DE GRUYTER
OPEN

TATRA
MOUNTAINS
Mathematical Publications
DOI: 10.2478/tmmp-2014-0020
Tatra Mt. Math. Publ. **59** (2014), 79–92

CALCULATING POWER INTEGRAL BASES BY SOLVING RELATIVE THUE EQUATIONS

István Gaál — László Remete — Tímea Szabó

ABSTRACT. In our recent paper I. Gaál: *Calculating "small" solutions of relative Thue equations*, J. Experiment. Math. (to appear) we gave an efficient algorithm to calculate "small" solutions of relative Thue equations (where "small" means an upper bound of type 10^{500} for the sizes of solutions). Here we apply this algorithm to calculating power integral bases in sextic fields with an imaginary quadratic subfield and to calculating relative power integral bases in pure quartic extensions of imaginary quadratic fields. In both cases the crucial point of the calculation is the resolution of a relative Thue equation. We produce numerical data that were not known before.

1. Introduction

Calculating power integral bases is a classical field of algebraic number theory (c.f. [7]). Considering several types of number fields we have seen that this problem often leads to the resolution of various types of Thue equations [3]–[6], [9], [10].

We often used the method of A. Pethő [19], based on the continued fraction algorithm, which gave an efficient way to calculate "small" solutions of Thue equations. "Small" yields here an upper bound, say 10^{500}, for the absolute values of the solutions. This was much faster than the complete resolution of the equation, and gave all solutions with very high probability, certainly, all that can be used in practice. (Our experience shows that such equations usually only have a few and rather small solutions.) It made possible to get an overview on the solutions of a huge number of equations. Applying it to problems on power integral

2010 Mathematics Subject Classification: Primary 11Y50; Secondary 11D59, 11R16.
Keywords: relative Thue equation, LLL reduction, relative cubic extension, relative quartic extension, power integral bases, supercomputers.
Partially supported by the European Union, and the European Social Fund through the project Supercomputer, the National Virtual Lab. (grant no.: TAMOP-4.2.2.C-11/1/KONV--2012-0010) and also supported in part by K67580 and K75566 from the Hungarian National Foundation for Scientific Research.

bases, we got an overview about the existence of power integral bases of a huge number of fields (cf., e.g., [13]).

We have also learnt that calculating power integral bases in higher degree number fields having certain subfields often leads to relative Thue equations [6], [9], [10]. Although there is an algorithm for the complete resolution of Thue equations [11], an analogue of Pethő's fast algorihtm [19] was missing in the relative case. Recently the first author [8] developed such a fast algorithm to calculate "small" solutions (e.g., with sizes less than 10^{500}) of relative Thue equations. The algorithm is based on the LLL reduction algorithm [16] as one could expect. Since in higher degree number fields even the calculation of basic field data (integral basis, fundamental units) can become a hard and time consuming problem, this algorithm seems to have several useful applications.

In this paper we present two applications. First we calculate power integral bases in sextic fields with an imaginary subfield. This type of problem we studied already in [9], our purpose to reconsider it is to compare CPU times and to extend the short list of results we got in [9].

Second, we consider pure quartic extensions of imaginary quadratic fields and calculate relative power integral bases in these relative quartic extensions. This calculation generalizes our recent results [13] on power integral bases in pure quartic fields.

2. Basic concepts of power integral bases

Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. An important task in algebraic number theory is to decide if K has *power integral bases*, that is integral bases of the form $\{1, \gamma, \gamma^2, \dots, \gamma^{n-1}\}$ and to determine all generators γ of power integral bases (cf. [7]). In general, if $\{1, \omega_2, \dots, \omega_n\}$ is an integral basis of K, then the discriminant of the linear form $\omega_2 X_2 + \cdots + \omega_n X_n$ can be written as

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

where D_K denotes the discriminant of the field K, and $I(X_2, \dots, X_n)$ is the *index form* corresponding to the above integral basis. As is known, for any primitive element $\gamma = x_1 + \omega_2 x_2 + \cdots + \omega_n x_n \in \mathbb{Z}_K$ (that is $K = \mathbb{Q}(\gamma)$) we have

$$I(\gamma) = \big(\mathbb{Z}_K^+ : \mathbb{Z}[\gamma]^+\big) = |I(x_2, \dots, x_n)|,$$

where the index of the additive groups of the corresponding rings are taken.

$I(\gamma)$ is the *index of* γ, which does not depend on x_1. Therefore the element $\gamma = x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$ generates a power integral basis of K if and only if $x_1 \in \mathbb{Z}$ and $(x_2, \dots, x_n) \in \mathbb{Z}^{n-1}$ is a solution of the *index form equation*

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

This is the way the problem of power integral bases reduces to the resolution of diophantine equations.

There is an extensive literature of index form equations and power integral bases (for a summary cf. [7]).

