

CONFLUENTES MATHEMATICI

Devendra PRASAD, Krishnan RAJKUMAR, and A. Satyanarayana REDDY

A Survey on Fixed Divisors

Tome 11, n° 1 (2019), p. 29-52.

http://cml.cedram.org/item?id=CML_2019__11_1_29_0

© Institut Camille Jordan, 2019, tous droits réservés.

L'accès aux articles de la revue « Confluentes Mathematici » (<http://cml.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://cml.cedram.org/legal/>). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

A SURVEY ON FIXED DIVISORS

DEVENDRA PRASAD, KRISHNAN RAJKUMAR, AND A. SATYANARAYANA REDDY

Abstract. In this article, we compile the work done by various mathematicians on the topic of the fixed divisor of a polynomial. This article explains most of the results concisely and is intended to be an exhaustive survey. We present the results on fixed divisors in various algebraic settings as well as the applications of fixed divisors to various algebraic and number theoretic problems. The work is presented in an orderly fashion so as to start from the simplest case of \mathbb{Z} , progressively leading up to the case of Dedekind domains. We also ask a few open questions according to their context, which may give impetus to the reader to work further in this direction. We describe various bounds for fixed divisors as well as the connection of fixed divisors with different notions in the ring of integer-valued polynomials. Finally, we suggest how the generalization of the ring of integer-valued polynomials in the case of the ring of $n \times n$ matrices over \mathbb{Z} (or a Dedekind domain) could lead to the generalization of fixed divisors in that setting.

NOTATIONS

We fix the notations for the whole paper.

R	=	Integral Domain
\mathbb{K}	=	Field of fractions of R
$N(I)$	=	Cardinality of R/I (Norm of an ideal $I \subseteq R$)
\mathbb{W}	=	$\{0, 1, 2, 3, \dots\}$
$A[\underline{x}]$	=	Ring of polynomials in n variables ($= A[x_1, \dots, x_n]$) with coefficients in the ring A
\underline{S}	=	Arbitrary (or given) subset of R^n such that no non-zero polynomial in $\mathbb{K}[\underline{x}]$ maps it to zero
S	=	\underline{S} in case when $n = 1$
$\text{Int}(\underline{S}, R)$	=	Polynomials in $\mathbb{K}[\underline{x}]$ mapping \underline{S} back to R
$\nu_k(S)$	=	Bhargava's (generalized) factorial of index k
$k!_{\underline{S}}$	=	k^{th} generalized factorial in several variables
$M_m(\underline{S})$	=	Set of all $m \times m$ matrices with entries in S
p	=	positive prime number
\mathbb{Z}_p	=	p -adic integers
$\text{ord}_p(n)$	=	p -adic ordinal (valuation) of $n \in \mathbb{Z}$.

1. INTRODUCTION

The term ‘*Fixed Divisor*’ is the English translation of the German word ‘*Fester Teiler*’ which seems to have been used for the first time by Nagell [79]. We start this section with the following definition

Math. classification: 11Sxx,11S05,13F20.

Keywords: Fixed divisors, Generalized factorials, Generalized factorials in several variables, Common factor of indices, Factoring of prime ideals, Integer valued polynomials.

DEFINITION 1.1. — Let A be a ring and $f(\underline{x}) \in A[\underline{x}]$ be a polynomial in n variables. Given $\underline{S} \subseteq A^n$, the fixed divisor of f over \underline{S} , denoted by $d(\underline{S}, f)$, is defined as the ideal of A generated by the values taken by f on \underline{S} .

In the case of a Unique Factorization domain (UFD) we can manipulate the Definition 1.1 as follows and we will observe that this definition is more useful than the above definition.

DEFINITION 1.2. — Let R be a UFD and $f(\underline{x}) \in R[\underline{x}]$. Given $\underline{S} \subseteq R^n$, then $d(\underline{S}, f)$ is defined as

$$d(\underline{S}, f) = g.c.d.\{f(\underline{a}) : \underline{a} \in \underline{S}\}.$$

Early scholars studied $d(\mathbb{Z}, f)$ (or $d(\mathbb{Z}^n, f)$) for a polynomial f with integer coefficients and so the term ‘fixed divisor of a polynomial’ was complete. But it can be seen that $d(S, f)$, where $S \subseteq \mathbb{Z}$ (or Dedekind domain) not only depends on f but also on the subset S (and the domain R). Thus, the term ‘fixed divisor of a polynomial over the set S in the ring R ’ (or $d(S, f)$ in R) seems more appropriate. However, for the sake of convenience, we will use the term ‘fixed divisor’, wherever the domain R and the subset \underline{S} will be clear from the context.

In section 2, we present formulae, methods of computation and various results related to fixed divisors. We first focus on the relation of the fixed divisor with generalized factorials in one and several variables depending on different notions of degrees of a multivariate polynomial. For instance, in one variable, we will see that the k th generalized factorial serves as the bound for fixed divisors of all primitive polynomials of degree k . We also present various methods of computation of fixed divisors in terms of generalized factorials.

In section 3, we define the notion of Fixed Divisor sequence and its relation with various sequences which have been studied recently in connection with the theory of integer-valued polynomials. Next, in section 4, we will see that, in the case of forms the bounds can be reduced further. We then present bounds for the fixed divisor of a polynomial involving its coefficients. At the end of this section we will see how rare it is for a polynomial $f \in \mathbb{Z}[x]$ to have $d(\mathbb{Z}, f) = 1$ along with the ideal of polynomials in $\mathbb{Z}[x]$ whose fixed divisor over \mathbb{Z} is a multiple of a given number d .

The study of fixed divisors is very closely related to the ring of integer-valued polynomials (see [25]) and has applications to the irreducibility of polynomials in this ring. In Section 5, we will present several approaches to test irreducibility of polynomials in $\text{Int}(S, R)$. In section 6, several concepts related to number fields and their connection with fixed divisors are given. At the end of this section, applications of the bound for the fixed divisor of a polynomial in terms of its coefficients to solve Selfridge’s question and its various generalizations is given. In Section 7, we define the notion of the fixed divisor of a polynomial in $M_m(R)[x]$. We will see that this definition is compatible with the recent generalization of $\text{Int}(M_m(R))$ and how different studies on this ring can be interpreted in terms of our definition.

2. FORMULAE AND BOUNDS FOR FIXED DIVISORS IN VARIOUS SETTINGS

The study of fixed divisors seems to have begun in 1896 with Hensel [64] (also see [41], p. 334), who gave a computational formula for $d(\underline{S}, f)$ in the case when $\underline{S} = \mathbb{Z}^n$.

THEOREM 2.1 (Hensel [64]). — *Let $f \in \mathbb{Z}[x]$ be a polynomial with degree m_i in x_i for $i = 1, 2, \dots, n$. Then $d(\mathbb{Z}^n, f)$ is equal to the g.c.d. of the values $f(r_1, r_2, \dots, r_n)$, where each r_i ranges over $m_i + 1$ consecutive integers.*

Thus, if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree k then

$$d(\mathbb{Z}, f) = (f(0), f(1), \dots, f(k)).$$

This is probably the simplest method to compute $d(\mathbb{Z}, f)$.

Pólya [90] (see also [81], Chapter III) in 1919 figured out a bound for $d(R, f)$ for a primitive polynomial $f \in R[x]$ of degree k , when R is the ring of integers of a number field. In this setting, he found a complete solution to the problem of determining the possible values of $d(R, f)$ for any primitive polynomial of degree k . For each pair of positive integers l and m , define

$$A(l, m) = \sum_{j \geq 1} \left\lfloor \frac{l}{m^j} \right\rfloor,$$

where $\lfloor \cdot \rfloor$ denotes the integer part. Pólya proved that for each nonzero prime ideal $P \subset R$, P^e divides $d(R, f)$ implies $e \leq A(k, N(P))$. On the other hand, for each $e \in \mathbb{N}$ with $e \leq A(k, N(P))$, he also constructed a primitive polynomial whose fixed divisor is exactly divisible by P^e . To be more precise, define

$$A_k = \prod_P P^{A(k, N(P))},$$

where the product is taken over all prime ideals of R for which $A(k, N(P)) \neq 0$ (which will be finitely many). Then, the results of Pólya remain true if we replace the ring of integers by any Dedekind domain with finite norm property. Hence, we can restate the above results as the following

THEOREM 2.2 (Pólya [90]). — *Let R be a Dedekind domain with finite norm property and $I \subseteq R$ be an ideal. Then I is the fixed divisor over R of some primitive polynomial of degree k in $R[x]$ iff I divides A_k .*

Observe that in the case $S = R = \mathbb{Z}$, $A_k = k!$. Thus, Pólya was the first one who gave a bound for the fixed divisor of a polynomial depending on its degree and he also studied the possible values taken by it in the case when R may not be \mathbb{Z} . Later Cahen [21] relaxed the condition of finite norm property in the above theorem.

Nagell [79] in 1919 studied fixed divisors in the multivariate case when $R = \mathbb{Z}$. He proved that for a primitive polynomial $f \in \mathbb{Z}[x]$ with partial degree m_i in each variable x_i , $d(\mathbb{Z}^n, f)$ divides $m_1! \cdots m_n!$ (this result is also a consequence of Theorem 2.1). He also gave a criteria for a number to be the fixed divisor of some polynomial generalizing Theorem 2.2 in this setting. This result was further generalized by Gunji & McQuillan (see Theorem 2.3). Gunji & McQuillan [56] studied $d(\underline{S}, f)$ in the case when \underline{S} is a product of arithmetical progressions in \mathbb{Z} .

THEOREM 2.3 (Gunji, McQuillan [56]). — *Let $A_i = \{sa_i + b_i\}_{s \in \mathbb{Z}}$, a_i and $b_i \in \mathbb{Z}$, be an arithmetic progression for $i = 1, 2, \dots, n$ and $A = A_1 \times A_2 \times \cdots \times A_n$. If f is a primitive polynomial in n variables with partial degree m_i in each variable x_i then $d(A, f)$ divides $\prod_{i=1}^n m_i! a_i^{m_i}$. Conversely, if d is any divisor of $\prod_{i=1}^n m_i! a_i^{m_i}$, then there exists a primitive polynomial $f \in \mathbb{Z}[x]$ with partial degree m_i in each variable x_i such that $d(A, f) = d$.*

They also proved that if $f \in \mathbb{Z}[\underline{x}]$ is primitive and $(a_1 a_2 \cdots a_n, f(b_1, \dots, b_n)) = 1$, then $d(A, f) = d(\mathbb{Z}^n, f)$. At the end of [56] they gave a relation connecting the fixed divisor of the product of polynomials to the product of their fixed divisors.

Gunji & McQuillan [57] also studied $d(S, f)$, where S is a coset of some ideal I in the ring of integers of a number field. They gave a formula for $d(S, f)$ in this setting and also proved that Theorem 2.2 remains true in this case, if A_k is replaced by $I^k A_k$. More precisely

THEOREM 2.4 (Gunji, McQuillan [57]). — *Let f be a primitive polynomial of degree k with coefficients in a number ring R and J be any coset of the ideal $I \subseteq R$. Then there exist $b_0, b_1, \dots, b_k \in R$ such that*

$$d(J, f) = (b_0 I^0 A_0, b_1 I^1 A_1, \dots, b_k I^k A_k).$$

The elements b_0, b_1, \dots, b_k depend only on J and are explicitly constructed (see Theorem 2.6 for the general construction). The last section of [57] was devoted to a different type of study which we will discuss in Section 6.

The general case was addressed by Bhargava [13] in 1998, where he found a formula for $d(S, f)$ for any polynomial f , in the case when R is any Dedekind domain, by introducing the famous notion of ‘Generalized Factorials’ $\nu_k(S)$ (see [12, 14]). For various definitions and a comprehensive introduction to these factorials, we highly recommend Chabert and Cahen [32] (also see [12, 14, 124]). For the sake of completeness we give the definition.

