



Some new diophantine results on decomposable polynomial equations and irreducible polynomials

doktori (PhD) értekezés

BÉRCZES ATTILA

Debreceni Egyetem

Debrecen, 2000

Ezen értekezést a Debreceni Egyetem Matematika doktori program Diofantikus és konstruktív számelmélet alprogramja keretében készítettem 1996–2000 között és ezúton benyújtom a Debreceni Egyetem doktori Ph.D. fokozatának elnyerése céljából.

Debrecen, 2000. november 25.

.....
Bérczes Attila
jelölt

Tanúsítom, hogy Bérczes Attila doktorjelölt 1996–2000 között a fent megnevezett doktori alprogram keretében irányításommal végezte munkáját. Az értekezésben foglaltak a jelölt önálló munkáján alapulnak, az eredményekhez önálló alkotó tevékenységével meghatározóan hozzájárult. Az értekezés elfogadását javaslom.

Debrecen, 2000. november 25.

.....
Dr. Győry Kálmán
témavezető

Köszönetnyilvánítás

Ezúton is szeretnék köszönetet mondani mindazoknak, akik közvetve vagy közvetlenül hozzájárultak a disszertációm elkészítéséhez.

Szüleimnek, akik felneveltek és elindítottak az életben,

Témavezetőmnek, Dr. Győry Kálmánnak, aki megszerettette velem a számelméletet, azért a rengeteg hasznos tanácsért, útmutatásért és bátorításért, amely nélkül ez a dolgozat nem készülhetett volna el,

Tanáraimnak, Dr. Pethő Attilának, Dr. Kiss Péternek és Dr. Gaál Istvánnak, akiktől nagyon sokat tanultam és tanulok,

Kollégáimnak, Dr. Brindza Bélának, Dr. Hajdu Lajosnak és Dr. Pintér Ákosnak, akikhez bármikor fordulhattam szakmai segítségért,

A Magyar Soros Alapítványnak az értekezés elkészítéséhez nyújtott anyagi támogatásáért, az MTA-nak, OTKA-nak, az Universitas Alapítványnak és a Pro Regione Alapítványnak pedig a kutatások elvégzése során nyújtott támogatásukért,

Végül pedig barátaimnak, Baran Ágnesnek, Baran Sándornak, Erdei Lászlónak, Fejes Istvánnak, Khaled Abdullának, Tóth Tibornak és Varga Zsoltnak.

Contents

Introduction	1
1 On the number of solutions of general decomposable polynomial equations	9
1.1 Introduction	9
1.2 Main new results	11
1.3 Some consequences and applications	13
1.4 Proofs	18
2 On the number of solutions of norm form equations	29
2.1 Introduction	29
2.2 New results	31
2.3 Auxiliary results	34
2.4 Proofs	36
3 On the number of solutions of index form and discriminant form equations	43
3.1 Introduction and new results	43
3.2 Proof of Theorem 3.1	47
4 On a problem of P. Turán concerning irreducible polynomials	53
4.1 Introduction	53
4.2 New results	55
4.3 Description of the algorithm	57
Summary	65
Összefoglaló (Hungarian summary)	69
Bibliography	75
A List of papers of the author, and citations to these publications	79
B List of conference talks of the author	81
C	83

Introduction

This PhD dissertation consists of four chapters, which all contain new results. These results have been published in our papers [3], [2], [1] and [5], respectively. Before giving an overview of the contents of the chapters, we make some introductory notes on the subject of our thesis.

In the first three chapters we deal with the numbers of solutions of various important classes of decomposable polynomial equations. Namely, we shall be concerned with diophantine equations of the form

$$F(\mathbf{x}) = b \quad \text{in} \quad \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \quad (0.1)$$

and, more generally,

$$\begin{aligned} F(\mathbf{x}) = b p_1^{z_1} \dots p_s^{z_s} \quad & \text{in} \quad \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m \\ & \text{and} \quad z_1, \dots, z_s \in \mathbb{Z}_{\geq 0} \\ & \text{with} \quad (x_1, \dots, x_m, p_1 \dots p_s) = 1 \text{ if } s > 0. \end{aligned} \quad (0.2)$$

and

$$F(\mathbf{x}) \in b\mathbb{Z}_S^* \quad \text{in} \quad \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \quad (0.3)$$

where $S = \{p_1, \dots, p_s\}$ is a finite set of $s \geq 0$ primes, $\mathbb{Z}_S$ is the ring of S -integers in $\mathbb{Q}$, $\mathbb{Z}_S^*$ denotes the unit group of $\mathbb{Z}_S$, b is a non-zero rational integer with $(b, p_1 \dots p_s) = 1$ if $s > 0$, and $F(\mathbf{X}) = F(X_1, \dots, X_m) \in \mathbb{Z}_S[X_1, \dots, X_m]$ is a *decomposable polynomial*, that is a polynomial which factorizes into linear factors with algebraic coefficients. Equations (0.1), (0.2) and (0.3) are called *decomposable polynomial equations*, and in particular (0.2) a *decomposable polynomial equation of Mahler type*. Very important is the case when F is homogeneous, in this case (0.1), (0.2) and (0.3) are called *decomposable form equations*. The most important classes of decomposable polynomial

equations are Thue equations, Thue-Mahler equations, norm form equations, discriminant form equations, index form equations, resultant form equations, and their inhomogeneous generalizations. They have many significant applications, among others in algebraic number theory. For the extremely rich literature of these equations and their applications, here we refer to the books [7], [19], [39], [40] and the survey papers [12], [16], [27], [28].

As is known, in case of decomposable form equations (0.2) and (0.3) are in fact equivalent, and the number of solutions of (0.2) coincides with the number of so-called “cosets of solutions” of (0.3) (cf. Chapters 2,3). In the inhomogeneous case, we cannot speak about “cosets of solutions”, but the number of solutions of (0.2) does not exceed that of (0.3). Hence, in this case it is enough to derive bounds for the number of solutions of (0.3).

The main results of the first chapter provide explicit upper bounds for the number of solutions of general decomposable polynomial equations of the form (0.1) and (0.3). Some consequences are also presented to certain important special types of decomposable polynomial equations. We note that all the results obtained in the first chapter are valid also in the case of homogeneous equations, but in this special situation slightly better results are known in the literature. Hence in this chapter we shall restrict ourselves mainly to inhomogeneous equations.

The second and third chapters are devoted to norm form, discriminant form and index form equations, which are particularly important from the point of view of applications. Under certain general conditions we give explicit upper bounds for the number of solutions which are much better than the bounds of the first chapter specialized to the homogeneous case, and provide significant improvements of the previous bounds which were earlier obtained on the equations under consideration.

In Chapters 1,2 and 3, we shall use several deep results from the literature to prove our theorems. We remark that some of these results have been established by means of various recent improvements of Schmidt’s powerful quantitative subspace theorem; for a survey on Schmidt’s theorem and its improvements see [17].

In the fourth chapter, a problem of P. Turán concerning irreducible polynomials is investigated. The problems studied in the first three chapters are clearly of diophantine nature. We note that the study of the irreducibility of polynomials with integer coefficients is also a diophantine question. Indeed, if such a polynomial is not irreducible, then it can be written as a product of

two polynomials with integer coefficients. Now regarding the coefficients of the factors as variables, calculating the product of the two factors and comparing the coefficients of the product with the original polynomial we get a system of diophantine equations to be solved.

In what follows, we briefly present the contents of chapters 1,2,3 and 4, respectively.

I

Decomposable form equations have been very extensively studied in the literature. Various ineffective finiteness results have been established which do not provide, however, any algorithm for determining the solutions. Later, several effective theorems have also been obtained which give explicit upper bounds for the solutions. Further, explicit upper bounds were derived for the number of solutions which bounds are independent of the coefficients of F . For such results we refer to the books [19], [39], [40], the survey papers [12], [16], [26], [27], [28] and the references given there.

The first (ineffective) upper bound for the number of solutions of general inhomogeneous decomposable polynomial equations was given by Evertse, Gaál and Györy in [10]. They provided a necessary and sufficient condition for equation (0.1) to have only finitely many solutions for every S and b . Further, under this finiteness condition they derived an upper bound for the numbers of solutions of such equations. This bound was given explicitly in terms of the numbers of solutions of some appropriate unit equations. However, when [10] was written, no explicit upper bound was known for the number of solutions of unit equations. It should be remarked that the results of [10] were established in a more general situation, for the case when the ground ring is an arbitrary finitely generated integral domain over $\mathbb{Z}$.

Combining the upper bound in [10] with a recent bound of Evertse [8] on the number of solutions of unit equations, one can now give easily an explicit upper bound for the number of solutions of equation (0.1). However, the bound so obtained is very large in terms of the degree of F , because it is an exponential function of the degree of the splitting field of F . In the first chapter we follow a completely different approach, and under the finiteness condition of [10] we give much better upper bounds for the the number of solutions of (0.1) which are already polynomial in terms of the degree of F . Further, we show

that the finiteness criteria of [10] is not valid in the case of the more general equations of the form (0.3). We also give a sufficient condition for the finiteness of the number of solutions of equation (0.3), and under this condition we derive an explicit upper bound for the number of solutions. Further, in the case $b = 1$ we give a bound for the number of solutions of (0.3) subject only to the condition that this number is finite. Several consequences of these results are also presented for special decomposable polynomial equations. We give among others upper bounds for the numbers of solutions of inhomogeneous Thue equations, discriminant polynomial equations, norm polynomial equations and resultant polynomial equations. To prove our theorems, we utilize some deep results of Győry [23] and Evertse and Győry [14] on the number of families of solutions of decomposable form equations whose proofs depend, among other things, on recent quantitative versions of Schmidt's subspace theorem. The results presented in the first chapter are joint results with my supervisor, Prof. K. Győry, and will be published in our joint paper [3].

II

In the second chapter we deal with norm form equations. A norm form is a decomposable form of the type

$$F(\mathbf{X}) := a_0 N_{K/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_m X_m),$$

where $\alpha_1, \dots, \alpha_m$ are linearly independent elements of a number field K of degree n over $\mathbb{Q}$, and a_0 is a non-zero rational number which is chosen so that F has its coefficients in $\mathbb{Z}$.

Let $p_1, \dots, p_s$ be rational primes with $s \geq 0$, and $b \in \mathbb{Z} \setminus \{0\}$ a rational integer which is relatively prime to $p_1, \dots, p_s$ if $s > 0$. The equations of the form

$$\begin{aligned} a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_m x_m) &= b p_1^{z_1} \cdots p_s^{z_s} \\ \text{in } x_1, \dots, x_m &\in \mathbb{Z}, \\ \text{and } z_1, \dots, z_s &\in \mathbb{Z}_{\geq 0} \\ \text{with } (x_1, \dots, x_m, p_1 \cdots p_s) &= 1 \text{ if } s > 0, \end{aligned} \tag{0.4}$$

are called *norm form equations*, and for $s > 0$, *norm form equations of Mahler type*.

In the case $s = 0$, Schmidt [36] gave a criterion for (0.4) to have only finitely many solutions for any $b \in \mathbb{Z} \setminus \{0\}$. In [35] Schlickewei extended Schmidt's result to the case $s > 0$. These results were proved by using Schmidt's subspace theorem, and thus they are ineffective.

Later, Győry and Papp ($s = 0$) and Győry ($s \geq 0$) derived effective finiteness results for a large class of norm form equations; see [19] and [20] for references. For example, Győry [20] derived explicit bounds for the solutions under the assumption that

- (i) $x_m \neq 0$, $\alpha_1 = 1, \alpha_2, \dots, \alpha_{m-1}$ are $\mathbb{Q}$ -linearly independent and α_m has degree at least 3 over $\mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})$,

or that

- (ii) the degree of α_i is at least 3 over $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$ for $i = 2, \dots, m$.

We remark that in (i) and (ii) the conditions concerning the degrees are necessary. Further, it is interesting to note that this finiteness result in the case (i) cannot be deduced even in an ineffective form from the finiteness theorems of Schmidt and Schlickewei. In 1985 Evertse and Győry [11] gave explicit upper bounds for the number of solutions of norm form equations of the form (0.4) under the hypotheses (i) and (ii). Later Győry [23], Evertse [8] and Evertse and Győry [14] derived general upper bounds for arbitrary norm form equations which include the case (ii), but not the case (i). For further results concerning norm form equations, see [39], [27] and the references given there.

In the second chapter we considerably improve the above-mentioned bounds of [11]. Following an idea of Győry, we reduce equation (0.4) to a relative Thue-Mahler equation, and then we use a result of Evertse [9] to estimate the number of solutions of this equation. We also give a further improvement on the number of solutions of (0.4) which is valid for all but at most finitely many possible values of the constant term b of the equation. Our bound obtained under the assumption (ii) is better for almost all b than the general bounds of [23], [8] and [14]. Further, we give an explicit upper bound for the number of exceptional values of b . To prove this result, first we apply Győry's method to reduce equation (0.4) to a system of unit equations and then we use results of Evertse, Győry, Stewart and Tijdeman [15] and Evertse and Győry [14] to derive our upper bound for the number of solutions. The bound for the number of exceptional values is obtained by combining results from [6], [17] and [22]. We note that in [15], [14], [17], and [22] the proofs

of the results in question involve, among other things, the Thue-Siegel-Roth-Schmidt method and its recent quantitative versions. The results of Chapter 2 are published in our paper [2].

III

In the third chapter we present our new results concerning the number of solutions of index form equations. An *index form equation of Mahler type* is an equation of the form

$$\begin{aligned} I(x_2, \dots, x_n) &= \pm I p_1^{z_1} \dots p_s^{z_s} \\ \text{in } x_2, \dots, x_n &\in \mathbb{Z}, \\ \text{and } z_1, \dots, z_s &\in \mathbb{Z}_{\geq 0} \\ \text{with } (x_2, \dots, x_n, p_1 \dots p_s) &= 1 \text{ if } s > 0, \end{aligned} \tag{0.5}$$

where $I(\mathbf{X}) = I(X_2, \dots, X_n)$ is the index form corresponding to a given integral basis of a given number field K , $p_1, \dots, p_s$ are rational primes with $s \geq 0$, and I is a rational integer which is relatively prime to $p_1, \dots, p_s$ if $s > 0$.

The first finiteness result concerning index form equations is due to Győry [18]. He considered the most interesting case when $s = 0$. He first reduced equation (0.5) to a system of unit equations and using his effective results on these equations he gave explicit upper bounds for the solutions of (0.5). Győry's result was later generalized to Mahler type equations by Trelina [42] and Győry and Papp [29].

In 1985, Evertse and Győry [11] derived an explicit upper bound for the number of solutions of equation (0.5). This bound was a consequence of their more general result on decomposable form equations. Later, Evertse [8] and Evertse and Győry [14] improved their results on decomposable form equations, and thereby also the bounds for the number of solutions of equation (0.5). For further results concerning discriminant and index form equations see the survey paper [28] and the references given there.

For given $n \geq 5$, almost all number fields K of degree n have the property that the Galois group of K (more precisely, that of the normal closure of K over $\mathbb{Q}$) is triply transitive. In the important special case when the Galois group, $\mathcal{G}$, of K is triply transitive, Győry [28] improved considerably the bounds established in [11] and [8] for the number of solutions of (0.5). In the third chapter, under the same assumptions on the Galois group $\mathcal{G}$ we considerably

improve the bound of Evertse and Győry [14] for almost all values of I , and we also give a bound for the number of exceptional values of I . To prove this result we use a similar method to that applied in Chapter 2 to norm form equations. We also combine Győry's method on reducing decomposable form equations to unit equations with the above-mentioned results from [15], [14], [6], [17] and [22]. As consequences of our result, we present some results concerning discriminant form equations and the number of elements with given discriminant in a given number field. The results of the third chapter are published in [1].

IV

In the fourth chapter some new results are presented on a problem of P. Turán concerning the “distance” of polynomials to irreducible polynomials. It is well-known that there are infinitely many irreducible polynomials in $\mathbb{Z}[x]$ for each given degree, and that (cf. H.-W. Knobloch [31]) the “majority” of these polynomials are irreducible. This suggests that the “distance” of a polynomial to the “nearest” irreducible polynomial cannot be too large. By the “distance” of two polynomials in $\mathbb{Z}[x]$ we mean the following. The sum of the absolute values of the coefficients of a polynomial $P \in \mathbb{Z}[x]$ is called the length of P , and is denoted by $|P|$. The distance of two polynomials $P, Q \in \mathbb{Z}[x]$ is then defined as $|P - Q|$.

P. Turán asked the following question: Does there exist an absolute constant C_1 such that for every $P(x) \in \mathbb{Z}[x]$ of degree n , there is a polynomial $Q(x) \in \mathbb{Z}[x]$ which is irreducible over $\mathbb{Q}$, and satisfies the conditions that $\deg(Q) \leq n$ and $|P - Q| \leq C_1$?

This problem turned out to be a very hard one. The best known result in this direction is due to Schinzel [34], who gave an affirmative answer to the above question in the case when we omit the condition $\deg(Q) \leq n$. For a related result see Győry [25].

Using computational methods, in [4] we proved with Hajdu that for polynomials of degree ≤ 22 we have $C_1 \leq 4$. This result was included in [30].

Later, we continued our work on Turán's problem, and the fourth chapter contains our new results on the topic. On one hand, we refined our algorithms and we extended our result to polynomials of degree ≤ 24 . These results have been published in [5]. On the other hand, quite recently we have obtained some new results concerning extreme polynomials (for a definition see Chapter 4). These results are not published yet.

Chapter 1

On the number of solutions of general decomposable polynomial equations

1.1 Introduction

Let $F(\mathbf{X}) = F(X_1, \dots, X_m) \in \mathbb{Q}[X_1, \dots, X_m]$ be a *decomposable polynomial* of degree $n \geq 3$ in $m \geq 2$ variables, that is a polynomial which can be written in the form

$$F(\mathbf{X}) = \prod_{i=1}^n l_i(\mathbf{X}),$$

where $l_1(\mathbf{X}), \dots, l_n(\mathbf{X})$ are linear polynomials with coefficients in an algebraic number field G . This factorization is unique up to proportional factors from G^* . Let $S = \{p_1, \dots, p_s\}$ be a finite set of $s \geq 0$ rational primes, and denote by $\mathbb{Z}_S$ the ring of S -integers in $\mathbb{Q}$. Consider the equation

$$F(\mathbf{x}) = b \quad \text{in } \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \quad (1.1)$$

where b is a given non-zero S -integer. We assume throughout the present chapter that F has its coefficients in $\mathbb{Z}_S$. Then (1.1) is called a *decomposable polynomial equation* over $\mathbb{Z}_S$. If in particular F is a form, (1.1) is a decomposable form equation.

We recall (cf. [13]) that if $\mathcal{F}$ is a finite set of linear forms in $G[X_1, \dots, X_k]$, $k \geq 2$, then a non-zero $\mathbb{Q}$ -linear subspace V of the vector space $\mathbb{Q}^k$ is called

$\mathcal{F}$ -non-degenerate if $\mathcal{F}$ contains a subset of at least three linear forms whose restrictions to V are linearly dependent, but pairwise linearly independent. Otherwise V is called $\mathcal{F}$ -degenerate. Further, V is called $\mathcal{F}$ -admissible if no form in $\mathcal{F}$ vanishes identically on V .

Denote by $\mathcal{L}$ a maximal subset of pairwise linearly independent polynomials among the linear factors $l_1, \dots, l_n$ of F over G . Put

$$\mathcal{L}^* = \{X_{m+1}\} \cup \left\{ X_{m+1} \cdot l \left(\frac{X_1}{X_{m+1}}, \dots, \frac{X_m}{X_{m+1}} \right) : l \in \mathcal{L} \right\}.$$

Then $\mathcal{L}^*$ consists of linear forms in $X_1, \dots, X_{m+1}$ with coefficients in G .

It was shown in [10], Theorem 1, that (1.1) has only finitely many solutions for every S and b if and only if the following condition holds: (i) the linear forms in $\mathcal{L}^*$ have rank $m+1$ over G , and every $\mathcal{L}^*$ -admissible linear subspace of $\mathbb{Q}^{m+1}$ of dimension ≥ 3 is $\mathcal{L}^*$ -non-degenerate. Further, under the assumption (i), a non-explicit bound was derived (cf. [10], Theorem 2) for the number of solutions of (1.1) which does not depend on the coefficients of F . This bound was given explicitly in terms of the numbers of solutions of some unit equations. However, when the paper [10] was written, no explicit upper bound was available on the number of solutions of unit equations. On combining the bound of [10] with an explicit upper bound of Evertse [8] on the number of solutions of unit equations, one can easily show that under the assumption (i), our equation (1.1) has at most

$$n (2^{18}m)^{g(m+2)^4(s+\omega_S(b)+1)/2} \quad (1.2)$$

solutions. Here $\omega_S(b)$ denotes the number of those distinct primes p , not contained in S , for which $p|b$ in $\mathbb{Z}_S$, and g denotes the degree of the field G over $\mathbb{Q}$. If G is chosen to be the splitting field of F over $\mathbb{Q}$ then $g \leq n!$, and this bound for g cannot be diminished in general.

In this chapter we give a much better explicit upper bound for the number of solutions of (1.1) which is already polynomial in terms of n . Further, we extend our result to the more general equation

$$F(\mathbf{x}) \in b\mathbb{Z}_S^* \quad \text{in } \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \quad (1.3)$$

where $\mathbb{Z}_S^*$ denotes the group of S -units in $\mathbb{Z}_S$. We point out that under the assumption (i) this equation may have infinitely many solutions. Then we show that (i) together with the condition that (i') for at least one polynomial

$l^* \in \mathcal{L}^*$ we have $l^*(\mathbf{a}) \neq 0$ for any $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$, imply already the finiteness of the number of solutions. Further, under these assumptions we derive explicit upper bounds for the number of solutions of (1.3). Moreover, for $b = 1$, we give a similar upper bound, provided only that the number of solutions of (1.3) is finite.

The significant improvement in our bounds is due to a new approach which is different from that of [10]. As a generalization of Schmidt's famous results [37] on norm form equations, Györy [23] proved that in case of homogeneous F , the set of solutions of both (1.1) and (1.3) is the union of finitely many so-called families of solutions. Further, he gave an explicit upper bound for the number of these families. This bound was later improved by Evertse and Györy [14]. In the proofs of our main results we first reduce equations (1.1) and (1.3) to homogeneous decomposable polynomial equations in $m+1$ unknowns. Then we apply the above-mentioned results of [23] and [14] to derive bounds for the numbers of solutions of (1.1) and (1.3).

We give several consequences for inhomogeneous Thue equations, discriminant polynomial equations, norm polynomial equations and resultant polynomial equations. In particular, our results are valid also in the homogeneous case. However, in this case slightly better estimates are known in the literature, hence we shall not deal here with applications of our results to decomposable form equations.

1.2 Main new results

To state our results we need some further notation. For a prime p not contained in S , denote by $\text{ord}_p(b)$ the greatest integer a such that $p^a | b$ in $\mathbb{Z}_S$. Put

$$\psi_S(b, n, m) = \binom{n+1}{m}^{\omega_S(b)} \prod_{\substack{p \text{ prime} \\ p \notin S}} \binom{\text{ord}_p(b) + m}{m}$$

where the product is taken over all primes p not contained in S , and let

$$\delta(m) = \frac{2}{3}(m+1)(m+2)(2m+3) - 4.$$

We note that $\delta(m) \leq 2(m+1)^3$. We also use the notation introduced in Section 1.1.

Theorem 1.1. *Suppose that*

- (i) the linear forms in $\mathcal{L}^*$ have rank $m+1$ over G , and every $\mathcal{L}^*$ -admissible linear subspace of $\mathbb{Q}^{m+1}$ of dimension ≥ 3 is $\mathcal{L}^*$ -non-degenerate.

