



Constructive methods for Diophantine Equations

doktori (Ph.D.) értekezés

JÁRÁSI ISTVÁN

Debreceni Egyetem

Debrecen, 2005

Ezen értekezést a Debreceni Egyetem TTK Matematika és Számítástudományok Doktori Iskola Diofantikus és konstruktív számelmélet programja keretében készítettem 2001–2005 között és ezúton benyújtom a Debreceni Egyetem TTK doktori Ph.D. fokozatának elnyerése céljából.

Debrecen, 2005. december ...

.....
Járási István
jelölt

Tanúsítom, hogy Járási István doktorjelölt 2001–2005 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, 2005. december ...

.....
Dr. Gaál István
témavezető

Köszönetnyilvánítás

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

Édesanyámnak, aki felnevelt, segített és elindított az életben,

Témavezetőmnek, Dr. Gaál Istvánnak, aki nélkül ez a dolgozat nem készülhetett volna el,

Tanáraimnak, Dr. Győry Kálmánnak és Dr. Pethő Attilának, akiktől nagyon sokat tanultam és tanulok,

Doktorandusz társaimnak, kollégáimnak, Barczy Mátyásnak, Dr. Olajos Péternek, Nyul Gábornak, Dr. Rakaczki Csabának, Pink Isvának, Dr. Bérczes Attilának, Dr. Hajdu Lajosnak, Dr. Pintér Ákosnak, Dr. Tengely Szabolcsnak, Dr. Turjányi Sándornak, akikhez bármikor segítségért fordulhattam.

Contents

Introduction	1
1 Index form equations in sextic fields with a cubic subfield	7
1.1 Introduction	7
1.2 Sextic fields with a cubic subfield	8
1.3 Determining the "small" solutions	9
1.3.1 The factorization of the index	9
1.3.2 An algorithm	12
1.3.3 Numerical examples	15
1.3.4 Constructing infinite parametric families of monogene sextic fields with a cubic subfield	16
1.4 Determining all solutions	18
1.4.1 The unit equation	19
1.4.2 Baker's method	22
1.4.3 LLL reduction of Baker's bound	23
1.4.4 Wildanger's method for the enumeration of the solutions of the unit equation	24
1.4.5 Sieving	26
1.4.6 A numerical example	26
2 Results on Heron triangles	29
2.1 Introduction	29
2.2 Proof of Theorem 4	31
2.2.1 The triangle is isosceles	31
2.2.2 The triangle is not isosceles	32
2.3 Proof of Theorem 5	35

2.4	Proof of Theorem 6	38
2.4.1	Isosceles triangles	38
2.4.2	Non-isosceles triangles	38
3	Applications of unit equations in three unknowns	45
3.1	Introduction	45
3.2	Preliminary definitions and results	46
3.2.1	Semi-orbits, enumerable semi-orbits	46
3.2.2	Reduction of enumerable semi-orbits	48
3.3	Unit equations in three variables	49
3.4	The enumeration method	50
3.4.1	Localizing the solutions of unit equations in three variables	51
3.4.2	The enumeration lemma and its application	53
3.5	Application to norm form equation	56
3.5.1	Norm form equations in three unknowns	56
3.5.2	A numerical example	57
3.6	Application to resultant form equations	58
3.7	Improvements of the method	59
3.7.1	Decreasing the number of enumerable sets	59
3.7.2	Enumerable sets of small rank	61
3.8	A numerical example	62
4	On the diophantine equation $x^n = Dy^2 + 1$	65
4.1	Introduction	65
4.2	The cases $n = 3$	67
4.3	The case $n = 5$	68
4.4	The case $n = 7$	71
	Summary	75
	Összefoglaló (Hungarian summary)	81
	Bibliography	85
A	List of papers of the author and citations to these papers	93
B	List of conference talks of the author	95

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 [25]). It is important to notice that the resulting procedures provide efficient tools to solve several other diophantine problems.

In the first chapter we give two algorithms for finding solutions of index form equations corresponding to sextic fields with a cubic subfield. First we give a fast method to determine the solutions having "small" coordinates in an integral basis using the properties of the index form of the field. This method is completely elementary. We also give an algorithm to determine all solutions by reducing the problem to unit equations in two unknowns. As an application of the first method, we give a sufficient condition for infinite parametric families of number fields of this type to have a power integral basis. To illustrate the statement we construct parametric families of fields and describe generators of power integral bases in them.

In the second chapter we consider Heron triangles. We prove that there are only finitely many Heron triangles whose sides a, b, c are coprime integers which are divisible only by primes from a given set $\mathcal{P}$. If $\mathcal{P}$ contains only one prime $\equiv 1 \pmod{4}$ then all these triangles can be effectively determined. Moreover for $\mathcal{P} = \{2, 3, 5, 7, 11\}$ all such triangles are explicitly given.

In the third chapter we consider unit equations in three unknowns. First we give a method to compute the "small" solutions of unit equations in three unknowns. In fact this procedure is an extension of Wildanger's method [85]

which is developed for unit equations in two unknowns. As an application we computed the "small" solutions of a given norm form equation. We also provide an application to resultant form equations, which needs some essential improvements. A numerical example is also presented.

In the fourth chapter we consider the diophantine equation

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

in integers n, x, y with $n \geq 3$, where D is a fixed squarefree integer. J.H.E. Cohn [12] gave all the solutions with $D \leq 100$ up to six pairs of (n, D) . Here we give the solutions of the equations corresponding to these exceptional pairs.

I

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

$$I(\alpha) = \frac{\prod_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|}{\sqrt{|D_K|}} \quad (1)$$

where α_i ($1 \leq i \leq n$) denote the conjugates of α and D_K is the discriminant of the field K .

It is obvious that $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ 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 $\{1, \omega_2, \dots, \omega_n\}$ be an arbitrary integral basis in K . Then the discriminant of the linear form $l(x) = x_2\omega_2 + \dots + x_n\omega_n$ can be written as

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

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

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

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 [36] 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 [44] and the monograph I.Gaál [25], 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 [25]. 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 [20], [19] and I.Gaál and M.Pohst [30]. 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.

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 [27] 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 [31] (see also [25]). This enumeration method is based on K. Wildanger's ideas, cf. [84], [85]. 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 [5] 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 [54] and [53].

II

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 [35]), and it is not known whether there exist Heron triangles having the property that the lengths of all their sides are Fibonacci numbers (see [49] and [50]). 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 [63]).

Let $P(k)$ denote the largest prime factor of k . We prove that $P(abc) \rightarrow \infty$ when $\max(a, b, c) \rightarrow \infty$ 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 $\mathcal{P}$ contains 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 [28].

III

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 [36],[37],[43],[45]), 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 [25] for an overview). These equations usually have only "small" solutions.

J.-H.Evertse and K.Győry (see e.g. [16]) 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 [85] and I.Gaál and M.Pohst [31] (see also [25]) and uses the method of U.Fincke and M.Pohst [18] 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 [23] 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

$$\text{Res}(P, Q) = a. \tag{2}$$

It is easy to see that if $(P(x), Q(x))$ is a solution to (2) then for any $b \in \mathbb{Z}$ $(P_1(x), Q_1(x)) = (P(x+b), Q(x+b))$ is also a solution to (2). 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 [38] that there exist only finitely many $\mathbb{Z}$ -equivalence classes of pairs of polynomials (P, Q) satisfying (2) 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 [40] 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 (2) 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 [56] 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 [24]. The results of this chapter are contained in [55] and [56].

IV

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

$$x^n = Dy^2 + 1. \tag{3}$$

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 [60] proved that for any D (3) has at most two positive solutions.

Using elementary and algebraic number theoretical tools J.H.E. Cohn [12] proved necessary conditions for the unsolvability of (3). Moreover, he solved (3) 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 has been published in [52].

Chapter 1

Index form equations in sextic fields with a cubic subfield

1.1 Introduction

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

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

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

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

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

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

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

the equality

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

holds. So the problem of determining power all integral basis is equivalent to determine the elements of index 1 or to solve the index form equation

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

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

$$I(\alpha) = \frac{\prod_{1 \leq i < j \leq n} |\alpha^{(i)} - \alpha^{(j)}|}{\sqrt{|D_K|}} \quad (1.1)$$

where $\alpha^{(i)}$ ($1 \leq i \leq n$) denote the conjugates of α .

For an arbitrary $z \in \mathbb{Z}$ the indices of $\pm\alpha + z$ are the same. These numbers are called equivalent.

1.2 Sextic fields with a cubic subfield

Let K be a sextic field having a cubic subfield M . Let us denote by $\mathbb{Z}_K$ and $\mathbb{Z}_M$ the rings of integers of K and M , respectively. We will consider in detail the most interesting case when M is totally real. The case of complex cubic subfields is much easier since in that case the unit rank of M is only 1.

Assume $M = \mathbb{Q}(\varrho)$ and $K = M(\vartheta)$ with algebraic integers ϱ, ϑ . For simplicity let us choose ϱ and ϑ so that $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K , so that an arbitrary $\alpha \in \mathbb{Z}_K$ can be written as

$$\alpha = x_0 + x_1\varrho + x_2\varrho^2 + y_0\vartheta + y_1\vartheta\varrho + y_2\vartheta\varrho^2, \quad (1.2)$$

where $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$. Note that if ϱ and ϑ with this property do not exist (this happens very seldom), then in the representation (1.2) we have to use a common denominator g . In such cases the same algorithm can be used, the only difference is that instead of ± 1 some constants depending on g appear on the right hand sides of our equations.

Let

$$X = x_0 + x_1\varrho + x_2\varrho^2, \quad Y = y_0 + y_1\varrho + y_2\varrho^2,$$

then X and Y are integers in M and

$$\alpha = X + \vartheta Y. \quad (1.3)$$

1.3 Determining the "small" solutions

1.3.1 The factorization of the index

We 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 $\varrho^{(i)}$. For any $\gamma \in K$ we denote by $\gamma^{(i1)}, \gamma^{(i2)}$ the conjugates of γ corresponding to $\vartheta^{(i1)}, \vartheta^{(i2)}$, respectively.

Using the integral basis $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ for the discriminant of the field K we get

$$\sqrt{|D_K|} = (\varrho^{(1)} - \varrho^{(2)})^2(\varrho^{(2)} - \varrho^{(3)})^2(\varrho^{(3)} - \varrho^{(1)})^2 \cdot (\vartheta^{(11)} - \vartheta^{(12)})(\vartheta^{(21)} - \vartheta^{(22)})(\vartheta^{(31)} - \vartheta^{(32)}).$$

Let

$$\beta_k = \frac{(\alpha^{(i1)} - \alpha^{(j1)})(\alpha^{(i2)} - \alpha^{(j2)})(\alpha^{(i2)} - \alpha^{(j1)})(\alpha^{(i1)} - \alpha^{(j2)})}{(\varrho^{(i)} - \varrho^{(j)})^2}, \quad (1.4)$$

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

Then the following theorem holds:

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 $k = 1, 2, 3$.*

Proof. First we show that β_k is an algebraic integer. Let $M^{(i)} = \mathbb{Q}(\varrho^{(i)})$. Since $\vartheta^{(i1)}, \vartheta^{(i2)}$ are the roots of a quadratic polynomial having algebraic coefficients in $\mathbb{Z}_{M^{(i)}}$ we have

$$\vartheta^{(i1)} = \frac{\nu^{(i)} + \sqrt{\mu^{(i)}}}{2}, \quad \vartheta^{(i2)} = \frac{\nu^{(i)} - \sqrt{\mu^{(i)}}}{2},$$

and similarly

$$\vartheta^{(j1)} = \frac{\nu^{(j)} + \sqrt{\mu^{(j)}}}{2}, \quad \vartheta^{(j2)} = \frac{\nu^{(j)} - \sqrt{\mu^{(j)}}}{2},$$

where $\nu, \mu \in \mathbb{Z}_M$ are algebraic integers, $\nu^{(i)}, \nu^{(j)}, \mu^{(i)}, \mu^{(j)}$ denote their conjugates. Since the relative norms are algebraic integers we have

$$\vartheta^{(i1)} \cdot \vartheta^{(i2)} = \frac{(\nu^{(i)})^2 - \mu^{(i)}}{4} \in \mathbb{Z}_{M^{(i)}}, \quad \vartheta^{(j1)} \cdot \vartheta^{(j2)} = \frac{(\nu^{(j)})^2 - \mu^{(j)}}{4} \in \mathbb{Z}_{M^{(j)}}.$$

Using (1.3) this implies

$$\begin{aligned}
& (\alpha^{(i1)} - \alpha^{(j1)})(\alpha^{(i1)} - \alpha^{(j2)}) = \\
& \left(X_i - X_j + \frac{\nu^{(i)} + \sqrt{\mu^{(i)}}}{2} Y_i - \frac{\nu^{(j)} + \sqrt{\mu^{(j)}}}{2} Y_j \right) \cdot \\
& \cdot \left(X_i - X_j + \frac{\nu^{(i)} + \sqrt{\mu^{(i)}}}{2} Y_i - \frac{\nu^{(j)} - \sqrt{\mu^{(j)}}}{2} Y_j \right).
\end{aligned}$$

It is obvious that the difference of the i -th and the j -th conjugates of integers in $\mathbb{Z}_M$ is divisible by $(\varrho^{(i)} - \varrho^{(j)})$ because of their representation in the basis $\{1, \varrho, \varrho^2\}$. So in both of the two factors $X_i - X_j$ is divisible by $(\varrho^{(i)} - \varrho^{(j)})$. It can be similarly shown that the same holds for the remaining factor, that is

$$\begin{aligned}
& \left(\frac{\nu^{(i)} + \sqrt{\mu^{(i)}}}{2} Y_i - \frac{\nu^{(j)} + \sqrt{\mu^{(j)}}}{2} Y_j \right) \left(\frac{\nu^{(i)} + \sqrt{\mu^{(i)}}}{2} Y_i - \frac{\nu^{(j)} - \sqrt{\mu^{(j)}}}{2} Y_j \right) = \\
& - \left(\frac{(\nu^{(i)})^2 - \mu^{(i)}}{4} Y_i^2 - \frac{(\nu^{(j)})^2 - \mu^{(j)}}{4} Y_j^2 \right) + \frac{\nu^{(i)} + \sqrt{\mu^{(i)}}}{2} Y_i (\nu^{(i)} Y_i - \nu^{(j)} Y_j)
\end{aligned}$$

is divisible by $(\varrho^{(i)} - \varrho^{(j)})$. Similarly, $(\alpha^{(i2)} - \alpha^{(j1)})(\alpha^{(i2)} - \alpha^{(j2)})$ is also divisible by $(\varrho^{(i)} - \varrho^{(j)})$.

Now we turn to prove that $\beta_k \in M_k = \mathbb{Q}(\varrho_k)$. Let Γ be the Galois group of the field $\overline{M} = \mathbb{Q}(\varrho^{(1)}, \varrho^{(2)}, \varrho^{(3)})$, and denote by Γ_0 its subgroup containing the automorphisms which leave M_k elementwise fixed. Put $\overline{K} = \mathbb{Q}(\vartheta^{(11)}, \vartheta^{(12)}, \vartheta^{(21)}, \vartheta^{(22)}, \vartheta^{(31)}, \vartheta^{(32)})$.

Let $\sigma \in \Gamma$ with $\sigma(\varrho^{(i)}) = \varrho_{j_i}$, $(i = 1, 2, 3)$, where (j_1, j_2, j_3) is a permutation of $(1, 2, 3)$. Let us extend this to an automorphism $\overline{\sigma}$ of $\overline{K}$ such that

$$\overline{\sigma}(\vartheta^{(i1)}) = \vartheta^{(j_i1)}, \overline{\sigma}(\vartheta^{(i2)}) = \vartheta^{(j_i2)}, (i = 1, 2, 3).$$

Denote by π_i be the automorphism of $\overline{K}$ for which

$$\pi_i(\vartheta^{(i1)}) = \vartheta^{(i2)}, \pi_i(\vartheta^{(i2)}) = \vartheta^{(i1)},$$

and

$$\pi_i(\vartheta^{(j1)}) = \vartheta^{(j1)}, \pi_i(\vartheta^{(j2)}) = \vartheta^{(j2)}$$

$$\pi_i(\vartheta^{(k1)}) = \vartheta^{(k1)}, \pi_i(\vartheta^{(k2)}) = \vartheta^{(k2)}$$

for $i = 1, 2, 3$, $\{j, k\} = \{1, 2, 3\} \setminus \{i\}$. Then any element of the Galois group of $\overline{K}$ can be written in the form

$$\overline{\sigma} \cdot \pi_1^{a_1} \cdot \pi_2^{a_2} \cdot \pi_3^{a_3}$$

where $\overline{\sigma}$ denotes the extension of $\sigma \in \Gamma$ with the above property, and a_1, a_2, a_3 are from $\{0, 1\}$.

It is easy to see, that the automorphisms of $\overline{K}$ which leave M_k elementwise fixed are of the form

$$\overline{\sigma}_0 \cdot \pi_1^{a_1} \cdot \pi_2^{a_2} \cdot \pi_3^{a_3}$$

where $\overline{\sigma}_0$ denotes the extension of $\sigma_0 \in \Gamma_0$ to $\overline{K}$. (These elements form a subgroup in the Galois group of $\overline{K}$). It is easily seen that $\overline{\sigma}_0, \pi_1, \pi_2, \pi_3$ leave β_k fixed, so using Galois theory $\beta_k \in M_k$ holds. $\square$

The following theorem describes the factors of the index of $\alpha \in \mathbb{Z}_K$. We note that our algorithm for finding "small" generators of power integral basis is based on Theorems 1, 2.

Theorem 2. *If $\alpha \in \mathbb{Z}_K$ represented in the form (1.2) generates a power integral basis, then*

$$N_{M/\mathbb{Q}}(y_0 + y_1\varrho + y_2\varrho^2) = \pm 1, \quad (1.5)$$

and

$$N_{M/\mathbb{Q}}(\beta) = \pm 1. \quad (1.6)$$

Proof. Recall that for the index of α we have (1.1). It is obvious that

$$\frac{\alpha^{(i1)} - \alpha^{(i2)}}{\vartheta^{(i1)} - \vartheta^{(i2)}} = y_0 + y_1\varrho^{(i)} + y_2(\varrho^{(i)})^2$$

is an algebraic integer in $M^{(i)} = \mathbb{Q}(\varrho^{(i)})$ for $i = 1, 2, 3$, these are conjugated to each other and their product is

$$N_{M/\mathbb{Q}}(y_0 + y_1\varrho + y_2\varrho^2).$$

The quotient of the remaining differences of conjugates of α and the remaining factor of $\sqrt{|D_K|}$ is

$$\beta_1\beta_2\beta_3 = N_{M/\mathbb{Q}}(\beta).$$

Since both of them are integers in $\mathbb{Z}$ and their product is ± 1 we obtain (1.5) and (1.6). $\square$

1.3.2 An algorithm

Our purpose is to determine elements of index 1 of $\mathbb{Z}_K$ for which

$$\max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < C. \quad (1.7)$$

In our examples we have $C = 10^5$. We consider only the case when M is totally real. Let $\{\varepsilon_1, \varepsilon_2\}$ be a set of fundamental units of M , and denote by $\varepsilon_1^{(i)}, \varepsilon_2^{(i)}$ ($i = 1, 2, 3$) their conjugates.

Step I.

By (1.5) we have

$$Y_i = \pm(\varepsilon_1^{(i)})^{b_1}(\varepsilon_2^{(i)})^{b_2}, \quad (i = 1, 2, 3) \quad (1.8)$$

with $b_1, b_2 \in \mathbb{Z}$. From this we conclude

$$b_1 \log |\varepsilon_1^{(i)}| + b_2 \log |\varepsilon_2^{(i)}| = \log |Y_i|. \quad (i = 1, 2, 3) \quad (1.9)$$

Using the notation (with i, j as in (1.4))

$$C_i = \max(\log(C \cdot r_j) + \log(C \cdot r_k), \log(C \cdot r_i))$$

$$C_j = \max(\log(C \cdot r_i) + \log(C \cdot r_k), \log(C \cdot r_j))$$

by (1.9) we have

$$\begin{aligned} |b_1| &\leq |f_{11}| \cdot C_i + |f_{12}| \cdot C_j \\ |b_2| &\leq |f_{21}| \cdot C_i + |f_{22}| \cdot C_j \end{aligned}$$

where f_{ij} denote the entries of the matrix

$$\begin{pmatrix} \log |\varepsilon_1^{(i)}| & \log |\varepsilon_2^{(i)}| \\ \log |\varepsilon_1^{(j)}| & \log |\varepsilon_2^{(j)}| \end{pmatrix}^{-1}.$$

The above upper bounds are valid for $(i, j) = (1, 2), (2, 3), (3, 1)$. Denote by C_{b_1} and C_{b_2} the minimum of the estimates for $|b_1|$ and $|b_2|$, respectively.

The following steps must be performed for all possible values of b_1 and b_2 with

$$-C_{b_1} \leq b_1 \leq C_{b_1}, \quad -C_{b_2} \leq b_2 \leq C_{b_2}.$$

Step II.

