New York Journal of Mathematics

New York J. Math. **30** (2024) 1585–1601.

An infinite families of number fields with fixed indices arising from quintinomials of type $x^n + ax^m + bx^2 + cx + d$

Omar Kchit

ABSTRACT. In this paper, for any rational prime p and for a fixed positive integer i_p, we provide infinite families of number fields defined by irreducible quintinomials of type $x^n + ax^m + bx^2 + cx + d \in \mathbb{Z}[x]$ satisfying $\nu_p(i(K)) = i_p$. We illustrate our results by some computational examples.

CONTENTS

1. Introduction

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n with ring of integers $\mathbb{Z}_K$, where α is a primitive integer of K. The index of α, denoted by $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, is the index of the Abelian group $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$. A well-known formula linking this index with the discriminants is given by:

$$\Delta(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 \cdot d_K, \tag{1.1}$$

where d_K is the absolute discriminant of K and $\Delta(\alpha)$ is the discriminant of the minimal polynomial of α over $\mathbb{Q}$. The index of K, denoted by $i(K)$, is defined as the greatest common divisor of the indices of all primitive integers of K. Say, $i(K) = \gcd\{(\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K\}$. Remark that for a monogenic number field K, the index is trivial; $i(K) = 1$. Therefore, a field with a non-trivial index is not monogenic. Dedekind was the first one who discovered a number field with non-trivial index ([3]). In 1930, for every number field K of degree $n \leq 7$ and every rational prime p, Engstrom established a connection between the prime ideal factorization of $p\mathbb{Z}_K$ and $\nu_p(i(K))$. This motivated a very

Received September 12, 2024.

2010 *Mathematics Subject Classification.* 11R04, 11Y40, 11R21.

Key words and phrases. Theorem of Dedekind, Theorem of Ore, prime ideal factorization, Newton polygon, index of a number field, monogenic.

ISSN 1076-9803/2024

important question, stated as problem 22 in Narkiewicz's book ([23]), which asks for an explicit formula of the highest power $\nu_p(i(K))$ for a given rational prime p dividing $i(K)$. In [28], Śliwa extended Engstrom's results to number fields up to degree 12, under the condition that p is unramified in K. These results were generalized by Nart ([24]), who developed a p-adic characterization of the index of a number field. In [22], Nakahara studied the indices of non-cyclic but abelian biquadratic number fields. In [12], Funakura showed that $i(K) = 1$ or 2 for every pure quartic number field K. In [14], Gaál et al. characterized the field indices of biquadratic number fields having Galois group V_4. In [29], Spearman and Williams characterized the indices of cyclic quartic number fields. In [27], Pethö and Pohst studied the index divisors of multiquadratic number fields. Recently, many authors are interested in the characterization of the prime power decomposition of the indices of number fields, especially those defined by trinomials and quadrinomials of fixed degrees (see [2, 4, 5, 6, 7, 8, 9, 12, 14, 19, 20, 21, 22, 27, 29]). In all the former papers, for a given number field K, the authors try to calculate the index $i(K)$. In contrast, the present paper introduces a new approach. Namely, for every rational prime p and some natural integers i_p, we construct infinite families of number fields defined by irreducible quintinomials of type $x^n+ax^m+bx^2+cx+d \in \mathbb{Z}[x]$, with p-indices i_p, where the p-index of a number field K is defined as the p-valuation of its index. Namely, $i_p = \nu_p(i(K))$. Especially, for the rational prime $p = 2$, we provide families of number fields having 2-indices $i_2 \in \{1, 2, 3, 4, 5\}$. For every odd rational prime p, we provide families of number fields with p-indices $i_p \in \{1, 2, p-2, p-1, p\}$. These results present infinite families of number fields defined by quintinomials with large indices independently of the degree of these fields.

2. Main results

We start by Table 1, which presents examples where, for some fixed values of i, we provide an example of a number field with index $i(K) = i$. All these examples are collected from some former papers (see [2, 4, 5, 7, 8, 9, 19, 20, 21]).

Given that for every natural integer i, $i = \prod_p p^{i_p}$, in the remainder of this paper, for every rational prime p and some fixed natural integers i_p, we provide infinite families of number fields defined by irreducible quintinomials of the form $F(x) = x^n + ax^m + bx^2 + cx + d \in \mathbb{Z}[x]$ with p-indices i_p. In each case, we establish sufficient conditions which guarantee that $\nu_p(i(K)) = i_p$.

Recall that, for every rational integer $z \in \mathbb{Z}$, the $(x-z)$-Taylor expansion of $F(x)$ is given by the following:

$$F(x) = \sum_{k=0}^{n} \frac{F^{(k)}(z)}{k!}(x-z)^k, \text{ where } n \text{ is the degree of } F(x).$$

TABLE 1. Examples of number fields defined by trinomials or quadrinomials with some specific indices

$F(x)$	The index $i(K)$
$x^4 + 48x + 15$	2
$x^5 + 143x^3 + 459$	3
$x^6 + 144x^5 + 399$	4
$x^9 + 1014x^5 - 1903125$	5
$x^7 + 1269x^3 + 4282$	6
$x^9 + 183x + 296$	8
$x^5 + 100x^3 + 142x + 54$	9
$x^9 + 109x^5 - 1668750$	10
$x^{12} + 1612500x^2 + 25410$	11
$x^5 + 352x^2 + 135x + 72$	12
$x^9 + 954x^5 + 118840625$	15
$x^7 + 188x + 576$	18
$x^9 + 139x^5 + 1412500$	20

We shall denote $A_k(z) = \dfrac{F^{(k)}(z)}{k!}$.

In the remainder, K is a number field defined by irreducible quintinomials of type $x^n + ax^m + bx^2 + cx + d \in \mathbb{Z}[x]$.
For $p = 2$ and $i_2 \in \{1, 2\}$, Theorem 2.1 provides sufficient conditions on $F(x)$, which guarantee that each number field of these infinite families has 2-index $i_2 \in \{1, 2\}$.

Theorem 2.1. *Table 2 provides sufficient conditions which guarantees that $\nu_2(i(K)) \in \{1, 2\}$.*

TABLE 2. Number fields defined by quintinomials with 2-indices $i_2 \in \{1, 2\}$

(a, b, c, d) (mod 2)	***Conditions***	$\nu_2(i(K))$
$(0, 1, 0, 0)$	$\nu_2(d) > 2\nu_2(c)$ *and* $n = 2k + 1$	1
	$\nu_2(d) > 2\nu_2(c)$, $n - 2 = 2^r$ *and* $A_0(1) \equiv 2 \pmod 4$	
	$\nu_2(d) > 2\nu_2(c)$, $n - 2 = 2^r$, $A_0(1) \equiv 0 \pmod 8$ *and* $A_1(1) \equiv 2 \pmod 4$	2
$(1, 0, 0, 0)$	$\nu_2(d) > 2\nu_2(c) - \nu_2(b)$, $(m - 2)\nu_2(c) > (m - 1)\nu_2(b)$ *and* $n \not\equiv m \pmod 2$	

Example 2.2. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{15} + 6x^{10} + 3x^2 + 18x + 24$. Since $a \equiv c \equiv d \equiv 0 \pmod 2$, $b \equiv 1 \pmod 2$, $\nu_2(d) = 3$, $\nu_2(c) = 1$ $n = 15$. Then by Theorem 2.1, $\nu_2(i(K)) = 1$.*

Example 2.3. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{22} + 25x^{13} + 10x^2 + 60x + 80$. Since $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$, $\nu_2(d) = 4$, $\nu_2(c) = 2$, $\nu_2(b) = 1$ and $n \not\equiv m \pmod 2$. Then by Theorem* 2.1*, $\nu_2(i(K)) = 2$.*

Theorems 2.4 and 2.6 provide infinite families of number fields with 2-indices $i_2 = 3$.

