Power Integral Bases in Cubic Relative Extensions

István Gaál

CONTENTS

Research supported in part by Grants 25157 and 29330 from the Hungarian National Foundation for Scientific Research and by the Foundation for Hungarian Higher Education and Research.

We give an efficient algorithm for computing relative power integral bases in cubic relative extensions. The problem leads to solving relative Thue equations as described by [Gaál and Pohst 1999] using the enumeration method of [Wildanger 1997].

The article is illustrated by examples of relative cubic extensions of quintic and sextic fields which emphasizes the power of the method. This is the first case that unit equations of 12 unknown exponents are completely solved. The experiences of our computations may be useful for other related calculations, as well.

1. INTRODUCTION

In a series of papers we investigated algorithms for computing power integral bases in cubic [Gaál and Schulte 1989], quartic [Gaál et al. 1993; 1996], quintic [Gaál and Pohst 1997; Gaál and Győry 1999] and some sextic [Gaál 1995; 1996; Gaál and Pohst 1996], octic [Gaál and Pohst 2000], and nonic [Gaál 2000] fields. For a recent survey of connected results see [Gaál 1999]. The enumeration method of [Wildanger 1997] made possible to extend these computations from cubic and quartic fields also to higher degree fields.

Recently we determined relative power integral bases in quartic relative extensions [Gaál and Pohst 2000]. In case of quadratic base fields the results were used to determine all power integral bases of octic fields.

In the present paper we consider the question of determining relative power integral bases in relative cubic extensions. The problem reduces to solving relative Thue equations as described by [Gaál and Pohst 1999], using the enumeration method of [Wildanger 1997].

We make interesting computational experiences about Wildanger's ellipsoid method. Surprisingly the method allows to determine relative power integral bases even for sextic base fields (in the totally real case) as illustrated by the examples. For sextic

1058-6458/2001 $0.50 per page

base fields the resolution of the corresponding relative Thue equation yields solving a unit equation of $r = 12$ unknown exponents. Note that formerly such equations were solved only with at most $r = 10$ unknowns [Wildanger 1997] and it was not obvious that the method works for $r > 10$. The computational experiences show that $r = 12$ is very likely the limit of the method.

2. RELATIVE CUBIC EXTENSIONS

Let M be a field of degree m and let $K = M(\xi)$ be a cubic extension of M, with an algebraic integer ξ. Denote by $\mathbb{Z}_M, \mathbb{Z}_K$ the rings of integers of M, K, respectively. Set $\mathcal{O} = \mathbb{Z}_M[\xi]$, let d be an integer with $d \cdot \mathbb{Z}_K \subseteq \mathcal{O}$ and set $i_0 = [\mathbb{Z}_K : \mathcal{O}]$.

Then any $\alpha \in \mathbb{Z}_K$ can be written in the form

$$\alpha = \frac{X_0 + X_1\xi + X_2\xi^2}{d} \tag{2–1}$$

with $X_0, X_1, X_2 \in \mathbb{Z}_M$. The relative index of α with respect to the extension K/M is

$$I_{K/M}(\alpha) = (\mathbb{Z}_K : \mathbb{Z}_M[\alpha]) = (\mathbb{Z}_K : \mathcal{O}) \cdot (\mathcal{O} : \mathbb{Z}_M[\alpha]). \tag{2–2}$$

For any $\gamma \in M$ denote its conjugates by $\gamma^{(i)}$, for $i = 1, \ldots, m$. For $\gamma \in K$ we denote by $\gamma^{(ij)}$, for $i = 1, \ldots, m$ and $j = 1, 2, 3$, the conjugates of γ so that $K^{(ij)}$ are the images of those embeddings of K which leave the conjugate fields $M^{(i)}$ of M elementwise fixed.