Then the number of solutions of equation (1.1) does not exceed the bounds

$$n \left(2^{17} n \right)^{\delta(m)(s+1)} \cdot \psi_S(b, n, m) \quad (1.4)$$

and

$$n \left(2^{17} n \right)^{\delta(m)(s+\omega_S(b)+1)}. \quad (1.5)$$

As is easily seen, the bound (1.5) is in general much better than (1.2). In the special case when in (1.1) F is homogeneous, the assumption (i) is equivalent (cf. [10], Corollary 1) to the fact that every $\mathcal{L}$ -admissible linear subspace of $\mathbb{Q}^m$ of dimension ≥ 2 is $\mathcal{L}$ -non-degenerate. In this case slightly better bounds are given in [8] and [14] for the number of solutions of (1.1).

Our example given below shows that in contrast with the case of decomposable form equations, Theorem 1.1 cannot be generalized for decomposable polynomial equations of the form (1.3). However, if we replace condition (i) of Theorem 1.1 with a stronger assumption, we are able to derive a finiteness theorem and explicit bounds for the number of solutions of (1.3).

Theorem 1.2. *Suppose that the condition (i) holds, and that*

- (i') *for at least one polynomial $l^* \in \mathcal{L}^*$ we have $l^*(\mathbf{a}) \neq 0$ for any $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$.*

Then the number of solutions of equation (1.3) does not exceed the bound

$$\left(2^{17} n \right)^{\delta(m)(s+\omega_S(b)+1)}. \quad (1.6)$$

As a consequence of Theorem 1.2 we give now another finiteness condition for the number of solutions of (1.3) which is sometimes easier to check. Let $\mathcal{L}_0^* = \mathcal{L}^* \setminus \{X_{m+1}\}$.

Corollary 1.1. *Suppose that*

- (ii') *$\mathcal{L}_0^*$ has rank $m+1$ over G , and that $l^*(\mathbf{a}) \neq 0$ for each $l^* \in \mathcal{L}_0^*$ and for any $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$.*

Then the number of solutions of (1.3) does not exceed the bound (1.6).

We note that in the inhomogeneous case our Theorem 1.2 and Corollary 1.1 provide bounds also for the number of solutions of the corresponding Mahler type equation of the form (0.2).

The following example shows that condition (i') in Theorem 1.2 is also necessary.

Example: Put $S = \{5, 13\}$ and consider the polynomial $F(X_1, X_2) = (4X_1 + 6X_2 - 5)(X_2 + 4)(X_2 + 12) \in \mathbb{Z}_S[X_1, X_2]$. This polynomial satisfies the condition (i) of Theorem 1.2, but there is no linear factor l of F for which the corresponding linear form $l^*(X_1, X_2, X_3)$ has the property that $l^*(x_1, x_2, x_3) \neq 0$ for $(0, 0, 0) \neq (x_1, x_2, x_3) \in \mathbb{Q}^3$. It is easy to see that the equation

$$F(x_1, x_2) \in \mathbb{Z}_S^* \text{ in } x_1, x_2 \in \mathbb{Z}_S$$

has infinitely many solutions of the form $(x_1, 1)$.

Theorem 1.3. *Assume that $\text{rank}(\mathcal{L}^*) = m + 1$ and $b = 1$. If the number of solutions of (1.3) is finite, then this number does not exceed the bound*

$$(2^{17}n)^{\delta(m)(s+1)}. \quad (1.7)$$

In the next section we formulate some consequences and applications of our Theorems 1.1 to 1.3. Following our proofs, our results could be extended to the case when the ground ring is a ring of S -integers of an arbitrary number field. We shall not work this out here.

1.3 Some consequences and applications

First let $F_0(\mathbf{X}) = F_0(X_1, \dots, X_m) \in \mathbb{Z}_S[X_1, \dots, X_m]$ be a *decomposable form* in $m \geq 2$ variables and assume that

$$F_0(\mathbf{X}) = \prod_{i=1}^n h_i(\mathbf{X})$$

with linear forms $h_i(\mathbf{X}) \in G[X_1, \dots, X_m]$ for $i = 1, \dots, n$. Let $\mathcal{L}_0$ denote a maximal subset of pairwise non-proportional linear forms in $\{h_1, \dots, h_n\}$ over G . Let Λ be the set of all n -tuples $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n) \in G^n$ for which the decomposable polynomial

$$F_{\boldsymbol{\lambda}}(\mathbf{X}) = \prod_{i=1}^n (h_i(\mathbf{X}) + \lambda_i)$$

has its coefficients in $\mathbb{Z}_S$. Clearly, $F_0(\mathbf{X}) = F_0(\mathbf{X})$, hence $\mathbf{0} \in \Lambda$. Our Theorem 1.1 implies the following.

Corollary 1.2. *Suppose that*

(ii) *every subspace of $\mathbb{Q}^m$ of dimension ≥ 2 is $\mathcal{L}_0$ -non-degenerate.*

Then for any $b \in \mathbb{Z}_S \setminus \{0\}$ and for every fixed $\lambda \in \Lambda$, the number of solutions of the equation

$$F_\lambda(\mathbf{x}) = b \quad \text{in } \mathbf{x} \in \mathbb{Z}_S^m \quad (1.8)$$

does not exceed the bounds occurring in (1.4) and (1.5).

In what follows, we apply Corollary 1.2 to inhomogeneous Thue equations, discriminant polynomial equations and norm polynomial equations. In case of equations considered over $\mathbb{Z}_S$, our Corollary 1.2 and Corollaries 1.3, 1.5 and 1.7 below give improved, explicit versions of Corollaries 2 to 5 of [10] in which non-explicit bounds were given for the numbers of solutions of the corresponding equations.

Let $F(X_1, X_2) \in \mathbb{Z}_S[X_1, X_2]$ be a decomposable polynomial of degree n . Assume that

$$F(X_1, X_2) = \prod_{i=1}^n (h_i(X_1, X_2) + \lambda_i) \quad (1.9)$$

where $h_i(X_1, X_2)$ is a linear form with coefficients in G and $\lambda_i \in G$ for $i = 1, \dots, n$. Let b be a non-zero S -integer.

Corollary 1.3. *Suppose that*

(iii) *there are at least three pairwise linearly independent forms among $h_1(X_1, X_2), \dots, h_n(X_1, X_2)$.*

Then the number of solutions of the inhomogeneous Thue equation

$$F(x_1, x_2) = b \quad \text{in } x_1, x_2 \in \mathbb{Z}_S \quad (1.10)$$

does not exceed the bounds

$$n (2^{17} n)^{52(s+1)} \cdot \psi_S(b, n, 2)$$

and

$$n (2^{17} n)^{52(s+\omega_S(b)+1)}.$$

From Theorem 1.2 we shall deduce the following.

Corollary 1.4. *Suppose that*

- (iii') *there are at least three linearly independent polynomials among $h_1(X_1, X_2) + \lambda_1, \dots, h_n(X_1, X_2) + \lambda_n$, and that for some i , $h_i(x_1, x_2) \notin \{0, -\lambda_i\}$ for any $(0, 0) \neq (x_1, x_2) \in \mathbb{Q}^2$.*

Then the number of solutions of the equation

$$F(x_1, x_2) \in b\mathbb{Z}_S^* \quad \text{in} \quad x_1, x_2 \in \mathbb{Z}_S \quad (1.11)$$

does not exceed the bound

$$(2^{17}n)^{52(s+\omega_S(b)+1)}.$$

The bounds in Corollaries 1.3 and 1.4 are valid also in the case of Thue and Thue-Mahler equations, when $\lambda_i = 0$ for $i = 1, \dots, n$. However, when in (1.10) $F(X_1, X_2)$ is an irreducible binary form, Evertse [9] obtained a much better bound for the numbers of solutions of (1.10) and (1.11).

Let M be a number field of degree $n \geq 3$, $\alpha_0 = 1, \alpha_1, \dots, \alpha_m$ linearly independent elements of M over $\mathbb{Q}$ such that $M = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$, and λ an arbitrary element of M . Let $\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_n$ be the $\mathbb{Q}$ -isomorphisms of M into $\mathbb{C}$. For any $\alpha \in M$, let $\alpha^{(i)} = \sigma_i(\alpha)$. Put

$$L^{(i)}(\mathbf{X}) := X_0 + \alpha_1^{(i)} X_1 + \dots + \alpha_m^{(i)} X_m + \lambda^{(i)}$$

with the convention that $L(\mathbf{X}) = L^{(1)}(\mathbf{X})$. Then the decomposable polynomial

$$D_{M/\mathbb{Q}}(L(\mathbf{X})) := \prod_{1 \leq i < j \leq n} (L^{(i)}(\mathbf{X}) - L^{(j)}(\mathbf{X}))^2$$

is called a *discriminant polynomial*. We consider the *discriminant polynomial equation*

$$a_0 D_{M/\mathbb{Q}}(\alpha_1 x_1 + \dots + \alpha_m x_m + \lambda) = b \quad \text{in} \quad x_1, \dots, x_m \in \mathbb{Z}_S, \quad (1.12)$$

where $a_0 \in \mathbb{Q}^*$, $b \in \mathbb{Z}_S \setminus \{0\}$. Further, suppose that a_0 is chosen such that the discriminant polynomial $a_0 D_{M/\mathbb{Q}}(\alpha_1 X_1 + \dots + \alpha_m X_m + \lambda)$ has its coefficients in $\mathbb{Z}_S$.

Corollary 1.5. *Under the above conditions, the number of solutions of equation (1.12) does not exceed the bounds (1.4) and (1.5) with n replaced by $n(n-1)$.*

In the important special case $\lambda = 0$, somewhat better bounds follow for the number of solutions of (1.12) from the results of [8] and [14] concerning decomposable form equations. Under some conditions on the normal closure of $M/\mathbb{Q}$, even better bounds can be found in [11], [1] and [28] for $\lambda = 0$.

With the above assumptions, consider the following generalization

$$a_0 D_{M/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_m x_m + \lambda) \in b \mathbb{Z}_S^* \quad \text{in } x_1, \dots, x_m \in \mathbb{Z}_S \quad (1.13)$$

of equation (1.12). From Corollary 1.1 we shall deduce the next

Corollary 1.6. *Suppose that the number field M has no proper subfield, and that $1, \alpha_1, \dots, \alpha_m, \lambda$ are linearly independent over $\mathbb{Q}$. Then the number of solutions of the equation (1.13) does not exceed the bound (1.6) with n replaced by $n(n-1)$.*

In the case $\lambda = 0$, the results of [8] and [14] concerning decomposable form equations provide somewhat better bounds for the number of solutions of (1.13).

Let again M be a number field of degree $n \geq 3$, $\alpha_1 = 1, \alpha_2, \dots, \alpha_m$ linearly independent elements of M over $\mathbb{Q}$ such that $M = \mathbb{Q}(\alpha_2, \dots, \alpha_m)$, and $\lambda \in M$. As above, put

$$L^{(i)}(\mathbf{X}) := \alpha_1^{(i)} X_1 + \cdots + \alpha_m^{(i)} X_m + \lambda^{(i)}.$$

Then the polynomial

$$N_{M/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_m X_m + \lambda) = \prod_{i=1}^n L^{(i)}(\mathbf{X})$$

is called a *norm polynomial*. Consider the *norm polynomial equation*

$$a_0 N_{M/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_m x_m + \lambda) = b \quad \text{in } x_1, \dots, x_m \in \mathbb{Z}_S, \quad (1.14)$$

where $b \in \mathbb{Z}_S \setminus \{0\}$, and $a_0 \in \mathbb{Q}^*$ is chosen so that the norm polynomial $a_0 N_{M/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_m X_m + \lambda)$ has its coefficients in $\mathbb{Z}_S$.

Denote by $\mathcal{M}$ the $\mathbb{Z}$ -module generated by $\alpha_1, \dots, \alpha_m$ in M . $\mathcal{M}$ is called *non-degenerate* if the $\mathbb{Q}$ -vector space generated by $\mathcal{M}$ does not contain any subspace of the form $\mu M'$ where $\mu \in M^*$ and M' is a subfield of M such that $\mathbb{Q} \subsetneq M' \subseteq M$. Otherwise $\mathcal{M}$ is called *degenerate*.

Corollary 1.7. *Suppose that*

(iv) $\mathcal{M}$ *is non-degenerate.*

Then the number of solutions of the equation (1.14) does not exceed the bounds occurring in (1.4) and (1.5).

We note that for $\lambda = 0$, slightly better bounds are given in [8] and [14] for the number of solutions of (1.14).

As a generalization of (1.14), consider now the equation

$$a_0 N_{M/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_m x_m + \lambda) \in b \mathbb{Z}_S^* \quad \text{in} \quad x_1, \dots, x_m \in \mathbb{Z}_S. \quad (1.15)$$

It is an immediate consequence of Corollary 1.1 that if $\alpha_1, \dots, \alpha_m$ and λ are linearly independent over $\mathbb{Q}$ then the number of solutions of equation (1.15) does not exceed the bound (1.6). However, the number of solutions of (1.15) can be finite also in the case when $\alpha_1, \dots, \alpha_m$ and λ are linearly dependent. The following corollary follows immediately from our Theorem 1.3.

Corollary 1.8. *Suppose that for $b = 1$ equation (1.15) has only finitely many solutions. Then the number of these solutions does not exceed the bound (1.7).*

Finally, we apply Corollary 1.2 to resultant equations. Let $P \in \mathbb{Z}_S[X]$ be a polynomial of degree $n \geq 3$ with leading coefficient a_0 and without multiple zeros. Let $\alpha_1, \dots, \alpha_n$ denote the zeros of P , and put $G = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Fix a positive integer m , and let $\lambda = (\lambda_1, \dots, \lambda_n) \in G^n$ such that the decomposable polynomial

$$a_0^m \prod_{i=1}^n (\alpha_i^m X_0 + \alpha_i^{m-1} X_1 + \cdots + X_m + \lambda_i) \quad (1.16)$$

has its coefficients in $\mathbb{Z}_S$. This is the case e.g. for $\lambda = \mathbf{0}$ when the corresponding decomposable form in (1.16) is just the resultant $\text{Res}(P, Q)$ of the polynomials $P(X)$ and $Q(X) = X_0 X^m + X_1 X^{m-1} + \cdots + X_m$. Hence in the case $\lambda = \mathbf{0}$ we call (1.16) a *resultant form*, and in general a *resultant polynomial*. We denote this polynomial by $\text{Res}_\lambda(P, Q)$ with the above Q . Consider the *resultant polynomial equation*

$$\text{Res}_\lambda(P, Q) = b \quad \text{in} \quad Q \in \mathbb{Z}_S[X], \quad (1.17)$$

where b is a given non-zero element of $\mathbb{Z}_S$.

It follows from Theorem 5 of [25] that for $\lambda = \mathbf{0}$, $b \in \mathbb{Z}_S^*$ and $m < n/2$, the number of solutions of (1.17) in $Q \in \mathbb{Z}_S[X]$ with degree m is at most

$$2 \left(2^{34} n^2 \right)^{(m+1)^3 (s+1)}. \quad (1.18)$$

Further, it was pointed out in [25] that the assumption $m < n/2$ cannot be replaced by $m \leq n/2$ in general.

From our Corollary 1.2 we shall deduce the following.

Corollary 1.9. *Let m be a positive integer with $m < n/2$, and suppose that $P(X)$ has no non-constant divisor of degree $< m$ in $\mathbb{Q}[X]$. Then the number of solutions $Q(X)$ of (1.17) with degree m does not exceed the bounds (1.4) and (1.5) with m replaced by $m + 1$.*

For $\lambda = \mathbf{0}$ and $b \in \mathbb{Z}_S^*$, our bound (1.5) provided by Corollary 1.9 can be compared with (1.18). It is likely that Corollary 1.9 remains still valid without the assumption that P has no non-constant factor with rational coefficients and with degree less than m .

We note that similar results can be deduced from Theorem 1.2 and Corollary 1.1 for the number of those polynomials $Q \in \mathbb{Z}_S[X]$ for which $\text{Res}_\lambda(P, Q) \in b\mathbb{Z}_S^*$.

1.4 Proofs

To prove our results we shall need some lemmas. First we introduce some further notation.

Let $\hat{F}(\mathbf{X}) \in \mathbb{Z}_S[X_1, \dots, X_k]$, $k \geq 2$, be a decomposable form of degree $r \geq 3$, and assume that there are k linearly independent linear forms among the linear factors of $\hat{F}$ over $\overline{\mathbb{Q}}$. Let b be a non-zero element of $\mathbb{Z}_S$, and consider the decomposable form equation

$$\hat{F}(\mathbf{x}) \in b\mathbb{Z}_S^* \quad \text{in} \quad \mathbf{x} = (x_1, \dots, x_k) \in \mathbb{Z}_S^k. \quad (1.19)$$

We recall that if $\mathbf{x}$ is a solution of (1.19) then so is $\varepsilon\mathbf{x}$ for each $\varepsilon \in \mathbb{Z}_S^*$. Such a set of solutions is called a $\mathbb{Z}_S^*$ -coset of solutions of (1.19). The form $\hat{F}$ is a product of norm forms. More precisely, it can be written in the form

$$\hat{F}(\mathbf{X}) = c \prod_{j=1}^t N_{M_j/\mathbb{Q}}(l_j(\mathbf{X})),$$

where $c \in \mathbb{Q}^*$, $M_1, \dots, M_t$ are algebraic number fields, and $l_j(\mathbf{X})$ is a linear form in $\mathbf{X} = (X_1, \dots, X_k)$ with coefficients in M_j for $j = 1, \dots, t$ (cf [7], pp. 77–81). Let

$$A = M_1 \oplus \dots \oplus M_t$$

denote the direct $\mathbb{Q}$ -algebra sum of $M_1, \dots, M_t$, i.e. the cartesian product $M_1 \times \dots \times M_t$ endowed with coordinatewise addition and multiplication. Thus A is an algebra over $\mathbb{Q}$ with unit element $1_A = (1, \dots, 1)$. Denote by A^* the multiplicative group of invertible elements in A , and by $N_{A/\mathbb{Q}}(a)$ the norm of $a = (\alpha_1, \dots, \alpha_t) \in A$. Then we have

$$N_{A/\mathbb{Q}}(a) = N_{M_1/\mathbb{Q}}(\alpha_1) \dots N_{M_t/\mathbb{Q}}(\alpha_t).$$

Denote by $\mathcal{M}_S$ the finitely generated $\mathbb{Z}_S$ -module

$$\{x = (l_1(\mathbf{x}), \dots, l_t(\mathbf{x})) : \mathbf{x} \in \mathbb{Z}_S^k\}$$

in the algebra A . Now equation (1.19) can be written in the form

$$cN_{A/\mathbb{Q}}(x) \in b\mathbb{Z}_S^* \quad \text{in} \quad x \in \mathcal{M}_S. \quad (1.20)$$

For any algebraic number field M we denote by $\mathcal{O}_{M,S}$ the integral closure of $\mathbb{Z}_S$ in M , and by $\mathcal{O}_{M,S}^*$ the unit group of $\mathcal{O}_{M,S}$. Similarly, for each $\mathbb{Q}$ -subalgebra B of A with $1_A \in B$ we denote by $\mathcal{O}_{B,S}$ the integral closure of $\mathbb{Z}_S$ in B , and by $\mathcal{O}_{B,S}^*$ the unit group of $\mathcal{O}_{B,S}$. The dimension of A as a $\mathbb{Q}$ -vector space is r , and the $\mathbb{Q}$ -vector space $V := \mathcal{M}_S \mathbb{Q}$ generated by $\mathcal{M}_S$ over $\mathbb{Q}$ has dimension k . Put

$$\hat{\psi}_S(b) = \binom{r}{k-1}^{\omega_S(b)} \prod_{\substack{p \text{ prime} \\ p \notin S}} \binom{\text{ord}_p(b) + k - 1}{k - 1}$$

and

$$e(k) = \frac{1}{3}k(k+1)(2k+1) - 2.$$

Lemma 1.1. *The set of solutions of equation (1.20) is contained in some finite union*

$$x_1 \mathcal{O}_{B_1,S}^* \cup \dots \cup x_w \mathcal{O}_{B_w,S}^* \quad \text{with} \quad w \leq (2^{33} r^2)^{e(k)(s+1)} \hat{\psi}_S(b) \quad (1.21)$$

such that for $i = 1, \dots, w$, B_i is a $\mathbb{Q}$ -subalgebra of A with $1_A \in B_i$, and $x_i \in A^*$ with $x_i B_i \subset V$.

Proof. This is a special case of Theorem 1 of [14]. We note that the proof of this theorem of [14] is based on a combination of some deep results of Györy [23] and Evertse [8]. The proof of the result used from [8] depends on Evertse's improvement (cf. [17]) of Schmidt's quantitative subspace theorem. $\square$

We note that the expression $\hat{\psi}_S(b)$ appears in Lemma 4 of [14], and it is an upper bound for the $\mathcal{O}_{A,S}^*$ -cosets of solutions of equation (1.20). Further, Lemma 4 of [14] will be used also in Chapters 2 and 3. So the expressions $\psi_S(b, n, m)$ occurring in Theorem 1.1, $\psi_m(b)$ in Chapter 2 and $\psi(I)$ in Chapter 3 are all derived from the same expression, namely from $\hat{\psi}_S(b)$.

Consider the above factorization of $\hat{F}$ into linear factors, and let $\hat{\mathcal{L}}$ be a maximal subset of pairwise linearly independent linear factors of $\hat{F}$. By the assumption made on the linear factors of $\hat{F}$, $\hat{\mathcal{L}}$ has rank k over $\overline{\mathbb{Q}}$. Hence the linear mapping

$$\Phi: \mathbb{Q}^k \rightarrow V : \quad \mathbf{x} \mapsto (l_1(\mathbf{x}), \dots, l_t(\mathbf{x}))$$

gives an isomorphism between $\mathbb{Q}^k$ and V .

Lemma 1.2. *Let H be a non-zero subspace of the vector space $\mathbb{Q}^k$. Then the following statements are equivalent:*

- (a) H is $\hat{\mathcal{L}}$ -admissible and $\hat{\mathcal{L}}$ -degenerate;
- (b) $\Phi(H) = xB$ for some $x \in \Phi(H) \cap A^*$ and some $\mathbb{Q}$ -subalgebra B of A with $1_A \in B$.

Proof. This is Lemma 8 of [23]. $\square$

Lemma 1.3. *Suppose that every $\hat{\mathcal{L}}$ -admissible linear subspace of $\mathbb{Q}^k$ of dimension ≥ 3 is $\hat{\mathcal{L}}$ -non-degenerate. Then all solutions of (1.19) are contained in a finite union*

$$H_1 \cup \dots \cup H_w$$

of at most two-dimensional subspaces $H_1, \dots, H_w$ of $\mathbb{Q}^k$ such that

$$w \leq (2^{33} r^2)^{e(k)(s+1)} \hat{\psi}_S(b).$$

Proof. Consider equation (1.19) in the form (1.20). By Lemma 1.1, the set of solutions of equation (1.20) is contained in some finite union of the form (1.21) with the properties specified in Lemma 1.1.