By (1.6) we have

$$\beta_k = \pm(\varepsilon_1^{(k)})^{d_1}(\varepsilon_2^{(k)})^{d_2} \quad (k = 1, 2, 3) \quad (1.10)$$

with $d_1, d_2 \in \mathbb{Z}$. From this we conclude

$$d_1 \log |\varepsilon_1^{(k)}| + d_2 \log |\varepsilon_2^{(k)}| = \log |\beta_k| \quad (k = 1, 2, 3).$$

It is easy to see that

$$\begin{aligned} \alpha^{(i1)} - \alpha^{(j1)} &= X_i - X_j + \vartheta^{(i1)}Y_i - \vartheta^{(j1)}Y_j, \\ \alpha^{(i2)} - \alpha^{(j2)} &= X_i - X_j + \vartheta^{(i2)}Y_i - \vartheta^{(j2)}Y_j, \\ \alpha^{(i2)} - \alpha^{(j1)} &= X_i - X_j + \vartheta^{(i2)}Y_i - \vartheta^{(j1)}Y_j, \\ \alpha^{(i1)} - \alpha^{(j2)} &= X_i - X_j + \vartheta^{(i1)}Y_i - \vartheta^{(j2)}Y_j. \end{aligned} \quad (1.11)$$

By (1.8) the values of b_1 and b_2 determine Y_i and Y_j . Using (1.4), (1.10), (1.11) and the estimate

$$\begin{aligned} |X_i - X_j| &= |x_1(\varrho^{(i)} - \varrho^{(j)}) + x_2((\varrho^{(i)})^2 - (\varrho^{(j)})^2)| \leq \\ &\leq C \cdot (|\varrho^{(i)} - \varrho^{(j)}| + |(\varrho^{(i)})^2 - (\varrho^{(j)})^2|) \end{aligned}$$

one can derive upper bounds for $|d_1|$ and $|d_2|$ for $(i, j) = (1, 2), (2, 3), (3, 1)$ similarly as in Step I. Denote by C_{d_1} and C_{d_2} the minimum of these bounds for $|d_1|$ and $|d_2|$, respectively.

The following steps must be performed for all possible values of d_1 and d_2 with

$$-C_{d_1} \leq d_1 \leq C_{d_1}, \quad -C_{d_2} \leq d_2 \leq C_{d_2}.$$

Step III.

Using the above type of indices i, j, k let

$$\begin{aligned} A_k &= X_i - X_j + \frac{(\vartheta^{(i1)} + \vartheta^{(i2)})Y_i - (\vartheta^{(j1)} + \vartheta^{(j2)})Y_j}{2}, \\ B_k &= Y_i(\vartheta^{(i1)} - \vartheta^{(i2)}), \\ C_k &= Y_j(\vartheta^{(j1)} - \vartheta^{(j2)}). \end{aligned} \quad (1.12)$$

Using this notation by (1.11) we have

$$\begin{aligned}\alpha^{(i1)} - \alpha^{(j1)} &= A_k - \frac{B_k + C_k}{2}, \\ \alpha^{(i2)} - \alpha^{(j2)} &= A_k - \frac{B_k - C_k}{2}, \\ \alpha^{(i2)} - \alpha^{(j1)} &= A_k + \frac{B_k - C_k}{2}, \\ \alpha^{(i1)} - \alpha^{(j2)} &= A_k + \frac{B_k + C_k}{2},\end{aligned}$$

so (1.10) is equivalent to

$$\begin{aligned}\left(A_k + \frac{B_k + C_k}{2}\right) \left(A_k - \frac{B_k + C_k}{2}\right) \left(A_k + \frac{B_k - C_k}{2}\right) \left(A_k - \frac{B_k - C_k}{2}\right) \\ = \pm (\varepsilon_1^{(k)})^{d_1} (\varepsilon_2^{(k)})^{d_2} \left(\varrho^{(i)} - \varrho^{(j)}\right)^2,\end{aligned}$$

that is

$$\begin{aligned}\left(A_k^2 - \left(\frac{B_k + C_k}{2}\right)^2\right) \left(A_k^2 - \left(\frac{B_k - C_k}{2}\right)^2\right) = \\ = \pm (\varepsilon_1^{(k)})^{d_1} (\varepsilon_2^{(k)})^{d_2} \left(\varrho^{(i)} - \varrho^{(j)}\right)^2.\end{aligned}$$

From this it is easy to see, that the above quartic equation in A_k can be reduced to quadratic equations in A_k . Note that this radically reduces the computational time, because it is much easier to solve a quadratic equation using only a square root than to solve a quartic equation using iteration methods.

Having solved the above equations in A_k , we can calculate $X_i - X_j$ by equation (1.12). For $k = 1, 2$ we calculate $X_2 - X_3, X_3 - X_1$ and then we can determine x_1 and x_2 from the system of equations

$$\begin{aligned}X_2 - X_3 &= x_1(\varrho^{(2)} - \varrho^{(3)}) + x_2((\varrho^{(2)})^2 - (\varrho^{(3)})^2), \\ X_3 - X_1 &= x_1(\varrho^{(3)} - \varrho^{(1)}) + x_2((\varrho^{(3)})^2 - (\varrho^{(1)})^2).\end{aligned}$$

If x_1 and x_2 are integers then we found a possible solution of our index form equation.

The values of the y_i -s for $i = 1, 2, 3$ can be determined similarly by solving the system of linear equations (cf. (1.8))

$$y_0 + y_1 \varrho^{(i)} + y_2 (\varrho^{(i)})^2 = \pm (\varepsilon_1^{(i)})^{b_1} (\varepsilon_2^{(i)})^{b_2} \quad (i = 1, 2, 3).$$

Obviously, this system of equations has integer solutions in y_0, y_1, y_2 , because by Theorem 2 the Y_i is a unit of $M^{(i)}$ and by our assumption $\{1, \varrho^{(i)}, (\varrho^{(i)})^2\}$ is an integral basis in $M^{(i)}$ ($i = 1, 2, 3$).

Note that one has to check all candidates of solutions $(x_1, x_2, y_0, y_1, y_2)$, whether α in (1.3) indeed has index 1.

The case of complex cubic subfields can be considered similarly. Since these fields have unit rank 1 in this case the computation is much easier.

The algorithms were implemented in Maple V and executed on a PII 350 MHz IBM PC compatible machine.

1.3.3 Numerical examples

Totally real cubic subfield M :

Example 1:

Let $g(x) = x^3 - 5x - 1$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = 11 \cdot 43$, a system of fundamental units is $\varepsilon_1 = \varrho, \varepsilon_2 = 2 + \varrho$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - 10x - \varrho$. Then its defining polynomial over $\mathbb{Q}$ is $f_0(x) = x^6 - 30x^5 + 300x^4 - 1000x^3 - 5x^2 + 50x - 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^6 \cdot 11^3 \cdot 43^2 \cdot 1409$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_{b_1} = 19$, $C_{b_2} = 14$, and $C_{d_1} \leq 205$, $C_{d_2} \leq 158$. The computations were performed with 100 digits of accuracy, the running time was 18 hours. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (0, -10, -5, 0, 1), (0, 0, -5, 0, 1), (0, 0, 1, 0, 0).$$

Example 2:

Let $g(x) = x^3 - 6x + 1$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = 3^3 \cdot 31$, a system of fundamental units is $\varepsilon_1 = \varrho, \varepsilon_2 = 3 - 6\varrho + 2\varrho^2$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - 6x - \varrho$. Then its defining polynomial over $\mathbb{Q}$ is $f_0(x) = x^6 - 18x^5 + 108x^4 - 216x^3 - 6x^2 + 36x + 1$, the discriminant of the field

$K = \mathbb{Q}(\vartheta)$ is $D_K = 2^7 \cdot 3^6 \cdot 31^2 \cdot 337$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_{b_1} = 16$, $C_{b_2} = 6$, and $C_{d_1} \leq 195$, $C_{d_2} \leq 142$. The computations were performed with 80 digits of accuracy, the running time was 16 hours. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (0, 6, 6, 0, -1), (0, 0, 6, 0, -1), (0, 0, 1, 0, 0).$$

Complex cubic subfield M :

Example 3:

Let $g(x) = x^3 + x^2 - 3x - 5$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = -2^2 \cdot 67$, a fundamental unit is $\varepsilon = -2 + \varrho$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - \varrho x + 1$. Then its defining polynomial over $\mathbb{Q}$ is $f_0(x) = x^6 + x^5 - 3x^3 + x + 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^4 \cdot 3 \cdot 67^2$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_b = 10$, and $C_d \leq 78$. The computations were performed with 100 digits of accuracy, the running time was 50 minutes. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (-3, -1, 3, 3, 1), (-1, 0, 1, 0, 0).$$

Example 4:

Let $g(x) = x^3 - x^2 + 4x - 2$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = -2^2 \cdot 53$, a fundamental unit is $\varepsilon = -1 + 2\varrho$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - \varrho x - 1$. Then its defining polynomial over $\mathbb{Q}$ is $f_0(x) = x^6 - x^5 + x^4 - x^2 - x - 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^6 \cdot 53^2$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_b = 9$, and $C_d \leq 71$. The computations were performed with 100 digits of accuracy, the running time was 40 minutes. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (0, 0, 1, 0, 0), (-1, 0, 1, 0, 0).$$

1.3.4 Constructing infinite parametric families of monogene sextic fields with a cubic subfield

In this section we give a sufficient condition for the existence of 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*

$$b_1^2 - c_0 c_1 b_1 + b_0 c_1^2 = \pm 1$$

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

$$\vartheta^{(i1)} + \vartheta^{(i2)} = \gamma^{(i)} \quad (1.13)$$

and

$$\vartheta^{(i1)} \vartheta^{(i2)} = \delta^{(i)} \quad \text{for } i = 1, 2, 3 \quad (1.14)$$

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.

Proof. By Theorem 2 the element $\alpha = \vartheta$ has index 1 if the corresponding β is a unit in $\mathbb{Q}(\varrho)$. Using the notation of Theorem 3 the element β_k can be written as

$$\beta_k = \frac{(\delta_i - \delta_j)^2 + (\gamma_i - \gamma_j)(\delta_j \gamma_i - \delta_i \gamma_j)}{(\varrho^{(i)} - \varrho^{(j)})^2}.$$

Substituting γ and δ from (1.13), (1.14) we obtain

$$\beta_k = b_1^2 - c_0 c_1 b_1 + b_0 c_1^2 = \pm 1$$

and this completes the proof. $\square$

Note that making more assumptions on $\mathbb{Q}(\varrho)$ one can prove similar results using the structure of its group of units.

Remark:

It is easy to see that the equation

$$b_1^2 - c_0 c_1 b_1 + b_0 c_1^2 = \pm 1 \quad (1.15)$$

has infinitely many solutions in $\mathbb{Z}$. For example let $c_0 = 2n$ ($n \in \mathbb{Z}$). Then one can see that $b_0 \leq n^2 + 1$ is necessary, and the solutions of (1.15) are obtained in the following way:

if the signs of c_1 and b_1 are the same, then

$$(c_0, c_1) = (2n, \pm 1), (b_0, b_1) = (n^2 + 1, \pm n),$$

$$(c_0, c_1) = (2n, \pm 1), (b_0, b_1) = (n^2 - 1, \pm n);$$

if $c_1 \in \mathbb{Z}$ arbitrary, then

$$(c_0, c_1) = (2n, c_1), (b_0, b_1) = (n^2, nc_1 \pm 1);$$

and for an arbitrary $b_0 = n^2 - k$, $1 < k \in \mathbb{N}$ one has to consider the infinitely many solutions of the Pellian equation

$$(nc_1 - b_1)^2 - kc_1^2 = \pm 1.$$

Of course in the construction one has to check whether the relative quadratic defining polynomial of ϑ is irreducible over $\mathbb{Q}(\varrho)$.

Examples:

Example 1: Let $x^3 - (4k^2 + 4k)x^2 - (4k^2 + 4k + 1)x - (4k^2 + 4k)$, $1 \leq k$ be the defining polynomial of ϱ . It is irreducible for $k \in \mathbb{Z}$, $k \neq -1, 0$. Let the coefficients of the quadratic relative defining polynomial of ϑ over $M = \mathbb{Q}(\varrho)$ be $\vartheta^{(i1)} + \vartheta^{(i2)} = -2n + \varrho$, $\vartheta^{(i1)}\vartheta^{(i2)} = n^2 + 1 - n\varrho$. Then one can see that the quadratic relative defining polynomial of ϑ over M is irreducible for $n \geq 1$ so by the theorem ϑ generates a power integral basis in the order $\mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$.

Example 2: Let $x^3 - nx^2 - (n + 1)x - 1$ be the defining polynomial of ϱ . Let the coefficients of the quadratic relative defining polynomial of ϑ over $M = \mathbb{Q}(\varrho)$ be $\vartheta^{(i1)} + \vartheta^{(i2)} = -2k + \varrho$, $\vartheta^{(i1)}\vartheta^{(i2)} = k^2 + 1 - k\varrho$. So the quadratic relative defining polynomial of ϑ over M is irreducible for arbitrary $k \in \mathbb{Z}$ so by the theorem ϑ generates a power integral basis in the order $\mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$.

Example 3:

Let $x^3 - (n - 1)x^2 - (n + 2)x - 1$ be the defining polynomial of ϱ . Let the coefficients of the quadratic relative defining polynomial of ϑ over $M = \mathbb{Q}(\varrho)$ be $\vartheta^{(i1)} + \vartheta^{(i2)} = -2k + \varrho$, $\vartheta^{(i1)}\vartheta^{(i2)} = k^2 + 1 - k\varrho$. So the quadratic relative defining polynomial of ϑ over M is irreducible for arbitrary $k \in \mathbb{Z}$ so by the theorem ϑ generates a power integral basis in the order $\mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$.

1.4 Determining all solutions

In this section we give an algorithm to compute all the solutions of the index form equation. In this case the index form equation is much more complicated

than in the previously considered sextic fields. In this section we 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. By an idea of I.Gaál and K.Győry [27] we can show that the rank of the unit groups involved is at most 11. These unit equations are solved by using the reduction method and enumeration method described by Gaál and Pohst [31]. This enumeration method is based on K. Wildanger's ideas, cf. [84], [85]. Below we consider in detail the most difficult case when the sextic field is totally real and has the largest possible Galois group $S_4 \times C_2$. Recently Y.Bilu, I.Gaál and K.Győry [5] gave an algorithm for solving index form equations in any sextic field but our methods are very much faster than that method.

1.4.1 The unit equation

Let K be a totally real sextic field with a cubic subfield M and with Galois group $S_4 \times C_2$. Note that this is the most difficult case, since any sextic number field with cubic subfield has Galois group having at most $48 = \#(S_4 \times C_2)$ elements.

In this section our purpose is to determine all solutions of the equation

$$I(\alpha) = g \quad (\alpha \in \mathbb{Z}_K) \quad (1.16)$$

for a fixed $g \in \mathbb{Z}$. For

$$1 \leq i, j \leq 3, 1 \leq p, q \leq 2, (i, p) \neq (j, q)$$

consider the linear forms

$$\begin{aligned} l^{(ip,jq)}(x_1, x_2, y_0, y_1, y_2) &= \\ &= (\varrho^{(i)} - \varrho^{(j)})x_1 + ((\varrho^{(i)})^2 - (\varrho^{(j)})^2)x_2 + \\ &+ (\vartheta^{(ip)} - \vartheta^{(jq)})y_0 + (\varrho^{(i)}\vartheta^{(ip)} - \varrho^{(j)}\vartheta^{(jq)})y_1 + ((\varrho^{(i)})^2\vartheta^{(ip)} - (\varrho^{(j)})^2\vartheta^{(jq)})y_2. \end{aligned}$$

Using (1.1) and this notation, (1.16) can be written as

$$\prod l^{(ip,jq)}(x_1, x_2, y_0, y_1, y_2) = \pm g \sqrt{|D_K|}, \quad (1.17)$$

where the product extends to the tuples (ip, jq) where $(i, p) \prec (j, q)$ in the lexicographical order. When we reduce an index form equation to unit equations,

we use the above defined linear forms. In this case we assume a cubic subfield, so we can have several types of unit equations depending on the choice of the linear forms. For $\{i, j, k\} = \{1, 2, 3\}$ and $1 \leq p, q, r \leq 2$ Siegel's-identity gets the form

$$l^{(ip,jq)} + l^{(jq,kr)} + l^{(kr,ip)} = 0 \quad (1.18)$$

in the variables x_1, x_2, y_0, y_1, y_2 .

Since the Galois group of the cubic subfield M is not cyclic (this is satisfied in our case, otherwise the Galois group of K has at most 24 elements), there is an automorphism of the Galois group of M interchanging $\varrho^{(i)}$ and $\varrho^{(j)}$ ($i \neq j$). In view of the arguments of the proof of Theorem 1 of [54], this can be extended to an automorphism of the Galois group of K , interchanging $\vartheta^{(ip)}$ and $\vartheta^{(jq)}$. This isomorphism leaves $L^{(ip,jq)} = \mathbb{Q}(\vartheta^{(ip)} + \vartheta^{(jq)}, \vartheta^{(ip)}\vartheta^{(jq)})$ fixed, hence it is a proper subfield of $K^{(ip)}K^{(jq)}$ which is also a proper subfield of the normal closure of K of degree $\#(S_4 \times C_2) = 48$. Hence the degree of $L^{(ip,jq)}$ cannot exceed 12, so its unit rank is ≤ 11 . (Note that in the totally real case under consideration this maximum is reached.) This idea was first used by Gaál and Györy [27].

Let $\alpha = x_0 + x_1\varrho + x_2\varrho^2 + y_0\vartheta + y_1\varrho\vartheta + y_2\varrho^2\vartheta$ be a solution of (1.16), and

$$\delta^{(ip,jq)} = \frac{\alpha^{(ip)} - \alpha^{(jq)}}{\vartheta^{(ip)} - \vartheta^{(jq)}}.$$

It is easy to see that there is an integer $d \in \mathbb{Z}$ such that arbitrary $\alpha \in \mathbb{Z}_K$ can be represented in the form

$$\alpha = \frac{z_0 + z_1\vartheta + z_2\vartheta^2 + z_3\vartheta^3 + z_4\vartheta^4 + z_5\vartheta^5}{d}$$

where $z_i \in \mathbb{Z}$ for $i = 0, \dots, 5$. (If $I(\vartheta) = 1$ then $d = 1$). Hence $d\delta^{(ip,jq)}$ will be an integer in $L^{(ip,jq)}$.

Using this notations (1.17) can be written as

$$\prod d\delta^{(ip,jq)} = \frac{\pm g d^{15}}{I(\vartheta)}, \quad (1.19)$$

where the product is taken for the same tuples (ip, jq) as (1.17). Again using the arguments of the proof of Theorem 1 of [54] it is easy to see that there exists an automorphism of the Galois group of K mapping $\vartheta^{(ip)}$ to $\vartheta^{(kr)}$ and simultaneously $\vartheta^{(jq)}$ to $\vartheta^{(ls)}$, if $1 \leq k, l \leq 3, k \neq l, 1 \leq r, s \leq 2$. (For this

observe that k or l is equal to i or j and recall that the Galois group of M is not cyclic.) This automorphism maps $\delta^{(ip,jq)}$ to $\delta^{(kr,ls)}$. Thus equation (1.19) is a norm equation in $L^{(ip,jq)}$, so there exists an integer $\gamma^{(ip,jq)}$ of norm $\frac{\pm q d^{15}}{I(\vartheta)}$ and a unit $\eta^{(ip,jq)} \in L^{(ip,jq)}$ such that

$$d\delta^{(ip,jq)} = \eta^{(ip,jq)} \gamma^{(ip,jq)}.$$

Note that the following computations must be performed for a complete set of non-associate integral elements γ of $L^{(ip,jq)}$ of norm $\frac{\pm q d^{15}}{I(\vartheta)}$, which can be determined e.g. by KASH [14]. Let

$$\beta^{(ip,jq,kr)} = \frac{\gamma^{(ip,jq)}(\vartheta^{(ip)} - \vartheta^{(jq)})}{\gamma^{(ip,kr)}(\vartheta^{(ip)} - \vartheta^{(kr)})}.$$

Using this and (1.18) we have

$$\beta^{(ip,jq,kr)} \frac{\eta^{(ip,jq)}}{\eta^{(ip,kr)}} + \beta^{(kr,jq,ip)} \frac{\eta^{(kr,jq)}}{\eta^{(kr,ip)}} = 1. \quad (1.20)$$

Since the η -s are conjugates of to each other, and they lie in a totally real field of degree 12, the number of unknown exponents in this unit equation is 11. (Here note again that in this section we deal with the most difficult case i.e. when the degree of $L^{(ip,jq)}$ is exactly 12 and it is also a totally real field, so its unit rank is 11. In general the unit rank is smaller than 11, since the degree of $L^{(ip,jq)}$ is at most 12)

Denote by $\{\varepsilon_1, \dots, \varepsilon_{11}\}$ a system of fundamental units of $L^{(ip,jq)}$. Let $\{i, j, k\} = \{1, 2, 3\}$ and $1 \leq p, q, r \leq 2$. Then there are rational integers $a_1, \dots, a_{11}$ such that

$$\eta^{(ip,jq)} = \pm \left(\varepsilon_1^{(ip,jq)} \right)^{a_1} \dots \left(\varepsilon_{11}^{(ip,jq)} \right)^{a_{11}}.$$

Introducing

$$\nu_h^{(ip,jq,kr)} = \frac{\varepsilon_h^{(ip,jq)}}{\varepsilon_h^{(ip,kr)}} \quad (h = 1, \dots, 11),$$

$$\mu^{(ip,jq,kr)} = \prod_{h=1}^{11} \left(\nu_h^{(ip,jq,kr)} \right)^{a_h}$$

and

$$\xi^{(ip,jq,kr)} = \beta^{(ip,jq,kr)} \mu^{(ip,jq,kr)},$$

by (1.20) we have

$$\begin{aligned} & \beta^{(ip,jq,kr)} \left(\nu_1^{(ip,jq,kr)} \right)^{a_1} \dots \left(\nu_{11}^{(ip,jq,kr)} \right)^{a_{11}} + \\ & + \beta^{(kr,jq,ip)} \left(\nu_1^{(kr,jq,ip)} \right)^{a_1} \dots \left(\nu_{11}^{(kr,jq,ip)} \right)^{a_{11}} = 1, \end{aligned}$$

or simply

$$\xi^{(ip,jq,kr)} + \xi^{(kr,jq,ip)} = 1.$$

This unit equation can be solved using Baker's method, reduction procedures and Wildanger's enumeration method. This procedure was first described by Gaál and Pohst [31].