Calculating the relative index analogously to the absolute case we have

$$\begin{aligned} d^{3m} \cdot (\mathcal{O} : \mathbb{Z}_M[\alpha]) &= \prod_{i=1}^{m} \prod_{1 \le j_1 < j_2 \le 3} \left| \frac{\alpha^{(ij_1)} - \alpha^{(ij_2)}}{\xi^{(ij_1)} - \xi^{(ij_2)}} \right| \\ &= \prod_{i=1}^{m} \prod_{1 \le j_1 < j_2 \le 3} \left| X_1^{(i)} + \left(\xi^{(ij_1)} + \xi^{(ij_2)}\right) X_2^{(i)} \right|. \end{aligned}$$

Denote by β the quadratic term of the cubic relative minimal polynomial of ξ over M, that is $\beta^{(i)} = -\xi^{(i1)} - \xi^{(i2)} - \xi^{(i3)}, i = 1, \ldots, m$. Then the above product can be written in the form

$$\prod_{i=1}^{m} \prod_{j=1}^{3} \left| X_1^{(i)} - \left(\beta^{(i)} + \xi^{(ij)}\right) X_2^{(i)} \right|.$$

It means that setting $\rho = \beta + \xi$ we have

$$d^{3m} \cdot (\mathcal{O} : \mathbb{Z}_M[\alpha]) = N_{M/\mathbb{Q}} \left(N_{K/M} \left(X_1 - \rho X_2\right)\right).$$

From this and (2–2) we deduce that the element α of (2–1) generates a power integral basis $\{1, \alpha, \alpha^2\}$ of $\mathbb{Z}_K$ over $\mathbb{Z}_M$ if and only if $i_0 = [\mathbb{Z}_K : \mathcal{O}] = 1$ and $X_1, X_2 \in \mathbb{Z}_M$ are solutions of the relative Thue equation

$$N_{M/\mathbb{Q}} \left(N_{K/M} \left(X_1 - \rho X_2\right)\right) = d^{3m}. \tag{2–3}$$

This equation can be solved by the method of [Gaál and Pohst 1999].

Let $\eta_1, \ldots, \eta_s$ be a system of fundamental units in M and extend this system to a maximal independent system $\eta_1, \ldots, \eta_s, \varepsilon_1, \ldots, \varepsilon_r$ of K. Then

$$X_1 - \rho X_2 = \nu \eta_1^{b_1} \ldots \eta_s^{b_s} \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}$$

with $b_1, \ldots, b_s, a_1, \ldots, a_r \in \mathbb{Z}$ and $\nu \in \mathbb{Z}_K$ is an element of norm d^{3m}. For $I = (ij_1j_2j_3)$ with $1 \le i \le m$, $\{j_1, j_2, j_3\} = \{1, 2, 3\}$ set

$$\beta^{(I)} = \frac{\nu^{(ij_1)} \left(\rho^{(ij_2)} - \rho^{(ij_3)}\right)}{\nu^{(ij_2)} \left(\rho^{(ij_1)} - \rho^{(ij_3)}\right)} \left(\frac{\varepsilon_1^{(ij_1)}}{\varepsilon_1^{(ij_2)}}\right)^{a_1} \cdots \left(\frac{\varepsilon_r^{(ij_1)}}{\varepsilon_r^{(ij_2)}}\right)^{a_r}.$$

The relative Thue equation (2–3) reduces to the unit equation [Gaál and Pohst 1999, (7)], that is

$$\beta^{(I)} + \beta^{(I')} = 1 \tag{2–4}$$

with $I = (ij_1j_2j_3)$, $I' = (ij_3j_2j_1)$ in the unknown exponents $a_1, \ldots, a_r$.

Baker's method gives an initial bound for $A = \max\{|a_1|, \ldots, |a_r|\}$ which is reduced in several steps by applying [Gaál and Pohst 1999, Lemma 1]. The reduced bound implies

$$\frac{1}{S} < \left|\beta^{(I)}\right| < S \tag{2–5}$$

for a certain large S. Set

$$\mathcal{I} = \{(ij_1j_2j_3) : 1 \le i \le m,\ \{j_1, j_2, j_3\} = \{1, 2, 3\}\}.$$

Note that $\mathcal{I}$ contains $3m$ elements. To replace S by a smaller s we have to enumerate those exponent vectors $a_1, \ldots, a_r$ for which

$$\begin{aligned} &\frac{1}{S} \le \left|\beta^{(I)}\right| \le S \quad \text{for all } I \in \mathcal{I}, \\ &\left|\beta^{(I')} - 1\right| \le \frac{1}{s-1} \quad \text{for some } I' \in \mathcal{I}. \end{aligned} \tag{2–6}$$

(compare [Gaál and Pohst 1999, Lemma 2]). The enumeration of this set means enumerating integer vectors in an ellipsoid. Note that we have $3 \cdot m$ such ellipsoids to enumerate. We replace S by smaller values in several consecutive steps. If S is small enough, the solutions $a_1, \dots, a_r$ of (2–4) are already easy to determine.

