Proceedings of the Edinburgh Mathematical Society (2024) **67**, 528–541
doi:10.1017/S0013091524000105

DISCRIMINANT AND INTEGRAL BASIS OF NUMBER FIELDS DEFINED BY EXPONENTIAL TAYLOR POLYNOMIALS

ANKITA JINDAL[1] AND SUDESH K. KHANDUJA[3,2]

[1] *Stat-Math Unit, Indian Statistical Institute Bangalore Centre, Bangalore, India*
(ankitajindal1203@gmail.com)
[2] *Department of Mathematical Sciences, Indian Institute of Science Education and Research Mohali, SAS Nagar, India* (skhanduja@iisermohali.ac.in)
[3] *Department of Mathematics, Panjab University, Chandigarh, India*

Dedicated to the memory of Peter Roquette.

(Received 21 September 2023)

Abstract Let $K_n = \mathbb{Q}(\alpha_n)$ be a family of algebraic number fields where $\alpha_n \in \mathbb{C}$ is a root of the nth exponential Taylor polynomial $\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + \frac{x^2}{2!} + \frac{x}{1!} + 1$, $n \in \mathbb{N}$. In this paper, we give a formula for the exact power of any prime p dividing the discriminant of K_n in terms of the p-adic expansion of n. An explicit p-integral basis of K_n is also given for each prime p. These p-integral bases quickly lead to the construction of an integral basis of K_n.

Keywords: discriminant; integral basis; p-integral basis

2020 Mathematics subject classification: 11R04; 11R29

1. Introduction and statements of results

The discriminant is a basic invariant associated with an algebraic number field. Its notion was first introduced by Dedekind in 1871. The problem of effective computation of discriminant as well as an integral basis of an infinite family of algebraic number fields which are defined over the field $\mathbb{Q}$ of rational numbers by certain types of irreducible polynomials has been tackled by several mathematicians (cf. [1, 2, 7, 10, 15, 17, 21]). In this paper, we deal with the above problem for the family of exponential Taylor polynomials:

$$T_n(x) = \frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + \frac{x^2}{2!} + \frac{x}{1!} + 1,$$

whose irreducibility over $\mathbb{Q}$ was proved by Schur in 1929 for $n \geq 1$ (see [6, 19, 20]). Let K_n denote the algebraic number field $\mathbb{Q}(\alpha_n)$, where $\alpha_n \in \mathbb{C}$ is a root of $T_n(x)$. In this paper, we calculate the discriminant of the field K_n and explicitly construct a p-integral

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

basis (defined below) of K_n for each prime number p and $n \geq 1$. These p-integral bases quickly lead to the construction of an integral basis of K_n as illustrated in Example 5.2. Our proofs are theoretical without involving computer programming and we use several well-known basic results of algebraic number theory besides the Theorem of Index of Ore.

We first introduce some notations. For an algebraic number field K, A_K will stand for its ring of algebraic integers and d_K for its discriminant. If $K = \mathbb{Q}(\theta)$ with θ an algebraic integer having minimal polynomial $f(x)$ over $\mathbb{Q}$, then the group index $[A_K : \mathbb{Z}[\theta]]$ will be denoted by ind θ and the discriminant of the polynomial $f(x)$ by $discr(f)$. For a prime number p, by $\mathbb{Z}_{(p)}$ we shall denote the localisation of the ring $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. If $I_{(p)}$ stands for the integral closure of the ring $\mathbb{Z}_{(p)}$ in an algebraic number field K, then $I_{(p)} = \{\frac{\alpha}{a} \mid \alpha \in A_K,\ a \in \mathbb{Z} \setminus p\mathbb{Z}\ \}$ is a free $\mathbb{Z}_{(p)}$-module of rank equal to the degree of the extension $K/\mathbb{Q}$. A basis of $I_{(p)}$ as a $\mathbb{Z}_{(p)}$-module is called a p-integral basis of K. Note that if $K = \mathbb{Q}(\theta)$ with θ in A_K and p is a prime number not dividing ind θ, then by Lagrange's theorem for finite groups, $A_K \subseteq \mathbb{Z}_{(p)}[\theta]$ and hence $I_{(p)} = \mathbb{Z}_{(p)}[\theta]$, i.e., $\{1,\theta,\dots,\theta^{n-1}\}$ is a p-integral basis of K, n being the degree of the extension $K/\mathbb{Q}$. Throughout v_p will stand for the p-adic valuation of $\mathbb{Q}$ defined for any non-zero integer m to be the highest power of the prime p dividing m. For a real number λ, we shall denote by $\lfloor \lambda \rfloor$ the largest integer not exceeding λ.

With the above notations, we prove

Theorem 1.1. *Let p be a prime number and let $n \geq 2$ be an integer having p-adic expansion:*

$$n = c_1 p^{m_1} + c_2 p^{m_2} + \cdots + c_s p^{m_s},$$

with $0 \leq m_1 < m_2 < \cdots < m_s$ and $0 < c_i < p$ for each i. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ a root of the irreducible polynomial $f_n(x) = x^n + \frac{n!}{(n-1)!}x^{n-1} + \cdots + \frac{n!}{2!}x^2 + \frac{n!}{1!}x + n!$ belonging to $\mathbb{Z}[x]$. Let d_K stand for the discriminant of K and d_i for the integer $\frac{p^{m_i}-1}{p-1}$. Then $v_p(\text{ind}\ \theta)$ and $v_p(d_K)$ are given by:

$$v_p(\text{ind}\ \theta) = \frac{1}{2}\sum_{i=1}^{s}[c_i d_i\,(c_i p^{m_i} + 2c_{i+1}p^{m_{i+1}} + \cdots + 2c_s p^{m_s} - p)], \tag{1}$$

$$v_p(d_K) = p\sum_{i=1}^{s} c_i d_i + \sum_{1 \leqslant i < j \leqslant s} \frac{c_i c_j (p^{m_j} - p^{m_i})}{p-1}. \tag{2}$$

The following corollaries will be quickly deduced from the above theorem.

