Nonmonogenity of number fields defined by trinomials

Anuj Jakhar

Abstract. Let \( f(x) = x^n - ax^m - b \) be a monic irreducible polynomial of degree \( n \) having integer coefficients. Let \( K = \mathbb{Q}(\vartheta) \) be an algebraic number field with \( \vartheta \) a root of \( f(x) \). In this paper, we provide some explicit conditions involving only \( a, b, m, n \) for which \( K \) is not monogenic. Further, as an application, in a special case, we show that if \( p \) is a prime number of the form \( 32k + 1, k \in \mathbb{Z} \) and \( \vartheta \) is a root of a monic polynomial \( x^{32n} - 64ax^m - p \) with \( 2 \nmid n, p \mid a \), then \( \mathbb{Q}(\vartheta) \) is not monogenic.

1. Introduction and statement of the result

For a given algebraic number field \( K \), it is a classical problem in Algebraic Number Theory whether \( K \) is monogenic or not. There are many results in the literature for testing the monogenity of number fields using different approaches (cf. [1], [3], [5], [6], [7], [8], [9], [12], [16], [2]). Let \( \mathbb{Z}_K \) denote the ring of algebraic integers of an algebraic number field \( K = \mathbb{Q}(\vartheta) \) where \( \vartheta \) is a root of a monic irreducible polynomial \( f(x) \) of degree \( n \) having coefficients from the ring \( \mathbb{Z} \) of integers. It is well-known that \( \mathbb{Z}_K \) is a free abelian group of rank \( n \). Let \( \text{ind} \vartheta \) denote the index of the subgroup \( \mathbb{Z}[\vartheta] \) in \( \mathbb{Z}_K \). The index \( i(K) \) of the field \( K \) is defined as

\[
  i(K) = \gcd\{\text{ind} \alpha \mid \alpha \in \mathbb{Z}_K \text{ generates the field extension } K/\mathbb{Q}\}.
\]

A prime number \( p \) dividing \( i(K) \) is called a prime common index divisor of \( K \). A number field \( K \) is called monogenic if there exists an element \( \alpha \in \mathbb{Z}_K \) such that \( \{1, \alpha, \ldots, \alpha^{n-1}\} \) is an integral basis of \( K \); if no such \( \alpha \) exists, then we say that \( K \) is not monogenic. In 2016, Ahmad, Nakahara, and Husnine [1] proved that
the sextic number field generated by \( b^{1/6} \) is not monogenic if \( b \equiv 1 \mod 4 \) and \( b \not\equiv \pm 1 \mod 9 \). In 2017, Gaál and Remete \([9]\) provided some new results on monogenicity of number fields generated by \( b^{1/6} \) with \( b \) a square free integer and \( 3 \leq n \leq 9 \) by applying the explicit form of the index equation. In 2021, Yakkou and Fadil \([2]\) studied the monogenity of number fields generated by \( b^{1/6} \), where \( b \) is a square free integer and \( q \) be a prime number. In this paper, using the splitting of primes in \( \mathbb{Z}_K \), we prove some results regarding the non-monogenity of a number field \( K \) defined by an irreducible trinomial of the type \( x^n - ax^m - b \) having integer coefficients. As an application of our results, we provide a class of non-monogenic number fields defined by irreducible trinomials (see Example 1.3).

For a prime number \( q \) and a non-zero \( a \) belonging to the ring \( \mathbb{Z}_q \) of \( q \)-adic integers, \( \nu_q(a) \) will be the highest power of \( q \) dividing \( a \) and \( \nu_q(a) = \infty \) when \( a = 0 \). Let \( \mathbb{F}_q \) denote the field with \( q \) elements and \( N(q, \ell) \) denote the number of irreducible polynomials of degree \( \ell \) over \( \mathbb{F}_q \). It is well known that

\[
N(q, \ell) = \frac{1}{\ell} \sum_{k|\ell} \mu(k)q^{\frac{k}{\ell}},
\]

where \( \mu \) is the Möbius function. Observe that

\[
N(q, 1) = q, \quad N(q, 2) = \frac{q(q - 1)}{2}, \quad N(q, 3) = \frac{q(q^2 - 1)}{3}.
\]

We now state our main result.

