mathematics

MDPI

Article

On Indices of Septic Number Fields Defined by Trinomials $x^7 + ax + b$

Lhoussain El Fadil

Department of Mathematics, Faculty of Sciences Dhar El Mahraz-Fes, Sidi Mohamed Ben Abdellah University, Fez P.O. Box 1796, Morocco; lhoussain.elfadil@usmba.ac.ma

Abstract: Let K be a septic number field generated by a root, α, of an irreducible trinomial, $x^7 + ax + b \in \mathbb{Z}[x]$. In this paper, for every prime integer, p, we calculate $\nu_p(i(K))$; the highest power of p dividing the index, $i(K)$, of the number field, K. In particular, we calculate the index, $i(K)$. In application, when the index of K is not trivial, then K is not monogenic.

Keywords: power integral bases; theorem of Ore; prime ideal factorization; common index divisor

MSC: 11R04; 11Y40; 11R21

1. Introduction

Let K be a number field of degree n and $\mathbb{Z}_K$ its ring of integers. It is well known that $\mathbb{Z}_K$ is a free abelian group of rank n, and so, for every primitive integral element, $\theta \in \mathbb{Z}_K$, of K, the quotient group, $\mathbb{Z}_K/\mathbb{Z}[\theta]$, is finite. Let $\theta \in \mathbb{Z}_K$ be a primitive element of K and $ind(\theta) = (\mathbb{Z}_K : \mathbb{Z}[\theta])$ the cardinal order of $\mathbb{Z}_K/\mathbb{Z}[\theta]$. The index $ind(\theta)$ is called the index of θ . The index of the number field, K, denoted $i(K)$, is the greatest common divisor of all indices of all integral primitive elements of K. Namely, $i(K) = GCD((\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta)$ and $\theta \in \mathbb{Z}_K)$. A rational prime integer p dividing $i(K)$ is called a prime common index divisor of K. If, for some $\theta \in \mathbb{Z}_K$, $(1, \theta, \ldots, \theta^{n-1})$ is a $\mathbb{Z}$ basis of $\mathbb{Z}_K$, then the number field, K, is said to be monogenic and θ is a generator of a power integral basis of K. Otherwise, the number field, K, is said to be non-monogenic. Remark that, if K is monogenic, then $i(K) = 1$. It follows that, if a number field has a prime common index divisor, then it is non-monogenic. Monogenity of number fields is a classical problem of algebraic number fields, going back to Dedekind, Hasse and Hensel; see for instance [1–3] for the present state of this area. Let $\theta \in \mathbb{Z}_K$ be a primitive element of K, d_K the absolute discriminant of K, and $\triangle(\theta)$ the discriminant of the minimal polynomial of θ over $\mathbb{Q}$. A well-known relation linking the discriminant and the index says that:

$$|\triangle(\theta)| = ind(\theta)^2 \cdot |d_K|$$

(see [3]).

Clearly, $(1, \theta, \ldots, \theta^{n-1})$ is a power integral basis of $\mathbb{Z}_K$ for some primitive element $\theta \in \mathbb{Z}_K$ of K if and only if $ind(\theta) = 1$.

The problem of studying monogenity of a number field and constructing all possible generators of power integral bases have been intensively studied during the last decades, mainly by Gaál, Nakahara, Pohst, and their collaborators (see for instance [4–6]). In 1871, Dedekind gave an example of a number field with a non-trivial index. He considered the cubic number field, K, generated by a root of $x^3 - x^2 - 2x - 8$, and he showed that the rational prime integer 2 splits completely in K ([7], § 5, page 30). In 1930, for every number field, K, of a degree less than 8 and for every prime integer $p \leq n$, Engstrom linked the p-index, $\nu_p(i(K))$, of the number field, K, and the prime ideal factorization of $p\mathbb{Z}_K$ [8]. He gave an an explicit formula linking the value of $\nu_p(i(K))$ and the factorization

check for updates

Citation: El Fadil, L. On Indices of Septic Number Fields Defined by Trinomials $x^7 + ax + b$. *Mathematics* **2023**, *11*, 4441. https://doi.org/10.3390/math11214441

Academic Editors: Diana Savin, Nicusor Minculete and Vincenzo Acciaro

Received: 11 September 2023
Revised: 18 October 2023
Accepted: 24 October 2023
Published: 26 October 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

of $p\mathbb{Z}_K$ into powers of prime ideals of K for every positive rational prime integer $p \leq n$. This motivated Narkiewicz to ask a very important question, stated as problem 22 in Narkiewicz's book ([9], Problem 22), which asks for an explicit formula of the highest power, $\nu_p(i(K))$, for a given rational prime p dividing $i(K)$. In [10], Nakahara characterized the index of abelian biquadratic number fields. Also in [11], Gaál et al. studied the indices of biquadratic number fields. Recently, many authors have focused on monogenity of number fields defined by trinomials. Based on the calculation of the p-index form of K using p-integral bases of K given in [12], Davis and Spearman [13] characterized the index of any quartic number field, K, generated by a root of an irreducible quartic irreducible trinomial, $F(x) = x^4 + ax + b \in \mathbb{Z}[x]$. In [14], based on Newton's polygon techniques, we reformulated Davis' and Spearman's results. In [15], El Fadil and Gaál characterized the index of quartic number fields, K, generated by a root of a quadratic irreducible trinomial of the form $F(x) = x^4 + ax^2 + b \in \mathbb{Z}[x]$. They gave necessary and sufficient conditions on a and b, which characterize when a prime, $p \in \{2, 3\}$, is a common index divisor of K. In [16], for a sextic number field, K, defined by a trinomial, $F(x) = x^6 + ax^3 + b \in \mathbb{Z}[x]$, Gaál calculated all possible generators of power integral bases of K. In [17], we extended Gaál's studies by providing all cases where K is not monogenic. Also in [18], we characterized when a prime integer, $p \in \{2, 3\}$, is a common index divisor of K, where K is a number field defined by an irreducible trinomial, $F(x) = x^5 + ax^2 + b \in \mathbb{Z}[x]$. In [19], for a number field defined by an irreducible trinomial, $F(x) = x^n + ax^m + b \in \mathbb{Z}[x]$, we provided some cases where $i(K)$ is not trivial, and so K is not monogenic. In this paper, for a septic number field generated by a root of an irreducible trinomial, $F(x) = x^7 + ax + b \in \mathbb{Z}[x]$, and for every prime integer, p, we calculate $\nu_p(i(K))$, the highest power of p dividing the index $i(K)$ of the septic field, K. Our study key is based on prime ideal factorization in number fields, which is carried out in [20,21] and in the thesis of Montes (1999). The author warmly thanks Professor Enric Nart who provided him with a copy of Montes' thesis.

2. Main Results

Let K be a septic number field generated by a root, α, of an irreducible trinomial, $F(x) = x^7 + ax + b \in \mathbb{Z}[x]$. Without loss of generality, we can assume that for every rational prime integer, p, $\nu_p(a) \leq 5$ or $\nu_p(b) \leq 6$. Let $a \in \mathbb{Z}$ be a rational integer and a prime integer, p. Along this paper, let $a_p = \dfrac{a}{p^{\nu_p(a)}}$.

