Constructive methods for Diophantine Equations

doktori (Ph.D.) értekezés tézisei

Járási István

Debreceni Egyetem
Debrecen, 2005

Introduction

In this thesis we describe new efficient algorithms for the resolution of four distinct diophantine problems, all detailed in separate sections. The common feature of these problems is that almost all involve the explicit resolution of certain types of unit equations, applying Baker type estimates, reduction procedures and enumeration algorithms. For the resolution of these diophantine problems we had to improve some known constructive methods (see I.Gaál [10]). It is important to notice that the resulting procedures provide efficient tools to solve several other diophantine problems.

1 Index form equations in sextic fields with a cubic subfield

Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. The index of a primitive $\alpha \in \mathbb{Z}_K$ is defined by

$$I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}^+[\alpha]).$$

Equivalently, the index of a primitive $\alpha \in \mathbb{Z}_K$ can be determined by

$$I(\alpha) = \frac{\prod_{1 \le i < j \le n} |\alpha^{(i)} - \alpha^{(j)}|}{\sqrt{|D_K|}}$$

where $\alpha^{(i)}$ $(1 \le i \le n)$ denote the conjugates of α and D_K is the discriminant of the field K.

It is obvious that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an integral basis if and only if $I(\alpha) = 1$. Such an integral basis is called power integral basis. If there exists such an $\alpha \in \mathbb{Z}_K$, then $\mathbb{Z}_K$ is called monogene.

Let $\{1, \omega_2, \ldots, \omega_n\}$ be an arbitrary integral basis in K. Then the discriminant of the linear form $l(x) = x_2\omega_2 + \ldots + x_n\omega_n$ can be written as

$$D(l(x)) = (I(x_2, \ldots, x_n))^2 \cdot D_K$$

where $I(x_2, \ldots, x_n)$ is the index form corresponding to the integral basis $\{1, \omega_2, \ldots, \omega_n\}$, and D_K is the discriminant of the field K. This index form has the property that for an arbitrary primitive element

$$\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$$

we have

$$I(\alpha) = |I(x_2, \dots, x_n)|.$$

So the problem of determining all generators of power integral bases is equivalent to determine the elements of index 1 or to solve the index form equation

$$I(x_2, \dots, x_n) = \pm 1 \quad (x_2, \dots, x_n \in \mathbb{Z}).$$

For an arbitrary $z \in \mathbb{Z}$ the indices of α and $\pm\alpha + z$ coincide. These numbers are called equivalent. In 1976 K.Győry [16] proved effectively that any index form equation has only finitely many solutions, that is up to equivalence there are only finitely many elements of $\mathbb{Z}_K$ of index 1. For results on power integral bases see the survey K.Győry [21] and the monograph I.Gaál [10], and the references given there.

In the first chapter we consider index form equations over sextic fields. There are no general feasible algorithms for solving such equations in full generality. Fast algorithms for solving index form equations have only been given for lower degree number fields and special higher degree number fields [10]. For sextic fields the only case the generators of power integral bases were determined relatively fast is when the sextic field has a quadratic subfield, cf. I.Gaál [7], [6] and I.Gaál and M.Pohst [13]. In this case the index form equation reduces to a relative Thue equation over the quadratic subfield which makes the resolution easier.

We consider sextic fields having a cubic subfield. This important case is not yet covered by former feasible methods. In this case the index form equation is much more complicated than in the previously considered sextic fields. Hence our first purpose is to determine the "small" solutions of the index form equation, that is to compute generators of power integral bases having "small" coordinates in an integral basis. By "small" solutions we mean solutions with coefficients bounded by about 10^5. Note that the experience suggests that it is very likely that all solutions are "small". Especially, the generators of power integral bases used in most practical applications have "small" coordinates.

Our result is an algorithm to determine the "small" solutions of the index form equation. It is based on the following theorems:

Let ϱ be a cubic algebraic integer. We may assume, that it generates a power integral basis in $\mathbb{Q}(\varrho)$, since the contrary case can be treated similarly. Let ϑ be a an algebraic integer which is quadratic over $\mathbb{Q}(\varrho)$. Denote by $\varrho^{(i)}$

the conjugates of ϱ for $i = 1, 2, 3$ and by $\vartheta^{(i1)}, \vartheta^{(i2)}$ the conjugates of ϑ over $M^{(i)} = \mathbb{Q}(\varrho^{(i)})$ for $i = 1, 2, 3$. In general for any $\gamma \in M$ we denote by $\gamma^{(i)}$ the conjugates of γ corresponding to $\varrho^{(i)}$.

Let

$$\beta_k = \frac{(\alpha^{(i1)} - \alpha^{(j1)})(\alpha^{(i2)} - \alpha^{(j2)})(\alpha^{(i2)} - \alpha^{(j1)})(\alpha^{(i1)} - \alpha^{(j2)})}{(\varrho^{(i)} - \varrho^{(j)})^2},$$

where $k = 1, 2, 3$ belong to $(i, j) = (2, 3), (3, 1), (1, 2)$, respectively.

