ([9, Theorem 4.8.5]), we obtain Table 2 which gives the form of the factorization of \(5\mathbb{Z}_K\).

<table>
<thead>
<tr>
<th>Conditions</th>
<th>(F(x)) (\pmod{5})</th>
<th>Factorization of (5\mathbb{Z}_K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(8\nu_3(a) &gt; 7\nu_3(b)) and (\nu_3(b) \in {1, 3, 5, 7})</td>
<td>(1^6)</td>
<td>([1^6])</td>
</tr>
<tr>
<td>(8\nu_3(a) &gt; 7\nu_3(b), \nu_3(b) \in {2, 6}) and (a_5 \equiv \pm 1\pmod{5})</td>
<td>(1^6)</td>
<td>([1^6, 1^1])</td>
</tr>
<tr>
<td>(8\nu_3(a) &gt; 7\nu_3(b), \nu_3(b) \in {2, 6}) and (a_5 \equiv \pm 2\pmod{5})</td>
<td>(1^8)</td>
<td>([2^4, 2^2])</td>
</tr>
<tr>
<td>(\nu_5(a) \geq 4, \nu_5(b) = 4) and (a_5 \equiv 1\pmod{5})</td>
<td>(1^8)</td>
<td>([2^4, 2^2])</td>
</tr>
<tr>
<td>(\nu_5(a) \geq 4, \nu_5(b) = 4) and (a_5 \equiv \pm 2\pmod{5})</td>
<td>(1^8)</td>
<td>([2^4, 2^2])</td>
</tr>
<tr>
<td>(\nu_5(a) \geq 4, \nu_5(b) = 4) and (a_5 \equiv -1\pmod{5})</td>
<td>(1^8)</td>
<td>([1^2, 1^2, 1^2, 1^2])</td>
</tr>
<tr>
<td>(8\nu_5(a) &lt; 7\nu_5(b)) and (\nu_5(a) \leq 6)</td>
<td>(1^6)</td>
<td>([1, 1^1])</td>
</tr>
<tr>
<td>(a \equiv 1\pmod{5}) and (b \equiv 2\pmod{5})</td>
<td>(1^4, 3^3)</td>
<td>([1, 1, 3, 3], [1^4, 3, 3, \text{ or } 2, 3, 3])</td>
</tr>
<tr>
<td>(a \equiv 2\pmod{5}) and (b \equiv 2\pmod{5})</td>
<td>(1^4, 3^3)</td>
<td>([1, 1, 3, 3], [1^4, 3, 3, \text{ or } 2, 3, 3])</td>
</tr>
<tr>
<td>(a \equiv -2\pmod{5}) and (b \equiv 2\pmod{5})</td>
<td>(1^4, 3^3)</td>
<td>([1, 1, 3, 3], [1^4, 3, 3, \text{ or } 2, 3, 3])</td>
</tr>
<tr>
<td>(a \equiv -1\pmod{5}) and (b \equiv 2\pmod{5})</td>
<td>(1^4, 3^3)</td>
<td>([1, 1, 3, 3], [1^4, 3, 3, \text{ or } 2, 3, 3])</td>
</tr>
</tbody>
</table>

Table 2. The factorization of \(5\mathbb{Z}_K\)

According to Table 2, \(L_5(1) \leq 4\) for all \(a\) and \(b\). By Lemma 3.1, we conclude that in every case, 5 does not divide \(i(K)\).

(3)– By the same method used above, we get that 7 is not a prime common index divisor of \(K\).

Now, let us prove Theorem 2.1.

Proof of Theorem 2.1

Case C1: \(a \equiv 1\pmod{2}\) and \(b \equiv 1\pmod{2}\). In this case, \(\overline{F(x)} = \phi_1(x)\phi_2(x)\pmod{F_2[x]}\), where \(\phi_1(x) = x^2 + x + 1\) and \(\phi_2(x) = x^6 + x^5 + x^3 + x^2 + 1\). By Corollary 3.2(1), we get \(2\mathbb{Z}_K = p_{111} \cdot p_{211}\), where \(f(p_{111}/2) = 2\) and \(f(p_{211}/2) = 6\). By Lemma 3.1, 2 does not divide \(i(K)\).

Case C2: \(a \equiv 1\pmod{2}\) and \(b \equiv 0\pmod{2}\). In this case, \(\overline{F(x)} = \phi_1(x)\phi_2(x)\phi_3(x)\phi_4(x)\pmod{F_2[x]}\), where \(\phi_1(x) = x\), \(\phi_2(x) = x + 1\), \(\phi_3(x) = x^3 + x + 1\) and \(\phi_4(x) = x^3 + x^2 + 1\). By Corollary 3.2(1), we see that

\[2\mathbb{Z}_K = p_{111} \cdot p_{211} \cdot p_{311} \cdot p_{411}.\]
where \( f(p_{111}/2) = f(p_{211}/2) = 1 \) and \( f(p_{311}/2) = f(p_{411}/2) = 3 \). Therefore, by Lemma 3.1, 2 does not divide \( i(K) \).