Now fix a coset $x_i \mathcal{O}_{B_i, S}^*$ from (1.21). We have $x_i \mathcal{O}_{B_i, S}^* \subset x_i B_i$. Since $x_i B_i$ is a $\mathbb{Q}$ -linear subspace of V with $1_A \in B_i$, there exists a linear subspace H_i of $\mathbb{Q}^k$ such that $\Phi(H_i) = x_i B_i$ and $x_i \in \Phi(H_i) \cap A^*$. Further, for each solution $\mathbf{x}$ of (1.20) which is contained in $x_i B_i$, the corresponding solution $\mathbf{x}$ of (1.19) is contained in H_i , and vica versa. Moreover, by Lemma 1.2 we infer that H_i is an $\hat{\mathcal{L}}$ -admissible and $\hat{\mathcal{L}}$ -degenerate subspace of $\mathbb{Q}^k$. However, by the assumption of our Lemma 1.3, every $\hat{\mathcal{L}}$ -admissible and $\hat{\mathcal{L}}$ -degenerate subspace of $\mathbb{Q}^k$ is of dimension ≤ 2 . This completes the proof of our lemma. $\square$

Lemma 1.4. *Suppose that equation (1.19) has only finitely many $\mathbb{Z}_S^*$ -cosets of solutions. Then this number is at most*

$$(2^{33} r^2)^{e(k)(s+1)} \hat{\psi}_S(b).$$

Proof. This is Corollary 2 in [14]. $\square$

To prove Theorems 1.1, 1.2 and 1.3, we first introduce some notation. Consider equations (1.1) and (1.3), where

$$F(\mathbf{X}) = F(X_1, \dots, X_m) \in \mathbb{Z}_S[X_1, \dots, X_m]$$

is a decomposable polynomial of degree $n \geq 3$ in $m \geq 2$ variables. Let $l_1, \dots, l_n$ denote the linear factors of F over G . Put

$$F^*(\mathbf{X}^*) = F^*(X_1, \dots, X_m, X_{m+1}) = X_{m+1}^{n+1} \cdot F\left(\frac{X_1}{X_{m+1}}, \dots, \frac{X_m}{X_{m+1}}\right),$$

$$l_i^*(\mathbf{X}^*) = X_{m+1} l_i\left(\frac{X_1}{X_{m+1}}, \dots, \frac{X_m}{X_{m+1}}\right), \quad i = 1, \dots, n$$

and

$$l_{n+1}^*(\mathbf{X}^*) = X_{m+1}.$$

Proof of Theorem 1.1. There is a one-to-one correspondence between the solutions $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m$ of (1.1) and the corresponding solutions $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$ of the equation

$$F^*(\mathbf{x}^*) = b \quad \text{in} \quad \mathbf{x}^* \in \mathbb{Z}_S^{m+1}. \quad (1.22)$$

We give an upper bound for the number of solutions of (1.22) with $x_{m+1} = 1$. By applying Lemma 1.3 to this equation we infer that all solutions of (1.22)

are contained in a union $\bigcup_{i=1}^w H_i$ of at most two-dimensional subspaces H_i of $\mathbb{Q}^{m+1}$ with

$$w \leq (2^{33}(n+1)^2)^{e(m+1)(s+1)} \psi_S(b, n, m). \quad (1.23)$$

If $\dim_{\mathbb{Q}} H_i = 1$ then (1.22) can have at most one solution contained in H_i with $x_{m+1} = 1$. Hence it suffices to prove that for each two-dimensional subspace H of $\mathbb{Q}^{m+1}$, there are at most n solutions $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ of (1.22) with $x_{m+1} = 1$ which are contained in H . Suppose that (1.22) has at least two such solutions, say $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$. Then they are $\mathbb{Q}$ -linearly independent elements of H . Fix these $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$. Then for any solution $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ of (1.22) with $x_{m+1} = 1$ which is contained in H , we can write

$$\mathbf{x}^* = \lambda \mathbf{x}_1^* + \mu \mathbf{x}_2^* \quad (1.24)$$

with suitable rational numbers λ, μ . This implies that

$$l_i^*(\mathbf{x}^*) = \lambda l_i^*(\mathbf{x}_1^*) + \mu l_i^*(\mathbf{x}_2^*), \quad i = 1, \dots, n+1 \quad (1.25)$$

which gives $\mu = 1 - \lambda$ for $i = n+1$. From (1.22) we infer that

$$b = F^*(\mathbf{x}^*) = \prod_{i=1}^{n+1} (l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*)\lambda + l_i^*(\mathbf{x}_2^*)) \quad (1.26)$$

which is a polynomial of degree at most n in λ . The assumption of Theorem 1.1 that $\mathcal{L}^*$ has rank $m+1$ over G implies that this is not a constant polynomial in λ . Hence there are at most n possible values of λ for which (1.26) and (1.24) hold. Since $2e(m+1) = \delta(m)$, this proves that the number of solutions of equation (1.1) does not exceed the bound occurring in (1.4).

Next we derive the second bound (1.5) for the number of solutions. Let $S' = S \cup \{p \mid p \text{ prime with } p|b \text{ in } \mathbb{Z}_S\}$ and s' the cardinality of S' . Then $s' = s + \omega_S(b)$. Put $F'(\mathbf{X}) = \frac{1}{b}F(\mathbf{X})$. Then from $F(\mathbf{X}) \in \mathbb{Z}_S[X_1, \dots, X_m]$, $b \in \mathbb{Z}_{S'}^*$ and $S \subset S'$ we deduce that $F'(\mathbf{X}) \in \mathbb{Z}_{S'}[X_1, \dots, X_m]$. Further, the number of solutions of equation (1.1) is not greater than the number of solutions of the equation

$$F'(\mathbf{x}) = 1 \quad \text{in} \quad \mathbf{x} \in \mathbb{Z}_{S'}^m. \quad (1.27)$$

However, the assumption (i) of our Theorem 1.1 clearly holds also for the polynomial F' . Hence, by applying the above-proved statement of our Theorem 1.1 we deduce that equation (1.27) cannot have more than

$$n (2^{17}n)^{\delta(m)(s'+1)} \cdot \psi_{S'}(1, n, m)$$

solutions. Since $\psi_{S'}(1, n, m) = 1$ and $s' = s + \omega_S(b)$, the proof of our Theorem 1.1 is completed. $\square$

Proof of Theorem 1.2. Let $\mathbb{Z}_{S'}$ be as above, and let $\mathbb{Z}_{S'}^*$ denote the unit group of $\mathbb{Z}_{S'}$. For every solution $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m$ of (1.3), the corresponding vector $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$ is a solution of the equation

$$F^*(\mathbf{x}^*) \in \mathbb{Z}_{S'}^* \quad \text{in } \mathbf{x}^* \in \mathbb{Z}_{S'}^{m+1}. \quad (1.28)$$

Further, each $\mathbb{Z}_{S'}^*$ -coset of solutions of (1.28) contains at most one solution of (1.3). Hence it suffices to derive an upper bound for the number of $\mathbb{Z}_{S'}^*$ -cosets of solutions of (1.28).

We may assume without loss of generality that the number field G is a normal extension of $\mathbb{Q}$. Let $\mathcal{O}_{G,S'}$ denote the integral closure of $\mathbb{Z}_{S'}$ in G . By Lemma 2 of [10] we may assume that the linear factors $l_1, \dots, l_n$ of F are chosen so that

$$l_i^*(\mathbf{x}^*) \in \mathcal{O}_{G,S'}^* \quad i = 1, \dots, n \quad (1.29)$$

for each solution $\mathbf{x}^* \in \mathbb{Z}_{S'}^{m+1}$ of (1.28). Further, we may also assume that each element σ of $\text{Gal}(G/\mathbb{Q})$ permutes the linear factors $l_1^*, \dots, l_n^*$ of F^* .

We first show that under the assumption of Theorem 1.2, equation (1.28) has only finitely many $\mathbb{Z}_{S'}^*$ -cosets of solutions. By using Lemma 1.3 we infer again as above that the solutions of (1.28) are contained in a finite union of at most two-dimensional subspaces of $\mathbb{Q}^{m+1}$. Each one-dimensional subspace contains at most one $\mathbb{Z}_{S'}^*$ -coset of solutions. Hence it remains to show that each fixed subspace H of $\mathbb{Q}^{m+1}$ of dimension 2 contains at most finitely many $\mathbb{Z}_{S'}^*$ -cosets of solutions.

The linear factor $l_{n+1}^* = X_{m+1}$ is a divisor of the form $F^*(\mathbf{X}^*)$ over $\mathbb{Z}_{S'}$. Hence (1.28) implies that each $\mathbb{Z}_{S'}^*$ -coset of solutions of (1.28) contains exactly one $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$. Such a solution $\mathbf{x}^*$ will be called normalized.

Suppose that H contains two distinct $\mathbb{Z}_{S'}^*$ -cosets of solutions, say $\mathbf{x}_1^* \mathbb{Z}_{S'}^*$ and $\mathbf{x}_2^* \mathbb{Z}_{S'}^*$, where $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$ are normalized solutions of (1.28). Fix $\mathbf{x}_1^*$ and

$\mathbf{x}_2^*$. Then for each $\mathbb{Z}_{S'}^*$ -coset of solutions $\mathbf{x}^* \mathbb{Z}_{S'}^* \subset H$ where $\mathbf{x}^*$ is normalized we deduce again (1.24), (1.25) and, in place of (1.26),

$$\prod_{i=1}^{n+1} (l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*)\lambda + l_i^*(\mathbf{x}_2^*)) = F^*(\mathbf{x}^*) \in \mathbb{Z}_{S'}^*. \quad (1.30)$$

In (1.24) $\mathbf{x}^*$, $\mathbf{x}_1^*$ and $\mathbf{x}_2^*$ are S' -integers and $\mathbf{x}_1^*$, $\mathbf{x}_2^*$ are fixed. Hence using Cramer's rule one can easily see that there is a finite set S'' of primes with $S'' \supseteq S'$ such that for each $\mathbf{x}^*$ considered above, the corresponding value of λ is contained in $\mathbb{Z}_{S''}$. We show that the polynomial

$$P(\lambda) = \prod_{i=1}^{n+1} (l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*)\lambda + l_i^*(\mathbf{x}_2^*))$$

in λ has at least two distinct zeros. Then, as is known (see e.g. [40], Ch. 10), equation (1.30) has finitely many solutions in λ .

Put $\kappa_i = l_i^*(\mathbf{x}_2^*)/l_i^*(\mathbf{x}_1^*)$ for $i = 1, \dots, n$. If $\kappa_i \in \mathbb{Q}$ for some i , then by (1.29), $\kappa_i \in \mathbb{Q} \cap \mathcal{O}_{G,S'}^* = \mathbb{Z}_{S'}^*$, and so $l_i^*(\mathbf{x}_2^* - \kappa_i \mathbf{x}_1^*) = 0$ where $\mathbf{0} \neq \mathbf{x}_2^* - \kappa_i \mathbf{x}_1^* \in \mathbb{Q}^{m+1}$. However, by our assumption, there is at least one $l^* \in \mathcal{L}^*$ such that $l^*(\mathbf{a}) \neq 0$ for all $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$. Consequently, there exists at least one i such that $\kappa_i \notin \mathbb{Q}$. But $\kappa_i \in G$, hence there is a κ_j which is different from κ_i such that $\kappa_j = \sigma(\kappa_i)$ for some $\sigma \in \text{Gal}(G/\mathbb{Q})$. Then it is easy to check that

$$-l_i^*(\mathbf{x}_2^*)/l_i^*(\mathbf{x}_1^* - \mathbf{x}_2^*) \quad \text{and} \quad -l_j^*(\mathbf{x}_2^*)/l_j^*(\mathbf{x}_1^* - \mathbf{x}_2^*)$$

are distinct zeros of $P(\lambda)$. As was mentioned above, this implies that (1.30) has only finitely many solutions $\lambda \in \mathbb{Z}_{S''}$. Then also equation (1.28) has only finitely many $\mathbb{Z}_{S'}^*$ -cosets of solutions. We can now apply Lemma 1.4 to equation (1.28) with the choice $r = n + 1$, $k = m + 1$, $b = 1$, $S = S'$, and we infer that the number of $\mathbb{Z}_{S'}^*$ -cosets of solutions of (1.28) does not exceed the bound

$$(2^{33}(n+1)^2)^{e(m+1)(s+\omega_S(b)+1)}.$$

Finally, as was mentioned above, this implies the bound (1.6) for the number of solutions of (1.3). □

Proof of Corollary 1.1. In view of Theorem 1.2 we only have to prove that condition (ii') implies conditions (i) and (i'). This means that we have to

prove that under the assumption of our Corollary 1.1 every $\mathcal{L}^*$ -admissible subspace H of $\mathbb{Q}^{m+1}$ of dimension ≥ 3 is $\mathcal{L}^*$ -non-degenerate.

Suppose that H is $\mathcal{L}^*$ -admissible and $\dim_{\mathbb{Q}} H = t \geq 3$. By our assumption we have $\text{rank}(\mathcal{L}_0^*) = m + 1$, and thus we get

$$X_{m+1} = \sum_{i=1}^n c_i l_i^*(\mathbf{X}^*) \quad (1.31)$$

with suitable constants c_i . The subspace H is $\mathcal{L}^*$ -admissible and thus X_{m+1} does not vanish on H . Thus there exists a basis $\mathbf{a}_1^*, \dots, \mathbf{a}_t^*$ of the subspace H such that the $(m+1)$ th coordinate of $\mathbf{a}_1^*$ is 1 and the $(m+1)$ th coordinates of the vectors $\mathbf{a}_2^*, \dots, \mathbf{a}_t^*$ are 0. Put

$$\mathbf{X}^* = Y_1 \mathbf{a}_1^* + \dots + Y_t \mathbf{a}_t^*.$$

Now X_{m+1} takes the form Y_1 on H , and we also have

$$l_i^*(\mathbf{X}^*) = Y_1 l_i^*(\mathbf{a}_1^*) + \dots + Y_t l_i^*(\mathbf{a}_t^*), \quad i = 1, \dots, n$$

on H . Further, by (ii') the coefficients of the forms $Y_1 l_i^*(\mathbf{a}_1^*) + \dots + Y_t l_i^*(\mathbf{a}_t^*)$ are non-zero. Thus among the restrictions of the forms $X_{m+1}, l_1^*(\mathbf{X}^*), \dots, l_n^*(\mathbf{X}^*)$ to the subspace H are at least two which are linearly independent. Further, by (1.31) there are at least three forms among these restrictions which are pairwise linearly independent. However, (1.31) implies that the restrictions of $X_{m+1}, l_1^*, \dots, l_n^*$ to H are linearly dependent. Hence H is $\mathcal{L}^*$ -non-degenerate and Corollary 1.1 follows from Theorem 1.2. $\square$

Proof of Theorem 1.3. Consider equation (1.3) and the corresponding equation (1.28) with $b = 1$. Then in (1.28) we have $S' = S$. Further, for every solution $\mathbf{x} = (x_1, \dots, x_m)$ of (1.3), $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$ is a solution of (1.28). Conversely, in view of $b = 1$ any $\mathbb{Z}_S^*$ -coset of solutions of (1.28) contains exactly one solution $\mathbf{x}^* = (x_1, \dots, x_m, x_{m+1})$ with $x_{m+1} = 1$ and then $\mathbf{x} = (x_1, \dots, x_m)$ is clearly a solution of (1.3). Hence the number of solutions of (1.3) coincides with the number of $\mathbb{Z}_S^*$ -cosets of solutions of (1.28). By applying now Lemma 1.4 to equation (1.28) with $r = n + 1$, $k = m + 1$, $b = 1$ the assertion immediately follows. $\square$

Proof of Corollary 1.2. It was proved in [10] that under the condition (ii) and the other assumptions concerning equation (1.8), the condition (i) of our Theorem 1.1 holds. Hence Corollary 1.2 follows at once from our Theorem 1.1. $\square$

Proof of Corollary 1.3. We prove that under the condition (iii), equation (1.10) satisfies condition (ii) of our Corollary 1.2. By (iii) there are at least three pairwise linearly independent linear forms in the set

$$\mathcal{L}_0 = \{h_1(X_1, X_2), \dots, h_n(X_1, X_2)\}.$$

We may suppose without loss of generality that these independent forms are $h_i(X_1, X_2) = a_i X_1 + b_i X_2$ for $i = 1, 2, 3$. These forms are obviously linearly dependent. Hence $\mathbb{Q}^2$ is $\mathcal{L}_0$ -non-degenerate, and so Corollary 1.3 follows at once from Corollary 1.2. $\square$

Proof of Corollary 1.4. It is easy to check that condition (iii') of Corollary 1.4 implies conditions (i) and (i') of Theorem 1.2 with $m = 2$. Hence Corollary 1.4 follows from Theorem 1.2. $\square$

Proof of Corollary 1.5. We keep the notation of Corollary 1.5. Using some ideas from the proof of Theorem 2 in [11] we prove that equation (1.12) satisfies condition (ii) of Corollary 1.2. Put

$$L_0^{(i)}(\mathbf{X}) := \alpha_1^{(i)} X_1 + \dots + \alpha_m^{(i)} X_m.$$

Denote by $\mathcal{L}_0$ a maximal subset of pairwise linearly independent forms among $L_0^{(i)} - L_0^{(j)}$, $1 \leq i \neq j \leq n$. Using the fact that $1, \alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Q}$ it is easy to see that $\mathcal{L}_0$ has rank m . The set $\mathcal{L}_0$ is spanned by the linear forms $L_0^{(1)} - L_0^{(j)}$, $2 \leq j \leq n$. Then one can easily show that for every subspace V of $\mathbb{Q}^m$ of dimension ≥ 2 there are at least two forms among $L_0^{(1)} - L_0^{(j)}$, $2 \leq j \leq n$, which are linearly independent on V . Without loss of generality we may suppose that these forms are $L_0^{(1)} - L_0^{(2)}$ and $L_0^{(1)} - L_0^{(3)}$. Then clearly $L_0^{(1)} - L_0^{(2)}$, $L_0^{(1)} - L_0^{(3)}$ and $L_0^{(2)} - L_0^{(3)}$ are pairwise linearly independent on V and

$$(L_0^{(1)} - L_0^{(2)}) - (L_0^{(1)} - L_0^{(3)}) + (L_0^{(2)} - L_0^{(3)}) = 0$$

which implies that condition (ii) of Corollary 1.2 holds. Now Corollary 1.5 is a simple consequence of Corollary 1.2. $\square$

Proof of Corollary 1.6. Keeping the above notation, put

$$l^{*(i)}(\mathbf{X}) := \alpha_1^{(i)} X_1 + \cdots + \alpha_m^{(i)} X_m + \lambda^{(i)} X_{m+1}.$$

Denote by $\mathcal{L}_0^*$ a maximal subset of pairwise linearly independent forms among $l^{*(i)} - l^{*(j)}$, $1 \leq i < j \leq n$. We can see as above that $\text{rank}(\mathcal{L}_0^*) = m + 1$. Further, if $l^{*(i)}(\mathbf{a}) - l^{*(j)}(\mathbf{a}) = 0$ for some distinct i, j and some $\mathbf{0} \neq \mathbf{a} \in \mathbb{Q}^{m+1}$, then $l^{*(i)}(\mathbf{a})$ cannot be a primitive element of M . However, by our assumptions the field M is primitive, hence it follows that $l^{*(i)}(\mathbf{a}) \in \mathbb{Q}$ which contradicts the fact that $1, \alpha_1, \dots, \alpha_m$ and λ are linearly independent over $\mathbb{Q}$. Thus the condition (ii') of Corollary 1.1 holds, and Corollary 1.6 follows from Corollary 1.1. $\square$

Proof of Corollary 1.7. As was showed in [10], under the assumptions made in Corollary 1.7, equation (1.14) satisfies the condition (ii) of our Corollary 1.2. Hence Corollary 1.7 follows immediately from Corollary 1.2. $\square$

For any system $\mathcal{F}$ of linear forms with coefficients in a number field G , denote by $\mathcal{V}_G(\mathcal{F})$ the G -vector space generated by the forms in $\mathcal{F}$.

Lemma 1.5. *Let $\hat{F}(X_0, X_1, \dots, X_k)$ ($k \geq 1$) be a decomposable form of degree n with coefficients in $\mathbb{Q}$ which factorizes into linear factors over a number field G . Suppose that any $k + 1$ linear factors in the factorization of $\hat{F}$ are linearly independent. Denote by $\hat{\mathcal{L}}$ a maximal subset of pairwise linearly independent forms among the linear factors of $\hat{F}$. Then for each proper non-empty subset $\hat{\mathcal{L}}_1$ of $\hat{\mathcal{L}}$ we have*

$$\left(\mathcal{V}_G(\hat{\mathcal{L}}_1) \cap \mathcal{V}_G(\hat{\mathcal{L}} \setminus \hat{\mathcal{L}}_1) \right) \cap \hat{\mathcal{L}} \neq \emptyset.$$

Proof. This is proved in the proof of Theorem 3 in [24]. $\square$

Lemma 1.6. *Under the assumptions of Lemma 1.5 the following two statements are equivalent:*

- (a) *Every $\hat{\mathcal{L}}$ -admissible subspace of G^{k+1} of dimension ≥ 2 is $\hat{\mathcal{L}}$ -non-degenerate;*
- (b) *The forms in $\hat{\mathcal{L}}$ have rank $k + 1$ over G and for each proper non-empty subset $\hat{\mathcal{L}}_1$ of $\hat{\mathcal{L}}$ we have*

$$\left(\mathcal{V}_G(\hat{\mathcal{L}}_1) \cap \mathcal{V}_G(\hat{\mathcal{L}} \setminus \hat{\mathcal{L}}_1) \right) \cap \hat{\mathcal{L}} \neq \emptyset.$$

Proof. This is the Proposition in [13]. $\square$

Proof of Corollary 1.9. For convenience, we denote by $F_{\lambda}(X_0, \dots, X_m)$ the resultant polynomial occurring in (1.16). Then for each solution $Q(X) = x_0 X^m + \dots + x_m$ of (1.17), $x_0, \dots, x_m$ is a solution of the equation

$$F_{\lambda}(x_0, \dots, x_m) = b \quad \text{in } x_0, \dots, x_m \in \mathbb{Z}_S. \quad (1.32)$$

Let $\mathcal{L}_0$ denote the set of linear forms

$$h_i(\mathbf{X}) = \alpha_i^m X_0 + \alpha_i^{m-1} X_1 + \dots + X_m, \quad i = 1, \dots, n.$$

It is clear that any $m+1$ forms in $\mathcal{L}_0$ are linearly independent over G , the splitting field of F_{λ} over $\mathbb{Q}$.

By our assumptions, $P(X)$ has no non-constant factor of degree $< m$ in $\mathbb{Q}[X]$. This implies that for given i with $1 \leq i \leq n$, there are no linearly independent vectors $\mathbf{a}_1, \mathbf{a}_2$ in $\mathbb{Q}^{m+1}$ such that $h_i(\mathbf{a}_1) = h_i(\mathbf{a}_2) = 0$. This means that every linear subspace of $\mathbb{Q}^{m+1}$ of dimension ≥ 2 is $\mathcal{L}_0$ -admissible.