Theorem 2.4. *Suppose that $a \equiv 1 \pmod 2$ and $b \equiv c \equiv d \equiv 0 \pmod 2$. If the following conditions simultaneously hold, then $\nu_2(i(K)) = 3$.*

(1) $m \geq 4$ *and* $n - m = 2^r$ $(r \geq 2)$.
(2) $A_0(1) \equiv 0 \pmod 4$ *and* $A_1(1) \equiv 2 \pmod 4$.
(3) $\nu_2(d) < 2\nu_2(c) - \nu_2(b)$ *and* $(m-2)\nu_2(d) > m\nu_2(b)$.
(4) $\nu_2(d) \not\equiv \nu_2(b) \pmod 2$ *and* $\gcd(m-2, \nu_2(b)) = 1$.

Example 2.5. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{16} + 21x^{12} + 14x^2 + 56x + 28$. Since $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$, $\nu_2(d) = 2$, $\nu_2(c) = 3$, $\nu_2(b) = 1$, $\nu_2(A_0(1)) = 3$ and $\nu_2(A_1(1)) = 1$. Then by Theorem* 2.4*, $\nu_2(i(K)) = 3$.*

Theorem 2.6. *Suppose that $a \equiv 1 \pmod 2$ and $b \equiv c \equiv d \equiv 0 \pmod 2$. If the following conditions simultaneously hold, then $\nu_2(i(K)) = 3$.*

(1) $n - m = 3$.
(2) $\nu_2(c) - \nu_2(d) < \nu_2(b) - \nu_2(c) < \dfrac{-\nu_2(b)}{m-2}$.
(3) $\gcd(m-2, \nu_2(b)) = 3$.

Example 2.7. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{23} + 15x^{20} + 72x^2 + 480x + 192$. Since $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$, $n - m = 3$, $\nu_2(d) = 6$, $\nu_2(c) = 4$, $\nu_2(b) = 3$ and $m - 2 = 18$. Then by Theorem* 2.6*, $\nu_2(i(K)) = 3$.*

The following theorem provides infinite families of number fields with 2-indices $i_2 \in \{4, 5\}$.

Theorem 2.8. *Suppose that $a \equiv 1 \pmod 2$ and $b \equiv c \equiv d \equiv 0 \pmod 2$. If the following conditions simultaneously hold, then $\nu_2(i(K)) = 4$ or 5.*

(1) $n - m = 2^r$.
(2) $A_0(1) \equiv 0 \pmod 8$ *and* $A_1(1) \equiv 2 \pmod 4$.
(3) $\nu_2(c) - \nu_2(d) < \nu_2(b) - \nu_2(c) < \dfrac{-\nu_2(b)}{m-2}$.
(4) $m - 2 = 2k + 1$ *divides* $\nu_2(b)$.

More precisely, if $r \geq 2$, then $\nu_2(i(K)) = 4$ and $\nu_2(i(K)) = 5$ if $r = 1$.

Example 2.9. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{35} + 25x^3 + 30x^2 + 40x + 1920$. Since $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$, $n - m = 2^5$, $\nu_2(d) = 7$, $\nu_2(c) = 3$, $\nu_2(b) = 1$, $\nu_2(A_0(1)) = 5$ and $\nu_2(A_1(1)) = 1$. Then by Theorem* 2.8, *$\nu_2(i(K)) = 4$.*

In the remainder of this section, for every odd rational prime p and $i_p \in \{1, 2, p-2, p-1, p\}$, we provide infinite families of number fields with $\nu_p(i(K)) = i_p$. We shall denote $B_p = \dfrac{B}{p^{\nu_p(B)}}$ for every rational integer B.
In particular, Theorem 2.10 provides infinite families of number fields K with p-indices $i_p = 1$ for every odd rational prime p.

Theorem 2.10. *Suppose that $b \equiv -1 \pmod p$, $a \equiv c \equiv d \equiv 0 \pmod p$, $n - 2 = k(p - 1)$ and $n \not\equiv 2 \pmod p$. If any of the following conditions is satisfied, then $\nu_p(i(K)) = 1$.*

(1) *$\nu_p(d) > 2\nu_p(c)$.*
(2) *$\nu_p(d) = 2h < 2\nu_p(c)$ and $d_p \equiv 1 \pmod p$.*

Example 2.11. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{18} + 15x^{13} + 9x^2 + 45x + 375$. Since $b \equiv -1 \pmod 5$, $a \equiv c \equiv d \equiv 0 \pmod 5$, $\nu_5(c) = 1$, $\nu_5(d) = 3$ and $n \equiv 3 \pmod 5$. Then by Theorem* 2.10 *(1), $\nu_5(i(K)) = 1$.*

For every odd rational prime p and $i_p = 2$, Theorem 2.12 provides infinite families of number fields with p-indices $i_p = 2$.

Theorem 2.12. *Suppose that $a \equiv -1 \pmod p$, $b \equiv c \equiv d \equiv 0 \pmod p$ and $n-m = k(p-1)$. If the following conditions simultaneously hold, then $\nu_p(i(K)) = 2$.*

(1) *$n \not\equiv m \pmod p$.*
(2) *$\nu_2(c) - \nu_2(d) < \nu_2(b) - \nu_2(c) < \dfrac{-\nu_2(b)}{m-2}$.*
(3) *$\gcd(\nu_p(b), m - 2) = 1$.*

Example 2.13. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{52} + 54x^{22} + 2 \cdot 11x^2 + 4 \cdot 11^2x + 2 \cdot 11^4$. Since $a \equiv -1 \pmod{11}$, $b \equiv c \equiv d \equiv 0 \pmod{11}$, $\nu_{11}(b) = 1$, $\nu_{11}(c) = 2$, $\nu_{11}(d) = 4$, $n \not\equiv m \pmod{11}$ and $n - m = 3(11 - 1)$. Then by Theorem* 2.12, *$\nu_{11}(i(K)) = 2$.*

For every rational prime p, the next theorem provides infinite families of number fields with p-indices $i_p = p - 2$.

Theorem 2.14. *Suppose that $a \equiv -1 \pmod p$, $b \equiv c \equiv d \equiv 0 \pmod p$, $\nu_p(d) < 2\nu_p(c) - \nu_p(d)$ and $(m - 2)\nu_p(d) < m\nu_p(b)$. If the following conditions simultaneously hold, then $\nu_p(i(K)) = p - 2$.*

(1) *$m = k(p-1)$ divides $\nu_p(d)$.*
(2) *$n - m = h(p-1)$.*
(3) *$\gcd(k,h) = 1$ and $kh \not\equiv 0 \pmod{p}$.*
(4) *$d_p \equiv 1 \pmod{p}$.*

Example 2.15. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{72}+20x^{16}+5\cdot 7^8x^2+5\cdot 7^7x+15\cdot 7^6$. Since $a \equiv -1 \pmod{7}$, $b \equiv c \equiv d \equiv 0 \pmod{7}$, $\nu_7(d) = 6$, $\nu_7(c) = 7$, $\nu_7(b) = 8$, $m = (7-1)$ divides $\nu_7(d)$, $n - m = 11(7-1)$, $\gcd(11,1) = 1$, $11 \not\equiv 0 \pmod{7}$ and $d_7 \equiv 1 \pmod{7}$. Then by Theorem 2.14, $\nu_7(i(K)) = 5$.*

Theorem 3.1 provides infinite families of number fields with p-indices $i_p = p-1$ for every odd rational prime p.