3. Sextic fields with an imaginary quadratic subfield

In this section we recall the method of [9] based on the input data of M. Olivier [18], calculating power integral bases in sextic fields with an imaginary quadratic subfield. In [9] we calculated all generators of power integral bases in 25 sextic fields of this type. Here we only give the most important steps of the calculation, our point is to compare CPU times with that of [9] and to extend considerably the list of [9] by applying the method of [8].

In the table of [18] the discriminant D_K of the sextic field K, the discriminant D_L of its imaginary quadratic subfield and the cubic minimal polynomial $f(x)$ of ϑ generating K over L is given.

Let $\{1, \omega\}$ be the integral basis of L. The element ϑ is choosen (see [9]) to have relative index 1 over L so that all integral elements of K can be written in the form

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

with $x_i, y_i \in \mathbb{Z}$ $(i = 0, 1, 2)$. Let $\varrho = -\vartheta^{(1)} - \vartheta^{(2)}$ with two distinct roots of $f(x)$. The element α of (2) generates a power integral basis of K if and only if the quadratic integers $X = x_1 + \omega y_1$, $Y = x_2 + \omega y_2$ satisfy the relative Thue equation

$$N_{K/L}(X - \varrho Y) = \nu \qquad \text{in} \quad X, Y \in \mathbb{Z}_L \tag{3}$$

(with a unit ν of L) and x_1, x_2, y_0, y_1, y_2 is a solution of a degree 9 polynomial equation

$$F(x_1, x_2, y_0, y_1, y_2) = \pm 1 \qquad \text{in} \quad x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z} \tag{4}$$

(for the construction of F see [9]). Therefore in order to determine all generators of power integral bases (2) of K one has to determine x_1, x_2, y_1, y_2 by solving the relative Thue equation (3) and to calculate y_0 from (4) ($x_0 \in \mathbb{Z}$ is arbitrary).

In [9] for the complete resolution of the relative Thue equation one had to calculate the basic data (integral basis, fundamental units) of K. We represented $X - \varrho Y$ as a power product of the fundamental units of K and the calculation was focused on the unknown exponents. We used Baker's method, reduction of the bounds and then enumerated the small exponents. The CPU time was about 20 minutes per example.

In our present calculation we compute the solutions of (3) with

$$\max(\overline{|X|}, \overline{|Y|}) < 10^{250} \tag{5}$$

($\overline{|\gamma|}$ denotes the *size* of γ, which is the maximum absolute value of its conjugates). This yields that we calculate all generators of power integral bases of K with $\max(|x_1|, |x_2|, |y_1|, |y_2|) < C$, where C is of magnitude 10^{250} (the exact value of C can be easily calculeted in view of ω). Our list of solutions contains all solutions with very high probability, certainly, all that can be used in practical calculations. Our calculation is focused on the solutions themselves, we do not need any additional calculation of the basic field data. The running time of this method was about 2-5 minutes per example, therefore it was at least 5-10 time faster and made possible to list the results of the first 100 number fields of the smallest discriminant in absolute value.

In the following table for brevity we only list the coordinates $(x_1, x_2, y_1, y_2, y_0)$ of those generators of power integral bases of K (satisfying (5)) which have one or more coordinates ≥ 3 in absolute value. We indicate if there are no solutions (no generators of power integral bases) at all. In all lines where only the field data appear we mean that all solutions have coordinates ≤ 2 in absolute value. In the lines where solutions appear we skiped the solutions with coordinates ≤ 2 in absolute value.

The complete list can be fould at `http://www.math.unideb.hu/~igaal/`.

$D_K = -\,9747, \;\; \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - (1 + \omega)x^2 + \omega x + (1 - \omega);$

$D_K = -\,10816, \omega = i, f(x) = x^3 - (1 + \omega)x^2 + 5\omega x - (1 + 4\omega), (02 - 306), (02 - 307), (01 - 203),$
$(01 - 103), (1 - 121 - 4), (1 - 121 - 3), (1 - 231 - 7), (1 - 231 - 6), (22 - 316), (21 - 112),$
$(31 - 122), (3002 - 1), (3 - 122 - 5), (3 - 122 - 4), (52 - 334), (52 - 235);$

$D_K = -\,11691, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - (1 + \omega)x^2 + (-2 + 2\omega)x + 1, (2 - 201 - 3);$

$D_K = -\,12167, \omega = (1 + i\sqrt{23})/2, f(x) = x^3 - (1 + \omega)x^2 + (-2 + \omega)x + 1;$

$D_K = -\,14283, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 + (1 - \omega)x - 1, (2 - 3 - 304), (33 - 2 - 3 - 4);$

$D_K = -\,16551, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - (1 + \omega)x^2 + 2x + (-1 + \omega), (11 - 413), (30 - 321);$

$D_K = -\,16807, \omega = (1 + i\sqrt{7})/2, f(x) = x^3 - \omega x^2 + (-1 + \omega)x + 1;$