Our computations show that equation (2–3) is feasible to solve even for quintic or sextic base fields M. Note that this is the first case when cubic relative Thue equations are solved over quintic and sextic fields. For the resolution of these relative Thue equations we have to the solve the unit equation (2–4) in $r = 10$ and $r = 12$ unknown exponents, respectively.

3. EXAMPLES

Example 1. Cubic extension of a quintic field

Let $M = \mathbb{Q}(\mu)$ where μ has minimal polynomial $f(x) = x^5 - 5x^3 + x^2 + 3x - 1$. This totally real quintic field has integral basis $\{1, \mu, \mu^2, \mu^3, \mu^4\}$ and discriminant $D_M = 24217 = 61 \cdot 397$.

Consider now the cubic field $L = \mathbb{Q}(\xi)$ where ξ has minimal polynomial $g(x) = x^3 - x^2 - 4x + 3$. This totally real cubic field has integral basis $\{1, \xi, \xi^2\}$ and discriminant $D_L = 257$.

The totally real composite field $K = LM$ is of degree 15 generated by $\mu\xi$ over $\mathbb{Q}$ with minimal polynomial

$$\begin{aligned} h(x) = x^{15} - 45x^{13} + 4x^{12} + 661x^{11} - 76x^{10} - 3763x^9 \\ + 599x^8 + 9774x^7 - 1911x^6 - 11785x^5 \\ + 2565x^4 + 5877x^3 - 1323x^2 - 972x + 243. \end{aligned}$$

Since $(D_M, D_L) = 1$ the elements

$$\{\mu^i \xi^j : i = 0, \dots, 4,\ j = 0, 1, 2\}$$

form an integral basis of K; compare [Gaál 1998]. We have

$$\begin{aligned} D_K &= 1592306404762918796720884 1 \\ &= 61^3 \cdot 397^3 \cdot 257^5. \end{aligned}$$

Hence $d = 1$ in (2–1) and $i_0 = [\mathbb{Z}_K : \mathcal{O}] = 1$.

The fundamental units of K and M were computed by using Kash [Daberkow et al. 1997]. The set of fundamental units of M formed a subset of the set of fundamental units of K. Hence we had $r = 10$ relative units.

In the unit equation (2–4) we had $r = 10$ unknown exponents. Baker's method gave $A < 10^{86}$ for the exponents of this unit equation. The reduction algorithm of [Gaál and Pohst 1999, Lemma 1] was used

step	X_0	H	X	digits	min
1	10^{86}	10^{900}	1962	1500	180
2	1962	10^{50}	113	150	3
3	113	10^{40}	92	150	3
4	92	10^{35}	80	150	3
5	80	10^{33}	75	150	3

TABLE 1. Original bound X_0, constant H, reduced bound X, number of digits and CPU time in minutes needed for the computation of Example 1.

with 11 terms in the linear form, as shown in Table 1. In the notation of [Gaál and Pohst 1999, Lemma 1], in each step X_0 denotes the original bound for A, H is the constant playing an important role in the corresponding lattice, and X is the reduced bound for A. Table 1 includes the number of digits used for the computation and the execution time of the reduction step. The final bound $A < 75$ implied the bound $S = 10^{1518}$ in (2–5) (compare [Gaál and Pohst 1999]).

In the enumeration procedure (2–6) we had 15 ellipsoids in 10 variables. The enumeration of the integer points of the ellipsoids were performed in several steps, as shown in Table 2. Using the notation of [Gaál and Pohst 1999], the table includes S, s from (2–6), the number of digits used, the number of tuples enumerated in the 15 ellipsoids together and the execution time. The last line corresponds to the ellipsoid [Gaál and Pohst 1999, (23)].

The exponent tuples were tested if there are solutions corresponding to them. The element $\alpha \in \mathbb{Z}_K$ generates a relative power integral basis of K over M if and only if it is of the form

$$\alpha = X_0 + \varepsilon(X_1\xi + X_2\xi^2) \tag{3–1}$$

with arbitrary $X_0 \in \mathbb{Z}_M$, an arbitrary unit ε in M and $X_1 = x_{1,0} + x_{1,1}\mu + x_{1,2}\mu^2 + x_{1,3}\mu^3 + x_{1,4}\mu^4$, $X_2 = x_{2,0} + x_{2,1}\mu + x_{2,2}\mu^2 + x_{2,3}\mu^3 + x_{2,4}\mu^4$, whose coordinates are listed in Table 3.