We now show that every linear subspace V of $\mathbb{Q}^{m+1}$ of dimension ≥ 2 is $\mathcal{L}_0$ -non-degenerate. Our equation (1.32) satisfies the conditions of Lemma 1.5. Hence we have

$$(\mathcal{V}_G(\mathcal{L}_1) \cap \mathcal{V}_G(\mathcal{L}_0 \setminus \mathcal{L}_1)) \cap \mathcal{L}_0 \neq \emptyset$$

for each proper non-empty subset $\mathcal{L}_1$ of $\mathcal{L}_0$. By Lemma 1.6, this statement is equivalent to the fact that every $\mathcal{L}_0$ -admissible G -linear subspace of G^{m+1} of dimension ≥ 2 is $\mathcal{L}_0$ -non-degenerate. However, this implies that every $\mathcal{L}_0$ -admissible linear subspace V of $\mathbb{Q}^{m+1}$ of dimension ≥ 2 is also $\mathcal{L}_0$ -non-degenerate. This proves our claim above. Therefore condition (ii) of Corollary 1.2 holds for equation (1.32), and Corollary 1.9 follows from Corollary 1.2 with the choice $m+1$ in place of m . $\square$

Chapter 2

On the number of solutions of norm form equations

2.1 Introduction

Let $\alpha_1 = 1, \alpha_2, \dots, \alpha_m$ be linearly independent algebraic numbers over $\mathbb{Q}$ and put $K := \mathbb{Q}(\alpha_1, \dots, \alpha_m)$. Denote by n the degree $[K : \mathbb{Q}]$ of the field K over the rationals and let $\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_n$ be the $\mathbb{Q}$ -isomorphisms of K into $\mathbb{C}$. For any $\alpha \in K$, put $\alpha^{(i)} = \sigma_i(\alpha)$. Consider the linear forms $l^{(i)}(\mathbf{X}) = \alpha_1^{(i)} X_1 + \dots + \alpha_m^{(i)} X_m$ for $i = 1, \dots, n$. We can choose a non-zero rational integer a_0 such that the *norm form*

$$F(\mathbf{X}) := a_0 N_{K/\mathbb{Q}}(\alpha_1 X_1 + \dots + \alpha_m X_m) = a_0 \prod_{i=1}^n l^{(i)}(\mathbf{X})$$

has its coefficients in $\mathbb{Z}$. Let $S = \{p_1, \dots, p_s\}$ be a set of $s \geq 0$ rational primes, and $b \in \mathbb{Z} \setminus \{0\}$ a rational integer which is relatively prime to $p_1, \dots, p_s$ if $s > 0$. The equation

$$\begin{aligned} a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \dots + \alpha_m x_m) &= b p_1^{z_1} \dots p_s^{z_s} \\ \text{in } x_1, \dots, x_m &\in \mathbb{Z}, \\ \text{and } z_1, \dots, z_s &\in \mathbb{Z}_{\geq 0} \\ \text{with } (x_1, \dots, x_m, p_1 \dots p_s) &= 1 \text{ if } s > 0 \end{aligned} \tag{2.1}$$

is called a *norm form equation*, more precisely, for $s > 0$, a *norm form equation of Mahler type*. We note that the well-known Thue equations and Thue-Mahler

equations are special cases of equation (2.1).

Throughout this chapter we identify solutions $\mathbf{x} = (x_1, \dots, x_m), z_1, \dots, z_s$ and $\mathbf{x}' = (x'_1, \dots, x'_m), z'_1, \dots, z'_s$ of equation (2.2) if $\mathbf{x}' = \pm \mathbf{x}$.

Denote by $\mathcal{M} = \{\alpha_1, \dots, \alpha_m\}$ the $\mathbb{Z}$ -module generated by $\alpha_1, \dots, \alpha_m$ in K . In the case when $\mathcal{M}$ is degenerate there is a $b \in \mathbb{Z} \setminus \{0\}$ for which (2.1) has infinitely many solutions for $s = 0$. Using his subspace theorem, Schmidt [36] in the case $s = 0$ showed that if $\mathcal{M}$ is non-degenerate then (2.1) has only finitely many solutions for every $b \in \mathbb{Z} \setminus \{0\}$. This result was generalized to the case $s > 0$ by Schlickewei [35]. Later Schmidt [37] proved that for $s = 0$, the set of solutions of (2.1) is the union of finitely many so-called “families of solutions”. This theorem was generalized to equation (2.1) by Schlickewei [35], to the so-called finitely generated case by Laurent [32], and to arbitrary decomposable form equations by Györy [23].

The results mentioned above are all ineffective. For a large class of norm form equations, effective finiteness results were established by Györy and Papp and Györy; for references see [19] and [20]. In [20] Györy proved in an effective form that if α_m has degree at least 3 over the field $\mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})$ then equation (2.1) has only finitely many solutions with $x_m \neq 0$. In this theorem $x_m \neq 0$ and the condition concerning the degree of α_m are necessary. Further, in this finiteness assertion it can happen that $\mathcal{M}$ is degenerate. Hence this result of Györy does not follow from the theorems of Schmidt and Schlickewei. Evertse and Györy [11] proved in 1985 that under the assumption of Györy’s theorem the number of solutions of (2.1) with $x_m \neq 0$ does not exceed

$$(4 \cdot 7g^{(2s+2\omega(b)+3)})^{m-1}, \quad (2.2)$$

where g denotes the degree of the normal closure of K over $\mathbb{Q}$, and $\omega(b)$ denotes the number of distinct prime factors of b . As a consequence, they obtained a similar bound for the number of all solutions, subject to the condition that the degree of α_i is at least 3 over $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$ for $i = 2, \dots, m$.

For non-degenerate $\mathcal{M}$ and $s = 0$, Schmidt ([38], see also [39]) derived an explicit upper bound for the number of solutions of (2.1), which depends only on n, m and the total number $\Omega(b)$ of prime factors of b . In the proof Schmidt used his quantitative subspace theorem. As a consequence of a more general theorem concerning decomposable form equations, Györy [23] derived an explicit upper bound for the number of families of solutions of (2.1). In particular, this gave an explicit upper bound for the number of solutions, which depends only on n, m, s and $\Omega(b)$, provided that the number of solutions is finite. Under this assumption, Evertse [8] derived later the bound $(2^{33}n^2)^{m^3(s+1)}$

for the number of solutions when $b = 1$. Under the same assumption, Evertse and Győry [14] have recently established the bound

$$(2^{33}n^2)^{e(m)(s+1)} \cdot \psi_m(b) \quad (2.3)$$

for the number of solutions, where $e(m) = \frac{1}{3}m(m+1)(2m+1) - 2$ and

$$\psi_m(b) = \binom{n}{m-1}^{\omega(b)} \prod_{\substack{p|b \\ p \text{ prime}}} \binom{\text{ord}_p(b) + m - 1}{m - 1}.$$

Further, they gave the upper bound

$$(2^{33}n^2)^{e(m)(s+\omega(b)+1)} \quad (2.4)$$

in the non-degenerate case.

Our Corollaries 1.7 and 1.8 in Chapter 1 provide bounds also for the number of solutions of norm *form* equations, but these bounds are slightly weaker than the above-mentioned bounds of Evertse and Győry [14].

In this chapter we give significant improvements of the earlier bounds under the assumptions considered in Győry [20] and Evertse and Győry [11].

2.2 New results

Keeping the notation of Section 2.1, let again $\alpha_1 = 1, \alpha_2, \dots, \alpha_m$ be linearly independent algebraic numbers over $\mathbb{Q}$, let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$, and let $a_0 \neq 0$ be a rational integer such that the norm form $a_0 N_{K/\mathbb{Q}}(\alpha_1 X_1 + \dots + \alpha_m X_m)$ has its coefficients in $\mathbb{Z}$. Let $S = \{p_1, \dots, p_s\}$ be a set of $s \geq 0$ rational primes, denote by $\mathbb{Z}_S$ the ring of S -integers and by Z_S^* the group of S -units in $\mathbb{Q}$, and let b be a non-zero rational integer which is relatively prime to $p_1, \dots, p_s$ if $s > 0$.

Theorem 2.1. *Under the above assumptions, let $L = \mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})$, $d = [K : L]$ and $f = [L : \mathbb{Q}]$. Suppose that $d \geq 3$. Then the number of solutions of equation (2.1) with $x_m \neq 0$ is at most*

$$(5 \cdot 10^6 d)^{(s+\omega(b)+1)f}. \quad (2.5)$$

The bound (2.5) is a significant improvement of the bound (2.2), since it does not depend on the degree of the normal closure of K . It is likely that the factor f is unnecessary in the exponent of our bound. In our case $f \geq m - 1$ holds. When $e(m) > f$, (2.5) is better than (2.4). However, in the non-degenerate case (2.4) is valid for all solutions, including the case $x_m = 0$.

We note that under the conditions of Theorem 2.1, equation (2.1) can have infinitely many solutions with $x_m = 0$ if the $\mathbb{Z}$ -module $\{\alpha_1, \dots, \alpha_{m-1}\}$ is degenerate. Hence the above-mentioned results of [38], [23], [8] and [14] cannot be applied to our situation.

Following a standard argument from [20] or [11], our Theorem 2.1 could be applied to the situation when α_i has degree $d \geq 3$ over $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$ for $i = 2, \dots, m$. Then, with the notation $f = [\mathbb{Q}(\alpha_1, \dots, \alpha_{m-1}) : \mathbb{Q}]$, Theorem 2.1 would give essentially the same bound as in (2.5) for the number of solutions of (2.1). But in this case we have $f \geq 3^{m-1}$, hence (2.4) gives in general a better bound for the number of solutions.

If $s > 0$ and the equation

$$a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \dots + \alpha_m x_m) \in b \mathbb{Z}_S^* \quad \text{in } x_1, \dots, x_m \in \mathbb{Z}_S \quad (2.6)$$

possesses a solution, then clearly it has infinitely many solutions. Indeed, if $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m$ is a solution of equation (2.6) then each element of the set

$$\mathbf{x} \mathbb{Z}_S^* := \{(\varepsilon x_1, \dots, \varepsilon x_m) : \varepsilon \in \mathbb{Z}_S^*\}$$

is also a solution of equation (2.6). Such a set is called a $\mathbb{Z}_S^*$ -coset of solutions of the equation (2.6). Further, for any solution $\mathbf{x}, z_1, \dots, z_s$ of equation (2.1) $\mathbf{x} \mathbb{Z}_S^*$ is a coset of solutions of equation (2.6), and conversely, in each coset of solutions of equation (2.6) there exists exactly one solution of equation (2.1). Thus Theorem 2.1 implies the following corollary.

Corollary 2.1. *Under the assumptions of Theorem 2.1 the number of $\mathbb{Z}_S^*$ -cosets of solutions of the equation (2.6) does not exceed the bound in (2.5).*

Let $\psi_m(b)$ denote the expression defined in Section 2.1.

Theorem 2.2. *Let the assumptions be the same as in Theorem 2.1, and let $n = [K : \mathbb{Q}]$. Then apart from finitely many values of b , equation (2.1) has at most*

$$2\psi_m(b) \quad (2.7)$$

solutions with $x_m \neq 0$. Further, the number of exceptional b 's is at most

$$e^{3 \cdot 30^{20}(n(s+1)+1)}. \quad (2.8)$$

When b is not exceptional and $\text{ord}_p(b)$ is small for all prime divisors p of b , (2.7) gives a considerable improvement of (2.2). As a consequence of Theorem 2.2, we get the following:

Corollary 2.2. *Suppose that in (2.1) α_i has degree at least 3 over the field $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$ for $i = 2, \dots, m$. Then apart from finitely many values of b , equation (2.1) has at most*

$$2m \binom{n}{r}^{\omega(b)} \prod_{\substack{p|b \\ p \text{ prime}}} \binom{\text{ord}_p(b) + m - 1}{m - 1} \quad (2.9)$$

solutions. Here $r = \lfloor n/2 \rfloor$ is the integer part of $n/2$. Further, the number of the exceptional b 's is at most

$$me^{3 \cdot 30^{20}(n(s+1)+1)}.$$

In the case when b is not exceptional and $\text{ord}_p(b)$ is small for each prime $p|b$, our Corollary 2.2 considerably improves Theorem 8 of Evertse and Györy [11] over $\mathbb{Q}$. Furthermore, under the assumptions of the Corollary 2.2 our bound (2.9) is much better than the general bound in (2.3).

Applying the results of our Theorem 2.2 to the case of equation (2.6) we get the following corollary.

Corollary 2.3. *Let the assumptions be the same as in Theorem 2.2. Apart from finitely many values of b , the number of $\mathbb{Z}_S^*$ -cosets of solutions of equation (2.6) does not exceed the bound in (2.7), and the number of exceptional values of b is bounded from above by the expression in (2.8).*

We note that Corollary 2.2 can also be applied similarly to equation (2.6).

Our Theorems 2.1 and 2.2 are valid for $m = 2$, i.e. for the Thue-Mahler equation as well. However, in this special case much better bounds have been established by Evertse [9] and Stewart [41], respectively.

2.3 Auxiliary results

Let F be a number field and let U denote a finite set of places of F , containing all infinite places. Denote the set of U -integers and U -units in F by $\mathcal{O}_U$ and $\mathcal{O}_U^*$, respectively. Let $f(x, y)$ denote a form of degree $r \geq 3$ with coefficients from $\mathcal{O}_U$ and suppose that f is irreducible over F . Then the equation

$$f(x, y) \in \mathcal{O}_U^* \quad \text{in } (x, y) \in \mathcal{O}_U^2 \quad (2.10)$$

is called a Thue-Mahler equation. A coset of solutions of (2.10) is a set $\{\eta(x, y) : \eta \in \mathcal{O}_U^*\}$, where (x, y) is a solution of (2.10).

Lemma 2.1. *The number of cosets of solutions of equation (2.10) is at most*

$$(5 \cdot 10^6 r)^u,$$

where u denotes the cardinality of U .

Proof. This is Theorem 1 in Evertse [9] □

Lemma 2.2. *Let G be a finitely generated subgroup of $(\mathbb{C}^*)^2$ with rank r . Then the number of solutions of the equation*

$$x + y = 1 \quad \text{in } (x, y) \in G \quad (2.11)$$

is bounded by 2^{8r+8} .

Proof. This is a special case of Theorem 1.1 of [6]. □

Let $G \subset \mathbb{C}^*$ be a finitely generated subgroup of the multiplicative group $\mathbb{C}^*$, and let a, b, a', b' be non-zero complex numbers. Then the equations

$$ax + by = 1 \quad \text{in } x, y \in G \quad (2.12)$$

and

$$a'x' + b'y' = 1 \quad \text{in } x', y' \in G$$

are called *equivalent* if $a/a' \in G$ and $b/b' \in G$. Equivalent equations have obviously the same number of solutions.

The number of solutions of the equation

$$x_1 + \cdots + x_n = 1 \quad \text{in } x_1, \dots, x_n \in G$$

with $\sum_{i \in I} x_i \neq 0$ for each non-empty subset I of $\{1, \dots, n\}$ (2.13)

is finite. Denote by $\nu_n = \nu_{n,G}$ this number.

Lemma 2.3. *The number of equivalence classes of equations of the form (2.12) which have more than two solutions is at most*

$$\nu_5 + 12\nu_3 + 30\nu_2^2.$$

Proof. See [22]. This lemma is a quantitative version of the main result of [15]; see also [16]. $\square$

Lemma 2.4. *Let G be a finitely generated subgroup of $\mathbb{C}^*$ with rank r . Then equation (2.13) has at most*

$$e^{(r+2)(6n)^{4n}}$$

solutions.

Proof. Lemma 2.4 is a special case of Theorem 2 of [17]. $\square$

Lemmas 2.3 and 2.4 give the following

Lemma 2.5. *The number of equivalence classes of equations (2.12) having more than two solutions is at most*

$$2e^{(r+2)30^{20}}.$$

Let $T = \{q_1, \dots, q_t\}$ be a set of $t \geq 0$ rational primes. Let $\mathbb{Z}_T$ denote the ring of T -integers, and $\mathbb{Z}_T^*$ the group of T -units in $\mathbb{Q}$. For any algebraic number field L , denote by $\mathcal{O}_L$ the ring of integers and by $\mathcal{O}_L^*$ the group of units in L . Further, denote by M_L the set of all places of L , and by T_L the subset of M_L consisting of all infinite places of L and of those finite places of L which correspond to prime ideals of $\mathcal{O}_L$ lying above rational primes from T . Consider the ring of T_L -integers $\mathcal{O}_{L,T}$ and the group of T_L -units $\mathcal{O}_{L,T}^*$ in L .

Suppose that L is of degree l over $\mathbb{Q}$. Let $\mathcal{M}$ denote a finitely generated $\mathbb{Z}_T$ -module in L . By the dimension of $\mathcal{M}$ we mean the dimension of the $\mathbb{Q}$ -vector space $\mathcal{M}\mathbb{Q}$. Assume that $\mathcal{M}$ has dimension k over $\mathbb{Q}$. Let $\alpha_1, \dots, \alpha_m$ be a set of generators of $\mathcal{M}$ and let $l(\mathbf{X}) := \alpha_1 X_1 + \dots + \alpha_m X_m$. Then $\mathcal{M} = \{x = l(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}_T^m\}$. Fix an element $c \in \mathbb{Q}^*$ for which $cN_{L/\mathbb{Q}}(l(\mathbf{X}))$ has its coefficients in $\mathbb{Z}_T$. Consider the equation

$$cN_{L/\mathbb{Q}}(x) \in I \cdot \mathbb{Z}_T^* \text{ in } x \in \mathcal{M}, \quad (2.14)$$

where I denotes a fixed positive rational integer which is relatively prime to $q_1, \dots, q_t$ if $t > 0$.

Lemma 2.6. *The set of solutions of (2.14) is contained in some union $x_1\mathcal{O}_{L,T}^* \cup \cdots \cup x_r\mathcal{O}_{L,T}^*$, where*

$$r \leq \binom{l}{k-1}^{\omega(I)} \cdot \prod_{\substack{p|I \\ p \text{ prime}}} \binom{\text{ord}_p(I) + k - 1}{k - 1}$$

and where $x_1, \dots, x_r$ are solutions of (2.14).

Proof. This is a special case of Lemma 4 of [14]. □

The statement of Lemma 2.6 is similar to that of our Lemma 1.1 which is a special case of Theorem 1 of [14]. However, Lemma 1.1 gives a more precise description of the set of solutions. On the other hand, in the proofs below the use of our Lemma 2.6 will yield better bounds for the numbers of solutions. We remark that Lemma 4 of [14] was an intermediate step in the proof of Theorem 1 of [14].

2.4 Proofs

Proof of Theorem 2.1. We keep the notation introduced in the previous sections. Further, $\alpha_1, \dots, \alpha_m$, K, L, d and f have the same meaning as in the statement of Theorem 2.1.

Put $n = [K : \mathbb{Q}]$, $l(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_m X_m$ and $l_0(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_{m-1} X_{m-1}$. Suppose that $K = \mathbb{Q}(\xi)$ and denote by $\xi = \xi^{(1)}, \xi^{(2)}, \dots, \xi^{(n)}$ the conjugates of ξ . Let $S' = \{p_1, \dots, p_s, p_{s+1}, \dots, p_{s+\omega(b)}\}$, where the primes $p_{s+1}, \dots, p_{s+\omega(b)}$ are the prime factors of b . As in the previous section, denote by $\mathbb{Z}_{S'}$ and $\mathbb{Z}_{S'}^*$ the ring of S' -integers and the group of S' -units in $\mathbb{Q}$, respectively. Further, we also adopt the notation $\mathcal{O}_{L,S'}$ and $\mathcal{O}_{L,S'}^*$ from the previous section.

Every solution of equation (2.1) is also a solution of the equation

$$a_0 N_{K/\mathbb{Q}}(l(\mathbf{x})) \in \mathbb{Z}_{S'}^* \quad \text{in } \mathbf{x} \in \mathbb{Z}_{S'}^m. \quad (2.15)$$

If equation (2.1) has no solution, then Theorem 2.1 is true. Thus we may suppose that (2.1) has at least one solution. Let $\mathbf{x}_0$ be a solution of (2.1). Thus $\mathbf{x}_0$ satisfies also equation (2.15) and we get $a_0 N_{K/\mathbb{Q}}(l(\mathbf{x}_0)) \in \mathbb{Z}_{S'}^*$. Hence equation (2.15) can be written into the form

$$N_{K/\mathbb{Q}}(l(\mathbf{x})/l(\mathbf{x}_0)) \in \mathbb{Z}_{S'}^*.$$

Further, the form $N_{K/\mathbb{Q}}(l(\mathbf{X})/l(\mathbf{x}_0))$ has its coefficients in $\mathbb{Z}_{S'}$. Thus we get the equation

$$a'_0 N_{K/L}(l(\mathbf{x})) \in \mathcal{O}_{L,S'}^* \quad (2.16)$$

where $a'_0 = 1/N_{K/L}(l(\mathbf{x}_0)) \in L$ and the form $a'_0 N_{K/L}(l(\mathbf{X}))$ has its coefficients in $\mathcal{O}_{L,S'}$. Setting $y = l_0(\mathbf{x}) \in \mathcal{O}_L$, for any solution of equation (2.16) we get a solution (y, x_m) of the equation

$$a'_0 N_{K/L}(y + \alpha_m x_m) \in \mathcal{O}_{L,S'}^* \quad \text{in } y, x_m \in \mathcal{O}_{L,S'}, \quad \text{with } x_m \neq 0. \quad (2.17)$$

Further, for such a solution we have $x_m \in \mathbb{Q}$. Equation (2.17) is in fact a relative Thue-Mahler equation of the form (2.10). Indeed, $[K : L] \geq 3$ and α_m is a primitive element of K over L . Thus we can apply Lemma 2.1, and we get the following: there are at most $N = (5 \cdot 10^6 d)^{(s+\omega(b)+1)f}$ pairs $(\hat{y}, \hat{x}_m) \in \mathcal{O}_{L,S'}^2$ such that any solution (y, x_m) of equation (2.17) can be written in the form

$$y = \eta \hat{y}, \quad x_m = \eta \hat{x}_m, \quad \eta \in \mathcal{O}_{L,S'}^*. \quad (2.18)$$

Each pair $(\hat{y}, \hat{x}_m) \in \mathcal{O}_{L,S'}^2$ can be chosen such that $\hat{x}_m \in \mathbb{Q}$.

Now fix such a pair $(\hat{y}, \hat{x}_m)$. Consider an arbitrary solution $x_1, \dots, x_m$ of (2.1) with $x_m \neq 0$ for which $y = \alpha_1 x_1 + \dots + \alpha_{m-1} x_{m-1} = \eta \hat{y}$, $x_m = \eta \hat{x}_m$ with $\eta \in \mathcal{O}_{L,S'}^*$. Then

$$\alpha_1 \frac{x_1}{\eta} + \dots + \alpha_{m-1} \frac{x_{m-1}}{\eta} = \hat{y}, \quad \frac{x_m}{\eta} = \hat{x}_m.$$

This implies that $\eta \in \mathbb{Z}_{S'}^*$. If now $x'_1, \dots, x'_m$ is another solution of (2.1) with $x'_m \neq 0$ such that $y = \alpha_1 x'_1 + \dots + \alpha_{m-1} x'_{m-1} = \eta' \hat{y}$, $x'_m = \eta' \hat{x}_m$ with some $\eta' \in \mathcal{O}_{L,S'}^*$, then we infer that $x'_i = \frac{\eta'}{\eta} x_i$, $i = 1, \dots, m$. But, by assumption, $(x_1, \dots, x_m, p_1 \dots p_s) = 1$ if $s > 0$. Hence it follows from the equation (2.1) that $\eta' = \pm \eta$. This altogether shows that the number of solutions of equation (2.1) does not exceed the number of pairs $(\hat{y}, \hat{x}_m)$. This means that equation (2.1) has at most N solutions, and this was to be proved. $\square$

Proof of Theorem 2.2. We shall use the previously introduced notation: $\alpha_1, \dots, \alpha_m$, K, L, d and n have the same meaning as in the statement of Theorem 2.2, and we also use the earlier notation $\xi^{(i)}, l(\mathbf{X}), l_0(\mathbf{X}), \mathbb{Z}_S, \mathbb{Z}_S^*, \mathcal{O}_{K,S}$ and $\mathcal{O}_{K,S}^*$, where $S = \{p_1, \dots, p_s\}$.

Each solution $\mathbf{x}$ of equation (2.1) yields a solution of the equation

$$a_0 N_{K/\mathbb{Q}}(l(\mathbf{x})) \in b \cdot \mathbb{Z}_S^* \text{ in } l(\mathbf{x}) \quad (2.19)$$

and we can use Lemma 2.6 to see that the set of solutions $l(\mathbf{x})$ of (2.19) is contained in a union $\delta_1 \mathcal{O}_{K,S}^* \cup \dots \cup \delta_q \mathcal{O}_{K,S}^*$, where $q \leq \psi_m(b)$, with $\psi_m(b)$ introduced in Section 2.1.