$D_K = -\,19683, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 + (-1 + \omega);$

$D_K = -\,21168, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - x^2 + (1 - 2\omega)x + 1;$

$D_K = -\,21296, \omega = (1 + i\sqrt{11})/2, f(x) = x^3 - \omega x^2 + (-1 + \omega)x + 1;$

$D_K = -\,22592, \omega = i, f(x) = x^3 - (1 + \omega)x^2 + (1 + 2\omega)x - \omega, (12 - 336);$

$D_K = -\,22707, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - (1 + \omega)x^2 + 2\omega x + (1 - 2\omega);$

$D_K = -\,23031, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - x^2 + (-1 + \omega);$

$D_K = -\,24003, \omega = (1 + i\sqrt{3})/2, f(x) = x^3 - x^2 - x + (1 - \omega);$

$D_K = -\,25947, \omega = (1+i\sqrt{3})/2, f(x) = x^3 + x + 1;$

$D_K = -\,29791, \omega = (1+i\sqrt{31})/2, f(x) = x^3 - (1+\omega)x^2 + (-2+\omega)x + 1;$

$D_K = -\,30976, \omega = i, f(x) = x^3 - x^2 + (2-\omega)x - 1;$

$D_K = -\,31347, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + 3\omega x - \omega;$

$D_K = -\,33856, \omega = i, f(x) = x^3 + x - \omega;$

$D_K = -\,34371, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (-1+4\omega)x + (2-\omega), (1-100-3),$
$(2-1-322), (3-2-420);$

$D_K = -\,34992, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + 3\omega x + (1-2\omega);$

$D_K = -\,36963, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + \omega x + (-1+\omega);$

$D_K = -\,40203, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (-2+3\omega)x + (2-\omega);$

$D_K = -\,41472, \omega = i\sqrt{2}, f(x) = x^3 + (1-\omega)x - 1;$

$D_K = -\,41823, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (5-5\omega)x + (-6+2\omega), (0-2-217),$
$(0-1-113), (110-1-3), (2-1-2-15), (310-3-1);$

$D_K = -\,44496, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + 2x - 2, nosolutions;$

$D_K = -\,47680, \omega = i, f(x) = x^3 - \omega x - 1, (3310-1);$

$D_K = -\,47979, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - 2\omega x + (-1+2\omega);$

$D_K = -\,49408, \omega = i, f(x) = x^3 - x^2 + x + \omega;$

$D_K = -\,50139, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - x + (-1+\omega), (4-2-32-1);$

$D_K = -\,52272, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (4-\omega)x + (-3-2\omega), (0-1-113),$
$(1-2-115);$

$D_K = -\,53568, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - \omega x - \omega, nosolutions;$

$D_K = -\,53824, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (2+2\omega)x - 1, nosolutions;$

$D_K = -\,54675, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (2-\omega)x + \omega;$

$D_K = -\,57591, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (3-3\omega)x + 1, (1-2403), (20-311),$
$(3-1-111);$

$D_K = -\,59648, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-1+\omega)x + (1+\omega);$

$D_K = -\,59967, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+2\omega)x - \omega;$

$D_K = -\,60992, \omega = i, f(x) = x^3 - x^2 - (1+\omega)x + 1, (8-4101);$

$D_K = -\,61504, \omega = i, f(x) = x^3 + x - 1;$

$D_K = -\,64827, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - 2x + 1, nosolutions;$

$D_K = -\,65600, \omega = i, f(x) = x^3 - (1+\omega)x^2 - \omega x - 1;$

$D_K = -\,70659, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - 2x + (1-\omega);$

$D_K = -\,72716, \omega = (1+i\sqrt{7})/2, f(x) = x^3 - (1+\omega)x^2 + (-1+2\omega)x + 1, (3-200-1);$

$D_K = -\,73008, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (3-2\omega)x - 1;$

$D_K = -\,73467, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - 2\omega x + 1;$

$D_K = -\,82496, \omega = i, f(x) = x^3 - (1+\omega)x^2 + 1;$

$D_K = -\,82971, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (2+\omega)x + (-2+\omega);$

$D_K = -85131, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (3-2\omega)x + (-1+\omega), (1-1-113);$

$D_K = -86528, \omega = i\sqrt{2}, f(x) = x^3 - \omega x^2 - \omega x - 1;$

$D_K = -87616, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-2+\omega)x + 1;$

$D_K = -87831, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + 2\omega x - (1+\omega);$

$D_K = -91719, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (-1+4\omega)x - 2\omega, (2-211-5);$

$D_K = -92416, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-1+\omega), nosolutions;$

$D_K = -93987, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - 2\omega x + 1, nosolutions;$

$D_K = -94311, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - 3\omega x + (-1+4\omega), (10-1-13);$