**Case C3:** \( 1 \leq \nu_2(a) \leq 6 \) and \( 8\nu_2(a) < 9\nu_2(b) \). In this case, \( F(x) = \phi_1(x)^8 \) in \( \mathbb{F}_2[x] \), where \( \phi_1(x) = x \). Thus, \( N_{\phi_1}^+(F) = S_{11} \) has two sides of degree 1 each joining the points \((0, \nu_2(b)), (1, \nu_2(a))\) and \((8, 0)\) with respective ramification indices \( e_{11} = 1 \) and \( e_{12} = 7 \). Thus, for \( k = 1, 2 \), \( R_{\lambda_k}(F)/(y) \) is irreducible as it is linear. Thus, \( F(x) \) is 2-regular. By applying Theorem 3.2(2), we see that

\[
2\mathbb{Z}_K = p_{111} \cdot p_{211}^7,
\]

where \( p_{111} \) and \( p_{211} \) are two prime ideals of \( \mathbb{Z}_K \) of residue degree 1 each. Hence, 2 does not divide \( i(K) \).

**Case C4:** \( \nu_2(b) \in \{1, 3, 5, 7\} \) and \( 8\nu_2(a) > 9\nu_2(b) \). As well as, \( F(x) = \phi_1(x)^8 \) in \( \mathbb{F}_2[x] \), where \( \phi_1(x) = x \). Moreover, \( N_{\phi_1}^+(F) = S_{11} \) has only one side of degree 1 joining the points \((0, \nu_2(b)), (8, 0)\) with a ramification index equals to 8. Using Corollary 3.3(2), we get \( 2\mathbb{Z}_K = p_{111} \), where \( f(p_{111}/2) = 1 \). Therefore, 2 does not divide \( i(K) \).

**Case C5:** \( \nu_2(b) \in \{2, 6\} \) and \( 8\nu_2(a) > 9\nu_2(b) \). In this case, \( F(x) = \phi_1(x)^8 \) in \( \mathbb{F}_2[x] \), where \( \phi_1(x) = x \). Further, \( N_{\phi_1}^+(F) = S_{11} \) has only one side of degree 2 joining the points \((0, 2)\) and \((8, 0)\) with ramification index \( e_{11} = 4 \). It follows that \( 2\mathbb{Z}_K = a^4 \), where \( a \) is a non-zero ideal of \( \mathbb{Z}_K \). By the Fundamental Equality (2.2), the factorization of \( 2\mathbb{Z}_K \) has the form \([18], [1^4, 1^4] \) or \([2^4]\). By Lemma 3.1, 2 does not divide \( i(K) \).

- In the cases C6-C7-C8, we have \( \nu_2(a) \geq 4, \nu_2(b) = 4 \), \( F(x) = \phi_1(x)^8 \) in \( \mathbb{F}_2[x] \), where \( \phi_1(x) = x \). Further, \( N_{\phi_1}^+(F) = S_{11} \) has only one side of degree 4 joining the points \((0, 4)\) and \((8, 0)\) with slope \( \lambda_{11} = \frac{1}{4} \). Its attached residual polynomial \( R_{\lambda_1}(y) = (y-1)^4 \in \mathbb{F}_{\phi_1}[y] \) is not separable. Thus, \( F(x) \) is not 2-regular with respect to \( \nu_2 \). So, Ore's Theorem (Theorem 3.2) is not applicable. To factorize the ideal \( 2\mathbb{Z}_K \), we analyze second order Newton polygons. Let \( \psi(y) = y - 1 \) and \( \Phi_2(x) = x^2 - ax - \beta \in \mathbb{Z}_2[x] \), where \( a \) and \( \beta \) are 2-adic numbers such that \( \nu_2(a) \geq 1 \) and \( \nu_2(\beta) = 1 \). One can check that \( \Phi_2(x) \) is a key polynomial with respect \( \lambda_{11}, \phi_1(x) \) and \( \psi(y) \). Let \( \nu_2^{(2)} \) be the valuation of second order induced by \( \Phi_2 \). The \( \Phi_2 \)-adic development of \( F(x) \) is given by:

\[
F(x) = \Phi_2(x)^4 + A_3(x)\Phi_2(x)^3 + A_2(x)\Phi_2(x)^2 + A_1(x)\Phi_2(x) + A_0(x), \quad (4.3)
\]

where:

- \( A_0(x) = (a^7 + 4a^5\beta + 8a^3\beta^2 + 4a^3\beta + a)x + 2a^6 + 6a^2\beta^3 + a^6\beta + a^4\beta^2 + b + \beta^4 \),
- \( A_1(x) = (10a^5 + 34a^3\beta + 24a\beta^2)x + a^5 + 12a^4\beta + 30a^2\beta + 8\beta^3 \),
- \( A_2(x) = (14a^3 + 12a\beta)x + 9a^4 + 30a^2\beta + 6\beta^2 \),
- \( A_3(x) = 4ax + 6a^2 + 4\beta \).