Theorem 2.16. *Suppose that $a \equiv -1 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$, $(m-1)\nu_p(d) > m\nu_p(c)$ and $(m-2)\nu_p(c) < (m-1)\nu_p(b)$. If the following conditions simultaneously hold, then $\nu_p(i(K)) = p-1$.*

(1) *$m - 1 = k(p-1)$ divides $\nu_p(c)$.*
(2) *$n - m = h(p-1)$.*
(3) *$\gcd(k,h) = 1$ and $kh \not\equiv 0 \pmod{p}$.*
(4) *$c_p \equiv 1 \pmod{p}$.*

Example 2.17. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{141} + 28x^{29} + 14\cdot 29^{30}x^2 + 2^4\cdot 7^2\cdot 29^{28}x + 7\cdot 29^{31}$. Since $a \equiv -1 \pmod{29}$, $b \equiv c \equiv d \equiv 0 \pmod{29}$, $\nu_{29}(b) = 30$, $\nu_{29}(c) = 28$, $\nu_{29}(d) = 31$, $m-1 = (29-1)$ divides $\nu_{29}(c)$, $n - m = 4(29-1)$, $4 \not\equiv 0 \pmod{29}$ and $c_{29} \equiv 1 \pmod{29}$. Then by Theorem 2.16, $\nu_{29}(i(K)) = 28$.*

In the next theorem, for every odd rational prime p, we provide infinite families of number fields K with p-indices $i_p = p$.

Theorem 2.18. *Suppose that $a \equiv -1 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$ and $\nu_p(c) - \nu_p(d) < \nu_p(b) - \nu_p(c) < \dfrac{-\nu_p(b)}{m-2}$. If the following conditions simultaneously hold, then $\nu_p(i(K)) = p$.*

(1) *$m - 2 = k(p-1)$ divides $\nu_p(b)$.*
(2) *$n - m = h(p-1)$.*
(3) *$\gcd(k,h) = 1$ and $kh \not\equiv 0 \pmod{p}$.*
(4) *$b_p \equiv 1 \pmod{p}$.*

Example 2.19. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{283} + 163x^{42} + 42\cdot 41^{40}x^2 + 9\cdot 41^{42}x + 3\cdot 41^{48}$. Since $a \equiv -1 \pmod{41}$, $b \equiv c \equiv d \equiv 0 \pmod{41}$, $\nu_{41}(d) = 48$, $\nu_{41}(c) = 42$, $\nu_{41}(b) = 40$, $m = (41-1)$ divides $\nu_{41}(b)$, $n - m = 6(41-1)$, $\gcd(6,1) = 1$, $6 \not\equiv 0 \pmod{41}$ and $b_{41} \equiv 1 \pmod{41}$. Then by Theorem 2.18, $\nu_{41}(i(K)) = 41$.*

The following example provides a number field with index $i(K) = 2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19^{18}$.

Example 2.20. *Let $K = \mathbb{Q}(\alpha)$ be a number field defined by the monic irreducible quintinomial $F(x) = x^{55} + ax^{19} + bx^2 + cx + d$, where*

$$\begin{array}{rcl} a & = & 2^3 \cdot 3 \cdot 1801, \\ b & = & 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19^{18}, \\ c & = & 2^{15} \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19^{18} \textit{ and} \\ d & = & 2^{32} \cdot 3 \cdot 5^5 \cdot 7^5 \cdot 13^7 \cdot 19^{20}. \end{array}$$

By the index formula (1.1)*, one can check easily that the rational prime candidates to divide the index $i(K)$ are $p = 2, 3, 5, 7, 13$ and 19.*

(1) *For $p = 2$, we have $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$, $\nu_2(d) = 3$, $\nu_2(c) = 1$ and n is odd. Then by Theorem* 2.1*, $\nu_2(i(K)) = 1$.*
(2) *For $p = 3$, $F(x)$ is 3-Eisenstein. Hence $\nu_3(i(K)) = 0$.*
(3) *For $p = 5$, we have $a \equiv -1 \pmod 5$, $b \equiv c \equiv d \equiv 0 \pmod 5$, $\nu_5(b) = 1$, $\nu_5(c) = 2$, $\nu_5(d) = 5$, $n-m = 9(5-1)$, $n \not\equiv m \pmod 5$ and $\gcd(\nu_5(b), m-2) = 1$. Then by Theorem* 2.12*, $\nu_5(i(K)) = 2$.*
(4) *For $p = 7$, we have $a \equiv -1 \pmod 7$, $b \equiv c \equiv d \equiv 0 \pmod 7$, $\nu_7(b) = 1$, $\nu_7(c) = 2$, $\nu_7(d) = 5$, $n-m = 6(7-1)$, $n \not\equiv m \pmod 7$ and $\gcd(\nu_7(b), m-2) = 1$. Then by Theorem* 2.12*, $\nu_7(i(K)) = 2$.*
(5) *For $p = 13$, we have $a \equiv -1 \pmod{13}$, $b \equiv c \equiv d \equiv 0 \pmod{13}$, $\nu_{13}(b) = 1$, $\nu_{13}(c) = 2$, $\nu_{13}(d) = 5$, $n - m = 3(13 - 1)$, $n \not\equiv m \pmod{13}$ and $\gcd(\nu_{13}(b), m - 2) = 1$. Then by Theorem* 2.12*, $\nu_{13}(i(K)) = 2$.*
(6) *For $p = 19$, we have $a \equiv -1 \pmod{19}$, $b \equiv c \equiv d \equiv 0 \pmod{19}$, $\nu_{19}(b) = 18$, $\nu_{19}(c) = 18$, $\nu_{19}(d) = 20$, $m - 1 = (19 - 1)$ divides $\nu_{19}(c)$, $n - m = 2(19 - 1)$, $\gcd(1, 2) = 1$, $2 \not\equiv 0 \pmod{19}$ and $c_{19} \equiv 1 \pmod{19}$. Then by Theorem* 2.16*, $\nu_{19}(i(K)) = 18$.*

Finally, we conclude that $i(K) = 2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19^{18}$.

3. Preliminaries

Our proofs are based on Newton polygon techniques applied on prime ideal factorization, which is rather technical but very efficient to apply. We have introduced the corresponding concepts in several former papers. Here we only give the theorem of index of Ore which plays a key role for proving our main results. For more details, we refer to [10] and [16].

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$. We shall use Dedekind's theorem [25, Chapter I, Proposition 8.3] and Dedekind's criterion [1, Theorem 6.1.4]. Let $\phi \in \mathbb{Z}_p[x]$ be a monic lift to an irreducible factor of $F(x)$ modulo p, $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_k(x)\phi(x)^k$ the ϕ-expansion of $F(x)$ and $N_\phi^+(F)$ the principal ϕ-Newton polygon of $F(x)$, which can be obtained only by considering the principal ϕ-expansion of $F(x)$. As defined in [10, Def. 1.3], the ϕ-index of $F(x)$, denoted $\mathrm{ind}_\phi(F)$, 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 beyond the vertical axis. Let $\mathbb{F}_\phi$ be the field $\mathbb{F}_p[x]/(\overline{\phi})$ and $u_i = \nu_p(a_i(x))$, then to every side S of $N_\phi^+(F)$ with initial point (s, u_s), length $l = l(S)$ and every $i = 0, \dots, l$, let the residue coefficient $c_i \in \mathbb{F}_\phi$ 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 and $l = l(S)$ its length. Then $d = l/e$ is the degree of S. Hence, if i is not a multiple of e, then $(s+i, u_{s+i})$ does not lie on S and $c_i = 0$. Let $R_\lambda(F)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$ be the residual polynomial of $F(x)$ associated to the side S, where for every $i = 0, \dots, d$, $t_i = c_{s+ie}$. If $R_\lambda(F)(y)$ is square-free for each side of the polygon $N_\phi^+(F)$, then we say that $F(x)$ is ϕ-regular.