Consider now those solutions $\mathbf{x}, z_1, \dots, z_s$ of (2.1) for which the corresponding $l(\mathbf{x})$ belong to the same coset, say $\delta_1 \mathcal{O}_{K,S}^*$. This means that $l(\mathbf{x}) = \delta_1 \varepsilon$, with a suitable $\varepsilon \in \mathcal{O}_{K,S}^*$. Having $[K : L] \geq 3$, the field K has at least 3 $\mathbb{Q}$ -isomorphisms, say $\sigma_1 : \xi^{(1)} \mapsto \xi^{(1)}$, $\sigma_2 : \xi^{(1)} \mapsto \xi^{(2)}$ and $\sigma_3 : \xi^{(1)} \mapsto \xi^{(3)}$ which act on L as the identity map. This means that $l_0^{(1)}(\mathbf{x}) = l_0^{(2)}(\mathbf{x}) = l_0^{(3)}(\mathbf{x}) = \mathbf{y} \in L$, and thus we have the identity

$$(\alpha_m^{(1)} - \alpha_m^{(2)})l^{(3)}(\mathbf{x}) + (\alpha_m^{(2)} - \alpha_m^{(3)})l^{(1)}(\mathbf{x}) + (\alpha_m^{(3)} - \alpha_m^{(1)})l^{(2)}(\mathbf{x}) = 0.$$

This yields

$$\rho_1^* \frac{l^{(1)}(\mathbf{x})}{l^{(3)}(\mathbf{x})} + \rho_2^* \frac{l^{(2)}(\mathbf{x})}{l^{(3)}(\mathbf{x})} = 1 \quad (2.20)$$

with $\rho_1^* = \frac{\alpha_m^{(3)} - \alpha_m^{(2)}}{\alpha_m^{(1)} - \alpha_m^{(2)}}$ and $\rho_2^* = \frac{\alpha_m^{(1)} - \alpha_m^{(3)}}{\alpha_m^{(1)} - \alpha_m^{(2)}}$. Further, we have $l(\mathbf{x}) = \delta_1 \varepsilon$ where $\varepsilon \in \mathcal{O}_{K,S}^*$. Thus (2.20) can be written in the form

$$\rho_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}} + \rho_2 \frac{\varepsilon^{(2)}}{\varepsilon^{(3)}} = 1 \quad (2.21)$$

where $\rho_1 = \frac{\delta_1^{(1)}}{\delta_1^{(3)}} \rho_1^*$ and $\rho_2 = \frac{\delta_1^{(2)}}{\delta_1^{(3)}} \rho_2^*$. Equation (2.21) is a unit equation in the variables $\left(\frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}, \frac{\varepsilon^{(2)}}{\varepsilon^{(3)}}\right)$. Let $\{\varepsilon_1, \dots, \varepsilon_t\}$ be a system of fundamental $S_{K^{(3)}}$ -units for the field $K^{(3)} := \mathbb{Q}(\xi^{(3)})$. Then $t \leq n(s+1) - 1$ and

$$\varepsilon^{(3)} = \theta \varepsilon_1^{a_1} \dots \varepsilon_t^{a_t}$$

where θ is a root of unity in $K^{(3)}$. Now let φ and χ be $\mathbb{Q}$ -isomorphisms of $K^{(3)}$ such that $\varphi(\varepsilon^{(3)}) = \varepsilon^{(1)}$ and $\chi(\varepsilon^{(3)}) = \varepsilon^{(2)}$. Then (2.21) takes the form

$$\rho_1 \frac{\varphi(\theta)}{\theta} \left(\frac{\varphi(\varepsilon_1)}{\varepsilon_1} \right)^{a_1} \dots \left(\frac{\varphi(\varepsilon_t)}{\varepsilon_t} \right)^{a_t} + \rho_2 \frac{\chi(\theta)}{\theta} \left(\frac{\chi(\varepsilon_1)}{\varepsilon_1} \right)^{a_1} \dots \left(\frac{\chi(\varepsilon_t)}{\varepsilon_t} \right)^{a_t} = 1.$$

Now suppose that equation (2.1) has two different solutions $\mathbf{x}, z_1, \dots, z_s$ and $\mathbf{x}', z'_1, \dots, z'_s$ (both corresponding to δ_1) for which the corresponding solutions $\left(\frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}, \frac{\varepsilon^{(2)}}{\varepsilon^{(3)}}\right)$ and $\left(\frac{\varepsilon'^{(1)}}{\varepsilon'^{(3)}}, \frac{\varepsilon'^{(2)}}{\varepsilon'^{(3)}}\right)$ of (2.21) coincide, that is

$$\frac{\varepsilon^{(1)}}{\varepsilon^{(3)}} = \frac{\varepsilon'^{(1)}}{\varepsilon'^{(3)}} \quad \text{and} \quad \frac{\varepsilon^{(2)}}{\varepsilon^{(3)}} = \frac{\varepsilon'^{(2)}}{\varepsilon'^{(3)}}.$$

This, using the notation $\beta := \beta^{(1)} := \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}$ leads to the relation

$$\beta^{(1)} = \beta^{(2)} = \beta^{(3)},$$

which means that $L(\beta)$ is a proper subfield of the field K . From $\beta = \frac{l(\mathbf{x})}{l(\mathbf{x}')}$ we get $l(\mathbf{x}) - \beta l(\mathbf{x}') = 0$, that is $(l_0(\mathbf{x}) - \beta l_0(\mathbf{x}')) + \alpha_m(x_m - \beta x'_m) = 0$. If $x_m - \beta x'_m \neq 0$ we have $\alpha_m = -(l_0(\mathbf{x}) - \beta l_0(\mathbf{x}'))/(x_m - \beta x'_m)$, which means that $\alpha_m \in L(\beta)$, which contradicts the fact that $L(\beta)$ is a proper subfield of the field $K = L(\alpha_m)$. Thus we get $x_m - \beta x'_m = 0$, and so $\beta = \frac{x_m}{x'_m} \in \mathbb{Q}$. Hence $\beta \in \mathbb{Z}_S^*$. Further, $l_0(\mathbf{x}) = \beta l_0(\mathbf{x}')$. The last equality yields

$$(x_1 - \beta x'_1)\alpha_1 + \dots + (x_{m-1} - \beta x'_{m-1})\alpha_{m-1} = 0.$$

By assumption $\alpha_1 = 1, \alpha_2, \dots, \alpha_{m-1}$ are linearly independent over $\mathbb{Q}$, hence this implies that $x_i = \beta x'_i$ for $i = 1, \dots, m-1$. This together with the conditions $(x_1, \dots, x_m, p_1 \dots p_s) = 1$ and $(x'_1, \dots, x'_m, p_1 \dots p_s) = 1$ leads to the conclusion $\beta = \pm 1$. This proves that distinct solutions of equation (2.1) which correspond to the same δ , lead to distinct solutions of equation (2.21).

Now suppose that equation (2.1) has more than two solutions corresponding to the same δ_1 . Then equation (2.21) has also at least 3 solutions. But equation (2.21) is of the type (2.12), where the generators of G are

$$\left\{ \frac{\varphi(\theta)}{\theta}, \frac{\varphi(\varepsilon_1)}{\varepsilon_1}, \dots, \frac{\varphi(\varepsilon_t)}{\varepsilon_t}, \frac{\chi(\theta)}{\theta}, \frac{\chi(\varepsilon_1)}{\varepsilon_1}, \dots, \frac{\chi(\varepsilon_t)}{\varepsilon_t} \right\}.$$

This means that the number of generators of G is at most $2t + 2$ and we can use Lemma 2.5. Thus there exists a finite set $\mathcal{C}_1$ of pairs $(\kappa_1, \kappa_2) \in (\mathbb{C}^*)^2$, which is independent of b , such that

$$\rho_1 = \kappa_1 \eta_1 \quad \text{and} \quad \rho_2 = \kappa_2 \eta_2$$

with $(\kappa_1, \kappa_2) \in \mathcal{C}_1$ and with some fixed $\eta_1, \eta_2 \in G$. Furthermore, by Lemma 2.5

$$\#\mathcal{C}_1 \leq 2 \cdot e^{(2t+3)30^{20}} =: c_1(t).$$

For the moment fix $(\kappa_1, \kappa_2) \in (\mathbb{C}^*)^2$. Then $\left(\eta_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}, \eta_2 \frac{\varepsilon^{(2)}}{\varepsilon^{(3)}}\right)$ will be a solution of the equation

$$\kappa_1 u + \kappa_2 v = 1 \quad \text{in } u, v \in G. \quad (2.22)$$

Equation (2.22) can be transformed into an equation of type (2.11). More precisely it can be written in the form

$$u' + v' = 1 \quad \text{in } (u', v') \in G', \quad (2.23)$$

where G' is the subgroup of $(\mathbb{C}^*)^2$ generated by

$$\begin{aligned} & \left\{ (\kappa_1, 1), \left(\frac{\varphi(\theta)}{\theta}, 1\right), \left(\frac{\varphi(\varepsilon_1)}{\varepsilon_1}, 1\right), \dots, \left(\frac{\varphi(\varepsilon_t)}{\varepsilon_t}, 1\right), \right. \\ & \quad \left(\frac{\chi(\theta)}{\theta}, 1\right), \left(\frac{\chi(\varepsilon_1)}{\varepsilon_1}, 1\right), \dots, \left(\frac{\chi(\varepsilon_t)}{\varepsilon_t}, 1\right), \\ & \quad (1, \kappa_2), \left(1, \frac{\varphi(\theta)}{\theta}\right), \left(1, \frac{\varphi(\varepsilon_1)}{\varepsilon_1}\right), \dots, \left(1, \frac{\varphi(\varepsilon_t)}{\varepsilon_t}\right), \\ & \quad \left. \left(1, \frac{\chi(\theta)}{\theta}\right), \left(1, \frac{\chi(\varepsilon_1)}{\varepsilon_1}\right), \dots, \left(1, \frac{\chi(\varepsilon_t)}{\varepsilon_t}\right) \right\}. \end{aligned}$$

By Lemma 2.2 equation (2.23) has at most

$$2^{8(4t+6)+8} =: c_2(t)$$

solutions. Thus for a fixed pair $(\kappa_1, \kappa_2) \in (\mathbb{C}^*)^2$, $\left(\kappa_1 \eta_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}, \kappa_2 \eta_2 \frac{\varepsilon^{(2)}}{\varepsilon^{(3)}}\right)$ can take at most $c_2(t)$ different values. Now if (κ_1, κ_2) runs through the set $\mathcal{C}_1$, we see that $\kappa_1 \eta_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}$ can take at most $c_1(t)c_2(t)$ different values. Further,

$$c_1(t)c_2(t) \leq e^{3 \cdot 30^{20}(t+1)} \leq e^{3 \cdot 30^{20}(n(s+1)+1)} =: c(n, s).$$

This means that $\kappa_1 \eta_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}$ can take at most $c(n, s)$ different values. Further, we have

$$\kappa_1 \eta_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}} = \rho_1 \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}} = \rho_1^* \frac{\delta_1^{(1)}}{\delta_1^{(3)}} \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}}$$

where ρ_1^* is fixed. Thus we get

$$\delta_1^{(1)} \varepsilon^{(1)} = \mu \delta_1^{(3)} \varepsilon^{(3)} \quad (2.24)$$

where μ can take at most $c(n, s)$ different values. Put $K^{(ij)} := K^{(i)}K^{(j)}$, and take the norm of both sides of (2.24) with respect to $K^{(1,3)}/\mathbb{Q}$. Then from (2.24) and (2.19) we get

$$(b/a_0)^l \mathbb{Z}_S^* \ni N_{K^{(1,3)}/\mathbb{Q}}(\delta_1^{(1)} \varepsilon^{(1)}) = N_{K^{(1,3)}/\mathbb{Q}}(\mu \delta_1^{(3)}) N_{K^{(1,3)}/\mathbb{Q}}(\varepsilon^{(3)})$$

where $l := [K^{(1,3)} : K^{(1)}]$, $N_{K^{(1,3)}/\mathbb{Q}}(\varepsilon^{(3)})$ is an S -unit and $N_{K^{(1,3)}/\mathbb{Q}}(\mu \delta_1^{(3)})$ can take at most $c(n, s)$ values. Thus also b can take at most $c(n, s)$ values, provided that equation (2.1) has more than two solutions corresponding to the same δ_1 .

Otherwise, if b is different from these “exceptional” values, then (using that $\alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Q}$) we find, that equation (2.1) has at most 2 solutions corresponding to the same δ . Thus in this case (2.1) has at most

$$2\psi_m(b)$$

solutions, and this completes the proof of Theorem 2.2. $\square$

Proof of Corollary 2.2. Let $N := e^{3 \cdot 30^{20}(n(s+1)+1)}$. First we prove by induction on m that, under the assumptions of the Corollary 2.2, there is a set $B(m)$ of cardinality $\leq mN$, such that for $b \notin B(m)$, the number of solutions of equation (2.1) is at most $A_m(b) := 2(\psi_m(b) + \dots + \psi_2(b)) + 1$. For $m = 1$ this is obviously true. Suppose that it is true for $m = k - 1$ where $k \geq 2$. Consider (2.1) with $m = k$. By restricting to the solutions with $x_k = 0$ we get a similar equation with the same hypotheses on α_i but with $m = k - 1$. So by the induction hypothesis, there is a finite set $B(k - 1)$ of cardinality $\leq (k - 1)N$ such that for $b \notin B(k - 1)$, the number of solutions of (2.1) with $x_k = 0$ is at most $A_{k-1}(b)$. By Theorem 2.2, there is a finite set $C(k)$ of cardinality $\leq N$ such that for $b \notin C(k)$ equation (2.1) has at most $2\psi_k(b)$ solutions with $x_k \neq 0$. This implies that for $b \notin B(k) := B(k - 1) \cup C(k)$, equation (2.1) has altogether at most $A_{k-1}(b) + 2\psi_k(b) = A_k(b)$ solutions. This completes the induction step. However, $A_m(b) \leq 2m \binom{n}{r}^{\omega(b)} \prod_{\substack{p|b \\ p \text{ prime}}} \binom{\text{ord}_p(b) + m - 1}{m - 1}$, which concludes the proof of Corollary 2.2. $\square$

Chapter 3

On the number of solutions of index form and discriminant form equations

3.1 Introduction and new results

Let K be an algebraic number field of degree $n \geq 3$ with discriminant D_K and ring of integers $\mathcal{O}_K$. Let $\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_n$ denote the $\mathbb{Q}$ -isomorphisms of K in $\mathbb{C}$. For any $\alpha \in K$, put $\alpha^{(i)} = \sigma_i(\alpha)$. Consider an integral basis $\{1, \alpha_2, \dots, \alpha_n\}$ in $\mathcal{O}_K$, and the linear forms $l^{(i)}(\mathbf{X}) = X_1 + \alpha_2^{(i)}X_2 + \dots + \alpha_n^{(i)}X_n$ for $i = 1, \dots, n$, with the convention that $l^{(1)}(\mathbf{X}) = l(\mathbf{X})$. Putting $l_{ij}(\mathbf{X}) = l^{(i)}(\mathbf{X}) - l^{(j)}(\mathbf{X})$,

$$D_{K/\mathbb{Q}}(l(\mathbf{X})) := \prod_{1 \leq i < j \leq n} l_{ij}^2(\mathbf{X}) \quad (3.1)$$

is a decomposable form with coefficients in $\mathbb{Z}$, which is called the *discriminant form* corresponding to the basis $\{1, \alpha_2, \dots, \alpha_n\}$. It can be written in the form

$$D_{K/\mathbb{Q}}(l(\mathbf{X})) = (I(\mathbf{X}))^2 D_K, \quad (3.2)$$

where $I(\mathbf{X}) = I(X_2, \dots, X_n)$ is a decomposable form of degree $n(n-1)/2$ with coefficients in $\mathbb{Z}$. If α is a primitive integral element of K and $\alpha = x_1 + x_2\alpha_2 + \dots + x_n\alpha_n$ with $x_1, \dots, x_n \in \mathbb{Z}$, then $|I(x_2, \dots, x_n)|$ is precisely the index $I(\alpha)$ of α , i.e. the index of the subgroup $\mathbb{Z}^+[\alpha]$ in the additive group $\mathcal{O}_K^+$ of $\mathcal{O}_K$. Hence $I(\mathbf{X})$ is called the *index form* of the basis $\{1, \alpha_2, \dots, \alpha_n\}$.

Let I denote a positive rational integer, and $S = \{p_1, \dots, p_s\}$ a finite set of $s \geq 0$ distinct rational primes. Consider the *index form equation*

$$\begin{aligned} I(x_2, \dots, x_n) &= \pm I p_1^{z_1} \dots p_s^{z_s} \\ &\text{in } x_2, \dots, x_n \in \mathbb{Z}, \\ &\text{and } z_1, \dots, z_s \in \mathbb{Z}_{\geq 0} \\ &\text{with } (x_2, \dots, x_n, p_1 \dots p_s) = 1 \text{ if } s > 0. \end{aligned} \tag{3.3}$$

We may and shall assume that I is relatively prime to $p_1, \dots, p_s$. For $s = 0$, the assumption $(x_2, \dots, x_n, p_1 \dots p_s) = 1$ is omitted. We identify the solutions $\mathbf{x} = (x_2, \dots, x_n), z_1, \dots, z_s$ and $\mathbf{x}' = (x'_2, \dots, x'_n), z'_1, \dots, z'_s$ of (3.3) if $\mathbf{x}' = \pm \mathbf{x}$.

In the most interesting case when $s = 0$, Győry [18] proved that (3.3) has only finitely many solutions, and gave an effective upper bound for the solutions. Later, this theorem was extended to the case $s > 0$ by Trelina [42] and Győry and Papp [29]. For surveys presenting further generalizations, we refer to [19], [21], [17].

The first explicit upper bound for the number of solutions of (3.3) was derived by Evertse and Győry [11]. They showed as a consequence of a more general result that (3.3) has at most

$$(4 \cdot 7^{g(2s+2\omega(I)+3)})^{n-2} \tag{3.4}$$

solutions. Here $\omega(I)$ denotes the number of distinct prime factors of I , and g is the degree of the normal closure of K over $\mathbb{Q}$. Hence $n \leq g \leq n!$.

It follows from a result of Evertse [8] on decomposable form equations that the number of solutions of (3.3) does not exceed

$$(2^{33} r^2)^{(n-1)^3(s+\omega(I)+1)}, \tag{3.5}$$

where $r = n(n-1)/2$. When n is large and g is large with respect to n , this bound is better than (3.4).

We recall some notation from Chapters 1 and 2. Put

$$\psi(I) = \binom{r}{n-2}^{\omega(I)} \prod_{\substack{p|I \\ p \text{ prime}}} \binom{\text{ord}_p(I) + n - 2}{n - 2}$$

with $r = n(n-1)/2$, where the product is taken over all distinct prime factors of I and $\text{ord}_p(I)$ denotes the greatest rational integer a for which p^a divides I

in $\mathbb{Z}$. As a consequence of a more general theorem concerning decomposable form equations, Evertse and Györy [14] derived in 1997 the upper bound

$$(2^{33}r^2)^{e(n)(s+1)}\psi(I) \quad (3.6)$$

for the number of solutions of (3.3). Here $e(n) = \frac{1}{3}(n-1)n(2n-1) - 2$. The bound (3.6) is better than (3.5) when all the exponents $\text{ord}_p(I)$ are small.

Our Corollaries 1.5 and 1.6 in Chapter 1 provide bounds also for the number of solutions of index *form* and discriminant *form* equations, but these bounds are slightly weaker than the above-mentioned bounds of Evertse and Györy [14].

An important special case is when the Galois group, $\mathcal{G}$, of the normal closure of K over $\mathbb{Q}$ is triply transitive. In other words, for any ordered subsets $\{i_1, i_2, i_3\}$ and $\{i'_1, i'_2, i'_3\}$ of $\{1, \dots, n\}$ there is a $\sigma \in \mathcal{G}$ such that if $\alpha \in K$ then $\sigma(\alpha^{(i_k)}) = \alpha^{(i'_k)}$ for $k = 1, 2, 3$. For example, $\mathcal{G}$ is triply transitive if $n \geq 5$ and $\mathcal{G} = S_n$ or A_n . It is important to note that for given n , the Galois group $\mathcal{G}$ is triply transitive for almost all number fields of degree n . Under this assumption concerning $\mathcal{G}$, Györy [28] has recently showed that for $s = 0$ *, equation (3.3) has at most

$$2^{4n(n-1)(\omega(I)+1)+8}$$

solutions. This is a considerable improvement of (3.4) and (3.5) for $s = 0$. In this chapter we improve (3.6) under the same assumption concerning $\mathcal{G}$.

Theorem 3.1. *Suppose that the Galois group $\mathcal{G}$ is triply transitive. Then apart from finitely many values of I , equation (3.3) has at most*

$$2\psi(I)$$

solutions. Further, the number of the exceptional I 's is at most

$$e^{30^{20}n^2(s+1)}.$$

This means that under the assumption of Theorem 3.1 and apart from finitely many values of I , the factor $(2^{33}r^2)^{e(n)(s+1)}$ in (3.6) can be replaced by 2.

*For simplicity, this result was proved in [28] for $s = 0$ only, but the same arguments work for $s > 0$ as well and give the same upper bound with $\omega(I) + s$ instead of $\omega(I)$.

Denote by $\mathbb{Z}_S$ the ring of S -integers, and by $\mathbb{Z}_S^*$ the group of S -units in $\mathbb{Z}$, respectively. The equation

$$I(x_2, \dots, x_n) \in I\mathbb{Z}_S^* \text{ in } x_2, \dots, x_n \in \mathbb{Z}_S \quad (3.7)$$

clearly has infinitely many solutions, provided that it has at least one solution. Indeed, if $\mathbf{x} = (x_2, \dots, x_n) \in \mathbb{Z}_S^{n-1}$ is a solution of equation (3.7) then each element of the set

$$\mathbf{x}\mathbb{Z}_S^* := \{(\varepsilon x_2, \dots, \varepsilon x_n) : \varepsilon \in \mathbb{Z}_S^*\}$$

is also a solution of equation (3.7). Such a set is called a $\mathbb{Z}_S^*$ -coset of solutions of (3.7). Further, for any solution $\mathbf{x}, z_1, \dots, z_s$ of equation (3.3) $\mathbf{x}\mathbb{Z}_S^*$ is a $\mathbb{Z}_S^*$ -coset of solutions of equation (3.7), and conversely, in each coset of solutions of equation (3.7) there exists exactly one solution of equation (3.3). Thus Theorem 3.1 implies the following corollary.

Corollary 3.1. *Let the assumptions be the same as Theorem 3.1. For all but finitely many values of I the number of $\mathbb{Z}_S^*$ -cosets of solutions of equation (3.7) is at most $2\psi(I)$. Further, the number of the exceptional values of I is at most $e^{30^{20}n^2(s+1)}$.*

In view of (3.2) equation (3.7) is equivalent to the discriminant form equation

$$D_{K/\mathbb{Q}}(l(\mathbf{x})) \in D\mathbb{Z}_S^* \text{ in } x_2, \dots, x_m \in \mathbb{Z}_S, \quad (3.8)$$

provided that e.g. $D = I^2 D_K$. We may assume that D is an integer with $(D, p_1 \dots p_s) = 1$ if $s > 0$. Denote by D_K^* the S -free part of the discriminant D_K of the field K . Then (3.8) can have a solution only if $I := \sqrt{|D/D_K^*|}$ is a rational integer. From Theorem 3.1 we get the following corollary.