Theorem 1. *If $\alpha \in \mathbb{Z}_K$ generates a power integral basis in K, then β_k is an algebraic integer in $M^{(k)} = \mathbb{Q}(\varrho^{(k)})$ for $k = 1, 2, 3$.*

Theorem 2. *If $\alpha \in \mathbb{Z}_K$ represented in the form $x_0 + x_1\varrho + x_2\varrho^2 + y_0\vartheta + y_1\vartheta\varrho + y_2\vartheta\varrho^2$ generates a power integral basis, then*

$$N_{M/\mathbb{Q}}(y_0 + y_1\varrho + y_2\varrho^2) = \pm 1,$$

and

$$N_{M/\mathbb{Q}}(\beta) = \pm 1.$$

As an application, we also give several numerical examples. We also constructed an infinite parametric families of monogene sextic fields with a cubic subfield:

Theorem 3. *Let b_0, b_1, c_0, c_1 be integers such that*

$$b_1^2 - c_0c_1b_1 + b_0c_1^2 = \pm 1$$

holds.

Let ϱ be an arbitrary cubic algebraic integer, $M = \mathbb{Q}(\varrho)$, $\gamma = c_0 + c_1\varrho$, $\delta = b_0 + b_1\varrho$. Let the coefficients of the quadratic relative defining polynomial of ϑ over M be

$$\vartheta^{(i1)} + \vartheta^{(i2)} = \gamma^{(i)}$$

and

$$\vartheta^{(i1)}\vartheta^{(i2)} = \delta^{(i)}. \quad \text{for } i = 1, 2, 3$$

Then in the order $\mathcal{O} = \mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$ the element ϑ generates a power integral basis.

In the second part of the chapter we also give a feasible algorithm for the *complete* resolution of index form equations in such fields. Using standard arguments we reduce the index form equation to unit equations in two variables. The idea used in I.Gaál and K.Győry [11] implies that the rank of the corresponding unit groups is at most 11. These unit equations are solved using the reduction method and enumeration method described by Gaál and Pohst [14] (see also [10]). This enumeration method is based on K. Wildanger's ideas, cf. [32], [33]. We consider in detail the most difficult case when the sextic field is totally real and has the largest possible Galois group $S_4 \times C_2$. Note that recently Y.Bilu, I.Gaál and K.Győry [1] gave an algorithm for solving index form equations in any sextic field but our methods are much faster than that method.

The results of this chapter published in [27] and [26].

2 Results on Heron triangles

A *Heron* triangle is a triangle having integral area and side lengths. There are several open questions concerning the existence of Heron triangles with certain properties. For example, it is not known whether there exist Heron triangles with integral median lengths (see [15]), and it is not known whether there exist Heron triangles having the property that the lengths of all their sides are Fibonacci numbers (see [23] and [24]). Another unsolved problem asks for the existence of a perfect cuboid, i.e., a rectangular box such that the lengths of all sides, face diagonals, and main diagonal are integers. This problem is related to the existence of a Heron triangle having the lengths of its sides perfect squares and the lengths of its bisectors positive integers (see [31]).

Let $P(k)$ denote the largest prime factor of k. We prove that $P(abc) \to \infty$ when $\max(a, b, c) \to \infty$ over the triples of positive integers (a, b, c) which are the sides of reduced Heron triangles. The proof is based on the finiteness of the number of solutions of $\mathcal{S}$-unit equations in three unknowns and hence it is ineffective.

Assuming that the prime divisors of abc are of certain shape, we obtain effective results. Let $\mathcal{P}$ be a fixed set of primes and let S denote the set of integers divisible only by primes in $\mathcal{P}$. We prove that there are only finitely many Heron triangles whose sides $a, b, c \in S$ with $\gcd(a, b, c) = 1$. If $\mathcal{P}$ con-

tains only one prime $\equiv 1 \pmod 4$ then all such triangles can be effectively determined. Moreover, if $\mathcal{P} = \{2, 3, 5, 7, 11\}$ then all such triangles are given explicitly. The above results has been published in [12].