After solving this equation in the variables $a_1, \dots, a_{11}$ one has to consider the system of linear equations

$$l^{(ip,jq)}(x_1, x_2, y_0, y_1, y_2) = \pm (\vartheta^{(ip)} - \vartheta^{(jq)}) \gamma^{(ip,jq)} \left(\varepsilon_1^{(ip,jq)} \right)^{a_1} \dots \left(\varepsilon_{11}^{(ip,jq)} \right)^{a_{11}} \quad (1.21)$$

for all possible indices, and solving this it is easy to calculate x_1, x_2, y_0, y_1, y_2 .

1.4.2 Baker's method

Taking logarithms for each possible indices we have

$$a_1 \log |\nu_1^{(ip,jq,kr)}| + \dots + a_{11} \log |\nu_{11}^{(ip,jq,kr)}| = \log |\mu^{(ip,jq,kr)}|.$$

One can consider the above equations (for each possible indices) as a system of linear equations in $a_1, \dots, a_{11}$. The matrix of this system of linear equations has linearly independent columns, cf. [27]. Hence one can select eleven tuples (ip, jq, kr) of indices such that the coefficient matrix M of the left hand side will have rank 11. Let (i_0p, j_0q, k_0r) be the index for which $|\log |\mu^{(ip,jq,kr)}||$ attains its maximum. Then by multiplication by the inverse of M one can express the variables $a_1, \dots, a_{11}$, and we conclude

$$A = \max_{1 \leq h \leq 11} |a_h| \leq c_1 |\log |\mu^{(i_0p, j_0q, k_0r)}||,$$

where c_1 denotes the row norm of M^{-1} , that is, the maximal sum of the absolute values of the elements in the rows of M^{-1} . Note that M should be

chosen such that c_1 becomes as small as possible. Now if $|\mu^{(i_0p, j_0q, k_0r)}| < 1$ then $\log |\mu^{(i_0p, j_0q, k_0r)}| \leq -A/c_1$, and if $|\mu^{(i_0p, j_0q, k_0r)}| > 1$ then the same holds for $\mu^{(i_0p, k_0q, j_0r)} = 1/\mu^{(i_0p, j_0q, k_0r)}$. Hence we conclude that

$$|\mu^{(i_0p, j_0q, k_0r)}| < \exp(-\frac{A}{c_1}) \quad (1.22)$$

for a certain index. Set $c_2 = |\beta^{(i_0p, j_0q, k_0r)}|$. Then using the inequality $|\log x| \leq 2|x - 1|$ holding for $|x - 1| < 0.795$, we have

$$\begin{aligned} & |\log |\beta^{(k_0r, j_0q, i_0p)}| + a_1 \log |\nu_1^{(k_0r, j_0q, i_0p)}| + \dots + a_{11} \log |\nu_{11}^{(k_0r, j_0q, i_0p)}|| = \\ & = |\log |\beta^{(k_0r, j_0q, i_0p)} \mu^{(k_0r, j_0q, i_0p)}|| \leq 2|1 - |\beta^{(k_0r, j_0q, i_0)} \mu^{(k_0r, j_0q, i_0p)}|| \leq \\ & \leq 2|1 - \beta^{(k_0r, j_0q, i_0p)} \mu^{(k_0r, j_0q, i_0p)}| = 2|\beta^{(i_0p, j_0q, k_0r)} \mu^{(i_0p, j_0q, k_0r)}| \leq \\ & \leq 2c_2 \exp(-A/c_1), \end{aligned}$$

provided that the right hand side is < 0.795 , but in the opposite case we get a much better estimate for A . In our example the terms in the above linear form in logarithms were linearly independent over $\mathbb{Q}$, so we can apply the estimates of Baker and Wüstholz [2] to derive a lower estimate

$$\begin{aligned} & |\log |\beta^{(k_0r, j_0q, i_0p)}| + a_1 \log |\nu_1^{(k_0r, j_0q, i_0p)}| + \dots + a_{11} \log |\nu_{11}^{(k_0r, j_0q, i_0p)}|| > \\ & > \exp(-C_0 \log A), \end{aligned}$$

with a large constant C_0 . This inequality compared with (1.22) implies an upper bound A_0 for A . In our example we get $A_0 = 10^{104}$.

1.4.3 LLL reduction of Baker's bound

For a fixed index (ip, jq, kr) consider the lattice L spanned by the columns of the 13×12 matrix

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ C \log |\beta^{(kr, jq, ip)}| & C \log |\nu_1^{(kr, jq, ip)}| & \dots & C \log |\nu_{11}^{(kr, jq, ip)}| \end{pmatrix}$$

where the constant C will be specified later. Denote by b_1 the first vector of the LLL reduced basis of L . Now Lemma 1 of Gaál and Pohst [31] (cf. also Gaál [25]) yields the following:

Lemma 1. *If $A = \max |a_h| < A_0$ and*

$$|b_1| > \sqrt{13} \cdot 2^{11/2} A_0$$

then for all solutions of the inequality

$$|\log |\beta^{(kr,jq,ip)}| + a_1 \log |\nu_1^{(kr,jq,ip)}| + \dots + a_{11} \log |\nu_{11}^{(kr,jq,ip)}|| < 2c_2 \exp(-A/c_1)$$

we have

$$A < c_1(\log C + \log(2c_2) - \log A_0).$$

Note that one has to perform this reduction for all possible tuples of indices. After getting Baker's bound we can use this very efficient lemma to reduce A . One should apply the lemma 4-5 times, taking the previous bound (initially Baker's bound) as A_0 . To ensure the condition of the lemma a suitable choice of the constant C is described in Section 7.

The lemma is very efficient in the first and second steps, when the new bound is about the logarithm of the previous one, but after 4-5 steps the new bound will not improve the previous one. In our example the final reduced bound was 164. The first step was hard to perform, because we had to use 1500 digits of accuracy.

1.4.4 Wildanger's method for the enumeration of the solutions of the unit equation

In this section we use the construction of Gaál and Pohst [31] which is in fact a variant of Wildanger's method [85]. Note that in [31] the relative extension is of degree $n \geq 3$ so in our case we have to use a modified version of Lemma 2 of [31].

For all possible tuples $I = (ip, jq, kr)$ set

$$\xi^{(I)} = \xi^{(ip,jq,kr)}, \quad \beta^{(I)} = \beta^{(ip,jq,kr)}$$

and

$$\nu_h^{(I)} = \nu_h^{(ip,jq,kr)} \text{ for } h = 1, \dots, 11$$

Let $I^* = \{I_1, \dots, I_t\}$ be a nonempty set of indices with the following properties:

1 if $(ip, jq, kr) \in I^*$ then either $(kr, ip, jq) \in I^*$ or $(kr, jq, ip) \in I^*$

2 if $(ip, jq, kr) \in I^*$ then either $(jq, kr, ip) \in I^*$ or $(jq, ip, kr) \in I^*$

3 the vectors

$$\underline{e}_h = \begin{pmatrix} \log |\nu_h^{(I_1)}| \\ \vdots \\ \log |\nu_h^{(I_t)}| \end{pmatrix} \text{ for } h = 1, \dots, 11$$

are linearly independent.

Set

$$\underline{g} = \begin{pmatrix} \log |\beta^{(I_1)}| \\ \vdots \\ \log |\beta^{(I_t)}| \end{pmatrix}, \underline{b} = \begin{pmatrix} \log |\xi^{(I_1)}| \\ \vdots \\ \log |\xi^{(I_t)}| \end{pmatrix}.$$

Using this notation we have

$$\underline{b} = \underline{g} + a_{11}\underline{e}_1 + \dots + a_{11}\underline{e}_{11}.$$

Let A_r be the reduced bound obtained in the previous section, and let

$$\log S_0 = \max_{I \in I^*} (|\log |\alpha^I|| + A_r |\log |\nu_1^{(I)}|| + \dots + A_r |\log |\nu_{11}^{(I)}||). \quad (1.23)$$

From this it is easy to see that

$$\frac{1}{S_0} \leq |\xi^{(I)}| \leq S_0 \text{ for all } I \in I^* \quad (1.24)$$

The following lemma will help us to replace S_0 by a smaller constant in (1.24). Note that it is a variant of Lemma 2 of Gaál and Pohst [31], (cf. also Gaál [25]):

Lemma 2. *Let $1 < s < S$ be given constants and assume that*

$$\frac{1}{S} \leq |\xi^{(I)}| \leq S \text{ for all } I \in I^*.$$

Then either

$$\frac{1}{s} \leq |\xi^{(I)}| \leq s \text{ for all } I \in I^*$$

or there is an $I \in I^*$ with

$$|\xi^{(I)} - 1| \leq \frac{1}{s-1}.$$

Proof. Note that the proof of Lemma 2 in [31] is based on the multiplicative and additive relations between the $\beta^{(I)}$ -s for which $I \in I^*$. In our construction I^* is defined so that the $\xi^{(I)}$ -s for which $I \in I^*$ have the same properties. $\square$

Summarizing, the constant S can be replaced by the smaller constant s if for each t_0 ($1 \leq t_0 \leq t$) we enumerate directly the set H_{t_0} of those exponents $a_1, \dots, a_{11}$ for which

$$\frac{1}{S} \leq |\xi^{(I)}| \leq S \text{ for all } I \in I^* \text{ and } |\xi^{(I_{t_0})} - 1| \leq \frac{1}{s-1}$$

Such exponent vectors are contained in an ellipsoid. To enumerate the points of this ellipsoid we use the algorithm of Fincke and Pohst [18]. This is the critical step of the algorithm, for details see [25] and [31].

1.4.5 Sieving

As one could see in the last section, the enumeration method gives a very large number of exponent vectors $(a_1, \dots, a_{11})$. To reduce this we insert a modular test to eliminate as much vectors as possible.

1.4.6 A numerical example

Using our algorithm we computed all power integral basis in a totally real sextic field having a cubic subfield with Galois group $S_4 \times C_2$. The method was implemented in Maple and was executed on a 333MHz Pentium PC. The defining polynomials, integral basis and fundamental units were computed by the KANT package [14]. Here we summarize our computational experiences.

Consider the totally real sextic field $K = \mathbb{Q}(\vartheta)$ where the minimal polynomial of ϑ is

$$x^6 - 17x^4 + 25x^3 + 3x^2 - 6x + 1.$$

The field has a cubic subfield $M = \mathbb{Q}(\varrho)$ where the minimal polynomial of ϱ is

$$x^3 - 4x - 1,$$

and has Galois group $S_4 \times C_2$. The ϱ has index 1 in M and $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . The field $L^{(11,21)} = \mathbb{Q}(\vartheta^{(11)} + \vartheta^{(21)}, \vartheta^{(11)}\vartheta^{(21)})$ is generated by $\vartheta^{(11)}\vartheta^{(21)}$. In this case both $\vartheta^{(11)} + \vartheta^{(21)}$ and $\vartheta^{(11)}\vartheta^{(21)}$ generate

a field of degree 12, hence they generate the same field. The element $\vartheta^{(11)}\vartheta^{(21)}$ has a simpler defining polynomial, namely

$$x^{12} + 4x^{11} - 50x^{10} - 57x^9 + 302x^8 + 348x^7 - \\ -433x^6 - 450x^5 + 278x^4 + 181x^3 - 80x^2 - 8x + 1$$

Baker's method gave the initial bound $A_0 = 10^{104}$ for A which was reduced to 164, using Lemma 1, by the following steps:

Step	Previous bound	Reduced bound	C
I	$A_0 = 10^{104}$	$A_1 = 2982$	A_0^{11}
II	$A_1 = 2982$	$A_2 = 199$	A_1^{20}
III	$A_2 = 199$	$A_3 = 167$	A_2^{25}
IV	$A_3 = 167$	$A_4 = 164$	A_3^{25}

The first step took about 8.3 hours, and we had to use 1500 digits of accuracy. The following steps took only a few minutes, and it was sufficient to use 150 digits of accuracy.

The final reduced bound was 164 and it gave $S_0 = 10^{1679}$ for the final enumeration (cf. (1.23)).

For the final enumeration we used the set of 18 ellipsoids defined by

$$I^* = \{(2p, 1q, 3r), (3p, 1q, 2r), (1p, 3q, 2r) \mid (p, q, r) \in \Gamma\}$$

where (p, q, r) runs through the set

$$\Gamma = \{(1, 2, 1), (1, 1, 2), (2, 2, 2), (1, 2, 2), (2, 1, 2), (2, 2, 1)\}.$$

In the following table we summarize the final enumeration using Wildanger's method. cf. Lemma 2. We display S, s , the approximate number of exponent vectors $(a_1, \dots, a_{11})$ enumerated in the 18 ellipsoids, the number of the exponent vectors surviving the modular tests and in the last column we display the CPU time. The last line represents the enumeration of the single ellipsoid containing the exponent vectors with coordinates ≤ 3 in absolute value (cf. [31]).

Step	S	s	Enumerated	Survived	CPU Time
I	10^{1679}	10^{100}	0	0	1.5h
II	10^{100}	10^{50}	0	0	0.3h
III	10^{50}	10^{20}	1	0	0.1h
IV	10^{20}	10^{15}	30	0	0.1h
V	10^{15}	10^{12}	1300	0	0.1h
VI	10^{12}	10^{10}	14200	0	0.2h
VII	10^{10}	10^9	22700	0	0.2h
VIII	10^9	10^8	78300	0	0.6h
IX	10^8	10^7	246000	0	1.6h
X	10^7	10^6	650000	0	3.7h
XI	10^6	$5 \cdot 10^5$	366000	0	1.7h
XII	$5 \cdot 10^5$	10^5	1033000	2	4.8h
XIII	10^5	$5 \cdot 10^4$	328000	2	2.7h
XIV	$5 \cdot 10^4$	10^4	1971000	12	6.5h
XV	10^4	$5 \cdot 10^3$	711000	16	2.7h
XVI	$5 \cdot 10^3$	10^3	1688000	38	5.9h
XVII	10^3	$5 \cdot 10^2$	500000	42	1.5h
XVIII	$5 \cdot 10^2$	10^2	902000	76	3.3h
XIX	10^2	10^1	278000	149	1.8h
XX	10^1	3	1800	128	0.03h
XXI	3	0	3	3	0.01h

From the surviving exponent vectors we calculated the coordinates in the basis $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ of the corresponding elements of K by (1.21) and tested if they really generate power integral basis. We got the following solutions:

$$(x_1, x_2, y_0, y_1, y_2) = (0, 0, 1, 0, 0), (1, 0, 7, 0, -2).$$

We note that if α generates power integral basis, then for arbitrary $z \in \mathbb{Z}$ the element $\pm\alpha + z$ generates also power integral basis.

Chapter 2

Results on Heron triangles

2.1 Introduction

Let a, b, c be positive integers which can be the sides of an arbitrary triangle and let $d := \gcd(a, b, c)$. It is then easy to see that the triangle whose sides are a, b, c is Heron (i.e., its area is an integer), if and only if the triangle whose sides are $\frac{a}{d}, \frac{b}{d}, \frac{c}{d}$ is Heron as well. Thus, we will restrict our analysis to the Heron triangles which are *reduced*, i.e, for which the greatest common divisor of the lengths of its sides is 1.

For any non-zero integer k let $P(k)$ be the largest prime divisor of k with the convention that $P(\pm 1) = 1$. In [57] A.Kramer and F.Luca showed that $P(A) \rightarrow \infty$ when $\max(a, b, c)$ tends to infinity over all the triples (a, b, c) which are the sides of reduced Heron triangles and they computed all Heron triangles having $P(A) < 5$. In [64] F.Luca found all the Heron triangles whose sides are prime powers. We prove the following Theorem.

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

Very few results of this kind have been proved so far. Until recently it was not even known that for distinct positive integers a, b, c the number $P((ab + 1)(ac + 1)(bc + 1))$ tends to infinity when $\max(a, b, c)$ tends to infinity, although partial results concerning this problem are obtained by Bugeaud [7], K. Győry, A. Sárközy and C. L. Stewart [46], K. Győry and A. Sárközy [47], C. L. Stewart and R. Tijdeman [77]. The fact that this is indeed the case has been shown

by P. Corvaja and U. Zannier [13] and by S. Hernandez and F. Luca [51]. The proof of Theorem 4 is based on the finiteness of number of solutions of an $\mathcal{S}$ -unit equation and hence it is ineffective. We can obtain an effective result at the cost of assuming that the prime divisors of abc have a certain shape.

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 $abc \in \mathcal{S}$.*

By noticing that the second largest prime number which is congruent to 1 modulo 4 is 13, by Theorem 5 it follows that there are only finitely many effectively computable reduced Heron triangles whose sides have lengths a, b, c with $P(abc) < 13$. All these triangles are listed below.

Theorem 6. *The only reduced Heron triangles whose sides are of lengths $a \leq b \leq c$ 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

Note that in the above theorem we only list the non-degenerate solutions for which $c < a + b$ holds.

Let a, b, c be the sides of a reduced Heron triangle and let A be its area. Set $s := \frac{a+b+c}{2}$ to be its semiperimeter. By the Heron formula, we get

$$A = \sqrt{s(s-a)(s-b)(s-c)}, \quad (2.1)$$

which is equivalent to

$$(4A)^2 = -a^4 - b^4 - c^4 + 2a^2b^2 + 2a^2c^2 + 2b^2c^2. \quad (2.2)$$

It is easy to see that one of the three numbers a , b , c is even and the other two are odd. Notice that the point $(x, y, z, t) = (a, b, c, 4A)$ lies on the surface

$$-x^4 - y^4 - z^4 + 2x^2y^2 + 2x^2z^2 + 2y^2z^2 = t^2. \quad (2.3)$$

Conversely, if x, y, z, t are positive integers satisfying equation (2.3), then x , y , z are the sides of a triangle whose area is an integer. Clearly, we may assume that $\gcd(x, y, z) = 1$, because with $d := \gcd(x, y, z)$ we get that $d^2 \mid t$ and that the positive integer point $(x_1, y_1, z_1, t_1) = \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}, \frac{t}{d^2}\right)$ satisfies equation (2.3) as well. Since x , y and z have no nontrivial common divisor, by looking at equation (2.3) modulo 8, it follows immediately that one of the three numbers x , y , and z is even and the other two are odd. In particular, all four numbers $x + y + z$, $x + y - z$, $x + z - y$, and $y + z - x$ are even, and now rewriting equation (2.3) as

$$(x + y + z)(x + y - z)(x + z - y)(y + z - x) = t^2, \quad (2.4)$$

we get that $4 \mid t$. Moreover, since x , y and z are positive, from equation (2.4) we also read that x , y and z form a triangle (i.e., the largest one is smaller than the sum of the other two), and the area of this triangle is $t/4$, therefore an integer. Thus, the study of Heron triangles reduces to the study of the positive integer solutions of equation (2.3).

2.2 Proof of Theorem 4

Let $\mathcal{P}$ be any finite set of prime numbers. Without loss of generality we may assume that $2 \in \mathcal{P}$. Let $\mathcal{S}$ be the set of all positive integers whose prime factors belong to $\mathcal{P}$. To prove Theorem 4, it suffices to show that there are only finitely many reduced Heron triangles whose sides have lengths a , b , c such that $abc \in \mathcal{S}$. We distinguish two cases.

2.2.1 The triangle is isosceles

Assume that $a = b$. In this case, c is even and if we denote by h_c the length of the altitude orthogonal to the side of length c , then $(a, h_c, c/2)$ is a reduced

Pythagorean triple. In particular, we get

$$h_c^2 = a^2 - \left(\frac{c}{2}\right)^2. \quad (2.5)$$

With $y := a^2 \in \mathcal{S}$ and $z := \left(\frac{c}{2}\right)^2 \in \mathcal{S}$, equation (2.5) is a special case of an equation of the form

$$x^2 = y - z \quad \gcd(x, y, z) = 1 \text{ and } yz \in \mathcal{S}, \quad (2.6)$$

and by the work of de Weger [83] we know that the above equation has only finitely many, even effectively computable, positive solutions x, y, z .