Further, by [23] Theorem 2.11 and Proposition 2.7, we have

- \( \nu_2^{(2)}(\Phi_2(x)) = 2 \),
- \( \nu_2^{(2)}(\Phi_2^2(x)) = 8 \),
- \( \nu_2^{(2)}(A_3(x)\Phi_2(x)^3) \geq 12 \),
- \( \nu_2^{(2)}(A_2(x)\Phi_2(x)^2) = 10 \),
- \( \nu_2^{(2)}(A_1(x)\Phi_2(x)) = 13 \).
Thus, $N_2(F)$; the $\Phi_2$-Newton polygon of second order with respect $\nu_2^{(2)}$, is the lower convex hull of the points $(0, \mu_0^{(2)}), (1, 13), (2, 10)$ and $(4, 8)$, where $\mu_0^{(2)} = \nu_2^{(2)}(A_0(x))$. Note that in this case, the residual field in second order $\mathbb{F}^{(2)} = \mathbb{F}_{\phi_1}[y]/(y-1)$ isomorphic to $\mathbb{F}_2$.

**Case C6:** $a \equiv 16 \pmod{32}$ and $b \equiv 16 \pmod{32}$. In this case, $\nu_2(a) = 4$. Thus, $\mu_0^{(2)} = 9$. It follows by (4.3) that $N_2(F) = S_{11}^{(2)}$ has only one side of degree 1 with slope $\lambda_{11}^{(2)} = \frac{-1}{4}$ joining the points $(0, 9)$ and $(4, 8)$. Thus $R_{11}^{(2)}(F)(y)$ is separable as it is of degree 1. Using Theorems 3.1 and 3.4 of [23], we see that $2\mathbb{Z}_K = (p_{111}^{4})^2 = p_{111}^{8}$, where $p_{111}$ is a prime ideal of $\mathbb{Z}_K$ of residue degree 1.

**Case C7:** $a \equiv 32 \pmod{64}$ and $b \equiv 48 \pmod{64}$. Take $\beta = 2$. Note that $\nu_2(a) = 5$. It follows that $\mu_0^{(2)} = 11$. We proceed as in the above case, we see that the factorization of $2\mathbb{Z}_K$ has the form $[18]$.

**Case C8:** $a \equiv 0 \pmod{64}$ and $b \equiv 48 \pmod{128}$. Take again $\beta = 2$. Here, $\nu_2(a) \geq 6$, $\nu_2(b+16) = 6$. So, $\mu_0^{(2)} = 12$. It follows by (4.3) that $N_2(F) = S_{11}^{(2)}$ has only one side of degree 2 joining the points $(0, 12), (2, 10)$ and $(4, 0)$. Its slope is $\lambda_{11}^{(2)} = -1$. Further, $R_{11}^{(2)}(F)(y) = y^2 + y + 1$. Then it is irreducible in $\mathbb{F}^{(2)}[y]$. So, $F(x)$ is 2-regular with respect to $\nu_2^{(2)}$. By Theorems 3.1 and 3.4 in [23], we see that $2\mathbb{Z}_K = p_{111}^{6}$, where $p_{111}$ is a prime ideal of $\mathbb{Z}_K$ of residue degree 2.

- In the rest of the cases, 2 divides $a$, but does not divide $b$. Then $\bar{F}(x) = \phi_1(x)^8$ in $\mathbb{F}_2[x]$, where $\phi_1(x) = x - 1$. As in [6], the $\phi_1$-adic development of $F(x)$ is

$$F(x) = 1 + a + b + (a + 8)\phi_1(x) + \sum_{j=2}^{8} \binom{8}{j} \phi_1(x)^j.$$  \hspace{1cm} (4.4)

Let $\mu_0 = \nu_2(1 + a + b)$ and $\mu_1 = \nu_2(8 + a)$. Notice that $\nu_2\left(\binom{8}{j}\right) = 3 - \nu_2(j)$, for every $j = 2, \ldots, 8$. It follows that $N_{\phi_1}^{+}(F)$ is the lower convex hull of the points $(0, \mu_0), (1, \mu_1), (2, 2), (4, 1)$ and $(8, 0)$.

