On the Resolution of Index Form Equations in Biquadratic Number Fields, IV

István Gaál, [*]
Kossuth Lajos University, Mathematical Institute
H-4010 Debrecen Pf.12., Hungary

Attila Pethő [†]
University Medical Schoole of Debrecen, Laboratory for Informatics
Nagyerdei krt. 98, H-4028 Debrecen, Hungary

and Michael Pohst [‡]
Fachbereich 3 Mathematik, TU Berlin
Straße des 17.Juni 135, D–1000 Berlin 12, Germany

November 28, 2009

Abstract

In the present paper we describe a new algorithm to determine the minimal index and all elements with minimal index in totally real biquadratic fields with Galois group D8. The method is based on sieving procedures and can be successfully applied in about 70 % of the cases. If the method applicable, then it produces the results very fast, moreover we can characterize the cases, when it is applicable. At the end of the paper we include some tables, demonstrating our computations by using this method.

We also consider the possibilities of applying the Baker–Davenport reduction algorithm in our case. Further, we give an infinite family of totally real quartic fields with Galois group D8 having minimal index 1.

[*] The author is greatful to the Alexander von Humboldt Stiftung for supporting his work and also to the Mathematisches Institut der Heinrich–Heine–Universität Düsseldorf for its hospitality during the author's stay there as a Humboldt–fellow.

[†] Research supported in part by Hungarian National Foundation for Scientific Research Grant 1641/90

[‡] Research supported in part by the Deutsche Forschungsgemeinschaft

1 Introduction

Let K be a quartic number field with Galois group D_8. All such fields can be obtained in the form $K = \mathbf{Q}(\sqrt{\mu})$ with $\mu = (e + f\sqrt{m})/2$ (cf. [13]), where $e, m, f \in \mathbb{Z}$, m is square free, μ is totally positive and not a square in the quadratic subfield $L = \mathbf{Q}(\sqrt{m})$. Let $g = h = 1$ if $m \equiv 1 (\mathrm{mod}\ 4)$ and $g = 0, h = 2$ if $m \equiv 2, 3 (\mathrm{mod}\ 4)$ so that setting $\omega = (g + h\sqrt{m})/2$ we become an integral basis $\{1, \omega\}$ of L. We assume, that there exist $a, b, c, d \in \mathbb{Z}$ such that taking $\psi = \left(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{\mu}\right)/4$ we obtain an integral basis $\{1, \omega, \psi, \omega\psi\}$ of K. If L has class number one, then K has such an integral basis, cf. [13]. We recall (cf. (2) of [4]) that the discriminant of K is

$$D_K = \left((\omega - \omega')^2 (\psi_1 - \psi_3)(\psi_2 - \psi_4)\right)^2$$

where ω' is the conjugate of $\omega \in L$ over $\mathbf{Q}$ and $\psi_i (i = 1, \ldots, 4)$ are the conjugates of $\psi \in K$ over $\mathbf{Q}$. Note that the conjugates of $\sqrt{\mu} \in K$ over $\mathbf{Q}$ are $\sqrt{\mu}, \sqrt{\mu'}, -\sqrt{\mu}, -\sqrt{\mu'}$. with $\mu' = (e - f\sqrt{m})/2$.

Denote by $l_i(\underline{X}) = l_i(X_2, X_3, X_4)$ the conjugates of the linear form $l(\underline{X}) = \omega X_2 + \psi X_3 + \omega\psi X_4$ for $1 \le i, j \le 4$. Then we obtain the six forms

$$\begin{array}{rlll}
l_{12}(\underline{X}) = & (\omega - \omega')X_2 + & (\psi_1 - \psi_2)X_3 + (\omega\psi_1 - \omega'\psi_2)X_4 \\
l_{23}(\underline{X}) = & (\omega' - \omega)X_2 + & (\psi_2 - \psi_3)X_3 + (\omega'\psi_2 - \omega\psi_3)X_4 \\
l_{34}(\underline{X}) = & (\omega - \omega')X_2 + & (\psi_3 - \psi_4)X_3 + (\omega\psi_3 - \omega'\psi_4)X_4 \\
l_{41}(\underline{X}) = & (\omega' - \omega)X_2 + & (\psi_4 - \psi_1)X_3 + (\omega'\psi_4 - \omega\psi_1)X_4 \\
l_{13}(\underline{X}) = & & (\psi_1 - \psi_3)(X_3 + \omega X_4) \\
l_{24}(\underline{X}) = & & (\psi_2 - \psi_4)(X_3 + \omega' X_4) & .
\end{array}$$

The discriminant form

$$D_{K/Q}(\omega X_2 + \psi X_3 + \omega\psi X_4) = \prod_{1 \le i, j \le 4} l_{ij}(\underline{X})$$

can be rewritten as

$$D_{K/Q}(\omega X_2 + \psi X_3 + \omega\psi X_4) = (I(X_2, X_3, X_4))^2 D_K$$

where $I(X_2, X_3, X_4)$ is a form of degree 6 with integer coefficients called the **index form** corresponding to the basis $\{1, \omega, \psi, \omega\psi\}$ of K.