$D_K = -95607, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + 2x + \omega;$

$D_K = -96512, \omega = i, f(x) = x^3 - x^2 - x - \omega;$

$D_K = -96579, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (1-\omega)x + (-2+\omega);$

$D_K = -96832, \omega = i, f(x) = x^3 - (1+\omega)x^2 + \omega x + \omega;$

$D_K = -103383, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (3-3\omega)x + (-3+2\omega), (1-1-103);$

$D_K = -104112, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (-2+3\omega)x + (1-2\omega);$

$D_K = -104571, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - (1+2\omega)x + 3\omega;$

$D_K = -106560, \omega = i, f(x) = x^3 - (1+\omega)x^2 - x - 1;$

$D_K = -107163, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (1-2\omega)x + (-2+3\omega), (0100-3);$

$D_K = -107811, \omega = (1+i\sqrt{11})/2, f(x) = x^3 - \omega x^2 + (-3+\omega)x + \omega;$

$D_K = -108459, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (3-3\omega)x + (-2+\omega);$

$D_K = -108544, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-2+\omega)x + (1+\omega);$

$D_K = -108731, \omega = (1+i\sqrt{7})/2, f(x) = x^3 - (1+\omega)x^2 - x + \omega;$

$D_K = -108800, \omega = i, f(x) = x^3 - x^2 + (1-2\omega)x + \omega;$

$D_K = -109539, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + 3x - \omega, (1-1-113);$

$D_K = -109744, \omega = (1+i\sqrt{19})/2, f(x) = x^3 - (1+\omega)x^2 + (-2+\omega)x + 1;$

$D_K = -110079, \omega = (1+i\sqrt{3})/2, f(x) = x^3 + (1-2\omega)x + (2-\omega);$

$D_K = -110144, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-3-\omega)x + (2+3\omega), (02-10-3), (1101-3);$

$D_K = -112192, \omega = i, f(x) = x^3 - x^2 + (-2-3\omega)x - 2\omega, (1-12-13), (4-2011);$

$D_K = -114399, \omega = (1+i\sqrt{3})/2, f(x) = x^3 + (4-\omega)x + (1-3\omega), (2-3-304);$

$D_K = -116800, \omega = i, f(x) = x^3 + (1-3\omega)x + (-2+\omega);$

$D_K = -117207, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - 2x + (1+\omega);$

$D_K = -118287, \omega = (1+i\sqrt{3})/2, f(x) = x^3 + (-2-\omega)x + \omega, (11-1-34);$

$D_K = -122256, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 - x + (1-\omega), nosolutions;$

$D_K = -124848, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - 4\omega x + (-2+4\omega), (0-1-103), (00-1-13),$
$(10-4-37), (1330-7);$

$D_K = -129088, \omega = i, f(x) = x^3 - x^2 + (1-2\omega)x + (1+\omega);$

$D_K = -130032, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (-5+5\omega)x + (6-5\omega), nosolutions;$

$D_K = -130304, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-3+2\omega)x + 2\omega, (4-210-3);$

$D_K = -131787, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (2-3\omega)x + (-1+\omega);$

$D_K = -133407, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 - (1+\omega)x - 1, (4-2-320);$

$D_K = -133839, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 - (1+\omega)x + 2, (10-12-5);$

$D_K = -134811, \omega = (1+i\sqrt{3})/2, f(x) = x^3 + (2-2\omega)x - (1+\omega);$

$D_K = -137200, \omega = (1+i\sqrt{7})/2, f(x) = x^3 - \omega x^2 + (-2+\omega)x + \omega;$

$D_K = -137403, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (-2+3\omega)x + (2-3\omega), nosolutions;$

$D_K = -139023, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (1+2\omega)x - 2;$

$D_K = -139520, \omega = i, f(x) = x^3 + (1-\omega)x - (1+\omega);$

$D_K = -139968, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 - (1+\omega)x + \omega, nosolutions;$

$D_K = -141939, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 - x - \omega;$

$D_K = -143872, \omega = i\sqrt{2}, f(x) = x^3 - \omega x^2 - (1+\omega)x - 1;$

$D_K = -143883, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + \omega x - (1+\omega), nosolutions;$

$D_K = -144207, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - (1+\omega)x^2 + (2-2\omega)x + (-2+\omega), (20-311);$

$D_K = -144448, \omega = i, f(x) = x^3 - (1+\omega)x^2 - (1+\omega)x - 1;$

$D_K = -147008, \omega = i, f(x) = x^3 - (1+\omega)x^2 - (1+2\omega)x + 1;$

$D_K = -147520, \omega = i, f(x) = x^3 - (1+\omega)x^2 + (-2+\omega)x + (2+\omega);$

$D_K = -149283, \omega = (1+i\sqrt{3})/2, f(x) = x^3 - x^2 + (3-\omega)x + (-2+\omega).$