Corollary 1.2. *Let n and $K = \mathbb{Q}(\theta)$ be as in the above theorem. Then a prime number p divides $[A_K : \mathbb{Z}[\theta]]$ if and only if p^2 divides $n!$. In particular, $A_K = \mathbb{Z}[\theta]$ if and only if n is 2 or 3.*

Corollary 1.3. *With notations as in the above corollary, a prime number p divides d_K if and only if p divides $n!$.*

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

Recall that for a non-zero polynomial $g(x) = \sum\limits_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$, the Newton polygon of $g(x)$ with respect to a prime number p is the polygonal path along the lower convex hull of the points in the set $\{(i, v_p(a_{n-i})) \mid 0 \leq i \leq n,\ a_{n-i} \neq 0\}$ (see Definition 2.1).

Theorem 1.4. *Let $K = \mathbb{Q}(\theta)$ and $f_n(x)$ be as in Theorem 1.1 and let p be a prime number. For any integer j with $1 \leq j \leq n-1$, let $u_j(x)$ denote the polynomial $x^j + \frac{n!}{(n-1)!}x^{j-1} + \cdots + \frac{n!}{(n-j)!}$ with coefficients in $\mathbb{Z}$. Then a p-integral basis of K is given by $\{1, \beta_1, \cdots, \beta_{n-1}\}$ with $\beta_j = \frac{u_j(\theta)}{p^{\lfloor y_j \rfloor}}$ for $1 \leq j \leq n-1$, where y_j stands for the ordinate of the point with abscissa j on the Newton polygon of $f_n(x)$ with respect to the prime p.*

The following theorem proved in [10, Theorem 1.2] gives a method to construct an integral basis of an algebraic number field using its p-integral bases.

Theorem 1.A. *Let $L = \mathbb{Q}(\xi)$ be an algebraic number field of degree n with ξ an algebraic integer. Let $p_1, \ldots, p_s$ be all the prime numbers dividing* ind *ξ and $\{1, \alpha_{r1}, \ldots, \alpha_{r(n-1)}\}$ be a p_r-integral basis of L, $1 \leq r \leq s$ with:*

$$\alpha_{ri} = \frac{c_{i0}^{(r)} + c_{i1}^{(r)}\xi + \cdots + c_{i(i-1)}^{(r)}\xi^{i-1} + \xi^i}{p_r^{k_{i,r}}}, \quad 1 \leq i \leq n-1,$$

where $c_{ij}^{(r)}$ and $0 \leq k_{i,r} \leq k_{i+1,r}$ are integers. If $c_{ij} \in \mathbb{Z}$ are such that $c_{ij} \equiv c_{ij}^{(r)}$ $(\bmod\ p_r^{k_{i,r}})$ for $1 \leq r \leq s$ and if t_i stands for $\prod\limits_{r=1}^{s} p_r^{k_{i,r}}$, then $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ is an integral basis of L where

$$\alpha_i = \frac{c_{i0} + c_{i1}\xi + \cdots + c_{i(i-1)}\xi^{i-1} + \xi^i}{t_i}, \quad 1 \leq i \leq n-1.$$

It may be pointed out that for any algebraic number field $L = \mathbb{Q}(\xi)$, a p-integral basis of the type given in the above theorem always exists for each prime p in view of [11, Theorem 2.34]. We shall illustrate Theorems 1.4 and Theorem 1.A by constructing an explicit integral basis of $K = \mathbb{Q}(\theta)$ when θ is a root of $f_6(x)$ or $f_7(x)$ in Example 5.2.

2. Preliminary results

The following lemma is essentially proved in [6, p. 187]. For reader's convenience, we prove it here.

Lemma 2.A. *Let $n \geq 2$ be an integer. Then the discriminant of the polynomial $f_n(x) = x^n + \frac{n!}{(n-1)!}x^{n-1} + \cdots + \frac{n!}{2!}x^2 + \frac{n!}{1!}x + n!$ is $(-1)^{\frac{n(n-1)}{2}}(n!)^n$.*

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

Proof. It can be easily seen that:

$$f_n^{'}(x) = nf_{n-1}(x), \quad f_n(x) = x^n + nf_{n-1}(x). \tag{3}$$

Let $\beta_1, \beta_2, \ldots, \beta_n$ be the roots of $f_n(x)$ in $\mathbb{C}$. Then the discriminant of $f_n(x)$ is given by:

$$discr(f_n) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} f_n^{'}(\beta_j).$$

Therefore using (3), we see that:

$$discr(f_n) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} (nf_{n-1}(\beta_j)) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} \left(-\beta_j^n\right) = (-1)^{\frac{n(n-1)}{2}} (n!)^n.$$

□

The following simple result is well known (see [3, p. 122], [6]). Its proof is omitted.

Lemma 2.B. *Let p be a prime number and m be a positive integer. If $m = a_0 + a_1p + \cdots + a_rp^r$ with $0 \le a_i < p$ for each i, then*

$$v_p(m!) = \frac{m - (a_0 + a_1 + \cdots + a_r)}{p-1}.$$

The elementary lemma stated below is also well known (cf. [14, Problem 435]).

Lemma 2.C. *Let t, n be positive integers. Let $\mathcal{P}$ denote the set of points in the plane with positive integer entries lying inside or on the triangle with vertices $(0,0), (n,0), (n,t)$ which do not lie on the line $x = n$. Then the number of elements in $\mathcal{P}$ is $\frac{1}{2}[(n-1)(t-1) + \gcd(t,n) - 1]$.*

For proving Theorem 1.1, we will use the classical Theorem of Index of Ore (stated as Theorem 2.E below) in addition to carrying out several simplifications. To state this theorem, we introduce the notions of valuation, Gauss valuation, ϕ-Newton polygon, ϕ-index of a polynomial, where $\phi(x)$ belonging to $\mathbb{Z}[x]$ is a monic polynomial which is irreducible modulo a given prime p.

As usual, by a valuation v of a field K, we shall mean a mapping $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ which satisfies the following properties for all α, β in K.

(i) $v(\alpha) = \infty$ if and only if $\alpha = 0$,

(ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$,

(iii) $v(\alpha + \beta) \ge \min\{v(\alpha), v(\beta)\}$.