**Theorem 1.1.** Let \( K = \mathbb{Q}(\theta) \) be an algebraic number field with \( \theta \) a root of a monic irreducible polynomial \( f(x) = x^n - ax^m - b \) of degree \( n \) having integer coefficients. Let \( q \) be a prime factor of \( n \) with \( n = q^r u \), \( q \nmid u \). Assume that \( q^{r+1} \) divides \( a \) and \( q \nmid b \). Suppose \( \phi(x) \) is a monic irreducible factor of degree \( \ell \) of the polynomial \( x^u - b \) over \( \mathbb{F}_q \) and \( N(q, \ell) \) is as above. If \( r_1 \) stands for the integer \( \nu_q(b^{q^{r-1}} - 1) \), then in the following cases \( q \) divides \( i(K) \).

1. \( q \neq 2 \) and \( N(q, \ell) < r_1 \leq r \).
2. \( q = 2 \) and \( N(2, \ell) + 2 < r_1 \leq r \).
3. \( N(q, \ell) + 1 < r < r_1 \).

In the special case when \( \ell = 1 \), the following corollary is an immediate consequence of the above theorem.

**Corollary 1.2.** Let \( K = \mathbb{Q}(\theta) \), \( f(x) = x^n - ax^m - b \), \( r \) and \( r_1 \) be as in Theorem 1.1. If \( q^{r+1} \) divides \( a \), \( b \equiv 1 \mod q \) and \( \min\{r, r_1\} > q + 2 \), then \( K \) is not monogenic.

It may be pointed out that if we have \( b = 1 \) in the above corollary, then \( K \) is not monogenic for \( r > q + 2 \).

As an application, we provide a class of non-monogenic number fields defined by irreducible trinomials.
2. **Preliminary Results**

Let $K = Q(\theta)$ be an algebraic number field with $\theta$ a root of an irreducible polynomial $f(x)$ having integer coefficients and $Z_K$ denote the ring of algebraic integers of $K$. Let $q$ be a prime number. If $q$ does not divide $\text{ind} \theta$, then Dedekind [4] proved a significant theorem in 1878 which relates the decomposition of $f(x)$ modulo $q$ with the factorization of $qZ_K$ into a product of prime ideals of $Z_K$. Precisely, he proved the following.

**Dedekind Theorem.** Let $K = Q(\theta)$ be an algebraic number field of degree $n$ with $\theta$ an algebraic integer. Let $f(x)$ be the minimal polynomial of $\theta$ over $Q$ and $q$ be a rational prime not dividing $\text{ind} \theta$. Let $f(x) = g_1(x)^{e_1} \cdots g_t(x)^{e_t}$ be the factorization of $f(x)$ into powers of distinct irreducible polynomials over $Z/qZ$, where each $g_i(x) \in Z[x]$ is monic. Then $\mathfrak{p}_i = \langle g_i(\theta), q \rangle$ for $1 \leq i \leq t$ are distinct prime ideals of $Z_K$ and $qZ_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$, moreover the norm of $\mathfrak{p}_i$ is $q^{\deg g_i(x)}$ for $1 \leq i \leq t$.

The following lemma is an immediate consequence of Dedekind’s theorem. It plays a key role in the proof of Theorem 1.1. We shall denote by $F_q$ the field with $q$ elements.

**Lemma 2.1.** Let $K$ be a number field and $q$ be a prime number. For every positive integer $f$, let $N(q, f)$ denote the number of irreducible polynomials of $F_q[x]$ of degree $f$ and $P(q, f)$ denote the number of distinct prime ideals of $Z_K$ lying above $q$ having residual degree $f$. If $P(q, f) > N(q, f)$ for some $f$, then for every algebraic integer $\alpha$ generating the field extension $K/Q$, the prime $q$ divides $\text{ind} \alpha$.

