Annales Univ. Sci. Budapest., Sect. Comp. 18 (1999) 61-87

POWER INTEGER BASES IN ALGEBRAIC NUMBER FIELDS

I. Gaál (Debrecen, Hungary)

Dedicated to the memory of I. Környei and B. Kovács

Abstract. The main purpose of the paper is to give a survey of the presently known algorithms on the resolution of index form equations, especially on determining power integral bases of number fields. There are satisfactory methods for lower degree number fields and some partial results for higher degree number fields. The summary of these investigations might be helpful for the further research of these and connected diophantine equations.

1. Introduction

1.1. Basic concepts

It is a classical problem in algebraic number theory (dating back to Hasse) to decide if an algebraic number field K admits a **power integer basis**, that is an integer basis of the form

$$\{1, \alpha, \dots, \alpha^{n-1}\} \tag{1}$$

generated by the powers of a single element α. In case such an element α exists, the ring of integers $\mathbb{Z}_K$ of K is a simple extension of $\mathbb{Z}$, and is therefore called **monogene**.

Research supported in part by Grants 16791 and 16975 from the Hungarian National Foundation for Scientific Research and by the Foundation for Hungarian Higher Education and Research.

For any primitive element $\alpha \in \mathbb{Z}_K$ the **index of** α is defined as the module index

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

Obviously, the discriminant and index of α satisfy

$$D_{K/\mathbb{Q}}(\alpha) = I(\alpha)^2 D_K,$$

where D_K is the discriminant of the field K. The **minimal index** m_K of K is defined as the minimum of the indices of all primitive integers in K. The integers $\alpha, \beta \in \mathbb{Z}_K$ are called **equivalent** if $\alpha + \beta$ or $\alpha - \beta \in \mathbb{Z}$. Any two equivalent primitive integers of K have the same index. We also remark that obviously $\alpha \in \mathbb{Z}_K$ generates a power integer basis if and only if $I(\alpha) = 1$.

Let $\{1, \omega_2, \ldots, \omega_n\}$ be any integer basis of K. Then the discriminant of the linear form $X_2\omega_2 + \ldots + X_n\omega_n$ can be written as

$$D_{K/\mathbb{Q}}(X_2\omega_2 + \ldots + X_n\omega_n) = (I(X_2, \ldots, X_n))^2 D_K,$$

where $I(X_2, \ldots, X_n)$ is a form in $n-1$ variables of degree $n(n-1)/2$ with integer coefficients, called the **index form** corresponding to the above integer basis. For any $\alpha \in \mathbb{Z}_K$ represented as

$$\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n,$$

we have

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

independently of the value of the first coordinate x_1.

1.2. Purpose

The most important question in this context is to decide if the number field K admits power integral bases. This question is interesting both from a theoretical and a practical point of view. To determine all generators of power integral bases of K is equivalent to solving the **index form equation**

$$I(x_2, \ldots, x_n) = \pm 1 \quad \text{in} \quad x_2, \ldots, x_n \in \mathbb{Z}. \tag{2}$$

All generators of power integral bases can be represented in the form

$$\alpha = x_1 \pm (x_2\omega_2 + \ldots + x_n\omega_n), \tag{3}$$

where $x_1 \in \mathbb{Z}$ is arbitrary, and $(x_2, \ldots, x_n)$ is a solution of (2).

1.3. Baker's method

Using Baker's method upper bounds for the solutions of (2) were first given by Győry [34], then by Győry and Papp [35], and independently by Trelina [50]. Let A be an upper bound for the absolute values of the conjugates of the basis elements $\{1, \omega_2, \dots, \omega_n\}$. A typical theorem of this type is the following:

Theorem 1. *(Győry [34]). All solutions of (2) satisfy*

$$\max_{2 \le i \le n} |x_i| < \exp\{(5n^3)^{33n^3}(m^2A^n)^{5n^2}(\log(|m|A))^{3n^3}\}. \tag{4}$$

The latest improvements on the bounds of the index form equations can be found in [36]. These upper bounds imply that (2) has only finitely many solutions, hence (up to equivalence) there are only finitely many integers in K with index one. Unfortunately these bounds are so large, that in practice it is impossible to determine the solutions just by testing all values of the variables under the bound. For this reason it was necessary to develop constructive algorithms for computing the solutions.

2. Constructive algorithms

The computer resolution of diophantine equations is a fast developing branch of number theory involving efficient algorithms that make it possible in practice to find all solutions of certain equations.

In solving index form equations if possible we follow a **refined approach** taking into consideration the structure of the field and the factors of the index form. This way we can often reduce the index form equation to simpler types of equations. Such ideas make the resolution much more efficient. As we shall see, **Thue equations** and their generalizations, **relative Thue equations** and **inhomogeneous Thue equations** often play an important role. Fortunately there are efficient algorithms for the resolution of such equations, cf. Bilu and Hanrot [4], Gaál and Pohst [26], Gaál [8], respectively. If such equations occur, they make the resolution much easier.

On the other hand there is a **direct approach** of solving index form equations, namely, following the ideas of Győry [34] index form equations (as well as many other types of decomposable form equations) can be reduced to **unit equations in two variables**. This way Smart [47] (cf. also [49]) solved index form equations in certain sextic fields with a quadratic subfield, and Wildanger [53] in certain normal fields. Note that this direct approach is not applicable for higher degree fields because the unit equations become too complicated to solve. For lower degree fields the above refined approach is much more efficient when applicable. The direct approach is useful in some cases (e.g. for quintic fields cf. chapter 5) when no other method is known and the degree is low.

Both using the direct approach and e.g. solving a relative Thue equation we have to deal with a unit equation in two variables of type

$$\nu \rho_1^{a_1} \dots \rho_p^{a_p} + \mu \tau_1^{b_1} \dots \tau_q^{b_q} = 1 \tag{5}$$

with algebraic bases, where $\rho_1, \dots, \rho_p$ resp. $\tau_1, \dots, \tau_q$ are multiplicatively independent and the variables are $a_1, \dots, a_p, b_1, \dots, b_q \in \mathbb{Z}$. This equation is appropriate to give a brief description of the algorithm we usually apply.

2.1. Application of Baker-type estimates

For simplicity we demonstrate the procedure for the totally real case. Using elementary estimates equation (5) implies

$$\Lambda = |\log|\nu| + a_1 \log|\rho_1| + \dots + a_p \log|\rho_p|| < \exp(-c_1 A), \tag{6}$$

where $A = \max(|a_1|, \dots, |a_p|)$ and $c_1, c_2, \dots$ are explicitely given positive constants. The above inequality holds by taking suitable conjugates that we omit here for making the formulation simpler. In order to get an upper bound for A we apply Baker-type estimates for the above linear forms in the logarithms of algebraic numbers. For many applications the best known result of this type is the theorem of Baker and Wüstholz [3]. This gives a lower bound of the form

$$\exp(-c_2 \log A) < \Lambda$$

with a hugh constant c_2. Comparing this with (6) we obtain an upper bound A_B for A which is about 10^{20} for $p = 2$ and goes up to 10^{500} for $p = 8, 9$.