**Case C9:** $(a, b) \in \{(0, 1), (2, 3)\} \pmod{4}$. In this case, $\mu_0 = 1$ and $\mu_1 \geq 1$. It follows that $N_{\phi_1}^{+}(F) = S_{11}$ has only one side of degree 1 with ramification index equals 8. Using Corollary [3.3][2], we see that $2\mathbb{Z}_K = p_{111}^{6}$, where $f(p_{111}/2) = 1$. Consequently, 2 is not a prime common index divisor of $K$.

**Case C10:** $a \equiv 2 \pmod{4}$ and $b \equiv 1 \pmod{4}$. In this case, $\mu_0 \geq 2$ and $\mu_1 = 1$. Thus, $N_{\phi_1}^{+}(F) = S_{11} + S_{12}$ has two sides of degree 1 each joining the points $(0, \mu_0), (1, 1)$ and $(8, 0)$ with respective ramification indices 1 and 7. Their attached residual polynomials are $R_{\lambda_{11}}(F)(y) = R_{\lambda_{12}}(F)(y) = y - 1 \in \mathbb{F}_{\phi_1}[y]$. Thus, $F(x)$ is 2-regular. By Theorem [3.2][2], we obtain that $2\mathbb{Z}_K = p_{111} \cdot p_{121}$, where $p_{111}$ and $p_{121}$ are two prime ideals of $\mathbb{Z}_K$ of residue degree 1 each. In view of Lemma [3.1][2] does not divide $i(K)$.

**Case C11:** $(a, b) \in \{(0, 4), (4, 7)\} \pmod{8}$. In this case, $\mu_0 = 2$ and $\mu_1 \geq 2$. It follows that $N_{\phi_1}^{+}(F) = S_{11}$ has only one side of degree 2 joining the points $(0, 2), (4, 1)$ and $(8, 0)$ with ramification index equals 4. Further, we have $R_{\lambda_{11}}(F)(y) = y^2 + y + 1$, which is separable over $\mathbb{F}_{\phi_1} \cong \mathbb{F}_2$. So, Theorem [3.2][2] is applicable. Therefore, we see that $2\mathbb{Z}_K = p_{111}^{4}$, where $f(p_{111}/2) = 2$. So, 2 does not divide $i(K)$.
Case C12: $a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$. This case has been previously studied (see Theorem 2.1 of [6]). We found that $2\mathbb{Z}_K = p_{111} \cdot p_{121} \cdot p_{131}^{3}$, where $f(p_{1k1}/2) = 1$ for $k = 1, 2, 3$. By Lemma 3.1, $2$ divides $i(K)$. Further, according to Figure 2, Page 621 of [6], and by Theorem 3.2, we see that $\nu_2(\mathbb{Z}_K : \mathbb{Z}[\theta]) = 5$.

Case C13: $(a, b) \in \{(0, 7), (8, 15)\} \pmod{16}$. In this case, $\mu_0 = 3$ and $\mu_1 \geq 3$. It follows that $N^+_{\phi_1}(F) = S_{11} + S_{12} + S_{13}$ joining the points $(0, 3), (2, 2), (4, 1)$ and $(8, 0)$. Here, we have $d(S_{11}) = 2, d(S_{12}) = 4, \lambda_{11}(F) = y^2 + y + 1, \lambda_{12}(F) = y + 1 \in \mathbb{F}_{\phi_1}[y]$. So, Theorem 3.2 is applicable. Therefore, $2\mathbb{Z}_K = p_{111}^2 \cdot p_{121}^4 \cdot p_{131}^4$, where $f(p_{111}/2) = 2$ and $f(p_{1k1}/2) = 1$ for $k = 2, 3$. Hence, by Lemma 3.1, $2$ does not divide $i(K)$.

Case C14: $(a, b) \in \{(0, 15), (16, 31)\} \pmod{32}$. In this case, $\mu_0 = 4$ and $\mu_1 = 3$. It follows that $N^+_{\phi_1}(F) = S_{11} + S_{12} + S_{13}$ joining the points $(0, 4), (1, 3), (2, 2), (4, 1)$ and $(8, 0)$. Further, we have $d(S_{11}) = 2, d(S_{12}) = d(S_{13}) = 4, e_{11} = 2, e_{12} = 2, e_{13} = 4$ and $R_{\lambda_{11}}(F) = y^2 + y + 1, R_{\lambda_{12}}(F) = R_{\lambda_{13}}(F) = y + 1 \in \mathbb{F}_{\phi_1}[y]$. Thus, $F(x)$ is 2-regular. By Theorem 3.2, we have $2\mathbb{Z}_K = p_{111}^2 \cdot p_{121}^4 \cdot p_{131}^4$, where $f(p_{1k1}/2) = 2$ and $f(p_{1k1}/2) = 1$ for $k = 2, 3$. Hence, by Theorem 3.2, we get $\nu_2(\mathbb{Z}_K : \mathbb{Z}[\theta]) = 7$.