Our results summarized in the following theorems:

Theorem 4. *$P(abc) \to \infty$ when $\max(a, b, c) \to \infty$ over the triples of positive integers (a, b, c) which are the sides of reduced Heron triangles.*

Theorem 5. *Let $\mathcal{P}$ be a finite set of prime numbers containing exactly one prime $p \equiv 1 \pmod 4$. Let $\mathcal{S}$ be the set of all positive integers whose prime factors belong to $\mathcal{P}$. Then there are only finitely many effectively computable reduced Heron triangles whose sides have lengths $a,\ b,\ c$ such that $abc \in \mathcal{S}$.*

Theorem 6. *The only reduced Heron triangles whose sides are of lengths $a \le b \le c$ with $P(abc) < 13$ are given by:*

a	b	c
3	4	5
5	5	6
5	5	8
7	15	20
7	24	25
11	25	30
14	25	25
25	25	48
35	44	75
55	84	125
88	125	125
625	625	672

3 Applications of unit equations in three unknowns

Several classes of decomposable form equations such as Thue equations, discriminant form, index form and norm form equations of special type can be reduced to unit equations in two variables of the shape

$$\alpha_1 u_1 + \alpha_2 u_2 = 1$$

(see [16],[17],[20],[22]), where u_1, u_2 are unknown units and α_1, α_2 are fixed algebraic numbers. By Baker's method K.Győry derived effective upper bounds for the solutions of such equations.

Applying reduction methods and the enumeration procedures due to K.Wildanger, recently it became possible to solve completely some of these equations (see [10] for an overview). These equations usually have only "small" solutions.

J.-H.Evertse and K.Győry (see e.g. [4]) showed that arbitrary decomposable form equations are equivalent to a system of unit equations in *several variables*.

By our present knowledge, Baker's method is not applicable to unit equations in more than two variables, so using this approach there is no hope to solve completely these equations. Hence we are going to give an algorithm for calculating all "small" solutions of unit equations in three variables. The application of this method makes it possible to find all "small" solutions of some classes of decomposable form equations, that formerly could not be treated with the above standard tools. The method is based on the ideas of K.Wildanger [33] and I.Gaál and M.Pohst [14] (see also [10]) and uses the method of U.Fincke and M.Pohst [5] for enumerating points in ellipsoids.

In the first application we enumerate the "small" solutions of a norm form equation. Note that formerly the only algorithmic result for solving norm form equations in several variables was that of I.Gaál [8] which deals with a more special case, but gives all solutions.

In our second application we considered resultant form equations. This type of equations can be reduced to unit equations in three unknowns, so we can apply our method. More precisely, we consider the following problem. Let K be a fixed algebraic number field and a a fixed non-zero integer. Find all polynomials $P, Q \in \mathbb{Z}[x]$ with all their zeros in K and

$$Res(P, Q) = a. \tag{1}$$

It is easy to see that if $(P(x), Q(x))$ is a solution to (1) then for any $b \in \mathbb{Z}$ $(P_1(x), Q_1(x)) = (P(x+b), Q(x+b))$ is also a solution to (1). In this case the pairs $(P(x), Q(x))$ and $(P_1(x), Q_1(x))$ are called $\mathbb{Z}-$ equivalent.

It was shown by K.Győry [18] that there exist only finitely many $\mathbb{Z}$-equivalence classes of pairs of polynomials (P, Q) satisfying (1) such that $deg(P) \geq 2$, $deg(Q) \geq 2$, $deg(P) + deg(Q) \geq 5$ and both P and Q has simple roots. He also showed that the same assertion is valid if $\mathbb{Z}$ is replaced by any

finitely generated and integrally closed domain over $\mathbb{Z}$. In [19] Győry gave an explicit upper bound for the degrees of P and Q and for the number of solutions (P, Q).

We determine the "small" solutions of (1) such that P and Q are irreducible polynomials with roots generating the fixed number fields M_1 and M_2, respectively. This is a special case of the above problem. We reduce the problem to unit equations in three unknowns and we use the method of [29] to handle such equations. Since the direct application of that method would require far too much CPU time, we have developed two essential improvements which enable us to perform the computations within feasible CPU time. For a former algorithmic result on special resultant type equations see I.Gaál [9]. The results of this chapter are contained in [28] and [29].

4 On the diophantine equation $x^n = Dy^2 + 1$

A classical problem in the theory of diophantine equations is to find the solutions of

$$x^n = Dy^2 + 1. \tag{2}$$

in integers x, y, n with $n \geq 3$, where D is a fixed squarefree integer.

For given D this equation has only finitely many solutions in positive integers x, y and $n \geq 3$. For $n = 4$ Ljunggren [30] proved that for any D (2) has at most two positive solutions.

Using elementary and algebraic number theoretical tools J.H.E. Cohn [3] proved necessary conditions for the unsolvability of (2). Moreover, he solved (2) completely for $D \leq 100$ up to six pairs of (n, D). We complete Cohn's result by solving the remaining six equations.

Our results are summarized in the following

Theorem 7. *Apart from* $(x, y) = (1, 0)$ *equation*

$$x^n = Dy^2 + 1$$

has the solutions

$$
\begin{array}{lll}
(x,y) = (5, \pm 12), & \textit{if} & (n,D) = (3,31) \\
(x,y) = (2, \pm 1), & \textit{if} & (n,D) = (5,31) \\
(x,y) = (7, \pm 3), & \textit{if} & (n,D) = (3,38) \\
(x,y) = (13, \pm 6), & \textit{if} & (n,D) = (3,61) \\
\textit{none}, & \textit{if} & (n,D) = (5,71) \\
\textit{none}, & \textit{if} & (n,D) = (7,71).
\end{array}
$$

Our results has been published in [25].