2.2. Reduction

Consider the lattice $\mathcal{L}$ spanned by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & & 0 \\ 0 & 1 & & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & & 1 \\ H \log|\nu| & H \log|\rho_1| & & H \log|\rho_p| \end{pmatrix}$$

where H is a large constant to be specified later. A typical lemma that makes possible to reduce the bound A_B is the following (Gaál and Pohst [26] Lemma 1):

Lemma 1. *If in inequality (6) $A \leq A_0$ and for the first vector b_1 of the LLL-reduced basis of $\mathcal{L}$*

$$|b_1| \geq \sqrt{(p+2)2^p} \tag{7}$$

then

$$A \leq \frac{\log H - \log A_0}{c_1}. \tag{8}$$

In the first step we set $A_0 = A_B$. Usually an appropriate choice for H is A_0^{p+1} in order to satisfy (7). Then, by (8) we get a new bound for A of magnitude $\log A_B$. This procedure can be repeated about 4-5 times until the new bound still improves the previous one. The final reduced bound A_R for A is of magnitude 100.

Note that here the LLL basis reduction algorithm plays an essential role cf. [39] and its modified version [46]. Similar ideas were used by de Weger [52] and Pethő and Schulenberg [45].

2.3. Enumeration

If r, s are larger than 3, it is still a nontrivial problem to test all possible exponents $a_1, \ldots, a_p, b_1, \ldots, b_q$ laying under the reduced bound A_R, of magnitude, say 100. This problem can be solved by using sieve methods for small values of p, q, cf. Tzanakis and de Weger [51], Smart [48]. Unfortunately these sieve methods are also not applicable within feasible time for $p, q \geq 5$.

For p, q larger than 5 the main difficulty in the resolution of unit equations (5) is in fact the test of "small solutions", the possible values of the exponents under the reduced bound. Recently Wildanger [53] elaborated an enumeration method that solves this problem up to unit rank about 10. This procedure is based on the ellipsoid method of Fincke and Pohst [7]. This algorithm has already several applications. Gaál and Pohst [26] worked out a suitable version of it for the resolution of relative Thue equations. Using this version Gaál and Győry [16] solved index form equations in quintic fields (see Chapter 5) and Gaál [15] solved certain norm form equations.

We give the essence of Wildanger's enumeration method. The reduced bound A_R for A implies a bound S such that each conjugate of $\nu\rho_1^{a_1}\ldots\rho_p^{a_p}$ and

$\mu\tau_1^{b_1}\dots\tau_q^{b_q}$ are between $1/S$ and S in absolute value. Our purpose is to reduce S since if S is small and the above property holds, then it is easy to test the corresponding exponents.

Let $s < S$. Then either the above assumption holds for s instead of S, or there exists a conjugate j_0 such that

$$\left|\nu^{(j_0)}\left(\rho_1^{(j_0)}\right)^{a_1}\dots\left(\rho_p^{(j_0)}\right)^{a_p}-1\right|$$

is small (similarly for $\mu\tau_1^{b_1}\dots\tau_q^{b_q}$), of magnitude $1/s$. We build vectors $\underline{g},\underline{e}_1,\dots,\underline{e}_p$ from the logarithms of sufficiently many conjugates (their number will be denoted by t) of $\nu,\rho_1,\dots,\rho_p$, respectively. For a vector $\underline{x}=(x_1,\dots,x_t)$ set $\varphi_{j_0}(x)=(\lambda_1x_1,\dots,\lambda_tx_t)$, where the weights λ_j are equal to $1/\log S$ except the one corresponding to the j_0-th conjugate that we set large so that

$$||\varphi_{j_0}(\underline{g})+a_1\varphi_{j_0}(\underline{e}_1)+\dots a_p\varphi_{j_0}(\underline{e}_p)||\le t.$$

This inequality defines an ellipsoid. If we enumerate these ellipsoids for all possible j_0, then we can replace S by s. We can repeat this procedure several times by taking s in the role of S in the following step until we get a sufficiently small constant. For more details cf. Wildanger [53] or Gaál and Pohst [26].

In the following we give a list of our results on the resolution of index form equations in an increasing order of field degree.

3. Cubic fields

The problem of the existence of power integer bases in number fields was first considered in cyclic cubic number fields by M.N.Gras [29], [30] and Archinard [1], who gave necessary and sufficient conditions for the monogenity. Dummit and H.Kisilevsky [5] showed that infinitely many totally real cyclic cubic fields have power integral bases, and on the other hand the minimum index of such fields can be arbitrary large.

For cubic number fields the index form equation is a **cubic Thue equation** that can be solved by the methods described above. Gaál and Schulte [28] gave a table of all power integral bases of totally real and also complex cubic fields with small discriminants.

Example. Consider the cubic field $K=\mathbb{Q}(\xi)$ generated by ξ, with minimal polynomial $f(x)=x^3-x^2-6x+7$ having discriminant $D_K=361$, with integer basis $\{1, \xi, \xi^2\}$. The index form equation corresponding to this integer basis is

$$I(x, y) = x^3 + 2x^2y - 5xy^2 + y^3 = \pm 1 \tag{9}$$

with solutions $(x, y) = (-7, 2), (1, 1), (9, 7), (0, 1), (2, 9), (1, 0)$.

4. Quartic fields

Also for quartic fields the question of monogenity was first investigated in the cyclic fields. M.N.Gras [31] gave necessary and sufficient conditions for the existence of power integer bases in such fields. She showed, that imaginary cyclic quartic fields can have power integral bases only in two trivial cases. Nakahara [43] proved, that the minimum index of cyclic quartic fields can be arbitrary large.

Concerning quartic fields with Galois group V4 (Klein four group) Nakahara [42] showed, that infinitely many of such fields admit power integral bases, and on the other hand, the minimal index of such fields can be arbitrary large. M.N.Gras and Tanoe [33] gave necessary and sufficient conditions for the monogenity of these fields.

For quartic number fields, Gaál, Pethő and Pohst developed constructive algorithms for the resolution of index form equations in a series of papers [17]-[23].

In [18] we reduced the index form equation in totally real cyclic quartic number fields to unit equations in two variables over the same field.

Example. Consider the totally real cyclic quartic field $K = \mathbb{Q}(\sqrt{\mu})$, $\mu = 55 + 22\sqrt{5}$, with discriminant $D_K = 15125$. An integer basis of it is $\{1, \omega, \psi, \omega\psi\}$ with $\omega = (1 + \sqrt{5})/2, \psi = (1 + \sqrt{\mu})/2$. The corresponding index form is

$$\begin{aligned} I(x, y, z) = &(y^2 + yz - z^2) \cdot (-5x^4 - 10x^3z + 55x^2y^2 + 165x^2yz + 130x^2z^2 + \\ &+ 55xy^2z + 165xyz^2 + 135xz^3 - 121y^4 - 847y^3z - 2134y^2z^2 - \\ &- 2288yz^3 - 881z^4). \end{aligned}$$

The solutions of the index form equation $I(x, y, z) = \pm 1$ are $(x, y, z) = = (-1, -2, 1), (-1, -1, 1), (0, -2, 1), (0, -1, 1)$.

In case of quartic fields with dihedral (D8) Galois group the index form equation was reduced to the problem of searching for elements of type x^2+c in second order linear recurrence sequences, cf. [17], [23].

For quartic number fields with Galois group V4, the index form has three quadratic factors. A theorem of K.S.Williams [54], giving the integer basis of such fields in a parametric form, was very useful in investigating these fields (cf. [20]). The index form equation was reduced to a system of two simultaneuos Pellian equations [19].