Corollary 3.2. *Under the assumptions of Theorem 3.1, for all but finitely many values of D , the number of cosets of solutions of the discriminant form equation (3.8) is at most $2\psi(I)$ with $I := \sqrt{|D/D_K^*|} \in \mathbb{Z}$. Further, the number of exceptional values of D is at most $e^{30^{20}n^2(s+1)}$.*

Applying Theorem 3.1 to equation (3.3) in the case $s = 0$, we obtain as a special case the following result for the equation

$$I(x_2, \dots, x_n) = \pm I \text{ in } x_2, \dots, x_n \in \mathbb{Z}. \quad (3.9)$$

Theorem 3.2. *Suppose again that the Galois group $\mathcal{G}$ is triply transitive. Then apart from at most $e^{30^{20}n^2}$ values of I , equation (3.9) has at most $2\psi(I)$ solutions.*

Theorem 3.2 implies e.g. results concerning the numbers of elements of given discriminant. If in K there exists at least one element with discriminant D then $I := \sqrt{|D/D_K|}$ is a rational integer. Further, if the element $\alpha \in \mathcal{O}_K$ takes the form

$$\alpha = x_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

in the integral basis $1, \alpha_2, \dots, \alpha_n$ with some $x_1, \dots, x_n \in \mathbb{Z}$ then $D_{K/\mathbb{Q}}(x_1 + x_2\alpha_2 + \cdots + x_n\alpha_n)$ is just the discriminant of α . Two elements $\alpha, \beta \in \mathcal{O}_K$ are called *equivalent* if $\alpha - \beta$ is a rational integer. Clearly, equivalent elements have the same discriminant. It follows from the above-mentioned result of Evertse and Györy [14] on the number of solutions of (3.3) that for given $0 \neq D \in \mathbb{Z}$ for which $I = \sqrt{|D/D_K|} \in \mathbb{Z}$, the number of pairwise inequivalent elements in $\mathcal{O}_K$ having discriminant D does not exceed the bound (3.6) with the choice $s = 0$. Our Theorem 3.2 implies that this bound can be considerably improved for almost all D , provided that the Galois group of K is triply transitive.

Corollary 3.3. *Suppose that the Galois group $\mathcal{G}$ is triply transitive. Then for all but finitely many integer values of D , the number of pairwise inequivalent elements of $\mathcal{O}_K$ having discriminant D is at most $4\psi(I)$ with $I = \sqrt{|D/D_K|} \in \mathbb{Z}$, and the number of exceptional values of D is at most $e^{30^{20}n^2}$.*

3.2 Proof of Theorem 3.1

In the proof of Theorem 3.1 we shall combine some methods from [19] and [28] with some recent results from [22], [6], [14] and [17].

To prove Theorem 3.1 we will use Lemma 2.2, Lemma 2.5 and Lemma 2.6 from the previous chapter. We shall also need the following result.

Lemma 3.1. *Suppose that K is an algebraic number field and $L = K(\xi)$ is a finite extension of K of degree n . Further, suppose that the Galois group $\mathcal{G}$ of the normal closure of L over K is doubly transitive. Then L is a primitive extension of K .*

Proof. The above lemma and its proof is well-known in the literature. For convenience of the reader, we present here a short proof of the lemma.

For $\alpha \in L$ denote by $\alpha^{(1)} = \alpha, \dots, \alpha^{(n)}$ the conjugates of α with respect to the extension L/K . Suppose that there is an element $\alpha \in L \setminus K$ such that it has at least two conjugates over K which are equal. We may assume without loss of generality that $\alpha^{(1)} = \alpha^{(2)}$. By the doubly transitivity of $\mathcal{G}$ we infer that there exist $\phi_2, \dots, \phi_n \in \mathcal{G}$ such that $\phi_i(\alpha^{(1)}) = \alpha^{(1)}$ and $\phi_i(\alpha^{(2)}) = \alpha^{(i)}$ for $i = 2, \dots, n$. This means that $\alpha^{(1)} = \alpha^{(2)} = \dots = \alpha^{(n)}$ and thus $\alpha \in K$ follows, which is a contradiction. This completes the proof of Lemma 3.1. $\square$

We shall use Lemma 2.6 and Györy's method (see e.g. [19], Ch. IV and [28], Section 5) to reduce equation (3.3) to an appropriate system of unit equations. Then we shall apply Lemmas 2.2 and 2.5 concerning unit equations.

First we introduce some further notation and make some preliminary observations. Let ξ be a primitive integral element of K . Denote by d the index of ξ in $\mathcal{O}_K$. Then $D_{K/\mathbb{Q}}(\xi) = d^2 \cdot D_K$. In view of (3.1) and (3.2) it follows that each solution $\mathbf{x} \in \mathbb{Z}^{n-1}$, $z_1, \dots, z_s \in \mathbb{Z}_{\geq 0}$ of (3.3) satisfies

$$\prod_{1 \leq i < j \leq n} l_{ij}^2(\mathbf{x}) = D_K I^2 p_1^{2z_1} \dots p_s^{2z_s},$$

whence

$$c \prod_{1 \leq i < j \leq n} \frac{d \cdot l_{ij}(\mathbf{x})}{\xi^{(i)} - \xi^{(j)}} = \pm I p_1^{z_1} \dots p_s^{z_s} \quad (3.10)$$

where $c = d^{1 - \frac{n(n-1)}{2}}$.

Let $K^{(i)} := \mathbb{Q}(\xi^{(i)})$ for $i = 1, \dots, n$. For any distinct i, j in $\{1, \dots, n\}$ consider the subfield $K_{ij} = \mathbb{Q}(\xi^{(i)} + \xi^{(j)}, \xi^{(i)} \cdot \xi^{(j)})$ of the field $K^{(i)}K^{(j)}$. By our assumption on $\mathcal{G}$, the Galois group of the normal closure of K over $\mathbb{Q}$ is triply transitive. Hence the field $K^{(i)}K^{(j)}$ is of degree $n(n-1)$ over $\mathbb{Q}$. Each $\sigma \in \mathcal{G}$ permutes the elements of $\{1, \dots, n\}$ where $\sigma(i)$ is defined by $\sigma(\xi^{(i)}) = \xi^{\sigma(i)}$. This implies a Galois action on the ordered pairs (i, j) . Each $\sigma \in \mathcal{G}$ for which $\sigma(i, j) = (j, i)$ leaves the elements of K_{ij} fixed. Therefore K_{ij} is a proper subfield of $K^{(i)}K^{(j)}$. The numbers $\xi^{(i)}$ and $\xi^{(j)}$ are zeros of the quadratic polynomial

$$X^2 - (\xi^{(i)} + \xi^{(j)})X + \xi^{(i)}\xi^{(j)},$$

which has its coefficients in K_{ij} . This implies that $K^{(i)}K^{(j)}$ is a quadratic extension of K_{ij} , and hence K_{ij} is of degree $n(n-1)/2$ over $\mathbb{Q}$. Denote by

$\lambda^{(i,j)}$ the conjugate of any $\lambda = \lambda^{(1,2)} \in K_{1,2}$ corresponding to $\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)}$ ($1 \leq i < j \leq n$) and for simplicity let $\lambda^{(i,j)} = \lambda^{(j,i)}$.

Since $d\mathcal{O}_K \subseteq \mathbb{Z}[\xi]$, it follows that for every $\alpha \in \mathcal{O}_K$ and each different i, j from $\{1, \dots, n\}$, $\frac{d(\alpha^{(i)} - \alpha^{(j)})}{\xi^{(i)} - \xi^{(j)}}$ is an integer in K_{ij} . Denote by $\mathcal{M}$ the $\mathbb{Z}_S$ -module in $K_{1,2}$, generated by the coefficients of the linear form $\frac{d \cdot l_{1,2}(\mathbf{X})}{\xi^{(1)} - \xi^{(2)}}$. The module $\mathcal{M}$ is of rank at most $n - 1$. For any solution $\mathbf{x}, z_1, \dots, z_s$ of (3.3), put

$$\delta = \delta^{(1,2)} = \frac{d \cdot l_{1,2}(\mathbf{x})}{\xi^{(1)} - \xi^{(2)}}.$$

Then $\delta \in K_{1,2}$, and the numbers $\delta^{(i,j)} = \frac{d \cdot l_{ij}(\mathbf{x})}{\xi^{(i)} - \xi^{(j)}}$ are the conjugates of δ with respect to $K_{1,2}/\mathbb{Q}$. Hence equation (3.10) leads to the equation

$$cN_{K_{1,2}/\mathbb{Q}}(\delta) \in I\mathbb{Z}_S^* \text{ in } \delta \in \mathcal{M}. \quad (3.11)$$

By Lemma 2.6 we deduce that there are solutions $\delta_1, \dots, \delta_q$ of (3.11) such that any solution δ of (3.11) is contained in $\delta_1 \mathcal{O}_{K_{1,2},S}^* \cup \dots \cup \delta_q \mathcal{O}_{K_{1,2},S}^*$ and that $q \leq \psi(I)$ with the $\psi(I)$ introduced in Section 3.1.

Consider now those solutions $\mathbf{x}, z_1, \dots, z_s$ of (3.3) for which the corresponding δ belong to the same coset, say $\delta_1 \mathcal{O}_{K_{1,2},S}^*$. Let i, j, k be arbitrary, but fixed and pairwise distinct elements of $\{1, \dots, n\}$. Then we have

$$l_{ij}(\mathbf{x}) + l_{jk}(\mathbf{x}) + l_{ki}(\mathbf{x}) = 0 \quad (3.12)$$

for any solution $\mathbf{x}, z_1, \dots, z_s$ under consideration. We can write $\delta = \delta^{(1,2)} = \delta_1^{(1,2)} \varepsilon^{(1,2)}$ with an appropriate $\varepsilon^{(1,2)} \in \mathcal{O}_{K_{1,2},S}^*$. Now we infer from (3.12) that

$$\rho_1 \frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}} + \rho_2 \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}} = 1 \quad (3.13)$$

where

$$\rho_1 = \frac{\delta_1^{(i,j)}(\xi^{(i)} - \xi^{(j)})}{\delta_1^{(i,k)}(\xi^{(i)} - \xi^{(k)})} \quad \text{and} \quad \rho_2 = \frac{\delta_1^{(j,k)}(\xi^{(j)} - \xi^{(k)})}{\delta_1^{(i,k)}(\xi^{(i)} - \xi^{(k)})}.$$

Observe that (3.13) is a unit equation in the unknowns $\left(\frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}}, \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}}\right)$. For given i, k , let $\{\varepsilon_1, \dots, \varepsilon_t\}$ be a fundamental system of $S_{K_{ik}}$ -units in the field K_{ik} . Then

$$t \leq \frac{n(n-1)}{2}(s+1).$$

Further, we have

$$\varepsilon^{(i,k)} = \theta \varepsilon_1^{b_1} \dots \varepsilon_t^{b_t},$$

where θ is a root of unity of K_{ik} and $b_1, \dots, b_t$ are rational integers. As $\varepsilon^{(i,j)}$ and $\varepsilon^{(j,k)}$ are conjugates of $\varepsilon^{(i,k)}$, there exist $\mathbb{Q}$ -isomorphisms φ and χ of K_{ik} such that $\varepsilon^{(i,j)} = \varphi(\varepsilon^{(i,k)})$ and $\varepsilon^{(j,k)} = \chi(\varepsilon^{(i,k)})$. Then (3.13) can be written in the form

$$\rho_1 \frac{\varphi(\theta)}{\theta} \left(\frac{\varphi(\varepsilon_1)}{\varepsilon_1} \right)^{b_1} \dots \left(\frac{\varphi(\varepsilon_t)}{\varepsilon_t} \right)^{b_t} + \rho_2 \frac{\chi(\theta)}{\theta} \left(\frac{\chi(\varepsilon_1)}{\varepsilon_1} \right)^{b_1} \dots \left(\frac{\chi(\varepsilon_t)}{\varepsilon_t} \right)^{b_t} = 1.$$

Now suppose that equation (3.3) has two different solutions $\mathbf{x}, z_1, \dots, z_s$ and $\mathbf{x}', z'_1, \dots, z'_s$ for which the corresponding solutions $\left(\frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}}, \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}} \right)$ and $\left(\frac{\varepsilon'^{(i,j)}}{\varepsilon'^{(i,k)}}, \frac{\varepsilon'^{(j,k)}}{\varepsilon'^{(i,k)}} \right)$ of (3.13) coincide, that is

$$\frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}} = \frac{\varepsilon'^{(i,j)}}{\varepsilon'^{(i,k)}} \quad \text{and} \quad \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}} = \frac{\varepsilon'^{(j,k)}}{\varepsilon'^{(i,k)}},$$

whence

$$\frac{\varepsilon^{(i,j)}}{\varepsilon'^{(i,j)}} = \frac{\varepsilon^{(k,i)}}{\varepsilon'^{(k,i)}} = \frac{\varepsilon^{(j,k)}}{\varepsilon'^{(j,k)}}.$$

Put $\beta^{(i,j)} = \frac{\varepsilon^{(i,j)}}{\varepsilon'^{(i,j)}}$. Then $\beta^{(i,j)}$ is an $S_{K_{ij}}$ -unit in the field K_{ij} . Since $\mathcal{G}$ is triply transitive, $K^{(i)}K^{(j)}$ has a $\mathbb{Q}$ -isomorphism which leaves $\xi^{(i)}$ fixed and moves $\xi^{(j)}$ to $\xi^{(l)}$ for arbitrary $l \in \{1, 2, \dots, n\} \setminus \{i\}$. Among the conjugates of $\beta^{(i,j)}$ there are at least two, namely $\beta^{(i,j)} = \beta^{(k,i)}$, which are equal. But $\beta^{(i,j)}$ and $\beta^{(k,i)}$ are conjugates over $K^{(i)}$, too. Furthermore, $\mathcal{G}$ being triply transitive, the Galois group of the normal closure of $K^{(i)}K^{(j)}$ over $K^{(i)}$ is doubly transitive, and thus by Lemma 3.1 it follows that $K^{(i)}K^{(j)}$ is a primitive extension of $K^{(i)}$. Together with $\beta^{(i,j)} = \beta^{(k,i)}$ this means that all conjugates of $\beta^{(i,j)}$ over $K^{(i)}$ are equal. Thus $\beta^{(i,j)} \in K^{(i)}$, and similarly $\beta^{(k,i)} \in K^{(k)}$. But $\beta^{(i,j)} = \beta^{(k,i)}$, hence we get $\beta^{(i,j)} \in K^{(i)} \cap K^{(k)}$. It follows from the triply transitivity of $\mathcal{G}$ that $[K^{(i)}K^{(k)} : K^{(i)}] = n - 1$ and thus $K^{(i)} \neq K^{(k)}$. Further, because of the doubly transitivity of $\mathcal{G}$, by Lemma 3.1 we see that $K^{(i)}$ is a primitive extension of $\mathbb{Q}$. Hence we get $K^{(i)} \cap K^{(k)} = \mathbb{Q}$ and so $\beta^{(i,j)} \in \mathbb{Q}$. But $\beta^{(i,j)}$ is an $S_{K_{ij}}$ -unit, thus we get $\beta^{(i,j)} \in \mathbb{Z}_S^*$.

The above arguments lead us to the conclusion that $\varepsilon = \eta \varepsilon'$, with some $\eta \in \mathbb{Z}_S^*$, where $\varepsilon = (\varepsilon^{(i,j)})_{1 \leq i \neq j \leq n}$ and $\varepsilon' = (\varepsilon'^{(i,j)})_{1 \leq i \neq j \leq n}$. Thus $l_{ij}(\mathbf{x}) =$

$\eta^{l_{ij}}(\mathbf{x}')$ for $1 \leq i, j \leq n$ with $i \neq j$ and so

$$(\alpha_2 - \alpha_2^{(2)})(x_2 - \eta x_2') + \cdots + (\alpha_n - \alpha_n^{(2)})(x_n - \eta x_n') = 0.$$

Since K is a primitive extension of $\mathbb{Q}$ and $\alpha_2, \dots, \alpha_n$ are $\mathbb{Q}$ -linearly independent, it follows that $\alpha_2 - \alpha_2^{(2)}, \dots, \alpha_n - \alpha_n^{(2)}$ are also $\mathbb{Q}$ -linearly independent. Hence we infer that $\mathbf{x} = \eta \mathbf{x}'$ with $\eta \in \mathbb{Z}_S^*$. But by assumption $(x_2, \dots, x_n, p_1 \dots p_s) = 1$ and $(x_2', \dots, x_n', p_1 \dots p_s) = 1$, hence $\eta = \pm 1$ follows. Thus we have shown that different solutions of (3.3) correspond to different solutions of the unit equation (3.13).

Now suppose that equation (3.3) has more than two solutions corresponding to the same δ_1 . Then for every fixed i, j, k , equation (3.13) has also at least three solutions. Equation (3.13) can be considered as an equation of the type (2.12), where G is the subgroup of $\mathbb{C}^*$ generated by

$$\left\{ \frac{\varphi(\theta)}{\theta}, \frac{\varphi(\varepsilon_1)}{\varepsilon_1}, \dots, \frac{\varphi(\varepsilon_t)}{\varepsilon_t}, \frac{\chi(\theta)}{\theta}, \frac{\chi(\varepsilon_1)}{\varepsilon_1}, \dots, \frac{\chi(\varepsilon_t)}{\varepsilon_t} \right\}.$$

Thus by Lemma 2.5 there exists a finite set $\mathcal{C}_1$ of pairs $(\kappa_1, \kappa_2) \in (\mathbb{C}^*)^2$ which is independent of I such that

$$\rho_1 = \kappa_1 \eta_1 \quad \text{and} \quad \rho_2 = \kappa_2 \eta_2$$

with $(\kappa_1, \kappa_2) \in \mathcal{C}_1$ and with some fixed $\eta_1, \eta_2 \in G$. Furthermore, by Lemma 2.5

$$\#\mathcal{C}_1 \leq 2 \cdot e^{(2t+4)30^{20}} \leq 2 \cdot e^{(n(n-1)(s+1)+4)30^{20}} =: c_1(n, s).$$

For the moment fix $(\kappa_1, \kappa_2) \in (\mathbb{C}^*)^2$. Then $\left(\eta_1 \frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}, \eta_2 \frac{\varepsilon^{(j,k)}}{\varepsilon^{(k,i)}} \right)$ is a solution of the equation

$$\kappa_1 u' + \kappa_2 v' = 1 \quad \text{in } u', v' \in G. \quad (3.14)$$

However, this equation leads to

$$u'' + v'' = 1 \quad \text{in } (u'', v'') \in G' \quad (3.15)$$

where G' is the subgroup of $(\mathbb{C}^*)^2$ generated by

$$\begin{aligned} & \left\{ (\kappa_1, 1), \left(\frac{\varphi(\theta)}{\theta}, 1 \right), \left(\frac{\varphi(\varepsilon_1)}{\varepsilon_1}, 1 \right), \dots, \left(\frac{\varphi(\varepsilon_t)}{\varepsilon_t}, 1 \right), \right. \\ & \quad \left(\frac{\chi(\theta)}{\theta}, 1 \right), \left(\frac{\chi(\varepsilon_1)}{\varepsilon_1}, 1 \right), \dots, \left(\frac{\chi(\varepsilon_t)}{\varepsilon_t}, 1 \right), \\ & \quad (1, \kappa_2), \left(1, \frac{\varphi(\theta)}{\theta} \right), \left(1, \frac{\varphi(\varepsilon_1)}{\varepsilon_1} \right), \dots, \left(1, \frac{\varphi(\varepsilon_t)}{\varepsilon_t} \right), \\ & \quad \left. \left(1, \frac{\chi(\theta)}{\theta} \right), \left(1, \frac{\chi(\varepsilon_1)}{\varepsilon_1} \right), \dots, \left(1, \frac{\chi(\varepsilon_t)}{\varepsilon_t} \right) \right\}. \end{aligned}$$

Then $(\kappa_1 \eta_1 \frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}, \kappa_2 \eta_2 \frac{\varepsilon^{(j,k)}}{\varepsilon^{(k,i)}})$ is a solution of equation (3.15), which by Lemma 2.2 has at most

$$2^{8(4t+6)+8} \leq 2^{8(2n(n-1)(s+1)+6)+8} =: c_2(n, s)$$

solutions. Thus, allowing now (κ_1, κ_2) to vary through $\mathcal{C}_1$, $\rho_1 \frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}} = \kappa_1 \eta_1 \frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}$ can assume at most $c(n, s) := c_1(n, s) \cdot c_2(n, s)$ different values and so does

$$\frac{\delta_1^{(i,j)}}{\delta_1^{(k,i)}} \cdot \frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}.$$

Taking $k = 1$, this yields that for every distinct i, j ,

$$\delta_1^{(i,j)} \varepsilon^{(i,j)} = \mu_{ij} \delta_1^{(1,i)} \varepsilon^{(1,i)},$$

where $\mu_{i,j}$ can assume at most $c(n, s)$ values. Put $i := 2$, $j := 3$, $L := K^{(1)}K^{(2)}K^{(3)}$ and $l := [L : K_{2,3}]$. Taking the $L/\mathbb{Q}$ -norm of the above equation and using (3.11) we have

$$(I/c)^l \mathbb{Z}_S^* \ni N_{L/\mathbb{Q}}(\delta_1^{(2,3)} \varepsilon^{(2,3)}) = N_{L/\mathbb{Q}}(\delta_1^{(1,2)}) \cdot N_{L/\mathbb{Q}}(\varepsilon^{(1,2)}) \cdot N_{L/\mathbb{Q}}(\mu_{2,3}).$$

However, c and δ_1 are fixed and $N_{L/\mathbb{Q}}(\mu_{2,3})$ can take at most $c(n, s)$ distinct values. So it follows that apart from a factor from $\mathbb{Z}_S^*$, I can assume also at most $c(n, s)$ distinct values. Now a simple calculation proves the bound for the number of exceptional I 's, given in Theorem 3.1.

If I does not take any of these values, then the number of solutions of (3.3) is at most the product of the number of solutions of (3.13) and the number of the possibilities for δ_1 . Because of the choice of I (3.13) has at most 2 solutions. Further, by Lemma 2.6 we have at most $\psi(I)$ choices for δ_1 . This completes the proof of Theorem 3.1. $\square$

Chapter 4

On a problem of P. Turán concerning irreducible polynomials

4.1 Introduction

Many important and interesting problems of mathematics are related to the distribution of irreducible elements in various special structures. It is well-known that the number of primes in $\mathbb{N}$ is infinite. However, the set of prime numbers is of density zero and the gap between two consecutive primes can be arbitrarily large. In $\mathbb{Z}[x]$ there are infinitely many irreducible polynomials. Nevertheless, it seems that there are only few common properties of the distribution of irreducible elements in $\mathbb{Z}$ and in $\mathbb{Z}[x]$. Indeed, if we denote by $P(N)$ resp. $R(N)$ the number of polynomials resp. irreducible polynomials in $\mathbb{Z}[x]$ of given degree and of height at most N , then we have (cf. [31])

$$\frac{R(N)}{P(N)} \rightarrow 1 \text{ as } N \rightarrow \infty.$$

In other words 'almost all' polynomials in $\mathbb{Z}[x]$ are irreducible.

The above result suggests that the 'gap' between 'neighbouring' irreducible polynomials in $\mathbb{Z}[x]$ cannot be too large. These facts led P. Turán in 1962 to propose the following interesting problem. To formulate his problem, we need the concept of the length $|P|$ of a polynomial $P(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

which is defined by the expression

$$|P| = \sum_{k=0}^n |a_k|.$$

By the distance of $P, Q \in \mathbb{Z}[x]$ we mean $|P - Q|$. It follows easily from Eisenstein's theorem that for given $P \in \mathbb{Z}[x]$ of degree n there is an irreducible polynomial $Q \in \mathbb{Z}[x]$ of degree n such that $|P - Q| \leq n + 2$. P. Turán asked the following (cf.[33]):

Does there exist an absolute constant C_1 such that for every $P(x) \in \mathbb{Z}[x]$ of degree n , there is a polynomial $Q(x) \in \mathbb{Z}[x]$ irreducible over $\mathbb{Q}$, satisfying $\deg(Q) \leq n$ and $|P - Q| \leq C_1$?