The subring R_v of K defined by $R_v = \{\alpha \in K \mid v(\alpha) \ge 0\}$ is called the valuation ring of v. It has a unique maximal ideal $\mathcal{M}_v = \{\alpha \in K \mid v(\alpha) > 0\}$ and $R_v/\mathcal{M}_v$ is called the residue field of v. A valuation v' of an overfield K' of K is said to be an extension or a prolongation of v to K' if v' coincides with v on K.

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

Notations. For a prime number p, as usual $\mathbb{Z}_p$ will stand for the ring of p-adic integers and $\mathbb{Q}_p$ for its quotient field. We shall also denote by v_p the unique prolongation of the p-adic valuation to the field $\mathbb{Q}_p$ of p-adic numbers. If v_1 denotes the prolongation of v_p to a finite extension of $\mathbb{Q}_p$, then for any polynomial $g_1(x)$ with coefficients in the valuation ring of v_1, $\overline{g}_1(x)$ will stand for the polynomial obtained by replacing each coefficient of $g_1(x)$ by its image under the canonical homomorphism from the valuation ring of v_1 onto its residue field.

We shall denote by v_p^x the Gaussian valuation of the field $\mathbb{Q}_p(x)$ of rational functions in an indeterminate x which extends the valuation v_p of $\mathbb{Q}_p$ and is defined on $\mathbb{Q}_p[x]$ by:

$$v_p^x\left(\sum_i c_i x^i\right) = \min_i\{v_p(c_i)\}, \quad c_i \in \mathbb{Q}_p.$$

If $\phi(x)$ is a fixed monic polynomial with coefficients in an integral domain R, then any polynomial $g(x) \in R[x]$ can be uniquely written as a finite sum $\sum\limits_i g_i(x)\phi(x)^i$ with $\deg g_i(x) < \deg \phi(x)$ for each i; this expansion will be referred to as the ϕ-expansion of $g(x)$.

The following definition extends the notion of Newton polygon of a polynomial with respect to a prime p.

Definition 2.1. *Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial which is irreducible modulo a given prime p. Let $g(x)$ belonging to $\mathbb{Z}_p[x]$ be a polynomial having ϕ-expansion $\sum\limits_{i=0}^{n} g_i(x)\phi(x)^i$ with $g_0(x)g_n(x) \neq 0$. Let P_i stand for the point in the plane having coordinates $(i, v_p^x(g_{n-i}(x)))$ when $g_{n-i}(x) \neq 0$, $0 \leq i \leq n$. Let μ_{ij} denote the slope of the line joining the points P_i and P_j if $g_{n-i}(x)g_{n-j}(x) \neq 0$. Let i_1 be the largest index $0 < i_1 \leq n$ such that:*

$$\mu_{0i_1} = \min\{\mu_{0j} \mid 0 < j \leq n,\ g_{n-j}(x) \neq 0\}.$$

If $i_1 < n$, let i_2 be the largest index $i_1 < i_2 \leq n$ satisfying:

$$\mu_{i_1 i_2} = \min\{\mu_{i_1 j} \mid i_1 < j \leq n,\ g_{n-j}(x) \neq 0\},$$

and so on. The ϕ-Newton polygon of $g(x)$ with respect to p is the polygonal path having segments $P_0P_{i_1}, P_{i_1}P_{i_2}, \ldots, P_{i_{k-1}}P_{i_k}$ with $i_k = n$. These segments are called the edges of the ϕ-Newton polygon of $g(x)$ and their slopes from left to right form a strictly increasing sequence. In particular when $\phi(x) = x$, the ϕ-Newton polygon of $g(x)$ with respect to p will be referred to as the Newton polygon of $g(x)$ with respect to p.

Definition 2.2. *Let $\phi(x)$ and $g(x)$ be as in Definition 2.1. Let N denote the number of points with positive integer coordinates lying on or below the ϕ-Newton polygon of $g(x)$ away from the vertical line passing through the last vertex of this polygon. As in [13], the ϕ-index of g (with respect to p) is defined to be $N \deg \phi(x)$ and will be denoted by $i_\phi(g)$.*

The following example illustrates the above definition.

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

Example 2.3. Let $g(x) = f_4(x) = x^4 + \frac{4!}{3!}x^3 + \frac{4!}{2!}x^2 + \frac{4!}{1!}x + 4!$. Consider $\phi(x) = x$. Note that the ϕ-Newton polygon of $g(x)$ with respect to the prime 2 being the lower convex hull of the points $(0, 0), (1, 2), (2, 2), (3, 3)$ and $(4, 3)$ consists of a single edge joining the point $(0, 0)$ with $(4, 3)$. Thus $i_\phi(g) = 3$ (with respect to 2). Next consider $\phi_1(x) = x + 1$. It can be easily checked that $g(x) = (x+1)^4+6(x+1)^2+8(x+1)+9$. So the ϕ_1-Newton polygon of $g(x)$ with respect to 3 being the lower convex hull of the points $(0, 0), (2, 1), (3, 0)$ and $(4, 2)$ consists of two edges; the first edge joins the point $(0, 0)$ with $(3, 0)$ and the second edge is the line segment joining the points $(3, 0)$ and $(4, 2)$. Thus $i_{\phi_1}(g) = 0$ (with respect to 3).

We now state a theorem originally proved by Ore (see [13, Theorem 1.2], [18]).

Theorem 2.D. *Let $L = \mathbb{Q}(\xi)$ be an algebraic number field with ξ satisfying a monic irreducible polynomial $g(x) \in \mathbb{Z}[x]$ and p be a prime number. Let $\overline{\phi}_1(x)^{e_1} \cdots \overline{\phi}_r(x)^{e_r}$ be the factorization of $g(x)$ modulo p into a product of powers of distinct irreducible polynomials over the finite field $\mathbb{F}_p$ of p elements, where each $\phi_i(x) \neq g(x)$ belonging to $\mathbb{Z}[x]$ is monic. Then, $v_p(\text{ind } \xi) \geq \sum\limits_{j=1}^{r} i_{\phi_j}(g)$.*

Ore also gave a sufficient condition so that the inequality in the above theorem becomes equality. For this, he associated with each edge S_{ij} of the ϕ_i-Newton polygon of $g(x)$ having positive slope, a polynomial $T_{ij}(Y)$ in an indeterminate Y with coefficients from the field $\mathbb{F}_q$ having $q = p^{deg\phi_i(x)}$ elements described in the following definitions.