Case C15: $(a, b) \in \{(0, 31), (16, 15)\} \pmod{32}$. This case has been studied in [6, Theorem 2.1]. We obtained that $2\mathbb{Z}_K = p_{111} \cdot p_{121}^2 \cdot p_{131}^2 \cdot p_{141}^4$, where $f(p_{1k1}/2) = 1$, for $k = 1, 2, 3, 4$. So, $2$ divides $i(K)$. Further, by the description of the polygon $N_{\phi_1}$ given in Page 621 of [6], and using Theorem 3.2, we see that

Case C16: $a \equiv 8 \pmod{16}, b \equiv 7 \pmod{32}$ and $\omega$ is odd ($\omega \geq 5$). Let $r = \frac{-b}{a^2}$ and $\psi_1(x) = x - r$ (here, $s = r$). Note $\nu_2(r) = 0$, because $\nu_2(a) = 3$. Using Binomial Theorem, we see that

$$F(x) = r^8 + ax + b + (8r^7 + a)\psi_1(x) + \sum_{j=2}^{8} \binom{8}{j} r^{8-j} \psi_1(x)^j. \tag{4.5}$$

Let

$$\begin{align*}
A_0 &= r^8 + ar + b, \\
A_1 &= 8r^7 + a, \\
\omega_0 &= \nu_2(A_0), \\
\omega_1 &= \nu_2(A_1).
\end{align*}$$

After calculations, we find that
\[
\begin{aligned}
A_0 &= \frac{2^{24}(b^7 - 7^7a_2^8)}{(7a)^8}, \\
A_1 &= \frac{-2^{24}(b^7 - 7^7a_2^8)}{(7a)^7}.
\end{aligned}
\]

It follows that \(\omega_0 = \omega\) and \(\omega_1 = \omega + 3\). Thus, \(N_{\psi_1}^+(F) = S_{11} + S_{12} + S_{13}\) has three sides of degree 1 each joining the points \((0, \omega), (2, 2), (4, 1)\) and \((8, 0)\). So, \(F(x)\) is 2-regular. By Theorem 3.2, the factorization of \(2\mathbb{Z}_K\) has the form \([1^2, 1^2, 1^4]\). Hence, 2 is a common index divisor of \(K\). Moreover, by Theorem 3.2, we get \(\nu_2((\mathbb{Z}_K : \mathbb{Z}[\theta])) = \frac{\omega + 9}{2}\).

**Case C17:** \(a \equiv 8 \pmod{16}, b = -9 \pmod{32}\) and \(A_{a,b} \equiv 0 \pmod{4}\). In this case, \(\omega = 4\). Let \(\psi_1(x) = x - 2 - r\) (here, \(s = 2 + r\)). Write

\[
F(x) = (2 + r)^8 + a(2 + r) + b + (8(2 + r)^7 + a)\psi_1(x) + \sum_{j=2}^{8} \binom{8}{j}(2 + r)^{8-j}\psi_1(x)^j. \tag{4.6}
\]

Let \(A_0 = (2 + r)^8 + a(2 + r) + b, A_1 = 8(2 + r)^7 + a, \omega_0 = \nu_2(A_0)\) and \(\omega_1 = \nu_2(A_1)\). We have

\[
A_1 = 8(2 + r)^7 + a = 2^3((2 + r)^7 + a_2).
\]

By using Binomial Theorem, we see that

\[
(2 + r)^7 = 2(7r^6 + u) + r^7,
\]

where \(u = \sum_{j=0}^{5} \binom{7}{j}2^{7-j}r^j\). It follows that

\[
A_1 = 2^3(2(7r^6 + u) + r^7 + a_2).
\]

Moreover, we have

\[
r^7 + a_2 = \frac{-2^{24}(b^7 - 7^7a_2^8)}{(7a)^7}.
\]

Thus, \(\nu_2(r^7 + a_2) = w = 4\). Note also that \(\nu_2(u) \geq 1\). Hence, \(\omega_1 = \nu_2(A_1) = 4\). On the other hand, we have

\[
A_0(x) = r^8 + ar + b + 2^4(a_2 + r^6 + r^7) + 2^8(35r^4 + 14r^5) + 2^8(1 + 4r + 7r^2 + 7r^3).
\]