Bevezető

A disszertációban négy különböző diofantikus probléma megoldására adunk új, hatékony algoritmust. Ezen problémák közös tulajdonsága, hogy majdnem mindegyikük ún. egységegyenletek megoldására vezethető vissza, és ezen egységegyenletek a Baker módszer, redukciós eljárások és leszámlálási algoritmusok használatával oldhatóak meg. A tézisbeli problémák megoldásához azonban a már meglévő konstruktív módszereket (áttekintésért lásd: Gaál I. [10]) kell lényegesen továbbfejlesztenünk. Fontos megjegyeznünk, hogy az így nyert módszerek más diofantikus problémák megoldásához is hatékony eszközt szolgáltatnak.

5 Index forma egyenletek harmadfokú résztesttel rendelkező hatodfokú számtestekben

Legyen K egy n-ed fokú algebrai számtest, $\mathbb{Z}_K$ a K-beli algebrai egészek gyűrűje. Ekkor

$$I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}^+[\alpha])$$

az $\alpha \in \mathbb{Z}_K$ primitív elem indexe. Az α indexe kifejezhető az

$$I(\alpha) = \frac{\prod_{1 \le i < j \le n} |\alpha^{(i)} - \alpha^{(j)}|}{\sqrt{|D_K|}}$$

alakban is, ahol $\alpha^{(i)}$ $(1 \le i \le n)$ jelöli az α konjugáltjait, D_K a K diszkriminánsa. Az

$$I(\alpha) = I$$

tipusú egyenletet, ahol I egy adott egész, α ismeretlen elem $\mathbb{Z}_K$-ből, index forma egyenletnek nevezzük.

Tetszőleges $z \in \mathbb{Z}$-re az α és $\pm\alpha + z$ indexe megegyezik. Ezen elemeket ekvivalensnek nevezzük. 1976-ban Győry K. [16] effektíven bebizonyította, hogy egy index forma egyenletnek csak véges sok megoldása lehet, azaz ekvivalenciától eltekintve csak véges sok adott indexű egész elem van K-ban.

Nem ismeretes azonban általános hatékony algoritmus index forma egyenletek megoldására. Hatékony algoritmusok csak kis fokszámú számtestek esetében ismertek, valamint néhány speciális magasabb fokú test esetén (lásd [10]). A

másodfokú résztesttel rendelkező hatodfokú testek esetére Gaál I. [7], [6] és Gaál I. and M.Pohst [13] adott algoritmust.

Az első fejezetben harmadfokú résztesttel rendelkező hatodfokú számtestekben előforduló index forma egyenleteket vizsgálunk. Két algoritmust adunk meg. Az első az ilyen tipusú egyenletek "kis" megoldásainak megkeresésére szolgál. Ehhez a tetszőleges elem indexét megadó formula tulajdonságai szolgáltatnak alapot. Módszerünket egy numerikus példával illusztráljuk. Ugyancsak az index tulajdonságaira alapozva megadjuk számtestek egy végtelen parametrikus családját, melyben egy "nagy" rend monogén.

Első algoritmusunk alapjait a következő tételekben foglaljuk össze.

Legyen ϱ egy harmadfokú algebrai egész. Tegyük fel, hogy ϱ hatvány egész bázist generál $\mathbb{Q}(\varrho)$-ban, mivel az ellenkező hasonlóan kezelhető. Legyeb ϑ egy a $\mathbb{Q}(\varrho)$ felett másodfokú algebrai egész. Jelölje $\varrho^{(i)}$ a ϱ konjugáltjait $i = 1, 2, 3$-re és $\vartheta^{(i1)}, \vartheta^{(i2)}$ a ϑ $M^{(i)} = \mathbb{Q}(\varrho^{(i)})$ feletti konjugáltjait $i = 1, 2, 3$-re. Általában tetszőleges $\gamma \in M$-re jelölje $\gamma^{(i)}$ a γ elem $\varrho^{(i)}$-re vonatkozó konjugáltjait.

Legyen

$$\beta_k = \frac{(\alpha^{(i1)} - \alpha^{(j1)})(\alpha^{(i2)} - \alpha^{(j2)})(\alpha^{(i2)} - \alpha^{(j1)})(\alpha^{(i1)} - \alpha^{(j2)})}{(\varrho^{(i)} - \varrho^{(j)})^2},$$

ahol $k = 1, 2, 3$ rendre az $(i, j) = (2, 3), (3, 1), (1, 2)$ párhoz tartozik.