DEFINITION 2.5. — Let S be an arbitrary subset of a Dedekind domain R and $P \subset R$ be a fixed prime ideal. A P -ordering of S is a sequence a_0, a_1, a_2, \dots in S , such that for all $k \geq 1$, a_k is an element minimizing the highest power of P dividing $\prod_{i=0}^{k-1} (a_k - a_i)$.

Thus, a P -ordering gives rise to a sequence of ideals which are the minimized powers of P at each step. For an element $a \in R$, denote by $w_P(a)$ the highest power of P dividing a . The sequence $w_P(\prod_{i=0}^{k-1} (a_k - a_i)) = P^{e(k,P)}$ is said to be the P -sequence of S associated to the P -ordering a_0, a_1, a_2, \dots . Though a P -ordering is never unique, yet surprisingly, the associated P -sequence is independent of the choice of any P -ordering of S . The *generalized factorial of index $k \geq 1$* is defined as

$$\nu_k(S) = \prod_P P^{e(k,P)},$$

with the convention that $\nu_0(S) = R$. This sequence is a generalization to subsets S of R of the sequence A_k defined earlier for the whole ring R . Recall that $\text{Int}(S, R)$ is the ring of all polynomials of $\mathbb{K}[x]$ which maps S back to R , where \mathbb{K} is the field of fractions of R . These generalized factorials can also be defined by using the notion of $\text{Int}(S, R)$ as follows

$$\nu_k(S) = \{a \in R : a \text{Int}_k(S, R) \subseteq R[x]\},$$

where $\text{Int}_k(S, R)$ is the set of polynomials in $\text{Int}(S, R)$ of degree at most k and R is a Dedekind domain.

With all these definitions the work of Bhargava can be summarized as follows

THEOREM 2.6 (Bhargava [13]). — *Let S be an arbitrary subset of a Dedekind domain R . Then there exists a unimodular matrix $W_k(S)$ over R , such that if $f(x) = \sum_{i=0}^k c_i x^i$ is a primitive polynomial in $R[x]$, and*

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_k \end{pmatrix} = W_k(S) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_k \end{pmatrix}.$$

Then $d(S, f)$ is given by

$$d(S, f) = (b_0 \nu_0(S), b_1 \nu_1(S), \dots, b_k \nu_k(S)).$$

Hence, $d(S, f)$ divides $\nu_k(S)$. Conversely, if I is any ideal which divides $\nu_k(S)$, then there exists a primitive polynomial $f(x) \in R[x]$ such that $d(S, f) = I$.

In 2000, Bhargava [14] suggested a further generalization of factorials to the multivariate case and claimed that for a primitive multivariate polynomial of total degree k , this factorial gives bounds for fixed divisors as in previous theorems. In 2012, Evrard [44] pointed out that this factorial is not in increasing order and so cannot be a correct bound. She also proposed a new factorial which compensates the above drawback. For each $k \in \mathbb{N}$ and $\underline{S} \subseteq R^n$, this *factorial ideal of index k* is defined as

$$k!_{\underline{S}} = \{a \in R : a \text{Int}_k(\underline{S}, R) \subseteq R[\underline{x}]\},$$

where $\text{Int}_k(\underline{S}, R)$ is the set of polynomials in $\text{Int}(\underline{S}, R)$ of total degree at most k . This factorial can also be obtained by the analogue of P -ordering in several variables (see [44]). Using this factorial Evrard proved

THEOREM 2.7 (Evrard [44]). — *Let f be a primitive polynomial of total degree k in n variables and $\underline{S} \subseteq R^n$, then $d(\underline{S}, f)$ divides $k!_{\underline{S}}$ and this is sharp.*

The sharpness of the statement denotes (and will denote in the future) the existence of a polynomial f satisfying the conditions of the theorem such that $d(\underline{S}, f) = k!_{\underline{S}}$. Observe that in the case of multivariate polynomials, Theorem 2.3 and Theorem 2.7 take into account different notions of degree and derive different bounds for fixed divisors. We can combine both of these notions of degrees to construct a new bound which is sharper than both of these bounds.

Define the *degree* of a polynomial $f \in \mathbb{K}[\underline{x}]$ as a vector $\mathbf{m} \in \mathbb{W}^n$ in which i^{th} component denotes the partial degree of f in x_i . We will say that f is of *type* (\mathbf{m}, k) if degree of f is \mathbf{m} and total degree is k . Further we define $\mathbf{m} \leq \mathbf{n}$ for $\mathbf{m}, \mathbf{n} \in \mathbb{W}^n$, if each component of \mathbf{m} is less than or equal to the corresponding component of \mathbf{n} .

For $\mathbf{m} \in \mathbb{W}^n, k \in \mathbb{W}$, and $\underline{S} \subseteq R^n$, where R is a Dedekind domain, define

$$\text{Int}_{\mathbf{m}, k}(\underline{S}, R) = \{f \in \text{Int}(\underline{S}, R) : \text{degree of } f \leq \mathbf{m} \text{ and total degree of } f \leq k\}.$$

Rajkumar, Reddy and Semwal [91] defined the *generalized factorial of index k with respect to \mathbf{m}* as follows

$$\Gamma_{\mathbf{m}, k}(\underline{S}) = \{a \in R : a \text{Int}_{\mathbf{m}, k}(\underline{S}, R) \subseteq R[\underline{x}]\}.$$

The function defined above satisfies all the important properties of factorials (see Chabert [31]) and hence generalizes Bhargava's factorials in several variables. For a polynomial of type (\mathbf{m}, k) , the authors proved the following analogue of Theorem 2.2.

THEOREM 2.8 (Rajkumar, Reddy and Semwal [91]). — *Let R be a Dedekind domain and $f \in R[\underline{x}]$ be a primitive polynomial of type (\mathbf{m}, k) , then $d(\underline{S}, f)$ divides $\Gamma_{\mathbf{m}, k}(\underline{S})$ and this is sharp. Conversely, for any divisor I of $\Gamma_{\mathbf{m}, k}(\underline{S})$, there exists a primitive polynomial $f \in R[\underline{x}]$ of type (\mathbf{m}, k) such that $d(\underline{S}, f) = I$.*

Let $\underline{S} = S_1 \times S_2 \times \cdots \times S_n$ be a subset of R^n , where each S_i is a subset of the Dedekind domain R . For a given n -tuple $(i_1, i_2, \dots, i_n) = \mathbf{i}$, denote its sum of components by $|\mathbf{i}|$. For such \underline{S} , the authors proved that

$$\Gamma_{\mathbf{m}, k}(\underline{S}) = \operatorname{lcm}_{\mathbf{0} \leq \mathbf{i} \leq \mathbf{m}, |\mathbf{i}| \leq k} \mathbf{i}!_{\underline{S}},$$

where $\mathbf{i}!_{\underline{S}}$ denotes $i_1!_{S_1} \cdots i_n!_{S_n}$ for a given tuple \mathbf{i} . In this setting, the authors proved the following analogue of Theorem 2.6.

THEOREM 2.9 (Rajkumar, Reddy and Semwal [91]). — *Let $f \in R[\underline{x}]$ be a primitive polynomial of type (\mathbf{m}, k) and \underline{S} be the Cartesian product of sets as above. Then there exist elements $b(\mathbf{0}), \dots, b(\mathbf{i}), \dots, b(\mathbf{j})$ in R which generate the unit ideal and depend on \underline{S} , such that*

$$d(\underline{S}, f) = (b(\mathbf{0})\Gamma_{\mathbf{0}, 0}(\underline{S}), \dots, b(\mathbf{i})\Gamma_{\mathbf{i}, |\mathbf{i}|}(\underline{S}), \dots, b(\mathbf{j})\Gamma_{\mathbf{j}, |\mathbf{j}|}(\underline{S})).$$

Here the indices $\mathbf{i} \in \mathbb{W}^n$ run over all $\mathbf{i} \leq \mathbf{m}$, $|\mathbf{i}| \leq k$ and \mathbf{j} is one of the indices satisfying $|\mathbf{j}| = k$. If we relax the condition of total degree in the above theorem, we get (a generalization of) Bhargava's work in the multivariate Cartesian product case as follows.

COROLLARY 2.10 (Bhargava [13]). — *Let $f \in R[\underline{x}]$ be a primitive polynomial of degree \mathbf{m} . Then there exist elements $b(\mathbf{0}), \dots, b(\mathbf{i}), \dots, b(\mathbf{m})$ in R which generate the unit ideal and depends on \underline{S} such that*

$$d(\underline{S}, f) = (b(\mathbf{0})\mathbf{0}!_{\underline{S}}, \dots, b(\mathbf{i})\mathbf{i}!_{\underline{S}}, \dots, b(\mathbf{m})\mathbf{m}!_{\underline{S}}).$$

Hence, $d(\underline{S}, f)$ divides $\mathbf{m}!_{\underline{S}}$ and this is sharp. Conversely, for each I dividing $\mathbf{m}!_{\underline{S}}$, there exists a primitive polynomial f of degree \mathbf{m} with $d(\underline{S}, f) = I$.

Corollary 2.10 and Theorem 2.7 give different bounds for fixed divisors and these bounds are not comparable in general. However, the factorial introduced in [91] always gives a stronger result and may not be equal to the *g.c.d.* of $k!_{\underline{S}}$ and $\mathbf{m}!_{\underline{S}}$, as the following example suggests.

Example 2.11. — If $f \in \mathbb{Z}[\underline{x}]$ is a primitive polynomial of type $((2, 2), 3)$, then we have the following bounds for $d(\mathbb{Z} \times 2\mathbb{Z}, f)$:

- (1) Theorem 2.7 gives $3!_{\mathbb{Z} \times 2\mathbb{Z}} = 2^3 3!$
- (2) Theorem 2.6 (or Theorem 2.3) gives $2!_{\mathbb{Z}} 2!_{2\mathbb{Z}} = 2! 2^2 2!$
- (3) Theorem 2.9 gives $\Gamma_{(2,2),3}(\mathbb{Z} \times 2\mathbb{Z}) = 2^2 2!$.

Hence, the polynomial $\frac{f}{2^4}$ cannot be integer-valued since 2^4 exceeds $\Gamma_{(2,2),3}(\mathbb{Z} \times 2\mathbb{Z})$.

In [91], it was also shown that for every $\underline{a} \in \underline{S}$ there exists an element $\underline{b} \in R^n$, such that $f(\underline{a})$ and $f(\underline{b})$ completely determine $d(\underline{S}, f)$.

3. FIXED DIVISOR SEQUENCES AND RELATED NOTIONS

In the case when $S \subseteq R$ contains a sequence which is a P -ordering for all prime ideals P of the domain (called a *Simultaneous P -ordering*), then $d(S, f)$ is determined by the f -images of the first $k + 1$ consecutive terms of this sequence, where k is the degree of f .

The notion of simultaneous P -ordering was given by Mulay [75] before Bhargava. He denoted this sequence by the term ‘*special sequence*’. He also constructed a sequence of ideals which are very closely connected to Bhargava’s factorials. He subsequently generalized this sequence of ideals to the case of several variables and these ideals are closely connected to Evrard’s factorials (see [76]). The beauty of this sequence of ideals is that it does not require R to be a Dedekind domain. These can be defined in any domain (which is not a field). Though the question of finding this type of ordering remains open, some interesting results can be seen in [1, 5, 65, 124]. Mulay [77] also found special types of polynomials which map special sequences back to special sequences.