After calculations, we see that

\[
r^8 + ar + b + 2^4(a_2 + r^6 + r^7) = \frac{2^{24}}{(7a)^8} \left[ b(b^7 - 7^7a_2^8) + 7 \times 2^4 \cdot a_2(7^7a_2^8 - b^7 + b^6a_2) \right],
\]

\[
= \frac{2^4}{(7a_2)^8} \left[ b(b^7 - 7^7a_2^8) + 7a_2(7^7a_2^8 - b^7 + b^6a_2) \right],
\]

\[
= \frac{2^4}{(7a_2)^8} A_{a,b}. \tag{4.8}
\]

Since \(A_{a,b} \equiv 0 \pmod{4}, \omega_0 = 5\). By the \(\psi_1\)-adic development \([4.6]\) of \(F(x)\), we have \(N_{\psi_1}^+(F) = S_{11} + S_{12} + S_{13}\) has three sides of degree 1 each joining the points \((0, 5), (2, 2), (4, 1)\) and \((8, 0)\). So, \(F(x)\) is 2-regular. By Theorem 3.2, the factorization of \(2\mathbb{Z}_K\) has the
form \([1^2, 1^2, 1^4]\). So, 2 is a common index divisor of \(K\). Further, by Theorem 3.2[1), we get \(\nu_2(\mathbb{Z}_K : \mathbb{Z}[\theta]) = 7\).

**Case C18:** \(a \equiv 8 (\text{mod } 16), b \equiv -9 (\text{mod } 32), A_{1,b}^1 \equiv 2 (\text{mod } 4)\) and \(A_{2,b}^1 \equiv 2 (\text{mod } 4)\). Write

\[
A_0 = 2^{5} \left[ (b(b^7 - 7^2 a_2^8) + 7a_2(7^2 a_2^8 - b^7 + b^8 a_2))_2 + b^4(245a_2 - 14b) \right] + 2^8(1 + 4r + 7r^2 + 7r^3).
\]

In this case, \(\omega_0 = 6\). It follows from (4.6) that \(N_{\psi_1}^+(F) = S_{11} + S_{12} + S_{13}\) has three sides of joining the points \((0, 6), (1, 4), (2, 2), (4, 1)\) and \((8, 0)\) such that \(d(S_{11}) = 2, e_{11} = 1\) and \(R_{\lambda_1}(F)(y) = y^2 + y + 1\), which is irreducible over \(\mathbb{F}_2 \simeq \mathbb{F}_2\). So, \(F(x)\) is 2-regular. By Theorem 3.2, the factorization of \(2\mathbb{Z}_K\) has the form \([2, 1^2, 1^4]\). By Lemma 3.1, 2 does not divide \(i(K)\).

**Case C19:** \(a \equiv 8 (\text{mod } 16), b \equiv -9 (\text{mod } 32), A_{1,b}^1 \equiv 2 (\text{mod } 4)\) and \(A_{2,b}^1 \equiv 0 (\text{mod } 4)\). In this case, \(\omega_0 \geq 7\). It follows that \(N_{\psi_1}^+(F) = S_{11} + S_{12} + S_{13} + S_{14}\) has four sides of degree 1 each, joining the points \((0, \omega_0), (1, 4), (2, 2), (4, 1)\) and \((8, 0)\), with \(e_{11} = e_{12} = 1\). Therefore, the factorization of \(2\mathbb{Z}_K\) has the form \([1, 1^2, 1^3]\). So, 2 divides \(i(K)\). Also, by Theorem 3.2[1), we get \(\nu_2(\mathbb{Z}_K : \mathbb{Z}[\theta]) = 8\).

\[\bullet\] From **Case C20**, we have \(\omega\) is an even natural integer greater than 6. Set \(w = 2 + 2k\) with \(k \geq 2\). Let \(\psi_1(x) = x - 2^k - r\) (here \(s = 2^k + r\)). Using Binomial Theorem, we write

\[
F(x) = (2^k + r)^8 + a(2^k + r) + b + (8(2^k + r)^7 + a)\psi_1(x) + \sum_{j=2}^{8} \binom{8}{j}(2^k + r)^{8-j}\psi_1(x)^j. \tag{4.9}
\]

Let

\[
\begin{cases}
A_0 = (2^k + r)^8 + a(2^k + r) + b, \\
\omega_0 = \nu_2(A_0), \\
A_1 = 8(2^k + r)^7 + a, \\
\omega_1 = \nu_2(A_1).
\end{cases}
\]