When Dedekind’s theorem fails, i.e., $q$ divides $i(K)$, then Ore developed an alternative approach in 1928 for obtaining the prime ideal factorization of the rational primes in a number field $K$ by using Newton polygons (cf. [14], [15]).

We now introduce the notion of Gauss valuation which is required for defining the $\phi$-Newton polygon of a polynomial, where $\phi(x)$ belonging to $Z_q[x]$ is a monic polynomial with $\phi(x)$ irreducible over $F_q$.

We shall denote by $v_{q,x}$ the Gauss valuation of the field $Q_q(x)$ of rational functions in an indeterminate $x$ which extends the valuation $v_q$ of $Q_q$ and is defined on $Q_q[x]$ by

$$v_{q,x}(\sum_i b_i x^i) = \min_i \{v_q(b_i)\}, b_i \in Q_q. \quad (2.1)$$

---

1It is known that there exists infinitely many primes of the form $32k + 1, k \in Z$. 

---
Now we define the notion of $\phi$-Newton polygon with respect to some prime $q$.

**Definition 2.2.** Let $q$ be a prime number and $\phi(x) \in \mathbb{Z}_q[x]$ be a monic polynomial which is irreducible modulo $q$. Let $f(x) \in \mathbb{Z}_q[x]$ be a monic polynomial not divisible by $\phi(x)$ with $\phi$-expansion $\sum_{i=0}^{n} a_i(x) \phi(x)^i$, $\deg a_i(x) < \deg \phi(x)$, $a_n(x) \neq 0$ which is obtained on dividing $f(x)$ by successive powers of $\phi(x)$. To each non-zero term $a_k(x) \phi(x)^k$, we associate the point $(n-k, v_{q,x}(a_k(x)))$ and form the set

$$P = \{(k, v_{q,x}(a_{n-k}(x))) \mid 0 \leq k \leq n, a_{n-k}(x) \neq 0\}.$$  

The $\phi$-Newton polygon of $f(x)$ with respect to $q$ is the polygonal path formed by the lower edges along the convex hull of the points of $P$. The slopes of the edges are increasing when calculated from left to right. The principal $\phi$-Newton polygon of $f(x)$ with respect to $q$ is the part of the $\phi$-Newton polygon of $f(x)$, which is determined by joining all edges of positive slopes.

**Example 2.3.** Let $f(x) = (x + 5)^4 - 5$. Here take $\phi(x) = x$. Then the $x$-Newton polygon of $f(x)$ with respect to prime 2 consists of only one edge joining the points $(0,0)$ and $(4,2)$ with the lattice point $(2,1)$ lying on it (see Figure 1).

![Figure 1. x-Newton polygon of f(x) with respect to prime 2](image)

**Definition 2.4.** Let $q$ be a prime number and $\phi(x) \in \mathbb{Z}_q[x]$ be a monic polynomial which is irreducible modulo $q$ having a root $\alpha$ in the algebraic closure $\overline{\mathbb{Q}}_q$ of $\mathbb{Q}_q$. Let $f(x) \in \mathbb{Z}_q[x]$ be a monic polynomial not divisible by $\phi(x)$ with $\phi$-expansion $\phi(x)^n + a_{n-1}(x) \phi(x)^{n-1} + \cdots + a_0(x)$. Suppose that the $\phi$-Newton polygon of $f(x)$ with respect to $q$ consists of a single edge, say $S$ having positive slope denoted by $\frac{d}{e}$ with $d, e$ coprime, i.e.,

$$\min \left\{ \frac{v_{q,x}(a_{n-i}(x))}{i} \mid 1 \leq i \leq n \right\} = \frac{v_{q,x}(a_0(x))}{n} = \frac{d}{e}$$

so that $n$ is divisible by $e$, say $n = et$ and $v_{q,x}(a_{n-ej}(x)) \geq dj$ for $1 \leq j \leq t$.