2.2.2 The triangle is not isosceles

Formula (2.4) gives

$$(a + b + c)(a + b - c)(a + c - b)(b + c - a) = (4A)^2. \quad (2.7)$$

We note that

$$\gcd(a+b+c, a+b-c) \mid 2c, \quad \gcd(a+b+c, a+c-b) \mid 2b, \quad \gcd(a+b+c, b+c-a) \mid 2a, \quad (2.8)$$

therefore

$$\gcd(a + b + c, (a + b - c)(a + c - b)(b + c - a)) \in \mathcal{S}. \quad (2.9)$$

From (2.7) and (2.9) it follows that there exists a square-free number $d_1 \in \mathcal{S}$ such that

$$a + b + c = d_1 x_1^2 \quad (2.10)$$

holds with some positive integer x_1 . In a similar way, we also get that there exist six positive integers $d_2, d_3, d_4, x_2, x_3, x_4$ such that d_2, d_3, d_4 are square-free integers in $\mathcal{S}$ and

$$a + b - c = d_2 x_2^2, \quad a + c - b = d_3 x_3^2, \quad b + c - a = d_4 x_4^2. \quad (2.11)$$

Let $p_1 < p_2 < \dots < p_t$ be the prime numbers in $\mathcal{P}$ and let $\mathbb{K} := \mathbb{Q}[\sqrt{p_i} \mid i = 1, \dots, t]$. Let $h := h_{\mathbb{K}}$ be the class number of $\mathbb{K}$, and let $\mathbb{Z}_{\mathbb{K}}$ be the ring of integers in $\mathbb{K}$. Let $\pi_1, \dots, \pi_l$ be all the prime ideals in $\mathbb{Z}_{\mathbb{K}}$ whose norms lie above

the prime numbers in $\mathcal{P}$. Let a_i be a generator of the principal ideal $[\pi_i]^h$. It is well-known that there exists a positive integer u and some computable algebraic numbers $b_1, \dots, b_u$ in $\mathbb{Z}_{\mathbb{K}}$ such that if $c \in \mathbb{Z}_{\mathbb{K}}$ has the property that the norm of c in $\mathbb{K}$ is an element of $\mathcal{S}$, then c can be written in the form

$$c = b_j \zeta a_1^{m_1} \dots a_l^{m_l}$$

where $j \in \{1, \dots, u\}$, ζ is a unit in $\mathbb{K}$, and m_i are non-negative integers for $i = 1, \dots, l$ (see [75]). Let $\widehat{\mathcal{S}}$ be the set of all algebraic integers in $\mathbb{Z}_{\mathbb{K}}$ which can be written in the form $\zeta a_1^{m_1} \dots a_l^{m_l}$ with some unit ζ in $\mathbb{K}$ and some non-negative integers m_i for $i = 1, \dots, l$. In particular, if $c \in \mathbb{Z}_{\mathbb{K}}$ is such that the norm of c is an element of $\mathcal{S}$, then c can be written in the form $c = b_j s$ for some $j = 1, \dots, u$, and some $s \in \widehat{\mathcal{S}}$. We now return to equations (2.10) and (2.11) and note that

$$2c = d_1 x_1^2 - d_2 x_2^2 = (\sqrt{d_1} x_1 - \sqrt{d_2} x_2)(\sqrt{d_1} x_1 + \sqrt{d_2} x_2)$$

and

$$2b = d_1 x_1^2 - d_3 x_3^2 = (\sqrt{d_1} x_1 - \sqrt{d_3} x_3)(\sqrt{d_1} x_1 + \sqrt{d_3} x_3).$$

By taking norms in $\mathbb{K}$ in the above equations, we get that $N_{\mathbb{K}}(\sqrt{d_1} x_1 \pm \sqrt{d_i} x_i)$ are in $\mathcal{S}$ for $i = 1, 2$. Thus, there exist four indices i_1, i_2, i_3, i_4 in $\{1, \dots, u\}$ and four numbers s_1, s_2, s_3, s_4 in $\widehat{\mathcal{S}}$ such that

$$\sqrt{d_1} x_1 - \sqrt{d_2} x_2 = b_{i_1} s_1, \quad \sqrt{d_1} x_1 + \sqrt{d_2} x_2 = b_{i_2} s_2$$

and

$$\sqrt{d_1} x_1 - \sqrt{d_3} x_3 = b_{i_3} s_3, \quad \sqrt{d_1} x_1 + \sqrt{d_3} x_3 = b_{i_4} s_4.$$

From the four equations above we get that

$$\sqrt{d_3} x_3 - \sqrt{d_2} x_2 = b_{i_1} s_1 - b_{i_3} s_3 = b_{i_4} s_4 - b_{i_2} s_2.$$

Thus,

$$b_{i_1} s_1 + b_{i_2} s_2 - b_{i_3} s_3 - b_{i_4} s_4 = 0. \tag{2.12}$$

Suppose now that there are infinitely many reduced Heron triangles which are not isosceles and for which $abc \in \mathcal{S}$. Each one of these triangles will lead to an equation of the form (2.12) in $\mathbb{Z}_{\mathbb{K}}$. Since there are only finitely many choices for the quadruple of indices (i_1, i_2, i_3, i_4) , it follows that there

is a fixed quadruple (i_1, i_2, i_3, i_4) for which equation (2.12) admits infinitely many solutions $(s_1, s_2, s_3, s_4) \in \widehat{\mathcal{S}}^4$. Write $\beta_1 := b_{i_1}$, $\beta_2 := b_{i_2}$, $\beta_3 := -b_{i_3}$ and $\beta_4 := -b_{i_4}$. We first check that the equation

$$\beta_1 s_1 + \beta_2 s_2 + \beta_3 s_3 + \beta_4 s_4 = 0 \quad (2.13)$$

is non-degenerate, that is no proper subsum is zero. Since $\beta_i s_i \neq 0$, it follows that the only way that some proper subsum of (2.13) is zero is when

$$\beta_1 s_1 + \beta_2 s_2 = \beta_3 s_3 + \beta_4 s_4 = 0, \quad (2.14)$$

or when

$$\beta_1 s_1 + \beta_3 s_3 = \beta_2 s_2 + \beta_4 s_4 = 0, \quad (2.15)$$

or when

$$\beta_1 s_1 + \beta_4 s_4 = \beta_2 s_2 + \beta_3 s_3 = 0. \quad (2.16)$$

If (2.14) holds, we get $0 = \beta_1 s_1 + \beta_2 s_2 = b_{i_1} s_1 + b_{i_2} s_2 = 2\sqrt{d_1}x_1$, which is impossible. If (2.15) holds, we get $0 = \beta_1 s_1 + \beta_3 s_3 = b_{i_1} s_1 - b_{i_3} s_3 = \sqrt{d_3}x_3 - \sqrt{d_2}x_2$, therefore $d_3 x_3^2 = d_2 x_2^2$, or, equivalently $b = c$, which is impossible because we are assuming that the triangle is not isosceles. Finally, if (2.16) holds, we then get $0 = \beta_1 s_1 + \beta_4 s_4 = b_{i_1} s_1 - b_{i_4} s_4 = -\sqrt{d_2}x_2 - \sqrt{d_3}x_3$, leading again to $d_2 x_2^2 = d_3 x_3^2$, which is impossible again. Thus, equation (2.13) is non-degenerate. It follows from the classical results on non-degenerate S -unit equations (see [17]), that there exist finitely many quadruples of solutions (S_1, S_2, S_3, S_4) with $S_i \in \widehat{\mathcal{S}}$ for $i = 1, \dots, 4$. So for every solution (s_1, s_2, s_3, s_4) with $s_i \in \widehat{\mathcal{S}}$ of equation (2.12) there exists a number $\rho \in \widehat{\mathcal{S}}$ and one of these finitely many quadruples of solutions, say (S_1, S_2, S_3, S_4) , so that

$$s_i = S_i \rho \quad \text{for } i = 1, \dots, 4. \quad (2.17)$$

Let us call the collection of (the finitely many) such solutions (S_1, S_2, S_3, S_4) of equation (2.12) as the collection of *reduced* solutions. Let C be an upper bound for $N_{\mathbb{K}}(b_j)$ for $j = 1, \dots, u$ and for $N_{\mathbb{K}}(S_i)$ for $i = 1, \dots, 4$ over all the finitely many reduced solutions. With equation (2.17), we get

$$2\sqrt{d_1}x_1 = b_{i_1} s_1 + b_{i_2} s_2 = \rho(b_{i_1} S_1 + b_{i_2} S_2),$$

therefore ρ divides $2\sqrt{d_1}x_1$. In particular, ρ^2 divides $4(a + b + c)$. In a similar way, we get that ρ^2 divides $4(a + b - c)$ and $4(a + c - b)$. Since $\gcd(a, b, c) = 1$,

and precisely one of the numbers a , b , c is even and the other two are odd, we get that $\gcd(a+b+c, a+b-c, a+c-b) = 2$. Thus, ρ^2 divides 8, therefore ρ divides 4. Thus, $N_{\mathbb{K}}(\rho)$ divides $N_{\mathbb{K}}(4) = 4^{2^t}$, and in particular $N_{\mathbb{K}}(\rho)$ is bounded. Since

$$2c = d_1x_1^2 - d_2x_2^2 = (\sqrt{d_1}x_1 - \sqrt{d_2}x_2)(\sqrt{d_1}x_1 + \sqrt{d_2}x_2) = b_{i_1}b_{i_2}S_1S_2\rho^2,$$

and

$$2b = d_1x_1^2 - d_3x_3^2 = (\sqrt{d_1}x_1 - \sqrt{d_3}x_3)(\sqrt{d_1}x_1 + \sqrt{d_3}x_3) = b_{i_3}b_{i_4}S_3S_4\rho^2,$$

we get that $b^{2^t} = N_{\mathbb{K}}(b)$ and $c^{2^t} = N_{\mathbb{K}}(c)$ are both bounded. So, b and c can take only finitely many values. Since the same argument works for any pair of side lengths, we get that there are indeed only finitely many reduced Heron triangles with $abc \in \mathcal{S}$.

2.3 Proof of Theorem 5

The following Lemma is from [64], but we shall include it here for the completeness of the argument.

Lemma 3. *Assume that a, b, c are the lengths of sides of a non-isosceles Heron triangle. Suppose that p is a prime number, $p \not\equiv 1 \pmod{4}$ such that $p^\alpha \mid a$. Then $p^{\alpha+1} \mid (b^2 - c^2)$ if $p = 2$ and $p^\alpha \mid (b^2 - c^2)$ if $p > 2$.*

Proof. We treat only the case $p > 2$ since the case $p = 2$ can be dealt with similarly. We rewrite equation (2.2) as

$$2a^2(b^2 + c^2) - a^4 - (b^2 - c^2)^2 = (4A)^2. \quad (2.18)$$

One may reduce equation (2.18) modulo $p^{2\alpha}$ and get

$$-(b^2 - c^2)^2 \equiv (4A)^2 \pmod{p^{2\alpha}}. \quad (2.19)$$

Observe that equation (2.19) forces $p^\alpha \mid (b^2 - c^2)$. Indeed, assume that this is not the case. It then follows that if $p^\delta \parallel (b^2 - c^2)$, then $\delta < \alpha$. Simplifying both sides of equation (2.19) by $p^{2\delta}$, we get

$$-\left(\frac{b^2 - c^2}{p^\delta}\right)^2 \equiv \left(\frac{4A}{p^\delta}\right)^2 \pmod{p^{2(\alpha-\delta)}}. \quad (2.20)$$

However, notice that congruence (2.20) is impossible because -1 is not a quadratic residue modulo p . Hence, p^α divides both $(b^2 - c^2)$ and A . The Lemma is therefore proved. $\square$

We are now ready to prove Theorem 5. Let p_1 be the unique prime number in $\mathcal{P}$ which is congruent to 1 modulo 4 and assume that $p_2 < p_3 < \dots < p_t$ are the other prime numbers belonging to $\mathcal{P}$. Since $\gcd(a, b, c) = 1$, it follows that at least one of the three numbers a , b and c is not a multiple of p_1 . Assume that a is coprime to p_1 and write

$$a = p_2^{\alpha_2} \cdots p_t^{\alpha_t}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}, \quad c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_t^{\gamma_t}. \quad (2.21)$$

We may restrict ourselves to treating the case of the non-isosceles triangles by Theorem 4. Write $b_1 = \frac{b}{p_1^{\beta_1}}$, $c_1 = \frac{c}{p_1^{\gamma_1}}$, and set $X := \max\{\alpha_i, \beta_i, \gamma_i \mid i = 1, \dots, t\}$, where we assume that $X > e$. Repeated applications of the Lemma 1 give

$$a \mid b^2 - c^2, \quad b_1 \mid a^2 - c^2, \quad c_1 \mid a^2 - b^2. \quad (2.22)$$

For every prime number p and every non-zero rational number r let $\text{ord}_p(r)$ denote the order at which the prime number p divides r (r is written in reduced form). We use the divisibility relations (2.22) and lower bounds for linear forms in p -adic logarithms to bound $\max\{\alpha_i, \beta_i, \gamma_i \mid i = 2, \dots, t\}$ linearly in $\log X$. Let us take the first divisibility relation (2.22) and let $i \in \{2, \dots, t\}$. If $\alpha_i = 0$, then we are done. If not, then since $\gcd(a, b, c) = 1$, it follows that bc is not a multiple of p_i and that

$$\begin{aligned} \alpha_i &= \text{ord}_{p_i}(a) \leq \text{ord}_{p_i}(b^2 - c^2) = \text{ord}_{p_i}(1 - b^{-2}c^2) \\ &= \text{ord}_{p_i}(1 - p_1^{2(\gamma_1 - \beta_1)} p_2^{2(\gamma_2 - \beta_2)} \cdots p_t^{2(\gamma_t - \beta_t)}). \end{aligned} \quad (2.23)$$

We use standard lower bounds for linear forms in p -adic logarithms (see, for example, [87]) to deduce that inequality (2.23) implies that

$$\alpha_i < C_1 \log X \quad (2.24)$$

where C_1 is an effectively computable constant depending only on P , the largest prime number in $\mathcal{P}$, and t , the number of elements of $\mathcal{P}$. Similar arguments show that

$$\max\{\alpha_i, \beta_i, \gamma_i \mid i = 2, \dots, t\} < C_1 \log X. \quad (2.25)$$

It remains to bound β_1 and γ_1 . Assume that $\beta_1 \leq \gamma_1$. From the triangular inequality, we have

$$0 < |b - c| < a$$

and p^{β_1} divides $b - c$. So,

$$p_1^{\beta_1} < a. \quad (2.26)$$

Therefore

$$\beta_1 \log p_1 < \log a.$$

In particular,

$$\beta_1 < \frac{C_1 t \log P}{\log p_1} \log X, \quad (2.27)$$

and

$$\log b = \beta_1 \log p_1 + \sum_{i=2}^t \beta_i \log p_i < \sum_{i=2}^t (\alpha_i + \beta_i) \log p_i < C_2 \log X,$$

where $C_2 = 2C_1 t \log P$. Finally, we use the triangular inequality again to get

$$p_1^{\gamma_1} \leq c \leq a + b < 2\max(a, b), \quad (2.28)$$

therefore

$$\gamma_1 \log p_1 < \log 2 + \max(\log a, \log b) < \log 2 + C_2 \log X,$$

which implies that

$$\gamma_1 < \frac{\log 2}{\log p_1} + \frac{C_2}{\log p_1} \log X. \quad (2.29)$$

Since X was the maximum of all the exponents $\alpha_i, \beta_i, \gamma_i$ with $i = 1, \dots, t$, we get from inequalities (2.25)-(2.29) that

$$X < \frac{\log 2}{\log p_1} + \frac{2C_1 t \log P}{\log p_1} \log X,$$

which implies that $X < C_3$. Hence Theorem 5 is proved.

2.4 Proof of Theorem 6

2.4.1 Isosceles triangles

We denote by S the set of positive integers divisible by 2, 3, 5, 7, 11 only. We assume that in our isosceles triangle $a = b$, and we denote by h_c the altitude orthogonal to c . In this case c is even. By (2.5) we have

$$\left(\frac{c}{2}\right)^2 = (a + h_c)(a - h_c)$$

which implies that $(a + h_c), (a - h_c) \in S$. Further,

$$x + y = z \quad (x, y, z \in S) \tag{2.30}$$

holds for $x = (a + h_c)$, $y = (a - h_c)$, $z = 2a$. Using equation (2.5) and $\gcd(a, c) = 1$, we obtain that $\gcd((a + h_c), (a - h_c), 2a)$ is 1 or 2. Hence the values of $(a + h_c)$, $(a - h_c)$, $2a$, that is, the values of $a = b$ and c , can be obtained from the primitive solutions of equation (2.30).

The primitive solutions of equation (2.30) were described by [82] (see Theorem 6.3 on page 123) for an even larger set of primes including also 13. To list the primitive solutions of (2.30) we just had to select the solutions not divisible by 13 from the list of de Weger's theorem. We tested these candidates against the condition that they are the sides of a triangle whose area is an integer. This yielded the solutions (5,5,6), (5,5,8), (14,25,25), (25,25,48), (88,125,125), (625,625, 672).

2.4.2 Non-isosceles triangles

Explicit upper bounds

Set $p_1 = 5, p_2 = 2, p_3 = 3, p_4 = 7, p_5 = 11$. These are all the primes less than 13, and p_1 is the only one congruent to 1 mod 4. We keep the notation of the proof of Theorem 5, cf. (2.21). We shall use

$$\tilde{X} := \max_{2 \leq i \leq 5} \{\alpha_i, \beta_i, \gamma_i\}$$

and

$$X := \max\{\beta_1, \gamma_1, \tilde{X}\}$$

will be the same as before.

We first make explicit the estimates of the proof of Theorem 5. Let $t = 5$. If $\alpha_i > 0$ for $2 \leq i \leq 5$, then (2.23) holds. Note that by the remark before (2.23) it follows that if $\alpha_i > 0$ then the i -th factor of the last product in (2.23) does not appear because of $\beta_i = \gamma_i = 0$ ($i = 2, 3, 4, 5$). We apply the estimates of [87] (a more explicit formulation can be found in the book [Smart 98], p.225). We obtain

$$\alpha_i \leq \text{ord}_{p_i} (1 - p_1^{2(\gamma_1 - \beta_1)} p_2^{2(\gamma_2 - \beta_2)} \dots p_5^{2(\gamma_5 - \beta_5)}) \leq C_1 \log X, \quad (2.31)$$

where the values of C_1 are different for the different primes, but all of them satisfy

$$C_1 \leq 1.4 \cdot 10^{25}.$$

We obtain similar estimates for β_i, γ_i ($2 \leq i \leq 5$), that is we infer

$$\tilde{X} < C_1 \cdot \log X. \quad (2.32)$$

We only have to bound β_1 and γ_1 . Similarly as in (2.26), we have

$$\beta_1 \log p_1 < \log a = \alpha_2 \log p_2 + \dots + \alpha_5 \log p_5 \leq \tilde{X} \log 462,$$

that is, by (2.32)

$$\beta_1 < \frac{\log 462}{\log 5} \cdot \tilde{X} \leq 3.82 \cdot \tilde{X} \leq 3.82 \cdot C_1 \cdot \log X. \quad (2.33)$$

By (2.28) and the above inequalities, we obtain

$$\gamma_1 \leq \frac{\log(a+b)}{\log p_1} \leq \frac{1}{\log 5} \cdot \log \left(5^{3.82\tilde{X}} \cdot 462^{\tilde{X}} + 462^{\tilde{X}} \right) \quad (2.34)$$

whence

$$\gamma_1 \leq \frac{\log 2 + 3.82\tilde{X} \log 5 + \tilde{X} \log 462}{\log 5} \leq 8.07 \cdot \tilde{X} < 8.07 \cdot C_1 \log X, \quad (2.35)$$

which finally implies

$$X < 1.13 \cdot 10^{26} \cdot \log X,$$

whence

$$X < 10^{28}. \quad (2.36)$$

Reduction

Let again $2 \leq i \leq 5$, then if $\alpha_i > 0$ we have (cf. (2.31))

$$0 < \alpha_i \leq \text{ord}_{p_i}(2(\gamma_1 - \beta_1) \log_{p_i} p_1 + \dots + 2(\gamma_5 - \beta_5) \log_{p_i} p_5) \quad (2.37)$$

where in the above sum the term with index i does not occur. We are now going to reduce the bound (2.36). For this purpose, we apply the following statement.