4. Relative power integral bases of pure quartic extensions of imaginary quadratic fields

In a recent paper [13] we considered power integral bases in pure quartic fields. Using a general result of I. Gaál, A. Pethő and M. Pohst [12] on quartic fields this problem could be reduced to the resolution of Thue equations. For pure quartic fields this Thue equation happend to be a binomial Thue equation of type $x^4 - my^4 = \pm 1$. Using the fast algorithm of A. Pethő [19] we calculated the solutions with $\max(|x|, |y|) < 10^{500}$ of these binomial Thue equations up to $m < 10^7$ and used these data for listing all generators of power integral bases of the pure quartic field $K = \mathbb{Q}(\sqrt[4]{m})$ with coefficients in absolute values less than 10^{1000}.

As we shall see in the following, the generalization [10] of [12] can be applied to calculate relative power integral bases of quartic extensions. Moreover, if we consider pure quartic extensions $K = L(\sqrt[4]{m})$ of imaginary quadratic fields L, then we obtain a binomial relative Thue equation for the resolution of which we can efficiently use our algorithm [8].

To fix our notation we let $d > 1$ be a square free integer and $L = \mathbb{Q}(i\sqrt{d})$. We assume $-d \equiv 1 (\mathrm{mod}\ 4)$ therefore $D_L = -d$ and an integer basis of L is $\{1, \omega\}$ with $\omega = (1+i\sqrt{d})/2$.

Let m be a positive integer and consider the pure quartic field $M = \mathbb{Q}(\sqrt[4]{m})$. Set $\xi = \sqrt[4]{m}$. Assume that m is square free, $m \neq \pm 1$ and $m \equiv 2, 3 \pmod 4$. According to A. Hameed, T. Nakahara, S. M. Husnine and S. Ahmad [15] $\{1, \xi, \xi^2, \xi^3\}$ is an integer basis in M with discriminant $D_M = -256m^3$.

As it is well known ([17], [4]), if $(D_L, D_M) = 1$, then

$$\{1, \xi, \xi^2, \xi^3, \omega, \omega\xi, \omega\xi^2, \omega\xi^3\}$$

is an integral basis in the composite field $K = LM = \mathbb{Q}(i\sqrt{d}, \sqrt[4]{m})$. To use this property we shall assume that $-d \equiv 1 (\bmod 4)$, $1 < m \equiv 2, 3 \pmod 4$ and $(d, m) = 1$. Moreover, since our arguments use that $\mathbb{Z}_L$ has unique factorization, we assume that $-d$ is any of -3, -7, -11, -19, -43, -67, -163 (cf. [1]).

Then we can write any $\alpha \in \mathbb{Z}_K$ in the form

$$\alpha = H + X\xi + Y\xi^2 + Z\xi^3 \tag{6}$$

with $H, X, Y, Z \in \mathbb{Z}_L$. We apply now the main result of I. Gaál, A. Pethő and M. Pohst [10] to our relative quartic extension K/L.

Lemma 1. *Let*

$$F(U, V) = U(U^2 - 4mV^2), \quad Q_1 = X^2 - mZ^2, \quad Q_2 = Y^2 - XZ.$$

If α of (6) *generates a relative power integral basis in K over L, then there are $U, V \in \mathbb{Z}_L$ such that*

$$N_{K/L}\big(F(U, V)\big) = \pm 1$$

with

$$Q_1(X, Y, Z) = U, \quad Q_2(X, Y, Z) = V.$$

Proof. This is a direct consequence of [10] using that ξ has relative defining polynomial $x^4 - m$ over L. □

4.1. From index equations to binomial Thue equations

In this section we show that using Lemma 1, determining elements of $\mathbb{Z}_K$ generating relative power integral bases over L can be reduced to solving quartic relative binomial Thue equations over L.

Theorem 2. *If $\alpha = H + X\xi + Y\xi^2 + Z\xi^3$ of* (6) *generates a relative power integral basis of K over L, then there exist a solution $(X_0, Y_0) \in \mathbb{Z}_L^2$ of the relative binomial Thue equation*

$$X_0^4 - mY_0^4 = \zeta \quad \textit{(with a unit } \zeta \in L)$$

such that

$$X = X_0^2\varepsilon_0, \quad Y = \pm X_0Y_0\varepsilon_0, \quad Z = Y_0^2\varepsilon_0. \tag{7}$$

Proof. Assume that $\alpha = H + X\xi + Y\xi^2 + Z\xi^3$ of (6) generates a relative power integral basis of K over L. The first equation of Lemma (1) implies that

$$U\bigl(U^2 - 4mV^2\bigr) = \nu$$

with a unit ν in L. Moreover $U = \eta$ is also a unit in L. Hence

$$V^2 = \frac{\eta^2 - \nu/\eta}{4m}$$

which implies that the only possible value of V is $V = 0$.