Example. In case $m \equiv 2 \pmod 4$, $n \equiv 3 \pmod 4$ an integer basis of $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ is $\{1, \sqrt{m}, \sqrt{n}, (\sqrt{m} + \sqrt{m_1 n_1})/2\}$, where $n_1 = n/d, m_1 = m/d$ with $d = (n, m)$. The index form factorizes as

$$I(x,y,z) = \left(\frac{d}{2}(2x+z)^2 - \frac{n_1}{2}z^2\right) \cdot \left(2dy^2 - \frac{m_1}{2}z^2\right) \cdot \left(2n_1y^2 - \frac{m_1}{2}(2x+z)^2\right),$$

where all factors are polynomials with integer coefficients. In case $m = 2, n = 11$, the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$ has discriminant $D_K = 30976$, and all solutions of $I(x,y,z) = \pm 1$ are $(x,y,z) = (-1,0,1), (0,0,1)$.

4.1. A general theorem

Denote by $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ the minimal polynomial of the generating element of $K = \mathbb{Q}(\xi)$. Assume, that any $\alpha \in \mathbb{Z}_K$ can be represented in the form

$$\alpha = \frac{a + x\xi + y\xi^2 + z\xi^3}{g}, \tag{10}$$

with $a, x, y, z \in \mathbb{Z}$, and with a fixed common denominator $g \in \mathbb{Z}$. Set

$$\begin{aligned} F(u,v) &= u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3, \\ Q_1(x,y,z) &= x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + \\ &\quad + (a_3 - a_1a_2)yz + (-a_1a_3 + a_2^2 + a_4)z^2, \\ Q_2(x,y,z) &= y^2 - xz - a_1yz + a_2z^2, \end{aligned}$$

and consider the equation

$$I(\alpha) = m \quad \text{in} \quad \alpha \in \mathbb{Z}_K. \tag{11}$$

The remaining possible Galois groups in the quartic case are A4 and S4, when the index form is irreducible. These cases are also covered by the following theorem [21]:

Theorem 2. *The element $\alpha \in \mathbb{Z}_K$, represented in the form (10), is a solution of (11) if and only if there exists a solution $(u, v) \in \mathbb{Z}^2$ of*

$$F(u, v) = \pm \frac{g^6 m}{I(\xi)} = \pm I, \tag{12}$$

with

$$Q_1(x, y, z) = u, \tag{13}$$

$$Q_2(x, y, z) = v. \tag{14}$$

The polynomial $F(u, 1)$ is the cubic resolvent polynomial of $f(x)$. If K has proper subfields, then $F(u, v)$ is reducible and (12) is trivial to solve. Otherwise (for Galois groups A4 and S4) (12) is a **cubic Thue equation**, that can also be easily solved. For all solutions (u, v) of (12) one has to solve the system of equations (13), (14). We remark, that independently Koppenhöfer [37] obtained a result similar to Theorem 2 by algebraic tools.

4.2. Totally complex quartic fields

For totally complex quartic fields the system (13), (14) can be solved easily [21]:

Theorem 3. *If K is a totally complex quartic field, then the polynomial $F(u, 1)$ has three real roots $\lambda_1 < \lambda_2 < \lambda_3$. The quadratic form*

$$Q_1(x, y, z) + \lambda Q_2(x, y, z)$$

is positive definite if and only if $\lambda_1 < \lambda < \lambda_2$.

In view of this theorem, taking $\lambda \in (\lambda_1, \lambda_2)$, for a given solution (u, v) of (12) one merely has to enumerate and test the solutions of

$$Q_1(x, y, z) + \lambda Q_2(x, y, z) = u + \lambda v \quad \text{in} \quad x, y, z \in \mathbb{Z},$$

where the left hand side is a positive definite quadratic form.

4.3. Families of totally complex quartic fields

Theorem 3 enables one also to solve completely index form equations in orders of infinite parametric families of totally complex quartic fields. The following example is one of the families investigated in [10]:

Example. Consider the infinite parametric family of fields $K = \mathbb{Q}(\xi)$, generated by ξ, with minimal polynomial $f(x) = x^4 + x^3 + kx^2 - x + 1$, where $0 < k \in \mathbb{Z}$ is a parameter. One can easily see, that $f(x)$ is irreducible, totally complex, $D(f) = (k^2 - 4k + 8)(7 + 4k)^2$, the Galois group of f is D8 for $k \neq 2$, and V4 for $k = 2$. Unfortunately we cannot describe the integer basis of K in a parametric form, hence we study the problem of power integer bases in the equation order $\mathcal{O} = \mathbb{Z}[\xi]$ (which often coincides with $\mathbb{Z}_K$). For this purpose we apply Theorem 3 with $g = n = m = 1$. The equation

$$F(u, v) = (u + 2v)(u^2 - (k + 2)uv + (2k - 1)v^2) = \pm 1$$

has only the trivial solutions $(u, v) = (\pm 1, 0)$. The roots of $F(u, 1) = 0$ satisfy $-2 = \lambda_1 < 0 < \lambda_2 < \lambda_3$, hence we can take $\lambda = 0$. Then we have to solve the equation

$$Q_1(x, y, z) =$$

$$\frac{1}{4}(2x - y + (1 - 2k)z)^2 + \frac{1}{4(4k-1)}((4k - 1)y - (4k + 1)z)^2 + \frac{4k - 2}{4k - 1}z^2 = 1$$

whence $z = 0$ or $z = 1$, and we get the corresponding solutions $(x, y, z) = (1, 0, 0)$, and $(k, 1, 1)$. Thus, up to equivalence, the only power integral bases of $\mathcal{O}$ are generated by ξ and $k\xi + \xi^2 + \xi^3$.

4.4. Arbitrary quartic fields

Using an idea of Mordell [41] one can solve the system of equations (13), (14) in any quartic field, as well. For a solution (u, v) of (12) set

$$Q_0(X, Y, Z) = uQ_2(X, Y, Z) - vQ_1(X, Y, Z). \tag{15}$$

If α of (10) is a solution of (11), then $Q_0(x, y, z) = 0$. Let $(x_Q, y_Q, z_Q) \in \mathbb{Z}^3$ be an arbitrary non–trivial solution of (15) with (e.g.) $z_Q \neq 0$. Then x, y, z can be represented as

$$x = rx_Q + p, \quad y = ry_Q + q, \quad z = rz_Q \tag{16}$$

with $p, q, r \in \mathbb{Q}$. Now $Q_0(x, y, z) = 0$ implies

$$r(c_1p + c_2q) = (c_3p^2 + c_4pq + c_5q^2), \tag{17}$$

with certain explicitely given integer coefficients $c_1, c_2, \ldots$. Multiplying the equations of (16) by $(c_1 p + c_2 q)$, equation (17) implies

$$kx = f_x(p,q), \quad ky = f_y(p,q), \quad kz = f_z(p,q), \tag{18}$$

with a common factor $k \neq 0$, where $f_x, f_y, f_z \in \mathbb{Z}[x,y]$ are quadratic forms. By multiplying the above equations by the square of the common denominators of p and q, we can replace p, q, k with integer parameters p, q, k. Further, it can be shown, that k can only take a few values, namely k divides $I|z_Q|^3$ (cf. (12)). Substituting the forms (18) into (13), (14) we obtain quartic equations in the integer variables p, q:

$$F_1(p,q) = Q_1(f_x(p,q), f_y(p,q), f_z(p,q)) = k^2 u \text{ in } p,q \in \mathbb{Z}, \tag{19}$$

$$F_2(p,q) = Q_2(f_x(p,q), f_y(p,q), f_z(p,q)) = k^2 v \text{ in } p,q \in \mathbb{Z}. \tag{20}$$

It was suprising to realize, that [22]

Theorem 4. *At least one of the equations (19), (20) is a quartic Thue equation in $p, q \in \mathbb{Z}$ over the same field K.*

It is important to remark that Theorems 2 and 4 imply, that the resolution of index form equations in quartic fields can be reduced to the resolution of a **cubic Thue equation** (12) and to some corresponding **quartic Thue equations** (19), (20).