Tétel 1. *Ha $\alpha \in \mathbb{Z}_K$ hatvány egész bázist generál K-ban, akkor β_k algebrai egész $M^{(k)} = \mathbb{Q}(\varrho^{(k)})$-ban $k = 1, 2, 3$-re.*

Tétel 2. *Ha $\alpha = x_0 + x_1\varrho + x_2\varrho^2 + y_0\vartheta + y_1\vartheta\varrho + y_2\vartheta\varrho^2 \in \mathbb{Z}_K$ hatvány egész bázist generál, akkor*

$$N_{M/\mathbb{Q}}(y_0 + y_1\varrho + y_2\varrho^2) = \pm 1,$$

és

$$N_{M/\mathbb{Q}}(\beta) = \pm 1.$$

Módszerünk illusztrálásaként egy numerikus példát is bemutatunk. További alkalmazásként számtestek egy végtelen parametrikus családját is megadjuk, melyben egy "nagy" rend monogén.

Tétel 3. *Legyenek b_0, b_1, c_0, c_1 olyan egészek, melyekre*

$$b_1^2 - c_0c_1b_1 + b_0c_1^2 = \pm 1.$$

Legyen ϱ egy tetszőleges harmadfokú algebrai egész, $M = \mathbb{Q}(\varrho)$, $\gamma = c_0 + c_1\varrho$, $\delta = b_0 + b_1\varrho$. Legyenek a ϑ elem M feletti kvadratikus relatív definiáló polinomjának együtthatói

$$\vartheta^{(i1)} + \vartheta^{(i2)} = \gamma^{(i)}$$

és

$$\vartheta^{(i1)}\vartheta^{(i2)} = \delta^{(i)}. \quad \textit{ahol } i = 1, 2, 3$$

Ekkor a $K = \mathbb{Q}(\vartheta)$ test $\mathcal{O} = \mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ rendjében a ϑ elem hatvány egész bázist generál.

A második algoritmus segítségével meghatározhatjuk a fenti tipusú számtestek összes adott indexű elemét. Ehhez a problémát kétváltozós egységegyenletek megoldására vezetjük vissza. Gaál I. és Győry K. [11] egy ötletéből következően a szóban forgó egységcsoport rangja ≤ 11. Ezen egységegyenleteket az Gaál I. és M.Pohst [14] által kidolgozott (lásd még [10]) redukciós és leszámlálási eljárásokkal oldjuk meg. A leszámlálási eljárások K.Wildanger [33] módszerén alapulnak. Egy numerikus példát is bemutatunk, melyben az alaptest Galois csoportja a lehető legnagyobb elemszámú, azaz $S_4 \times C_2$. Megjegyezzük, hogy Y.Bilu, Gaál I. és Győry K. [1] módszert adott a tetszőleges hatodfokú számtestek esetére is, de az itt bemutatott módszerek lényegesen gyorsabbak ebben a speciális esetben. Ezen fejezet eredményei [27]-ben és [26]-ben jelentek meg.

6 Heron háromszögekre vonatkozó eredmények

A második fejezetben Heron háromszögekkel foglalkozunk. Azon háromszögeket, melyeknek oldalai és területe is egész, Heron háromszögeknek nevezzük. Számos nyitott probléma ismert ilyen háromszögekre vonatkozóan (lásd [15]).

Jelölje $P(k)$ a k legnagyobb prímosztóját. Megmutatjuk, hogy $P(abc) \to \infty$ ha $\max(a, b, c) \to \infty$ és az (a, b, c) számhármasok Heron háromszögek oldalai (a, b, c relatív prímek). A bizonyításban felhasználjuk az $\mathcal{S}$-egység egyenletek megoldásszámára vonatkozó végességi tételeket, így eredményünk ineffektív.

Effektív eredményeket nyerhetünk, ha az abc prímosztóiról feltesszük hogy egy adott tulajdonságú halmazból valóak. Legyen $\mathcal{P}$ prímek egy rögzített halmaza és legyen S azon egészek halmaza, melyek prímosztói $\mathcal{P}$-beliek. Megmutattuk, hogy csak véges sok $a, b, c \in S$ oldalú Heron háromszög létezik

melyre (a, b, c) relatív prím. Ha $\mathcal{P}$-ben csak egy prím van mely $\equiv 1 \pmod 4$, akkor ezen háromszögek effektíven meghatározhatóak. Továbbá, a $\mathcal{P} = \{2, 3, 5, 7, 11\}$ esetben az összes ilyen megoldást meghatározzuk.