Lemma 4. *Let p be a prime, $\vartheta_1, \dots, \vartheta_n \in \Omega_p$, where Ω_p is the completion of the algebraic close of the field of p -adic numbers. Let also $\Lambda = \sum_{i=1}^n x_i \vartheta_i$ be with coefficients $x_1, \dots, x_n \in \mathbb{Z}$, $X := \max |x_i|$ and c_1, c_2 be positive constants. Assume that $\text{ord}_p(\vartheta_i)$ is minimal for $i = n$, let*

$$\vartheta'_i = -\vartheta_i / \vartheta_n \quad (i = 1, \dots, n-1),$$

and

$$\Lambda' = \Lambda / \vartheta_n = - \sum_{i=1}^{n-1} x_i \vartheta'_i + x_n.$$

Let $0 < \mu \in \mathbb{Z}$, and for any $\vartheta \in \Omega_p$ let $\vartheta^{(\mu)}$ be a rational integer with $\text{ord}_p(\vartheta - \vartheta^{(\mu)}) \geq \mu$. Denote by Γ_μ the lattice spanned by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \vartheta'_1 & \vartheta'_2 & \cdots & \vartheta'_{n-1} & p^\mu \end{pmatrix}.$$

Denote by b_1 the first vector of the LLL-reduced basis of Γ_μ . If

$$\|b_1\| > 2^{\frac{n-1}{2}} \sqrt{n} X_0$$

then the inequality

$$\text{ord}_p(\Lambda) \geq c_1 + c_2 x_j, \quad X \leq X_0$$

has no solutions $x_1, \dots, x_n$ with

$$\frac{\mu - 1 + \text{ord}_p(\vartheta_n) - c_1}{c_2} \leq X \leq X_0.$$

Proof. This is Lemma 3.14 of [82] combined with the well known estimate for the shortest lattice vector in terms of b_1 . The formulation of the statement in terms of b_1 makes it easier to apply. $\square$

In view of (2.36), we have the initial bound $X_0 = 10^{28}$ for X . Note that in our case $n = 4$ (the term with index i does not occur in the linear form (2.37)), and the constants in the above lemma are $c_1 = 0$, $c_2 = 1$. Having the bound X_0 for X , the coefficients of (2.37) can be bounded (in absolute value) by $2X_0$ (each prime occurs in exactly one of a , b_1 , c_1). In order to perform the reduction, we must have

$$\|b_1\| > 2^{\frac{3}{2}} 2 (2X_0) = 2^{\frac{7}{2}} X_0. \quad (2.38)$$

Note that the value of $\text{ord}_p(\vartheta_n)$ was 2 in case of $p = 2$ and 1 for $p = 3, 7, 11$. If (2.38) is satisfied for a certain μ , then by Lemma 4 we conclude

$$\alpha_i \leq \mu - 1 + 2 = \mu + 1. \quad (2.39)$$

For $2 \leq i \leq 5$ we perform reductions for α_i and similarly for β_i and γ_i just interchanging the roles of a , b , c . The reductions for β_i and γ_i are formally the same as for α_i . That is, we have to perform reductions for the linear forms having the following coefficients:

p	ϑ_1	ϑ_2	ϑ_3	ϑ_4
2	$\log_2 3$	$\log_2 5$	$\log_2 7$	$\log_2 11$
3	$\log_3 2$	$\log_3 5$	$\log_3 7$	$\log_3 11$
7	$\log_7 2$	$\log_7 3$	$\log_7 5$	$\log_7 11$
11	$\log_{11} 2$	$\log_{11} 3$	$\log_{11} 5$	$\log_{11} 7$

If for a certain μ (2.38) is satisfied for all linear forms, then by (2.39) we get $\tilde{X} \leq \mu + 1$. Then by (2.33) and (2.34) we derive a new bound for X . Using this new bound, the reduction can be repeated, as long as the new bound for X is less than the previous one. The following table gives a summary of the reduction process:

Step	X	$\ b_1\ >$	μ	new bound for $\tilde{X}$	new bound for X
I.	10^{28}	$1.131 \cdot 10^{29}$	390	391	2984
II.	2984	33749.04	61	62	473
III.	473	5349.63	51	52	396
IV.	396	4478.76	$p = 2 : 50$	51	
IV.	396	4478.76	$p = 3 : 32$	32	
IV.	396	4478.76	$p = 7 : 20$	20	
IV.	396	4478.76	$p = 11 : 15$	15	

In Step IV. we used different values for μ in order to get the best possible bounds for the exponents of 2, 3, 7, and 11, respectively.

Enumeration

Using the reduced bounds we have the following possibilities for a, b, c :

$$\begin{aligned}
a &= 2^{\alpha_2} 3^{\alpha_3} 7^{\alpha_4} 11^{\alpha_5} \\
b_1 &= 2^{\beta_2} 3^{\beta_3} 7^{\beta_4} 11^{\beta_5} \\
c_1 &= 2^{\gamma_2} 3^{\gamma_3} 7^{\gamma_4} 11^{\gamma_5}
\end{aligned}$$

where

$$\begin{aligned}
0 &\leq \alpha_2, \beta_2, \gamma_2 \leq 51 \\
0 &\leq \alpha_3, \beta_3, \gamma_3 \leq 32 \\
0 &\leq \alpha_4, \beta_4, \gamma_4 \leq 20 \\
0 &\leq \alpha_5, \beta_5, \gamma_5 \leq 15
\end{aligned}$$

where in addition for all i ($1 \leq i \leq 4$) at most one of $\alpha_i, \beta_i, \gamma_i$ can be non-zero. We enumerate all these values of a, b_1, c_1 . For all these triples we let β_1 run through the interval

$$0 \leq \beta_1 \leq \frac{\log a}{\log 5}.$$

We then set $b := 5^{\beta_1} \cdot b_1$ and test if $c_1 | a^2 - b^2$ (cf. (2.22)). If so, we then let γ_1 run through the interval

$$0 \leq \gamma_1 \leq \frac{\log(a+b) - \log c_1}{\log 5}$$

(recall that $c \leq a+b$ must hold). Finally, we set $c := 5^{\gamma_1} \cdot c_1$, test if the three sides are distinct, and if $b_1 | a^2 - c^2$ and $a | b^2 - c^2$ (cf. (2.22)). We further test the surviving triples to see if they can be sides of a triangle whose area is an integer.

Remarks on CPU times

The reduction procedure took just some minutes of CPU time. On the other hand, the enumeration of the possible exponents was a hard task, taking about a week of CPU time. Our programs were written in Maple and were executed on a PC with 350Mhz processor.

Note that omitting one prime the same computation took just 20 minutes. This shows that it is not feasible to extend the present computation for more primes.

Chapter 3

Applications of unit equations in three unknowns

3.1 Introduction

K.Győry (see e.g. [37],[43],[45]) investigated general decomposable form equations, which contain as special cases Thue equations, norm form, discriminant form, index form and resultant form equations. General discriminant form and index form equations and a large class of norm form equations (including Thue equations) were reduced by K.Győry to unit equations in two variables of type

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

(in the unknown units u_1, u_2) for which he applied ([36a],[36b],[8],[43],[45]) Baker's method to derive upper bounds for the solutions. Applying reduction methods and enumeration processes due to K.Wildanger recently it became possible to solve some of these equations completely (see [25]). These equations usually only have "small" solutions. These methods are described in the monograph I.Gaál [25].

J.-H.Evertse and K.Győry (see e.g. [16]) showed that arbitrary decomposable form equations are equivalent to a system of unit equations in *several variables*.

Presently Baker's method seems to be not be applicable to unit equations in more than two variables, so using this approach there is no hope to solve

these equations completely.

We are going to give an algorithm for calculating "small" solutions of unit equations in three variables. The application of this method makes possible to find "small" solutions of some classes of decomposable form equations, that formerly could not be dealt with by using the above standard tools. The method is based on the ideas of K.Wildanger [85] and I.Gaál and M.Pohst [31] (see also [25]) and uses the method of U.Fincke and M.Pohst [18] for enumerating points in ellipsoids.

3.2 Preliminary definitions and results

3.2.1 Semi-orbits, enumerable semi-orbits

Let $x, y \in \mathbb{C}^*$. The set

$$\mathfrak{D}(x, y) = \left\{ x, \frac{1}{x}, y, \frac{1}{y}, -\frac{x}{y}, -\frac{y}{x} \right\}$$

is called the *semi-orbit* of x and y . The elements x and y are the generators of the semi-orbit $\mathfrak{D}(x, y)$.

One can see that if $x = \varepsilon$ is an exceptional unit (i.e. ε and $1 - \varepsilon$ are both units) of an algebraic number field, then

$$\mathfrak{D}(\varepsilon, 1 - \varepsilon) = \Omega(\varepsilon)$$

where $\Omega(\varepsilon)$ is the orbit of ε , that is

$$\Omega(\varepsilon) = \left\{ \varepsilon, 1 - \varepsilon, \frac{1}{\varepsilon}, \frac{1}{1 - \varepsilon}, \frac{\varepsilon}{\varepsilon - 1}, \frac{\varepsilon - 1}{\varepsilon} \right\}$$

in the terminology of K.Wildanger [85].

We will call a semi-orbit $\mathfrak{D}(x, y)$ *enumerable* if for all $u \in \mathfrak{D}(x, y)$ there is a $v \in \mathfrak{D}(x, y)$ such that

$$|u + v| \leq 2 \quad \text{and} \quad \frac{u}{v} \in \mathfrak{D}(x, y).$$

In this case we will use the notation $\mathfrak{D}^2(x, y)$.

Lemma 5. Let $x_1, x_2, x_3 \in \mathbb{C}^*$ and

$$M_0(x_1, x_2, x_3) = \{x_1, x_2, x_3\} \quad M_1(x_1, x_2, x_3) = \left\{ \frac{1}{x_1}, -\frac{x_2}{x_1}, -\frac{x_3}{x_1} \right\}$$

$$M_2(x_1, x_2, x_3) = \left\{ \frac{1}{x_2}, -\frac{x_1}{x_2}, -\frac{x_3}{x_2} \right\} \quad M_3(x_1, x_2, x_3) = \left\{ \frac{1}{x_3}, -\frac{x_1}{x_3}, -\frac{x_2}{x_3} \right\}$$

Then

$$\max_{i=0,\dots,3} (\min(M_i^{\parallel}(x_1, x_2, x_3))) \geq 1$$

where $M^{\parallel}$ consists of the absolute values of the elements of M and $\min(M^{\parallel})$ is the minimum of the set $M^{\parallel}$.

Proof. Using symmetry considerations we have the following four cases:

1.

$$|x_1| \geq 1 \quad |x_2| \geq 1 \quad |x_3| \geq 1$$

This implies $\min M_0^{\parallel}(x_1, x_2, x_3) \geq 1$.

2.

$$|x_1| \geq 1 \quad |x_2| \geq 1 \quad |x_3| \leq 1$$

In this case one can check that $\min M_3^{\parallel}(x_1, x_2, x_3) \geq 1$.

3.

$$|x_1| \geq 1 \quad |x_2| \leq 1 \quad |x_3| \leq 1$$

In this case we may also assume that $|x_3| \geq |x_2|$. Using this it is easy to see that $\min M_2^{\parallel}(x_1, x_2, x_3) \geq 1$.

4.

$$|x_1| \leq 1 \quad |x_2| \leq 1 \quad |x_3| \leq 1$$

In this case one can also assume that x_1 has the least absolute value. Then $\min M_1^{\parallel}(x_1, x_2, x_3) \geq 1$.

□

Corollary 1. *Let $x_1, x_2, x_3 \in \mathbb{C}^*$ be such that*

$$x_1 + x_2 + x_3 = 1.$$

Then there are $i \in \{0, \dots, 3\}$ and $u, v \in M_i(x_1, x_2, x_3)$ such that $\mathfrak{D}(u, v)$ is enumerable.

Proof. We apply the previous lemma for x_1, x_2, x_3 . Using symmetry considerations, we may also assume that $\min M_1^{\parallel}(x_1, x_2, x_3) \geq 1$. This also means that

$$\max\left(\frac{1}{|x_1|}, \frac{1}{|x_2|}, \frac{1}{|x_3|}\right) \leq 1 \text{ which yields}$$

$$\begin{aligned} \left| -\frac{x_2}{x_1} - \frac{x_3}{x_1} \right| &= \left| 1 - \frac{1}{x_1} \right| \leq 2, \\ \left| -\frac{x_1}{x_2} - \frac{x_3}{x_2} \right| &= \left| 1 - \frac{1}{x_2} \right| \leq 2, \\ \left| -\frac{x_1}{x_3} - \frac{x_2}{x_3} \right| &= \left| 1 - \frac{1}{x_3} \right| \leq 2. \end{aligned}$$

Using these equations one can see that if $u = -\frac{x_2}{x_1}$ and $v = -\frac{x_3}{x_1}$ then $\mathfrak{D} = \mathfrak{D}(u, v)$ is enumerable, since for every element of $\mathfrak{D}$ the desired other element is the one appearing in the same equation listed above. $\square$

Remark 1. *Using the above Corollary one can choose $\binom{3}{2} = 3$ such pairs of (u, v) -s from the four M_i -s. This gives $3 \cdot 4 = 12$ pairs. In fact by*

$$\mathfrak{D}(u, v) = \mathfrak{D}\left(\frac{1}{u}, -\frac{v}{u}\right) = \mathfrak{D}\left(\frac{1}{v}, -\frac{u}{v}\right)$$

we have only four possible pairs of (u, v) that generates pairwise different semi-orbits. These four pairs will be called the primitive pairs corresponding to (x_1, x_2, x_3) .

3.2.2 Reduction of enumerable semi-orbits

Lemma 6. *Let $x, y \in \mathbb{C}^*$, and let $S > s > 2$ be real numbers such that for all $z \in \mathfrak{D}^2(x, y)$*

$$\frac{1}{S} \leq |z| \leq S.$$

Then

1. either for all $z \in \mathfrak{D}^2(x, y)$ we have

$$\frac{1}{s} \leq |z| \leq s$$

2. or there is a $z \in \mathfrak{D}^2(x, y)$ such that

$$|\log |z|| \leq \frac{2}{s-2}$$

Proof. Suppose that the first case does not hold. Then there is an $u \in \mathfrak{D}^2(x, y)$ such that

$$s \leq |u| \leq S.$$

We also have a v in $\mathfrak{D}^2(x, y)$ such that

$$||u| - |v|| \leq |u + v| \leq 2 \quad \text{and} \quad \frac{u}{v} \in \mathfrak{D}^2(x, y).$$

By $s \leq |u|$ we also have

$$\min(|u|, |v|) \geq s - 2$$

and using Lagrange's Mean Value Theorem we get

$$\left| \log \frac{|u|}{|v|} \right| = |\log |u| - \log |v|| \leq \frac{1}{\min(|u|, |v|)} ||u| - |v|| \leq \frac{2}{s-2}.$$

Observe that $\frac{u}{v}$ is also in $\mathfrak{D}^2(x, y)$ so the second case of the statement of the lemma is satisfied with $z = \frac{u}{v}$. $\square$

This lemma shows the importance of the enumerable semi-orbits $\mathfrak{D}^2(x, y)$.

3.3 Unit equations in three variables

Let K be an algebraic number field of degree $[K : \mathbb{Q}] = d > 3$. In the following we construct a method to determine the "small" solutions of unit equations of type

$$u^{(1)} + u^{(2)} + u^{(3)} + u^{(4)} = 0 \tag{3.1}$$

where (and in the following) $u^{(i)}$ denotes the i -th conjugate of a unit $u \in K$. The diophantine equations we consider in Section 5 lead in fact to this special

type of unit equations (written in a homogeneous form). Without significant changes, our method can also be applied to general unit equations of the form

$$a_1u^{(1)} + a_2u^{(2)} + a_3u^{(3)} + a_4u^{(4)} = 0 \quad (3.2)$$

where the a_i -s are given elements in $\overline{K}$ (the normal closure of K).

Obviously, equation (3.1) can be written in the following four equivalent inhomogeneous forms:

$$\begin{aligned} -\frac{u^{(2)}}{u^{(1)}} - \frac{u^{(3)}}{u^{(1)}} - \frac{u^{(4)}}{u^{(1)}} &= 1, \\ -\frac{u^{(1)}}{u^{(2)}} - \frac{u^{(3)}}{u^{(2)}} - \frac{u^{(4)}}{u^{(2)}} &= 1, \\ -\frac{u^{(1)}}{u^{(3)}} - \frac{u^{(2)}}{u^{(3)}} - \frac{u^{(4)}}{u^{(3)}} &= 1, \\ -\frac{u^{(1)}}{u^{(4)}} - \frac{u^{(2)}}{u^{(4)}} - \frac{u^{(3)}}{u^{(4)}} &= 1. \end{aligned}$$

These are indeed special forms of *unit equations* in three variables.

Several types of decomposable form equations can be reduced to unit equations in three variables, for example norm form equations in three unknowns and resultant form equations. In Section 3.5 we outline an application of our method to norm form equations. For the application to resultant form equations see [55].

3.4 The enumeration method

Let r be the unit rank of K , and let $\varepsilon_i, i = 1, \dots, r$ be a system of fundamental units of K . It is important to remark that we do not really need the system of fundamental units. Without significant changes our method can be applied to a system of r independent units. See the corresponding paper of G.Hanrot [48].

Let $\mathfrak{D}$ be a set containing some nontrivial quotients of the units in equation (3.1), that is

$$\mathfrak{D} = \left\{ \frac{u^{(i)}}{u^{(j)}} \mid (i, j) \in \Gamma_{\mathfrak{D}} \right\}$$

where $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) | l = 1, \dots, g\}$ is a suitable index set. We shall call $\Gamma_{\mathfrak{D}}$ the *index set* corresponding to $\mathfrak{D}$. If such an $\mathfrak{D}$ is a union of semi-orbits then it will be called an *enumerable set*.

In the enumeration method we will need the following

Definition 1. Let $\mathfrak{D}$ be an enumerable set with corresponding index set $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) | l = 1, \dots, g\}$. By the rank of $\mathfrak{D}$ we mean the dimension of the vector space spanned by the vectors

$$\underline{e}_k = \begin{pmatrix} \log \left| \frac{\varepsilon_k^{(i_1)}}{\varepsilon_k^{(j_1)}} \right| \\ \vdots \\ \log \left| \frac{\varepsilon_k^{(i_g)}}{\varepsilon_k^{(j_g)}} \right| \end{pmatrix} \text{ for } k = 1, \dots, r.$$

In fact the rank of such an enumerable set can be exactly determined. Let $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) | l = 1, \dots, g\}$ be the corresponding index set. Let R be the regulator matrix of K i.e. $R_{ij} = \log(\varepsilon_j^{(i)})_{i,j=1}^r$. Let T be the matrix in which the l -th row contains 1 at the i_l -th place and -1 at j_l -th place, and the others are zeros for $l = 1, \dots, g$. Then the product $T \cdot R$ contains the vectors $\underline{e}_k$ as columns. Since the rank of R is the unit rank of K (so R has maximal rank) and the rank of T can be computed using integer arithmetic, the rank of $T \cdot R$ whence the rank of the enumerable set can be computed explicitly, as it will be the rank of T . In our numerical examples we used this method to compute the ranks.

3.4.1 Localizing the solutions of unit equations in three variables

The basic idea of the enumeration method was settled by K.Wildanger [85]. These ideas were further developed to the case of conjugate units by I.Gaál and M.Pohst [31], see also [25]. Here we extend these ideas to our case of unit equations in three variables.

Theorem 7. For every unit equation in three variables of type (3.1) and every $g \in \{1, \dots, d\}$ there are enumerable sets $\mathfrak{D}_1, \dots, \mathfrak{D}_{4^g}$ such that if u is a solution of (3.1) then there is an $i \in \{1, \dots, 4^g\}$ and g triples of indices (j_m, k_m, l_m)

for $m = 1, \dots, g$ with

$$\mathfrak{D}_i = \bigcup_{m=1}^g \mathfrak{D}^2\left(-\frac{u^{(j_m)}}{u^{(l_m)}}, -\frac{u^{(k_m)}}{u^{(l_m)}}\right).$$

Proof. Suppose that u is a solution of (3.1). To construct the enumerable sets choose some conjugates of (3.1), say the first g of them, where $1 \leq g \leq d$. Using the equivalent forms of this equation (see Section 3) one can apply Corollary 1 to the tuples

$$\left(-\frac{(u^{(2)})^{(i)}}{(u^{(1)})^{(i)}}, -\frac{(u^{(3)})^{(i)}}{(u^{(1)})^{(i)}}, -\frac{(u^{(4)})^{(i)}}{(u^{(1)})^{(i)}}\right)$$

for $i = 1, \dots, g$ where $(u^{(j)})^{(i)}$ is the image of $u^{(j)}$ under the Galois action of the normal closure of K which sends $u^{(1)}$ to $u^{(i)}$. For every tuple we have four possible primitive pairs

$$(v_{i_1}, w_{i_1}), (v_{i_2}, w_{i_2}), (v_{i_3}, w_{i_3}), (v_{i_4}, w_{i_4})$$

for $i = 1, \dots, g$. Now construct the 4^g enumerable sets by building the union of the semi-orbits generated by one of the four primitive pairs for every $i = 1, \dots, g$. Suppose they are given by $\mathfrak{D}_1, \dots, \mathfrak{D}_{4^g}$.

Since u is a solution of (3.1), for every $i = 1, \dots, g$ there is a primitive pair (u_{ji}, v_{ji}) such that $\mathfrak{D}(u_{ji}, v_{ji})$ is enumerable, so the enumerable set constructed with these primitive pairs is suitable. $\square$

Remark: In the above theorem g is arbitrary with $1 \leq g \leq d$. It is even possible to choose $g = 1$, but in that case it is too complicated to enumerate the possible solutions. Taking $g = d$ it is the easiest to enumerate the solutions in the enumerable sets, but then there are too many solutions. Therefore we have to make a compromise in choosing g .

This theorem localizes all (!) solutions of unit equations in three unknowns in finitely many enumerable sets. Equivalently, it is enough to deal with enumerable sets. Since there is no effective upper bound for the heights of the solutions, there is no hope to determine all solutions in this way. Our purpose is to calculate the "small" solutions with

$$A \leq A_0$$

where $A = \max(|a_1|, \dots, |a_r|)$ and $A_0 > 0$ is given, using the representation

$$\log |u^{(i)}| = a_1 \log |\varepsilon_1^{(i)}| + \dots + a_r \log |\varepsilon_r^{(i)}|.$$

We note that this bound on the absolute values of the exponents can be translated to a bound on the absolute values of the u_i -s and conversely. In our example $A_0 = 200$ which is a usual bound solving practically unit equations in two unknowns. In fact these "small" solutions usually cover all solutions (the experiments show that such equations only have "small" solutions) but we cannot prove that there are no "large" ones.