We now introduce the notion of the fixed divisor sequence which is also related to that of simultaneous P -ordering. We denote by P_k , the set of all polynomials of $R[x]$ of total degree k . For a given subset $\underline{S} \subseteq R^n$, a *fixed divisor sequence (FD sequence)* is defined as follows.

DEFINITION 3.1. — For a given subset $\underline{S} \subseteq R^n$, a sequence $\underline{a}_0, \underline{a}_1, \dots$ of distinct elements of \underline{S} is said to be a fixed divisor sequence (FD sequence) if for every $k \geq 1, \exists l \in \mathbb{N}$, such that for every polynomial $f \in P_k$, we have

$$d(\underline{S}, f) = (f(\underline{a}_0), f(\underline{a}_1), \dots, f(\underline{a}_l)),$$

and no proper subset of $\{\underline{a}_0, \underline{a}_1, \dots, \underline{a}_l\}$ determines $d(\underline{S}, f)$ of all $f \in P_k$.

Such a sequence may not always exist and sometimes may contain only finitely many elements. The smallest such number l , which gives fixed divisors of degree k polynomials is denoted by l_k . This number depends on \underline{S} and the sequence chosen, which will be clear from the context. In the case when $S = R = \mathbb{Z}$, we have $l_k = k$ by Theorem 2.1. Thus, a FD sequence gives rise to a sequence of numbers (l_1, l_2, \dots) called the *sequence of lengths* corresponding to the given FD sequence. Volkov and Petrov [115] conjectured that in the case of $S = R = \mathbb{Z}[i]$, l_k grows as $\frac{\pi}{2}k + o(k)$ and asymptotically sharp example is realized on the set of integer points inside the circle of radius $\sqrt{n/2} + o(\sqrt{n})$. Recently, Byszewski, Fraczyk and Szumowicz [20] found the growth of l_k in the general case. They proved that in the case when $S = R$, where R is any Dedekind domain, we have $l_k \leq k + 1$, contradicting the conjecture.

With the above definitions, the following question is interesting.

QUESTION. — *What are the subsets $\underline{S} \subseteq R^n$, for which a FD sequence exist?*

Note that whenever a subset of a Dedekind domain admits a simultaneous P -ordering, then that sequence is itself a FD sequence, but not conversely. A FD sequence is a simultaneous P -ordering iff $l_k = k$.

In the last few decades two more interesting sequences emerged in the study of integer valued polynomials, which are known as Newton sequence and Schinzel sequence and are defined as follows.

DEFINITION 3.2. — Let $\{u_n\}_{n \geq 0}$ in R be a sequence.

(i) If for each $n \geq 0$ and each polynomial $f \in \mathbb{K}[x]$ of degree $m \leq n$, we have

$$f \in \text{Int}(R) \iff f(u_r) \in R \quad \forall r \leq n,$$

then $\{u_n\}_{n \geq 0}$ is said to be a Newton sequence.

(ii) If for each ideal I , the first $N(I)$ terms of the sequence $\{u_n\}_{n \geq 0}$ represent all residue classes modulo I , then it is said to be a Schinzel sequence.

For some interesting results on these sequences we refer to [2, 20, 23, 66, 117, 118]. A Newton sequence can be a Schinzel sequence (see for instance [4, 3]) and vice-versa. In the case of a Dedekind domain, a Newton sequence is nothing but a simultaneous P -ordering and hence a FD sequence.

Another notion which is related to FD sequences is that of n -universal sets (see [27, 115]). A finite subset $S \subset R$ is said to be a n -universal set if for every polynomial $f \in \mathbb{K}[x]$ of degree at most n , $f \in \text{Int}(R)$ if and only if $f(S) \subset R$. The first l_n terms of all FD sequences are n -universal sets for all $n \geq 1$.

An R -module basis of $\text{Int}(S, R)$ is said to be *regular basis* if it contains one and only one polynomial of each degree. Its study was begun with Pólya [90] and Ostrowski [83] in 1919. After their seminal work, the next major step in this direction was taken by Zantema [125]. He introduced the name *Pólya fields* for those number fields \mathbb{K} , such that $\text{Int}(R)$ admits a regular basis where R is the ring of integers of \mathbb{K} . He proved that cyclotomic fields are Pólya fields. The study of Pólya fields has now become very important in the theory of integer valued polynomials. Some interesting results can be seen in [63, 67, 68, 70, 69, 107, 108, 126]. A sufficient condition for a number field to be a Pólya field can be obtained from FD sequences and fixed divisors as follows.

Let R be a number ring in which a FD sequence a_0, a_1, \dots exists. Define a sequence of polynomials $\{F_j\}_{j \geq 0}$ corresponding to this sequence by

$$F_j(x) = (x - a_0)(x - a_1) \dots (x - a_{j-1})$$

with $F_0 = 1$. It can be seen that $\text{Int}(R)$ admits a regular basis if $d(R, F_i) = (F_i(a_i))$ for all $i \geq 1$. This result can be extended to the case of any subset $\underline{S} \subseteq R^n$, for which an FD sequence exists.

Take the unitary monomial basis of $\mathbb{K}[\underline{x}]$ and place a total order on it which is compatible with the total degree. Thus, the monomials are arranged in a sequence $(p_j)_{j \geq 0}$ with $p_0 = 1$ and total degree of p_i is less than or equal to that of p_j if $i < j$.

For any sequence of elements $\underline{b}_0, \underline{b}_1, \dots, \underline{b}_r$ in R^n , define

$$\Delta(\underline{b}_0, \underline{b}_1, \underline{b}_2, \dots, \underline{b}_r) = \det(p_j(\underline{b}_i))_{0 \leq i, j \leq r}.$$

With all these notations we have the following theorem.

THEOREM 3.3. — Let $\underline{S} \subseteq R^n$ be a subset and $\{\underline{a}_i\}_{i \geq 0}$ be a FD sequence of \underline{S} . If for all $i \geq 1$, $d(R, F_i) = (F_i(\underline{a}_i))$, where $F_r(\underline{x}) = \Delta(\underline{a}_0, \dots, \underline{a}_{r-1}, \underline{x})$ with $F_0(\underline{x}) = 1$, then, an R -module basis for $\text{Int}(\underline{S}, R)$ is given by

$$\frac{F_r(\underline{x})}{F_r(\underline{a}_r)}, \quad r = 0, 1, \dots$$

4. RESULTS ON FIXED DIVISORS IN SOME SPECIAL CASES

The study of fixed divisors of forms (homogeneous polynomials with integer coefficients) was initiated by Nagell in 1919. Nagell proved the following theorem for forms in two variables.

THEOREM 4.1 (Nagell [79]). — *For the polynomial*

$$f(x, y) = y^{m-1}x(x+y)(x+2y) \cdots (x+y(m-1)),$$

$d(\mathbb{Z}^2, f)$ is multiple of $m!$.

Schinzel [100] continued the legacy of Nagell on the fixed divisor of forms. He started this work by giving bounds for fixed divisors in various cases. We recall that for a polynomial $f(\underline{x}) \in \mathbb{Z}[\underline{x}]$, $d(\mathbb{Z}^n, f)$ is the greatest positive integer dividing $f(\underline{a})$ for all $\underline{a} \in \mathbb{Z}^n$. For the work of Schinzel we fix the following notations.

$$S_{k,n} = \{f \in \mathbb{Z}[\underline{x}] : f \text{ is a homogeneous primitive polynomial of total degree } k\},$$

$$S_{k,n}^1 = \{f \in S_{k,n} : f \text{ splitting over } \mathbb{Z}\},$$

$$S_{k,n}^0 = \{f \in S_{k,n} : f \text{ splitting over } \mathbb{C}\},$$

$$D_{k,n} = \max_{f \in S_{k,n}} d(\mathbb{Z}^n, f), \text{ and } D_{k,n}^1 = \max_{f \in S_{k,n}^1} d(\mathbb{Z}^n, f).$$

With these notations Schinzel gave the following bound.

THEOREM 4.2 (Schinzel [100]). — *For all $f \in S_{k,n}^0$ and for all primes p*

$$\text{ord}_p d(\mathbb{Z}^n, f) \leq \text{ord}_p \left(\left(p \left\lfloor \frac{(p^{n-1} - 1)k}{p^n - 1} \right\rfloor \right)! \right),$$

$$\text{ord}_p D_{k,2}^1 \geq \text{ord}_p \left(\left(p \left\lfloor \frac{k}{p+1} \right\rfloor \right)! \right) \quad \text{and}$$

$$\text{ord}_p D_{k,n}^1 \geq (p^{n-1} - 1)q^{n-1} \text{ord}_p((pq)!) + \text{ord}_p \left(\left(p \left\lfloor \frac{k - (p^n - 1)q^n}{p+1} \right\rfloor \right)! \right) \text{ for } n > 2,$$

where $q = \left\lfloor \sqrt[n]{\frac{k}{p^n - 1}} \right\rfloor$.

This theorem also answered a question asked by Nagell [79] in 1919. Since $S_{k,2}^1 \subseteq S_{k,2}^0$, the results of the above theorem can be combined to get $D_{k,2} = D_{k,2}^1$. He also proved that $D_{k,n}$ divides $(k-1)!$ and becomes equal to D_{k,n_k} for all integers $k \geq 4$ and $n \geq n_k$, where $n_k = k - \text{ord}_2 \left(\left(2 \left\lfloor \frac{k}{3} \right\rfloor \right)! \right)$. If $k \leq 6$ and $n \geq 2$, then $D_{k,n}$ is equal to $D_{k,2}$, though we always have $D_{9,3}^1 = D_{9,2}^1$. The growth of $D_{k,n}$ is similar to that of the factorial, i.e., $\log D_{k,n} = k \log k + O(k)$. With these results in hand, Schinzel conjectured

CONJECTURE 4.3 (Schinzel [100]). — *For all positive integers k and n , we always have $D_{k,n} = D_{k,n}^1$.*

Schinzel proved this conjecture for $k \leq 9$ and for all n , but the general case remains open. One more interesting result in the same article is

THEOREM 4.4 (Schinzel [100]). — *Let $k_n(m)$ be the least integer k such that $m! \mid D_{k,n}$. Then, for all n , the limit $l_n = \lim_{m \rightarrow \infty} \frac{k_n(m)}{m}$ exists and satisfies*

$$l_n \leq \frac{2^n - 1}{2^n - 2},$$

where equality holds if Conjecture 4.3 is true.

Subsequently, in his next article Schinzel [99] established upper and lower bounds on $D_{k,n}^1$.

THEOREM 4.5 (Schinzel [100]). — *For all integers $n \geq 2$ and $k \geq 2^n$, we have*

$$\log D_{k,n}^1 = \log(k-1)! + \frac{\zeta'(n)}{\zeta(n)}k + e(k, n),$$

where $e(k, n)$ is the error term.

So far we have seen bounds for fixed divisors depending only on degree. We can also get bounds for fixed divisors depending on the coefficients of the polynomial. Vajaitu [111] (also see [110]) in 1997 studied the relation between bounds for the fixed divisor of a polynomial and its coefficients. For every primitive polynomial $f = \sum_{i=0}^k a_i x^i \in R[x]$, when R is a Dedekind domain with finite norm property, Vajaitu proved that the cardinality of the ring $R/d(R, f)$ cannot exceed the cardinality of $R/(k!a_0)^{k2^{k+1}}$. In the case when $R = \mathbb{Z}$, he gave the following sharp bound for the fixed divisor.