Eredményünket a következő tételekben foglaljuk össze:

Tétel 4. *$P(abc) \to \infty$ amint $\max(a, b, c) \to \infty$ ahol (a, b, c) pozitív egészekből álló számhármasok, melyek redukált Heron háromszögek oldalai.*

Tétel 5. *Legyen $\mathcal{P}$ prímek egy olyan véges halmaza, melyben csak egy elem $\equiv 1 \pmod 4$. Legyen $\mathcal{S}$ azon pozitív egészek halmaza, melyek prímosztói $\mathcal{P}$-beliek. Ekkor csak véges sok, effektíven meghatározható redukált Heron háromszög van, melynek oldalai a, b, c és $abc \in \mathcal{S}$ teljesül.*

Tétel 6. *Azon redukált Heron háromszögek, melyeknek oldalai $a \leq b \leq c$ és $P(abc) < 13$ a következőek:*

a	b	c
3	4	5
5	5	6
5	5	8
7	15	20
7	24	25
11	25	30
14	25	25
25	25	48
35	44	75
55	84	125
88	125	125
625	625	672

7 Háromváltozós egységegyenletek alkalmazásai

A harmadik fejezetben háromváltozós egységegyenletekkel foglalkozunk. Fő eredményünkként módszert adunk háromváltozós egységegyenletek "kis" megoldásainak megkeresésére. Az általunk adott algoritmus K.Wildanger kétváltozós egységegyenletekre adott módszerének általánosítása. Eredményünket norma forma egyenletekre alkalmazzuk. A módszerünket jelentős továbbfejlesztéssel alkalmassá tettük rezultáns forma egyenletek "kis" megoldásainak meghatározására is. Mindkét eredményt numerikus példákkal illusztráljuk.

Számos szétesõ forma egyenlet, mint a Thue egyenletek, diszkrimináns forma, index forma, rezultáns forma és speciális norma forma egyenletek megoldása visszavezethetõ

$$\alpha_1 u_1 + \alpha_2 u_2 = 1$$

alakú kétváltozós egységegyenletek megoldására (lásd [16],[17],[20],[22]), ahol u_1, u_2 ismeretlen egységek és α_1, α_2 rögzített algebrai számok. Baker módszerének felhasználásával Győry K. effektív felső korlátot adott a fenti egyenletek megoldásainak nagyságára.

Redukciós módszereket és K.Wildanger leszámlálási módszerét alkalmazva mód nyílt arra hogy ilyen típusú egyenleteket teljesen megoldjunk (lásd [10]). Ezen egyenleteknek általában "kis" megoldásaik vannak csak.

J.-H.Evertse és Győry K. [4] megmutatta, hogy minden szétesõ forma egyenlet visszavezethetõ két- vagy többváltozós egyenletek rendszerére.

Jelenlegi ismereteink szerint Baker módszere nem alkalmas kettőnél több változós egységegyenletek megoldására, így ezzel a módszerrel nincs remény a fenti típusú egyenletek teljes megoldására. Ezért a kétváltozós egységegyenletekre vonatkozó eredményekből a "kis" megoldások meghatározásával kapcsolatosakat általánosítjuk háromváltozós egységegyenletekre. Így lehetővé válik számos szétesõ forma egyenlet "kis" megoldásainak megkeresése, melyre eddigi eszközökkel nem volt lehetőség. Módszerünk K.Wildanger [33] és M.Pohst és Gaál I. [14] módszerének általánosítása melynek alapja U.Fincke és M.Pohst [5] algoritmusa ellipszoidok egész pontjainak leszámlálására.

Módszerünk egyik alkalmazásaként eljárást adunk bizonyos típusú többváltozós norma forma egyenletek "kis" megoldásainak megkeresésére. Megjegyezzük, hogy többváltozós normaforma egyenletek numerikus megoldására eddig mindössze Gaál I. [8] adott módszert, mely az itt bemutatottnál speciálisabb esetben az összes megoldást meghatározza.

Módszerünk másik alkalmazásként rezultáns forma egyenleteket tekintettünk. Ezen egyenletek háromváltozós egységegyenletekre vezethetőek vissza, ezért módszerünk alkalmazható. Pontosabban a következő problémát vizsgáljuk. Legyen K egy rögzített számtest, és a egy szintén rögzített nem nulla egész. Ekkor keressük azon $P, Q \in \mathbb{Z}[x]$ polinomokat, melynek közös felbontási testje K és

$$Res(P, Q) = a. \tag{3}$$

Nyilván ha $(P(x), Q(x))$ megoldása (3)-nek, akkor tetszőleges $b \in \mathbb{Z}$ esetén $(P_1(x), Q_1(x)) = (P(x + b), Q(x + b))$ szintén megoldás. Ebben az esetben

$(P(x), Q(x))$-t és $(P_1(x), Q_1(x))$-t $\mathbb{Z}-$ ekvivalensnek nevezzük.

Győry K. [18] Megmutatta, hogy véges sok olyan $\mathbb{Z}$-ekvivalencia osztálya van (P, Q) polinompároknak melyek teljesítik (3)-t és $deg(P) \geq 2$, $deg(Q) \geq 2$, $deg(P) + deg(Q) \geq 5$ feltételeket, valamint P és Q gyökei egyszeresek. Ugyancsak Győry K. [19] adott explicit felső korlátot P és Q fokára és a megoldások számára.