This problem is very difficult. It turns to be somewhat easier if one removes the condition $\deg(Q) \leq n$. In 1970, A. Schinzel [34] proved the following deep theorem:

Theorem A. (A. Schinzel [34]) *For any nonzero integers a, b and any polynomial P with integral coefficients, such that $P(0) \neq 0$ and $P(1) \neq -a - b$, there exist infinitely many irreducible polynomials $ax^n + bx^m + P(x)$ with $n > m > \deg(P)$. One of them satisfies*

$$n < \exp\{(5 \deg(P) + 2 \log |ab| + 7)(|P| + a^2 + b^2)\},$$

where $|P|$ denotes the sum of the squares of the coefficients of P .

As a consequence of this theorem Schinzel showed that for every $P \in \mathbb{Z}[x]$ of degree n there are infinitely many irreducible $Q \in \mathbb{Z}[x]$ such that

$$|P - Q| \leq \begin{cases} 2 & \text{if } P(0) \neq 0, \\ 3 & \text{otherwise.} \end{cases}$$

Further, one of these irreducible polynomials Q satisfies

$$\deg(Q) \leq e^{(5n+7)(|P|^2+3)}.$$

This result gives a partial answer to Turán's question.

For the sake of completeness, now we present another, similar problem, which was proposed in 1984 by M. Szegedy (cf. [25]). He asked the following:

Does there exist a constant C_2 depending only on n such that for any $P \in \mathbb{Z}[x]$ of degree n , $P(x) + b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \leq C_2$?

This seems also to be a very hard question. In 1994, Györy [25] succeeded to give an affirmative answer to Szegedy's problem in case of monic polynomials. This is a consequence of his following theorem.

Theorem B. (K. Györy [25]) *Let $P \in \mathbb{Z}[x]$ be a polynomial of degree n with leading coefficient a_0 . There exist an effectively computable constant C_3 depending only on n and $\omega(a_0)$, and $b \in \mathbb{Z}$ with $|b| \leq C_3$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$. (Here $\omega(a_0)$ denotes the number of distinct prime divisors of a_0 .)*

We remark that in [25] C_3 is given explicitly.

In our paper [4] we gave upper bounds for the Turán constant C_1 for monic polynomials P of degree not greater than 22. In fact we could prove that for such polynomials $C_1 = 4$ can be chosen. Slightly improving our algorithms, in [5] we extended our result to polynomials of degree at most 24.

4.2 New results

For a positive integer n , denote by c_n the smallest integer with the property that for any monic polynomial $P \in \mathbb{Z}[x]$ of degree n one can choose an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ of degree n , such that $|P - Q| \leq c_n$. One can verify easily that for every positive n , c_n exists. Using this notation, our result in [4] says that

$$c_n \leq 4 \text{ for every positive integer } n \leq 22.$$

We prove the following extension.

Theorem 4.1. *For every positive integer $n \leq 24$ and for every monic polynomial $P \in \mathbb{Z}[x]$ of degree n there exists an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ of degree n such that*

$$|P - Q| \leq 4.$$

For smaller degrees, our computations imply a slightly better result. In fact we could prove that $c_1 = 0$, $c_2 = 1$, $c_n = 2$ for $3 \leq n \leq 6$, $c_n \leq 3$ for $7 \leq n \leq 12$, and $c_n \leq 4$ for $13 \leq n \leq 24$ (see also Table 1). Summarizing these assertions, we can state that for any positive integer $n \leq 24$, we have $c_n \leq 4$.

To make clear the main idea behind the proof we need some further notation. Denote by $\mathbb{Z}_p[x]$ the residue class ring $\mathbb{Z}[x] \pmod{p}$. For any polynomial $R \in \mathbb{Z}[x]$ denote by R_p the image of R under the natural homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}_p[x]$. Each polynomial $P \in \mathbb{Z}[x]$ has a representative which has its coefficients in the interval $]-\frac{p}{2}, \frac{p}{2}]$. The sum of the absolute values of the coefficients of the representative of this type of a polynomial $P \in \mathbb{Z}_p[x]$ is called the p -length of P and it is denoted by $|P|_p$. By the $\pmod{p}$ distance of two polynomials $P, Q \in \mathbb{Z}[x]$ we mean the p -length of the polynomial $(P - Q)_p$. Similarly, by the $\pmod{p}$ distance of two polynomials $P, Q \in \mathbb{Z}_p[x]$ we mean the p -length of the polynomial $P - Q$.

For every positive integer n let us denote by $c_n(p)$ the smallest integer with the property that for each monic polynomial $P \in \mathbb{Z}_p[x]$ of degree n there exists an irreducible monic polynomial $Q \in \mathbb{Z}_p[x]$ of degree n for which $|P - Q|_p \leq c_n(p)$.

The main idea of the proof is based on the fact that $c_n \geq c_n(p)$ for any prime number p . Indeed, by the definition of $c_n(p)$, for an arbitrary but fixed polynomial $P \in \mathbb{Z}[x]$ there exists an irreducible monic polynomial $R \in \mathbb{Z}_p[x]$ such that $|P_p - R|_p \leq c_n(p)$. Now it is easy to prove that there exists a monic polynomial $Q \in \mathbb{Z}[x]$ such that $|P - Q| = |P_p - R|_p \leq c_n(p)$ and $Q_p = R$. Finally, this last equality, together with the assumption that R is irreducible in $\mathbb{Z}_p[x]$ shows that Q is irreducible in $\mathbb{Z}[x]$.

Thus it is enough to give upper bounds for $c_n(p)$ for each $1 \leq n \leq 24$ with at least one prime p . But then, for fixed n , the polynomials in $\mathbb{Z}_p[x]$ of degree at most n are finite in number. This makes it possible to use computational methods in order to obtain bounds for $c_n(p)$. In fact we have investigated the case $p = 2$ in the range $1 \leq n \leq 24$ and the case $p = 3$ in the range $1 \leq n \leq 12$. The case $1 \leq n \leq 22$ was included in our paper [4]. Our algorithms are exponential in n , and thus we were not able to use them for large values of n . However, later we have slightly refined our algorithms, slightly decreasing the time of computation and so we managed to investigate the case $p = 2$ in the range $1 \leq n \leq 24$. We summarized our results in Table 1, below.

Table 1: $c_n(2)$, $c_n(3)$, and bounds for c_n

Degree n	$c_n(2)$	$c_n(3)$	Bound for c_n
1	0	0	0
2	2	1	1
3	2	2	2
4	3	2	2
5	3	2	2
6	3	2	2
7	3	3	3
8	4	3	3
9	3	3	3
10	4	3	3
11	4	3	3
12	4	3	3
13	4	—	4
14	4	—	4
15	4	—	4
16	4	—	4
17	4	—	4
18	4	—	4
19	4	—	4
20	4	—	4
21	4	—	4
22	4	—	4
23	4	—	4
24	4	—	4

4.3 Description of the algorithm

In view of the previous section we have to prove the validity of the values of $c_n(2)$ for $1 \leq n \leq 24$ and $c_n(3)$ for $1 \leq n \leq 12$ contained in Table 1. To do so, it is enough to check that for each monic polynomial P of degree n with coefficients in $\mathbb{Z}_p$ and with $P(0) \neq 0$ we can find a monic irreducible polynomial $Q \in \mathbb{Z}_p[x]$ such that $|P - Q|_p \leq c_n(p) - 1$. This is the computational part of our proof. Now we present a short description of the algorithms we used for

obtaining Table 1. In fact we implemented three algorithms. Two of them, A) and B) below, were included also in [4], thus here we only mention them. The third algorithm, i.e. C) below, is a refined version of one of the algorithms used in [4], thus we give a more detailed description of it.

- A) The first algorithm was used to check the case $p = 2$ for the degrees $1 \leq n \leq 13$. In this part we used the 'compare everything with everything' method. However, the computations for the case $n = 13$ took several hours, thus we decided to use some filter conditions for higher degrees.
- B) The second algorithm was used for the case $p = 3$ and it is the same as in [4], and the 'compare everything with everything' method is refined only by a very simple idea (see [4]).
- C) This algorithm, used in the case $p = 2$, $14 \leq n \leq 24$ is as follows. For a fixed n we have to check whether for each monic polynomial P of degree n with coefficients in $\mathbb{Z}_2$ and with $P(0) \neq 0$ we could find an irreducible monic polynomial $Q \in \mathbb{Z}_2[x]$ such that the 2-distance of P and Q is at most $\hat{c}_n(2)$, where $\hat{c}_n(2)$ is defined by $\hat{c}_n(2) := c_n(2) - 1$.

Denote by $\mathcal{P}_n$ the set of all monic polynomials P of degree n with coefficients in $\mathbb{Z}_2$ and with $P(0) \neq 0$, and by $\mathcal{D}_n^{(k)}$ the set of all polynomials of degree at most n with coefficients in $\mathbb{Z}_2$ and with $|D|_2 \leq k$.

To check whether $\hat{c}_n(2) \leq k$, it is enough to check the following for each monic polynomial $P \in \mathcal{P}_n$: add a polynomial $D \in \mathcal{D}_n^{(k)}$ to P and check whether $P + D$ is irreducible. If not, take the following $D \in \mathcal{D}_n^{(k)}$. *If for at least one polynomial $P \in \mathcal{P}_n$ does not exist a polynomial $D \in \mathcal{D}_n^{(k)}$, such that $P + D$ is irreducible, then we get $\hat{c}_n(2) > k$, and we have to do the same procedure for $k + 1$. If for each $P \in \mathcal{P}_n$ we find a polynomial $D \in \mathcal{D}_n^{(k)}$, such that $P + D$ is irreducible, then we have proved the statement $\hat{c}_n(2) \leq k$.* We start with $k = 2$. When for a fixed value of k we get $\hat{c}_n(2) > k$, then we increase k with 1. The first value of k for which we find that for each $P \in \mathcal{P}_n$ there exists a polynomial $D \in \mathcal{D}_n^{(k)}$ is clearly $k = \hat{c}_n(2)$. When working with $k = \hat{c}_n(2) - 1$, we get some polynomials $P \in \mathcal{P}_n$ for which does not exist a polynomial $D \in \mathcal{D}_n^{(k)}$ such that $P + D$ is irreducible. We call these polynomials extreme polynomials. The existence of extreme polynomials shows that for every $2 \leq n \leq 24$ the corresponding value of $c_n(2)$ is sharp. In fact,

for every fixed $14 \leq n \leq 24$ we got $k \leq 3$ and $k > 2$, and this proves $c_n(2) = 4$ for $14 \leq n \leq 24$.

In the third column of Table 2 we list for each $2 \leq n \leq 24$ the number $e_2(n)$ of extreme polynomials of minimal 2-length. We note that if $P(x)$ is an extreme polynomial of minimal length then so does

$$P^*(x) = x^n \left(P\left(\frac{1}{x}\right) + 1 \right) - 1.$$

Further we have $(P^*)^* = P$. In the fourth column of Table 2 we list all extreme polynomials of minimal length except that for pairs P, P^* we list only one of them. It is interesting to note that it may happen that $P(x) = P^*(x)$. Thus $e_2(n)$ may take odd values, too.

We also note that the results concerning extreme polynomials of minimal length have not yet been published, they are not contained neither in [4] nor in [5].

Table 2: Extreme polynomials

n	$c_n(2)$	$e_2(n)$	All extreme polynomials of minimal 2-length
2	2	1	x^2
3	2	1	x^3
4	3	1	$x^4 + x^2$
5	3	2	$x^5 + x$
6	3	2	$x^6 + x^2$
7	3	2	$x^7 + x^2$
8	4	1	x^8
9	3	4	$x^9 + x^2$ $x^9 + x^3$
10	4	1	$x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x^2$
11	4	2	$x^{11} + x^9 + x^8 + x^7 + x^5$
12	4	2	$x^{12} + x^9 + x^7 + x^2 + x$
13	4	1	x^{13}
14	4	3	$x^{14} + x^{10} + x^4$ $x^{14} + x^{11} + x^2$
15	4	12	$x^{15} + x^7 + x^5 + x^3 + x$ $x^{15} + x^{10} + x^7 + x^6 + x^4$

Table 2: (continued)

n	$c_n(2)$	$e_2(n)$	All extreme polynomials of minimal 2-length
			$x^{15} + x^{10} + x^9 + x^2 + x$ $x^{15} + x^{11} + x^{10} + x^9 + x^2$ $x^{15} + x^{13} + x^9 + x^7 + x$ $x^{15} + x^{14} + x^5 + x^3 + x$
16	4	1	x^{16}
17	4	11	$x^{17} + x^{10} + x^8 + x^5 + x^3$ $x^{17} + x^{11} + x^9 + x^7 + x^2$ $x^{17} + x^{11} + x^{10} + x^4 + x$ $x^{17} + x^{11} + x^{10} + x^5 + x^3$ $x^{17} + x^{13} + x^7 + x^6 + x^4$ $x^{17} + x^{15} + x^{14} + x^3 + x^2$
18	4	3	$x^{18} + x^4 + x^2$ $x^{18} + x^{14} + x^4$
19	4	1	x^{19}
20	4	9	$x^{20} + x^8 + x^2$ $x^{20} + x^9 + x^6$ $x^{20} + x^{13} + x^6$ $x^{20} + x^{14} + x^2$ $x^{20} + x^{14} + x^6$
21	4	9	$x^{21} + x^5 + x^4$ $x^{21} + x^{10} + x^8$ $x^{21} + x^{12} + x^4$ $x^{21} + x^{12} + x^9$ $x^{21} + x^{13} + x^8$ $x^{21} + x^{20} + x$
22	4	10	$x^{22} + x^6 + x^4$ $x^{22} + x^{10} + x^2$ $x^{22} + x^{10} + x^8$ $x^{22} + x^{15} + x^3$ $x^{22} + x^{18} + x^4$ $x^{22} + x^{20} + x^2$
23	4	68	$x^{23} + x^{11} + x^9 + x^3 + x^2$ $x^{23} + x^{11} + x^{10} + x^6 + x^2$

Table 2: (continued)

n	$c_n(2)$	$e_2(n)$	All extreme polynomials of minimal 2-length
			$x^{23} + x^{12} + x^7 + x^3 + x^2$ $x^{23} + x^{13} + x^{12} + x^{10} + x^7$ $x^{23} + x^{14} + x^{11} + x^9 + x^7$ $x^{23} + x^{14} + x^{13} + x^8 + x$ $x^{23} + x^{14} + x^{13} + x^8 + x^6$ $x^{23} + x^{15} + x^{14} + x^8 + x^3$ $x^{23} + x^{16} + x^{12} + x^{10} + x^3$ $x^{23} + x^{16} + x^{13} + x^8 + x$ $x^{23} + x^{16} + x^{14} + x^8 + x^3$ $x^{23} + x^{16} + x^{14} + x^{11} + x^3$ $x^{23} + x^{17} + x^{11} + x^4 + x$ $x^{23} + x^{17} + x^{13} + x^4 + x$ $x^{23} + x^{17} + x^{16} + x^{10} + x^3$ $x^{23} + x^{18} + x^{10} + x^7 + x^3$ $x^{23} + x^{18} + x^{15} + x^5 + x^4$ $x^{23} + x^{18} + x^{17} + x^{13} + x^2$ $x^{23} + x^{19} + x^{11} + x^7 + x^2$ $x^{23} + x^{19} + x^{14} + x^4 + x$ $x^{23} + x^{19} + x^{16} + x^4 + x^2$ $x^{23} + x^{20} + x^5 + x^2 + x$ $x^{23} + x^{20} + x^7 + x^6 + x^3$ $x^{23} + x^{20} + x^8 + x^5 + x^2$ $x^{23} + x^{20} + x^{11} + x^9 + x^2$ $x^{23} + x^{20} + x^{13} + x^9 + x^3$ $x^{23} + x^{20} + x^{14} + x^{13} + x$ $x^{23} + x^{20} + x^{15} + x^9 + x$ $x^{23} + x^{21} + x^8 + x^7 + x^2$ $x^{23} + x^{21} + x^{16} + x^4 + x$ $x^{23} + x^{21} + x^{16} + x^6 + x^2$ $x^{23} + x^{21} + x^{17} + x^9 + x$ $x^{23} + x^{21} + x^{18} + x^8 + x$ $x^{23} + x^{22} + x^{14} + x^4 + x$
24	4	29	$x^{24} + x^6 + x^5$

Table 2: (continued)

n	$c_n(2)$	$e_2(n)$	All extreme polynomials of minimal 2-length
			$x^{24} + x^8 + x^4$ $x^{24} + x^{11} + x^7$ $x^{24} + x^{12} + x$ $x^{24} + x^{12} + x^4$ $x^{24} + x^{12} + x^5$ $x^{24} + x^{12} + x^8$ $x^{24} + x^{12} + x^{11}$ $x^{24} + x^{13} + x^9$ $x^{24} + x^{14} + x^4$ $x^{24} + x^{16} + x^4$ $x^{24} + x^{16} + x^8$ $x^{24} + x^{18} + x$ $x^{24} + x^{18} + x^4$ $x^{24} + x^{20} + x^4$ $x^{24} + x^{22} + x^2$

The function

$$f_2 : \mathbb{Z}_2[x] \mapsto \mathbb{N}, \quad f_2(P) := P(2)$$

gives a bijection between the polynomials of $\mathbb{Z}_2[x]$ and the natural numbers. Coding the polynomials in this simple manner as natural numbers we included some filter conditions in this algorithm. (When in this paragraph we speak about correspondence between polynomials and natural numbers we always mean the correspondence given by f_2 .)

Denote by L_1 and L_2 the list of all natural numbers corresponding to polynomials of degree ≤ 12 with nonzero constant term in $\mathbb{Z}_2[x]$ whose 2-length is even and odd, respectively. These lists can be constructed recursively, as follows. Suppose that for $0 \leq h \leq 12$, $L_1^{(h)}$ (resp. $L_2^{(h)}$) denotes the set of numbers corresponding to those polynomials which are in L_1 (resp. L_2) and are of degree $\leq h$. Put

$$M_1^{(h+1)} := \{2n + 1 \mid n \in L_2^{(h)}\} \quad \text{and} \quad M_2^{(h+1)} := \{2n + 1 \mid n \in L_1^{(h)}\}.$$

Then we clearly have

$$L_1^{(h+1)} = L_1^{(h)} \cup M_1^{h+1} \quad \text{and} \quad L_2^{(h+1)} = L_2^{(h)} \cup M_2^{h+1},$$

and finally $L_1 = L_1^{(12)}$ and $L_2 = L_2^{(12)}$.

Let T be a list of 2^{n-12} elements containing zeros and ones, the k th element of T being 0 if the 2-length of the polynomial corresponding to the number $2^n + (k-1)2^{12}$ is even, and 1 otherwise. To build this list we use the following recursion: $T(1) = 1, T(2) = 0, T(2^k + l) = a_l + 1 \pmod{2}$ for all $k \in \mathbb{N}$ and $1 \leq l \leq 2^k$.

For $i = 0, 1, 2, 3$ let $A_i^{(n)}$ be the set of all polynomials $D \in \mathbb{Z}_2[x]$ of degree $\leq n-1$, with the properties $D(0) = 0$ and $|D|_2 = i$.

For any polynomial P of degree n , the parity of the 2-length of P can be determined easily with the help of the lists L_1, L_2 , and T . Now we have to add to P either the polynomials $D \in A_1^{(n)} \cup A_3^{(n)}$ or $D \in A_0^{(n)} \cup A_2^{(n)}$.

When we checked the irreducibility of a polynomial we stored the informations in a list I . More precisely we started with an empty list I and when checking the irreducibility of a polynomial (e.g. the polynomial corresponding to the natural number j), we put as the j th element of I the value 'true' if it was irreducible and 'false' otherwise. This way we had to check the irreducibility of a polynomial only once. This was one of the improvements which reduced slightly the running time and made it possible to extend our bounds for $n = 23, 24$. However, while improving the running time, this change also increased the needed memory, and thus for $n \geq 25$ we run out of memory, and were not able to continue the calculations.

Our algorithms were written in MAPLE, and the running time for the case $p = 2$ and $n = 24$ was 250 hours on a SUN Sparcstation 10.

Summary

This dissertation consists of four chapters.

The first chapter contains results concerning the number of solutions of general decomposable polynomial equations. In 1989 Evertse, Gaál and Győry [10] gave a necessary and sufficient condition for the finiteness of the number of solutions of the general decomposable polynomial equation (0.1) in S -integers. Under this condition they gave a non-explicit upper bound for the number of solutions, which bound was given explicitly in terms of the numbers of solutions of appropriate unit equations. Since then explicit upper bounds have been obtained for the number of solutions of unit equations, thus the bound of Evertse, Gaál and Győry can be made completely explicit. Following a different approach, in the first chapter we significantly improve this bound. Further, we prove that the finiteness condition mentioned above does not imply the finiteness of the number of solutions of the corresponding more general decomposable polynomial equation (0.3). We give a sufficient condition for the finiteness of the number of solutions of (0.3), and subject to this condition we derive an explicit upper bound for the number of solutions. Moreover, we derive a similar upper bound for the number of solutions, provided only that the number of solutions is finite.

In the first chapter several consequences and applications are also presented. We obtain upper bounds for the numbers of solutions of decomposable polynomial equations of special types, namely for inhomogeneous Thue equations, discriminant polynomial equations, norm polynomial equations and resultant polynomial equations. The results of this chapter have been established jointly with my supervisor, Prof. K. Győry. They will be published in our joint paper [3].

The second chapter is devoted to the study of the number of solutions of norm form equations. Let $p_1, \dots, p_s$ be primes with $s \geq 0$, and $b \in \mathbb{Z} \setminus \{0\}$ which is relatively prime to $p_1, \dots, p_s$ if $s > 0$. In 1985 Evertse and Győry [11]

gave explicit upper bounds for the number of solutions of norm form equations of the form

$$\begin{aligned} a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_m x_m) &= b p_1^{z_1} \cdots p_s^{z_s} \text{ in } x_1, \dots, x_m \in \mathbb{Z}, \\ \text{and } z_1, \dots, z_s &\in \mathbb{Z}_{\geq 0} \\ \text{with } (x_1, \dots, x_m, p_1 \cdots p_s) &= 1 \text{ if } s > 0 \end{aligned} \tag{0.4}$$

under the hypotheses that (i) $x_m \neq 0$, $\alpha_1 = 1, \alpha_2, \dots, \alpha_m$ are $\mathbb{Q}$ -linearly independent elements of K and α_m has degree at least 3 over $\mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})$ or that (ii) the degree of α_i is at least 3 over $\mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})$ for $i = 2, \dots, m$. Under the same assumptions we considerably improve the bounds of [11]. Using an idea of Győry, we reduce equation (0.4) to a relative Thue-Mahler equation and then we use a result of Evertse [9] to estimate the number of solutions of this equation. In the second chapter we also give a further improvement on the number of solutions of (0.4) which is valid for all but at most finitely many possible values of the constant term b of the equation. Our bound obtained under the assumption (ii) is better for almost all b than the general bounds of [20], [8] and [14]. Further, we give an explicit upper bound for the number of the exceptional values of b . To prove this result we use Győry's method to reduce equation (0.4) to a system of unit equations and then we use results of Evertse, Győry, Stewart and Tijdeman [15] and Evertse and Győry [14] to derive our upper bound for the number of solutions. The bound for the number of exceptional values of b is obtained by combining results from [6], [17] and [22]. Our results presented in this chapter are published in [2].