Example 2. Cubic extension of a sextic field

Let $M = \mathbb{Q}(\mu)$ where μ has minimal polynomial $f(x) = x^6 - 5x^5 + 2x^4 + 18x^3 - 11x^2 - 19x + 1$. This totally real quintic field has integral basis

$$\{1, \mu, \mu^2, \mu^3, \mu^4, \mu^5\}$$

and discriminant $D_M = 592661$ (prime).

step	S	s	digits	tuples	min
1	10^{1518}	10^{50}	200	0	7.0
2	10^{50}	10^{20}	70	0	2.7
3	10^{20}	10^{12}	50	28	1.9
4	10^{12}	10^{10}	50	30	1.5
5	10^{10}	10^{8}	50	617	1.5
6	10^{8}	10^{7}	50	899	1.6
7	10^{7}	10^{6}	50	2629	2.0
8	10^{6}	10^{5}	50	6513	2.7
9	10^{5}	$10^{4.5}$	50	4016	2.1
10	$10^{4.5}$	10^{4}	50	4974	2.2
11	10^{4}	6000	40	2848	1.5
12	6000	3000	40	3390	1.6
13	3000	1500	40	3192	1.5
14	1500	1000	40	2132	1.3
15	1000	500	40	2554	1.3
16	500	250	40	2007	1.2
17	250	150	40	1137	0.9
18	150	100	40	722	0.8
19	100	50	40	715	0.9
20	50	25	40	345	0.7
21	25	12	40	136	0.5
22	12	6	40	45	0.4
23	6	3	40	30	0.3
24	3		40	2	0.2

TABLE 2. Values of S and s, plus computational parameters, arising in the enumeration procedure for Example 1.

$x_{1,0}$	$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$	$x_{2,0}$	$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$
15	−3	−27	1	5	−54	15	96	−8	−20
−1	3	−1	−4	2	0	−1	6	−3	0
−262	77	471	−36	−97	−219	65	394	−30	−81
11	−5	−21	2	4	8	−2	−14	1	3
3	−3	−5	1	1	−7	2	14	−1	−3
7	−13	−1	3	0	3	−10	4	2	−1
−6	0	0	0	0	−5	0	0	0	0
0	−1	0	0	0	−2	1	4	0	−1
2	0	0	0	0	−7	0	0	0	0
−2	5	−4	−1	1	1	6	−5	−1	1
−11	0	24	−1	−5	3	1	−5	0	1
4	4	−1	−1	0	3	4	−1	−1	0
−1	2	4	−1	−1	3	−6	−13	2	3
−5	2	9	−1	−2	−3	−1	5	0	−1
1	−3	−4	1	1	3	−2	−9	1	2
3	−3	−9	1	2	1	0	0	0	0
−2	5	−4	−1	1	4	−3	−5	1	1
0	1	1	0	0	0	−1	0	0	0
−3	0	0	0	0	1	0	0	0	0
0	−3	−4	1	1	3	−3	−9	1	2
0	−1	0	0	0	−1	3	4	−1	−1
−2	3	4	−1	−1	2	0	−5	0	1
−1	0	0	0	0	−1	0	0	0	0
0	0	0	0	0	1	0	0	0	0
1	0	0	0	0	0	0	0	0	0

TABLE 3. Coefficients of X_1 and X_2 (defined by (3–1) for Example 1.

Now consider the cubic field $L = \mathbb{Q}(\xi)$ where ξ has minimal polynomial $g(x) = x^3 - x^2 - 4x + 3$ (same totally real cubic field of Example 1). L has integral basis $\{1, \xi, \xi^2\}$ and discriminant $D_L = 257$.

The totally real composite field $K = LM$ is of degree 18 generated by $\mu\xi$ over $\mathbb{Q}$ with minimal polynomial

$$\begin{aligned} h(x) = x^{18} - 5x^{17} - 82x^{16} + 397x^{15} + 2501x^{14} \\ -11919x^{13} - 34100x^{12} + 169532x^{11} + 187998x^{10} \\ - 1174096x^9 - 154240x^8 + 3624928x^7 \\ - 1182695x^6 - 4239690x^5 + 1472949x^4 \\ + 1786860x^3 - 107325x^2 - 18468x + 729. \end{aligned}$$

Since $(D_M, D_L) = 1$, the elements

$$\{\mu^i \xi^j : i = 0, \dots, 5,\ j = 0, 1, 2\}$$

form an integral basis of K (compare [Gaál 1998]). We have

$$\begin{aligned} D_K &= 599815643792382999560919222221869 \\ &= 257^6 \cdot 592661^3. \end{aligned}$$

Hence $d = 1$ in (2–1) and $i_0 = (\mathcal{O} : \mathbb{Z}_M[\xi]) = 1$.