By using the above method we could solve index form equations in any quartic field, also for Galois groups S4 and A4.

Example. Consider the totally real field $K = \mathbb{Q}(\xi)$, generated by ξ, with minimal polynomial $f(x) = x^4 - x^3 - 16x^2 - 11x + 7$, having discriminant $D_K = 848241$, and Galois group A4. The index form corresponding to the integer basis $\{1, \xi, \xi^2, (1+\xi^3)/2\}$, is the irreducible form

$$\begin{aligned} I(x,y,z) = & -58x^4y^2 + 101x^4yz + 1347x^4z^2 - 126x^3y^3 - 1613x^3y^2z - \\ & - 99x^3yz^2 + 10730x^3z^3 + 414x^2y^4 - 449x^2y^3z - 13632x^2y^2z^2 - \\ & - 9105x^2yz^3 + 42617x^2z^4 + 6157xy^4z + 10545xy^3z^2 - 34771xy^2z^3 \\ & - 45514xyz^4 + 1797y^4z^2 + 25112y^3z^3 - 5993y^2z^4. \end{aligned}$$

The minimal index of the field is $m_K = 2$, all solutions of $I(x,y,z) = \pm 2$ are $(1,0,0), (2,2,-1), (7,1,-1), (406,15,-50)$.

Using the above algorithms we made extensive calculations in quartic fields with small discriminants. For tables about the distribution and behavior of the minimal indices, see [21].

5. Quintic fields

M.N.Gras [32] showed that a totally real cyclic field of prime degree $p \geq 5$ can only have power integral basis if the field is the maximal real subfield of a cyclotomic field.

5.1. An infinite parametric family

Gaál and Pohst [25] considered the totally real cyclic quintic fields $K_n = \mathbb{Q}(\vartheta_n)$, generated by a root ϑ_n of the polynomial

(21)
$$\begin{aligned} f_n(x) =& x^5 + n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 + \\ &+ (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1. \end{aligned}$$

This family was first inverstigated by Emma Lehmer [38]. Assuming that $m = n^4 + 5n^3 + 15n^2 + 25n + 25$ is square free, we computed explicitely an **integral basis** and a set of **fundamental units** of K_n. Using only *congruence considerations* we proved that K_n has a power integral basis only for $n = -1, -2$. For $n = -1, -2$ (both values presenting the same field) all generators of power integral bases were computed.

5.2. A general method

Gaál and Győry [16] gave a feasible algorithm for solving index form equations in arbitrary quintic fields, based on Wildanger's enumeration method as worked out by Gaál and Pohst [26], and using ideas of Győry [36]. The algorithm works in a field of degree 10, having at most 9 fundamental units. The necessary CPU time is unfortunately too long, about 24 hours per example.

Example. Consider the totally real quintic field $K = Q(\xi)$ where ξ is defined by the polynomial $f(x) = x^5 - 5x^3 + x^2 + 3x - 1$. This field has discriminant $D_K = 24217$, Galois group S_5 and integral basis $\{1, \xi, \xi^2, \xi^3, \xi^4\}$.

The coefficients of the generators of power integral bases with respect to this integral basis are:

$$\begin{aligned}(x_2,x_3,x_4,x_5)=&(0,1,0,0),\ (0,2,1,-1),\ (0,4,0,-1),\ (0,5,0,-1),\\ &(1,-5,0,1),\ (1,-4,0,1),\ (1,-1,0,0),\ (1,0,0,0),\\ &(1,1,-2,-1),\ (1,4,0,-1),\ (2,-1,-1,0),\ (2,4,-1,-1),\\ &(2,9,-1,-2),\ (2,15,-1,-3),\ (2,10,-1,-2),\ (3,4,-1,-1),\\ &(3,5,-1,-1),\ (3,9.-1,-2),\ (3,10,-1,-2),\ (3,14,-1,-3),\\ &(3,18,-2,-4),\ (4,-1,-1,0),\ (4,0,-1,0),\ (4,5,-1,-1),\\ &(4,24,-2,-5),\ (4,29,-2,-6),\ (5,-4,-1,1),\ (5,8,-2,-2),\\ &(5,33,-2,-7),\ (7,5,-2,-1),\ (7,9,-2,-2),\ (7,14,-2,-3),\\ &(9,18,-3,-4),\ (11,-13,-2,3),\ (12,27,-4,-6),\\ &(17,28.-6,-6),\ (33,30,-51,-26),\ (83,170,-25,-39),\\ &(124,246,-40,-55).\end{aligned}$$

6. Sextic fields

As we shall see, in case the sextic field admits a quadratic subfield, the index form has always a factor that implies a **relative Thue equation** of degree 3 over the quadratic subfield. In case the sextic field has additional special properties, the resolution of index form equations can be simplified further.

6.1. Sextic fields with a quadratic subfield

Let M be a quadratic field with integral basis $\{1,\omega\}$. Let $f(t) = t^3+\gamma_2 t^2+\gamma_1 t+\gamma_0 \in \mathbb{Z}_M[t]$ be the minimal polynomial of ϑ over M. Consider the sextic field $K = \mathbb{Q}(\vartheta)$. For simplicity we assume that K admits a relative integral basis $\{1,\vartheta,\vartheta^2\}$ over M, by remarking that this is the case most often and our method applies also in the opposite case, with minor changes in the theory, but needs longer computation time.

Let $\alpha = x_0+x_1\vartheta+x_2\vartheta^2+y_0\omega+y_1\omega\vartheta+y_2\omega\vartheta^2$ be an integer in K satisfying $I(\alpha)=1$ and consider the corresponding index form equation

$$I(x_1,x_2,y_0,y_1,y_2)=\pm 1 \quad \text{in } x_1,x_2,y_0,y_1,y_2 \in \mathbb{Z}. \tag{22}$$

Let ϑ_1 and ϑ_2 be distinct roots of $f(x)$ and put $\rho = -\vartheta_1 - \vartheta_2$. For a solution $(x_1, x_2, y_0, y_1, y_2)$ of (22) set $X = x_1 + \omega y_1, Y = x_2 + \omega y_2$.

It is easily seen (cf. [12], [24]), that in our case the index form has at least two factors with integer coefficients, implying, that our equation (22) splits into a system of equations. Namely, we have

Theorem 5. *If $(x_1, x_2, y_0, y_1, y_2)$ is a solution of (22), then $(X, Y) = (x_1 + \omega y_1, x_2 + \omega y_2)$ is a solution of*

$$N_{K/M}(X - \rho Y) = \nu \quad \text{in} \quad X, Y \in \mathbb{Z}_M \tag{23}$$

where ν is a unit in M.

For a fixed ν equation (23) is a cubic **relative Thue equation** over M. This equation can be solved completely by the known methods, and for this purpose one has to make computations only in the field K.