Let $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi_i}^{k_i}$ be the factorization of $F(x)$ into powers of monic irreducible coprime polynomials over $\mathbb{F}_p$, 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 $i = 1, \dots, r$. 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 $j = 1, \dots, r_i$, let $R_{\lambda_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $R_{\lambda_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of index of Ore:

Theorem 3.1. (*Ore*) ([10, Theorem 1.7 and Theorem 1.9])
Under the above hypothesis, we have the following:

(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*
$$p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{r_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}}$$
is the factorization of $p\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$, where 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 $f_{ijs} = \deg(\phi_i) \cdot \deg(\psi_{ijs})$ for every (i, j, s).

For the proof of our results, we need the following lemma, which characterizes the prime divisors of $i(K)$.

Lemma 3.2. (*Hensel*) ([11])
Let p be a rational prime and K a number field. For every positive integer f, let $\mathcal{P}_f$ be the number of distinct prime ideals of $\mathbb{Z}_K$ lying above p with residue degree f and $\mathcal{N}_f$ the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. Then p divides the index $i(K)$ if and only if $\mathcal{P}_f > \mathcal{N}_f$ for some positive integer f.

For every number field of degree $n \leq 7$ and every rational prime p, Engstrom established a connection between $i_p = \nu_p(i(K))$ and the prime ideal factorization of $p\mathbb{Z}_K$. That is, from the factorization of $p\mathbb{Z}_K$, one can determine explicitly i_p. Moreover, he provided some formulas which allow us to evaluate i_p for some particular number fields of degree $n \geq 8$ (for more details, see [11]). Also, Śliwa extended Engstrom's results to number fields up to degree 12, under the condition that p is unramified in the extension $K/\mathbb{Q}$ (see [28]).

4. Proofs of main results

Recall that, according to the factorization given in Theorem 3.1, we use the triple indices in the factorization of $p\mathbb{Z}_K$. Namely,

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

Here e_{ij} is the ramification index of $\mathfrak{p}_{ijs}$ and $f_{ijs} = \deg(\phi_i)\cdot\deg(\psi_{ijs})$ is its residue degree for every (i,j,s).

Proof of Theorem 2.1.

(1) If $a \equiv c \equiv d \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$, then $F(x) \equiv x^n - x^2 \equiv x^2(x^{n-2}-1) \pmod 2$. Let $\phi_1 = x$. Since $\nu_2(d) > 2\nu_2(c)$, then $N_{\phi_1}^{+}(F) = S_{11} + S_{12}$ has two sides joining $(0,\nu_2(d))$, $(1,\nu_2(c))$ and $(2,0)$. Thus the degree of each side of $N_{\phi_1}^{+}(F)$ is 1. Hence ϕ_1 provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1. On the other hand, we have the following:

(a) If n is odd, then $x^{n-2}-1$ is a separable polynomial over $\mathbb{F}_2$. Since $x-1$ divides $x^{n-2}-1$ and $x^{n-2}-1 \equiv (x-1)U(x) \pmod 2$ with $\gcd(x-1, U(x)) = 1$. Then $x-1$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1. The prime ideals provided by $U(x)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. We conclude that $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{211}\mathfrak{a}$ with $f_{111} = f_{121} = f_{211} = 1$ and the prime ideal factorization of $\mathfrak{a}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. By Lemma 3.2, 2 divides $i(K)$. Applying [11, Theorem 4], we get $\nu_2(i(K)) = 1$.

(b) If $n-2 = 2^r$ $(r \geq 1)$, then $F(x) \equiv x^2(x-1)^{2^r} \pmod 2$. Let $\phi_2 = x-1$. Then $F(x) = \sum_{i=0}^{n} A_i(1)\phi_2^i$. Since $A_0(1) \equiv 2 \pmod 4$, $N_{\phi_2}^{+}(F) =$

S_{21} has a single side of height 1. Thus $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{211}^{2^r}$ with residue degree 1 each ideal factor. Applying [11, Corollary], we get $\nu_2(i(K)) = 1$.

(c) If $n-2 = 2^r$ $(r \geq 1)$, then $F(x) \equiv x^2(x-1)^{2^r} \pmod 2$. Let $\phi_2 = x-1$. Then $F(x) = \sum_{i=0}^{n} A_i(1)\phi_2^i$. Since $A_0(1) \equiv 0 \pmod 8$ and $A_1(1) \equiv 2 \pmod 4$, then $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has two sides joining $(0, \nu_2(A_0(1)))$, $(1, \nu_2(A_1(1)))$ and $(2^r, 0)$. Thus the degree of each side of $N_{\phi_2}^+(F)$ is 1, and so $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{211}\mathfrak{p}_{221}^{2^r-1}$ with residue degree 1 each ideal factor. If $r = 1$, then by [11, Theorem 4], $\nu_2(i(K)) = 2$. If $r \geq 2$, then by [11, Corollary], we get $\nu_2(i(K)) = 2$ also.

(2) If $a \equiv 1 \pmod 2$ and $b \equiv c \equiv d \equiv 0 \pmod 2$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{n-m} - 1) \pmod 2$. Let $\phi_1 = x$. Since $\nu_2(d) > 2\nu_2(c) - \nu_2(b)$ and $(m-2)\nu_2(c) > (m-1)\nu_2(b)$, then $N_{\phi_1}^+(F) = S_{11} + S_{12} + S_{13}$ has three sides joining $(0, \nu_2(d))$, $(1, \nu_2(c))$, $(2, \nu_2(b))$ and $(m, 0)$. Thus the degree of each side of $N_{\phi_1}^+(F)$ is 1. Hence ϕ_1 provides three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1. On the other hand, $n \not\equiv m \pmod 2$, then $x^{n-m} - 1$ is separable over $\mathbb{F}_2$. Since $x-1$ divides $x^{n-m}-1$, and $x^{n-m} - 1 \equiv (x-1)U(x) \pmod 2$ with $\gcd(x-1, U(x)) = 1$, then $x-1$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1. The prime ideals provided by $U(x)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. We conclude that $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{131}^{m-2}\mathfrak{p}_{211}\mathfrak{a}$ with $f_{111} = f_{121} = f_{131} = f_{211} = 1$ and the prime ideal factorization of $\mathfrak{a}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. If $m = 3$, then by [11, Theorem 4], we get $\nu_2(i(K)) = 2$. If $m \geq 4$, then by [11, Corollary], we get $\nu_2(i(K)) = 2$ also.

□

Proof of Theorem 2.4.