The fundamental units of K and M were computed by using Kash [Daberkow et al. 1997]. The set of fundamental units of M formed a subset of the set of fundamental units of K. Hence we had $r = 12$ relative units.

Baker's method gave $A < 10^{104}$ for the exponents of the unit equation (2–4). The reduction algorithm [Gaál and Pohst 1999, Lemma 1] was used with 13 terms in the linear form, as shown in Table 4. In the table we use the notation as in Example 1. The final bound $A < 86$ implied the bound $S = 10^{2405}$ in (2–5).

In the enumeration procedure we had 18 ellipsoids in 12 variables. The enumeration of the integer points of the ellipsoids were performed in several steps, as shown in Table 5.

The exponent tuples were tested if there are solutions corresponding them. The test of the 565869 exponent tuples took about 240 minutes of CPU time.

step	X_0	H	X	digits	min
1	10^{104}	10^{900}	1246	1500	290
2	1246	10^{80}	121	200	19
3	121	10^{60}	91	150	14
4	91	10^{57}	86	150	13

TABLE 4. Original bound X_0, constant H, reduced bound X, number of digits and CPU time in minutes needed for the computation of Example 2.

The element $\alpha \in \mathbb{Z}_K$ generates a relative power integral basis of K over M if and only if it is of the form

$$\alpha = X_0 + \varepsilon(X_1\xi + X_2\xi^2)$$

with arbitrary $X_0 \in \mathbb{Z}_M$, an arbitrary unit ε in M and $X_1 = x_{1,0}+x_{1,1}\mu+x_{1,2}\mu^2+x_{1,3}\mu^3+x_{1,4}\mu^4+x_{1,5}\mu^5$, $X_2 = x_{2,0} + x_{2,1}\mu + x_{2,2}\mu^2 + x_{2,3}\mu^3 + x_{2,4}\mu^4 + x_{2,5}\mu^5$, whose coordinates are listed in Table 7 on the next page.

step	S	s	digits	tuples	min
1	10^{2405}	10^{50}	200	0	15
2	10^{50}	10^{20}	100	4	6
3	10^{20}	10^{15}	80	8	4
4	10^{15}	10^{12}	80	396	4
5	10^{12}	10^{10}	80	3419	6
6	10^{10}	10^9	80	4574	6
7	10^9	10^8	80	14413	9
8	10^8	10^7	80	39283	18
9	10^7	$5{\cdot}10^6$	80	18093	11
10	$5{\cdot}10^6$	10^6	80	55989	24
11	10^6	$5{\cdot}10^5$	80	33578	16
12	$5{\cdot}10^5$	10^5	80	95078	37
13	10^5	$5{\cdot}10^4$	80	44819	20
14	$5{\cdot}10^4$	10^4	80	113397	43
15	10000	5000	80	38527	20
16	5000	3000	80	27479	14
17	3000	1500	80	27714	14
18	1500	800	80	19034	11
19	800	400	80	14137	9
20	400	200	80	8529	6
21	200	100	80	4447	5
22	100	50	80	1982	3
23	50	25	80	688	2
24	25	10	80	222	2
25	10	3	80	62	1
26	3		80	2	0.5

TABLE 5. Values of S and s, plus computational parameters, arising in the enumeration procedure for Example 2.

4. COMPUTATIONAL EXPERIENCES

The algorithms were developed in Maple and executed on a 350 MHz Pentium II PC under Linux. The integral bases, discriminants and fundamental units were calculated using Kash [Daberkow et al. 1997]. Note that already the calculation of these basic data is a hard problem in the totally real fields of degree 15 and 18 we investigated. Nevertheless, Kash managed this computation in a couple of minutes. The remaining times were as shown in Table 6.