6.2. Sextic fields with a real quadratic subfield

If M is a **real quadratic field**, there are infinitely many possible values for ν. Despite of it, one can determine finitely many pairs (X, Y), such that all solutions of (23) are of the form

$$x_1 + \omega y_1 = \pm \mu^l X, \quad x_2 + \omega y_2 = \pm \mu^l Y, \tag{24}$$

where (X, Y) is one of the abovementioned pairs, μ is the fundamental unit of M, and $l \in \mathbb{Z}$, whence

$$x_1 = \pm \frac{\bar{\omega}\mu^l X - \omega \bar{\mu}^l \bar{X}}{\bar{\omega} - \omega}, \quad y_1 = \pm \frac{\mu^l X - \bar{\mu}^l \bar{X}}{\omega - \bar{\omega}},$$
$$x_2 = \pm \frac{\bar{\omega}\mu^l Y - \omega \bar{\mu}^l \bar{Y}}{\bar{\omega} - \omega}, \quad y_2 = \pm \frac{\mu^l Y - \bar{\mu}^l \bar{Y}}{\omega - \bar{\omega}},$$

where $\bar{\gamma}$ denotes the conjugate of an element $\gamma \in M$. Substituting these expressions into the other factor of the index form we obtain an equation of the form

$$\prod_{i=1}^{9} (A_i \mu^l + B_i \bar{\mu}^l + C_i y_0) = \pm 1, \tag{25}$$

where $A_i, B_i, C_i \in K$ $(1 \le i \le 9)$ are explicitely given and $l, y_0 \in \mathbb{Z}$ are unknowns. This equation has a similar structure, like an **inhomogeneous Thue equation** of degree 9 (cf. [8]), and can be solved in a similar manner.

(Assuming $\mu > 1, l > 0$, the variables μ^l, y_0 are dominating, while $\bar{\mu}^l$ is non-dominating).

In [11] we worked out this method for totally real cyclic sextic fields (cf. [40], [6]) when there is also a cubic subfield and equation (25) splits into a cubic and a sextic equation of the same type.

Example. Let $\omega = (1+\sqrt{5})/2$, and let ϑ be a root of $f(t) = t^3 + (-6-6\omega)t + (6+11\omega)$. The field $K = \mathbb{Q}(\vartheta)$ is totally real, cyclic, with discriminant $D_K = 820125$. The solutions of the index form equation (22) corresponding to the integer basis $\{1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2\}$ are

$$\begin{aligned}(x_1, x_2, y_0, y_1, y_2) =&(-10,8,4,6,-5),\ \ (-4,3,2,2,-2),\ \ (-4,11,16,2,-7),\\ &(-1,0,0,1,0),\ \ (-1,1,3,0,-1),\ \ (-1,1,5,0,-1),\\ &(0,-2,8,-3,0),\ \ (0,0,-2,1,0),\ \ (0,0,8,-2,-1),\\ &(1,0,-4,2,0),\ \ (1,1,-5,1,0),\ \ (1,1,-3,1,0),\\ &(1,2,-8,2,0),\ \ (2,-4,-10,0,3),\ \ (2,-1,-12,2,2),\\ &(2,-1,-4,0,1),\ \ (2,0,-9,1,1),\ \ (2,0,-7,1,1),\\ &(2,1,2,-2,-1),\ \ (3,2,-26,5,2),\ \ (3,2,-22,6,2),\\ &(6,3,0,-4,-2),\ \ (8,4,-68,13,6),\ \ (9,4,-60,15,6).\end{aligned}$$

6.3. Sextic fields with an imaginary quadratic subfield

In this case the index form has in general only two factors, one of them implying equation (23), where ν can attain only a few possible values. By solving this equation, we find the (finitely many) possible tuples (x_1, y_1, x_2, y_2). We substitute these tuples into the equation we get from the other factor of the index form, and obtain a polynomial equation of degree 9 in y_0 with integer coefficients. This method is described in [24].

Example. Let $\omega = (1+i\sqrt{3})/2$, and let ϑ be a root of $f(t) = t^3 + (-1-\omega)t^2 + \omega t + (1-\omega)$. The field $K = \mathbb{Q}(\vartheta)$ has discriminant $D_K = -9747$, and integer basis $\{1,\vartheta,\vartheta^2,\omega,\omega\vartheta,\omega\vartheta^2\}$. All solutions of the index form equation (22) are

$$\begin{aligned}(x_1,x_2,y_0,y_1,y_2) =&(-2,0,1,2,-1),\ \ (-1,0,0,1,-1),\ \ (-1,0,-1,2,-1),\\ &(0,0,0,1,-1),\ \ (0,0,-1,2,-1),\ \ (-1,0,0,0,0),\\ &(-1,0,1,0,0),\ \ (-1,0,-1,1,0),\ \ (-1,0,0,1,0),\\ &(0,0,0,-1,0),\ \ (0,0,1,-1,0),\ \ (-2,1,0,1,-1),\\ &(-2,1,-2,2,-1),\ \ (-1,1,0,0,-1),\ \ (-1,1,0,1,-1),\\ &(0,1,0,0,-1),\ \ (-1,1,1,-1,0),\ \ (-1,1,0,0,0),\\ &(0,1,1,-2,0),\ \ (0,1,0,-1,0),\ \ (0,1,1,0,0).\end{aligned}$$

6.4. Totally complex cyclic sextic fields

Let ϑ be a totally real cubic algebraic integer and let m be a square-free positive integer. Let us consider the sextic field $K = \mathbb{Q}(\vartheta, i\sqrt{m})$, with discriminant D_K and ring of integers $\mathbb{Z}_K$. Let $M = \mathbb{Q}(i\sqrt{m})$, and $L = \mathbb{Q}(\vartheta)$ be the subfields of K. (We remark that our algorithm works not only in totally complex cyclic sextic fields, but also in any sextic field containing both an imaginary quadratic and a real cubic subfield.) Set

$$\omega = \begin{cases} (1+i\sqrt{m})/2 & \text{if } -m \equiv 1 \bmod 4, \\ i\sqrt{m} & \text{if } -m \equiv 2,3 \bmod 4. \end{cases} \tag{26}$$

We represent any $\alpha \in \mathbb{Z}_K$ in the form

$$\alpha = \frac{x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2}{g} \tag{27}$$

with $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ and with a fixed common denominator $g \in \mathbb{Z}$.

Set $\mathcal{O} = \mathbb{Z}[1,\vartheta,\vartheta^2,\omega,\omega\vartheta,\omega\vartheta^2]$ and denote by $D_{\mathcal{O}}$ the discriminant of this order.

Index form equations over sextic fields of this type are considered in [12]. In the present situation the index form equation has three factors.

Theorem 6. *If (x_1,x_2,y_0,y_1,y_2) is a solution of (22), $X = x_1 + \omega y_1$, $Y = y_1 + \omega y_2$, then*

$$N_{K/M}(X - \rho Y) = \nu, \tag{28}$$

and

$$(29) \qquad N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2) = d,$$

with $\nu \in \mathbb{Z}_M$ *and* $d \in \mathbb{Z}$, *such that* $d \cdot N_{M/Q}(\nu)$ *divides*

$$I_1 = \frac{g^{15}\sqrt{|D_K|}}{\sqrt{|D_O|}} \in \mathbb{Z}.$$

Obviously there are only finitely many possible values for ν, d.

The main goal of the investigations of index form equations in such fields is, that we could show, that in this case the resolution of the relative Thue equation (28) can be reduced to solving a single cubic **Thue inequality** over $\mathbb{Z}$ (cf. Theorem 7).