In the third chapter we are concerned with the number of solutions of index form equations. In Evertse and Győry [11], [14] and Evertse [8] explicit upper bounds have been established for the number of solutions of index form equations. Recently, in the case when the Galois group of the splitting field of the index form is triply transitive, Győry [28] has considerably improved the bounds of [11] and [8]. Under the same assumption concerning the Galois group, we give a significant improvement of the bound in [14], which is valid for all but at most finitely many possible values of the constant term of the equation. To prove this result we use a similar method to that applied in Chapter 2 to norm form equations. We also combine Győry's method on reducing decomposable form equations to unit equations with the above-mentioned results from [15], [14], [6], [17] and [22]. Our results presented in Chapter 3 are published in [1].

In the fourth chapter some new results are established on a problem of P.

Turán concerning irreducible polynomials. The distance of two polynomials with integer coefficients is defined as the sum of the absolute values of the coefficients of the difference polynomial. P. Turán asked the following: Does there exist an absolute constant C such that for every polynomial with integer coefficients and of degree n , there exists an irreducible polynomial with integer coefficients and of degree at most n , such that their distance is not greater than C ? First we reduce the problem in $\mathbb{Z}[x]$ to that in the residue class ring $\mathbb{Z}[x] \pmod{p}$, where $p = 2$ or 3 . Then we apply computational methods to prove that $C \leq 4$ for all polynomials of degree not greater than 24. We give a description of our method and some related results. The results presented in Chapter 4 have been obtained jointly with Hajdu. Most of our results have been published in [5]. The remaining part is still unpublished.

Összefoglaló

A disszertáció négy fejezetből áll.

Az **első fejezet**ben általános széteső polinom egyenletek megoldásszámára adunk korlátokat. Legyen $F(\mathbf{X}) = F(X_1, \dots, X_m) \in \mathbb{Q}[X_1, \dots, X_m]$ egy széteső polinom, $S = \{p_1, \dots, p_s\}$ racionális prímek egy véges halmaza, és jelölje $\mathbb{Z}_S$ a $\mathbb{Q}$ -beli S -egészek gyűrűjét. Evertse, Gaál és Győry [10] 1989-ben szükséges és elégséges feltételt adott arra, hogy az

$$F(\mathbf{x}) = b \quad \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \quad (1)$$

széteső polinom egyenletnek véges sok megoldása legyen minden S és minden $b \in \mathbb{Z} \setminus \{0\}$ esetén. Ugyanezen feltétel mellett az egyenlet megoldásszámára korlátot is adtak, amely bizonyos kapcsolódó egységegyenletek megoldásszámának függvényében explicit módon volt megadva. Abban az időben még nem volt ismert explicit korlát egységegyenletek megoldásszámára. Így a [10]-ben szereplő korlát nem volt explicit. Evertse [8] azóta született eredményét és a [10]-ben szereplő korlátot felhasználva ma már könnyen explicit korlát adható széteső polinom egyenletek megoldásszámára. Ebben a fejezetben lényegesen megjavítjuk az így nyerhető korlátot. Megmutatjuk továbbá, hogy ugyanezen feltételek mellett a megfelelő általánosabb

$$F(\mathbf{x}) \in b\mathbb{Z}_S^* \quad \mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}_S^m, \quad (2)$$

egyenletnek akár végtelen sok megoldása is lehet. Megadunk egy elégséges feltételt, melynek teljesülése esetén a (2) egyenletnek csak véges sok megoldása van. Sőt, a $b = 1$ esetben egy jóval gyengébb, már szükséges feltétel mellett is sikerült hasonló alakú felső korlátot adnunk a megoldásszámról, feltéve, hogy a megoldások száma véges.

A felsorolt eredményeknek kilenc következményét adjuk, amelyeket az említett eredmények speciális esetekben való alkalmazása útján nyertünk. Így korlátot adunk inhomogén Thue egyenletek, diszkrimináns polinom, norma polinom és rezultáns polinom egyenletek megoldásszámára is. Az ebben a fejezetben közölt eredmények témavezetőmmel, Dr. Győry Kálmánnal közösen elért eredmények, melyeket a [3] közös cikk formájában kívánunk megjelentetni.

A **második fejezet** norma forma egyenletek megoldásszámával kapcsolatos eredményeket tartalmaz. Tegyük fel, hogy $\alpha_1 = 1, \alpha_2, \dots, \alpha_m$ egy K algebrai számtest $\mathbb{Q}$ felett lineárisan független elemei. Legyen $S = \{p_1, \dots, p_s\}$ prímszámok egy véges halmaza és b az S elemeihez relatív prím racionális egész szám. A második fejezetben

$$\begin{aligned} a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \dots + \alpha_m x_m) &= b p_1^{z_1} \dots p_s^{z_s} \\ x_1, \dots, x_m &\in \mathbb{Z}, \\ z_1, \dots, z_s &\in \mathbb{Z}_{\geq 0} \\ (x_1, \dots, x_m, p_1 \dots p_s) &= 1 \text{ ha } s > 0 \end{aligned} \tag{3}$$

alakú norma forma egyenletek megoldásszámára vonatkozó felső becsléseket adunk. Itt a_0 -t úgy választjuk meg, hogy (3) baloldala $x_1, \dots, x_m$ egész együtthatós polinomja legyen. Nem teszünk különbséget (3) azon $\mathbf{x} = (x_1, \dots, x_m), z_1, \dots, z_s$ és $\mathbf{x}' = (x'_1, \dots, x'_m), z'_1, \dots, z'_s$ megoldásai között, melyekre $\mathbf{x}' = \pm \mathbf{x}$ teljesül. Győry [20]-ban effektív formában bebizonyította, hogy amennyiben az α_m foka a $\mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})$ test felett legalább 3, akkor a (3) egyenletnek csak véges sok olyan megoldása lehet, melyre $x_m \neq 0$ teljesül. Ugyanezen feltételek mellett Evertse és Győry [14]-ben explicit korlátot adott a megoldásszámra. Megjegyezzük, hogy a fenti feltételek mellett a norma forma elfajuló is lehet, és akár végtelen sok $x_m = 0$ feltételt teljesítő megoldása is létezhet. Ezért az ilyen típusú eredmények még ineffektív formában sem következnek Schmidt és Schlickevei korábbi, nem-elfajuló norma forma egyenletekre vonatkozó ineffektív végességi eredményeiből. Később a nem-elfajuló esetben Schmidt [39], Győry [23], $b = 1$ esetén Evertse [8], míg általában Evertse és Győry [14] ugyan adtak explicit korlátokat a megoldásszámra, de mint már említettük, ezekből nem következik új korlát a fenti esetre, amely [20]-ban és [14]-ben szerepelt.

Norma forma egyenletekkel kapcsolatos további eredmények találhatók a [27] áttekintő dolgozatban, a [39] könyvben és az ezekben idézett dolgozatok-

ban.

A második fejezetben a [20]-ban és [14]-ben tekintett feltételek mellett lényegesen javítjuk a megoldásszámmra adott korlátot. Ennek bizonyításához Győry egy ötletét felhasználva a norma forma egyenletet visszavezetjük egy relatív Thue-Mahler egyenletre, majd ennek megoldásszámát becsüljük Evertse egy eredményét [9] felhasználva. Ugyanezen feltételek mellett egy még jobb korlátot is levezetünk, amelyet azonban csak véges sok b értéktől eltekintve tudunk bizonyítani. A kivételes b értékek számára szintén adunk egy felső becslést. Ezen eredményünk bizonyításában Győry módszerét felhasználva az eredeti egyenletet alkalmas egységegyenletekből álló egyenletrendszerre vezetjük vissza, majd Evertse és Győry [14] valamint Evertse, Győry, Stewart és Tijdeman [15] eredményeinek felhasználásával kapjuk a korlátot a megoldásszámmra. A kivételek számára Győry [22], Beukers és Schlickewei [6] valamint Evertse és Schlickewei [17] eredményeit felhasználva adódik a korlát. Az ebben a fejezetben feldolgozott eredményeink a [2] cikkünkben fognak megjelenni.

A **harmadik fejezetben** index forma egyenletek megoldásszámára vonatkozó eredmények szerepelnek. Legyen K egy algebrai számtest és tegyük fel, hogy $\{1, \alpha_2, \dots, \alpha_n\}$ egész bázis K algebrai egészeinek gyűrűjében. Jelölje D_K a K test diszkriminánsát és $I(X_2, \dots, X_n)$ az $\{1, \alpha_2, \dots, \alpha_n\}$ egész bázishoz tartozó index formát. Legyen $S = \{p_1, \dots, p_s\}$ racionális prímek egy halmaza és I egy S elemeihez relatív prím racionális egész szám. Tekintsük az

$$\begin{aligned} I(x_2, \dots, x_n) &= \pm I p_1^{z_1} \dots p_s^{z_s} \\ x_2, \dots, x_n &\in \mathbb{Z}, \\ z_1, \dots, z_s &\in \mathbb{Z}_{\geq 0} \\ (x_2, \dots, x_n, p_1 \dots p_s) &= 1 \text{ ha } s > 0. \end{aligned} \tag{4}$$

index forma egyenletet. Itt sem fogunk különbséget tenni a (4) egyenlet $\mathbf{x} = (x_2, \dots, x_n), z_1, \dots, z_s$ és $\mathbf{x}' = (x'_2, \dots, x'_n), z'_1, \dots, z'_s$ megoldásai között, ha $\mathbf{x}' = \pm \mathbf{x}$ teljesül.

Az $s = 0$ esetben Győry [18]-ban bebizonyította, hogy a (4) egyenletnek csak véges sok megoldása lehet, s explicit korlátot adott a megoldásokra. Győry eredményét Trelina [42], illetve Győry és Papp [29] egymástól függetlenül terjesztették ki az $s > 0$ esetre. Az első, $\alpha_2, \dots, \alpha_n$ -től független korlát a megoldásszámmra Evertse és Győry [11] nevéhez fűződik. Később Evertse [8] illetve Evertse és Győry [14] javították ezt a korlátot. Diszkrimináns és index forma egyenletekkel kapcsolatos további eredmények találhatók a [28]

áttekintő dolgozatban és az ott idézett cikkekben.

Nemrég Györy [28] lényegesen javította a megoldásszámra vonatkozó [11]-beli korlátot abban a fontos speciális esetben, amikor a K test $\mathbb{Q}$ feletti normális lezártjának $\mathcal{G}$ Galois csoportja háromszorosan tranzitív.

A harmadik fejezetben ugyanezen feltétel mellett lényegesen javítjuk a megoldásszámra vonatkozó [14]-beli korlátot, azzal a megszorítással, hogy az így kapott korlát csak véges sok I értéktől eltekintve lesz érvényes. Ezen felül korlátot adunk a kivételes I értékek számára is. Eredményünk következményeként korlátot adunk diszkrimináns forma egyenletek megoldásszámára, továbbá adott diszkriminánsú elemek számára is. A tétel igazolása a norma forma egyenletekre vonatkozó hasonló eredmény bizonyításához hasonlóan történik, és szintén Györy módszerén és a [14], [15], [22] [17], [6] eredményeinek alkalmazásán múlik. A fejezet új eredményeit az [1] dolgozat tartalmazza.

A **negyedik fejezetben** Turán Pál egy irreducibilis polinomokkal kapcsolatos problémájának vizsgálatára kerül sor. Itt meg kell jegyezni, hogy egész együtthatós polinomok irreducibilitásának a vizsgálata diofantikus problémára vezet. Valóban, ha egy egész együtthatós polinom felbomlik két egész együtthatós polinom szorzatára, akkor a két tényező együtthatóit ismeretlennek tekintve, és a szorzat együtthatóit összevetve az eredeti polinom együtthatóival, egy diofantikus egyenletrendszert kapunk.

Egy $P \in \mathbb{Z}[x]$ polinom $|P|$ hosszán a polinom együtthatói abszolút értékeinek az összegét értjük. Két egész együtthatós polinom távolságán különbségük hosszát szokás érteni.

Turán Pál a következő problémát vetette fel: Létezik-e olyan C abszolút konstans, hogy minden n -ed fokú $P(x) \in \mathbb{Z}[x]$ polinomhoz található legyen olyan $Q(x) \in \mathbb{Z}[x]$ irreducibilis polinom, melyre $\deg(Q) \leq n$ és $|P - Q| \leq C$ teljesül. A probléma igen nehéznek bizonyult. A legjobb eredményt Schinzel érte el, aki a következőt bizonyította: Bármely $P \in \mathbb{Z}[X]$ polinomhoz létezik végtelen sok $Q \in \mathbb{Z}[x]$ irreducibilis polinom, melyekre

$$|P - Q| \leq \begin{cases} 2 & \text{ha } P(0) \neq 0, \\ 3 & \text{egyébként.} \end{cases}$$

Ezen kívül legalább egy ilyen Q polinom teljesíti a következő feltételt is:

$$\deg(Q) \leq e^{(5 \deg(P) + 7)(|P|^2 + 3)}.$$

A Hajdu Lajossal közös [4] cikkünkben beláttuk, hogy 22-nél nem magasabb fokú polinomok esetén C választható 4-nek.

A negyedik fejezetben megmutatjuk, hogy $C \leq 4$ a legfeljebb 24-ed fokú polinomok esetén is igaz. A módszer alapötlete megegyezik azzal, amit [4]-ben alkalmaztunk, azaz a problémát véges testek felett kezeljük, így adott fokszám esetén a problémát végeessé tesszük, majd számítógép segítségével ellenőrizzük az állítást. Az erre vonatkozó része a fejezetnek a Hajdu Lajossal közös [5] cikkünkben jelent meg. A negyedik fejezet ugyanakkor tartalmaz mindezidáig még nem közölt eredményeket (táblázatokat) az általunk vizsgált ún. extrémális polinomokkal kapcsolatban. Ezeket szintén Hajdu Lajossal közösen végzett vizsgálataink során nyertük.

Bibliography

- [1] A. BÉRCZES, On the number of solutions of index form equations, *Publ. Math. Debrecen*, **56** (2000), 251–262.
- [2] A. BÉRCZES, On the number of solutions of norm form equations, *Periodica Math. Hungar.*, accepted for publication.
- [3] A. BÉRCZES and K. GYÖRY, On the number of solutions of decomposable polynomial equations, in preparation.
- [4] A. BÉRCZES and L. HAJDU, Computational experiences on the distances of polynomials to irreducible polynomials, *Math. Comp.*, **66** (1997), 391–398.
- [5] A. BÉRCZES and L. HAJDU, On a problem of P. Turán concerning irreducible polynomials, in: *Number theory (Eger, 1996)*, de Gruyter, Berlin, 1998, pp. 95–100.
- [6] F. BEUKERS and H. P. SCHLICKWEI, The equation $x + y = 1$ in finitely generated groups, *Acta Arith.*, **78** (1996), 189–199.
- [7] Z. I. BOREVICH and I. R. SHAFAREVICH, *Number Theory*, Academic Press, New-York, 1967, 2nd ed.
- [8] J.-H. EVERTSE, The number of solutions of decomposable form equations, *Invent Math.*, **122** (1995), 559–601.
- [9] J.-H. EVERTSE, The number of solutions of the Thue-Mahler equation, *J. Reine Angew. Math.*, **482** (1997), 121–149.
- [10] J.-H. EVERTSE, I. GAÁL and K. GYÖRY, On the numbers of solutions of decomposable polynomial equations, *Archiv Math.*, **52** (1989), 337–353.

- [11] J.-H. EVERTSE and K. GYÖRY, On unit equations and decomposable form equations, *J.Reine Angew. Math.*, **358** (1985), 6–19.
- [12] J.-H. EVERTSE and K. GYÖRY, Decomposable form equations, in: *New advances in transcendence theory (Durham, 1986)*, Cambridge Univ. Press, Cambridge, 1988, pp. 175–202.
- [13] J.-H. EVERTSE and K. GYÖRY, Finiteness criteria for decomposable form equations, *Acta Arith.*, **50** (1988), 357–379.
- [14] J.-H. EVERTSE and K. GYÖRY, The number of families of solutions of decomposable form equations, *Acta Arith.*, **80** (1997), 367–394.
- [15] J.-H. EVERTSE, K. GYÖRY, C. L. STEWART and R. TIJDEMAN, On S -unit equations in two unknowns, *Invent. Math.*, **92** (1988), 461–477.
- [16] J.-H. EVERTSE, K. GYÖRY, C. L. STEWART and R. TIJDEMAN, S -unit equations and their applications, in: *New advances in transcendence theory (Durham, 1986)*, Cambridge Univ. Press, Cambridge, 1988, pp. 110–174.
- [17] J.-H. EVERTSE and H. P. SCHLICKWEI, The absolute subspace theorem and linear equations with unknowns from a multiplicative group, in: *Number Theory in Progress* (K. GYÖRY, H. IWANIEC and J. URBANOWICZ, eds.), Walter de Gruyter, Berlin – New York, 1999, pp. 121–142.
- [18] K. GYÖRY, Sur les polynômes à coefficients entiers et de discriminant donné III, *Publ. Math. Debrecen*, **23** (1976), 141–165.
- [19] K. GYÖRY, Résultats effectifs sur la représentation des entiers par des formes décomposables, *Queen’s Papers in Pure and Applied Math.*, No. 56, Kingston, Canada, 1980.
- [20] K. GYÖRY, On the representation of integers by decomposable forms in several variables, *Publ. Math. Debrecen*, **28** (1981), 89–98.
- [21] K. GYÖRY, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta Math. Hungar.*, **42** (1983), 45–80.
- [22] K. GYÖRY, Upper bounds for the number of solutions of unit equations in two unknowns, *Lithuanian Math. J.*, **32** (1992), 40–44.

- [23] K. GYÖRY, On the numbers of families of solutions of systems of decomposable form equations, *Publ. Math. Debrecen*, **42** (1993), 65–101.
- [24] K. GYÖRY, Some applications of decomposable form equations to resultant equations, *Colloq. Math.*, **65** (1993), 267–275.
- [25] K. GYÖRY, On the irreducibility of neighbouring polynomials, *Acta Arith.*, **67** (1994), 283–294.
- [26] K. GYÖRY, Recent bounds for the solutions of decomposable form equations, in: *Number Theory*, Walter de Gruyter, Berlin – New York, 1998, pp. 255–270.
- [27] K. GYÖRY, On the distribution of solutions of decomposable form equations, in: *Number Theory in Progress*, Walter de Gruyter, Berlin – New York, 1999, pp. 237–265.
- [28] K. GYÖRY, Discriminant form and index form equations, in: *Algebraic Number Theory and Diophantine Analysis*, Walter de Gruyter, Berlin – New York, 2000, pp. 191–214.
- [29] K. GYÖRY and Z. Z. PAPP, On discriminant form and index form equations, *Studia Sci. Math. Hungar.*, **12** (1977), 47–60, (1980).
- [30] L. HAJDU, *Some new results on polynomials and diophantine equations*, PhD thesis, Debrecen, 1997.
- [31] H.-W. KNOBLOCH, Zum Hilbertschen Irreduzibilitätssatz, *Abh. Math. Sem. Univ. Hamburg*, **19** (1955), 176–190.
- [32] M. LAURENT, Equations diophantiennes exponentielles, *Invent. Math.*, **78** (1984), 299–327.
- [33] A. SCHINZEL, Reducibility of polynomials and covering systems of congruences, *Acta Arith.*, **13** (1967), 91–101.
- [34] A. SCHINZEL, Reducibility of lacunary polynomials II, *Acta Arith.*, **16** (1970), 371–392.
- [35] H. P. SCHLICKWEI, On norm form equations, *J. Number Theory*, **9** (1977), 370–380.

- [36] W. M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.*, **191** (1971), 1–20.
- [37] W. M. SCHMIDT, Norm form equations, *Ann. of Math.*, **96** (1972), 525–551.
- [38] W. M. SCHMIDT, The number of solutions of norm form equations, *Trans. Amer. Math. Soc.*, **317** (1990), 197–227.
- [39] W. M. SCHMIDT, *Diophantine approximations and diophantine equations*, Springer-Verlag, 1991.
- [40] T. N. SHOREY and R. TIJDEMAN, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge–New York, 1986.
- [41] C. L. STEWART, On the number of solutions of polynomial congruences and Thue equations, *J. Amer. Math. Soc.*, **4** (1991), 793–835.
- [42] L. A. TRELINA, On the greatest prime factor of an index form (in Russian), *Dokl. Akad. Nauk BSSR*, **21** (1977), 975–976.

Appendix A

List of papers of the author, and citations to these publications

1. A. BÉRCZES and L. HAJDU, Computational experiences on the distances of polynomials to irreducible polynomials, *Math. Comp.*, **66** (1997), 391–398.
 - L. HAJDU, *Some new results on polynomials and diophantine equations*, PhD thesis, Debrecen, 1997.
 - A. SCHINZEL, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge, 2000, with an appendix by Umberto Zannier.
2. A. BÉRCZES and L. HAJDU, On a problem of P. Turán concerning irreducible polynomials, in: *Number theory (Eger, 1996)*, de Gruyter, Berlin, 1998, pp. 95–100.
3. A. BÉRCZES, B. BRINDZA and L. HAJDU, On the power values of polynomials, *Publ. Math. Debrecen*, **53** (1998), 375–381.
 - B. BRINDZA, Diofantikus egyenletek megoldásszámára vonatkozó becslések, Akadémiai doktori értekezés, 1997.
 - B. BRINDZA, On a generalization of the Ramanujan-Nagell equation, *Publ. Math. Debrecen*, **53** (1998), 225–233.

- K. GYÖRY, Solving diophantine equations by Baker's theory, to appear.
4. A. BÉRCZES, On the number of solutions of index form equations, *Publ. Math. Debrecen*, **56** (2000), 251–262.
 - K. GYÖRY, Discriminant form and index form equations, in: *Algebraic Number Theory and Diophantine Analysis*, Walter de Gruyter, Berlin – New York, 2000, pp. 191–214.
 5. A. BÉRCZES, On the number of solutions of norm form equations, *Periodica Math. Hungar.*, accepted for publication.
 6. A. BÉRCZES and K. GYÖRY, On the number of solutions of decomposable polynomial equations, in preparation.

Appendix B

List of conference talks of the author

1. On a problem of P. Turán, Number Theory Conference, Eger 1996.
2. On power values of polynomials, 13th Czech and Slovak International Number Theory Conference, Ostravice 1997.
3. Diszkrimináns forma egyenletek megoldásszámára vonatkozó becslések, Magyar Matematikus Doktoranduszok Konferenciája, Szeged 1998.
4. On index form equations, 14th Czech and Slovak International Number Theory Conference, Liptovsky Jan 1999.
5. On the number of solutions of norm form equations, Colloquium on Number Theory, Debrecen 2000.

Appendix C

As was mentioned on page 17, in (1.15) the linear independence of $\alpha_1, \dots, \alpha_m, \lambda$ over $\mathbb{Q}$ implies that the number of solutions of equation (1.15) does not exceed the bound (1.6). This is a special case of our Corollary 1.1. This special case was proved independently by J.-H. Evertse, C.L. Stewart and R. Tijdeman (private communication).

**Some new diophantine results on decomposable
polynomial equations and irreducible polynomials**

Értekezés a doktori (PhD) fokozat megszerzése érdekében a
matematika tudományában.

Írta: Bérczes Attila okleveles matematikus,
matematika tanár és angol-magyar szakfordító

Készült a Debreceni Egyetem Matematika doktori programja
(Diofantikus és konstruktív számelmélet alprogramja) keretében

Témavezető: Dr. Győry Kálmán

A doktori szigorlati bizottság:

elnök: Dr.

tagok: Dr.

Dr.

A doktori szigorlat időpontja 200... ..

Az értekezés bírálói:

Dr.

Dr.

Dr.

A bírálóbizottság :

elnök: Dr.

tagok: Dr.

Dr.

Dr.

Dr.

Az értekezés védésének időpontja: 200... ..