Our first main result characterizes when is $\mathbb{Z}[\alpha]$ the ring of integers of K?

Theorem 1. *The ring, $\mathbb{Z}[\alpha]$, is the ring of integers of K if and only if every prime integer, p, satisfies one of the following conditions:*

1. *If $p|a$ and $p|b$, then $\nu_p(b) = 1$.*
2. *If $p = 2$, p divides b and does not divide a, then $(a, b) \in \{(1, 0), (3, 2)\} \pmod 4$.*
3. *If $p = 3$, p divides b and $a \equiv -1 \pmod 3$, then $(a, b) \in \{(2, 0), (8, 3), (8, 6)\} \pmod 9$.*
4. *If $p = 3$, p divides b and $a \equiv 1 \pmod 3$, then $(a, b) \not\equiv (1, 0) \pmod 9$.*
5. *If $p = 7$, p divides a and does not divide b, then $\nu_7(1 - a - b^6) = 1$.*
6. *If $p \notin \{2, 3, 7\}$, p does not divide both a and b, then $\nu_p(7^7 b^6 + 6^6 a^7) \leq 1$.*

The following is an example of a monogenic septic number field defined by a non-monogenic irreducible trinomial.

Example 1. Let K be the number field generated by a root, α, of $F(x) = x^7 + 16x + 16 \in \mathbb{Z}[x]$. Then $F(x)$ is irreducible over $\mathbb{Q}$, which is a non-monogenic polynomial, and K is a monogenic number field.

Indeed, since $\triangle(F) = -2^{24} \cdot 977 \cdot 1607$ is the discriminant of $F(x)$, and $\overline{F(x)} = x^7$ in $\mathbb{F}_2[x]$, then according to the notations of Section 3, let $\phi = x$ and $N_\phi(F)$ be the ϕ-Newton polygon of $F(x)$ with respect to $p = 2$. Then, $N_\phi(F) = S$ has a single side of degree 1. Thus

by Remark 2 (2) of [22], $F(x)$ is irreducible over $\mathbb{Q}$. Let θ be a root of $F(x)$. Since the height $h(S) = 4$, by Theorem 5, $\nu_2(ind(\theta)) \geq ind_\phi(F) = 9$. Therefore, $F(x)$ is a non-monogenic polynomial. Let $\alpha = \frac{\theta^2}{2}$. Then $G(x) = x^7 + 4x^4 + 4x - 2$ is the minimal polynomial of α over $\mathbb{Q}$. So α is a primitive integral element of K. Therefore, in order to show that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, we need to show that $\nu_2(ind(\alpha)) = 0$. Since $\triangle(F) = -2^6 \cdot 977 \cdot 1607$ is the discriminant of $G(x)$, then thanks to the formula

$$|\triangle(\theta)| = ind(\theta)^2 \cdot |d_K|,$$

the unique prime candidate to divide $ind(\alpha)$ is 2. Let $N_\phi(G)$ be the ϕ-Newton polygon of $G(x)$ with respect to $p = 2$. Then $N_\phi(G) = T$ has a single side of height 1, by Theorem 6, $\nu_2(ind(\alpha)) = 0$. Thus K is monogenic and α generates a power integral basis of K.

For every $(a, b) \in \mathbb{Z}^2$, such that $x^7 + ax + b$ is irreducible over $\mathbb{Q}$, let $\triangle = -(6^6a^7 + 7^7b^6)$ be the discriminant of $F(x)$. Let p be a prime integer and $\triangle_p = \frac{\triangle}{p^{\nu_p(\triangle)}}$. In the remainder of this section, for every prime integer, p, and for every value of a and b, we calculate $\nu_p(i(K))$.

Theorem 2. *The following table provides the value of* $\nu_2(i(K))$.

conditions	$\nu_2(i(K))$
$a \equiv 28 \pmod{32}$ *and* $b \equiv 0 \pmod{32}$	1
$a \equiv 112 \pmod{128}$ *and* $b \equiv 0 \pmod{128}$	1
$a \equiv 1 \pmod 8$ *and* $b \equiv 2 \pmod 4$ $\nu_2(\triangle)$ *even and* $\triangle_2 \equiv 3 \pmod 4$	1
$a \equiv 3 \pmod 8$ *and* $b \equiv 4 \pmod 8$	1
$a \equiv 3 \pmod 4$ *and* $b \equiv 0 \pmod 8$	3
$(a, b) \in \{(5, 2), (5, 6), (13, 2), (13, 14)\} \pmod{16}$	1
Otherwise	0

Theorem 3. *The following table provides the value of* $\nu_3(i(K))$.

conditions	$\nu_3(i(K))$
$a \equiv 5 \pmod 9$ *and* $b \in \{3, 6\} \pmod 9$	1
$a \equiv 8 \pmod 9$ *and* $b \equiv 0 \pmod 9$	2
$a \equiv 2 \pmod 9$ *and* $b \in \{3, 6\} \pmod 9$ $\nu_3(\triangle) = 2k$ *and* $k \geq 5$	1
$a \equiv 2 \pmod 9$ *and* $b \in \{3, 6\} \pmod 9$ $\nu_3(\triangle) = 2k + 1$, $k \geq 5$ *and* $\triangle_3 \equiv 1 \pmod 3$	2
Otherwise	0

Theorem 4. *Let* $p \geq 5$ *be a prime integer and* $(a, b) \in \mathbb{Z}^2$, *such that* $F(x) = x^7 + ax + b$ *is irreducible over* $\mathbb{Q}$. *Let* K *be the number field generated by a root,* α, *of* $F(x)$. *Then* p *does not divide* $i(K)$.

Corollary 1. *Let* $(a, b) \in \mathbb{Z}^2$, *such that* $F(x) = x^7 + ax + b$ *is an irreducible polynomial over* $\mathbb{Q}$. *Then* $i(K) \in \{1, 2, 3, 6, 8, 9, 18, 24, 72\}$.

Remark 1.

(1) *The field K can be non monogenic even if the index* $i(K) = 1$.
(2) *The unique method that characterises the monogenity of K is to calculate the solutions of the index form equation of K (see for instance [3,23]).*