Denote by γ_i $(i = 1, 2, 3)$, the conjugates of any $\gamma \in L$. Let $\rho = -\vartheta_1 - -\vartheta_2$. Assume, that (X, Y) is a solution of equation (28). Choose the indices $\{r, s, t\} = \{1, 2, 3\}$ according to

$$(30) \qquad |X - \rho_r Y| \leq |X - \rho_s Y| \leq |X - \rho_t Y|.$$

Set

$$c_m = \begin{cases} 2 & \text{if } -m \equiv 1 \pmod 4, \\ 1 & \text{if } -m \equiv 2, 3 \pmod 4, \end{cases}$$

$$c_1 = 9c_m^3|\nu|, \quad c_2 = \min(|\rho_r - \rho_s|, |\rho_r - \rho_t|), \quad c_3 = |\rho_r - \rho_s| \cdot |\rho_r - \rho_t|,$$

$$c_4 = \max\left\{\frac{2|\nu|^{1/3}}{c_2}, \frac{4c_m|\nu|}{c_3\sqrt{m}}\right\}, \quad c_5 = \left(\frac{8|\nu|}{c_2c_3}\right)^{1/3},$$

and put

$$F(x, y) = \prod_{j=1}^{3}(x - \rho_j y) \in \mathbb{Z}[x, y].$$

Theorem 7. *Let* $X = x_1 + \omega y_1, Y = x_2 + \omega y_2 \in \mathbb{Z}_M$ *be a solution of (28) according to (30). Suppose* $|Y| > c_4$. *We have*

$$(31) \qquad x_1y_2 = x_2y_1.$$

Further, in case $-m \equiv 1 \pmod 4$

$$\begin{array}{ll} \textit{if}\ \ |2x_2+y_2| \geq 2c_5 & \textit{then}\ \ |F(2x_1+y_1, 2x_2+y_2)| \leq c_1, \\ \textit{if}\ \ |y_2| \geq 2c_5/\sqrt{m} & \textit{then}\ \ |F(y_1,y_2)| \leq c_1/(\sqrt{m})^3 \end{array}$$

and in case $-m \equiv 2,3 \pmod 4$

$$\begin{array}{ll} \textit{if}\ \ |x_2| \geq c_5 & \textit{then}\ \ |F(x_1,x_2)| \leq c_1, \\ \textit{if}\ \ |y_2| \geq c_5/\sqrt{m} & \textit{then}\ \ |F(y_1,y_2)| \leq c_1/(\sqrt{m})^3. \end{array}$$

In view of Theorem 7 we can determine the possible tuples (x_1, x_2, y_1, y_2) by solving a single cubic Thue inequality over $\mathbb{Z}$. An efficient method based on continued fraction expansion for solving Thue inequalities can be found in Pethő [44]. The corresponding values of y_0 are determined from equation (29).

6.5. An infinite parametric family of totally complex cyclic sextic fields

As an application of the results of the preceeding section we consider now the index form equation in a **two parametric infinite family** of totally complex cyclic sextic fields, composed of Shanks' simplest cubics with imaginary quadratic number fields, [12].

Let a be a natural number, let ϑ be a root of

$$f(x) = x^3 - ax^2 - (a+3)x - 1, \tag{32}$$

and let m be a square-free positive integer. Consider the two parametric family $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ of totally complex cyclic sextic fields. Define ω as in (26) and set $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ with discriminant $D_{\mathcal{O}}$ as before. Unfortunately it seems to be difficult to describe an integer basis of K. On the other hand, the order $\mathcal{O}$ is very often the principal order of K. Hence we restrict ourselves to considering power integral bases in $\mathcal{O}$. Put

$$m_0 = \begin{cases} 19 & \text{if } -m \equiv 1 \pmod 4, \\ 5 & \text{if } -m \equiv 2,3 \pmod 4. \end{cases}$$

Theorem 8. *Assume that* $a \geq 3$ *and* $m \geq m_0$. *Then the order* $\mathcal{O}$ *has no power integral bases.*

7. Octic fields with a quadratic subfield

Let $K = \mathbb{Q}(\xi)$ be a field of degree eight with a quadratic subfield M. Index form equations in such octic fields were considered by Gaál and Pohst [27]. In this case we represent the integers of the octic field in the form

$$\alpha = \frac{X_0 + X_1\xi + X_2\xi^2 + X_3\xi^3}{d}$$

with quadratic integers X_0, X_1, X_2, X_3 in M and a common denominator $d \in \mathbb{Z}$. We follow the main steps of Section 4.4 (the corresponding algorithm for quartic fields [22]) in a relative sense. We obtain similar equations as in (12), (13), (14) just with quadratic integers as variables. It can be shown (not trivial at all) that the analogue of the transformation (16) can also be used similarly. One of the equations analogue to (19), (20) is a quartic relative Thue equation over M. Solving the above equations we can determine the coefficients (X_1, X_2, X_3) corresponding to α up to a unit factor in M. To determine this unit factor and the remaining variable X_0 we have to solve certain corresponding equations of degree 16 that are similar to *inhomogeneous Thue equations* cf. [8], [11].

Example. Consider the field K generated by a root ξ of the polynomial

$$f(x) = x^8 - x^7 + x^6 + 2x^5 - 2x^4 + 2x^2 - x - 1.$$

This field has signature (2,6) and discriminant

$$D_K = -4461875 = -5^4 \cdot 11^2 \cdot 59.$$

The field K has $M = \mathbb{Q}(\sqrt{5})$ as a subfield. Set $\omega = \mu = \frac{1+\sqrt{5}}{2}$. The relative defining polynomial of ξ over M is

$$f_M(x) = x^4 + (-1 + \omega)x^3 + x^2 + (1 + \omega)x + \omega.$$

Equation (12) has the form

$$(U + \omega V) \cdot (U^2 + (-1 - \omega)UV + (1 - \omega)V^2) = \varepsilon,$$

where ε is a unit in M. The solutions are $(U, V) = (1, 0), (1 + \omega, 1), (0, \omega)$. The corresponding *quartic relative Thue equations* are

$$F_1(P, Q) = P^4 + (\omega - 1)P^3Q + P^2Q^2 + (\omega + 1)PQ^3 + \omega Q^4 = \varepsilon,$$
$$F_2(P, Q) = (1 + \omega)(P^4 + (3 - 3\omega)P^3Q + (4 - 3\omega)P^2Q^2 + 2PQ^3 + Q^4) = \varepsilon,$$
$$F_2(P, Q) = (1 + 2\omega)(P^4 - 2\omega P^3Q + 3\omega P^2Q^2 + (-2 - \omega)PQ^3 + \omega Q^4) = \varepsilon,$$

where ε is a unit. Finally, the following integers (and their translations by elements of $\mathbb{Z}$) generate power integral bases in K:

$$\begin{aligned}
\alpha &= \xi, \\
\alpha &= \xi + (-1+\omega)\xi^2, \\
\alpha &= (1-\omega)\xi + (-1+\omega)\xi^2.
\end{aligned}$$

The total CPU time was about 8 hours on a PC.

8. Index form equations in composites of fields

Let L be a number field of degree r with integral basis $\{l_1 = 1, l_2, \ldots, l_r\}$ and discriminant D_L. Denote the index form corresponding to the integral basis $\{l_1 = 1, l_2 \ldots, l_r\}$ of L by $I_L(x_2, \ldots, x_r)$. Similarly, let M be a number field of degree s with integral basis $\{m_1 = 1, m_2, \ldots, m_s\}$ and discriminant D_M. Denote the index form corresponding to the integral basis $\{m_1 = 1, m_2 \ldots, m_s\}$ of M by $I_M(x_2, \ldots, x_s)$.