Definition 2.4. *Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial which is irreducible modulo a given prime p having a root α in a finite extension of $\mathbb{Q}_p$. Let $g(x) \in \mathbb{Z}_p[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\phi(x)^n + g_{n-1}(x)\phi(x)^{n-1} + \cdots + g_0(x)$ such that $\overline{g}(x)$ is a power of $\overline{\phi}(x)$. Suppose that the ϕ-Newton polygon of $g(x)$ consists of a single edge, say S having positive slope denoted by $\frac{d}{e}$ with integers d, e coprime, i.e., $\min\{\frac{v_p^x(g_{n-i}(x))}{i} \mid 1 \leq i \leq n\} = \frac{v_p^x(g_0(x))}{n} = \frac{d}{e}$ so that n is divisible by e, say $n = et$ and $v_p^x(g_{n-ej}(x)) \geq dj$ for $1 \leq j \leq t$. Thus the polynomial $h_j(x) := \frac{g_{n-ej}(x)}{p^{dj}}$ has coefficients in $\mathbb{Z}_p$ and hence $h_j(\alpha) \in \mathbb{Z}_p[\alpha]$ for $1 \leq j \leq t$. The polynomial $T(Y)$ in an indeterminate Y defined by $T(Y) = Y^t + \sum\limits_{j=1}^{t} \overline{h_j}(\overline{\alpha})Y^{t-j}$ having coefficients in $\mathbb{F}_p[\overline{\alpha}]$ is said to be the polynomial associated to $g(x)$ with respect to (ϕ, S).*

The example given below illustrates the above definition.

Example 2.5. Let $g(x) = f_4(x) = x^4 + \frac{4!}{3!}x^3 + \frac{4!}{2!}x^2 + \frac{4!}{1!}x + 4!$. Clearly $g(x) \equiv x^4 \pmod 2$. Consider $\phi(x) = x$. One can check that the ϕ-Newton polygon of $g(x)$ with respect to the prime 2 consists of a single edge S joining the points $(0, 0)$ and $(4, 3)$. With notations as in the above definition, we see that $d = 3$, $e = 4$ and the polynomial associated to $g(x)$ with respect to (ϕ, S) is $T(Y) = Y + \overline{1}$ belonging to $\mathbb{F}_2[Y]$.

We now extend the notion of associated polynomial when $g(x)$ is more general.

Definition 2.6. *Let $p, \phi(x)$ and α be as in Definition 2.4. Let $G(x) \in \mathbb{Z}_p[x]$ be a monic polynomial not divisible by $\phi(x)$ such that $\overline{G}(x)$ is a power of $\overline{\phi}(x)$. Let $\lambda_1 < \cdots < \lambda_k$ be*

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

the slopes of the edges of the ϕ-Newton polygon of G(x) and S_i denote the edge with slope λ_i. In view of the Theorem of Product by Ore (cf. [5, Theorem 1.5*], [12, Theorem 1.1]), we can write $G(x) = H_1(x)\cdots H_k(x)$, where the ϕ-Newton polygon of $H_i(x) \in \mathbb{Z}_p[x]$ has a single edge, say S_i' which is a translate of S_i. Let $T_i(Y)$ belonging to $\mathbb{F}_p[\overline{\alpha}][Y]$ denote the polynomial associated to $H_i(x)$ with respect to (ϕ, S_i') described as in Definition 2.4. The polynomial G(x) is said to be p-regular with respect to ϕ if none of the polynomials $T_i(Y)$ has a repeated root in the algebraic closure of $\mathbb{F}_p$, $1 \leq i \leq k$. In general, if g(x) belonging to $\mathbb{Z}_p[x]$ is a monic polynomial and $\overline{g}(x) = \overline{\phi}_1(x)^{e_1}\cdots\overline{\phi}_r(x)^{e_r}$ is its factorization modulo p into irreducible polynomials with each $\phi_i(x)$ belonging to $\mathbb{Z}[x]$ monic and $e_i > 0$, then by Hensel's Lemma [4, Chapter* 4*, Section* 3*], there exist monic polynomials $G_1(x), \ldots, G_r(x)$ belonging to $\mathbb{Z}_p[x]$ such that $g(x) = G_1(x)\cdots G_r(x)$ and $\overline{G}_i(x) = \overline{\phi}_i(x)^{e_i}$ for each i. The polynomial g(x) is said to be p-regular with respect to $\phi_1, \ldots, \phi_r$ if each $G_i(x)$ is p-regular with respect to ϕ_i.*

We give below a simple example of a p-regular polynomial with respect to any monic polynomial $\phi(x) \in \mathbb{Z}[x]$ which is irreducible modulo a given prime p.

Example 2.7. If $p, \phi(x)$ are as above and $G(x) \neq \phi(x)$ belonging to $\mathbb{Z}_p[x]$ is a monic polynomial with $\overline{G}(x) = \overline{\phi}(x)$, then the ϕ-Newton polygon of $G(x)$ with respect to p is a line segment S joining the point $(0, 0)$ with $(1, c)$ for some $c > 0$. Consequently, the polynomial associated to $G(x)$ with respect to (ϕ, S) is linear and $i_\phi(G) = 0$. In particular, $G(x)$ is p-regular with respect to ϕ.

We now state a celebrated result to be used in the sequel known as the Theorem of Index of Ore (cf. [13, Theorem 1.4], [18]).

Theorem 2.E. *Let $L = \mathbb{Q}(\xi), g(x), p$ and $\phi_1(x), \ldots, \phi_r(x)$ be as in Theorem 2.D. If g(x) is p-regular with respect to $\phi_1, \ldots, \phi_r$, then $v_p(\text{ind } \xi) = \sum\limits_{j=1}^{r} i_{\phi_j}(g)$.*

Keeping in mind Example 2.7, the following corollary is an immediate consequence of Theorem 2.E.