Thus the polynomial $\frac{a_{n-ej}(x)}{q^{dj}} = b_j(x)$ (say) has coefficients in $\mathbb{Z}_q$ and hence
$b_j(\alpha) \in \mathbb{Z}_q[\alpha]$ for $1 \leq j \leq t$. The polynomial $T(y)$ in an indeterminate $y$ defined by $T(y) = y^t + \sum_{j=1}^t b_j(\alpha)y^{t-j}$ having coefficients in $\mathbb{F}_q[\alpha]$ is said to be the polynomial associated to $f(x)$ with respect to $(\phi,S)$; here the field $\mathbb{F}_q[\alpha]$ is isomorphic to the field $\mathbb{F}_q[\alpha]/(\phi(x))$.

**Example 2.5.** Consider $f(x) = (x + 5)^d - 5$. Then, as in Example 2.3, the $x$-Newton polygon of $f(x)$ with respect to prime $2$ consists of only one edge joining the points $(0,0)$ and $(4,2)$ with the lattice point $(2,1)$ lying on it. With notations as in the above definition, we see that $e = 2$, $d = 1$ and the polynomial associated to $f(x)$ with respect to $(x,S)$ is $T(y) = y^2 + y + 1$ belonging to $\mathbb{F}_2[y]$.

We now state a weaker version of Theorem 1.2 of [13].

**Theorem 2.6.** Let $L = \mathbb{Q}(\eta)$ be an algebraic number field with $\eta$ satisfying a monic irreducible polynomial $g(x) \in \mathbb{Z}[x]$ and $q$ be a prime number. Let $\phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r}$ be the factorization of $g(x)$ modulo $q$ into a product of powers of distinct irreducible polynomials over $\mathbb{F}_q$ with each $\phi_i(x) \neq g(x)$ belonging to $\mathbb{Z}[x]$ monic. Assume that, for a fixed $i$, the $\phi_i$-Newton polygon of $g(x)$ has $k$ edges, say $S_j$ having positive slopes $\lambda_j = \frac{d_j}{e_j}$ with $\gcd(d_j,e_j) = 1$ for $1 \leq j \leq k$.

If the polynomial $T_j(y)$ associated to $f(x)$ with respect to $(\phi_i,S_j)$ is linear for $k_1$ edges with $1 \leq j \leq k_1 \leq k$, then there are at least $k_1$ distinct prime ideals of $\mathbb{Z}_L$ having residual degree $\deg \phi_i(x)$.

In [10], Guàrdia, Montes, and Nart introduced the notion of $\phi$-admissible expansion, which is used in order to treat some special cases when the $\phi$-expansion of a polynomial $g(x)$ is not obvious.

Let $q$ be a prime number and $f(x) \in \mathbb{Z}_q[x]$ be a monic polynomial not divisible by $\phi(x)$ with $\phi(x)$-development $\sum_{j=0}^n a'_j(x)\phi(x)^j, \ a'_j(x) \in \mathbb{Z}_q[x]$; here $\deg a'_j(x)$ can be greater than or equal to $\deg \phi(x)$. Analogous to the definition of $\phi$-Newton polygon of $f(x)$ with respect to $q$, to each non-zero term $a'_k(x)\phi(x)^k$, we associate the point $(n-k, v_{q,x}(a'_k(x)))$ and the polygonal path formed by the lower edges along the convex hull of the points of $\{(k, v_{q,x}(a'_{n-k}(x))) \ | \ 0 \leq k \leq n, a'_{n-k}(x) \neq 0\}$ defines the $\phi$-development Newton polygon of $f(x)$ with respect to $q$ in this case. Now as in Definition 2.4, suppose that the $\phi$-development Newton polygon of $f(x)$ with respect to $q$ consists of a single edge, say $S'$ having positive slope denoted by $\frac{d}{e}$ with $d, e$ coprime, i.e.,

$$\min\left\{\frac{v_{q,x}(a'_{n-i}(x))}{i} \mid 1 \leq i \leq n\right\} = \frac{v_{q,x}(a'_0(x))}{n} = \frac{d}{e}.$$
so that $n$ is divisible by $e$, say $n = et$ and $\nu_q(x(a'_{n-ej}(x))) \geq dj$ for $1 \leq j \leq t$.