THEOREM 4.6 (Vajaitu [111]). — *Let $f \in \mathbb{Z}[x]$ be a primitive polynomial, p be a prime number dividing $d(\mathbb{Z}, f)$ and $|f|$ denote number of non-zero coefficients of f . Then $p > \frac{1}{2} + \sqrt{n}$ implies $\text{ord}_p(d(\mathbb{Z}, f)) \leq |f| - 1$. Hence, we have*

$$d(\mathbb{Z}, f) \leq a \prod_{\substack{p < \frac{1}{2} + \sqrt{n} \\ p = \text{prime}}} p^{\text{ord}_p(k!)} \prod_{\substack{\frac{1}{2} + \sqrt{n} < p \leq n \\ p = \text{prime}}} p^{\min(|f|-1, \lfloor \frac{n}{p} \rfloor)},$$

where a is the leading coefficient of f .

The bound for $d(\mathbb{Z}, f)$ in the above theorem remains true for non-primitive polynomials too. This theorem was further studied by Evrard and Chabert [34], which we present here in the local case. They extended this result to the global case and also to the case of \mathbb{Z} .

THEOREM 4.7 (Evrard and Chabert [34]). — *Let V be a Discrete Valuation Domain with valuation ν , maximal ideal M and finite residue field of characteristic p . Let $S \subseteq V$ contain at least $r \geq 2$ distinct classes modulo M and $f = \sum_{i=0}^k a_i x^i \in \mathbb{K}[x]$ be a polynomial of degree k . If $k \leq p(r-1) + 1$ then*

$$\nu(d(S, f)) < \nu(f) + \nu_M(f),$$

where $\nu(f) = \inf_{0 \leq i \leq k} \nu(a_i)$ and $\nu_M(f) = |\{i : \nu(a_i) = \nu(f)\}|$. Moreover, the inequality also holds as soon as

- (1) $k < pr$ when $M \not\subseteq S$,
- (2) $k \leq pr$ when $\emptyset \neq S \cap M \neq M$.

Turk [109] in 1986 studied probabilistic results on fixed divisors in the case when $R = \mathbb{Z}$. For $f = \sum_{i=0}^k a_i x^i \in \mathbb{Z}[x]$, define its height by $h(f) = \max_{0 \leq j \leq n} |a_j|$. For any subset T of $\mathbb{Z}[x]$ define the probability that an $f \in \mathbb{Z}[x]$ of degree $\leq k$ belongs to T as

$$\text{Prob}(f \in T : \deg(f) \leq k) = \lim_{h \rightarrow \infty} \frac{|\{f \in T : \deg(f) \leq k, h(f) \leq h\}|}{|\{f \in \mathbb{Z}[x] : \deg(f) \leq k, h(f) \leq h\}|},$$

provided the limit exist. Here, $|A|$ for a set A denotes its cardinality. Turk's result can be stated as

THEOREM 4.8 (Turk [109]). — *Let $f \in \mathbb{Z}[x]$ be a polynomial of degree at most k and μ be the Möbius function. Then the probability of $d(\mathbb{Z}, f)$ to be equal to d , denoted by $P(d, k)$, is given by*

$$P(d, k) = \sum_{n=1}^{\infty} \mu(n) \prod_{i=0}^k \frac{(i!, nd)}{nd}.$$

From this result, it follows that $P(1, k) = \prod_p (1 - p^{-\min(k+1, p)})$. Letting k tend to infinity, we get the following corollary.

COROLLARY 4.9. — *The probability for a polynomial $f \in \mathbb{Z}[x]$ to have $d(\mathbb{Z}, f) = 1$ is $\prod_p (1 - p^{-p})$, which is approximately 0.722.*

Hence, we can conclude that 28 percent of the polynomials in $\mathbb{Z}[x]$ have fixed divisors greater than 1. Turk also extended this result to several variables and proved that this probability is equal to $\prod_p (1 - p^{-p^n})$, where n is number of variables.

Peruginelli [86] worked on the ideal of the polynomials in $\mathbb{Z}[x]$ whose fixed divisor over \mathbb{Z} is a multiple of a given number. He completely determined this ideal. Recall that the prime ideals of $\text{Int}(\mathbb{Z})$ which lie over a prime $p \in \mathbb{Z}$, are of the form

$$\mathfrak{M}_{p, \alpha} = \{f \in \text{Int}(\mathbb{Z}) : f(\alpha) \in p\mathbb{Z}_p\},$$

where $\alpha \in \mathbb{Z}_p$. It can be shown that for $f \in \mathbb{Z}[x]$ we have $d(\mathbb{Z}, f) = \bigcap_p d(\mathbb{Z}_p, f)$ and if p^e is the highest power of p dividing $d(\mathbb{Z}, f)$ then $d(\mathbb{Z}_p, f) = p^e \mathbb{Z}_p$ (see [86, 57]).

THEOREM 4.10 (Peruginelli [86]). — *Let $p \in \mathbb{Z}$ be a prime and $n \in \mathbb{W}$ such that $p \geq n$, and $f(x) = \prod_{i=0}^{p-1} (x - i)$. Let I_{p^e} be the ideal of polynomials in $\mathbb{Z}[x]$ whose fixed divisor is a multiple of p^e for some $e \in \mathbb{W}$ that is $I_{p^e} = \bigcap_{\alpha \in \mathbb{Z}_p} (\mathfrak{M}_{p, \alpha}^e \cap \mathbb{Z}[x])$. Then we have*

$$I_{p^n} = (p, f)^n.$$

The other case, i.e., when $p < n$, was handled by the construction of certain types of polynomials. While the problem of determining the ideal I_{p^n} was completely solved by Peruginelli, we would like to point out that he was not the first to study this ideal. Various scholars have worked with this ideal in different contexts (see [12, 38, 54, 92, 102, 101, 122]). Note that, if we have determined the ideal of polynomials in $(\mathbb{Z}/p^n\mathbb{Z})[x]$ which maps each element of $\mathbb{Z}/p^n\mathbb{Z}$ to zero, then we can easily determine I_{p^n} . Bandini [10] studied I_{p^n} as a kernel of the natural map from $\mathbb{Z}[x]$ to the set of all functions of $\mathbb{Z}/p^n\mathbb{Z}$ to itself.

5. APPLICATIONS OF FIXED DIVISORS IN IRREDUCIBILITY

It is well known that when R is a Unique Factorization Domain (UFD) then a primitive polynomial $f \in \mathbb{K}[x]$ is irreducible in $\mathbb{K}[x]$ iff f is irreducible in $R[x]$. This result is not true in general if $\mathbb{K}[x]$ is replaced by $\text{Int}(R)$, i.e., a primitive irreducible polynomial in $R[x]$ may be reducible in $\text{Int}(R)$. For instance, consider the irreducible primitive polynomial $f = x^2 + x + 4 \in \mathbb{Z}[x]$ which can be factorized as $\frac{x^2+x+4}{2} \times 2$ in the ring $\text{Int}(\mathbb{Z})$ (note that $\frac{x^2+x+4}{2}$ maps \mathbb{Z} back to \mathbb{Z}). Since the

only units in $\text{Int}(\mathbb{Z})$ are ± 1 (see [24]), the factorization is proper. Thus, it is natural to ask the following question: *for an irreducible polynomial $f \in R[x]$, where R is a UFD, what are the elements $d \in R$ such that $\frac{f}{d} \in \text{Int}(R)$ (or $\text{Int}(S, R)$)?*

The role of the fixed divisor in answering this question was brought to the fore by Chapman and McClain [35] in 2005.

THEOREM 5.1 (Chapman and McClain [35]). — *Let R be a unique factorization domain and $f(x) \in R[x]$ be a primitive polynomial. Then $f(x)$ is irreducible in $\text{Int}(S, R)$ if and only if $f(x)$ is irreducible in $R[x]$ and $d(S, f) = 1$.*

Their next result addressed the case when the fixed divisor may not be one.

THEOREM 5.2 (Chapman and McClain [35]). — *Let R be a unique factorization domain and $f(x) \in R[x]$ be a primitive polynomial. Then the following statements are equivalent.*

- (1) $\frac{f(x)}{d(S, f)}$ is irreducible in $\text{Int}(S, R)$.
- (2) Either $f(x)$ is irreducible in $R[x]$ or for every pair of non-constant polynomials $f_1(x), f_2(x)$ in $R[x]$ with $f(x) = f_1(x)f_2(x)$, $d(S, f) \nmid d(S, f_1)d(S, f_2)$.

Theorem 5.2 becomes more practical in the study of irreducibility in $\text{Int}(S, R)$, if we classify those polynomials whose fixed divisor of product is equal to the product of their fixed divisors. We ask this as an open question.

QUESTION. — *What are the subsets S of a Dedekind domain R and the sets of polynomials $f_1, f_2, \dots, f_r \in R[x]$ such that*

$$d(S, f_1 f_2 \dots f_r) = d(S, f_1) d(S, f_2) \dots d(S, f_r) ?$$

A polynomial in $\text{Int}(R)$ which is irreducible in $\mathbb{K}[x]$, may be reducible in $\text{Int}(R)$. Cahen and Chabert [24] proved that a polynomial $f \in \text{Int}(R)$, which is irreducible in $\mathbb{K}[x]$, is irreducible in $\text{Int}(R)$ iff $d(R, f) = R$.

There exist domains in which some elements can be written as product of irreducibles in various ways and the number of irreducibles may not be the same in each factorization. More precisely, if $a \in R$, then it may have two factorizations into irreducibles $a = a_1 a_2 \dots a_r = b_1 b_2 \dots b_s$, such that $r > s$. The supremum of $\frac{r}{s}$ over all factorizations of a , when a varies in R is said to be the *elasticity* of R [114]. The study of elasticity is very broad and we refer to [6] for a survey. Though the elasticity of \mathbb{Z} is 1, but that of $\text{Int}(\mathbb{Z})$ is infinite (see [24, 26]). So if we take any $f \in \mathbb{Z}[x]$, it may not factor uniquely in $\text{Int}(\mathbb{Z})$. For a given polynomial $f \in \mathbb{Z}[x]$, one may ask whether its factorization is unique in $\text{Int}(\mathbb{Z})$ or not? For example, if $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial with $d(\mathbb{Z}, f) = 1$, then from Theorem 5.1, f is irreducible in $\text{Int}(\mathbb{Z})$. More generally we have

THEOREM 5.3 (Chapman and McClain [35]). — *Let R be a unique factorization domain and $f(x) \in R[x]$ be a polynomial with $d(S, f) = 1$, then f factors uniquely as a product of irreducibles in $\text{Int}(S, R)$.*

Chapman and McClain proved another interesting result: for every m and $n \in \mathbb{N}$, there are infinitely many irreducible polynomials $f(x) \in \mathbb{Z}[x]$ with leading coefficient n for which $d(\mathbb{Z}, f) = m$.

We have seen that a given polynomial $f \in \text{Int}(\mathbb{Z})$ may not have the same number of irreducibles in its factorizations in $\text{Int}(\mathbb{Z})$. One question is very pertinent here:

suppose we have two numbers m and n , does there exist a polynomial in $\text{Int}(\mathbb{Z})$ which factors only in two ways and has the number of irreducibles m and n in these factorizations? Frisch [50] answered this question in the general setting by using the fixed divisor.

THEOREM 5.4 (Frisch [50]). — *Let m_1, m_2, \dots, m_n be natural numbers greater than 1, then we can construct a polynomial $f(x) \in \text{Int}(\mathbb{Z})$ having exactly n different factorizations into irreducibles in $\text{Int}(\mathbb{Z})$, with the length of these factorizations equal to m_1, m_2, \dots, m_n , respectively.*

Fixed divisors also enable us to understand the behavior of irreducibility in special type of rings (pullback rings) studied by Boynton [19] (see also [17, 18]). Boynton [19] extended the notion of fixed divisors to these types of rings and found their applications in understanding the behavior of irreducibility.