3.4.2 The enumeration lemma and its application

Lemma 7. *Let $S > s > 2$ and let $\mathfrak{D}$ be an enumerable set which is the union of enumerable semi-orbits. Suppose that for every $u \in \mathfrak{D}$ we have*

$$\frac{1}{S} \leq |u| \leq S.$$

Then

1. *either for all $u \in \mathfrak{D}$*

$$\frac{1}{s} \leq |u| \leq s$$

2. *or there is a $u \in \mathfrak{D}$ such that*

$$|\log |u|| \leq \frac{2}{s-2}.$$

Proof. Since $\mathfrak{D}$ is the union of enumerable semi-orbits, one can use Lemma 2. □

This lemma can be applied in the following way (we detail only the totally real case, the complex case is similar):

Let $S_0 > S_1 > \dots > S_m > 2$ be a sequence of positive numbers such that

$$\frac{1}{S_0} \leq \left| \frac{u^{(i)}}{u^{(j)}} \right| \leq S_0 \quad \text{for all possible } i, j.$$

Such an S_0 can be determined by

$$\log S_0 = A_0 \max \left(\left| \log \left| \frac{\varepsilon_1^{(i)}}{\varepsilon_1^{(j)}} \right| \right| + \cdots + \left| \log \left| \frac{\varepsilon_r^{(i)}}{\varepsilon_r^{(j)}} \right| \right| \right), \quad (3.3)$$

where A_0 is the maximum of the exponents mentioned above.

The constant S_{n-1} can be replaced by the smaller constant S_n if for each $(i_0, j_0) \in \Gamma_{\mathfrak{D}}$ we enumerate directly the set $H_{i_0 j_0}$ of those exponent vectors $(a_1, \dots, a_r)$ for which

$$\frac{1}{S_{n-1}} \leq \left| \frac{u^{(i)}}{u^{(j)}} \right| \leq S_{n-1} \text{ for all } (i, j) \in \Gamma_{\mathfrak{D}} \text{ and } \left| \log \left| \frac{u^{(i_0)}}{u^{(j_0)}} \right| \right| \leq \frac{2}{S_n - 2}.$$

We show that such exponent vectors are contained in an ellipsoid. To enumerate the points of this ellipsoid we use the algorithm of U.Fincke and M.Pohst [18]. The application of this lemma is similar as in [31], see also [25].

In order to be able to use the above lemma, the union of a d -tuple of enumerable semi-orbits has to have full rank. Note that since this union is an enumerable set, it has a well defined rank, see the beginning of Section 4. In our example we always found d -tuples with rank less than r . In that case one has to add some more $-\frac{u^{(i')}}{u^{(j')}} to $\mathfrak{D}$ to make its rank full. These will be called *additional elements*. For details see the numerical results in Section 5.2.$

For this purpose let $\mathfrak{D}'$ be the set of additional elements such that $\mathfrak{D} \cup \mathfrak{D}'$ has full rank. Denote by $\Gamma_{\mathfrak{D} \cup \mathfrak{D}'} = \{(i_1, j_1), \dots, (i_t, j_t)\}$ the index set corresponding to $\mathfrak{D} \cup \mathfrak{D}'$ and let (i_0, j_0) be a fixed pair in $\Gamma_{\mathfrak{D}}$. Further let

$$\underline{e}_h = \begin{pmatrix} \log \left| \frac{\varepsilon_h^{(i_1)}}{\varepsilon_h^{(j_1)}} \right| \\ \vdots \\ \log \left| \frac{\varepsilon_h^{(i_t)}}{\varepsilon_h^{(j_t)}} \right| \end{pmatrix} \text{ for } h = 1, \dots, r,$$

$$\lambda_p = \begin{cases} \frac{1}{\log S_{n-1}} & \text{for } (i_p, j_p) \neq (i_0, j_0) \text{ and } (i_p, j_p) \in \Gamma_{\mathfrak{D}} \\ \frac{S_n - 2}{2} & \text{for } (i_p, j_p) \neq (i_0, j_0) \\ \frac{1}{\log S_0} & \text{for } (i_p, j_p) \in \Gamma_{\mathfrak{D}'} \end{cases}$$

$$\phi_{i_0 j_0}(\underline{b}) = \begin{pmatrix} \lambda_1 \log \left| \frac{u^{(i_1)}}{u^{(j_1)}} \right| \\ \vdots \\ \lambda_t \log \left| \frac{u^{(i_t)}}{u^{(j_t)}} \right| \end{pmatrix}$$

and

$$\phi_{i_0 j_0}(\underline{e}_k) = \begin{pmatrix} \lambda_1 \log \left| \frac{\varepsilon_k^{(i_1)}}{\varepsilon_k^{(j_1)}} \right| \\ \vdots \\ \lambda_t \log \left| \frac{\varepsilon_k^{(i_t)}}{\varepsilon_k^{(j_t)}} \right| \end{pmatrix} \quad \text{for } k = 1, \dots, r$$

Since $\underline{e}_1, \dots, \underline{e}_r$ are linearly independent, so are their images. So we have

$$\phi_{i_0 j_0}(\underline{b}) = a_1 \phi_{i_0 j_0}(\underline{e}_1) + \dots + a_r \phi_{i_0 j_0}(\underline{e}_r).$$

Moreover, we have

$$|a_1 \phi_{i_0 j_0}(\underline{e}_1) + \dots + a_r \phi_{i_0 j_0}(\underline{e}_r)|^2 = |\phi_{i_0 j_0}(\underline{b})|^2 = \sum_{p=0}^t \lambda_p^2 \log^2 \left| \frac{u^{(i_p)}}{u^{(j_p)}} \right| \leq t$$

which means that the $(a_1, \dots, a_r)$ are contained in an ellipsoid which we can enumerate by the method of U.Fincke and M.Pohst [18].

After this we have to consider the smallest solutions, for which

$$\frac{1}{3} \leq \left| \frac{u^{(i)}}{u^{(j)}} \right| \leq 3 \quad \text{for all } (i, j) \in \Gamma_{\mathfrak{D}}.$$

In this case there are two possibilities:

- 1 If the set $\mathfrak{D}$ has full rank, then the corresponding exponent vectors can be covered by an ellipsoid, for details see [85],[25].
- 2 If the set $\mathfrak{D}$ has rank $r_1 < r$, then one should choose a generating subset of the vectors $\{\underline{e}_i | i = 1, \dots, r\}$ (here the $\underline{e}_i$ -s have coordinates corresponding only to $\mathfrak{D}$). Suppose that the first r_1 vectors are linearly independent. This means that there are $\mu_{kl} \in \mathbb{R}$ such that

$$\underline{e}_{r_1+i} = \mu_{i1}\underline{e}_1 + \dots + \mu_{ir_1}\underline{e}_{r_1} \quad \text{for } i = 1, \dots, r - r_1$$

so for every $(a_{r_1+1}, \dots, a_r) \in ([-A, A] \cap \mathbb{Z})^{r-r_1}$ the vector

$$a_{r_1+1}\underline{e}_{r_1+1} + \dots + a_r\underline{e}_r$$

is a linear combination of the vectors $\underline{e}_1, \dots, \underline{e}_{r_1}$. Then for every fixed $(a_{r_1+1}, \dots, a_r) \in ([-A, A] \cap \mathbb{Z})^{r-r_1}$ one has to construct the ellipsoids using the vectors

$$a_1\underline{e}_1 + \dots + a_{r_1}\underline{e}_{r_1} + a_{r_1+1}\underline{e}_{r_1+1} + \dots + a_r\underline{e}_r$$

which will define ellipsoids containing only the exponent vectors $(a_1, \dots, a_{r_1})$.

3.5 Application to norm form equation

3.5.1 Norm form equations in three unknowns

In the following we use the results of the previous sections to enumerate the "small" solutions of a given norm form equation in three variables.

Let $K = \mathbb{Q}(\alpha)$ be a totally real quintic number field, and let $\alpha \in \mathbb{Z}_K$. In the following we would like to determine the small solutions of the equation

$$N_{K/\mathbb{Q}}(x_1 + \alpha x_2 + \alpha^2 x_3) = \pm 1$$

in the integer unknowns x_1, x_2, x_3 . We note that one can substitute ± 1 by any given integer $m \neq 0$ and can use our method without significant changes.

For any $\gamma \in K$ denote by $\gamma^{(i)}$ its conjugate for $i = 1, \dots, 5$. Then

$$N_{K/\mathbb{Q}}(x_1 + \alpha x_2 + \alpha^2 x_3) = \prod_{i=1}^5 (x_1 + \alpha^{(i)} x_2 + (\alpha^{(i)})^2 x_3)$$

holds. Using this we can write

$$x_1 + \alpha^{(i)} x_2 + (\alpha^{(i)})^2 x_3 = \pm \left(\varepsilon_1^{(i)} \right)^{a_1} \dots \left(\varepsilon_4^{(i)} \right)^{a_4} \quad (3.4)$$

where $\varepsilon_1, \dots, \varepsilon_4$ is a system of fundamental units of K , the a_k -s are in $\mathbb{Z}$.

Let i, j, k, l be four distinct indices from the index set $\{1, 2, 3, 4, 5\}$ such that $i \leq j \leq k \leq l$. Let

$$u^{(i)} = \prod_{p=1}^4 (\varepsilon_p^{(i)})^{a_p},$$

and

$$|1, \alpha, \alpha^2|^{(jkl)} = \begin{vmatrix} 1 & \alpha^{(j)} & (\alpha^{(j)})^2 \\ 1 & \alpha^{(k)} & (\alpha^{(k)})^2 \\ 1 & \alpha^{(l)} & (\alpha^{(l)})^2 \end{vmatrix}.$$

Then using standard arguments one has

$$u^{(i)}|1, \alpha, \alpha^2|^{(jkl)} - u^{(j)}|1, \alpha, \alpha^2|^{(ikl)} + u^{(k)}|1, \alpha, \alpha^2|^{(ijl)} - u^{(l)}|1, \alpha, \alpha^2|^{(ijk)} = 0 \quad (3.5)$$

and to this equation we use our method with $A = \max_{i=1,\dots,4}(|a_i|) \leq A_0 = 200$.

We note that if one would try all the $(2 \cdot 200 + 1)^4 = 25856961601 \approx 2.6 \cdot 10^{10}$ possibilities for the exponent vectors, then the test would take about 2600 days on the same machine we have used.

3.5.2 A numerical example

Let K be generated by a root α of $x^5 - 5x^3 + x^2 + 3x - 1$. This is a totally real quintic field with unit rank 4. Consider the equation

$$N_{K/\mathbb{Q}}(x + y\alpha + z\alpha^2) = \pm 1. \quad (3.6)$$

Using our method we have enumerated all solutions of (3.6) with

$$X = \max(|x|, |y|, |z|) \leq 10^{10}. \quad (3.7)$$

Applying standard tools one can see that this set is covered by

$$A = \max(|a_1|, |a_2|, |a_3|, |a_4|) \leq A_0 = 200$$

where the a_i -s correspond to the representation (3.4).

We have used 2 of the 5 conjugates of the unit equation (3.5) so we had to perform $4^2 = 16$ reduction and enumeration processes.

In six of the processes the set $\mathfrak{D}$ (the union of the enumerable semi-orbits) had rank 4, so we did not need any additional terms. In these cases the CPU time was quite short, about 2 minutes on a Celeron 800 Mhz processor.

In nine of the processes the set $\mathfrak{D}$ had rank 3, so we had to choose one more additional term. In these cases the average CPU time was about 2 hours per process, using the same machine. Since the rank of $\mathfrak{D}$ is 3, the enumeration of the smallest ellipsoid took more time. The average CPU time of the enumeration of the smallest ellipsoids were 12 minutes.

In one of the processes the set $\mathfrak{D}$ had rank 2, so we had to choose two additional terms in this case. The CPU time was about 124 hours. The enumeration of the smallest ellipsoid took 30 hours.

In the enumeration processes we have also used a simple modular sieve to test the vector found in the ellipsoids.

Finally we summarize the solutions of equation (3.6) we have found:

$$\begin{aligned} (x, y, z) \in \{ & (-1, 5, -5), (2, -3, -6), (0, 1, -1), (2, -2, -1), (3, -3, -2), \\ & (1, -1, -1), (1, -2, 1), (1, 1, 0), (1, -1, 0), (2, 1, -1), (0, 1, 1), \\ & (1, -2, -1), (2, -1, 0), (1, 0, -2), (0, 0, 1), (1, 0, 0), (1, 2, 1), \\ & (4, -4, 1), (-4, 9, 5), (-1, 2, 2), (0, 2, -1), (1, 0, -1), (0, 1, 0), \\ & (-2, 8, -7), (2, -3, 1), (1, -3, 1)\}. \end{aligned}$$

The total CPU time was 175 hours on a PC with a Celeron 800 Mhz processor. We implemented the method in Maple and executed the programs in Windows.

3.6 Application to resultant form equations

We will solve the following problem:

Let M_1 and M_2 be cubic algebraic number fields. Let $K = M_1M_2$ be the composite of M_1 and M_2 . Assume that the degree of K is 9, and denote by r its unit rank. Our purpose is to determine the "small" solutions of the equation

$$Res(f_1, f_2) = \pm 1 \tag{3.8}$$

in monic cubic polynomials f_1, f_2 with integer coefficients, such that a root of f_i generates M_i ($i = 1, 2$). We note that our method can be applied without significant changes to the same problem with a given integer a in place of ± 1 on the right hand side, i.e. to the equation

$$Res(f_1, f_2) = a.$$

Let $\alpha^{(i)}$ and $\beta^{(i)}$ ($i = 1, 2, 3$) denote the roots of f_1 and f_2 , respectively. Then

$$Res(f_1, f_2) = \prod_{i=1}^3 \prod_{j=1}^3 (\alpha^{(i)} - \beta^{(j)})$$

holds. For any $\gamma \in K$ denote by $\gamma^{(ij)}$ its conjugate corresponding to $\alpha^{(i)}, \beta^{(j)}$ ($1 \leq i, j \leq 3$). Then we can write

$$\alpha^{(i)} - \beta^{(j)} = \pm \left(\eta_1^{(ij)} \right)^{a_1} \cdots \left(\eta_r^{(ij)} \right)^{a_r}$$

where $\eta_k^{(ij)}$ is a system of fundamental units of K and $a_k \in \mathbb{Z}$ ($k = 1, \dots, r$).

As an analogue of Siegel's identity in our case we have:

$$(\alpha^{(i)} - \beta^{(k)}) + (\alpha^{(j)} - \beta^{(l)}) - (\alpha^{(i)} - \beta^{(l)}) - (\alpha^{(j)} - \beta^{(k)}) = 0.$$

That is

$$\mu^{(ij)} + \mu^{(kl)} - \mu^{(il)} - \mu^{(jk)} = 0 \quad (3.9)$$

with $\mu^{(mn)} = \alpha^{(m)} - \beta^{(n)}$. Since the $\mu^{(mn)}$ are the conjugates of a suitable unit of $\mathbb{Z}_K$, (3.9) is a unit equation in three variables (in homogeneous form) for which we can apply our method.

We call a solution (f_1, f_2) of (3.8) "small" if $\max(H(f_1), H(f_2)) \leq H_0$, where $H(f)$ is the maximum of the absolute values of the coefficients of f and H_0 is a given constant. In our numerical example we set $H_0 = 10^{85}$. Clearly, in this case searching directly for the "small" solutions is hopeless.

3.7 Improvements of the method

3.7.1 Decreasing the number of enumerable sets

First let us see what it means if we fix an enumerable semi-orbit using Corollary 1 of [56]. For this purpose let u be a solution of (3.1), that is

$$-\frac{u^{(1)}}{u^{(4)}} - \frac{u^{(2)}}{u^{(4)}} - \frac{u^{(3)}}{u^{(4)}} = 1.$$

We apply Corollary 2.2 of [56] to this equation with

$$x_i = -\frac{u^{(i)}}{u^{(4)}} \quad (i = 1, 2, 3).$$

We obtain that one of the four pairs

$$\left(-\frac{u^{(2)}}{u^{(1)}}, -\frac{u^{(3)}}{u^{(1)}}\right), \left(-\frac{u^{(2)}}{u^{(4)}}, -\frac{u^{(3)}}{u^{(4)}}\right), \left(-\frac{u^{(1)}}{u^{(3)}}, -\frac{u^{(4)}}{u^{(3)}}\right), \left(-\frac{u^{(1)}}{u^{(2)}}, -\frac{u^{(4)}}{u^{(2)}}\right)$$

say $(-\frac{u^{(2)}}{u^{(1)}}, -\frac{u^{(3)}}{u^{(1)}})$, generates an enumerable semi-orbit. This property is equivalent to

$$\left| -\frac{u^{(1)}}{u^{(3)}} \right| \geq 1, \quad \left| -\frac{u^{(2)}}{u^{(3)}} \right| \geq 1, \quad \left| -\frac{u^{(4)}}{u^{(3)}} \right| \geq 1$$

or

$$\left| u^{(1)} \right| \geq \left| u^{(3)} \right|, \quad \left| u^{(2)} \right| \geq \left| u^{(3)} \right|, \quad \left| u^{(4)} \right| \geq \left| u^{(3)} \right|. \quad (3.10)$$

In other words, fixing a primitive pair is equivalent to fixing an $u^{(i)}$ with the least absolute value.

In our method we use enumerable sets which are the unions of enumerable semi-orbits corresponding to different conjugates of equation (3.1). Let $\mathfrak{D}$ be such an enumerable set:

$$\mathfrak{D} = \bigcup_{i=1}^g \mathfrak{D}^2(-\frac{u^{(j_i)}}{u^{(k_i)}}, -\frac{u^{(l_i)}}{u^{(k_i)}}).$$

By the above formulas, fixing an enumerable set is equivalent to choosing the unit with smallest absolute value from $\{(u^{(1)})^{(i)}, (u^{(2)})^{(i)}, (u^{(3)})^{(i)}, (u^{(4)})^{(i)}\}$ for each $i = 1, \dots, g$. For every fixed conjugation we obtain a system of inequalities similar to (3.10). After combining these inequalities, we may obtain two conjugates of u -say $u^{(i)}$ and $u^{(j)}$ - appearing in the same equation

$$u^{(i)} + u^{(j)} + u^{(k)} + u^{(l)} = 0. \quad (3.11)$$

Here

$$\left| u^{(i)} \right| \geq \left| u^{(j)} \right| \quad \text{and} \quad \left| u^{(j)} \right| \geq \left| u^{(i)} \right|$$

hold, whence

$$\left| u^{(i)} \right| = \left| u^{(j)} \right|.$$

Let $\varepsilon = \frac{u^{(i)}}{u^{(j)}}$. Then ε is a unit in $\mathbb{Z}_{\overline{K}}$ ($\overline{K}$ is the normal closure of K) with $|\varepsilon| = 1$, so it is a root of unity. However, this means that (3.11) can be written as

$$(1 + \varepsilon)u^{(i)} + u^{(k)} + u^{(l)} = 0$$

which is a unit equation in two unknowns (in homogeneous form). When $u^{(i)}$ and $u^{(j)}$ are real units then $\varepsilon = \pm 1$ so (3.11) reduces either to

$$u^{(k)} + u^{(l)} = 0$$

or to

$$2u^{(j)} + u^{(k)} + u^{(l)} = 0.$$

Hence none of these equations can be a conjugate of (3.1), so we have a contradiction. This means this $\mathfrak{D}$ can be dropped. In Section 3.8 we detail a numerical example and there one can see that using this consideration we dropped quarter of the enumerable sets.

3.7.2 Enumerable sets of small rank

In the following we show how one can substitute a given enumerable set with four new enumerable sets of rank which is greater than or equal to the original one's rank. If all of the four new enumerable sets have greater ranks then there is a better chance to enumerate the possible solutions in them in reasonable time.

Lemma 8. *Let u be a solution to (3.1). Using the first $d_1 < d$ conjugates of (3.1) construct the 4^{d_1} enumerable sets as in Theorem 4.2 in [56]. Let $\mathfrak{D}$ be one of them. Then there are enumerable sets $\mathfrak{D}_1, \mathfrak{D}_2, \mathfrak{D}_3, \mathfrak{D}_4$ such that*

$$\mathfrak{D} \subset \bigcup_{i=1}^4 \mathfrak{D}_i$$

and $\mathfrak{D}_i$ has rank greater than or equal to the rank of $\mathfrak{D}$ for $i = 1, \dots, 4$.

Proof. Construct the four enumerable semi-orbits by the help of one of the remaining $d - d_1$ conjugates of equation (3.1) using Theorem 4.2 of [56] for a $g \in \{d_1 + 1, \dots, d\}$. Let these semi-orbits be

$$\mathfrak{D}_1^2, \mathfrak{D}_2^2, \mathfrak{D}_3^2, \mathfrak{D}_4^2.$$

Then put

$$\mathfrak{D}_1 = \mathfrak{D} \cup \mathfrak{D}_1^2, \quad \mathfrak{D}_2 = \mathfrak{D} \cup \mathfrak{D}_2^2, \quad \mathfrak{D}_3 = \mathfrak{D} \cup \mathfrak{D}_3^2, \quad \mathfrak{D}_4 = \mathfrak{D} \cup \mathfrak{D}_4^2.$$

It is easy to see that

$$\mathfrak{D} \subset \bigcup_{i=1}^4 \mathfrak{D}_i.$$

Since in each $\mathfrak{D}_i$ there are more elements than in $\mathfrak{D}$ so their ranks are greater than or equal to the rank of $\mathfrak{D}$. $\square$

3.8 A numerical example

We take M_1 to be generated by a root of $x^3 - x^2 - 6x + 5$ and M_2 to be generated by a root of $x^3 - 9x + 6$. One can check that M_1 and M_2 are totally real cubic fields, so their unit rank $r = 8$.