A considerable amount of CPU time was taken by the reduction procedure. Proceeding from $r = 10$ to $r = 12$ the reduction times are still comparable but the necessary CPU time for enumeration is about 8 times more. (Note that for $r = 10$ we had 15 ellipsoids, for $r = 12$ we had 18 ellipsoids to enumerate, so the main difference in the CPU times is caused by the difference in the number of variables.) Moreover for $r = 12$ considerable CPU time is taken also by testing the possible exponent vectors which was negligable for $r = 10$. These experiences show that $r = 12$ is about the limit of the applicability of the ellipsoid method [Wildanger 1997].

	Example 1	Example 2
reduction	192 min	336 min
enumeration	38.3 min	306.5 min
test	2 min	240 min
total	3.9 hours	14.7 hours

TABLE 6. Summary of the CPU times.

REFERENCES

[Daberkow et al. 1997] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, "KANT V4", *J. Symbolic Comp.* **24** (1997), 267–283.

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

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

[Gaál 1998] I. Gaál, "Power integral bases in composits of number fields", *Canad. Math. Bull.* **41** (1998), 158–165.

$x_{1,0}$	$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$	$x_{1,5}$	$x_{2,0}$	$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$	$x_{2,5}$
12	−150	−139	70	41	−15	−17	45	61	−23	−18	6
−16	−13	8	5	−2	0	5	26	13	−15	−3	2
−33	−13	33	1	−9	2	115	49	−116	−5	32	−7
−3	51	54	−32	−19	8	−1	38	39	−24	−14	6
4	−53	−52	31	17	−7	−1	7	3	−5	1	0
−2	23	8	−8	−2	1	0	−12	1	4	−1	0
−5	7	−6	−2	4	−1	−24	11	50	−12	−16	5
−1	17	19	−8	−6	2	4	−66	−69	33	22	−8
4	−71	−66	40	22	−9	0	−61	−58	34	20	−8
1	11	7	−6	−2	1	0	−31	−29	17	10	−4
0	−3	−7	2	3	−1	−1	28	29	−16	−10	4
0	19	19	−12	−7	3	1	−7	−16	5	6	−2
6	0	0	0	0	0	5	0	0	0	0	0
−3	−6	2	3	−1	0	−1	−11	−7	6	2	−1
0	12	13	−7	−5	2	−1	15	5	−8	−1	1
0	−17	−15	9	5	−2	3	−16	−16	9	5	−2
3	−60	−59	34	20	−8	−1	17	15	−9	−5	2
−2	0	0	0	0	0	7	0	0	0	0	0
1	−4	−9	3	3	−1	−6	−8	3	3	−1	0
−13	−12	15	3	−5	1	−11	−7	6	2	−1	0
2	−13	−15	8	5	−2	−2	5	9	−3	−3	1
−2	−2	1	0	0	0	7	8	−3	−3	1	0
−1	−6	−8	3	3	−1	1	0	0	0	0	0
12	9	−7	−2	1	0	−4	−6	2	3	−1	0
1	7	−2	−3	1	0	−1	12	7	−6	−2	1
1	−3	−7	2	3	−1	0	2	7	−2	−3	1
0	−2	10	0	−4	1	−2	29	−12	−11	7	−1
3	0	0	0	0	0	−1	0	0	0	0	0
1	0	0	0	0	0	−1	12	7	−6	−2	1
1	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0

TABLE 7. Coefficients of X_1 and X_2 for Example 2.

[Gaál 1999] I. Gaál, "Power integral bases in algebraic number fields", *Ann. Univ. Sci. Budapest. Sect. Comp.*, **18** (1999), 61–87.

[Gaál 2000] I. Gaál, "Solving index form equations in fields of degree nine with cubic subfields", *J. Symbolic Comput.* **30** (2000), 181–193.

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

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

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

[Gaál and Pohst 1999] I. Gaál and M. Pohst, "On the resolution of relative Thue equations", to appear in *Math. Comp.*

[Gaál and Pohst 2000] I. Gaál and M. Pohst, "Computing power integral bases in quartic relative extensions", *J. Number Theory* **85** (2000), 201–219.

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

[Gaál et al. 1993] I. Gaál, A. Pethő and M. Pohst, "On the resolution of index form equations in quartic number fields", *J. Symbolic Comput.* **16** (1993), 563–584.

[Gaál et al. 1996] 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.

[Wildanger 1997] 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, Technische Universität Berlin, 1997.

István Gaál, University of Debrecen, Mathematical Institute, H-4010 Debrecen Pf.12., Hungary (igaal@math.klte.hu)

Received February 25, 2000; accepted in revised form September 19, 2000