Clearly, for \(j = 2, \ldots, 8\), \(\nu_2\left(\binom{8}{j}(2^k + r)^{8-j}\right) = 3 - \nu_2(j)\), since \(\nu_2(r) = 0\). For \(A_1\), write

\[
A_1 = 2^3((2^k + r)^7 + a_2),
\]

\[
= 2^3(r^7 + a_2 + \sum_{j=0}^{6} \binom{7}{j} 2^{j} k r^j),
\]

\[
= 2^3(r^7 + a_2 + 2^{k} D_r),
\]

where \(D_r = \sum_{j=0}^{6} \binom{7}{j} 2^{(j-1)k} r^j\). Notice that \(D_r \in \mathbb{Z}_2\) with \(\nu_2(D_r) = 0\) and recall by 4.7 that \(\nu_2(r^7 + a_2) = \omega = 2 + 2k\). It follows that \(\omega_0 = 3 + k\). Thus, by the \(\psi_1\)-development 4.9 of \(F(x)\), \(N_{\psi_1}^+(F)\) is the lower convex hull of the points \((0, \omega_0), (1, k + 3), (2, 2), (4, 1)\) and \((8, 0)\). So, we need to compute \(\omega_0\). Using Binomial Theorem again, we get

\[
A_0 = r^8 + ar + b + 2^{2k+2} \times 7r^6 + 2^{k+3}(a_2 + r^7) + 2^{3k+3} F_r,
\]

for some 2-adic integer \(F_r\). Since \(\nu_2(a_2 + r^7) = \omega = 2 + 2k\), we see that

\[
A_0 = r^8 + ar + b + 2^{2k+2} \times 7r^6 + 2^{3k+3} E_r, \tag{4.10}
\]
where $E_r \in \mathbb{Z}_2$. Write

$$r^8 + ar + b + 2^{2k+2} \times 7r^6 = \frac{2^{24}(b^7 - 7^7a^8)}{(7a)^8} + 2^{2k+2} \times 7\left(\frac{-8b}{7a}\right)^6,$$

$$= \frac{2^{24}}{(7a)^8} \cdot 2^{2k+2} [(b^7 - 7^7a^8)_2 + 7^3 \cdot a^2b^6].$$

From the last equality and (4.10) $A_0$ becomes as follows

$$A_0 = \frac{2^{24}}{(7a)^8} \cdot 2^{2k+2} [(b^7 - 7^7a^8)_2 + 7^3 \cdot a^2b^6] + 2^{3k+3}E_r. \quad (4.11)$$

We distinguish it into three cases:

**Case C20:** $\omega \geq 6$ is even and $B_{a,b} \equiv 2 \pmod{4}$. According to (4.11) we have $\omega_0 = 2k + 3$. In follows by (4.9) that $N^+_\psi(F) = S_{11} + S_{12} + S_{13}$ has three sides of degree 1 each, joining the points $(0, 2k + 3), (2, 2), (4, 1)$ and $(8, 0)$. Their ramification indices are respectively $e_{11} = 2, e_{12} = 2$ and $e_{13} = 4$. Their attached residual polynomials $R_{\lambda_k}(F)(y)$ equal $1 + y$, for $k = 1, 2, 3$. Thus, $F(x)$ is 2-regular. By Theorem 3.2 we see that $2\mathbb{Z}_K = p_{111}^2 \cdot p_{121} \cdot p_{131}^4$, where $f(p_{1k1}/2) = 1$, for $k = 1, 2, 3$. By Lemma 3.1, 2 divides $i(K)$. Using Theorem 3.2 we have $\nu_2([\mathbb{Z}_K : \mathbb{Z}[\theta]]) = k + 6$.

**Case C21:** $\omega \geq 6$ is even and $B_{a,b} \equiv 4 \pmod{8}$. By (4.11) $\omega_0 = 2k + 4$. Thus, by (4.9) $N^+_\psi(F) = S_{11} + S_{12} + S_{13}$ has three sides, joining the points $(0, 2k + 4), (1, k+3), (2, 2), (4, 1)$ and $(8, 0)$, with $d(S_{11}) = 2, e_{11} = 1, d(S_{12}) = 1, e_{12} = 2, d(S_{13}) = 1$ and $e_{13} = 4$. Their attached residual polynomials are: $R_{\lambda_k}(F)(y) = y^2 + y + 1$, and $R_{\lambda_k}(F)(y) = y + 1$ for $k = 2, 3$, which are separable over $\mathbb{F}_2$. So, $F(x)$ is 2-regular. Therefore,

$$2\mathbb{Z}_K = p_{111} \cdot p_{121}^2 \cdot p_{131}^4,$$

where $f(p_{111}/2) = 2$ and $f(p_{1k1}/2) = 1$ for $k = 2, 3$. Consequently, 2 does not divide $i(K)$.