Another approach in testing irreducibility of a polynomial from $\text{Int}(\mathbb{Z})$ by using its fixed divisor was given by Peruginelli [87]. We will first recall a few definitions. Let $f \in \text{Int}(\mathbb{Z})$ be any polynomial. We will call f *image primitive*, *p -image primitive* and *p -primitive*, whenever $d(\mathbb{Z}, f) = 1$, p does not divide $d(\mathbb{Z}, f)$ and p does not divide content of f , respectively. Since Peruginelli's work is confined to the case when $S = R = \mathbb{Z}$, we state a few classical ways of computing $d(\mathbb{Z}, f)$.

THEOREM 5.5 (See [7, 26]). — *For*

$$f = b_0 + b_1x + b_2x(x-1) + \dots + b_kx(x-1)\dots(x-k+1) \in \mathbb{Z}[x],$$

all of the following are equal to $d(\mathbb{Z}, f)$:

- (1) $\text{g.c.d.}\{f(0), f(1), \dots, f(k)\}$,
- (2) $\sup\{n \in \mathbb{Z} : \frac{f(x)}{n} \in \text{Int}(\mathbb{Z})\}$,
- (3) $(b_00!, b_11!, \dots, b_kn!)$,
- (4) $(\Delta^0 f(0), \Delta^1 f(0), \dots, \Delta^n f(0))$.

Here Δ is the forward difference operator and is defined as $\Delta f(x) = f(x+1) - f(x)$.

Using the fact that \mathbb{Z} is a UFD, every polynomial f of $\mathbb{Q}[x]$ can be written as $f(x) = \frac{g(x)}{d}$, where $g \in \mathbb{Z}[x]$ and $d \in \mathbb{Z}$. Peruginelli considered two cases, i.e., when d is a prime number and square free number, respectively.

We start with the case when d is a prime number. We have

$$f(x) = \frac{g(x)}{p} = \frac{\prod_{i \in I} g_i(x)}{p},$$

where $g_i(x)$ are irreducibles in $\mathbb{Z}[x]$. To give the irreducibility criteria in this case, we will need a few definitions.

DEFINITION 5.6. — Let $g \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}$ be a prime. Define

$$C_{p,g} = \{j \in \{0, 1, \dots, p-1\} : p \mid g(j)\}.$$

DEFINITION 5.7. — Let $\mathcal{G} = \{g_i(x)\}_{i \in I}$ be a set of polynomials in $\mathbb{Z}[x]$ and $p \in \mathbb{Z}$ be a prime. For each $i \in I$, we set $C_i = C_{p,g_i}$. A p -covering for \mathcal{G} is a subset J of I such that

$$\bigcup_{i \in J} C_i = \{0, 1, \dots, p-1\}.$$

We say that J is minimal if no proper subset J' of J has the same property.

Now, the irreducibility criteria is given by the following lemma.

LEMMA 5.8 (Peruginelli [87]). — *Let $f(x) = \frac{g(x)}{p} = \frac{\prod_{i \in I} g_i(x)}{p}$, where $g_i(x)$ are irreducible in $\mathbb{Z}[x]$, then the following are equivalent :*

- (1) f is irreducible in $\text{Int}(\mathbb{Z})$,
- (2) $d(\mathbb{Z}, g) = p$,
- (3) I is a minimal p -covering.

Next, Peruginelli generalized the notion of p -covering to the case when we have more than one prime. He considered the case when d is a square free number.

We end this section with the following question.

QUESTION. — *What is the analogue of Lemma 5.8 in the case when d is not square free?*

6. APPLICATIONS OF FIXED DIVISORS IN NUMBER FIELDS

The first application of this section is from Gunji & McQuillan [57], where a new concept was introduced, which encapsulated the relationship between the arithmetic properties of an extension of a number field and the fixed divisors of certain minimal polynomial.

Let \mathbb{K} be an algebraic number field of finite degree and \mathbb{L} be a finite algebraic extension of \mathbb{K} of degree m . Let $\mathcal{O}_{\mathbb{K}}$ and $\mathcal{O}_{\mathbb{L}}$ be the ring of integers of \mathbb{K} and \mathbb{L} respectively. Let $S(\mathbb{L}|\mathbb{K})$ be the set of elements $a \in \mathcal{O}_{\mathbb{L}}$ such that $\mathbb{L} = \mathbb{K}(a)$ and $f_a(x)$ denote the minimal monic polynomial of a with coefficients in $\mathcal{O}_{\mathbb{K}}[x]$.

DEFINITION 6.1. — For a pair of number fields \mathbb{K} and \mathbb{L} , define $\mathfrak{J}(\mathbb{L}|\mathbb{K})$ to be the lcm of $d(\mathcal{O}_{\mathbb{K}}, f_a)$, where a varies over $S(\mathbb{L}|\mathbb{K})$.

With these terms, Gunji & McQuillan proved several interesting results like

- (i) there exists $a \in \mathcal{O}_{\mathbb{L}}$ such that $d(\mathcal{O}_{\mathbb{K}}, f_a) = \mathfrak{J}(\mathbb{L}|\mathbb{K})$, and
- (ii) $\mathfrak{J}(\mathbb{K}|\mathbb{Q})^m \mid \mathfrak{J}(\mathbb{L}|\mathbb{Q})$.

Building on these results, Ayad and Kihel [9] asked the following questions.

QUESTION (Ayad and Kihel [9]). — *Let $\omega_1, \dots, \omega_n$ be an integral basis of \mathcal{O}_K . Consider all the elements of the form $b = \sum_{i=1}^n x_i \omega_i$, where $x_i \in \{0, 1, \dots, p^e - 1\}$ for $e \leq \text{ord}_p(\mathfrak{J}(\mathbb{K}|\mathbb{Q}))$, such that p^e divides $d(\mathbb{Z}, f_b)$. Is any element among these elements primitive over \mathbb{Q} ?*

QUESTION (Ayad and Kihel [9]). — *Is the following statement correct? The relation $m \text{ord}_p(\mathfrak{J}(\mathbb{K}|\mathbb{Q})) = \text{ord}_p(\mathfrak{J}(\mathbb{L}|\mathbb{Q}))$ holds iff for any $b \in \mathbb{L}$ such that $\text{ord}_p(d(\mathbb{Z}, f_b)) = \text{ord}_p(\mathfrak{J}(\mathbb{L}|\mathbb{Q}))$, there exists $a \in \mathbb{K}$ such that $b \equiv a \pmod{p}$.*

Ayad and Kihel gave examples in support of these questions, but a rigorous proof is still required. In this setting, one question is pertinent: when is $\mathfrak{J}(\mathbb{L}|\mathbb{Q})$ a proper ideal of \mathcal{O}_K ? McCluer [72] answered this question completely in 1971.

THEOREM 6.2 (McCluer [72]). — *Let \mathbb{L} be number field such that $[\mathbb{L} : \mathbb{Q}] = m$, then $\mathfrak{J}(\mathbb{L}|\mathbb{Q}) > 1$ if and only if some prime $p \leq m$ possesses at least p distinct factors in \mathbb{L} . The set of such primes p is exactly the set of the prime divisors of $\mathfrak{J}(\mathbb{L}|\mathbb{Q})$.*

Combining the notion of $\mathfrak{J}(\mathbb{L}|\mathbb{K})$, the above theorem and a classical result of Hensel (see [59, 9]), Ayad and Kihel [9] gave one more interesting application of fixed divisors. Before proceeding we recall a few definitions.

For a number field \mathbb{K} define $\hat{\mathcal{O}}_{\mathbb{K}} = \{a \in \mathcal{O}_{\mathbb{K}} : \mathbb{Q}(a) = \mathbb{K}\}$, the set of all primitive elements of $\mathcal{O}_{\mathbb{K}}$. For a given $a \in \hat{\mathcal{O}}_{\mathbb{K}}$, its *index* $i(a)$ is defined as $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[a]]$ (cardinality of $\mathcal{O}_{\mathbb{K}}/\mathbb{Z}[a]$). Define $i(\mathbb{K}) = g.c.d._{a \in \hat{\mathcal{O}}_{\mathbb{K}}} i(a)$. A prime number p is called a *common factor of indices (cfi)* in $\mathcal{O}_{\mathbb{K}}$ if p divides $i(\mathbb{K})$. Existence of at least one cfi was shown by Dedekind [60]. For examples and criteria for a prime number to be a cfi in various extensions of \mathbb{Q} , we refer to [8, 11, 28, 29, 42, 43, 80, 82, 103, 104] [105, 116]. The following theorem characterizes the prime numbers which can be cfi in $\mathcal{O}_{\mathbb{K}}$.

THEOREM 6.3 (Ayad and Kihel [9]). — *Let p be a prime number and let \mathbb{K} be a number field. If p is a cfi in $\mathcal{O}_{\mathbb{K}}$, then $p \mid \mathfrak{J}(\mathbb{K}|\mathbb{Q})$.*

The converse of the above theorem may not be true in general, however we have the following

THEOREM 6.4 (Ayad and Kihel [9]). — *Suppose that \mathbb{K} is a Galois extension of \mathbb{Q} . Let $1 \leq d < n$ be the greatest proper divisor of n . Let $n > p > d$ be a prime number, then $p \mid \mathfrak{J}(\mathbb{K}|\mathbb{Q})$ if and only if p is a cfi in $\mathcal{O}_{\mathbb{K}}$.*

Let \mathbb{K} be an abelian extension of \mathbb{Q} of degree n and let $p < n$ be a prime number such that $(p, n) = 1$. If $p \mid \mathfrak{J}(\mathbb{K}|\mathbb{Q})$, then they showed that p is not ramified in its inertia field and p is a cfi in the decomposition field (see Marcus [73], for e.g., for the definitions). Moreover, if \mathbb{K}_0 is any subfield of the decomposition field, then p is a cfi in \mathbb{K}_0 . Studying various authors' work on the above topic, Ayad and Kihel arrived at the following question.

QUESTION (Ayad and Kihel [9]). — *Suppose \mathbb{K} is a number field and p is a prime number such that $p\mathcal{O}_{\mathbb{K}} = P_1^{e_1} \dots P_r^{e_r}$ with $r \geq p$, and f_i is the inertial degree of P_i , for $i = 1, \dots, r$. Can we compute $\text{ord}_p(\mathfrak{J}(\mathbb{K}|\mathbb{Q}))$ in terms of r, e_i and f_i ?*

With all assumptions as in Theorem 6.4 and the above Question, let $\rho(p)$ denote the number of $\bar{a} \in \mathcal{O}_{\mathbb{K}}/p\mathcal{O}_{\mathbb{K}}$ such that $p \mid d(\mathbb{Z}, f_a)$. Then Ayad and Kihel computed

$$\rho(p) = p^\lambda \sum_{j=0}^p \binom{p}{j} \prod_{i=1}^r (p^{f_i} - j),$$

where $\lambda = n - \sum_{i=1}^r f_i$. Connecting $\rho(p)$ to the splitting of p , they conjectured

CONJECTURE 6.5 (Ayad and Kihel [9]). — *If \mathbb{K} is a Galois extension of degree n over \mathbb{Q} and $p \mid \mathfrak{J}(\mathbb{K}|\mathbb{Q})$, then $\rho(p)$ determines the splitting of p in \mathbb{K} .*

Wood [124] also connected splitting of primes to fixed divisors. Let $R = \mathcal{O}_{\mathbb{K}}$ for a number field \mathbb{K} and S be the integral closure of R in a finite extension of \mathbb{K} . She observed that all of the following are equivalent.

- (i) All primes of R split completely in S .
- (ii) $\nu_k(R) = \nu_k(S)$ in the ring S for all k .
- (iii) For any $f(x) \in S[x]$, $d(R, f) = d(S, f)$.
- (iv) $\text{Int}(R, S) = \text{Int}(S, S)$.

For a more general version of these statements, we refer to the discussion in Section 7.