3. A Short Introduction to Newton's Polygon Techniques Applied on Prime Ideal Factorization

For a number field, K, generated by a root of a monic irreducible polynomial, $F(x) \in \mathbb{Q}[x]$, and for every prime integer, p, in 1894, Hensel developed a powerful technique by establishing a one–one correspondence between maximal ideals of $\mathbb{Z}_K$ containing p and monic irreducible factors of $F(x)$ with a coefficient in $\mathbb{Q}_p$. For every prime ideal corresponding to any irreducible factor, the ramification index and the residue degree together are the same as those of the local field defined by the associated irreducible factor [24]. Since then, to factorize $p\mathbb{Z}_K$, one needs to factorize $F(x)$ in $\mathbb{Q}_p[x]$. Newton's polygon techniques can be used to refine the factorization of $F(x)$. We have introduced the corresponding concepts in several former papers. Here, we only give a brief introduction, which makes our proofs understandable. For a detailed description, we refer to Ore's Paper [25] and Guardia, Montes, and Nart's paper [26]. For every prime integer, p, let ν_p be the p-adic valuation of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ the ring of p-adic integers. Let $F(x) \in \mathbb{Z}_p[x]$ be a monic polynomial and $\phi \in \mathbb{Z}_p[x]$ a monic lift of an irreducible factor of $\overline{F(x)}$ modulo p. Let $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^l$ be the ϕ-expansion of $F(x)$, $N_\phi(F)$ the ϕ-Newton polygon of $F(x)$, and $N_\phi^+(F)$ its principal part. Let $\mathbb{F}_\phi$ be the field $\mathbb{F}_p[x]/(\overline{\phi})$. For every side, S, of $N_\phi^+(F)$ with length l and initial point (s, u_s), for every $i = 0, \ldots, l$, let $c_i \in \mathbb{F}_\phi$ be the residue coefficient, defined as follows:

$$c_i = \begin{cases} 0, & \text{if } (s+i, u_{s+i}) \text{ lies strictly above } S, \\ \left(\dfrac{a_{s+i}(x)}{p^{u_{s+i}}}\right) \mod (p, \phi(x)), & \text{if } (s+i, u_{s+i}) \text{ lies on } S. \end{cases}$$

Let $-\lambda = -h/e$ be the slope of S, where h and e are two positive coprime integers. Then $d = l/e$ is the degree of S. Let $R_1(F)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$ be the residual polynomial of $F(x)$ attached to the side S, where for every $i = 0, \ldots, d$, $t_i = c_{ie}$. If $R_1(F)(y)$ is square free for each side of the polygon, $N_\phi^+(F)$, then we say that $F(x)$ is ϕ-regular.

Let $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi}_i^{l_i}$ be the factorization of $F(x)$ into powers of monic irreducible coprime polynomials over $\mathbb{F}_p$, and we say that the polynomial $F(x)$ is p-regular if $F(x)$ is a ϕ_i-regular polynomial with respect to p for every $i = 1, \ldots, r$. Let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{ir_i}$ be the ϕ_i-principal Newton polygon of $F(x)$ with respect to p. For every $j = 1, \ldots, r_i$, let $R_{1_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $R_{1_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$, where $R_{1_{ij}}(F)(y)$ is the residual polynomial of $F(x)$ attached to the side S_{ij}. Then we have the following theorem of index of Ore:

Theorem 5 (Theorems 1.7 and 1.9 of [12])**.**

1. $$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \sum_{i=1}^{r} ind_{\phi_i}(F).$$

   The equality holds if $F(x)$ is p-regular.
2. *If $F(x)$ is p-regular, then*

   $$p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{t_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}},$$

   where $\mathfrak{p}_{ijs}$ is a prime ideal of $\mathbb{Z}_K$ lying above p, e_{ij} is the smallest positive integer satisfying $e_{ij}\lambda_{ij} \in \mathbb{Z}$, and the residue degree of $\mathfrak{p}_{ijs}$ over p is given by $f_{ijs} = \deg(\phi_i) \times \deg(\psi_{ijs})$ for every (i, j, s).

The Dedekind's criterion can be reformulated as follows:

Theorem 6 (Theorem 1.1 of [27]). *Let* $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi_i}^{l_i}$ *be the factorization of* $F(x)$ *into powers of monic irreducible coprime polynomials over* $\mathbb{F}_p$. *For every* $i = 1, \ldots, r$, *let* $R_i(x)$ *be the remainder of the Euclidean division of* $F(x)$ *by* $\phi_i(x)$. *Then* $\nu_p(ind(\alpha)) = 0$ *if and only if* $l_i = 1$ *or* $\nu_p(R_i(x)) = 1$ *for every* $i = 1, \ldots, r$.

When the theorem of Ore fails, that is, $F(x)$ is not p-regular, then in order to complete the factorization of $F(x)$, Guardia, Montes, and Nart introduced the notion of *higher order Newton's polygons*. Analogous to the first order, for each order, r, the authors of [26] introduced the valuation, ω_r, of order r, the key polynomial, $\phi_r(x)$, of such a valuation, $N_r(F)$ the Newton polygon of any polynomial, $F(x)$, with respect to ω_r and $\phi_r(x)$, and for every side of $N_r(F)$ the residual polynomial $R_r(F)$, and the index of $F(x)$ in order r. For more details, we refer to [26].

4. Proofs of Our Main Results

Proof of Theorem 1.

1. If p divides a and b, then, by Theorem 6, p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_p(b) = 1$.
2. For $p = 2$, 2 divides b and does not divide a, we have $\overline{F(x)} = x(x-1)^2(x^2+x+1)^2$. Let $\phi_1 = x - 1$ and $\phi_2 = x^2 + x + 1$. Since $F(x) = \cdots - (4x-2)\phi_2 + (a+1)x + b$ and $F(x) = \cdots + (a+7)\phi_1 + (a+1+b)$, by Theorem 6, 2 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_2(b+a+1) = 1$ and $\nu_2((a+1)x+b) = 1$, which means $b \equiv 1 - a \pmod 4$ and $a \equiv 1 \pmod 4$ or $b \equiv 2 \pmod 4$. That is, $(a, b) \in \{(1,0), (3,2)\} \pmod 4$.
3. For $p = 3$, 3 divides b and $a \equiv 1 \pmod 3$, we have $\overline{F(x)} = x(x^2+1)^3$. Let $\phi = x^2 + 1$. Since $F(x) = x\phi^3 - 3x\phi^2 + 3x\phi + (a-1)x + b$, by Theorem 6, 3 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_3((a-1)x + b) = 1$, which means that $a \not\equiv 1 \pmod 9$ or $b \not\equiv 0 \pmod 9$. That is, $(a, b) \not\equiv (1, 0) \pmod 9$.
4. For $p = 3$, 3 divides b and $a \equiv -1 \pmod 3$, we have $\overline{F(x)} = x(x-1)^3(x+1)^2$. Let $\phi_1 = x - 1$ and $\phi_2 = x + 1$. Since $F(x) = \phi_1^7 + 7\phi_1^6 + 21\phi_1^5 + 35\phi_1^4 + 35\phi_1^3 + 21\phi_1^2 + (a+7)\phi_1 + (a+1+b)$ and $F(x) = \phi_1^7 - 7\phi_2^6 + 21\phi_2^5 - 35\phi_2^4 + 35\phi_2^3 - 21\phi_2^2 + (a+7)\phi_2 + (b-a-1)$, by Theorem 6, 3 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_2(a+1+b) = 1$ and $\nu_3(b-a-1) = 1$. That is, $(a, b) \in \{(2,0), (8,3), (8,6)\} \pmod 9$.
5. For $p = 7$, if 7 divides a and 7 does not divide b, then $\overline{F(x)} = (x+b)^7$. Let $\phi = x + b$. Then $F(x) = \phi^7 - 7b\phi^6 + 21b^2\phi^5 - 35b^3\phi^4 + 35b^4\phi^3 - 21b^5\phi^2 + (a+7b^6)\phi + (b - ab - b^7)$, by Theorem 6, 7 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_7(1 - a - b^6) = 1$.
6. For $p \notin \{2, 3, 7\}$ such that p does not divide both a and b, if p^2 does not divide $6^6a^7 + 7^7b^6$, then, by the formula $\triangle = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 d_K$, p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. If p^2 divides $6^6a^7 + 7^7b^6$, then let t be an integer such that $6at \equiv -7b \pmod{p^2}$. Then $(6a)^6F'(t) = 7(-7b)^6 + 6^6a^7 \equiv 0 \pmod{p^2}$ and $(6a)^7F(t) \equiv 0 \pmod{p^2}$. Thus $(x-t)^2$ divides $\overline{F(x)}$ in $\mathbb{F}_p[x]$. As $F(t)$ is the remainder of the Euclidean division of $F(x)$ by $x - t$, by Theorem 6, p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$.