If $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$ and $n-m = 2^r$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{2^r} - 1) \equiv x^m(x-1)^{2^r} \pmod 2$, where $r \geq 2$. Let $\phi_1 = x$ and $\phi_2 = x-1$. Then

$$\begin{aligned} F(x) &= \phi_1^n + a\phi_1^m + b\phi_1^2 + c\phi_1 + d, \\ &= \sum_{i=0}^{n} A_i(1)\phi_2^i. \end{aligned}$$

Since $A_0(1) \equiv 0 \pmod 4$ and $A_1(1) \equiv 2 \pmod 4$, then $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has two sides joining $(0, \nu_2(A_0))$, $(1, 1)$ and $(2^r, 0)$ with $\nu_2(A_0(1)) \geq 2$ (see Figure 1). Thus the degree of each side of $N_{\phi_2}^+(F)$ is 1. Hence ϕ_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1. On the other hand, $\nu_2(d) < 2\nu_2(c) - \nu_2(b)$ and $(m-2)\nu_2(d) > m\nu_2(b)$. Then $N_{\phi_1}^+(F) = S_{11} + S_{12}$ has two sides joining $(0, \nu_2(d))$, $(2, \nu_2(b))$ and $(m, 0)$ (see Figure 1). Since $\nu_2(d) \not\equiv \nu_2(b) \pmod 2$ and $\gcd(m-2, \nu_2(b)) = 1$, then $d(S_{11}) = d(S_{12}) = 1$. We conclude that $2\mathbb{Z}_K = \mathfrak{p}_{111}^2 \mathfrak{p}_{121}^{m-2} \mathfrak{p}_{211} \mathfrak{p}_{221}^{2^r-1}$ with residue degree 1 each ideal factor. Since $r \geq 2$ and $m \geq 4$, then $m-2 \geq 2$ and $2^r \geq 3$. Applying [11, Theorem 6], we get $\nu_2(i(K)) = 3$.

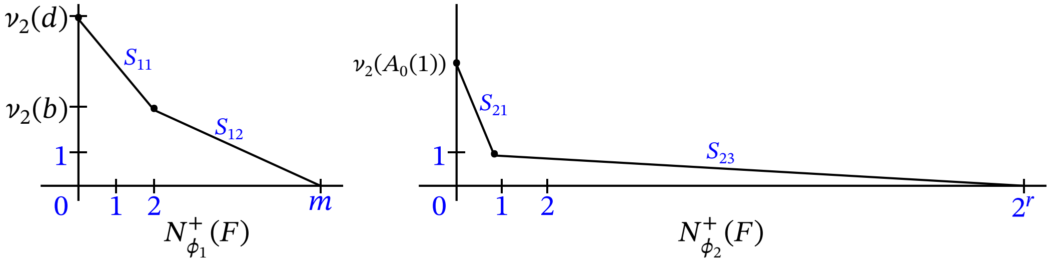

FIGURE 1. $N_{\phi_i}^+(F)$, $i = 1, 2$

□

Proof of Theorem 2.6.
If $a \equiv 1 \pmod 2$ and $b \equiv c \equiv d \equiv 0 \pmod 2$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{n-m}-1) \equiv x^m(x-1)(x^2+x+1) \pmod 2$. Let $\phi_1 = x$. Since $\nu_2(c)-\nu_2(d) < \nu_2(b) - \nu_2(c) < \dfrac{-\nu_2(b)}{m-2}$, then $N_{\phi_1}^+(F) = S_{11} + S_{12} + S_{13}$ has three sides joining $(0, \nu_2(d))$, $(1, \nu_2(c))$, $(2, \nu_2(b))$ and $(m, 0)$ with $d(S_{11}) = d(S_{12}) = 1$. Since $\gcd(m-2, \nu_2(b)) = 3$, then $R_{\lambda_{13}}(F)(y) = y^3 + 1 = (y+1)(y^2+y+1) \in \mathbb{F}_{\phi_1}[y]$. We conclude that $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{131}^e\mathfrak{p}_{132}^e\mathfrak{p}_{211}\mathfrak{p}_{311}$ with $e = \dfrac{m-2}{3}$, $f_{111} = f_{121} = f_{131} = f_{211} = 1$ and $f_{132} = f_{311} = 2$. Applying [11, Theorem 7], we get $\nu_2(i(K)) = 3$. □

Proof of Theorem 2.8.
If $a \equiv 1 \pmod 2$, $b \equiv c \equiv d \equiv 0 \pmod 2$ and $n - m = 2^r$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{2^r} - 1) \equiv x^m(x-1)^{2^r} \pmod 2$. Let $\phi_1 = x$ and $\phi_2 = x - 1$. Then

$$\begin{aligned} F(x) &= \phi_1^n + a\phi_1^m + b\phi_1^2 + c\phi_1 + d, \\ &= \sum_{i=0}^{n} A_i(1)\phi_2^i. \end{aligned}$$

Since $A_0(1) \equiv 0 \pmod 8$ and $A_1(1) \equiv 2 \pmod 4$, then $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has two sides joining $(0, \nu_2(A_0(1)))$, $(1, 1)$ and $(2^r, 0)$ with $\nu_2(A_0(1)) \geq 3$ (see Figure 2). Thus the degree of each side of $N_{\phi_2}^+(F)$ is 1. Hence ϕ_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1. On the other hand, $\nu_2(c) - \nu_2(d) < \nu_2(b) - \nu_2(c) < \dfrac{-\nu_2(b)}{m-2}$, then $N_{\phi_1}^+(F) = S_{11} + S_{12} + S_{13}$ has three sides joining $(0, \nu_2(d))$, $(1, \nu_2(c))$, $(2, \nu_2(b))$ and $(m, 0)$ with $d(S_{11}) = d(S_{12}) = 1$

(see Figure 2). Since $m-2=2k+1$ divides $\nu_2(b)$, then $d(S_{13})=m-2$ with $R_{\lambda_{13}}(F)(y)=y^{m-2}+1\in\mathbb{F}_{\phi_1}[y]$. Also, $m-2$ is odd, then $R_{\lambda_{13}}(F)(y)$ is separable over $\mathbb{F}_{\phi_1}$ and $R_{\lambda_{13}}(F)(y)=(y+1)U(y)\in\mathbb{F}_{\phi_1}[y]$ with $\gcd(y+1,U(y))=1$, then $y+1$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1. The prime ideals provided by $U(y)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f>1$ and satisfies $\mathcal{P}_f<\mathcal{N}_f$ for every integer f. We conclude that $2\mathbb{Z}_K=\mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{131}\mathfrak{p}_{211}\mathfrak{p}_{221}^{2^r-1}\mathfrak{a}$ with $f_{111}=f_{121}=f_{131}=f_{211}=f_{221}=1$ and the prime ideal factorization of $\mathfrak{a}$ contains only prime ideals with residue degrees $f>1$ satisfying $\mathcal{P}_f<\mathcal{N}_f$ for every positive integer f. If $r=1$, then by [11, Theorem 4], we get $\nu_2(i(K))=5$. If $r\geq 2$, then by [11, Corollary], we get $\nu_2(i(K))=4$.