Assume, that the discriminants are coprimes, that is

$$(D_L, D_M) = 1. \tag{33}$$

Denote by $K = LM$ the composite of L and M. In [13] we considered index form equations in this type of composite fields K. Any integer α of K can be represented in the form

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} l_i m_j \tag{34}$$

with $x_{ij} \in \mathbb{Z}$ $(1 \le i \le r, 1 \le j \le s)$. We proved

Theorem 9. *Assume $(D_L, D_M) = 1$. If α of (34) generates a power integral basis in $K = LM$, then*

$$N_{M/Q}\left(I_L \left(\sum_{i=1}^{s} x_{2i} m_i, \ldots, \sum_{i=1}^{s} x_{ri} m_i \right) \right) = \pm 1 \tag{35}$$

and

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2}l_i,\ldots,\sum_{i=1}^{r} x_{is}l_i\right)\right)=\pm 1. \tag{36}$$

The above equations are *relative index form equations* over the subfields of K. These equation give very much additional information about the unknowns x_{ij}.

8.1. Power integral bases in imaginary quadratic extensions of totally real cyclic fields of prime degree

In the following p will denote an odd prime. Let L be a totally real cyclic number field of degree p, with integral basis $\{l_1=1,l_2,\ldots,l_p\}$ and discriminant D_L. Denote by $I_L(x_2,\ldots,x_p)$ the index form corresponding to the integral basis $\{l_1=1,l_2,\ldots,l_p\}$. Also, let $0<m\in\mathbb{Z}$ be square-free with $m\neq 1,3$ and let $M=\mathbb{Q}(i\sqrt{m})$. An integral basis of M is given by $\{1,\omega\}$ with ω defined as in (26). The discriminant of M is

$$D_M=\begin{cases}-m & \text{if } -m\equiv 1 \bmod 4,\\ -4m & \text{if } -m\equiv 2,3 \bmod 4.\end{cases} \tag{37}$$

As above, we assume that $(D_L,D_M)=1$. Consider the field $K=LM$. The integers of K can be represented in the form

$$\alpha=x_1+x_2l_2+\ldots+x_pl_p+y_1\omega+y_2\omega l_2+\ldots+y_p\omega l_p \tag{38}$$

with $x_j,y_j\in\mathbb{Z}$, $(1\leq j\leq p)$.

Theorem 10. *(Gaál [13]) Assume $m\neq 1,3$ and $(D_L,D_M)=1$. If the integer α of (38) generates a power integral basis in $K=LM$, then*

$$I_L(x_2,\ldots,x_p)=\pm 1, \tag{39}$$

$y_1=\pm 1$ and $y_2=\ldots=y_p=0$.

An example. Consider the family of totally real cyclic quintic fields $L=\mathbb{Q}(\vartheta_n)$ generated by a root of the polynomial $f_n(x)$ as defined in (21) in Section 5.1. Let

$$c=n^4+5n^3+15n^2+25n+25,\quad d=n^3+5n^2+10n+7.$$

Let $0<m\in\mathbb{Z}$ be square-free with $m\neq 1,3$ and let $M=\mathbb{Q}(i\sqrt{m})$. Let ω and D_M be the same as in (26), (37). As a consequence of Theorem 10 we showed (cf. [13])

Theorem 11. *Assume that $m \neq 1,3$, c is square-free and coprime to D_M. Then the field $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ contains no power integral bases.*

9. Fields of degree nine with cubic subfields

As an application of Theorem 9 in [14] we considered fields of degree 9 that are composits of cubic subfields of coprime discriminants. We developed the method for complex cubic fields, but the same ideas work also in other cases.

Let L be a complex cubic field with fundamental unit ε, integral basis $\{1, l_2, l_3\}$ and denote by $I_L(x,y) \in \mathbb{Z}[x,y]$ the corresponding index form. Let M be a complex cubic field with fundamental unit η, integral basis $\{1, m_2, m_3\}$ and denote by $I_M(x,y) \in \mathbb{Z}[x,y]$ the corresponding index form. Assume that the discriminants are coprimes, $(D_L, D_M) = 1$.

Any integral element $\alpha \in K$ can be written as

$$\alpha = \sum_{i=1}^{3}\sum_{j=1}^{3} x_{ij} l_i m_j$$

with rational integers $x_{i,j}, 1 \leq i,j \leq 3$. Set

$$X = x_{12} + x_{22}l_2 + x_{32}l_3, \qquad Y = x_{13} + x_{23}l_2 + x_{33}l_3,$$
$$U = x_{21} + x_{22}m_2 + x_{23}m_3, \qquad V = x_{31} + x_{32}m_2 + x_{33}m_3.$$

If α generates a power integral basis in K then by Theorem 9 (cf. [13]) we have

$$N_{L/Q}(I_M(X,Y)) = \pm 1, \qquad N_{M/Q}(I_L(U,V)) = \pm 1.$$

These equations are **cubic relative Thue equations over cubic fields**. By solving these equations we can determine finitely many $X_0, Y_0, U_0, V_0 \in \mathbb{Z}_M$ such that all solutions are of the form

$$X = \pm\varepsilon^l X_0,\ Y = \pm\varepsilon^l Y_0,\ U = \pm\eta^k U_0,\ V = \pm\eta^k V_0$$

with arbitrary $l, k \in \mathbb{Z}$. Considering the structure of X, Y, U, V observe, that $x_{22}, x_{23}, x_{32}, x_{33}$ occur both in X or Y and U or V, that is by taking conjugates and using Cramer's rule we can express them both in terms of l and in terms of k. This way we get equations that relate the unknown exponents k and l:

$$\alpha_{i1}\left(\varepsilon^{(1)}\right)^l + \alpha_{i2}\left(\varepsilon^{(2)}\right)^l + \alpha_{i3}\left(\varepsilon^{(3)}\right)^l + \alpha_{i4}\left(\eta^{(1)}\right)^k + \alpha_{i5}\left(\eta^{(2)}\right)^k + \alpha_{i6}\left(\eta^{(3)}\right)^k = 0$$

for $i = 1,2,3,4$, where $\varepsilon^{(i)}, \eta^{(j)}$ denote the conjugates of ε, resp. η, with explicitly given algebraic coefficients α_{ij}. In the second part of the algorithm we used these equations to determine the exponents l, k which was still a quite complicated procedure requiring Baker's method and reduction.

Using the algorithm described above we made calculations for the following three examples:

$$\begin{array}{llll} 1. f(x) = x^3 - x + 1, & D_L = -23, & g(x) = x^3 - 2x + 2, & D_M = -76; \\ 2. f(x) = x^3 + x + 1, & D_L = -31, & g(x) = x^3 + x^2 + x + 2, & D_M = -83; \\ 3. f(x) = x^3 + 2x + 1, & D_L = -59, & g(x) = x^3 + x^2 - 2x - 3, & D_M = -87, \end{array}$$

where f and g denote the minimal polynomials of generating elements of L and M, respectively. In each step of the algorithm we had several solutions of the involved equations. However, finally there were no elements in the field $K = LM$ having index 1. The total CPU time for an example was about 1.5 hours on a PC.

10. Concluding remarks

As one can see, the efficients methods are different for each type of number fields. However, there are some common technics that were developed in the course of solving index form equations in cubic, quartic and higher degree number fields that have an important influence for the further development of the algorithms. We do believe that these methods will be applicable for the resolution of many other types of diophantine equations as well.