The proofs of Theorems 2 and 3 are based on Engstrom's results [28]. □

Proof of Theorem 2. By virtue of Engstrom's results [28], the proof is achieved if we provide the factorization of $2\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$. Based on Theorem 1, we deal with the cases: $2|a$ and $4|b$ or $(a, b) \in \{(1,2), (3,0)\} \pmod 4$.

1. If 2 divides a and 4 divides b, then, for $\phi = x$, we have $\overline{F(x)} = \phi^7$ in $\mathbb{F}_2[x]$.
   (a) If $N_\phi(F) = S$ has a single side, that is, $\nu_2(a) \geq \nu_2(b)$, then the side, S, is of degree 1. Thus there is a unique prime ideal of $\mathbb{Z}_K$ lying above 2.
   (b) If $N_\phi(F) = S_1 + S_2$ has two sides joining $(0, \nu_2(b))$, $(1, \nu_2(a))$, and $(7, 0)$, that is, $\nu_2(a) + 1 \leq \nu_2(b)$, then S_1 is of degree 1, and so it provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1. Let d be the degree of S_2.

i. If $\nu_2(a) \notin \{2,3,4\}$, then S_2 is of degree 1, and so there are exactly two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each.

ii. If $\nu_2(a) = 2$, then the slope of S_2 is $\frac{-1}{3}$ and $R_1(F)(y) = (y+1)^2$ is the residual polynomial of $F(x)$ attached to S_2. Thus, we have to use second order Newton polygon techniques. Let ω_2 be the valuation of a second order Newton polygon; defined by $\omega_2(P(x)) = \min\{3\nu_2(p_i) + ih, ß = 0, \ldots, n\}$ for every non-zero polynomial $P = \sum_{i=0}^{n} p_i x^i$. Let ϕ_2 be the key polynomial of ω_2 and let $N_2(F)$ be the ϕ_2-Newton polygon of $F(x)$ with respect to the valuation ω_2. It follows that:
if $\nu_2(b) = 3$, then for $\phi_2 = x^3 + 2x + 2$, we have $F(x) = x\phi_2^2 + (4 - 4x - 4x^2)\phi_2 + 8x^2 + (a-4)x + b - 8$. It follows that, if $\nu_2(a-4) = 3$, then $N_2(F) = T$ has a single side joining $(0,10)$ and $(2,7)$. Thus T is of degree 1, and so S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2. If $\nu_2(a-4) \geq 4$ and $\nu_2(b-8) \geq 4$, then $N_2(F) = T$ has a single side joining $(0,11)$, $(1,9)$, and $(2,7)$, with $R_2(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_2 = \mathbb{F}_0$. Thus, S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2. Hence 2 is not a common index divisor of K.
If $\nu_2(b) \geq 4$ and $\nu_2(a+4) = 3$, then, for $\phi_2 = x^3 + 2$, we have $F(x) = x\phi_2^2 - 4x\phi_2 + (a+4)x + b$ is the ϕ_2-expansion of $F(x)$, and so $N_2(F) = T$ has a single side joining $(0,10)$ and $(2,7)$. In this case the side T is of degree 1 and S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2. If $\nu_2(b) = 4$ and $\nu_2(a+4) \geq 4$, then for $\phi_2 = x^3 + 2$, $N_2(F) = T$ has a single side joining $(0,12)$ and $(2,7)$. Thus T is of degree 1, and so S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2.
If $\nu_2(b) \geq 5$ and $\nu_2(a+4) = 4$, then, for $\phi_2 = x^3 + 2$, we have $F(x) = x\phi_2^2 - 4x\phi_2 + (a+4)x + b$ as the ϕ_2-expansion of $F(x)$, and $N_2(F) = T$ has a single side joining $(0,13)$, $(1,10)$, and $(2,7)$. So, T is of degree 2 with attached residual polynomial $R_2(F) = y^2 + y + 1$ irreducible over $\mathbb{F}_2 = \mathbb{F}_0$. Thus, S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2.
If $\nu_2(b) \geq 5$ and $\nu_2(a+4) \geq 5$, then, for $\phi_2 = x^3 + 2$, $N_2(F) = T_1 + T_2$ has two sides joining $(0,v)$, $(1,10)$, and $(2,7)$ with $v \geq 15$. So, each T_i has degree 1, and so S_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. As S_1 provides a prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1, we conclude that there are three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each, and so 2 is a common index divisor of K. In this last case, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}^3\mathfrak{p}_{131}^3$ with residue degree 1 each prime ideal factor. Based on Engstrom's result, we conclude that $\nu_2(i(K)) = 1$.

iii. For $\nu_2(a) = 3$, we have $R_1(F)(y) = y^3 + 1 = (y^2 + y + 1)(y + 1)$ as the residual polynomial of $F(x)$ attached to T_1. Thus, T_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2, with residue degree 1 and a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2. Thus, $\nu_2(i(K)) = 0$.

iv. The case $\nu_2(a) = 4$ is similar to the case $\nu_2(a) = 2$. In this case, $\nu_2(i(K)) \geq 1$ if and only if $\nu_2(b) \geq 7$ and $\nu_2(a+16) \geq 7$. In this case, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}^3\mathfrak{p}_{131}^3$ with residue degree 1 each factor. Based on Engstrom's result, we conclude that $\nu_2(i(K)) = 1$.