Corollary 2.8. *Let $L = \mathbb{Q}(\xi), g(x), p$, $\phi_1(x), \ldots, \phi_r(x)$ and $e_1, \ldots, e_r$ be as in Theorem 2.D. If $e_i = 1$ for each $i > 1$ and g(x) is p-regular with respect to ϕ_1, then $v_p(\text{ind } \xi) = i_{\phi_1}(g)$.*

Let $g(x), p, \phi_1(x), \ldots, \phi_r(x)$ be as in Theorem 2.D. Then by Hensel's Lemma, we can write $g(x) = G_1(x)\cdots G_r(x)$ where $G_i(x) \in \mathbb{Z}_p[x]$ is a monic polynomial with $\overline{G}_i(x) = \overline{\phi_i}(x)^{e_i}$. If S is an edge of the ϕ_i-Newton polygon of $G_i(x)$, then for convenience, the polynomial associated to $G_i(x)$ with respect to $(\phi_i,\ S)$ will be referred to as the polynomial associated to $g(x)$ with respect to $(\phi_i,\ S')$ where S' is the edge of the ϕ_i-Newton polygon of $g(x)$ which is a translate of S, because the ϕ_i-Newton polygon of $g(x)$ can be obtained from the ϕ_i-Newton polygon of $G_i(x)$ by giving a horizontal translation in view of the following simple lemma proved in [5, Proposition 1.2, Theorem 3.2] and [12, Corollary 2.5].

Lemma 2.F *Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial which is irreducible modulo a given prime p and f(x), g(x) belonging to $\mathbb{Z}_p[x]$ be two monic polynomials not divisible by*

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

$\phi(x)$. If $\overline{\phi}(x)$ does not divide $\overline{g}(x)$, then the ϕ-Newton polygon of $g(x)$ is either a point or a horizontal line segment and the ϕ-Newton polygon of $f(x)g(x)$ is obtained by adjoining to the ϕ-Newton polygon of $g(x)$ a translate of the ϕ-Newton polygon of $f(x)$.

3. Proof of Theorem 1.1

The proof of Theorem 1.1 is divided in four steps.

Step I. In this step, we prove that for any prime p less than or equal to n, x is the only repeated factor of $f_n(x)$ modulo p. In view of Lemma 2.A and a well-known result [11, Corollary 2.16], we have

$$(-1)^{\frac{n(n-1)}{2}}(n!)^n = discr(f_n) = (\text{ind } \theta)^2 d_K. \tag{4}$$

So if a prime divides ind θ or d_K, then it divides $n!$. Let p be a prime dividing $n!$. Let k be the smallest non-negative integer not exceeding $n-2$ such that p divides $n-k$. Then

$$f_n(x) \equiv x^{n-k}\left(x^k + \frac{n!}{(n-1)!}x^{k-1} + \cdots + \frac{n!}{(n-k)!}\right) \pmod{p}.$$

Denote the polynomial $x^k + \frac{n!}{(n-1)!}x^{k-1} + \cdots + \frac{n!}{(n-k)!}$ by $h(x)$. Note that $h(x)$ is not divisible by x modulo p in view of the choice of k and $h(x) \equiv x^k + h'(x) \pmod{p}$. So $h(x)$ and $h'(x)$ are coprime modulo p, i.e., $h(x)$ has no repeated factor modulo p. Consequently x is the only repeated factor of $f_n(x)$ modulo p.

Step II. In this step, we prove that $f_n(x)$ is p-regular with respect to $\phi(x) = x$ for each prime p dividing $n!$. Let p be such a prime. Keeping in mind that x is the only repeated factor of $f_n(x)$ modulo p in view of Step I, it would follow from Corollary 2.8 that $v_p(\text{ind } \theta) = i_\phi(f_n)$ where $\phi(x) = x$, i.e.,

$$v_p(\text{ind } \theta) = N, \tag{5}$$

where N is the number of points with positive integer coordinates lying on or below the Newton polygon of $f_n(x)$ with respect to p away from the vertical line passing through the last vertex of this polygon.

By definition, the Newton polygon of $f_n(x)$ with respect to p is the polygonal path formed by the lower edges along the convex hull of points of the set $\mathcal{P}$ defined by

$$\mathcal{P} = \{(i, v_p(n!/(n-i)!)) \mid 0 \le i \le n\}.$$

Recall that

$$n = c_1p^{m_1} + c_2p^{m_2} + \cdots + c_sp^{m_s},$$

where $0 \le m_1 < m_2 < \cdots < m_s$ and $0 < c_i < p$ for each i. Set $z_0 = 0$ and

$$z_i = c_1p^{m_1} + \cdots + c_ip^{m_i}, \quad 1 \le i \le s. \tag{6}$$

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

As in [6], making use of Lemma 2.B, it can be easily shown that the Newton polygon of $f_n(x)$ with respect to p consists of s edges; the ith edge from left to right is the line segment joining the points:

$$(z_{i-1}, v_p(n!/(n-z_{i-1})!)),\ (z_i, v_p(n!/(n-z_i)!)).$$

Therefore using Lemma 2.B, we see that the slope λ_i of the ith edge of the Newton polygon of $f_n(x)$ with respect to p is given by:

$$\begin{aligned}\lambda_i &= \frac{-v_p((n-z_i)!)+v_p((n-z_{i-1})!)}{z_i-z_{i-1}}\\ &= \frac{z_i+(c_{i+1}+\cdots+c_s)-z_{i-1}-(c_i+\cdots+c_s)}{(z_i-z_{i-1})(p-1)}.\end{aligned}$$

So

$$\lambda_i = \frac{c_ip^{m_i}-c_i}{c_ip^{m_i}(p-1)} = \frac{p^{m_i}-1}{p^{m_i}(p-1)}.$$

Note that $f_n(x)$ has an edge with slope zero if and only if $m_1 = 0$, which happens only when $k > 0$ where k is as in Step I. In view of Hensel's Lemma and the Theorem of product by Ore (cf. [5, Theorem 1.5], [12, Theorem 1.1]), we can write $f_n(x) = G_1(x)\cdots G_s(x)$ where $G_i(x) \in \mathbb{Z}_p[x]$ has degree $z_i - z_{i-1} = c_ip^{m_i}$ and the Newton polygon of $G_i(x)$ with respect to p consists of only one edge S_i (say) having slope λ_i. When $\lambda_i > 0$, let $T_i(Y)$ belonging to $\mathbb{F}_p[Y]$ denote the polynomial associated to $G_i(x)$ with respect to $(\phi,\ S_i)$ as described in Definition 2.6, where $\phi(x) = x$. Note that the degree of $T_i(Y)$ is $c_i \le p-1$; consequently $T_i(Y)$ is a separable polynomial. This proves that $f_n(x)$ is p-regular with respect to $\phi(x) = x$.