Let $\frac{a'_{n-ej}(x)}{q^dj}$ is denoted by $b'_j(x)$. We define the polynomial $T'(y)$ in an indeterminate $y$ by $T'(y) = y^t + \sum_{j=1}^{t} b'_j(x)y^{t-j}$ having coefficients in $\left(\frac{\mathbb{F}_q[x]}{(\varphi(x))}\right)(\cong \mathbb{F}_q[\varphi])$.

$T'(y)$ is said to be the polynomial associated to $f(x)$ with respect to $(\varphi, S')$. We say that a $\varphi$-development of $f(x)$ is called admissible with respect to $(\varphi, S')$ if and only if $\varphi$ does not divide $b'_j(x)$ for each $j$. If the $\varphi$-development Newton polygon of a polynomial $f(x)$ has $\ell$ many edges $S_i$ having positive slopes, then $\varphi$-development of $f(x)$ is called admissible when $\varphi$-development of $f(x)$ is admissible with respect to $(\varphi, S_i)$ for each $i$, $1 \leq i \leq \ell$. It is proved in [10] that if a $\varphi$-development of $f(x)$ is admissible, then the principal $\varphi$-Newton polygon of $f(x)$ with respect to $q$ will be the same as $\varphi$-development Newton polygon of $f(x)$ with respect to prime $q$ for edges having positive slopes; in particular, for any edge $S$ having positive slope of the $\varphi$-Newton polygon of $f(x)$, we have $T(y) = T'(y)$.

3. PROOF OF THEOREM 1.1

Proof of Theorem 1.1. Keeping in mind that $q^r - 1 = (q - 1)m$ with $m \equiv 1 \mod q$ and $b^{q-1} \equiv 1 \mod q$, one can quickly verify that $\nu_q(b^{q-1} - 1) = \nu_q(b^{q-1} - 1) = r_1$.

Since $q | a$ and $q \nmid b$, we have $f(x) \equiv x^n - b \mod q$. Using Fermat’s little theorem and the fact that $n = q^ru$, $q \nmid u$, it follows that $f(x) \equiv (x^u - b)^q \mod q$. Since $q$ does not divide $ab$, the monic irreducible polynomial $x^u - b$ is separable in $\mathbb{F}_q[x]$. Let $\phi_1(x) \cdots \phi_t(x)$ be the factorization of $x^u - b$ into a product of monic irreducible polynomials in $\mathbb{F}_q[x]$, then $f(x) \equiv (\phi_1(x) \cdots \phi_t(x))^q \mod q$. Now we fix an irreducible factor $\hat{\varphi}(x) = \hat{\varphi}(x)$ of the polynomial $\hat{f}(x)$ in $\mathbb{F}_q[x]$. Write $x^u - b = \phi_1(x) \cdots \phi_t(x) + q^{k_1}h_1(x) = \phi(x)g_1(x) + q^{k_1}h_1(x)$, where $g_1(x) = \prod_{j=1}^{t} \phi_j(x), h_1(x) \in \mathbb{Z}[x]$ and $k_1 \geq 1$ is an integer such that $\hat{h}_1(x) \neq 0$. Note that $\hat{\varphi}(x) \nmid \hat{g}_1(x)$. Now we observe that there exists $g(x)$ and $\hat{h}(x)$ such that $\hat{\varphi}(x) \nmid \hat{g}(x)\hat{h}(x)$ and $x^u - b = \phi(x)g(x) + q^kh(x)$ for some $k \geq 1$. Because if $\hat{\varphi}(x)$ divides $\hat{h}_1(x)$, we can write $\hat{h}_1(x) = \hat{\varphi}(x)^r \hat{g}_2(x)$ such that $e \geq 1$ and $\hat{\varphi}(x) \nmid \hat{g}_2(x)$. So we have $h_1(x) = \phi(x)^r g_2(x) + q^k h_2(x)$ and $k_2$ is a positive integer such that $\hat{h}_2(x) \neq 0$. If $\hat{\varphi}(x) \nmid \hat{h}_2(x)$, then we set $g(x) = \hat{g}_1(x) + q^k \phi(x)^{r-1} g_2(x)$ and $h(x) = h_2(x)$ with $k = k_1 + k_2$. If $\hat{\varphi}(x)$ divides $\hat{h}_2(x)$, then we can repeat this process. Therefore, let $g(x), h(x) \in \mathbb{Z}[x]$ be such that