References

[1] **Archinard G.**, Extensions cubiques cycliques de $\mathbb{Q}$ dont l'annaeau des entiers est monogène, *Enseignement Math.*, **20** (1974), 179-203.

[2] Baker A. and Davenport H., The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford*, **20** (1969), 129-137.

[3] **Baker and G.Wüstholz**, Logarithmic forms and group varieties, *J.Reine Angew. Math.*, **442**(1993), 19–62.

[4] **Bilu Y. and Hanrot G.**, Solving Thue equations of high degree, *J.Number Theory,* **60** (1996), 373-392.

[5] **Dummy D.S. and Kisilevsky H.**, Indices in cyclic cubic fields, *"Number Theory and Algebra",* Academic Press, 1977, 29-42.

[6] **Ennola V., Mäki S. and Turunen R.**, On real cyclic sextic fields, *Math. Comp.,* **45** (1985), 591-611.

[7] **Fincke U. and Pohst M.**, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Math. Comp.,* **44** (1985), 463-471.

[8] **Gaál I.**, On the resolution of inhomogeneous norm form equations in two dominating variables, *Math. Comp.,* **51** (1988), 359-373.

[9] **Gaál I.**, On the resolution of some diophantine equations, *"Computational Number Theory",* Walter de Gruyter, Berlin–New York 1991, 261-280.

[10] **Gaál I.**, Power integral bases in orders of families of quartic fields, *Publ. Math. Debrecen,* **42** (1993), 253-263.

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

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

[13] **Gaál I.**, Power integral bases in composits of number fields, *Canad. Math. Bulletin,* **41** (1998), 158-165.

[14] **Gaál I.**, Solving index form equations in fields of degree nine with cubic subfields (to appear)

[15] **Gaál I.**, An efficient algorithm for the explicit resolution of norm form equations (manuscript)

[16] **Gaál I. and Győry K.**, On the resolution of index form equations in quintic fields, *Acta Arith.* (to appear)

[17] **Gaál I., Pethő A. and Pohst M.**, On the resolution of index form equations in biquadratic number fields I., *J.Number Theory,* **38** (1991), 18-34.

[18] **Gaál I., Pethő A. and Pohst M.**, On the resolution of index form equations in biquadratic number fields II., *J.Number Theory,* **38** (1991), 35-51.

[19] **Gaál I., Pethő A. and Pohst M.**, On the resolution of index form equations in biquadratic number fields III. The bicyclic biquadratic case, *J.Number Theory,* **53** (1995), 100-114.

[20] **Gaál I., Pethő A. and Pohst M.**, On the indices of biquadratic number fields having Galois group V_4, *Arch. Math.,* **57** (1991), 357-361.

[21] **Gaál I., Pethő A. and Pohst M.**, On the resolution of index form equations in quartic number fields, *J.Symbolic Computation,* **16** (1993), 563-584.

[22] **Gaál I., Pethő A. and Pohst M.**, 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.

[23] **Gaál I., Pethő A. and Pohst M.**, On the resolution of index form equations in dihedral number fields, *J. Experimental Math.,* **3** (1994), 245-254.

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

[25] **Gaál I. and Pohst M.**, Power integral bases in a parametric family of totally real quintics, *Math. Comp.,* **66** (1997), 1689-1696.

[26] **Gaál I. and Pohst M.**, On the resolution of relative Thue equations, *Math. Comp.* (to appear)

[27] **Gaál I. and Pohst M.**, Computing power integral bases in octic fields with a quadratic subfield (to appear)

[28] **Gaál I. and Schulte N.**, Computing all power integral bases of cubic number fields, *Math. Comp.,* **53** (1989), 689-696.

[29] **Gras M.N.**, Sur les corps cubiques cycliques dont l'anneau des entiers monogène, *Publ. Math. Fac. Sci. Besançon,* 1973.

[30] **Gras M.N.**, Lien entre le groupe des unités et la monogènéité des corps cubiques cycliques, *Théorie des Nombres Besançon,* 1975-76.

[31] **Gras M.N.**, Z-bases d'entiers $1, \vartheta, \vartheta^2, \vartheta^3$ dans les extensions cycliques de degré 4 de $\mathbb{Q}$, *Théorie des Nombres Besançon,* Années 1979-1980 et 1980-1981.

[32] **Gras M.N.**, Non monogènéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$, *J.Number Theory,* **23** (1986), 347-353.

[33] **Gras M.N. et Tanoe F.**, Corps biquadratiques monogènes, *Manuscripta Math.,* **86** (1995), 63-79.

[34] **Győry K.**, Sur les polynomes à coefficients entiers et de discriminant donné III., *Publ. Math. Debrecen,* **23** (1976), 141-165.

[35] **Győry K. and Papp Z.Z.**, Effective estimates for the integer solutions of norm form and discriminant form equations, *Publ. Math. Debrecen,* **25** (1978), 311-325.

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

[37] **Koppenhöfer D.**, *Über projektive Darstellungen von Algebren kleinen Ranges*, Dissertation, Univ. Tübingen, 1994.

[38] **Lehmer E.**, Connection between Gaussian periods and cyclic units, *Math. Comp.*, **50** (1988), 535-541.

[39] **Lenstra A.K., Lenstra H.W.Jr. and Lovász L.**, Factoring polynomials with rational coefficients, *Math. Ann.*, **261** (1982), 515-534.

[40] **Mäki S.**, *The determination of units in real cyclic sextic fields, Lecture Notes in Mathematics* **797**, 1980.

[41] **Mordell L.J.**, *Diophantine equations,* Academic Press, New York-London, 1969.

[42] **Nakahara T.**, On the indices and integral bases of non-cyclic but abelian biquadratic fields, *Archiv. der Math.*, **41** (1983), 504-508.

[43] **Nakahara T.**, On the minimum index of a cyclic quartic field, *Archiv. der Math.*, **48** (1987), 322-325.

[44] **Pethő A.**, On the resolution of Thue inequalities, *J.Symbolic Comput.*, **4** (1987), 103-109.

[45] **Pethő A. and Schulenberg R.**, Effektives Lösen von Thue Gleichungen, *Publ. Math. Debrecen,* **34** (1987), 189-196.

[46] **Pohst M.**, *Computational algebraic number theory,* DMV Seminar Band **21**, Birkhäuser, 1993.

[47] **Smart N.P.**, Solving discriminant form equations via unit equations, *J.Symbolic Computation*, **21** (1996), 367-374.

[48] **Smart N.P.**, Thue and Thue-Mahler equations over rings of integers, *J.London Math.Soc. (2),* **56** (1997), 455-462.

[49] **Smart N.P.**, *The algorithmic resolution of diophantine equations,* London Math. Soc., Student Texts **41**, Cambridge University Press, 1998.

[50] **Trelina L.A.**, On the greatest prime factor of an index form, *Dokl. Akad. Nauk BSSR,* **21** (1977), 975-976.

[51] **Tzanakis N. and de Weger B.M.M.**, How to explicitely solve a Thue Mahler equation, *Compositio Math.*, **84** (1992), 223-288.

[52] **de Weger B.M.M.**, *Algorithms for Diophantine Equations,* CWI Tract **65**, Amsterdam, 1989.

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

[54] **Williams K.S.**, Integers of biquadratic fields, *Canad. Math. Bull.*, **13** (1970), 519-526.

I. Gaál
Institute of Mathematics and Informatics
Kossuth Lajos University
P.O.B. 12
H-4010 Debrecen, Hungary
igaal@math.klte.hu