Step III. In this step, we prove that

$$N = \frac{1}{2}\sum_{i=1}^{s}[c_id_i\,(c_ip^{m_i}+2c_{i+1}p^{m_{i+1}}+\cdots+2c_sp^{m_s}-p)], \tag{7}$$

where N is as in (5). This will prove (1) at once.

Set $t_i = v_p(n!/(n-z_i)!)$ for $0 \le i \le s$. Using Lemma 2.B, it can be easily seen that $v_p(n!/(n-z_i)!) = v_p(z_i!)$ for $0 \le i \le s$. So $t_0 = 0$ and

$$t_i = v_p(z_i!) = c_1d_1+\cdots+c_id_i, \quad 1 \le i \le s. \tag{8}$$

As pointed out in Step II, the Newton polygon of $f_n(x)$ with respect to p consists of s edges; the ith edge from left to right is the segment joining the points (z_{i-1}, t_{i-1}), (z_i, t_i) and N is the number of points with positive integer coordinates lying on or below this Newton polygon which do not lie on the line $x = z_s$. We now count these points.

For $1 \le i \le s$, the number of points with positive integer coordinates lying on or in the triangle joining the points (z_{i-1}, t_{i-1}), (z_i, t_{i-1}), (z_i, t_i) away from its vertical side is same as number of such points in the case of the triangle joining $(0,0)$, $(z_i - z_{i-1}, 0)$,

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

$(z_i - z_{i-1}, t_i - t_{i-1})$. It is immediate from (6) and (8) that $z_i - z_{i-1} = c_i p^{m_i}$ and $t_i - t_{i-1} = c_i d_i$. In view of Lemma 2.C, this number is given by:

$$\frac{1}{2}[(c_i p^{m_i} - 1)\,(c_i d_i - 1) + c_i - 1] = \frac{1}{2}[c_i^2 d_i p^{m_i} - c_i d_i - c_i p^{m_i} + c_i] = \frac{1}{2} c_i d_i [c_i p^{m_i} - p].$$

For $2 \leq i \leq s$, the number of points with positive integer coordinates lying in or on the rectangle joining the points $(z_{i-1}, 0)$, $(z_i, 0)$, (z_i, t_{i-1}) and (z_{i-1}, t_{i-1}) which do not lie on the line $x = z_i$ is $(z_i - z_{i-1}) t_{i-1} = c_i p^{m_i}(c_1 d_1 + \cdots + c_{i-1} d_{i-1})$ by virtue of (6) and (8). Therefore

$$\begin{aligned} N &= \frac{1}{2}\sum_{i=1}^{s} c_i d_i [c_i p^{m_i} - p] + \sum_{i=2}^{s} [c_i p^{m_i}(c_1 d_1 + \cdots + c_{i-1} d_{i-1})] \\ &= \frac{1}{2}\sum_{i=1}^{s} c_i d_i [c_i p^{m_i} - p] + \sum_{i=1}^{s} [c_i d_i\,(c_{i+1} p^{m_{i+1}} + \cdots + c_s p^{m_s})] \\ &= \frac{1}{2}\sum_{i=1}^{s} [c_i d_i\,(c_i p^{m_i} + 2c_{i+1} p^{m_{i+1}} + \cdots + 2c_s p^{m_s} - p)]. \end{aligned}$$

This proves (7) and hence (1) is proved.

Step IV. In this step, we prove (2). It is immediate from (4) that $v_p(d_K) = n v_p(n!) - 2 v_p(\text{ind }\theta)$. Using Lemma 2.B, we see that

$$n v_p(n!) = (c_1 p^{m_1} + \cdots + c_s p^{m_s})\,(c_1 d_1 + \cdots + c_s d_s) = \sum_{i=1}^{s} [c_i d_i (c_1 p^{m_1} + \cdots + c_s p^{m_s})]. \tag{9}$$

It is immediate from (1) and (9) that

$$\begin{aligned} v_p(d_K) &= n v_p(n!) - 2 v_p(\text{ind }\theta) \\ &= \sum_{i=1}^{s} [c_i d_i (c_1 p^{m_1} + \cdots + c_s p^{m_s})] - \sum_{i=1}^{s} [c_i d_i\,(c_i p^{m_i} + 2c_{i+1} p^{m_{i+1}} + \cdots + 2c_s p^{m_s})] \\ &\qquad + p \sum_{i=1}^{s} c_i d_i \\ &= \sum_{i=1}^{s} [c_i d_i (c_1 p^{m_1} + \cdots + c_{i-1} p^{m_{i-1}} - c_{i+1} p^{m_{i+1}} - \cdots - c_s p^{m_s})] + p \sum_{i=1}^{s} c_i d_i. \end{aligned} \tag{10}$$

Keeping in mind that $d_i = \frac{p^{m_i} - 1}{p-1}$, it can be easily seen that: $d_j p^{m_i} - d_i p^{m_j} = \frac{p^{m_j} - p^{m_i}}{p-1}$ for $1 \leq i < j \leq s$. Using this equality, the first summand in (10) can be rewritten as:

$$\sum_{1 \leq j < i \leq s} (c_i c_j d_i p^{m_j}) - \sum_{1 \leq i < j \leq s} (c_i c_j d_i p^{m_j}) = \sum_{1 \leq i < j \leq s} [c_i c_j (d_j p^{m_i} - d_i p^{m_j})]$$

$$= \sum_{1\leqslant i<j\leqslant s} \frac{c_i c_j (p^{m_j} - p^{m_i})}{p-1}.$$

The desired inequality (2) now follows from (10).