2. $(a,b) \in \{(1,2),(3,0)\} \pmod 4$. In this case, $\overline{F(x)} = x(x-1)^2(x^2+x+1)^2$ modulo 2. Let $\phi = x - 1$, $g(x) = x^2 + x + 1$, $F(x) = \cdots - 21\phi^2 + (7+a)\phi + (b+a+1)$, and $F(x) = (x-3)g^3 + (5+3x)g^2 - (4x+2)g + (a+1)x + b$. Since x provides a unique

prime ideal of $\mathbb{Z}_K$ lying above 2, we conclude that 2 is a common index divisor of K if and only if ϕ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 of degree 1 each or ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 of degree 2, and g provides at least one prime ideal of $\mathbb{Z}_K$ lying above 2 of degree 2 or also g provides two prime ideals of $\mathbb{Z}_K$ lying above 2 of degree 2 each. That is if and only if one of the following conditions holds:

(a) If $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$, then $\nu_2(\triangle) \geq 7$ and $N_g^+(F)$ has a single side of height 1, and so g provides a unique prime ideal $\mathfrak{p}_{311}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 2. For $N_\phi^+(F)$, let $u = \dfrac{-7b_2}{3a}$. Then $u \in \mathbb{Z}_2$. Let $F(x+u) = x^7 + \cdots + 21u^5x^2 + Ax + B$, where $A = 7u^6 + a = \dfrac{-\triangle}{6^6a^6}$ and $B = u^7 + au + b = \dfrac{b\triangle}{6^7a^7}$. It follows that $\nu_2(A) = \nu_2(B) = \nu_2(\triangle) - 6$, and so $N_\phi^+(F) = S_1$ has a single side joining $(0, \nu_2(\triangle) - 6)$ and $(2, 0)$. Thus, if $\nu_2(\triangle)$ is odd, then ϕ provides a unique prime ideal $\mathfrak{p}_{211}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 1. If $\nu_2(\triangle) = 2(k+3)$ for some positive integer, k, then let $F(x + u + 2^k) = x^7 + \cdots + 21(u + 2^k)^5x^2 + A_1x + B_1$, where $A_1 = 7u^6 + a + 3 \cdot 2^{k+1}u^5 + 2^{2k}D = A + 3 \cdot 2^{k+1}u^5 + 2^{2k}D$ and $B_1 = B + A \cdot 2^k + 2^{2k} \cdot 21u^5 + 2^{3k}H = 2^{2k}(\dfrac{b_2\triangle_2}{3^7a^7} + 21u^5) + 2^{3k}H$ for some $D \in \mathbb{Z}_2$ and $H \in \mathbb{Z}_2$. Thus, $B_1 = 2^{2k}(3 \cdot a \cdot b_2\triangle_2 + 3 \cdot a \cdot b_2) + 2^{2k+3}L$ for some $L \in \mathbb{Z}_2$. Hence if $k \geq 2$, then $\nu_2(A_1) = k + 1$ and $\nu_2(B_1) \geq 2k + 1$. More precisely, if $\triangle_2 \equiv 1 \pmod 4$, then $\nu_2(B_1) = 2k + 1$, and so ϕ provides a unique prime ideal $\mathfrak{p}_{211}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 1. If $\triangle_2 \equiv 3 \pmod 4$, then $\nu_2(B_1) \geq 2k + 2$. It follows that, if $\nu_2(B_1) = 2k + 2$, and so ϕ provides a unique prime ideal $\mathfrak{p}_{211}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 2. If $\nu_2(B_1) \geq 2k + 3$, then $\nu_2(B_1) \geq 2k + 3$, and so ϕ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. In these last two cases, we have 2 divides $i(K)$ and $\nu_2(i(K)) = 1$.
For $k = 1$, we have $\nu_2(\triangle) = 8$ and $a \equiv 5 \pmod 8$. In this case, $\overline{F(x)} = x(x-1)^2(x^2+x+1)^2$ modulo 2. Let $\phi = x - 1$, $g(x) = x^2 + x + 1$, $F(x) = \cdots - 21\phi^2 + (7 + a)\phi + (b + a + 1)$, and $F(x) = (x - 3)g^3 + (5 + 3x)g^2 - (4x + 2)g + (a + 1)x + b$. Since x provides a unique prime ideal of of $\mathbb{Z}_K$ lying above 2 with residue degree 1 and g provides a unique prime ideal of of $\mathbb{Z}_K$ lying above 2 with residue degree 2, we conclude that $\nu_2(i(K)) \geq 1$ if and only if ϕ provides a unique prime ideal of of $\mathbb{Z}_K$ lying above 2 with residue degree 2 or ϕ provides two distinct prime ideals of of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. If $(a, b) \in \{(5, 10), (13, 2)\} \pmod{16}$, then ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2, and so $\nu_2(i(K)) = 1$. If $(a, b) \in \{(5, 10), (13, 10)\} \pmod{16}$, then ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1, and so $\nu_2(i(K)) = 0$. For $(a, b) \in \{(5, 6), (5, 14), (13, 6), (13, 14)\} \pmod{16}$, let us replace ϕ by $\phi' = x - 3$ and consider the ϕ'-Newton polygon of $F(x)$ with respect to ν_2. It follows that, if $(a, b) \in \{(5, 6), (13, 14)\} \pmod{16}$, then ϕ' provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each, and so $\nu_2(i(K)) = 1$. If $(a, b) \in \{(5, 14), (13, 6)\} \pmod{16}$, then ϕ' provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1, and so $\nu_2(i(K)) = 0$.

(b) $a \equiv 3 \pmod 4$ and $b \equiv -(a + 1) \pmod 8$ because $N_\phi^+(F)$ has two sides.

(c) If $a \equiv 3 \pmod 8$ and $b \equiv 0 \pmod 8$, then ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and g provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each because $N_g^+(F)$ has a single side of degree 2 with $(1 + x)y^2 + y + x = (x + 1)(y - 1)(y - x)$ its attached residual polynomial of $F(x)$. In this case, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{211}\mathfrak{p}_{311}\mathfrak{p}_{312}$ with residue degrees $f_{111} = 1$ and $f_{211} = f_{311} = f_{312} = 2$, and so $\nu_2(i(K)) = 3$.

(d) $a \equiv 7 \pmod 8$ and $b \equiv 0 \pmod 8$. In this case, ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and $N_g^+(F)$ has two sides. More precisely, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{211}\mathfrak{p}_{311}\mathfrak{p}_{321}$ with residue degrees $f_{111} = 1$ and $f_{211} = f_{311} = f_{312} = 2$, and so $\nu_2(i(K)) = 3$.

(e) If $a \equiv 5 \pmod 8$ and $b \equiv -(a+1) \pmod{16}$ because if $b \equiv -(a+1) \pmod{32}$, then $N_\phi^+(F)$ has two sides, and if $b \equiv -(a+1)+16 \pmod{32}$, then $N_\phi^+(F)$ has a single side of degree 2, which provides a single prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and $N_g^+(F)$ has a single side of degree 1. Thus, there are 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each.

(f) If $a \equiv 5 \pmod 8$ and $\nu_2(b+(a+1)) = 2$, then $\nu_2(b-(a+1)) \geq 3$. If $\nu_2(b-(a+1)) = 3$, then, for $\phi = x+1$, $N_\phi^+(F)$ has a single side of degree 1. Since $\nu_2(a+1) = 1$, then $N_g^+(F)$ has a single side of height 1. Thus, there are two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each and one prime ideal with residue degree 2. If $\nu_2(b-(a+1)) = 4$, then, for $\phi = x+1$, $N_\phi^+(F)$ has a single side of degree 2, and its attached residual polynomial of F is $R_1(F)(y) = y^2+y+1$. Since $b \equiv 6 \pmod 8$, we conclude that $N_g^+(F)$ has a single side of degree 1, and then there are 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each, and so 2 divides $i(K)$. If $\nu_2(b-(a+1)) \geq 5$, then, for $\phi = x+1$, $N_\phi^+(F)$ has two sides of degree 1 each, and so there are 3 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each, and so 2 divides $i(K)$.