Now we shed light on a beautiful number theoretic problem and its solution using a bound for the fixed divisor in terms of the coefficients of that polynomial. Selfridge (see [58], problem B47) asked the question: for what pairs of natural numbers m and n do we have $(2^m - 2^n) \mid (x^m - x^n)$ for all integers x ? In 1974, Ruderman posed a similar problem.

PROBLEM (Ruderman [93]). — *Suppose that $m > n > 0$ are integers such that $2^m - 2^n$ divides $3^m - 3^n$. Show that $2^m - 2^n$ divides $x^m - x^n$ for all natural numbers x .*

This problem still remains open but a positive solution to it will completely answer Selfridge's question. In 2011, Ram Murty and Kumar Murty [78] proved that there are only finitely many m and n for which the hypothesis in the problem holds. Rundle [96] also examined two types of generalizations of the problem. Selfridge's problem was answered by Pomerance [94] in 1977 by combining results of Schinzel [97] and Velez [95]. Q. Sun and M. Zhang [106] also answered Selfridge's question.

Once Selfridge's question is answered a natural question arises: what happens if we replace '2' by '3' or more generally by some other integer (other than ± 1). The arguments used to answer Selfridge's question were elementary and may not suffice to answer this question. Instead, the following argument will be helpful.

Observe that $a^m - a^n \mid x^m - x^n$ for all $x \in \mathbb{Z}$ iff $a^m - a^n \mid d(\mathbb{Z}, f_{m,n})$, where $f_{m,n}(x) = x^m - x^n$. Let a_1, a_2, \dots, a_k be non-zero elements of \mathbb{Z} and C be the set of all polynomials with the sequence of non-zero coefficients a_1, a_2, \dots, a_k , then $\{d(\mathbb{Z}, g) : g \in C\}$ is bounded (for a proof see Vajaitu [113]). In this case, the non-zero coefficients are 1, -1 and hence it follows that $d(\mathbb{Z}, f_{m,n}) \leq M$ for some real constant M and hence only finitely many pairs (m, n) are possible such that $a^m - a^n \mid x^m - x^n$ for all $x \in \mathbb{Z}$.

The above argument is the particular case of the argument given by Vajaitu [113] in 1999. He generalized Selfridge's question to a number ring and proved

THEOREM 6.6 (Vajaitu and Zaharescu [113]). — *Let R be a number ring of an algebraic number field, a_1, a_2, \dots, a_k, b be non-zero elements of R and b be a non unit, then there are only finitely many k tuples $(n_1, n_2, \dots, n_k) \in \mathbb{N}^k$ satisfying the following simultaneously*

- (i) $\sum_{i=1}^k a_i b^{n_i} \mid \sum_{i=1}^k a_i x_i^{n_i}$ for all $x \in R$,
- (ii) $\sum_{i \in S} a_i b^{n_i} \neq 0$ for all $\emptyset \neq S \subseteq \{1, 2, \dots, k\}$.

If the group of units of R is of finite order then the theorem can be further strengthened. Here the bound for the fixed divisor involving the coefficients plays a role through the observation : if $\sum_{i=1}^k a_i b^{n_i} \mid \sum_{i=1}^k a_i x_i^{n_i}$ for all $x \in R$, then $\sum_{i=1}^k a_i b^{n_i}$ divides the fixed divisor of $f(x) = \sum_{i=1}^k a_i x_i^{n_i}$ over R and hence $N(\sum_{i=1}^k a_i b^{n_i})$ divides $N(d(R, f))$ and we have $N(\sum_{i=1}^k a_i b^{n_i}) \leq N(d(R, f))$. Here (and further) norm of an

element is same as the norm of the ideal generated by the element. They proved that $N(d(R, f))$ is bounded above by $c_1|N(a_1)|^{c_2} \exp\left(c_3 a^{\frac{c_4}{\log \log a}}\right)$ and $N\left(\sum_{i=1}^k a_i b^{n_i}\right)$ is bounded below by $c|N(b)|^a$, where c, c_1, c_2, c_3, c_4 are constants independent of the choice of (n_1, n_2, \dots, n_k) and $a = \max\{n_1, \dots, n_k\}$. Putting these bounds together, we have

$$c|N(b)|^a \leq N\left(\sum_{i=1}^k a_i b^{n_i}\right) \leq N(d(R, f)) \leq c_1|N(a_1)|^{c_2} \exp\left(c_3 a^{\frac{c_4}{\log \log a}}\right).$$

In this way they got upper and lower bounds of $N(d(R, f))$. Comparing these bounds they concluded that a must be bounded and hence only finitely many solutions exist.

Recently Bose [15] also generalized Selfridge's question. In 2004, Choi and Zaharescu [39] generalized Theorem 6.6 to the case of n variables as follows.

THEOREM 6.7 (Choi and Zaharescu [39]). — *Let R be the ring of integers in an algebraic number field and let b_1, b_2, \dots, b_n be non-zero non-unit elements of R . Let $a_{i_1, \dots, i_n} \in R$ for all $1 \leq i_1 \leq k_1, \dots, 1 \leq i_n \leq k_n$. Then there are only finitely many n tuples $(\mathbf{m}_1, \mathbf{m}_2, \dots, \mathbf{m}_n) \in \mathbb{N}^{k_1} \times \mathbb{N}^{k_2} \times \dots \times \mathbb{N}^{k_n}$ satisfying the following simultaneously, where $\mathbf{m}_j = (m_{j1}, \dots, m_{jk_j})$:*

(i) For all $\underline{x} \in R^n$,

$$\sum_{i_1=1}^{k_1} \dots \sum_{i_n=1}^{k_n} a_{i_1, \dots, i_n} b_1^{m_{1i_1}} \dots b_n^{m_{ni_n}} \Big| \sum_{i_1=1}^{k_1} \dots \sum_{i_n=1}^{k_n} a_{i_1, \dots, i_n} x_1^{m_{1i_1}} \dots x_n^{m_{ni_n}}.$$

(ii) For all non-empty $S \subseteq \{1, 2, \dots, k_1\} \times \dots \times \{1, 2, \dots, k_n\}$,

$$\sum_{(i_1, \dots, i_n) \in S} a_{i_1, \dots, i_n} b_1^{m_{1i_1}} \dots b_n^{m_{ni_n}} \neq 0.$$

Choi and Zaharescu also strengthened this result for \mathbb{Z} and $\mathbb{Z}[i]$.

To conclude this section, we will describe an application of fixed divisors in Algebraic Geometry by Vajaitu [112]. Let $S \subseteq \mathbf{P}^n$ be an algebraic subset of a projective space \mathbf{P} over some algebraically closed field \mathbb{K} (see [61] for a general reference). We denote the degree of S by $\deg(S)$ and the number of non-zero coefficients in f_S by $|S|$, where f_S is the Hilbert polynomial associated with S . This polynomial has rational coefficients and so can be written as $\frac{f}{d}$ for f in $\mathbb{Z}[x]$ and $d \in \mathbb{Z}$. Vajaitu proved that $\dim(S) \leq \max\{\deg(S)^2, 4|S|^2\}$ by using Theorem 4.6 for the polynomial f .

7. FIXED DIVISORS FOR THE RING OF MATRICES

It can be seen that if R is a domain then $M_m(R)$ is a ring with usual addition and matrix multiplication. In recent years, several prominent mathematicians have studied the ring of polynomials in $M_m(\mathbb{K})[x]$ which maps $M_m(R)$ back to this ring, generally denoted by $\text{Int}(M_m(R))$. For various interesting results about this ring, we refer to [46, 45, 48, 52, 51, 62, 71, 84, 85, 88, 89, 120]. For a survey on $\text{Int}(M_m(R))$, the reader may consult [49, 123]. We have seen in the previous sections, the close relationship between $d(\underline{S}, f)$ and $\text{Int}(\underline{S}, R)$. We believe that the

systematic study of fixed divisors in this setting will be helpful in studying the properties of $\text{Int}(M_m(R))$.

We know that each ideal of $M_m(R)$ is of the form $M_m(I)$ for some ideal $I \subseteq R$, and the map $I \mapsto M_m(I)$ is a bijection between the set of ideals of R and the set of ideals of $M_m(R)$. Hence, we suggest the following definition for fixed divisors in this setting.

DEFINITION 7.1. — For a given subset $S \subseteq M_m(R)$ and a given polynomial $f \in M_m(R)[x]$, we define $d(S, f)$ to be the ideal of R generated by the entries of all matrices of the form $f(A)$, where $A \in S$.

This definition can be extended to the multivariate case as usual. For each positive integer l , define G_l as follows

$$G_l = \{f \in M_m(\mathbb{Z})[x] : f(M_m(\mathbb{Z})) \subseteq l \cdot M_m(\mathbb{Z})\}.$$

In other words, G_l is the set of polynomials of $M_m(\mathbb{Z})[x]$ whose fixed divisor is divisible by l . It can be seen that G_l is an ideal and this ideal was studied by Werner [120]. Werner also studied the classification of ideals of $\text{Int}(M_m(R))$ and found the ideal of polynomials in $M_m(R)[x]$ whose fixed divisor over a special set S (see section 2 of [120]) is a multiple of a given ideal $I \subseteq R$.

Define ϕ_l to be a monic polynomial of minimal degree in $G_l \cap \mathbb{Z}[x]$, where \mathbb{Z} is embedded in $M_m(\mathbb{Z})$ as scalar matrices and $\phi_1 = 1$. Werner proved the following theorem

THEOREM 7.2 (Werner [120]). — (1) $G_p = \langle \phi_p, p \rangle$.

(2) Let $l > 1$ and p_1, p_2, \dots, p_r be all the primes dividing l , then

$$G_l = (\phi_l, l) + p_1 G_{l/p_1} + p_2 G_{l/p_2} + \dots + p_r G_{l/p_r}.$$

(3) Let $l > 1$, then G_l is generated by $\{r\phi_{l/r} : r \text{ divides } l\}$.

Werner [119] also proved similar results in the case of ring of quaternions. The study of fixed divisors is also helpful in the study of lcm of polynomials done by Werner [121]. For a ring R and a subset X of $R[x]$, define a least common multiple for X , a monic polynomial $L \in R[x]$ of least degree such that $f|L$ for all $f \in X$. For any $n, D \in \mathbb{W}$ with $n > 1$ and $D > 0$, let $P(n, D)$ be the set of all monic polynomials in $\mathbb{Z}_n[x]$ of degree D . It can be seen that an lcm for $P(n, D)$ always exists, but may not be unique when n is not a prime number. However, its degree is always unique. The unique lcm for $P(p, D)$, where p is a prime, is $f = (x^{p^D} - x)(x^{p^{D-1}} - x) \cdots (x^p - x)$, which is the smallest degree polynomial with integer coefficients such that $d(M_D(\mathbb{Z}), f)$ is a multiple of p . We can also interpret $P(n, D)$ similarly. If we have determined the ideal of polynomials in $\mathbb{Z}[x]$, whose fixed divisor over $M_D(\mathbb{Z})$ is a multiple of a given number n , then the smallest degree polynomial in that ideal will give us the degree of lcm of all D degree polynomials in $\mathbb{Z}_n[x]$, giving more sharper results than [121]. Systematic study of fixed divisors will also answer the problems posed in the same article. Hence, these two studies are closely connected.

At this stage, we are familiar with various ways of computation of fixed divisors, various bounds for fixed divisors and various applications of fixed divisors. We ask the following question:

QUESTION. — For a Dedekind domain R , what are the pairs \underline{S} and \underline{T} of subsets of $(M_m(R))^n$, such that $d(\underline{S}, f) = d(\underline{T}, f)$ for all $f \in M_m(R)[\underline{x}]$?