Now we utilize the equations of Lemma 1 concerning Q_1 and Q_2. The equation $Q_1(X,Y,Z) = X^2 - mZ^2 = U = \eta$ implies (by unique factorization in L, being valid by the restricted values of d) that X, Z are coprime in $\mathbb{Z}_L$. From the equation $Q_2(X,Y,Z) = Y^2 - XZ = V = 0$ we confer $Y^2 = XZ$ whence (using that X, Z are coprime) $X = A^2\varepsilon_x, Z = B^2\varepsilon_y$ with certain $A, B \in \mathbb{Z}_L$ and units $\varepsilon_x, \varepsilon_y \in \mathbb{Z}_L$ such that their product is a square $\varepsilon_x\varepsilon_y = \varepsilon^2$. Substituting these into equation $Q_1(X,Y,Z) = X^2 - mZ^2 = U = \eta$ we obtain

$$A^4\varepsilon_x^2 - mB^4\varepsilon_y^2 = \eta,$$

whence

$$(A\varepsilon_x)^4 - mB^4\varepsilon_x^2\varepsilon_y^2 = \eta\varepsilon_x^2\,.$$

Finally by $\varepsilon_x\varepsilon_y = \varepsilon^2$ we get

$$(A\varepsilon_x)^4 - m(B\varepsilon)^4 = \eta\varepsilon_x^2\,.$$

This way we arrive at the relative binomial Thue equation

$$X_0^4 - mY_0^4 = \zeta \qquad \text{in} \quad X_0, Y_0 \in \mathbb{Z}_L, \tag{8}$$

where ζ is a unit in $\mathbb{Z}_L$.

Collecting the relations between X, Y, Z and X_0, Y_0 we obtain

$$X = A^2\varepsilon_x = X_0^2\varepsilon_x^{-1},$$

$$Z = B^2\varepsilon_y = \frac{Y_0^2}{\varepsilon^2}\varepsilon_y = Y_0^2\varepsilon_x^{-1},$$

finally

$$Y = \pm\sqrt{XZ} = \pm X_0Y_0\varepsilon_x^{-1}.$$

For any ε_x we can obviously choose an ε_y such that their product is a square. As we see, finally X, Y, Z are only related with X_0, Y_0 by means of ε_x, therefore we obtain the statement of Theorem 2 by taking $\varepsilon_0 = \varepsilon_x^{-1}$. □

4.2. Solutions of relative binomial Thue equations

It follows from Theorem 2 that in order to determine generators of relative power integral bases of K over L we have to solve the relative binomial Thue equation (8).

We have considered $-d = -3, -7, -11, -19, -43, -67, -163$. For all these values of d we used the algorithm [8] to calculate the solutions with $\max(\overline{|X_0|}, \overline{|Y_0|}) < 10^{250}$ of equation (8) over $L = \mathbb{Q}(i\sqrt{d})$, for all m with $1 < m \leq 5000$, $m \equiv 2, 3 \pmod 4$ and $(d, m) = 1$. In the following statements we list the solutions.

Theorem 3. *Let d be one of $-d = -3, -7, -11, -19, -43, -67, -163$, let $L = \mathbb{Q}(i\sqrt{d})$, $\omega = (1+i\sqrt{d})/2$. For $1 < m \leq 5000$, $m \equiv 2, 3(\bmod\ 4)$, $(d, m) = 1$, all solutions with $\max(\overline{|X_0|}, \overline{|Y_0|}) < 10^{250}$ of equation (8) in $(X_0, Y_0) \in \mathbb{Z}_L^2$ are*

1) $(\pm 1, 0)$ *for all d and m;*

2) *up to sign the following pairs for the listed m for all d:*

$$\begin{array}{ll}
m = 2 : (1,1) & m = 626 : (5,1), \\
m = 5 : (3,2) & m = 915 : (11,2), \\
m = 17 : (2,1) & m = 1297 : (6,1), \\
m = 39 : (5,2) & m = 1785 : (13,2), \\
m = 82 : (3,1) & m = 2402 : (7,1), \\
m = 150 : (7,2) & m = 3164 : (15,2), \\
m = 257 : (4,1) & m = 4097 : (8,1), \\
m = 410 : (9,2). &
\end{array}$$

3) *up to sign the following pairs for the listed m for special d:*

for $-d = -3$,

$m = 2 : (\omega, \omega), (-\omega + 1, -\omega + 1),$

$m = 5 : (3\omega, 2\omega), (-3\omega + 3, -2\omega + 2),$

$m = 10 : (-2\omega+1, 1), (-\omega+2, \omega), (-\omega+2, -\omega), (\omega+1, -\omega+1), (\omega+1, \omega - 1),$
$(2\omega - 1, 1),$