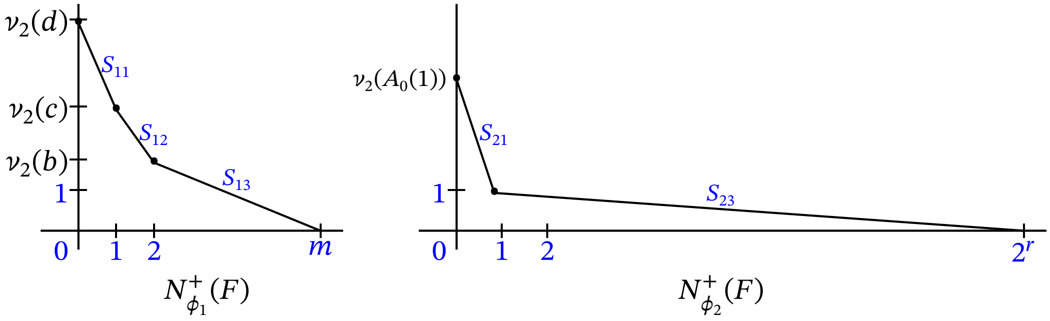

FIGURE 2. $N^+_{\phi_i}(F),\ i=1,2$

□

Proof of Theorem 2.10.
Since $b\equiv -1 \pmod p$, $a\equiv c\equiv d\equiv 0 \pmod p$ and $n-2=k(p-1)$, then $F(x)\equiv x^n-x^2\equiv x^2(x^{k(p-1)}-1) \pmod p$. Since $n\not\equiv 2 \pmod p$, then $x^{k(p-1)}-1$ is separable over $\mathbb{F}_p$ and $x^{k(p-1)}-1\equiv\prod_{i=1}^{p-1}(x-i)U(x) \pmod p$ with $\gcd(x-i,U(x))=1$. Let $\phi_i=x-i$ for every $i=0,\dots,p-1$. Then For every $i=1,\dots,p-1$, ϕ_i provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1. The prime ideals provided by $U(x)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f>1$ and satisfies $\mathcal{P}_f<\mathcal{N}_f$ for every integer f. For ϕ_0, we have the following:

(1) If $\nu_p(d)>2\nu_p(c)$, then $N^+_{\phi_0}(F)=S_{01}+S_{02}$ has two sides joining $(0,\nu_p(d))$, $(1,\nu_p(c))$ and $(2,0)$. Thus the degree of each side of $N^+_{\phi_0}(F)$ is 1. Hence $p\mathbb{Z}_K=\mathfrak{p}_{011}\mathfrak{p}_{021}\prod_{i=1}^{p-1}\mathfrak{p}_{i11}\mathfrak{a}$ with $f_{011}=f_{021}=f_{i11}=1$ for every $i=1,\dots,p-1$ and the prime ideal factorization of $\mathfrak{a}$ contains only prime ideals with residue degrees $f>1$ satisfying $\mathcal{P}_f<\mathcal{N}_f$ for every positive

integer f. By Lemma 3.2, p divides $i(K)$. Applying [11, Theorem 4], we get $\nu_p(i(K)) = 1$.

(2) If $\nu_p(d) = 2h < 2\nu_p(c)$, then $N^+_{\phi_0}(F) = S_{01}$ has a single side joining $(0, \nu_p(d))$ and $(2, 0)$. Since $\nu_p(d) = 2h$ and $d_p \equiv 1 \pmod{p}$, then $d(S_{01}) = 2$ with $R_{\lambda_{01}}(F)(y) = by^2 + d_p = -y^2 + 1 = -(y-1)(y+1) \in \mathbb{F}_{\phi_0}[y]$. Hence $p\mathbb{Z}_K = \mathfrak{p}_{011}\mathfrak{p}_{011}\prod_{i=1}^{p-1}\mathfrak{p}_{i11}\mathfrak{a}$ with $f_{011} = f_{012} = f_{i11} = 1$ for every $i = 1, \dots, p-1$ and the prime ideal factorization of $\mathfrak{a}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. By Lemma 3.2, p divides $i(K)$. Applying [11, Theorem 4], we get $\nu_p(i(K)) = 1$.

□

Proof of Theorem 2.12.

Since $a \equiv -1 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$ and $n - m = k(p-1)$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{k(p-1)} - 1) \pmod{p}$. Since $n \not\equiv m \pmod{p}$, then $x^{k(p-1)} - 1$ is separable over $\mathbb{F}_p$ and $x^{k(p-1)} - 1 \equiv \prod_{i=1}^{p-1}(x-i)U(x) \pmod{p}$ with $\gcd(x-i, U(x)) = 1$ for every $i = 1, \dots, p-1$. Let $\phi_i = x - i$ with $i = 0, \dots, p-1$. Then for every $i = 1, \dots, p-1$, ϕ_i provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1. The prime ideals provided by $U(x)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. For ϕ_0, since $\nu_p(c) - \nu_p(d) < \nu_p(b) - \nu_p(c) < \dfrac{-\nu_p(b)}{m-2}$, then $N^+_{\phi_0}(F) = S_{01} + S_{02} + S_{03}$ has three sides joining $(0, \nu_p(d))$, $(1, \nu_p(c))$, $(2, \nu_p(b))$ and $(m, 0)$ with $d(S_{01}) = d(S_{02}) = 1$ (see Figure 3). Since $\gcd(\nu_p(b), m-2) = 1$, then $d(S_{03}) = 1$ also. Finally, we get $p\mathbb{Z}_K = \mathfrak{p}_{011}\mathfrak{p}_{021}\mathfrak{p}_{031}^{m-2}\prod_{i=1}^{p-1}\mathfrak{p}_{i11}\mathfrak{a}$ with $f_{011} = \mathfrak{p}_{021} = f_{031} = f_{i11} = 1$ for every $i = 1, \dots, p-1$ and the prime ideal factorization of $\mathfrak{a}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. If $m = 3$, then by [11, Theorem 4], we get $\nu_p(i(K)) = 2$. If $m \geq 4$, then by [11, Corollary], we get $\nu_p(i(K)) = 2$ also.

□

Proof of Theorem 2.14.

Since $a \equiv -1 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$ and $n - m = h(p-1)$, then $F(x) \equiv x^n - x^m \equiv x^{k(p-1)}(x^{h(p-1)} - 1) \pmod{p}$. Since $h \not\equiv 0 \pmod{p}$, then $x^{h(p-1)} - 1$ is separable over $\mathbb{F}_p$ and $x^{h(p-1)} - 1 \equiv \prod_{i=1}^{p-1}(x-i)U(x) \pmod{p}$ with $\gcd(x-i, U(x)) = 1$ for every $i = 1, \dots, p-1$. Let $\phi_i = x - i$ with $i = 0, \dots, p-1$. Then for every $i = 1, \dots, p-1$, ϕ_i provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1. The prime ideals provided by $U(x)$, which we denote

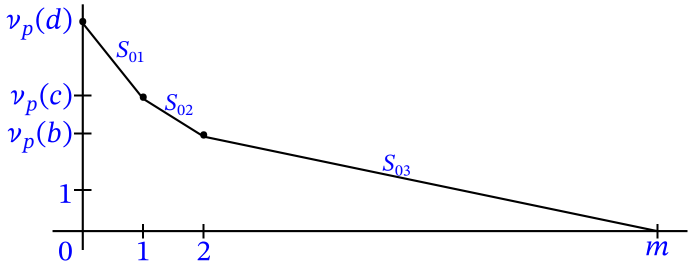

FIGURE 3. $N_{\phi_0}^+(F)$

by the unramified ideal $\mathfrak{a}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. For ϕ_0, since $\nu_p(d) < 2\nu_p(c) - \nu_p(d)$ and $(m-2)\nu_p(d) < m\nu_p(b)$, then $N_{\phi_0}^+(F) = S_{01}$ has a single side joining $(0, \nu_p(d))$ and $(m, 0)$. On the other hand, $m = k(p-1)$ divides $\nu_p(d)$. Thus $R_{\lambda_{01}}(F)(y) = ay^{k(p-1)} + d_p = -y^{k(p-1)} + 1 \in \mathbb{F}_{\phi_0}[y]$. Since $k \not\equiv 0 \pmod{p}$, then $R_{\lambda_{01}}(F)(y)$ is separable over $\mathbb{F}_{\phi_0}$ and $R_{\lambda_{01}}(F)(y) = -\prod_{j=1}^{p-1}(y-j)V(y) \in \mathbb{F}_{\phi_0}[y]$ with $\gcd(y-i, V(y)) = 1$ for every $i = 1, \dots, p-1$. Thus $y-j$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1 for every $j = 1, \dots, p-1$. The prime ideals provided by $V(y)$, which we denote by the unramified ideal $\mathfrak{b}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. Finally, we get $p\mathbb{Z}_K = \prod_{j=1}^{p-1} \mathfrak{p}_{01j} \prod_{i=1}^{p-1} \mathfrak{p}_{i11}\mathfrak{a}\mathfrak{b}$ with $f_{01j} = f_{i11} = 1$ for every $i, j = 1, \dots, p-1$. Since $\gcd(k, h) = 1$ and $\mathbb{F}_{\phi_0} \simeq \mathbb{F}_p$, then $\gcd(U(x), V(x)) = 1$. Therefore, the prime ideal factorization of $\mathfrak{a}\mathfrak{b}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. By [11, Theorem 4], $\nu_p(i(K)) = p-2$. □

Proof of Theorem 2.16.