$$x^u - b = \phi(x)g(x) + q^kh(x) \text{ with } k \geq 1, \hat{\varphi}(x) \nmid \hat{g}(x)\hat{h}(x). \quad (3.1)$$

Applying the binomial theorem, we see that

$$f(x) = (x^u - b + b)^q - ax^m - b = (\phi(x)g(x) + q^kh(x) + b)^q - ax^m - b$$
can be written as
\[ f(x) = \sum_{j=0}^{q^r-2} \left( \binom{q^r}{j} b^j g(x) \phi(x)^j \right) + (q^r h(x) + b) q^{r-1} \phi(x)^j - ax^m - b. \]

Let \( d(x) \in \mathbb{Z}[x] \) be a polynomial such that
\[ (q^r h(x) + b) q^{r-1} - b q^r = q^{r+k} d(x). \]
Then
\[ d(x) = b q^{r-1} h(x) + \frac{1}{q^{r+k}} \sum_{j=0}^{q^r-2} \binom{q^r}{j} b^j (q^r h(x)) q^{r-j}. \]
It follows that
\[ f(x) = (\phi(x) g(x))^q \]
\[ + \sum_{j=1}^{q^r-1} \binom{q^r}{j} (q^r h(x) + b) q^{r-j} g(x) \phi(x)^j + q^{r+k} d(x) - ax^m + b q^r - b. \]
Thus \( f(x) = \sum_{j=0}^{q^r-1} a'_j(x) \phi(x)^j \) is the \( \phi \)-development of \( f(x) \), where
\[ a'_0(x) = q^{r+k} d(x) - ax^m + b q^r - b. \]
\[ a'_j(x) = \sum_{j=1}^{q^r} \binom{q^r}{j} (q^r h(x) + b) q^{r-j} g(x)^j. \]

Note that
\[ v_{q,x}(\binom{q^r}{j}) (q^r h(x) + b) q^{r-j} g(x)^j = v_{q,j}(\binom{q^r}{j}) \]
for every \( j = 1, 2, \ldots, q^r \). (3.3)

We now divide our proof into two cases.