4. Proof of Corollaries 1.2, 1.3

Proof of Corollary 1.2. Let p be a prime number. In view of (1), $v_p(\text{ind }\theta) = 0$ if and only if the p-adic expansion of n is of the type $n = c_1$ or $n = p$ or $n = c_1 + p$ with $0 < c_1 < p$, which is equivalent to saying that $n < 2p$. This proves the first assertion of the corollary. The second assertion follows immediately from the first. □

Proof of Corollary 1.3. In view of (2), $v_p(d_K) = 0$ for a prime p if and only if the p-adic expansion of n is of the type $n = c_1$ with $0 < c_1 < p$, or equivalently n is less than p. This proves the corollary. □

5. Proof of Theorem 1.4

The following proposition to be used in the sequel is proved as Proposition 3.A in [10].

Proposition 5.A. *Let $L = \mathbb{Q}(\xi)$ be an algebraic number field of degree n with ξ an algebraic integer and let p be a prime number. Let $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ be p-integral elements of L of the type $\alpha_i = \frac{c_{i0}+c_{i1}\xi+\cdots+c_{i(i-1)}\xi^{i-1}+\xi^i}{p^{k_i}}$ where $c_{ij},\ k_i$ are in $\mathbb{Z}$ with $0 \le k_i \le k_{i+1}$ for $1 \le i \le n-2$. Then $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ is a p-integral basis of L if and only if $v_p(\text{ind }\xi) = \sum_{i=1}^{n-1} k_i$.*

Recall that an algebraic number η is integral over the localisation $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at a maximal ideal $p\mathbb{Z}$ if and only if $w(\eta) \ge 0$ for all prolongations w to $\mathbb{Q}(\eta)$ of the p-adic valuation of $\mathbb{Q}$ (cf. [4, Chapter 3, Theorem 6]). Keeping this in mind the next proposition follows immediately from Proposition 2.2 of [13]. Its proof is omitted.

Proposition 5.B. *Let $\mathbb{Q}(\xi)$ be an algebraic number field, where ξ is a root of a monic irreducible polynomial $g(x)$ belonging to $\mathbb{Z}[x]$. Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial different from $g(x)$ which divides $g(x)$ modulo a given prime p and is irreducible modulo p. Let $g(x) = \sum_{i=0}^{d} g_i(x)\phi(x)^i$ be the ϕ-expansion of $g(x)$ with $g_d(x) \neq 0$. Let $q_j(x)$ denote the quotient obtained on dividing $g(x)$ by $\phi(x)^j$, $1 \le j \le d$. If y_{d-j} stands for the ordinate of the point with abscissa $d-j$ on the ϕ-Newton polygon of $g(x)$ with respect to p, then $q_j(\xi)/p^{\lfloor y_{d-j} \rfloor}$ is integral over $\mathbb{Z}_{(p)}$.*

The result stated below is an immediate consequence of Corollary 2.8 and Propositions 5.A, 5.B.

Proposition 5.1. *Let $L = \mathbb{Q}(\xi)$ be an algebraic number field with ξ satisfying a monic irreducible polynomial $g(x) \in \mathbb{Z}[x]$ of degree n and let p be a prime number.*

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

Let $\overline{\phi}_1(x)^{e_1}\cdots\overline{\phi}_r(x)^{e_r}$ be the factorization of $g(x)$ modulo p into a product of powers of distinct irreducible polynomials over $\mathbb{F}_p$, where each $\phi_i(x) \neq g(x)$ belonging to $\mathbb{Z}[x]$ is monic. Assume that $\phi_1(x) = x$, $e_i = 1$ for each $i > 1$ and $g(x)$ is p-regular with respect to ϕ_1. Let $q_j(x)$ denote the quotient obtained on dividing $g(x)$ by x^j, $1 \leq j \leq n-1$. If y_{n-j} stands for the ordinate of the point with abscissa $n-j$ on the ϕ_1-Newton polygon of $g(x)$ with respect to p, then $\{1, q_1(\xi)/p^{\lfloor y_{n-1}\rfloor}, \ldots, q_{n-1}(\xi)/p^{\lfloor y_1\rfloor}\}$ is a p-integral basis of L.

Proof of Theorem 1.4. In view of Steps I and II of the proof of Theorem 1.1 given in § 3, we see that $f_n(x)$ satisfies the hypothesis of Proposition 5.1. Therefore, Theorem 1.4 follows immediately from Proposition 5.1, because with notations as in Proposition 5.1, we have $q_{n-j}(x) = x^j + \frac{n!}{(n-1)!}x^{j-1} + \cdots + \frac{n!}{(n-j)!} = u_j(x)$ for $1 \leq j \leq n-1$. □

Example 5.2. Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial,

$$f_6(x) = x^6 + \frac{6!}{5!}x^5 + \frac{6!}{4!}x^4 + \frac{6!}{3!}x^3 + \frac{6!}{2!}x^2 + \frac{6!}{1!}x + 6!.$$

Then by (2), $v_2(d_K) = 10$, $v_3(d_K) = 6$ and $v_5(d_K) = 6$. So $d_K = -2^{10}3^6 5^6$ in view of Lemma 2.A. By virtue of Corollary 1.2, we see that $v_p(\text{ind}\ \theta) > 0$ only when $p = 2$ or 3. For these two primes, we first find p-integral bases. Keeping the notations $u_j(x)$ and y_j of Theorem 1.4, we have

$$u_j(x) = x^j + \frac{6!}{5!}x^{j-1} + \cdots + \frac{6!}{(6-j)!}, \quad 1 \leq j \leq 5.$$

The Newton polygon of $f_6(x)$ with respect to the prime 2 has two edges joining the points $(0, 0)$ with $(2, 1)$ and $(2, 1)$ with $(6, 4)$. So $\lfloor y_1\rfloor = 0$, $\lfloor y_2\rfloor = \lfloor y_3\rfloor = 1$, $\lfloor y_4\rfloor = 2$ and $\lfloor y_5\rfloor = 3$. Therefore applying Theorem 1.4, we see that

$$\left\{1, \theta, \frac{\theta^2}{2}, \frac{\theta^3}{2}, \frac{\theta^4 + 2\theta^3 + 2\theta^2}{2^2}, \frac{\theta^5 + 6\theta^4 + 6\theta^3}{2^3}\right\}$$

is a 2-integral basis of K.