Crabbe [40] studied subsets S and T of \mathbb{Z} which have the same Bhargava's factorials, i.e., $\nu_k(S) = \nu_k(T)$ for all $k \in \mathbb{W}$. The above question is a vast generalization of his study.

One more interesting problem is the classification of the subsets S and T of R , such that $\text{Int}(S, R) = \text{Int}(T, R)$. Such a subsets are called *polynomially equivalent subsets*. For some results on this topic we refer [22, 30, 33, 36, 37, 47, 53, 55, 74]. It can be seen that for a Dedekind domain R and for a pair of subsets \underline{S} and \underline{T} of R^n , $\text{Int}(\underline{S}, R) = \text{Int}(\underline{T}, R)$ iff $d(\underline{S}, f) = d(\underline{T}, f)$ for all $f \in R[\underline{x}]$. Hence, the above question can be seen as another perspective of this problem, in the case when $m = 1$. In this case, Mulay [76] gave a necessary and sufficient condition to answer the above question, when R is a Dedekind domain or UFD. He also analyzed the same question in other cases.

Finally, we would like to ask the following question:

QUESTION. — What is the analogue of Theorem 2.2 in this setting?

This question could naturally be modified by replacing Theorem 2.2 with many of the results in the previous sections. The answer to the above question will completely determine generalized factorials for the ring of matrices (and their subsets). As we know, in the case of one variable, generalized factorials helped a lot in the study of integer-valued polynomials and other diverse applications. The generalized factorial, in the case of ring of matrices, may also give same kind of results.

In conclusion, we would like to remark that this article was an initiative to familiarize the reader with the notion of fixed divisors and how it can be helpful in the study of integer-valued polynomials and other number theoretic problems. We would especially wish to point out that there are several conjectures on polynomials, which need the fixed divisor to be equal to 1. For example, one very interesting conjecture is the Buniakowski conjecture [16], which states that any irreducible polynomial $f \in \mathbb{Z}[x]$ with $d(\mathbb{Z}, f) = 1$ takes infinitely many prime values. Schinzel's hypothesis H is a vast generalization of this conjecture. For a detailed exposition and excellent commentary on conjectures of this type, we refer to Schinzel [98]. We believe that the tools introduced so far may be helpful in studying these conjectures.

We also wish to highlight the various kinds of sequences and their interplay, which were outlined in Section 2. The study of these sequences seems to be a fertile area of research, which has not been explored in detail so far. We also introduced several questions and conjectures according to their context. Working on these seems to be a promising area of research.

ACKNOWLEDGMENTS

We thank Prof. Wladyslaw Narkiewicz, Prof. Andrej Schinzel, Prof. Marian Vajaitu and Mr. Cosmin Constantin Nitu for their suggestions and help which helped us to improve this paper. We are also indebted to the reviewer for providing insightful comments and time which invariably improved the paper.

REFERENCES

- [1] David Adam. Simultaneous orderings in function fields. *J. Number Theory*, 112(2):287–297, 2005.
- [2] David Adam. Pólya and Newtonian function fields. *Manuscripta Math.*, 126(2):231–246, 2008.
- [3] David Adam and Paul-Jean Cahen. Newton and Schinzel sequences in quadratic fields. *Actes des rencontres du CIRM*, 2(2):15–20, 2010.
- [4] David Adam and Paul-Jean Cahen. Newtonian and Schinzel quadratic fields. *J. Pure Appl. Algebra*, 215(8):1902–1918, 2011.
- [5] David Adam, Jean-Luc Chabert, and Youssef Fares. Subsets of \mathbb{Z} with simultaneous orderings. *Integers*, 10:A37, 437–451, 2010.
- [6] David F. Anderson. Elasticity of factorizations in integral domains: a survey. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 1–29. Dekker, New York, 1997.
- [7] David F. Anderson, Paul-Jean Cahen, Scott T. Chapman, and William W. Smith. Some factorization properties of the ring of integer-valued polynomials. In *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, volume 171 of *Lecture Notes in Pure and Appl. Math.*, pages 125–142. Dekker, New York, 1995.
- [8] Mohamed Ayad, Rachid Bouchenna, and Omar Kihel. Indices in a number field. *J. Théor. Nombres Bordeaux*, 29(1):201–216, 2017.
- [9] Mohamed Ayad and Omar Kihel. Common divisors of values of polynomials and common factors of indices in a number field. *Int. J. Number Theory*, 7(5):1173–1194, 2011.
- [10] Andrea Bandini. Functions $f : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ induced by polynomials of $\mathbb{Z}[X]$. *Ann. Mat. Pura Appl. (4)*, 181(1):95–104, 2002.
- [11] Michael Bauer. Über die außerwesentlichen Diskriminantenteiler einer Gattung. *Math. Ann.*, 64(4):573–576, 1907.
- [12] Manjul Bhargava. P -orderings and polynomial functions on arbitrary subsets of Dedekind rings. *J. Reine Angew. Math.*, 490:101–127, 1997.
- [13] Manjul Bhargava. Generalized factorials and fixed divisors over subsets of a Dedekind domain. *J. Number Theory*, 72(1):67–75, 1998.
- [14] Manjul Bhargava. The factorial function and generalizations. *Amer. Math. Monthly*, 107(9):783–799, 2000.
- [15] Arnab Bose. Investigations on some exponential congruences. Master’s thesis, University of Lethbridge, Canada, 2016.
- [16] V. Bouniakowsky. Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs. *Mém. Acad. Sc. St-Pétersbourg (6), Sci. Math. Phys.*, 6:305–329, 1857.
- [17] Jason Boynton. Pullbacks of arithmetical rings. *Comm. Algebra*, 35(9):2671–2684, 2007.
- [18] Jason G. Boynton and Sean Sather-Wagstaff. Regular pullbacks. In *Progress in commutative algebra 2*, pages 145–169. Walter de Gruyter, Berlin, 2012.
- [19] Jason Greene Boynton. Atomicity and the fixed divisor in certain pullback constructions. *Colloq. Math.*, 129(1):87–97, 2012.
- [20] Jakub Byszewski, Mikołaj Fraczyk, and Anna Szumowicz. Simultaneous p -orderings and minimizing volumes in number fields. *J. Number Theory*, 173:478–511, 2017.
- [21] Paul-Jean Cahen. Polynômes à valeurs entières. *Canad. J. Math*, 24:747–754, 1972.
- [22] Paul-Jean Cahen. Polynomial closure. *J. Number Theory*, 61(2):226–247, 1996.
- [23] Paul-Jean Cahen. Newtonian and Schinzel sequences in a domain. *J. Pure Appl. Algebra*, 213(11):2117–2133, 2009.
- [24] Paul-Jean Cahen and Jean-Luc Chabert. Elasticity for integral-valued polynomials. *J. Pure Appl. Algebra*, 103(3):303–311, 1995.
- [25] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.
- [26] Paul-Jean Cahen and Jean-Luc Chabert. What you should know about integer-valued polynomials. *Amer. Math. Monthly*, 123(4):311–337, 2016.
- [27] Paul-Jean Cahen and Jean-Luc Chabert. Test sets for polynomials: n -universal subsets and Newton sequences. *J. Algebra*, 502:277–314, 2018.

- [28] Leonard Carlitz. On abelian fields. *Trans. Amer. Math. Soc.*, 35(1):122–136, 1933.
- [29] Leonard Carlitz. A note on common index divisors. *Proc. Amer. Math. Soc.*, 3:688–692, 1952.
- [30] Jean-Luc Chabert. On the polynomial closure in a valued field. *J. Number Theory*, 130(2):458–468, 2010.
- [31] Jean-Luc Chabert. Integer-valued polynomials: looking for regular bases (a survey). In *Commutative algebra*, pages 83–111. Springer, New York, 2014.
- [32] Jean-Luc Chabert and Paul-Jean Cahen. Old problems and new questions around integer-valued polynomials and factorial sequences. In *Multiplicative ideal theory in commutative algebra*, pages 89–108. Springer, New York, 2006.
- [33] Jean-Luc Chabert, Scott T. Chapman, and William W. Smith. The Skolem property in rings of integer-valued polynomials. *Proc. Amer. Math. Soc.*, 126(11):3151–3159, 1998.
- [34] Jean-Luc Chabert and Sabine Evrard. On the ideal generated by the values of a polynomial. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 213–225. Chapman & Hall/CRC, Boca Raton, FL, 2005.
- [35] Scott T. Chapman and Barbara A. McClain. Irreducible polynomials and full elasticity in rings of integer-valued polynomials. *J. Algebra*, 293(2):595–610, 2005.
- [36] Scott T. Chapman and Vadim Ponomarenko. On image sets of integer-valued polynomials. *J. Algebra*, 348:350–353, 2011.
- [37] Scott T. Chapman, Vadim Ponomarenko, and William W. Smith. Robert Gilmer’s contributions to the theory of integer-valued polynomials. In *Multiplicative ideal theory in commutative algebra*, pages 109–122. Springer, New York, 2006.
- [38] Zhibo Chen. On polynomial functions from Z_n to Z_m . *Discrete Math.*, 137(1-3):137–145, 1995.
- [39] Geumlan Choi and Alexandru Zaharescu. A class of exponential congruences in several variables. *J. Korean Math. Soc.*, 41(4):717–735, 2004.
- [40] Andrew M. Crabbe. Generalized factorial functions and binomial coefficients. Undergraduate Honors Thesis, Trinity University, USA, 2001.
- [41] Leonard Eugene Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality*. Chelsea Publishing Co., New York, 1966.
- [42] D. S. Dummit and H. Kisilevsky. Indices in cyclic cubic fields. In *Number theory and algebra*, pages 29–42. Academic Press, New York, 1977.
- [43] Howard Theodore Engstrom. On the common index divisors of an algebraic field. *Trans. Amer. Math. Soc.*, 32(2):223–237, 1930.
- [44] Sabine Evrard. Bhargava’s factorials in several variables. *J. Algebra*, 372:134–148, 2012.
- [45] Sabine Evrard, Youssef Fares, and Keith Johnson. Integer-valued polynomials on lower triangular integer matrices. *Monatsh. Math.*, 170(2):147–160, 2013.
- [46] Sabine Evrard and Keith Johnson. The ring of integer-valued polynomials on 2×2 matrices and its integral closure. *J. Algebra*, 441:660–677, 2015.
- [47] Sophie Frisch. Substitution and closure of sets under integer-valued polynomials. *J. Number Theory*, 56(2):396–403, 1996.
- [48] Sophie Frisch. Polynomial separation of points in algebras. In *Arithmetical properties of commutative rings and monoids*, volume 241 of *Lect. Notes Pure Appl. Math.*, pages 253–259. Chapman & Hall/CRC, Boca Raton, FL, 2005.
- [49] Sophie Frisch. Integer-valued polynomials on algebras: a survey. *Actes des rencontres du CIRM*, 2(2):27–32, 2010.
- [50] Sophie Frisch. A construction of integer-valued polynomials with prescribed sets of lengths of factorizations. *Monatsh. Math.*, 171(3-4):341–350, 2013.
- [51] Sophie Frisch. Integer-valued polynomials on algebras. *J. Algebra*, 373:414–425, 2013.
- [52] Sophie Frisch. Corrigendum to “Integer-valued polynomials on algebras” [*J. Algebra* 373 (2013) 414–425]. *J. Algebra*, 412:282, 2014.
- [53] Robert Gilmer. Sets that determine integer-valued polynomials. *J. Number Theory*, 33(1):95–100, 1989.
- [54] Robert Gilmer. The ideal of polynomials vanishing on a commutative ring. *Proc. Amer. Math. Soc.*, 127(5):1265–1267, 1999.
- [55] Robert Gilmer and William W. Smith. On the polynomial equivalence of subsets E and $f(E)$ of \mathbb{Z} . *Arch. Math. (Basel)*, 73(5):355–365, 1999.