□

Proof of Theorem 3. By virtue of Engstrom's results [28], the proof is achieved if we provide the factorization of $3\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$. Based on Theorem 1, we deal with the cases:

1. $3|a$ and $9|b$.
2. $(a,b) \notin \{(2,0),(8,3),(8,6)\} \pmod 9$.
3. $(a,b) \equiv (1,0) \pmod 9$.

1. $3|a$ and $9|b$, then for $\phi = x$, $\overline{F(x)} = \phi^7$ in $\mathbb{F}_3[x]$. It follows that:

   (a) If $\nu_3(a) \geq \nu_3(b)$, then $N_\phi(F)$ has a single side of degree 1, and so there is a unique prime ideal of $\mathbb{Z}_K$ lying above 3.

   (b) If $\nu_3(a)+1 \leq \nu_3(b)$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0,\nu_3(b))$, $(1,\nu_3(a))$, and $(7,0)$. Since S_1 is of degree 1, S_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Thus, $\nu_3(i(K)) \geq 1$ if and only if S_2 provides at least three prime ideals of $\mathbb{Z}_K$ lying above 3, with residue degree 1 each. If $\nu_3(a) \notin \{2,3,4\}$, then S_2 is of degree 1, and so S_2 provides exactly one prime ideal of $\mathbb{Z}_K$ lying above 3, with residue degree 1 each. If $\nu_3(a) \in \{2,4\}$, then S_2 is of degree 2, and so S_2 provides at most two prime ideal of $\mathbb{Z}_K$ lying above 3. Hence 3 is not a common index divisor of K. If $\nu_3(a) = 3$, then S_2 is of degree 3 and its attached residual polynomial of $F(x)$ is $R_1(F)(y) = y^3 + a_3 = (y+a_3)^3$. So, we have to use a second order Newton polygon. Let ω_2 be the valuation of the second order Newton polygon. ω_2 is defined by $\omega_2(P) = \min\{2\nu_3(p_i)+i,\ i = 0,\ldots,n\}$ for every non-zero polynomial $p = \sum_{i=0}^{n} p_i x^i$ of $\mathbb{Q}_3[x]$. Let $\phi_2 = x^2 + 3a_3$ be a key polynomial of ω_2 and $N_2(F)$ the ϕ_2-Newton polygon of $F(x)$ with respect to ω_2. It follows that: if $a_3 \equiv 1 \pmod 3$, then, for $\phi_2 = x^2+3$, we have $F(x) = x\phi_2^3 - 9x\phi_2^2 + 27x\phi_2 + (a-27)x + b$ as the ϕ_2-expansion of $F(x)$. We have the following cases:

      i. If $\nu_3(b) = 4$, then $N_2(F) = T$ has a single side joining $(0,8)$ and $(3,7)$. Thus, T is of degree 1 and S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1.

ii. If $\nu_3(b) \geq 5$ and $\nu_3(a-27) = 4$, then $N_2(F) = T$ has a single side joining $(0,9)$ and $(3,7)$. Thus, T is of degree 1 and S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1.

iii. If $\nu_3(b) = 5$ and $\nu_3(a-27) \geq 5$, then $N_2(F) = T$ has a single side joining $(0,10)$ and $(3,7)$ and its attached residual polynomial of F is $R_2(F)(y) = xy^3 + xy + b_3$, which is irreducible over $\mathbb{F}_2 = \mathbb{F}_\phi$ because ϕ is of degree 1. Thus, S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 3.

iv. If $\nu_3(b) \geq 6$ and $\nu_3(a-27) \geq 5$, then $N_2(F) = T_1 + T_2$ has two sides joining $(0,v)$, $(2,9)$, and $(3,7)$ with $v \geq 11$. Thus, T_1 is of degree 1, T_2 of degree 2, and $R_2(F)(y) = xy^2 + x$ is its attached residual polynomial of $F(x)$, which is irreducible over $\mathbb{F}_2 = \mathbb{F}_\phi$. Thus, S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3, with residue degree 1 and a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 2.

Similarly, for $a_3 \equiv -1 \pmod 3$, let $\phi_2 = x^2 - 3$. Then, $F(x) = x\phi_2^3 + 9x\phi_2^2 + 27x\phi_2 + (a+27)x + b$ is the ϕ_2-expansion of $F(x)$. Analogous to the case $a_3 \equiv 1 \pmod 3$, in every case 3 does not divide $i(K)$. If $a \equiv 1 \pmod 3$, then $\overline{F(x)} = x(x^2+1)^3$ in $\mathbb{F}_3[x]$. So, there is exactly a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, and the other prime ideals of $\mathbb{Z}_K$ lying above 3 are of residue degrees at least 2 each prime ideal factor. Hence, $\nu_3(i(K)) = 0$.

(c) If $a \equiv -1 \pmod 3$, then $\overline{F(x)} = x(x-1)^3(x+1)^3$ in $\mathbb{F}_3[x]$. Let $\phi_1 = x-1$, $\phi_2 = x+1$, $F(x) = \phi_1^7 + 7\phi_1^6 + 21\phi_1^5 + 35\phi_1^4 + 35\phi_1^3 + 21\phi_1^2 + (7+a)\phi_1 + (b+a+1)$, and $F(x) = \phi_2^7 - 7\phi_2^6 + 21\phi_2^5 - 35\phi_2^4 + 35\phi_2^3 - 21\phi_2^2 + (7+a)\phi_2 + (b-(a+1))$. It follows that:

i. If $a \equiv 8 \pmod 9$ and $b \equiv 0 \pmod 9$, then $\nu_3(b+(1+a)) \geq 2$ and $\nu_3(b-(1+a)) \geq 2$. Thus, x a provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, and each ϕ_i provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each prime ideal factor. In these two cases, $\nu_3(i(K)) = 2$.

ii. If $a \equiv 5 \pmod 9$ and $b \equiv 3 \pmod 9$, then $\nu_3(b+(1+a)) \geq 2$ and $\nu_3(b-(1+a)) = 1$. Thus, x and ϕ_2 each provide a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, and ϕ_1 provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. Similarly, if $a \equiv 5 \pmod 9$ and $b \equiv 6 \pmod 9$, then $\nu_3(b-(1+a)) \geq 2$ and $\nu_3(b+(1+a)) = 1$. Thus, x and ϕ_1 each provide a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, and ϕ_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. In these two cases, $\nu_3(i(K)) = 1$.

iii. If $a \equiv 2 \pmod 9$ and $b \equiv (1+a) \pm 9 \pmod{27}$, then $N^+_{\phi_2}(F)$ has a single side joining $(0,2)$ and $(3,0)$, and $N^+_{\phi_1}(F)$ has a single side joining $(0,1)$ and $(3,0)$. Thus, there are 3 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each, and so $\nu_3(i(K)) = 0$.

iv. Similarly, if $a \equiv 2 \pmod 9$ and $b \equiv -(1+a) \pm 9 \pmod{27}$, then there are 3 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each, and so $\nu_3(i(K)) = 0$.

v. If $a \equiv 2 \pmod 9$ and $\nu_3(b) = 1$, then $\nu_3(\triangle) \geq 8$. Let $u = \dfrac{-7b_3}{2a}$. Then $u \in \mathbb{Z}_3$. Let $\phi = x - u$ and $F(x+u) = x^7 + \cdots + 35u^4x^3 + 21u^5x^2 + Ax + B$, where $A = 7u^6 + a = \dfrac{-\triangle}{6^6a^6}$ and $B = u^7 + au + b = \dfrac{b\triangle}{6^7a^7}$. It follows that $\nu_3(A) = \nu_3(B) = \nu_3(\triangle) - 6$, and so $N^+_\phi(F) = S_1$ has a single side joining $(0, \nu_3(\triangle) - 6)$ and $(3,0)$. Remark that, since $\nu_3(b) = 1$ and $\nu_3(B) \geq 2$, $\nu_3(-u^7 - au + b) = 1$, and so $(x+u)$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Thus,

$\nu_3(i(K)) \geq 1$ if and only if ϕ provides at least two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each prime ideal factor.