By looking at the Newton polygon of $f_6(x)$ with respect to the prime 3 and applying Theorem 1.4, it can be easily seen that $\left\{1, \theta, \theta^2, \frac{\theta^3}{3}, \frac{\theta^4}{3}, \frac{\theta^5}{3}\right\}$ is a 3-integral basis of K.

Therefore, using Theorem 1.A and Chinese Remainder Theorem, we see that:

$$\left\{1, \theta, \frac{\theta^2}{2}, \frac{\theta^3}{6}, \frac{\theta^4 + 6\theta^3 + 6\theta^2}{12}, \frac{\theta^5 + 6\theta^4 + 6\theta^3}{24}\right\},$$

is an integral basis of K.

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press

Example 5.3. Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial:

$$f_7(x) = x^7 + \frac{7!}{6!}x^6 + \frac{7!}{5!}x^5 + \frac{7!}{4!}x^4 + \frac{7!}{3!}x^3 + \frac{7!}{2!}x^2 + \frac{7!}{1!}x + 7!.$$

Then by (2), $v_2(d_K) = 14$, $v_3(d_K) = 8$ and $v_5(d_K) = v_7(d_K) = 7$. So $d_K = -2^{14}3^8 5^7 7^7$ by virtue of Lemma 2.A. In view of Corollary 1.2, $v_p(\mathrm{ind}\ \theta) > 0$ only when $p = 2$ or 3. For these two primes, we first find p-integral bases. With notations as in Theorem 1.4, we have:

$$u_j(x) = x^j + \frac{7!}{6!}x^{j-1} + \cdots + \frac{7!}{(7-j)!}, \quad 1 \leq j \leq 6.$$

Keeping in mind that the Newton polygon of $f_7(x)$ with respect to 2 is the polygonal path joining the points $(0,0), (1,0), (3,1), (7,4)$ and using Theorem 1.4, it can be checked that:

$$\left\{1, \theta, \theta^2, \frac{\theta^3 + \theta^2}{2}, \frac{\theta^4 + \theta^3}{2}, \frac{\theta^5 + 3\theta^4 + 2\theta^3 + 2\theta^2}{2^2}, \frac{\theta^6 + 7\theta^5 + 2\theta^4 + 2\theta^3}{2^3}\right\},$$

is a 2-integral basis of K. By similar arguments, we can show that $\left\{1, \theta, \theta^2, \theta^3, \frac{\theta^4+\theta^3}{3}, \frac{\theta^5+\theta^4}{3}, \frac{\theta^6+\theta^5}{3}\right\}$ is a 3-integral basis of K. Therefore, it follows from Theorem 1.A that:

$$\left\{1, \theta, \theta^2, \frac{\theta^3 + 3\theta^2}{2}, \frac{\theta^4 + \theta^3}{6}, \frac{\theta^5 + 7\theta^4 + 6\theta^3 + 6\theta^2}{12}, \frac{\theta^6 + 7\theta^5 + 18\theta^4 + 18\theta^3}{24}\right\},$$

is an integral basis of K.

Acknowledgement. The first author is grateful to the National Board for Higher Mathematics, Department of Atomic Energy, India for postdoctoral fellowship. The second author is thankful to the Indian National Science Academy for Honorary Scientistship.

References

(1) Ş. Alaca, p-Integral basis of a cubic field, *Proc. Amer. Math. Soc.* **126** (1998), 1949–1953.

(2) Ş. Alaca and K. S. Williams, p-Integral basis of a quartic field defined by a trinomial $x^4 + ax + b$, *Far East J. Math. Sci.* **12** (2004), 137–168.

(3) D. M. Burton, *Elementary Number Theory*, 7th edn., (India: McGraw-Hill, 2017).

(4) Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

(5) S. D. Cohen, A. Movahhedi and A. Salinier, Factorisation over local fields and the irreducibility of generalised difference polynomials, *Mathematika* **47** (2000), 173–196.

(6) R. F. Coleman, On the Galois groups of the exponential Taylor polynomials, *L'Enseignement Math.* **33** (1987), 183–189.

(7) T. Funakura, On integral bases of pure quartic fields, *Math. J. Okayama Univ* **26** (1984), 27–41.

(8) A. Jakhar, S. K. Khanduja and N. Sangwan, On integral basis of pure number fields, *Mathematatika* **67** (2021), 187–195.

(9) Kenzô Komatsu, Integral bases in algebraic number fields, *J. Reine Angew. Math.* **1975**(278–279) (1975), 137–144.

(10) S. Kaur and S. K. Khanduja, Discriminant and integral basis of sextic fields defined by $x^6 + ax + b$, *Commun. Algebra* **50** (2022), 4401–4436.

(11) S. K. Khanduja, *A Textbook of Algebraic Number Theory*, Unitext series 135, (Singapore: Springer, 2022).

(12) S. K. Khanduja and S. Kumar, On prolongations of valuations via Newton polygons and liftings of polynomials, *J. Pure Appl. Algebra* **216** (2012), 2648–2656.

(13) S. K. Khanduja and S. Kumar, A generalization of a theorem of Ore, *J. Pure Appl. Algebra* **218** (2014), 1206–1218.

(14) J. M. de Koninck and A. Mercier, *1001 Problems in Classical Number Theory*, American Mathematical Society, Providence, RI, 2007.

(15) P. Llorente, E. Nart and N. Vila, Effective determination of the decomposition of rational primes in a cubic field, *Amer. Math. Soc.* **87** (1983), 579–585.

(16) P. Llorente, E. Nart and N. Vila, Discriminants of number fields defined by trinomials, *Acta Arith.* **43** (1984), 367–373.

(17) P. Llorente, E. Nart and N. Vila, Decomposition of primes in number fields defined by trinomials, *J. Theor. Nr. Bordx.* **3** (1991), 27–41.

(18) Ø. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, *Math. Ann.* **99** (1928), 84–117.

(19) I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I, *Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl.* **14** (1929), 125–136.

(20) I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, II, *Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl.* **23** (1929), 1–24.

(21) J. Westlund, On the fundamental number of the algebraic number field $k(\sqrt[p]{m})$, *Trans. Amer. Math. Soc.* **11** (1910), 388–392.

https://doi.org/10.1017/S0013091524000105 Published online by Cambridge University Press