- [56] Hiroshi Gunji and Donald L. McQuillan. On polynomials with integer coefficients. *J. Number Theory*, 1:486–493, 1969.
- [57] Hiroshi Gunji and Donald L. McQuillan. On a class of ideals in an algebraic number field. *J. Number Theory*, 2:207–222, 1970.
- [58] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, second edition, 1994.
- [59] Marshall Hall. Indices in cubic fields. *Bull. Amer. Math. Soc.*, 43(2):104–108, 1937.
- [60] Harris Hancock. *Foundations of the theory of algebraic numbers. Vol. II: The general theory*. Dover Publications, Inc., New York, 1964.
- [61] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977.
- [62] Bahar Heidaryan, Matteo Longo, and Giulio Peruginelli. Galois structure on integral-valued polynomials. *J. Number Theory*, 171:198–212, 2017.
- [63] Bahar Heidaryan and Ali Rajaei. Biquadratic Pólya fields with only one quadratic Pólya subfield. *J. Number Theory*, 143:279–285, 2014.
- [64] K. Hensel. Ueber den grössten gemeinsamen Theiler aller Zahlen, welche durch eine ganze Function von n Veränderlichen darstellbar sind. *J. Reine Angew. Math.*, 116:350–356, 1896.
- [65] István Járasi. Remarks on P-orderings and simultaneous orderings. Preprint.
- [66] J. Latham. On sequences of algebraic integers. *J. London Math. Soc. (2)*, 6:555–560, 1973.
- [67] Amandine Leriche. Pólya fields and Pólya numbers. *Actes des rencontres du CIRM*, 2(2):21–26, 2010.
- [68] Amandine Leriche. Pólya fields, Pólya groups and Pólya extensions: a question of capitulation. *J. Théor. Nombres Bordeaux*, 23(1):235–249, 2011.
- [69] Amandine Leriche. Cubic, quartic and sextic Pólya fields. *J. Number Theory*, 133(1):59–71, 2013.
- [70] Amandine Leriche. About the embedding of a number field in a Pólya field. *J. Number Theory*, 145:210–229, 2014.
- [71] K. Alan Loper and Nicholas J. Werner. Generalized rings of integer-valued polynomials. *J. Number Theory*, 132(11):2481–2490, 2012.
- [72] Charles R. MacCluer. Common divisors of values of polynomials. *J. Number Theory*, 3:33–34, 1971.
- [73] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.
- [74] Donald L. McQuillan. On a theorem of R. Gilmer. *J. Number Theory*, 39(3):245–250, 1991.
- [75] Shashikant B. Mulay. On integer-valued polynomials. In *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, volume 171 of *Lecture Notes in Pure and Appl. Math.*, pages 331–345. Dekker, New York, 1995.
- [76] Shashikant B. Mulay. Integer-valued polynomials in several variables. *Comm. Algebra*, 27(5):2409–2423, 1999.
- [77] Shashikant B. Mulay. Polynomial-mappings and M -equivalence. *J. Algebra*, 302(2):862–880, 2006.
- [78] M. Ram Murty and V. Kumar Murty. On a problem of Ruderman. *Amer. Math. Monthly*, 118(7):644–650, 2011.
- [79] Trygve Nagell. Über zahlentheoretische Polynome. *Norsk. Mat. Tidsskr*, 1:14–23, 1919.
- [80] Trygve Nagell. Quelques résultats sur les diviseurs fixes de l’index des nombres entiers d’un corps algébrique. *Ark. Mat.*, 6:269–289, 1966.
- [81] Władysław Narkiewicz. *Polynomial mappings*, volume 1600 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.
- [82] Enric Nart. On the index of a number field. *Trans. Amer. Math. Soc.*, 289(1):171–183, 1985.
- [83] Alexander Ostrowski. Über ganzwertige Polynome in algebraischen Zahlkörpern. *J. Reine Angew. Math.*, 149:117–124, 1919.
- [84] Giulio Peruginelli. Integer-valued polynomials over matrices and divided differences. *Monatsh. Math.*, 173(4):559–571, 2014.
- [85] Giulio Peruginelli. Integral-valued polynomials over sets of algebraic integers of bounded degree. *J. Number Theory*, 137:241–255, 2014.
- [86] Giulio Peruginelli. Primary decomposition of the ideal of polynomials whose fixed divisor is divisible by a prime power. *J. Algebra*, 398:227–242, 2014.
- [87] Giulio Peruginelli. Factorization of integer-valued polynomials with square-free denominator. *Comm. Algebra*, 43(1):197–211, 2015.

- [88] Giulio Peruginelli and Nicholas J. Werner. Integral closure of rings of integer-valued polynomials on algebras. In *Commutative algebra*, pages 293–305. Springer, New York, 2014.
- [89] Giulio Peruginelli and Nicholas J. Werner. Properly integral polynomials over the ring of integer-valued polynomials on a matrix ring. *J. Algebra*, 460:320–339, 2016.
- [90] Georg Pólya. Über ganzwertige Polynome in algebraischen Zahlkörpern. *J. Reine Angew. Math.*, 149:97–116, 1919.
- [91] Krishnan Rajkumar, A Satyanarayana Reddy, and Devendra Prasad Semwal. Fixed divisor of a multivariate polynomial and generalized factorials in several variables. *J. Korean Math. Soc.*, 55(6):1305–1320, 2018.
- [92] Mark W. Rogers and Cameron Wickham. Polynomials inducing the zero function on local rings. *Int. Electron. J. Algebra*, 22:170–186, 2017.
- [93] Harry Ruderman, David Gale, C. Roger Glassey, G. Tsintsifas, David Shelupsky, and Robert Brooks. Problems and Solutions: Elementary Problems: E2468-E2473. *Amer. Math. Monthly*, 81(4):405–406, 1974.
- [94] Harry Ruderman and Carl Pomerance. Problems and Solutions: Solutions of Elementary Problems: E2468. *Amer. Math. Monthly*, 84(1):59–60, 1977.
- [95] Harry Ruderman and W. Y. Velez. Problems and Solutions: Solutions of Elementary Problems: E2468. *Amer. Math. Monthly*, 83(4):288–289, 1976.
- [96] Robert John Rundle. *Generalization of Ruderman’s Problem to Imaginary Quadratic Fields*. PhD thesis, Queen’s University, Canada, 2012.
- [97] Andrzej Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Philos. Soc.*, 58:555–562, 1962.
- [98] Andrzej Schinzel. *Selecta. Vol. II. Heritage of European Mathematics*. European Mathematical Society (EMS), Zürich, 2007.
- [99] Andrzej Schinzel. On fixed divisors of forms in many variables. II. In *Analytic and probabilistic methods in number theory*, pages 207–221. TEV, Vilnius, 2012.
- [100] Andrzej Schinzel. On fixed divisors of forms in many variables, I. *Math. Scand.*, 114(2):161–184, 2014.
- [101] David Singmaster. A maximal generalization of Fermat’s theorem. *Math. Mag.*, 39:103–107, 1966.
- [102] David Singmaster. On polynomial functions (mod m). *J. Number Theory*, 6:345–352, 1974.
- [103] Jan Śliwa. On the nonessential discriminant divisor of an algebraic number field. *Acta Arith.*, 42(1):57–72, 1982/83.
- [104] Blair K. Spearman and Kenneth S. Williams. Cubic fields with index 2. *Monatsh. Math.*, 134(4):331–336, 2002.
- [105] Blair K. Spearman and Kenneth S. Williams. The index of a cyclic quartic field. *Monatsh. Math.*, 140(1):19–70, 2003.
- [106] Qi Sun and Ming Zhi Zhang. Pairs where $2^a - 2^b$ divides $n^a - n^b$ for all n . *Proc. Amer. Math. Soc.*, 93(2):218–220, 1985.
- [107] Mohammed Taous. On the Pólya group of some imaginary biquadratic fields. In *Non-associative and non-commutative algebra and operator theory*, volume 160 of *Springer Proc. Math. Stat.*, pages 175–182. Springer, Cham, 2016.
- [108] Mohammed Taous and Abdelkader Zekhnini. Pólya groups of the imaginary bicyclic biquadratic number fields. *J. Number Theory*, 177:307–327, 2017.
- [109] Jan Turk. The fixed divisor of a polynomial. *Amer. Math. Monthly*, 93(4):282–286, 1986.
- [110] Marian Văjăitu. *Estimations of the ideal generated by the values of a polynomial over a Dedekind ring*. PhD thesis, University of Bucharest, Romania, 1994.
- [111] Marian Văjăitu. The ideal generated by the values of a polynomial over a Dedekind ring. *Rev. Roumaine Math. Pures Appl.*, 42(1-2):155–161, 1997.
- [112] Marian Văjăitu. An inequality involving the degree of an algebraic set. *Rev. Roumaine Math. Pures Appl.*, 43(3-4):451–455, 1998.
- [113] Marian Văjăitu and Alexandru Zaharescu. A finiteness theorem for a class of exponential congruences. *Proc. Amer. Math. Soc.*, 127(8):2225–2232, 1999.
- [114] Robert J. Valenza. Elasticity of factorization in number fields. *J. Number Theory*, 36(2):212–218, 1990.
- [115] Vladislav V. Volkov and Fedor V. Petrov. On the interpolation of integer-valued polynomials. *J. Number Theory*, 133(12):4224–4232, 2013.

- [116] E. von Žyliński. Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper. *Math. Ann.*, 73(2):273–274, 1913.
- [117] Bolesław Wantuła. Browkin’s problem for quadratic fields. *Zeszyty Nauk. Politech. Śląsk. Mat.-Fiz.*, 24:173–178, 1974.
- [118] Rolf Wasén. On sequences of algebraic integers in pure extensions of prime degree. *Colloq. Math.*, 30:89–104, 1974.
- [119] Nicholas J. Werner. Integer-valued polynomials over quaternion rings. *J. Algebra*, 324(7):1754–1769, 2010.
- [120] Nicholas J. Werner. Integer-valued polynomials over matrix rings. *Comm. Algebra*, 40(12):4717–4726, 2012.
- [121] Nicholas J. Werner. On least common multiples of polynomials in $\mathbb{Z}/n\mathbb{Z}[x]$. *Comm. Algebra*, 40(6):2066–2080, 2012.
- [122] Nicholas J. Werner. Polynomials that kill each element of a finite ring. *J. Algebra Appl.*, 13(3):1350111, 12, 2014.
- [123] Nicholas J. Werner. Integer-valued polynomials on algebras: a survey of recent results and open questions. In *Rings, polynomials, and modules*, pages 353–375. Springer, Cham, 2017.
- [124] Melanie Wood. P -orderings: a metric viewpoint and the non-existence of simultaneous orderings. *J. Number Theory*, 99(1):36–56, 2003.
- [125] Hans Zantema. Integer valued polynomials over a number field. *Manuscripta Math.*, 40(2-3):155–203, 1982.
- [126] Abdelkader Zekhnini. Imaginary biquadratic Pólya fields of the form $\mathbb{Q}(\sqrt{a}, \sqrt{-2})$. *Gulf J. Math.*, 4(4):182–188, 2016.

Manuscript received May 19, 2018,
revised November 25, 2018,
accepted December 19, 2018.

Devendra PRASAD

Department of Mathematics, Shiv Nadar University, Dadri, India-201314
dp742@snu.edu.in (Corresponding author)

Krishnan RAJKUMAR

School of Computer & Systems Sciences, Jawaharlal Nehru University, India-110067
krishnan.rjkmr@gmail.com

A. Satyanarayana REDDY

Department of Mathematics, Shiv Nadar University, Dadri, India-201314
satyanarayana.reddy@snu.edu.in