$m = 17 : (2\omega, \omega), (-2\omega + 2, -\omega + 1),$

$m = 39 : (5\omega, 2\omega), (-5\omega + 5, -2\omega + 2),$

$m = 82 : (3\omega, \omega), (-3\omega + 3, -\omega + 1),$

$m = 145 : (-4\omega + 2, 1), (-2\omega + 4, \omega), (-2\omega + 4, -\omega), (2\omega + 2, -\omega + 1),$
$(2\omega + 2, \omega - 1), (4\omega - 2, 1),$

$m = 150 : (7\omega, 2\omega), (-7\omega + 7, -2\omega + 2),$

$$
\begin{aligned}
m = {}& 257 : (4\omega,\omega), (-4\omega+4,-\omega+1),\\
m = {}& 410 : (9\omega,2\omega), (-9\omega+9,-2\omega+2),\\
m = {}& 455 : (8,-2\omega+1), (8,2\omega-1), (8\omega,-\omega+2), (-8\omega+8,\omega+1),\\
m = {}& 580 : (17,-4\omega+2), (17,4\omega-2), (17\omega,-2\omega+4), (-17\omega+17,2\omega+2),\\
m = {}& 626 : (5\omega,\omega), (-5\omega+5,-\omega+1),\\
m = {}& 730 : (-6\omega+3,1), (-3\omega+6,\omega), (-3\omega+6,-\omega), (3\omega+3,-\omega+1),\\
& (3\omega+3,\omega-1), (6\omega-3,1),\\
m = {}& 905 : (19,-4\omega+2), (19,4\omega-2), (19\omega,-2\omega+4), (-19\omega+19,2\omega+2),\\
m = {}& 915 : (11\omega,2\omega), (-11\omega+11,-2\omega+2),\\
m = {}& 1111 : (10,-2\omega+1), (10,2\omega-1), (10\omega,-\omega+2), (-10\omega+10,\omega+1),\\
m = {}& 1297 : (6\omega,\omega), (-6\omega+6,-\omega+1),\\
m = {}& 1785 : (13\omega,2\omega), (-13\omega+13,-2\omega+2),\\
m = {}& 2305 : (-8\omega+4,1), (-4\omega+8,\omega), (-4\omega+8,-\omega), (4\omega+4,-\omega+1),\\
& (4\omega+4,\omega-1), (8\omega-4,1),\\
m = {}& 2402 : (7\omega,\omega), (-7\omega+7,-\omega+1),\\
m = {}& 3164 : (15\omega,2\omega), (-15\omega+15,-2\omega+2),\\
m = {}& 4097 : (8\omega,\omega), (-8\omega+8,-\omega+1);
\end{aligned}
$$

for $-d=-7$,

$$
\begin{aligned}
m = {}& 3 : (-2\omega+1,2), (2\omega-1,2),\\
m = {}& 50 : (-2\omega+1,1), (2\omega-1,1),\\
m = {}& 248 : (-6\omega+3,2), (6\omega-3,2),\\
m = {}& 785 : (-4\omega+2,1), (4\omega-2,1),\\
m = {}& 1914 : (-10\omega+5,2), (10\omega-5,2),\\
m = {}& 3970 : (-6\omega+3,1), (6\omega-3,1);
\end{aligned}
$$

for $-d=-11$,

$$
\begin{aligned}
m = {}& 122 : (-2\omega+1,1), (2\omega-1,1),\\
m = {}& 1937 : (-4\omega+2,1), (4\omega-2,1);
\end{aligned}
$$

for $-d=-19$,

$$m = 362 : (-2\omega+1,1), (2\omega-1,1),$$

for $-d=-43$,

$$m = 1850 : (-2\omega+1,1), (2\omega-1,1);$$

for $-d = -67$,

$m = 4490 : (-2\omega + 1, 1)(2\omega - 1, 1)$;

for $-d = -163$,

$m = \ 328 : (-2\omega + 1, 3), (2\omega - 1, 3)$.

Using the solutions of the relative binomial Thue equations we construct the generators of relative power integral bases of K over L.

Theorem 4. *Let d be one of $-d = -3, -7, -11, -19, -43, -67, -163$, let $L = \mathbb{Q}(i\sqrt{d})$, $\omega = (1+i\sqrt{d})/2$. For $1 < m \leq 5000$, $m \equiv 2, 3(\bmod\ 4)$, $(d, m) = 1$, all generators $\alpha = H + X\xi + Y\xi^2 + Z\xi^3$ of relative power integral bases of K over L with $\max(\overline{|X|}, \overline{|Y|}, \overline{|Z|}) < 10^{500}$ are given by*

$$H \in \mathbb{Z}_L \text{ arbitrary}, \quad X = X_0^2\varepsilon_0, \quad Y = \pm X_0 Y_0 \varepsilon_0, \quad Z = Y_0^2\varepsilon_0,$$

where ε_0 is a unit in L and (X_0, Y_0) is listed in Theorem 3.