Since $a \equiv -1 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$ and $n - m = h(p-1)$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{h(p-1)} - 1) \pmod{p}$. Since $h \not\equiv 0 \pmod{p}$, then $x^{h(p-1)} - 1$ is separable over $\mathbb{F}_p$ and $x^{h(p-1)} - 1 \equiv \prod_{i=1}^{p-1}(x-i)U(x) \pmod{p}$ with $\gcd(x-i, U(x)) = 1$ for every $i = 1, \dots, p-1$. Let $\phi_i = x - i$ with $i = 0, \dots, p-1$. Then for every $i = 1, \dots, p-1$, ϕ_i provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1. The prime ideals provided by $U(x)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. For ϕ_0, since $(m-1)\nu_p(d) > m\nu_p(c)$ and $(m-2)\nu_p(c) < (m-1)\nu_p(b)$, then $N_{\phi_0}^+(F) = S_{01} + S_{02}$ has two sides joining $(0, \nu_p(d))$, $(1, \nu_p(c))$ and $(m, 0)$ with $d(S_{01}) = 1$. Since $m - 1 = k(p-1)$ divides $\nu_p(c)$, then $R_{\lambda_{02}}(F)(y) = ay^{k(p-1)} + c_p = -y^{k(p-1)} + 1 \in \mathbb{F}_{\phi_0}[y]$. Since $k \not\equiv 0 \pmod{p}$, then

$R_{\lambda_{02}}(F)(y)$ is separable over $\mathbb{F}_{\phi_0}$ and $R_{\lambda_{02}}(F)(y) = -\prod_{j=1}^{p-1}(y-j)V(y) \in \mathbb{F}_{\phi_0}[y]$ with $\gcd(y-i, V(y)) = 1$ for every $i = 1, \dots, p-1$. Thus $y-j$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1 for every $j = 1, \dots, p-1$. The prime ideals provided by $V(y)$, which we denote by the unramified ideal $\mathfrak{b}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. Finally, we get $p\mathbb{Z}_K = \mathfrak{p}_{011}\prod_{j=1}^{p-1}\mathfrak{p}_{02j}\prod_{i=1}^{p-1}\mathfrak{p}_{i11}\mathfrak{a}\mathfrak{b}$ with $f_{011} = f_{02j} = f_{i11} = 1$ for every $i, j = 1, \dots, p-1$. Since $\gcd(k, h) = 1$ and $\mathbb{F}_{\phi_0} \simeq \mathbb{F}_p$, then $\gcd(U(x), V(x)) = 1$. Therefore, the prime ideal factorization of $\mathfrak{a}\mathfrak{b}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. By [11, Theorem 4], $\nu_p(i(K)) = p-1$. □

Proof of Theorem 2.18.

Since $a \equiv -1 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$ and $n - m = h(p-1)$, then $F(x) \equiv x^n - x^m \equiv x^m(x^{h(p-1)} - 1) \pmod{p}$. Since $h \not\equiv 0 \pmod{p}$, then $x^{h(p-1)} - 1$ is separable over $\mathbb{F}_p$ and $x^{h(p-1)} - 1 \equiv \prod_{i=1}^{p-1}(x-i)U(x) \pmod{p}$ with $\gcd(x-i, U(x)) = 1$ for every $i = 1, \dots, p-1$. Let $\phi_i = x - i$ with $i = 0, \dots, p-1$. Then for every $i = 1, \dots, p-1$, ϕ_i provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1. The prime ideals provided by $U(x)$, which we denote by the unramified ideal $\mathfrak{a}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. For ϕ_0, since $\nu_p(c) - \nu_p(d) < \nu_p(b) - \nu_p(c) < \frac{-\nu_p(b)}{m-2}$, then $N^+_{\phi_0}(F) = S_{01} + S_{02} + S_{03}$ has three sides joining $(0, \nu_p(d))$, $(1, \nu_p(c))$, $(2, \nu_p(b))$ and $(m, 0)$ with $d(S_{01}) = d(S_{02}) = 1$. Since $m - 2 = k(p-1)$ divides $\nu_p(b)$, then $R_{\lambda_{03}}(F)(y) = ay^{k(p-1)} + b_p = -y^{k(p-1)} + 1 \in \mathbb{F}_{\phi_0}[y]$. Since $k \not\equiv 0 \pmod{p}$, then $R_{\lambda_{03}}(F)(y)$ is separable over $\mathbb{F}_{\phi_0}$ and $R_{\lambda_{03}}(F)(y) = -\prod_{j=1}^{p-1}(y-j)V(y) \in \mathbb{F}_{\phi_0}[y]$ with $\gcd(y-i, V(y)) = 1$ for every $i = 1, \dots, p-1$. Thus $y - j$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above p with residue degree 1 for every $j = 1, \dots, p-1$. The prime ideals provided by $V(y)$, which we denote by the unramified ideal $\mathfrak{b}$, have residue degrees $f > 1$ and satisfies $\mathcal{P}_f < \mathcal{N}_f$ for every integer f. Finally, we get $p\mathbb{Z}_K = \mathfrak{p}_{011}\mathfrak{p}_{021}\prod_{j=1}^{p-1}\mathfrak{p}_{03j}\prod_{i=1}^{p-1}\mathfrak{p}_{i11}\mathfrak{a}\mathfrak{b}$ with $f_{011} = f_{021} = f_{03j} = f_{i11} = 1$ for every $i, j = 1, \dots, p-1$. Since $\gcd(k, h) = 1$ and $\mathbb{F}_{\phi_0} \simeq \mathbb{F}_p$, then $\gcd(U(x), V(x)) = 1$. Therefore, the prime ideal factorization of $\mathfrak{a}\mathfrak{b}$ contains only prime ideals with residue degrees $f > 1$ satisfying $\mathcal{P}_f < \mathcal{N}_f$ for every positive integer f. By [11, Theorem 4], $\nu_p(i(K)) = p$. □

Acknowledgements. The author is deeply grateful to the anonymous referee for their valuable comments and suggestions, which have tremendously improved the quality of this paper, as well as for their prompt and efficient review. Also, he extends his sincere thanks to Professor Lhoussain El Fadil for his help and encouragement.