Meghatározzuk (3) "kis" megoldásait, melyekre P és Q gyökei rögzített M_1 és M_2 számtesteket generálnak. Ez speciális esete a fenti problémának. A problémát visszavezetjük háromváltozós egységegyenletekre, melyre alkalmazzuk módszerünket. Mivel ez a módszer közvetlenül nem alkalmazható, ezért két ponton jelentősen javítjuk, ezek segítségével lehetővé válik numerikus példánkban a számítások kivitelezése.

8 A $x^n = Dy^2 + 1$ diofantikus egyenlet

A negyedik fejezetben az

$$x^n = Dy^2 + 1$$

diofantikus egyenlettel foglalkozunk, ahol n, x, y ismeretlenek, $n \geq 3$ és D rögzített négyzetmentes egész. Adott D-re a tárgyalt egyenletnek véges sok x, y és $n \geq 3$ megoldása van. Az $n = 4$ esetben Ljunggren [30] megmutatta, hogy minden D-re legfeljebb két megoldás van. J.H.E. Cohn [3] az $D \leq 100$ eset összes megoldását megadta, hat (n, D) pár kivételével. Munkánkban megoldjuk az egyenletet a hat kivételes esetben-, így teljessé téve J.H.E.Cohn eredményét. Eredményünket a következő tételben foglaljuk össze:

Tétel 7. *Eltekintve az* $(x, y) = (1, 0)$ *triviális megoldástól, az*

$$x^n = Dy^2 + 1$$

egyenlet megoldásai az

$$\begin{array}{lll} (x, y) = (5, \pm 12), & ha & (n, D) = (3, 31) \\ (x, y) = (2, \pm 1), & ha & (n, D) = (5, 31) \\ (x, y) = (7, \pm 3), & ha & (n, D) = (3, 38) \\ (x, y) = (13, \pm 6), & ha & (n, D) = (3, 61) \\ nincs, & ha & (n, D) = (5, 71) \\ nincs, & ha & (n, D) = (7, 71). \end{array}$$

9 List of papers of the author and citations to these papers

1. I.Járási, *Power integral bases in sextic fields with a cubic subfield* Acta Sci. Math. (Szeged) **20** (2003), 291–303.

    - I.Gaál, Diophantine equations and power integral bases. New computational methods. Birkhäuser Boston, Inc., Boston, MA, 2002. xviii+184 pp.
    - P.Olajos, Power integral bases in families of number fields, PhD Disszertáció, Debreceni Egyetem
    - I.Gaál and P.Olajos, *Recent results on power integral bases of composite fields* Acta Acad. Paedagog. Agriensis Sect. Mat., **30** (2003), 45–54.
    - I.Gaál, Constructive methods for solving diophantine equations, MTA Doktori Értekezés, 2001.
    - W.Narkiewicz, Elementary and analytic theory of algebraic numbers, Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. xii+708 pp. 2004.
    - K.Győry,*Index form equations and their applications*, Proc. of the Institute of Math. of NAN, Belarus, **13** No. 1 (2005), 83–93.

2. I.Járási, *Computing all elements of given index in sextic fields with a cubic subfield* Acta Math. Inform. Univ. Ostraviensis **10** (2002), no. 1, 49–59.

    - W.Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. xii+708 pp.
    - K.Győry,*Index form equations and their applications*, Proc. of the Institute of Math. of NAN, Belarus, **13** No. 1 (2005), 83–93.

3. I.Gaál, I.Járási and F.Luca, *A remark on prime divisors of lengths of sides of Heron triangles*, Experim. Math. **12** (2003) 303–310.

4. E.Herrmann, I.Járási and A.Pethő, *Note on J.H.E. Cohn's paper "The Diophantine equation $x^n = Dy^2 + 1$"* Acta Arithm. **113** (2004) 69–76.

5. I.Járási, *Computing small solutions of unit equations in three variables I: Application to norm form equations* Periodica Mathematica Hungarica submitted.

6. I.Járási, *Computing small solutions of unit equations in three variables II: Applications to resultant form equations* Publ. Math. Debrecen **65** (2004) 399–408.

10 List of conference talks of the author

1. 1999. XXIV. OTDK, Debrecen: On the Carmichael numbers

2. 2001. XXV. OTDK, Pécs: Power integral bases in special sextic fields

3. 2001. september, 15th Czeh and Slovak International Conference of Number Theory, Ostravice: Computing all elements of given index in sextic fields with a cubic subfield

4. 2002. september, Explicit Algebraic Number Theory: NWO-OTKA Workshop, Leiden: Computing small solutions of resultant equations

5. 2003. july, 16th Czeh and Slovak International Conference of Number Theory, Pozsony: Computing the small solutions of unit equations: Norm forms

6. 2003. july, XXIII Journees Arithmetique, Graz: Computing the small solutions of unit equations: Norm forms

7. 2003. august, Worksop on Diophantine approximation, Leiden: Computing the small solutions of unit equations with an application to resultant form equations

8. 2004. october, Explicit algebraic number theory, Paris: Enumerating the solutions of unit equations

9. 2005. september, 17th Czeh and Slovak International Conference of Number Theory, Malenovice: Some results on P-orderings

References

[1] Y.Bilu, I.Gaál and K.Győry, *Index form equations in sextic fields: a hard computation*, Acta Arith., **115** (2004), 85–96.