**Case (1).** Suppose \( r_1 \leq r \). Keeping in mind that \( q^{r+1} \) divides \( a \), one can easily verify that the successive vertices of the \( \phi \)-development Newton polygon of \( f(x) \) with respect to an odd prime \( q \) is given by the set \( \{(0, 0), (q^r - q^{r-1}, 1), \ldots, (q^r - q^{r-r_1+1}, r_1 - 1), (q^r, r_1)\} \) having \( r_1 \) edges \( S'_i \) with slopes \( \lambda_i = \frac{1}{q^{r-i+1} - q^{r-i}} \) for \( 1 \leq i \leq r_1 - 1 \) and \( \lambda_{r_1} = \frac{1}{q^{r-r_1+1}} \). Since \( q \nmid b \) and \( \phi(x) \nmid g(x) \bar{h}(x) \), one can see that the \( \phi \)-development of \( f(x) \) is admissible with respect to \((\phi, S'_i)\) for each \( i \), and hence \( \phi \)-development of \( f(x) \) is admissible. Further, the polynomial associated to \( f(x) \) with respect to \((\phi, S'_i)\) is linear for \( 1 \leq i \leq r_1 \). Therefore, the \( \phi \)-Newton polygon of \( f(x) \) has \( r_1 \) edges and the polynomials associated to \( f(x) \) with respect to these edges are linear. Hence by Theorem 2.6, there are at least \( r_1 \) distinct prime ideals of \( \mathbb{Z}_K \) lying above \( q \) having residual degree \( \deg \phi(x) = \ell \). It is known [11] that the number of monic irreducible polynomials of degree \( \ell \) over \( \mathbb{F}_q \) are \( N(q, \ell) \). Therefore, if \( r_1 > N(q, \ell) \), then applying Lemma 2.1 it follows that \( q \) divides \( i(K) \). We now consider the situation when \( q = 2 \). In this situation, the successive vertices of the \( \phi \)-development Newton polygon of \( f(x) \) with respect
to 2 is given by the set \{0, (2^r - 2^-1, 1), \ldots, (2^r - 2^-1 + 1, r_1 - 2), (2^r, r_1)\} having \(r_1 - 1\) edges \(S'_1\) with slopes \(\lambda_i = \frac{1}{2^{r_i+1} - 2^{r_i}}\) for \(1 \leq i \leq r_1 - 2\) and \(\lambda_{r_1-1} = \frac{1}{2^{r_1+1}}\). The polynomial associated to \(f(x)\) with respect to \((\phi, S'_1)\) is linear for \(1 \leq i \leq r_1 - 2\) and the polynomial associated to \(f(x)\) with respect to \((\phi, S'_{r_1-1})\) is a second degree irreducible polynomial \(y^2 + y + 1\) over \(\mathbb{F}_2\). Since \(q \not| b\) and \(\phi(x) \not| g(x)\bar{h}(x)\), \(\phi\)-development of \(f(x)\) is admissible. Hence, the \(\phi\)-Newton polygon of \(f(x)\) has \(r_1 - 2\) edges such that the polynomials associated to \(f(x)\) with respect to these edges are linear. Therefore, by Theorem 2.6, there are at least \(r_1 - 2\) distinct prime ideals of \(\mathcal{O}_K\) lying above 2 having residual degree \(\ell\). So, if \(r_1 - 2 > N(2, \ell)\), then applying Lemma 2.1 it follows that \(2\) divides \(i(K)\).

**Case (2).** Suppose \(r_1 > r\). Keeping in mind that \(q^{r+1}\) divides \(a\), one can easily verify that the successive vertices of the \(\phi\)-development Newton polygon of \(f(x)\) with respect to an odd prime \(q\) are given by the set \{(0, 0), (q^r - q^{-1}, 1), \ldots, (q^r - q, r - 1), (q^r - 1, r), (q^r, z)\} having \(r + 1\) edges \(S'_1\) with \(z \geq r + 1\) and slopes \(\lambda_i = \frac{1}{q^{r+1} - q^{-r}}\) for \(1 \leq i \leq r\), \(\lambda_{r+1} = z - r\). Also, if \(v_q(x)(a'_q(x)) = r + 1\), then the successive vertices of the \(\phi\)-development Newton polygon of \(f(x)\) with respect to 2 is given by the set \{(0, 0), (2^r - 2^{r-1}, 1), \ldots, (2^r - 2, r - 1), (2^r, r + 1)\} having \(r\) edges \(S'_1\) with slopes \(\lambda_i = \frac{1}{2^{r+1} - 2^{r-1}}\) for \(1 \leq i \leq r - 1\) and \(\lambda_r = 1\). Arguing exactly as in the above case, we see that there are at least \(r - 1\) distinct prime ideals of \(\mathcal{O}_K\) lying above \(q\) having residual degree \(\ell\). So, if \(r - 1 > N(q, \ell)\), then applying Lemma 2.1 we see that \(q\) divides \(i(K)\). This completes the proof of the theorem. 

**Acknowledgement.** The author is grateful to the anonymous referee for the detailed report which has substantially improved the readability of the paper.

**References**


(Anuj Jakhar) DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY (IIT) BHILAI, CHHATTISGARH 492015, INDIA

anujjakhar@iitbhilai.ac.in; anujiisermohali@gmail.com

This paper is available via http://nyjm.albany.edu/j/2022/28-26.html.