Using the improvements of the method, we computed the "small" solutions of the equation

$$\text{Res}(f_1, f_2) = \pm 1$$

where the f_i -s are monic polynomials with integer coefficients such that a root of f_i generates M_i ($i = 1, 2$), and

$$\max(H(f_1), H(f_2)) \leq 10^{85}. \quad (3.12)$$

As we explained in Section 2, our problem can be reduced to finding the "small" solutions of the equation

$$\mu^{(ij)} + \mu^{(kl)} - \mu^{(il)} - \mu^{(jk)} = 0$$

with $\mu^{(mn)} = \alpha^{(m)} - \beta^{(n)} \in (M_1)^{(m)}(M_2)^{(n)}$. Since the $\mu^{(mn)}$ are conjugates of a suitable unit from $\mathbb{Z}_K$, this equation is a unit equation in three variables (in homogeneous form). Thus we obtain

$$\alpha^{(i)} - \beta^{(j)} = \pm \left(\eta_1^{(ij)}\right)^{a_1} \cdots \left(\eta_8^{(ij)}\right)^{a_8}$$

where $\eta_k^{(ij)}$ is a system of fundamental units of K and $a_k \in \mathbb{Z}$ ($k = 1, \dots, 8$). Using standard tools from (3.12) one can get a bound A_0 such that

$$\max_{i=1, \dots, 8} (|a_i|) \leq A_0.$$

In this case we have $A_0 = 200$ which is a typical bound in the case of unit equations in two variables obtained by the help of Baker's theory and LLL-reduction due to de Weger. For details see [25].

Now we apply our method. We take four conjugates of the unit equation. This yields 256 enumerable set. In the following table we summarize the number of enumerable sets without the recent improvements (second row), applying the first improvement (Section 3.7.1, third row) and applying both

improvements of this paper (Section 3.7.1 and 3.7.2, fourth row).

	# of e. s. of rank 8 (18 m)	# of e. s. of rank 7 (36 m)	# of e. s. of rank 6 (23 h 20 m)	# of e. s. of rank 5 (∞)	Total # of e.s.	Total CPU Time
none	30	145	74	7	256	∞
4.1	12	109	68	7	196	∞
4.1 + 4.2	12	125	70	0	207	72 days

In the first row in the brackets one can find the average CPU time on a 700 MHz Xeon processor of a single enumerable set of the corresponding rank (∞ stands for too much CPU time), and "e.s." stands for enumerable sets.

In the second row one can find the number of enumerable sets using the method of [56] of the corresponding rank. In the third row one can find the number of enumerable sets using our first improvement (Section 3.7.1). The last row contains the number of enumerable sets using both new improvements (Sections 3.7.1 and 3.7.2). It is clear from the table that our improvements are really essential.

We have found two solutions: $(f(x), g(x)) = (x^3 + x^2 - 6x - 5, x^3 - 9x + 6)$ and $(x^3 + 2x^2 - 9x + 5, x^3 - 9x + 6)$.

Chapter 4

On the diophantine equation

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

4.1 Introduction

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

$$x^n = Dy^2 + 1 \tag{4.1}$$

in integers x, y . This equation is a special hyperelliptic equation:

$$f(x) = by^n \tag{4.2}$$

This general equation was investigated by many authors. It was A.Baker in 1969 who gave the first explicit upper bound on the solutions of (4.2). When n is also unknown, it can be bounded. This is the famous theorem of A.Schinzel and R.Tijdeman [72]. Y.Bilu and G.Hanrot [4] gave an algorithm for the practical solutions of hyperelliptic equations.

Equation (4.1) is also a special case of

$$ax^2 + b = cy^n \tag{4.3}$$

Several results are known on the solutions of this equation, we refer to [9], [10], [11], [58], [59], [61], [62], [65], [88]. Another interesting case is the equation

$$x^2 + a^2 = 2y^n.$$

This case was investigated by I. Pink and Sz. Tengely [71].

Using elementary and algebraic number theoretical tools J.H.E. Cohn [12] proved necessary conditions for the unsolvability of (4.1). Moreover, he solved (4.1) completely for $D \leq 100$ up to the six pairs

$$(n, D) = (3, 31), (5, 31), (3, 38), (3, 61), (5, 71) \text{ and } (7, 71)$$

and parity conditions on x . We summarize our results in the following Theorem.

Theorem 8. *Apart from $(x, y) = (1, 0)$ equation (4.1) has the solutions*

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

This confirms the conjecture of Cohn [12] on the solutions of (4.1).

To prove the theorem recently developed techniques of numerical diophantine analysis are used. Notice that if $n = 3$ then (4.1) is an elliptic curve in canonical form over $\mathbb{Q}$ and if $n = 5$ then we can transform it by using a straightforward argument to some curve of genus one. In the case $n = 3$ one can use directly the method developed by J. Gebel, A. Pethő, H.G. Zimmer [33] and R.J. Stroeker and N. Tzanakis [78].

The equation

$$(D^2y)^2 = (Dx)^3 - D^3$$

was solved by Gebel, Pethő and Zimmer [34] for $D = 31$ and $D = 38$ assuming the Birch and Swinnerton-Dyer conjecture. This is equivalent to (4.1) for $(n, D) = (3, 31)$ and $(3, 38)$. To avoid the Birch and Swinnerton-Dyer conjecture in the above cases and to handle $(n, D) = (3, 61)$ we used J. Cremona's program *mwrank* combined with the method of [34].

If $n = 5$, then (4.1) can be easily transformed to some equations of the form

$$v^2 = Q(u),$$

where Q is a quartic polynomial with integer coefficients. We solve the resulting equations partly by referring to results of Cohn's paper and partly by

using the method of N. Tzanakis [80], which was implemented by the first author in the computer algebra system MAGMA [6].

When $n = 7$ we use the arguments of M. Mignotte and B.M.M. de Weger [67] and we reduce our equation to several Thue equations.

We are very grateful to Professor Walsh for calling our attention to the paper of Cohn.

4.2 The cases $n = 3$.

Cohn was not able to solve completely the equations

$$\mathcal{E}'_D : x^3 = Dy^2 + 1, \quad \text{with } D = 31, 38, 61 \text{ and } x \text{ odd.} \quad (4.4)$$

Multiplying both sides of (4.4) by D^3 we obtain

$$(Dx)^3 = (D^2y)^2 + D^3,$$

which with the notation $Dx = u$, $D^2y = v$ has the shape

$$\mathcal{E}_D : v^2 = u^3 - D^3. \quad (4.5)$$

Equation (4.5) represents a Mordell's equation $v^2 - u^3 = k$ and the integer points of this kind of equation were computed by Gebel, Pethő and Zimmer [33] for $|k| \leq 10^5$ provided that the Birch and Swinnerton-Dyer conjecture is true. For the values 31 and 38 the inequality $D^3 < 10^5$ holds, hence $|u| \leq 3.791 \cdot 10^9$ by [33, Table 8]. Using J. Cremona's *mwrank* [68] we checked the computation of [33] and observed that the results coincide, but now without the assumption of the Birch and Swinnerton-Dyer conjecture.

For $D = 61$ the value of D^3 is larger than 10^5 , hence we computed the solution of (4.5) in this case by using the computer algebra system MAGMA. We note that for $D \in \{31, 38, 61\}$ the torsion sub-group $\mathcal{E}_D^{\text{tors}}(\mathbb{Q})$ has order two and is generated by the point $(D, 0)$. The results of our computations are listed in Table 1.

TABLE 1.

D	$\mathcal{E}_D(\mathbb{Q})/\mathcal{E}_D^{\text{tors}}(\mathbb{Q})$	$\mathcal{E}_D(\mathbb{Z})$	$\mathcal{E}'_D(\mathbb{Z})$
31	$\langle (155, 1922) \rangle$	$(31, 0), (155, \pm 1922)$	$(1, 0), (5, \pm 2)$
38	$\langle (57, 361) \rangle \times \langle (522, 11924) \rangle$	$(522, \pm 11924), (38, 0)$ $(57, \pm 361), (266, \pm 4332)$	$(1, 0), (7, \pm 3)$
61	$\langle (\frac{610}{8}, \frac{3721}{8}) \rangle \times \langle (\frac{4230480540}{3796416}, \frac{141208887617}{3796416}) \rangle$	$(793, \pm 22326), (61, 0)$	$(1, 0), (13, \pm 6)$

4.3 The case $n = 5$.

In Cohn's paper two equations remain unsolved:

$$x^5 = 31y^2 + 1 \quad \text{and} \quad (4.6)$$

$$x^5 = 71y^2 + 1. \quad (4.7)$$

In both cases he did not determine the solutions with even x . Equations (4.6) and (4.7) have the common shape

$$x^5 - 1 = py^2.$$

By computing the factorization of the left hand side of this equation we obtain

$$(x - 1)(x^4 + x^3 + x^2 + x + 1) = py^2.$$

For integers x the greatest common divisor of $x - 1$ and $x^4 + x^3 + x^2 + x + 1$ is 1 or 5. Hence, it remains to consider the following systems of diophantine equations:

$$(I) \begin{cases} y_1^2 &= x - 1 \\ py_2^2 &= x^4 + x^3 + x^2 + x + 1 \end{cases}$$

$$(II) \begin{cases} py_1^2 &= x - 1 \\ y_2^2 &= x^4 + x^3 + x^2 + x + 1 \end{cases}$$

$$(III) \begin{cases} 5y_1^2 &= x - 1 \\ 5py_2^2 &= x^4 + x^3 + x^2 + x + 1 \end{cases}$$

$$(IV) \begin{cases} 5py_1^2 &= x - 1 \\ 5y_2^2 &= x^4 + x^3 + x^2 + x + 1. \end{cases}$$

The second equation of (II) is not solvable for even x by Lemma 2.3 [12]. For the second equation of (IV) we can apply Corollary 3 of [12] and conclude that its only solution is $(y_1, y_2) = (0, 1)$.

Therefore we have to deal in the sequel only with the equations (I) and (III) for $p = 31$ and 71 . To obtain the integral solutions of the occurring quartic elliptic equations we follow closely the arguments from the article of N. Tzanakis [80]. Since for each curve the calculation is similar we explain the method only for the equation

$$355y^2 = x^4 + x^3 + x^2 + x + 1 \quad (4.8)$$

which is, by putting $Y = 355y$ also given in the more suitable form

$$Y^2 = 355(x^4 + x^3 + x^2 + x + 1).$$

To apply the algorithm from [80] we have to find a non-trivial rational point on this curve. By a direct search the point $(-26/9, 11005/81)$ was found. We put

$$u = 9x \quad \text{and} \quad v = 81Y = 28755y.$$

This results in the quartic elliptic equation

$$\mathcal{Q} : v^2 = 355u^4 - 33725u^3 + 1219425u^2 - 19714925u + 121110025 =: Q(u) \quad (4.9)$$

for which we can apply the algorithm of Tzanakis. Note that $(0, 11005)$ is a rational point on this curve.

Using the birational map

$$\begin{aligned} x' &= \frac{22010\sqrt{Q(u)} - 19714925u + 22010}{u^2} + 406475 =: f^*(u) \\ y' &= - \frac{484440100\sqrt{Q(u)} + 5331263300500 - 433925499250u + \frac{569183383625}{62u^2}}{u^3} \\ &\quad + \frac{55535}{62}x' + \frac{437315625}{62} \end{aligned}$$

we obtain the elliptic curve

$$\mathcal{E} : y'^2 = x'^3 - 2756166750x' - 22014881915625 =: g(x')$$

which is in canonical form. Applying Cremona's program *mwrank* [68] we get that $\mathcal{E}$ has rank one over the rational numbers and that a generator of the infinite part of the Mordell-Weil group is given by

$$P_1 = (890919999/14161, -12337932682818/1685159).$$

The torsion sub-group has order two and is generated by $T = (-47925, 0)$.

The main idea of [80] is to express the elliptic integral related to the quartic elliptic equation by real values of elliptic logarithms u_i of points of $\mathcal{E}(\mathbb{R})$. Denote by ω the fundamental real period of the Weierstraß $\wp$ -function associated to $\mathcal{E}$ and by e_1 the largest real root of the equation $g(t) = 0$. Then by [89] we can define for every point $P = (x_P, y_P) \in \mathcal{E}(\mathbb{R})$ with $x_P \geq e_1$ the elliptic logarithm of P by

$$\psi(P) \equiv \pm \frac{1}{\omega} \int_{x_P}^{\infty} \frac{dt}{\sqrt{g(t)}} \pmod{1}.$$

We need some further notation. Denote by $(U, V) \in \mathcal{Q}(\mathbb{Z})$ an integral solution of equation (4.9) and by $P \in \mathcal{E}(\mathbb{R})$ the corresponding point on $\mathcal{E}$. Further let P_0 be the point $(x_0, y_0) = (22010\sqrt{355}+406475, 19714925\sqrt{355}+371143625) \in \mathcal{E}(\mathbb{R})$. We assume in this sequel that U is a positive integer. Then, by a simple but tedious calculation we have

$$\int_U^{\infty} \frac{du}{\sqrt{Q(u)}} = - \int_{x_0}^{f^*(U)} \frac{dt}{\sqrt{g(t)}}$$

if $U > 55$. Checking the criteria from [80] we see that relation (13) in [80] holds. Moreover, either P or $P + T$ may be written as $m_1 P_1$ for a suitable integer $m_1 \in \mathbb{Z}$. It follows

$$- \int_U^{\infty} \frac{du}{\sqrt{Q(u)}} = \psi(P_0) + m_1 \psi(P_1) + m_0 \omega.$$

Since P_0 and P_1 are linearly independent over the rational numbers the last equation defines already a linear form in elliptic logarithms. The values of these logarithms are given by

$$\omega = 0.09850931 \dots, \psi(P_0) = 0.00993580 \dots \quad \text{and} \quad \psi(P) = 0.05808409 \dots$$

Following the arguments in [80], we can derive an upper bound for the absolute value of the occurring linear form. A combination of this upper bound and the lower bound for linear forms in elliptic logarithms due to S. David [15] results in the upper bound $M \leq 10^{26}$ for the size of the absolute value $|m_1|$. From the normalization of the elliptic logarithm it is an immediate consequence that $|m_0|$ is bounded by $M + 1$. Applying two times standard reduction techniques in combination with Proposition 4 of [80] we are able to reduce the initial bound on M to 3. We compute all linear combinations m_1P_1 and $m_1P_1 + T$ for $|m_1| \leq 3$, map these points back to the quartic elliptic equation and check if we found an integral solution or not. Finally, we have to make sure that we found all 'small solutions'. This can be done by checking if $Q(u)$ is a square for integer values $0 \leq u \leq 55$. The calculation showed that the only integral solutions of equation (4.9) are given by $(0, \pm 11005)$.

Remark 2. *In the last computations we assumed $U > 0$. For negative values of U we have to do the same calculations for the quartic equation $v^2 = Q(-u)$. The computations for this curve have been done too and did not yield any new solutions. It follows that equation (4.8) has no integral solutions.*

The three remaining quartic elliptic equations were solved analogously. It turned out that all curves correspond to elliptic curves in canonical form with rank one over the rational numbers. Finally, we were able to show that only the elliptic curve $31y^2 = x^4 + x^3 + x^2 + x + 1$ has integral solutions. These solutions are given by $(2, \pm 1)$.

4.4 The case $n = 7$.

Finally we consider the diophantine equation

$$x^7 = 71y^2 + 1.$$

By putting $X = 71x$ and $Y = 71^4y$ we obtain the equation

$$X^7 = Y^2 + 71^6 \cdot 71. \tag{4.10}$$

The computation of all integer solutions of (4.10) can be reduced to the analysis of several Thue equations. This approach was used by M. Mignotte and B.M.M. de Weger to solve two similar equations of degree five [67]. In the sequel we follow the arguments from [67].

We denote by $\mathbb{K}$ the imaginary quadratic number field $\mathbb{Q}(\sqrt{-71})$. The class number of $\mathbb{K}$ is seven and an integral basis of $\mathbb{K}$ is given by the two generators $w_0 = 1$ and $w_1 = \frac{1+\sqrt{-71}}{2}$. To find the set of Thue equations corresponding to equation (4.10) we consider this equation as an equation in ideals in $\mathbb{K}$. Then we have

$$\langle Y + 71^3 \cdot \sqrt{-71} \rangle = \mathfrak{a}^7$$

for some integral ideal $\mathfrak{a}$ in $\mathbb{K}$. We observe that the prime 3 splits, say

$$\langle 3 \rangle = \mathfrak{p}\bar{\mathfrak{p}},$$

where $\mathfrak{p} = \langle 3, 1 + 2w_1 \rangle$. It follows that the ideal class of $\mathfrak{p}$ has order 7 in the classgroup and that there is an integer k with $|k| \leq 3$ such that $\mathfrak{p}^{-k}\mathfrak{a}$ is a principal ideal. Moreover there exist $u', v' \in N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p})^{-\max\{0, k\}} \cdot \mathbb{Z}$ with

$$\mathfrak{p}^{-k}\mathfrak{a} = \langle u' + v'w_1 \rangle.$$

It follows that

$$Y + 71^3 \cdot \sqrt{-71} = \gamma^k (u' + v'w_1)^7, \quad (4.11)$$

where γ is a generator of the principal ideal $\mathfrak{p}^7$. A value for γ may be computed by solving a norm equation in the number field $\mathbb{K}$. Our computation showed that we can take $\gamma = -45 - 2w_1$. Comparing the imaginary parts in equation (4.11) and multiplying by a common denominator leads to the desired Thue equations. By taking a closer look at these equations it follows by symmetry reasons that it suffices to restrict further considerations to the cases with $k \geq 0$.

Let $k \geq 0$ and denote by $u, v \in \mathbb{Z}$ integers, such that $u' = 3^{-k}u$ and $v' = 3^{-k}v$. We distinguish four cases:

In the case $k = 0$ we have

$$-3977u^7 + 6307u^6v + 5691u^5v^2 - 1225u^4v^3 - 595u^3v^4 + 21u^2v^5 + 7uv^6 = 715822$$

which can be solved quite easily. One can check that the only solution (u, v) in integers is given by $(1, -2)$. This solution corresponds to the trivial solution $(x, y) = (1, 0)$ of the original equation.

If $k = 1$ we have to find the integral solutions of the Thue equation

$$\begin{aligned} 219355u^7 - 228137u^6v - 293937u^5v^2 + 36155u^4v^3 + 29225u^3v^4 - 231u^2v^5 - \\ 329uv^6 - 2v^7 = 1565502714. \end{aligned}$$

It is not possible to solve this equation modulo 43, hence it has no solution in rational integers.

In the case $k = 2$ we have to consider the equation

$$184u^7 + 14959u^6v - 24675u^5v^2 - 1387435u^4v^3 - 647185u^3v^4 \\ + 14595987u^2v^5 + 7195195uv^6 - 11482961v^7 = 3423754435518.$$

One can observe that in this case we have $9|(u+v)$. This allows us to simplify the equation by putting $\frac{1}{9}(u+v) = U$ and $v = V$. Our equation is reduced to the equation

$$184U^7 + 1519U^6V - 1365U^5V^2 - 1435U^4V^3 + 665U^3V^4 + \\ 147U^2V^5 - 35V^6U - V^7 = 2 \cdot 71^3$$

We solved this equation by applying the **ThueSolve** function in MAGMA, and no solution was found.

Finally, we consider the case $k = 3$. This time we have to find the integral solutions (u, v) of

$$-12554u^7 - 656705u^6v + 2775297u^5v^2 + 63728945u^4v^3 - 19529965u^3v^4 \\ - 699990585u^2v^5 - 163022321uv^6 + 576703027v^7 = 7487750950477866.$$

One can observe that in this case we have $81|(u+10v)$. As in the previous case it is possible to do a simplification. This time we substitute $\frac{1}{81}(u+10v) = U$ and $v = V$. Then our equation is reduced to the equation

$$-12554U^7 + 8225U^6V + 21693U^5V^2 - 31535U^4V^3 \\ + 16835U^3V^4 - 4305U^2V^5 + 511UV^6 - 21V^7 = 2 \cdot 71^3.$$

We solved this equation by MAGMA, and no solution was found. This completes our arguments and the Theorem follows.

Summary

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 involves 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 [25]). It is important to notice that the resulting procedures provide efficient tools to solve several other diophantine problems.

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

$$I(\alpha) = \frac{\prod_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|}{\sqrt{|D_K|}} \quad (4.12)$$

where α_i ($1 \leq i \leq n$) denote the conjugates of α and D_K is the discriminant of the field K . An equation of the type

$$I(\alpha) = I$$

where I is a given integer, and α is an unknown element of $\mathbb{Z}_K$, is called an index from equation.

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 [36] proved effectively that an 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 [44] and the monograph I.Gaál [25], and the references given there.

There are no general feasible algorithms for solving such equations in full generality. 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 [20], [19] and I.Gaál and M.Pohst [30]. In this case the index form equation reduces to a relative Thue equation over the quadratic subfield which makes the resolution easier.