A. If $\nu_3(\triangle) = 8$, then $N_\phi^+(F)$ has a single side of degree 1, and so ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1.

B. If $\nu_3(\triangle) = 9$, then $N_\phi^+(F) = S$ has a single side joining $(0,3)$ and $(3,0)$, with $R_1(F)(y) = -u^4y^3 + u^5y^2 + B_3$ its attached residual polynomial of $F(x)$. Since $a \equiv -1 \pmod 3$ and $B = \frac{b\triangle}{6^7a^7}$, we have $u \equiv -b_3 \pmod 3$ and $B_3 \equiv b_3\triangle_3 \pmod 3$. Thus, $R_1(F)(y) = -y^3 - b_3y^2 + b_3\triangle_3$. Since $R_1(F)(y)$ is square free and $R_1(F)(0) \neq 0$, then $R_1(F)(y)$ has at most one root in $\mathbb{F}_\phi$. Thus, S provides at most a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Therefore, $\nu_3(i(K)) = 0$.

C. If $\nu_3(\triangle) \geq 10$, then $N_\phi^+(F) = S_1 + S_2$ has two sides joining $(0, v-6)$ and $(3,1)$. It follows that, since S_2 is of degree 1, it provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Moreover, if $\nu_3(\triangle)$ is even, then S_1 is of degree 1, and so ϕ provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. In this case, $\nu_3(i(K)) = 1$. If $\nu_3(\triangle) = 2(k+3)+1$, then S_1 is of degree 2, with residual polynomial $R_1(F)(y) = uy^2 + b_3\triangle_3$. Since $a \equiv -1 \pmod 3$, we have $2a \equiv 1 \pmod 3$ and $u \equiv -b_3 \pmod 3$. Thus, $R_1(F)(y) = -b_3(y^2 - \triangle_3)$. It follows that, if $(\frac{\triangle_3}{3}) = 1$, then $R_1(F)(y)$ has two different factors of degree 1 each, and so S_1 provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. In this case, there are exactly five prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each and, according to Engstrom's results, $\nu_3(i(K)) = 2$. But, if $(\frac{\triangle_3}{3}) = -1$, then $R_1(F)(y)$ is irreducible over $\mathbb{F}_\phi = \mathbb{F}_3$, and so S_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 2. In this last case, there are exactly three prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each, and so $\nu_3(i(K)) = 0$.

□

Proof of Theorem 4. We start by showing that 5 does not divide $i(K)$ for every integer of a and b, such that $x^7 + ax + b$ is irreducible. By virtue of Engstrom's results [28], the proof is achieved if we provide the factorization of $5\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$. Using the index formula $\triangle = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 d_K$, if 5^2 does not divide $\triangle$, then $\nu_5(i(K)) = 0$. So, we assume that 5^2 divides $\triangle$.

1. So, $6^6a^7 + 7^7b^6 \equiv 0 \pmod 5$. Since $a^5 \equiv a \pmod 5$ and $b^5 \equiv b \pmod 5$, then $a^3 \equiv 2b^2 \pmod 5$, which means $(a,b) \in \{(0,0),(3,1),(2,2),(2,3),(3,4)\} \pmod 5$. In order to show that $\nu_5(i(K)) = 0$, it suffices to show that for every value $(a,b) \in \mathbb{Z}^2$, such that $x^7 + ax + b$ is irreducible and $(a,b) \in \{(0,0),(2,1),(3,2),(3,3),(2,34\} \pmod 5$, there are at most four prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1, where K is the number field generated by a complex root of $x^7 + ax + b$.
   (a) For $(a,b) \equiv (0,0) \pmod 5$, if $\nu_5(a) \geq \nu_5(b)$, then $N_\phi(F) = S$ has a single side and it is of degree 1. Thus, there is a unique prime ideal, $\mathfrak{p}$, of $\mathbb{Z}_K$ lying above 5 with residue degree 1. More precisely, $5\mathbb{Z}_K = \mathfrak{p}^7$.
   If $\nu_5(a) + 1 \leq \nu_5(b)$, then $N_\phi(F) = S_1 + S_2$ has two sides. More precisely, S_1 is of degree 1. Let d be degree of S_2. Since 6 is the length of S_2, then $d \in \{1,2,3\}$. Thus, S_1 provides a unique prime ideal, $\mathfrak{p}$, of $\mathbb{Z}_K$ lying above 5 with residue

degree 1 and S_2 provides at most three prime ideals, $\mathfrak{p}$, of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.

(b) For $(a,b) \equiv (3,1) \pmod 5$, since $\overline{F(x)} = (x+4)^2(x+3)(x^4+4x^3+x^2+x+2)$ in $\mathbb{F}_5[x]$, there are at most three prime ideals, $\mathfrak{p}$, of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.

(c) For $(a,b) \equiv (2,2) \pmod 5$, since $\overline{F(x)} = (x^4+2x^3+4x^2+2x+2)(x+4)(x+2)^2$ in $\mathbb{F}_5[x]$, there are at most three prime ideals, $\mathfrak{p}$, of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.

(d) For $(a,b) \equiv (2,3) \pmod 5$, since $\overline{F(x)} = (x+1)(x+3)^2(x^4+3x^3+4x^2+3x+2)$ in $\mathbb{F}_5[x]$, there are at most three prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.

(e) For $(a,b) \equiv (3,4) \pmod 5$, since $\overline{F(x)} = (x^4+x^3+x^2+4x+2)(x+1)^2(x+2)$ in $\mathbb{F}_5[x]$, there are at most three prime ideals, $\mathfrak{p}$, of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.

We conclude that in all cases $\nu_5(i(K)) = 0$.

For $p \geq 7$, since the field K is of degree 7, there are at most 7 prime ideals of $\mathbb{Z}_K$ lying above p. The fact that there at least $p \geq 7$ monic irreducible polynomials of degree f in $\mathbb{F}_p[x]$ for every positive integer $f \in \{1,2,3\}$, we conclude that p does not divide $i(K)$. □

5. Examples

Let $F = x^7 + ax + b \in \mathbb{Z}[x]$ be a monic irreducible polynomial and K a number field generated by a root, α, of $F(x)$. In the following examples, we calculate the index of the field K. First based on Theorem 4, $\nu_p(i(K)) = 0$ for every prime integer $p \geq 5$. Thus, we need only to calculate $\nu_p(i(K))$ for $p = 2, 3$.