[2] Y.Bugeaud and K.Győry, *Bounds for the solutions of unit equations*, Acta Arith., **74** (1996), 67–80.

[3] J.H.E.Cohn. *The Diophantine equation* $x^n = Dy^2 + 1$, Acta Arith., **106** (2003), 73–83.

[4] J.-H.Evertse and K.Győry, *Finiteness criteria for decomposable form equations*, Acta Arith., **50** (1988), 357–379.

[5] U.Fincke and M.Pohst, *Improved methods for calculating vectors of short lenght in a lattice, including a complexity analysis*, Math. Comput., **44** (1985), 463–471.

[6] I.Gaál, *Computing elements of given index in totally complex cyclic sextic fields*, J.Symbolic Comput., **20** (1995), 61–69.

[7] I.Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp., **65** (1996), 801–822.

[8] I.Gaál, *An efficient algorithm for the explicit resolution of norm equations*, Publ. Math. Debrecen, **56** (2000), 375–390.

[9] I.Gaál, *On the resolution of resultant type equations*, J.Symbolic Comput., **34** (2002), 137–144.

[10] I.Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston, 2002.

[11] I.Gaál and K.Győry, *On the resolution of index form equations in quintic fields*, Acta Arith., **89** (1999), 379–396.

[12] I.Gaál, I.Járási and F.Luca, *A remark on prime divisors of lengths of sides of Heron triangles*, Experim. Math. **12** (2003), 303–310.

[13] I.Gaál and M.Pohst, *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J.Symbolic Comp., **22** (1996), 425–434.

[14] I.Gaál and M.Pohst, *On the resolution of relative Thue equations*, Math. Comput., **71** (2002), 429–440.

[15] R.K.Guy, Unsolved problems in number theory, Second edition. Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics, I. Springer-Verlag, New York, 1994.

[16] K.Győry, *Sur les polynomes a coefficients entiers et de discriminant donne, III*, Publ. Math.(Debrecen), **23** (1976), 141–165.

[17] K.Győry, Résultats effectifs sur la représentation des entiers par des formes décomposable, Kingston, Canada, 1980.

[18] K.Győry, *On arithemtic graphs associated with integral domains*, in: A tribute to Paul Erdős, Cambridge University Press, 1990. pp. 207–222.

[19] K.Győry, *On the number of pairs of polynomials with given resultant or given semi-resultant*, Acta Sci. Math., **57** (1993), 169–180.

[20] K.Győry, *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen, **52** (1998), 1–31.

[21] K.Győry, *Discriminant form and index form equations*, In: Algebraic number theory and diophantine analysis, Proc. Conf. Graz 1998, Walter de Gruyter 2000, 191–214.

[22] K.Győry and Y.Kunrui, *Bounds for the solutions of S-unit equations and decomposable form equations*, to appear.

[23] H.Harborth and A.Kemnitz, *Fibonacci triangles,* in: Applications of Fibonacci numbers, Vol. 3 (Pisa, 1988), Kluwer Acad. Publ., Dordrecht, 1990. 129–132.

[24] H.Harborth, A.Kemnitz and N.Robbins, *Non-existence of Fibonacci triangles*, in: Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing (Winnipeg, MB, 1995). Congr. Numer. **114** (1996), 29–31.

[25] E.Herrmann, I.Járási and A.Pethő, *Note on J.H.E. Cohn's paper "The Diophantine equation* $x^n = Dy^2 + 1$*"* Acta Arithm., **113** (2004), 69–76.

[26] I.Járási, *Computing all elements of given index in sextic fields with a cubic subfield*, Acta Math. Inform. Univ. Ostraviensis, **10** (2002), 49–59.

[27] I.Járási, *Power integral bases in sextic fields with a cubic subfield*, Acta Sci. Math. (Szeged), **20** (2003), 291–303.

[28] I.Járási, *Computing small solutions of unit equations in three variables II: Resultant form equations*, Publ. Math. Debrecen, **65** (2004), 399-408.

[29] I.Járási, *Computing small solutions of unit equations in three variables I: Application to norm form equations*, submitted.

[30] W.Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer usw.* Oslo Vid. Akad. Skrifter, **12** (1936)

[31] F.Luca, *Perfect cuboids and perfect square triangles*, Math. Mag., **73** (2000), 400-401.

[32] K.Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve*, Dissertation, Technical University, Berlin, (1997).

[33] K.Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J.Number Theory, **82** (2000), 188–224.