Proof. This is a consequence of Theorem 2. □

4.3. Specialities of the actual calculations

The algorithm for calculating small solutions of relative Thue equations given in [8] consists of two parts. First the bound on the variables (in our case 10^{250}) is reduced by using LLL reduction algorithm. In these examples the reduced bound was mostly between 10 and 200. In the second step the tiny solutions under the reduced bound (say 200 in our case) are enumerated. In our present calculation for relative binomial Thue equations we reorganized these two parts to make the procedure more efficient.

We proceeded for the given values of d separately.

The first part, the reduction was executed for all single m with the fixed d. (This yields about 3000 values of m allowed by the assumptions.) These (about 3000) reduction procedures were executed (all together) within about 3.2–3.6 hours of CPU time for each d.

The second part of the procedure described in [8], the enumeration of tiny values of the variables (with absolute values under the reduced bound, say 200 in our examples) was performed a different way. We proceeded for all values of d separately. It turned out to be very CPU time consuming to test the tiny values of x_1, y_1, x_2, y_2 for all m if they satisfy the relative Thue equation. On the other hand, we have run the cycles for all x_1, y_1, x_2, y_2 under the reduced bound and determined those m for which they yield a solution. Using integer arithmetic and obvious refinements in the enumeration process to test all x_1, y_1, x_2, y_2 and finding the suitable values of m it took about 3.5 hours.

4.4. CPU times

The CPU times of the paper refer to an average laptop. The programs were developed in Maple [2] and were executed under Linux. The same programs were also tested on the high performance computer (supercomputer) of the University of Debrecen, where we obtained about 20 % better results, calculated for a single processor node.

REFERENCES

[1] BAKER, A.: *Transcendental number theory*. Cambridge University Press, Cambridge, 1990.

[2] CHAR, B. W.—GEDDES, K. O.—GONNET, G.H.—MONAGAN, M. B.—WATT, S. M.: *MAPLE, Reference Manual*. Watcom Publications, Waterloo, Canada, 1988.

[3] GAÁL, I.: *Application of Thue equations to computing power integral bases in algebraic number fields*, in: Proc. of the 2nd Internat. Symposium on Algorithmic Number Theory–ANTS-II (H. Cohen, ed.), Talence, France, 1996, Lecture Notes in Computer Sci., Vol. 1122, Springer-Verlag, Berlin 1996, pp. 151–155.

[4] GAÁL, I.: *Power integral bases in composits of number fields*, Canad. Math. Bull. **41** (1998), 158–161.

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

[6] GAÁL, I.: *Power integral bases in cubic relative extensions*, Experiment. Math. **10** (2001), 133–139.

[7] GAÁL, I.: *Diophantine equations and power integral bases*, Boston, Birkhäuser, 2002.

[8] GAÁL, I.: *Calculating "small" solutions of relative Thue equations*, J. Experiment. Math. (to appear).

[9] GAÁL, I.—POHST, M.: *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J. Symbolic Comput. **22** (1996), 425–434.

[10] GAÁL, I.—POHST, M.: *On the resolution of index form equations in relative quartic extensions*, J. Number Theory **85** (2000), 201–219.

[11] GAÁL, I.—POHST, M.: *On the resolution of relative Thue equations*, Math. Comput. **71** (2002), 429–440.

[12] GAÁL, I.—PETHŐ, A.—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.

[13] GAÁL, I.—REMETE, L.: *Binomial Thue equations and power integral bases in pure quartic fields*, JP J. Algebra Number Theory Appl. **32** (2014), 49–61.

[14] GAÁL, I.—SZABÓ, T.: *Relative power integral bases in infinite families of quartic extensions of quadratic field*, JP J. Algebra Number Theory Appl. **29** (2013), 31–43.

[15] HAMEED, A.—NAKAHARA, T.—HUSNINE, S. M.—AHMAD, S.: *On the existence of canonical number system in certain classes of pure algebraic number fields*, J. Prime Res. Math. **7** (2011), 19–24.

[16] LENSTRA, A. K.—LENSTRA, H. W., JR.—LOVÁSZ, L.: *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[17] NARKIEWICZ, W.: *Elementary and Analytic Theory of Algebraic Numbers (2nd ed.)*. Springer-Verlag, Berlin, 1974.

[18] OLIVIER, M.: *Corps sextiques contenant un corps quadratique (I)*, Sémin. Théor. Nombres Bordx., Sér. II **1** (1989), 205–250.

[19] PETHŐ, A.: *On the resolution of Thue inequalities*, J. Symbolic Comput. **4** (1987), 103–109.

Received September 14, 2014

University of Debrecen
Mathematical Institute
H–4010-Debrecen Pf.12.
HUNGARY

E-mail: igaal@science.unideb.hu
remetel42@gmail.com
szabo.timea@science.unideb.hu