1. For $a = 6$ and $b = 6$, since $F(x)$ is p-Eisenstein for every $p = 2, 3$, we conclude that $F(x)$ is irreducible over $\mathbb{Q}$, and 2 (resp. 3) does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. Thus, 2 (resp. 3) does not divide $i(K)$), and so $i(K) = 1$.
2. For $a = 28$ and $b = 32$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_5$, $F(x)$ is irreducible over $\mathbb{Q}$. By the first item of Theorem 2, we have $\nu_2(i(K)) = 1$. By Theorem 3, $\nu_3(i(K)) = 0$. Thus, $i(K) = 2$.
3. For $a = 3$ and $b = 8$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_5$, $F(x)$ is irreducible over $\mathbb{Q}$. Again, since $a \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 8$, by Theorem 2, $\nu_2(i(K)) = 3$. By Theorem 3, $\nu_3(i(K)) = 0$. Thus, $i(K) = 8$.
4. For $a = -1$ and $b = 9$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_2$, $F(x)$ is irreducible over $\mathbb{Q}$. Since $2\mathbb{Z}_K$ is a prime ideal of $\mathbb{Z}_K$, $\nu_2(i(K)) = 0$. Also, since $a \equiv 8 \pmod 9$ and $b \equiv 0 \pmod 9$, by Theorem 3, $\nu_3(i(K)) = 2$. Thus, $i(K) = 9$.
5. For $a = 803$ and $b = 2112$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_5$, $F(x)$ is irreducible over $\mathbb{Q}$. Since $a \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 8$, by Theorem 2, $\nu_2(i(K)) = 3$. Similarly, since $a \equiv 5 \pmod 9$ and $b \equiv 6 \pmod 9$, by Theorem 3, $\nu_3(i(K)) = 1$. Thus, $i(K) = 24$.
6. For $a = 35$ and $b = 72$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_{11}$, $F(x)$ is irreducible over $\mathbb{Q}$. Since $a \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 8$, by Theorem 2, $\nu_2(i(K)) = 3$. Similarly, since $a \equiv 8 \pmod 9$ and $b \equiv 0 \pmod 9$, by Theorem 3, $\nu_3(i(K)) = 2$. Thus, $i(K) = 72$.

Funding: This research received no external funding.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Acknowledgments: The author is deeply grateful to the anonymous referees whose valuable comments and suggestions have tremendously improved the quality of this paper. As well as to István Gaál for his encouragement and advice and to Enric Nart who introduced him to Newton polygon techniques.

Conflicts of Interest: There are non-financial competing interests to report.

References

1. Hasse, H. *Zahlentheorie*; Akademie-Verlag: Berlin, Germany, 1963.
2. Hensel, K. *Theorie der Algebraischen Zahlen*; Teubner Verlag: Leipzig, Germany, 1908.
3. Gaál, I. *Diophantine Equations and Power Integral Bases, Theory and Algorithm*, 2nd ed.; Birkhäuser: Boston, MA, USA, 2019.
4. Ahmad, S.; Nakahara, T.; Hameed, A. On certain pure sextic fields related to a problem of Hasse. *Int. J. Alg. Comput.* **2016**, *26*, 577–583. [CrossRef]
5. Gaál, I.; Györy, K. Index form equations in quintic fields. *Acta Arith.* **1999**, 89, 379–396. [CrossRef]
6. Pethö, A.; Pohst, M. On the indices of multiquadratic number fields. *Acta Arith.* **2012**, *153*, 393–414. [CrossRef]
7. Dedekind, R. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Göttingen Abh.* **1878**, *23*, 1–23.
8. Endler, O. *Valuation Theory*; Springer: Berlin, Germany, 1972.
9. Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*; Springer: Berlin/Heidelberg, Germany, 2004.
10. Nakahara, T. On the indices and integral bases of non-cyclic but abelian biquadratic fields. *Arch. Der Math.* **1983**, *41*, 504–508. [CrossRef]
11. Gaál, I.; Pethö, A.; Pohst, M. On the indices of biquadratic number fields having Galois group V_4. *Arch. Math.* **1991**, *57*, 357–361. [CrossRef]
12. El Fadil, L.; Montes, J.; Nart, E. Newton polygons and p-integral bases of quartic number fields. *J. Algebra Appl.* **2012**, *11*, 1250073. [CrossRef]
13. Davis, C.T.; Spearman, B.K. The index of a quartic field defined by a trinomial $x^4 + ax + b$. *Alg. Its Appl.* **2018**, *17*, 1850197. [CrossRef]
14. El Fadil, L. A note on Indices of Quartic Number Fields Defined by Trinomials $x^4 + ax + b$. *Commun. Algebra.* **2023** . [CrossRef]
15. El Fadil, L.; Gaál, I. On non-monogenity of certain number fields defined by trinomials $x^4 + ax^2 + b$. *Mathematics* 2022, *submitted*.
16. Gaál, I. An experiment on the monogenity of a family of trinomials. *J. Algebra Number Theory Appl.* **2021**, *51*, 97–111.
17. El Fadil, L. On non monogenity of certain number fields defined by a trinomial $x^6 + ax^3 + b$. *J. Number Theory* **2022**, *239*, 489–500.. [CrossRef]
18. El Fadil, L. On common index divisor and monogenity of certain number fields defined by a trinomial $x^5 + ax^2 + b$. *Commun. Algebra* **2022**, *50*, 3102–3112. [CrossRef]
19. El Fadil, L. On index and monogenity of certain number fields defined by trinomials. *Math. Slovaca* **2023**, *73*, 861–870. [CrossRef]
20. Guardia, J.; Montes, J.; Nart, E. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. ThÉorie Des Nombres Bordeaux* **2011**, *23*, 3667–3696. [CrossRef]
21. LlOrente, P.; Nart, E.; Vila, N. Decomposition of primes in number fields defined by trinomials. *Séminaire Théorie Des Nombres Bordeaux* **1991**, *3*, 27–41. [CrossRef]
22. El Fadil, L. A generalization of Eisenstein-Shonemann's irreducibility criterion. *Tatra Mt. Math. Publ.* **2023**, *83*, 51–56.
23. Gaál, I.; Remete, L. Power integral bases and monogenity of pure fields. *J. Number Theory* **2017**, *173*, 129–146. [CrossRef]
24. Hensel, K. Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante. *J. FüR Die Reine Und Angew. Math.* **1894**, *113*, 61–83.
25. Ore, O. Newtonsche Polygone in der Theorie der algebraischen Korper. *Math. Ann.* **1928**, *99*, 84–117. [CrossRef]
26. Guardia, J.; Montes, J.; Nart, E. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.* **2012**, *364*, 361–416. [CrossRef]
27. Deajim, A.; El Fadil, L. On the integral closednessof $R[\alpha]$. *Math. Rep.* **2022**, *24*, 571–581.
28. Engstrom, H.T. On the common index divisors of an algebraic field. *Trans. Am. Math. Soc.* **1930**, *32*, 223–237. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.