**Case C22:** $\omega \geq 6$ is even and $B_{a,b} \equiv 0 \pmod{8}$. Using (4.11) we get $\omega_0 \geq 2k + 5$ (note that when $k \geq 2, 3k + 3 \geq 2k + 5$). In this case, $N^+_\psi(F) = S_{11} + S_{12} + S_{13} + S_{14}$ has four sides of degree 1 each, joining the points $(0, \omega_0), (1, k + 3), (2, 2), (4, 1)$ and $(8, 0)$. We are in the position to apply Theorem 3.2. Therefore, $2\mathbb{Z}_K = p_{111} \cdot p_{121} \cdot p_{131} \cdot p_{141}$, where $f(p_{1k1}/2) = 1$, for $k = 1, 2, 3, 4$. Here, 2 divides $i(K)$. Further, by Theorem 3.2 we get $\nu_2([\mathbb{Z}_K : \mathbb{Z}[\theta]]) = k + 7$. \hfill \Box

**AN UPPER BOUND OF THE INDEX $i(K)$**

Let $K = \mathbb{Q}(\theta)$ and $F(x)$ be as in Theorem 2.3. As mentioned in Remark 2.7(1), we cannot apply Štilica’s results to compute $\nu_2(i(K))$ when $i(K)$ it is not trivial. According to the definition (1.1) of the index $i(K)$, if $p$ divides $i(K)$, then $\nu_p(i(K)) \leq \nu_p([\mathbb{Z}_K : \mathbb{Z}[\eta]])$ for every $\eta \in \mathbb{Z}_K$ generating $K$. In particular, $\nu_p(i(K)) \leq \nu_p([\mathbb{Z}_K : \mathbb{Z}[\theta]])$. In the proof of Theorem 2.3 we saw that $F(x)$ is 2-regular. We have determined explicitly the corresponding principal Newton’s polygon. Moreover, we have used Theorem 3.2(1), then we obtained the $2$-adic valuation of $([\mathbb{Z}_K : \mathbb{Z}[\theta]])$ in every case when $i(K) > 1$. We propose $\nu_2([\mathbb{Z}_K : \mathbb{Z}[\theta]])$ as an upper bound of $\nu_2(i(K))$. Under the notations of Theorem 2.3 we summarize these computations in Table 3.
ON THE INDEX OF THE NUMBER FIELD DEFINED BY $x^8 + ax + b$

<table>
<thead>
<tr>
<th>Case</th>
<th>Conditions</th>
<th>$\nu_2(\mathbb{Z}_K : \mathbb{Z}[\theta])$</th>
<th>$\nu_2(i(K))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>C12</td>
<td>$a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$</td>
<td>5</td>
<td>$\leq 5$</td>
</tr>
<tr>
<td>C15</td>
<td>$(a, b) \in {(0, 31), (16, 15)} \pmod{32}$</td>
<td>7</td>
<td>$\leq 7$</td>
</tr>
<tr>
<td>C16</td>
<td>$a \equiv 8 \pmod{16}, b \equiv 7 \pmod{32}$ and $\omega$ is odd</td>
<td>$\frac{\omega + 1}{2}$</td>
<td>$\leq \frac{\omega + 1}{2}$</td>
</tr>
<tr>
<td>C17</td>
<td>$a \equiv 8 \pmod{16}, b \equiv -9 \pmod{32}$ and $A_{a,b}^1 \equiv 0 \pmod{4}$</td>
<td>7</td>
<td>$\leq 7$</td>
</tr>
<tr>
<td>C19</td>
<td>$a \equiv 8 \pmod{16}, b \equiv -9 \pmod{32}$, $A_{a,b}^1 \equiv 2 \pmod{4}$ and $A_{a,b}^2 \equiv 0 \pmod{4}$</td>
<td>8</td>
<td>$\leq 8$</td>
</tr>
<tr>
<td>C20</td>
<td>$\omega = 2 + 2k, k \geq 2$ and $B_{a,b} \equiv 2 \pmod{4}$</td>
<td>$k + 6$</td>
<td>$\leq k + 6$</td>
</tr>
<tr>
<td>C22</td>
<td>$\omega = 2 + 2k, k \geq 2$ and $B_{a,b} \equiv 0 \pmod{8}$</td>
<td>$k + 7$</td>
<td>$\leq k + 7$</td>
</tr>
</tbody>
</table>

**Table 3**

**References**


Faculty of Sciences Dhar El Mahraz, P.O. Box 1874 Atlas-Fes, Sidi Mohamed Ben Abdellah University, Morocco

Email address: beyakouhamid@gmail.com

Faculty of Sciences Dhar El Mahraz, P.O. Box 1874 Atlas-Fes, Sidi Mohamed Ben Abdellah University, Morocco

Email address: brahimboudine.bb@gmail.com