References

[1] COHEN, HENRI. A Course in Computational Algebraic Number Theory. *GTM 138, Springer-Verlag, Berlin, Heidelberg*, 1993. xii+534 pp. ISBN: 3-540-55640-0. MR1228206, Zbl 0786.11071. 1591

[2] DAVIS, CHAD T.; SPEARMAN, BLAIR K.. The index of a quartic field defined by a trinomial $x^4 + ax + b$. *J. Algebra Appl.* **17** (2018), no. 10, 185–197. MR3866770, Zbl 1437.11149, doi: 10.1142/S0219498818501979. 1586

[3] DEDEKIND, RICHARD. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Göttingen Abhandlungen* **23** (1878), 1–23. 1585

[4] EL FADIL, LHOUSSAIN. On the index divisors and monogenity of number fields defined $x^5 + ax^3 + b$. *Quaest. Math.* **46** (2023), no. 11, 2355–2365. MR4650431, doi: 10.2989/16073606.2022.2156000. 1586

[5] EL FADIL, LHOUSSAIN. On indices of septic number fields defined by trinomials x^7+ax+b. *Mathematics* **11** (2023), no. 21, 4441. arXiv:2202.09342, doi: 10.3390/math11214441. 1586

[6] EL FADIL, LHOUSSAIN; GAÁL, ISVÁN. On the monogenity of quartic number fields defined by $x^4 + ax^2 + b$. (2022). arXiv:2204.03226. 1586

[7] EL FADIL, LHOUSSAIN; KCHIT, OMAR. On index divisors and monogenity of certain sextic number fields defined by $x^6 + ax^5 + b$. *Vietnam J. Math.* (2024). arXiv:2206.05529, doi: 10.1007/s10013-023-00679-3. 1586

[8] EL FADIL, LHOUSSAIN; KCHIT, OMAR. On index divisors and monogenity of certain septic number fields defined by $x^7 + ax^3 + b$. *Commun. Algebra* **51** (2023), no. 6, 2349–2363. MR4563435, Zbl 1522.11108, doi: 10.1080/00927872.2022.2159035. 1586

[9] EL FADIL, LHOUSSAIN; KCHIT, OMAR. On index divisors and monogenity of certain number fields defined by $x^{12} + ax^m + b$. *Ramanujan J.* **63** (2024), no. 2, 451–482. MR4694516, arXiv:2211.04138, doi: 10.1007/s11139-023-00768-4. 1586

[10] EL FADIL, LHOUSSAIN; MONTES, JESÚS; NART, ENRIC. Newton polygons and p-integral bases of quartic number fields. *J. Algebra Appl.* **11** (2012), no. 4, 1250073. MR2959422, Zbl 1297.11134, arXiv:0906.2629, doi: 10.1142/S0219498812500739. 1591, 1592

[11] ENGSTROM; H. T. . On the common index divisor of an algebraic number field. *Trans. Amer. Math. Soc.* **32** (1930), 223–237. MR1501535, doi: 10.2307/1989492. 1593, 1594, 1595, 1596, 1597, 1598, 1599

[12] FUNAKURA, TAKEO. On integral bases of pure quartic fields. *Math J. Okayama Univ.* **26** (1984), 27–41. MR0779772, Zbl 0563.12003. 1586

[13] GAÁL, ISVÁN. Diophantine equations and power integral bases, Theory and algorithm. *Second edition, Boston, Birkhäuser*, 2019. xxii+326 pp. ISBN: 978-3-030-23864-3; 978-3-030-23867-4; 978-3-030-23865-0. MR3970246, Zbl 1465.11090.

[14] GAÁL, ISVÁN; ; PETHÖ, ATTILA; POHST, MICHAEL E.. On the indices of biquadratic number fields having Galois group V_4. *Arch. Math.* **57** (1991), no. 4, 357–361. MR1124498, Zbl 0724.11049, doi: 10.1007/BF01198960. 1586

[15] GAÁL, ISVÁN; ; PETHÖ, ATTILA; POHST, MICHAEL E.. On the resolution of index form equations in quartic number fields. *J. Symb. Comput.* **16** (1993), no. 6, 563–584. MR1279534, Zbl 0808.11023, doi: 10.1006/jsco.1993.1064.

[16] GUÀRDIA, JORDI; MONTES, JESÚS; NART, ENRIC. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.* **364** (2012), no. 1, 361–416. MR2833586, Zbl 1252.11091, arXiv:0807.2620, doi: 10.1090/S0002-9947-2011-05442-5. 1591

[17] GUÀRDIA, JORDI; NART, ENRIC. Genetics of polynomials over local fields. *Contemp. Math.* **637** (2015), 207–241. MR3364450, Zbl 1396.11143, arXiv:1309.4340, doi: 10.1090/conm/637/12767.

[18] HENSEL, KURT. Theorie der algebraischen Zahlen. *Teubner Verlag, Leipzig, Berlin*, 1908.

[19] KCHIT, OMAR. On the index divisors and monogenity of certain nonic number fields. *Rocky Mt. J. Math.* (2015), (To appear). arXiv:2307.03284. 1586

[20] KCHIT, OMAR. On the index of certain nonic number fields defined by $x^9 + ax^5 + b$. *P-Adic Num. Ultrametr. Anal. Appl.* **16** (2024), no. 2, 95–112. MR4745116, doi: 10.1134/S2070046624020018. 1586

[21] KCHIT, OMAR. On index divisors and non-monogenity of certain quintic number fields defined by x^5+ax^m+bx+c. *Commun. Algebra* **51** (2023), no. 8, 3172–3181. MR4585871, Zbl 1531.11103, doi: 10.1080/00927872.2023.2179633. 1586

[22] NAKAHARA, TORU. On the indices and integral bases of non-cyclic but abelian biquadratic fields. *Arch. Math.* **41** (1983), no. 6, 504–508. MR0731633, Zbl 0513.12005, doi: 10.1007/BF01198579. 1586

[23] NARKIEWICZ, WŁADYSŁAW. Elementary and analytic theory of algebraic numbers. *Springer Verlag, 3. Auflage, Berlin*, 2004. xii+708 pp. ISBN: 3-540-21902-1. MR2078267, Zbl 1159.11039. 1586

[24] NART, ENRIC. On the index of a number field. *Trans. Amer. Math. Soc.* **289** (1985), 171–183. MR0779058, Zbl 0563.12006. doi: 10.2307/1999694. 1586

[25] NEUKIRCH, JÜRGEN. Algebraic Number Theory. Transl. from the German by Norbert Schappacher. *Springer Verlag, Berlin*, 1999. xviii+571 pp. ISBN: 3-540-65399-6. MR1697859, Zbl 0956.11021. 1591

[26] ORE, ÖYSTEIN. Newtonsche Polygone in der Theorie der algebraischen Korper. *Math. Ann.* **99** (1928), 84–117. MR1512440, Zbl 54.0191.02. doi: 10.1007/BF01459087.

[27] PETHÖ, ATTILA; POHST, MICHAEL E.. On the indices of multiquadratic number fields. *Acta Arith.* **153** (2012), no. 4, 393–414. MR2925379, Zbl 1255.11052, doi: 10.4064/aa153-4-4. 1586

[28] ŚLIWA, JAN. On the nonessential discriminant divisor of an algebraic number field. *Acta Arith.* **42** (1982), 57–72. MR0678997, Zbl 0517.12005, doi: 10.4064/aa-42-1-57-72. 1586, 1593

[29] SPEARMAN, BLAIR K.; WILLIAMS, KENNETH S.. The index of a cyclic quartic field. *Monatsh. Math.* **140** (2003), no. 1, 519–70. MR2007140, Zbl 1049.11111, doi: 10.1007/s00605-002-0547-3. 1586

(Omar Kchit) GRADUATE NORMAL SCHOOL OF FEZ, SIDI MOHAMED BEN ABDELLAH UNIVERSITY, MOROCCO
omar.kchit@usmba.ac.ma

This paper is available via http://nyjm.albany.edu/j/2024/30-67.html.