In the first chapter we consider index form equations in sextic fields with a cubic subfield. We give two algorithms. The first is to determine the "small" solutions of such equations. This algorithm is based on the properties of the index of a given element. To illustrate the algorithm we present a numerical example. Using the properties of the index we also give a parametric family of sextic number fields with a cubic subfield containing a large order which is monogene. The second algorithm is to determine all elements of given index in the same kind of number fields. This is achieved by reducing the problem to unit equations in two unknowns. An idea used in I.Gaál and K.Győry [27] implies that the rank of the corresponding unit equation is at most 11. We used reduction and enumeration methods described by I.Gaál and M.Pohst [31] (see also [25]). This enumeration method is based on K.Wildanger's ideas [85]. A numerical example is also detailed, the number field in the example has the greatest possible Galois group $S_4 \times C_2$. Note that recently Y.Bilu, I.Gaál and K.Győry [5] gave an algorithm for solving index form equations in any sextic field but our methods are very much faster than that method. The results of this chapter appeared in [54] and [53].

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 [35]), and it is not known whether there exist Heron triangles having the property that the lengths of all their sides are Fibonacci numbers (see [49] and [50]). 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 has been 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 [63]).

Let $P(k)$ denotes the largest prime factor of k . We prove that $P(abc) \rightarrow \infty$ when $\max(a, b, c) \rightarrow \infty$ 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 is ineffective.

Assuming that the prime divisors of abc have a 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 $\mathcal{P}$ contains only one prime $\equiv 1 \pmod{4}$ then all these triangles can be effectively determined. Moreover, in case $\mathcal{P} = \{2, 3, 5, 7, 11\}$ all such triangles are explicitly given.

In the third chapter we consider unit equations in three unknowns. First we give a method to compute the "small" solutions of unit equations in three unknowns. In fact this procedure is an extension of Wildanger's method which is developed for unit equations in two unknowns. As an application we computed the "small" solutions of a given norm form equation. We also provide an application to resultant form equations, which needs some essential improvements. A numerical example is also detailed to this case.

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

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

(see [36],[37],[43],[45]), where u_1, u_2 are unknown units and α_1, α_2 are fixed algebraic numbers. By Baker's method Győry derived effective upper bounds for the solutions of such equations.

Applying reduction methods and enumeration procedures due to K.Wildanger, recently it became possible to solve these equations completely (see [25] for an overview). These equations usually have "small" solutions only.

J.-H.Evertse and K.Győry (see e.g. [16]) showed that arbitrary decomposable form equations are equivalent to a system of unit equations in *several variables*.

Presently Baker's method seems to be not applicable to unit equations in more than two variables, so using this approach there is no hope to solve these equations completely. Hence we are going to give an algorithm for calculating

"small" solutions of unit equations in three variables. The application of this method makes it possible to find "small" solutions of some classes of decomposable form equations, that formerly could not be dealt with by using the above standard tools. The method is based on the ideas of K.Wildanger [85] and I.Gaál and M.Pohst [31] (see also [25]) and uses the method of U.Fincke and M.Pohst [18] for enumerating points in ellipsoids.

As an application we enumerated 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 [23] which deals with a more special case.

As an other application, we consider 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 common splitting field K such that

$$\text{Res}(P, Q) = a. \quad (4.13)$$

It is easy to see that if $(P(x), Q(x))$ is a solution to (4.13) then for any $b \in \mathbb{Z}$ $(P_1(x), Q_1(x)) = (P(x+b), Q(x+b))$ is also a solution. In this case the pairs $(P(x), Q(x))$ and $(P_1(x), Q_1(x))$ are called $\mathbb{Z}$ -equivalent. This shows that solving (4.13), one should restrict to $\mathbb{Z}$ -equivalence classes of polynomials.

It was shown by K.Györy [38] that there exist only finitely many $\mathbb{Z}$ -equivalence classes of polynomials (P, Q) satisfying (4.13) 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 [40] Györy 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 (4.13) such that P and Q have roots generating the fixed number fields M_1 and M_2 , respectively. This is a special case of the above problem when P and Q have common splitting field K which is the normal closure of $M_1 M_2$. We reduce the problem to unit equations in three unknowns and we use the method of [56] 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 [24].

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

$$x^n = Dy^2 + 1. \quad (4.14)$$

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 $n \geq 3$. With $n = 4$ Ljunggren [60] proved that for any D has at most two positive solutions.

Using elementary and algebraic number theoretical tools J.H.E. Cohn [12] proved necessary conditions for the unsolvability of (4.14). Moreover, he solved (4.14) completely for $D \leq 100$ up to six pairs of (n, D) . We complete Cohn's result by solving the remaining six equations.

Összefoglaló

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. [25]) kell lényegesen továbbfejlesztenünk. Fontos megjegyeznünk, hogy az így nyert módszerek más diofantikus problémák megoldásához is hatékony eszközt szolgáltatnak.

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

$$I(\alpha) = \frac{\prod_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|}{\sqrt{|D_K|}} \quad (4.15)$$

alakban is, ahol α_i ($1 \leq i \leq n$) 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. [36] 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 [25]). A másodfokú résztesttel rendelkező hatodfokú testek esetére Gaál I. [20], [19] és Gaál I. and M.Pohst [30] adott algoritmust.

Az első fejezetben harmadfokú résztesttel rendelkező hatodfokú számtestekben előforduló index forma egyenleteket vizsgálunk. Két algoritmust adunk meg. Az első az ilyen típusú 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. A második algoritmus segítségével meghatározhatjuk a fenti típusú számtestek összes adott indexű elemét. Ehhez a problémát kétváltozós egységegyenletek megoldására redukáljuk. Gaál I. és Győry K. [27] egy ötletéből következően a szóban forgó egységcsoportha rangja ≤ 11 . Ezen egységegyenleteket az Gaál I. és M.Pohst [31] által kidolgozott (lásd még [25]) redukciós és leszámlálási eljárásokkal oldjuk meg. A leszámlálási eljárások K.Wildanger [85] 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. [5] módszert adott a tetszőleges hatodfokú számtestek esetére is, de az itt bemutatott módszerek lényegesen gyorsabbak ebben a speciális esetben. Ezen fejezet eredményei [54]-ben és [53]-ben jelentek meg.

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 [35]).

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

A harmadik fejezetben háromváltozós egységegyenletekkel foglalkozunk. Fő eredményünként 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 széteső forma egyenlet, mint a Thue egyenletek, diszkrimináns forma, index forma, rezultáns forma és speciális norma forma egyenletek megoldása visszavezethető

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

alakú kétváltozós egységegyenletek megoldására (lásd [36],[37],[43],[45]), 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 [25]). Ezen egyenleteknek általában "kis" megoldásaik vannak csak.

J.-H.Evertse és Győry K. [16] megmutatta, hogy minden széteső forma egyenlet visszavezethető 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 széteső forma egyenlet "kis" megoldásainak megkeresése, melyre eddigi eszközökkel nem volt lehetőség. Módszerünk K.Wildanger [85] és M.Pohst és Gaál I. [31] módszerének általánosítása melynek alapja U.Fincke és M.Pohst [18] algoritmus ellipszoidok egész pontjainak leszámlálására.

Módszerünk egyik alkalmazásaként eljárást adunk bizonyos típusú többvál-

tozós norma forma egyenletek "kis" megoldásainak megkeresésére. Megjegyezzük, hogy többváltozós normaforma egyenletek numerikus megoldására eddig mindössze Gaál I. [23] adott módszert, mely az itt bemutatottnál speciálisabb esetben az összes megoldást meghatározza.

Módszerünk másik alkalmazásként rezultáns forma egyenleteket tekintetünk. Ezen egyenletek háromváltozós egységegyenletekre vezethetők 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

$$\text{Res}(P, Q) = a. \quad (4.16)$$

Nyilván ha $(P(x), Q(x))$ megoldása (4.16)-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. [38] Megmutatta, hogy véges sok olyan $\mathbb{Z}$ -ekvivalencia osztálya van (P, Q) polinompárokra melyek teljesítik (4.16)-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. [40] adott explicit felső korlátot P és Q fokára és a megoldások számára.

Meghatározzuk (4.16) "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.

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 [75]. Az $n = 4$ esetben Ljunggren [60] megmutatta, hogy minden D -re legfeljebb két megoldás van. J.H.E. Cohn [12] az $D \leq 100$ eset összes megoldását megadta, hat (n, D) pár kivételével. Munkánkban megoldjuk ezt a hat kivételes esetet, így teljessé téve J.H.E.Cohn eredményét.

Bibliography

- [1] A.Baker and H.Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$* , Q. J. Math. Oxford, **20** (1969), 129–137.
- [2] A.Baker and G.Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math., **442** (1993), 19–62.
- [3] Y.Bilu and G.Hanrot, *Solving Thue equations of high degree*, J. Number Theory, **60** (1996), 373–392.
- [4] Y.Bilu and G.Hanrot, *Solving superelliptic Diophantine equations by Baker’s method*, Composito Math., **112** (1998), 273–312.
- [5] Y.Bilu, I.Gaál and K.Györy, *Index form equations in sextic fields: a hard computation*, Acta Arith., **115** (2004), 85–96.
- [6] W.Bosma, J.Cannon, and C.Playoust. *The Magma algebra system I: The user language*, J. Symb. Comp., **24** 3/4 (1997), 235–265. (See also the Magma home page at <http://www.maths.usyd.edu.au:8000/u/magma/>)
- [7] Y.Bugeaud, *On the greatest prime factor of $(ab+1)(bc+1)(ca+1)$* , Acta Arith., **86** (1998), 45–49.
- [8] Y.Bugeaud and K.Györy, *Bounds for the solutions of unit equations*, Acta Arith., **74** (1996), 67–80.
- [9] Y.Bugeaud and T.N.Shorey, *On the number of solutions of the generalized Ramanujan-Nagell equation*, J. Reine Angew. Math. **539** (2001), 55–74.
- [10] M.Cipu, *Bounds for the solutions of the Diophantine equation $D_1x^2 + D_2^m = 4y^n$* , Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), 179–180.

- [11] J.H.E.Cohn, *The diophantine equation $x^2 + C = y^n$* , Acta Arith., **65** (1993), 367–381.
- [12] J.H.E.Cohn. *The Diophantine equation $x^n = Dy^2 + 1$* , Acta Arith., **106** (2003), 73–83.
- [13] P.Corvaja and U.Zannier, *On the greatest prime factor of $(ab+1)(ac+1)$* , Proc. Amer. Math. Soc., **131** (2003), 1705–1709.
- [14] M.Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner and K.Wildanger, *KANT V4*, J. Symbolic Comput., **24** (1997), 267–283.
- [15] S.David, *Minorations de formes linéaires de logarithmes elliptiques*, Mémoires Soc. Math. France (N.S.), **62** (1995), iv+143p.
- [16] J.-H.Evertse and K.Győry, *Finiteness criteria for decomposable form equations*, Acta Arith., **50** (1988), 357–379.
- [17] J.-H.Evertse, K.Győry, 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) 110–174.
- [18] 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.
- [19] I.Gaál, *Computing elements of given index in totally complex cyclic sextic fields*, J.Symbolic Comput., **20** (1995), 61–69.
- [20] I.Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp., **65** (1996), 801–822.
- [21] I.Gaál, *Power integral bases in composites of number fields*, Canad. Math. Bull., **41** (1998), 158–165.
- [22] I.Gaál, *Power integer bases in algebraic number fields*, Ann. Univ. Sci. Budapest.Sect. Comput., **18** (1999), 61–87.
- [23] I.Gaál, *An efficient algorithm for the explicit resolution of norm equations*, Publ. Math. Debrecen, **56** (2000), 375–390.
- [24] I.Gaál, *On the resolution of resultant type equations*, J.Symbolic Comput., **34** (2002), 137–144.

- [25] I.Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston, 2002.
- [26] I.Gaál, *On the resolution of resultant type equations*, J.Symbolic Comput. **34** (2002), no. 2, 137–144.
- [27] I.Gaál and K.Győry, *On the resolution of index form equations in quintic fields*, Acta Arith., **89** (1999), 379–396.
- [28] I.Gaál, I.Járasi and F.Luca, *A remark on prime divisors of lengths of sides of Heron triangles*, Experim. Math. **12** (2003), 303–310.
- [29] I.Gaál, A.Pethő and M.Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields*, J.Number Theory, **57** (1996), 90–104.
- [30] 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.
- [31] I.Gaál and M.Pohst, *On the resolution of relative Thue equations*, Math. Comput., **71** (2002), 429–440.
- [32] I.Gaál and N.Schulte, *Computing all power integral bases of cubic number fields*, Math. Comp., **53** (1989), 689–696.
- [33] J.Gebel, A.Pethő and H.G.Zimmer, *Computing integral points on elliptic curves*, Acta. Arith., **68** (1994), 171–192.
- [34] J.Gebel, A.Pethő and H.G.Zimmer, *On Mordell’s equation*, Compositio Math., **110** (1998), 335–367.
- [35] 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.
- [36] K.Győry, *Sur les polynomes a coefficients entiers et de discriminant donne, III*, Publ. Math.(Debrecen), **23** (1976), 141–165.
- [36a] K.Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv., **54** (1979), 583–600.

- [36b] K.Győry, *On the solutions of linear Diophantine equations in algebraic integers of bounded norm*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **22/23** (1979/80), 225–233.
- [37] K.Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposable*, Kingston, Canada, 1980.
- [38] K.Győry, *On arithmetic graphs associated with integral domains*, in: A tribute to Paul Erdős, Cambridge University Press, 1990. pp. 207–222.
- [39] K.Győry, *Some recent applications of S -unit equations*, Astérisque, **209** (1992), 17–38.
- [40] K.Győry, *On the number of pairs of polynomials with given resultant or given semi-resultant*, Acta Sci. Math., **57** (1993), 169–180.
- [41] K.Győry, *Some applications of decomposable form equations to resultant form equations*, Colloq. Math., **65** (1993), 267–275.
- [42] K.Győry, *On the irreducibility of neighbouring polynomials*, Acta Arith., **67** (1994), 283–294.
- [43] K.Győry, *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen, **52** (1998), 1–31.
- [44] 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.
- [45] K.Győry and Y.Kunrui, *Bounds for the solutions of S -unit equations and decomposable form equations*, to appear.
- [46] K.Győry, A.Sárközy and C.L.Stewart, *On the number of prime factors of integers of the form $ab + 1$* , Acta Arith., **74** (1996), 365–385.
- [47] K.Győry and A.Sárközy, *On prime factors of integers of the form $(ab + 1)(bc + 1)(ca + 1)$* , Acta Arith. **79** (1997), 163–171.
- [48] G.Hanrot, *Solving Thue equations without the full unit group*, Math. Comp., **69** (2000), 395–405.

- [49] H.Harborth and A.Kemnitz, *Fibonacci triangles*, in: Applications of Fibonacci numbers, Vol. 3 (Pisa, 1988), Kluwer Acad. Publ., Dordrecht, 1990. 129–132.
- [50] 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.
- [51] S.Hernandez and F.Luca, *On the largest prime factor of $(ab + 1)(ac + 1)(bc + 1)$* , Bol. Soc. Math. Mexicana, **9** (2003), 235–244.
- [52] E.Herrmann, I.Járásí 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.
- [53] I.Járásí, *Computing all elements of given index in sextic fields with a cubic subfield*, Acta Math. Inform. Univ. Ostraviensis, **10** (2002), 49–59.
- [54] I.Járásí, *Power integral bases in sextic fields with a cubic subfield*, Acta Sci. Math. (Szeged), **20** (2003), 291–303.
- [55] I.Járásí, *Computing small solutions of unit equations in three variables II: Resultant form equations*, Publ. Math. Debrecen, **65** (2004), 399–408.
- [56] I.Járásí, *Computing small solutions of unit equations in three variables I: Application to norm form equations*, submitted.
- [57] A.-V.Kramer and F.Luca, *Some remarks on Heron triangles*, Acta Acad. Paedagog. Agriensis, Sect. Mat. (N.S.), **27** (2000), 25–38.
- [58] M.-H.Le, *Some Exponential Diophantine Equations, I: The Equation $D_1x^2 - D_2y^2 = \lambda k^z$* , J. Number Th., **55** (1995), 209–221.
- [59] M.-H.Le, *On the Diophantine Equation $D_1x^2 + D_2^m = 4y^n$* , Mh. Math. **120** (1995), 121–125.
- [60] W.Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer usw.* Oslo Vid. Akad. Skrifter, **12** (1936)
- [61] W.Ljunggren, *On the diophantine equation $Cx^2 + D = y^n$* , Pacific. J. Math., **14** (1964), 585–596.

- [62] W.Ljunggren, *On the diophantine equation $Cx^2 + D = 2y^n$* , Math. Scand., **18** (1966), 69–86.
- [63] F.Luca, *Perfect cuboids and perfect square triangles*, Math. Mag., **73** (2000), 400–401.
- [64] F.Luca, *Fermat primes and Heron triangles with prime power sides*, Am. Math. Monthly, **110** (2003), 46–49.
- [65] F.Luca, *On the Equation $x^2 + 2^a \cdot 3^b = y^n$* , Int. J. Math. Math. Sci., **29** (2002), 239–244.
- [66] M.Mignotte and N.Tzanakis, *On a family of cubics*, J.Number Theory, **39** (1991), 41–49.
- [67] M.Mignotte, B.M.M.de Weger, *On the diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$* , Glasgow Math. J., **38** (1996), 77–85.
- [68] mwrank. *A package to compute ranks of elliptic curves*, See J. Cremona's homepage at <http://www.maths.ott.ac.uk/personal/jec/ftp/progs>.
- [69] A.Pethő, *On the resolution of Thue inequalities*, J. Symbolic Comp., **4** (1987), 103–109.
- [70] A.Pethő and R.Schulenberg, *Effektives Lösen von Thue Gleichungen*, Publ. Math. Debrecen, **34** (1987), 189–196.
- [71] I.Pink and Sz.Tengely, *Full powers in arithmetic progressions*, Publ. Math. Debrecen **57** (2000), 535–545.
- [72] A.Schinzel and R.Tijdeman, *On the equations $y^m = P(x)$* , Acta Arith. **31** (1976) 199–204.
- [73] H.P.Schlickewei, *Inequalities for decomposable form equations*, Astérisque **41-42** (1977), 267–271.
- [74] W.M.Schmidt, *Inequalities for resultants and for decomposable forms*, in: Diophantine Approximation and its applications, Academic Press, New York 1973, pp. 235–253.
- [75] T.N.Shorey and R.Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics, **87** Cambridge University Press, Cambridge, 1986.

- [76] N.Smart, *The algorithmic resolution of diophantine equations*, London Math. Soc. Student Texts **41** Cambridge Univ. Press, 1998.
- [77] C.L.Stewart and R.Tijdeman, *On the greatest prime factor of $(ab+1)(ac+1)(bc+1)$* . Acta Arith., **79** (1997), 93–101.
- [78] R.J.Stroeker and N.Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith., **67** (1994), 177–196.
- [79] E.Thomas, *Complete solutions to a family of cubic diophantine equations*, J.Number Theory, **34** (1990), 235–250.
- [80] N.Tzanakis. *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*. Acta Arith., **75** (1996), 165–190.
- [81] N.Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory, **31** (1989), 99–132.
- [82] B.M.M.de Weger, *Algorithms for diophantine equations*, CWI Tracts **65**, Amsterdam, 1989.
- [83] B.M.M.de Weger, *The weighted sum of two S -units being a square*, Indag. Math. (N.S.), **1** (1990), 243–262.
- [84] 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).
- [85] K.Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J.Number Theory, **82** (2000), 188–224.
- [86] E.Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree*, in: Proc. Symp. Pure Math. **20** Amer. Math. Soc., Providence 1971, pp. 213–247.
- [87] K.Yu, *p -adic logarithmic forms and group varieties. II*, Acta Arith., **89** (1999), 337–378.

- [88] P.Yuan and J.Wang, *On the diophantine equation $x^2 + b^y = c^z$* , Acta Arith. **84** (1998), 145–147.
- [89] D.Zagier. *Large integral points on elliptic curves*. Math. Comp. **48** (1987), 425-436.

Appendix A

List of papers of the author and citations to these papers

1. I.Járási, *On the Carmichael numbers*, (In Hungarian) KöMaL, **50** (2000), 136–145.
 - E.Kiss, *Kétszáz éve született Bolyai János*, (In Hungarian) KöMaL, **52** (2002), 457–466.
2. 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.
3. I.Járasi, *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.
 4. I.Gaál, I.Járasi and F.Luca, *A remark on prime divisors of lengths of sides of Heron triangles*, Experim. Math. **12** (2003) 303–310.
 5. E.Herrmann, I.Járasi 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.
 6. I.Járasi, *Computing small solutions of unit equations in three variables I: Application to norm form equations* Periodica Mathematica Hungarica submitted
 7. I.Járasi, *Computing small solutions of unit equations in three variables II: Applications to resultant form equations* Publ. Math. Debrecen **65** (2004) 399–408.

Appendix B

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 Czech 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 Czech and Slovak International Conference of Number Theory, Pozsony: Computing the small solutions of unit equations: Norm forms
6. 2003. july, XXIII Journées Arithmétiques, Graz: Computing the small solutions of unit equations: Norm forms
7. 2003. august, Workshop 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 Czech and Slovak International Conference of Number Theory, Malenovice: Some results on P-orderings

Constructive methods for Diophantine Equations

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

Írta: Járási István okleveles matematikus

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

Témavezető: Dr. Gaál István

A doktori szigorlati bizottság:

elnök:	Dr. Bódi Béla	
tagok:	Dr. Mátyás Ferenc	
	Dr. Pintér Ákos	

A doktori szigorlat időpontja: 2005. október 13.

Az értekezés bírálói:

Dr.
Dr.

A bírálóbizottság:

elnök:	Dr.
tagok:	Dr.
	Dr.
	Dr.
	Dr.

Az értekezés védésének időpontja: 200... ..