In a series of papers ([4],[5],[6]) we considered the problem of the resolution of the index fom equation

$$I(x_1, x_2, x_3) = J \quad (x_2, x_3, x_4 \in \mathbb{Z}) \tag{1}$$

where J is a given non–zero integer. If $J = \pm 1$ the solutions give all power integral bases of K. In case of biquadratic fields with Galois group D8 we gave [4] a "fast" algorithm to determine the "small" solutions of (1). It means, our algorithm determines the solutions with e.g. $\max(|x_2|, |x_3|, |x_4|) < 10^{20}$ within some seconds. Methods for the complete resolution of (1) we could give until now only in case of quartic fields with Galois group C4 ([5]) and V4 ([6]). These methods produce all solutions of (1), however the computation time is the matter of minutes rather then seconds.

The purpose of the present paper is to describe an algorithm, that in general produces **all solutions** of (1) in quartic fields of Galois group D8, in a fast way. The present method bases on certain **sieving** methods, and reduces the problem of solving (1) to solving equations of type

$$G_n = x^2 + D \tag{2}$$

in $n, x \in \mathbb{Z}$ where G_n is a second order linear recurrence sequence and D is a given integer. The presented method is applicable for determining all solution of (1) only in about 70% of the cases. When it applies to (1), then it produces the all solutions very fast (in some seconds), moreover we characterize those cases when it can be applied successfully. The algorithm is suitable also for determining the minimal index of K (that is to finding the J with minimal absolute value for which (1) is solvable), and to determining all integers of K with minimal index.

Taking the occassion, that in this paper we again consider quartic fields with Galois group D8, our further purpose is to check some other possibilities for the resolution of (1). A well known general method for the resolution of some types of decomposable form equations, among others index form equations is to reduce the equation to a unit equation in two variables and applying the combination of Baker's method and the Baker–Davenport reduction algorithm to it. In Section 8 we show what kind of difficulties arise by an attempt to applying this a method to our equation (1).

In Section 10 we present an infinite family of totally real quartic fields of Galois group D8 with minimal index 1.

Finally, at the end of the paper we incude some numerical results, obtained by the sieving algorithm described in Sections 2–7.

2 From index form equations to linear recurrences

In this Section we show, how can we reduce the index form equation (1) to an equation of type (2), that is to searching for elements of type $x^2 + D$ in second order linear recurrence sequences.

The proofs of the following two statements are essentially those of Proposition 1 and Theorem 1 of [4]. In the sequel α' denotes the conjugate of $\alpha \in L$ over $\mathbf{Q}$.

Proposition 1 *Let $J \in \mathbb{Z} \setminus \{0\}$. $\underline{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ is a solution of (1) if and only if there exist $j_1, j_2 \in \mathbb{Z}$ such that $j_1 j_2 = J$ and*

$$x_3^2 + (w + w')x_3 x_4 + ww' x_4^2 = j_1 \tag{3}$$

and

$$l_{12}(\underline{x}) l_{23}(\underline{x}) l_{34}(\underline{x}) l_{41}(\underline{x}) = j_2 (w - w')^2. \tag{4}$$

Theorem 1 *If the system of equations (3) and (4) has a solution $\underline{x} \in \mathbb{Z}^3$, then there exists a $v \in \mathbb{Z}$ such that*

$$v^2 = j_1^2 \frac{e^2 - f^2 m}{4} \left(\frac{c^2 - d^2 m}{4} \right)^2 + 4 j_2 h^2 m \tag{5}$$

holds.

Now we prove:

Theorem 2 *Assume that the system of equations (3) and (4) has a solution $\underline{x} \in \mathbb{Z}^3$. Let $\varepsilon \geq 1$ be the fundamental unit of L and $\mathcal{B}$ be a maximal set of non-associated elements of $\mathbb{Z}_L$ with norm j_1. Then there exist $\beta \in \mathcal{B}; y, n, v \in \mathbb{Z}; v$ satisfying (5) such that*

$$\frac{(e + f\sqrt{m})(c + d\sqrt{m})^2 \beta^2 \varepsilon^{2n} + (e - f\sqrt{m})(c - d\sqrt{m})^2 \beta'^2 \varepsilon'^{2n}}{2} = my^2 + 8v. \tag{6}$$

For $m \equiv 2, 3 \pmod 4$ the coordinates x_2, x_3, x_4 satisfy

$$x_3 = \frac{\beta \varepsilon^n + \beta' \varepsilon'^n}{2}, \quad x_4 = \frac{\beta \varepsilon^n - \beta' \varepsilon'^n}{2\sqrt{m}} \text{ and } x_2 = \frac{-2(bx_3 + ax_4) + y}{8}$$

and for $m \equiv 1 \ (mod\ 4)$

$$x_3 = \frac{-w'\beta\varepsilon^n + w\beta'\varepsilon'^n}{\sqrt{m}}, \ x_4 = \frac{\beta\varepsilon^n - \beta'\varepsilon'^n}{\sqrt{m}} \ \textit{and} \ x_2 = \frac{-2bx_3 - (a+b)x_4 + y}{4}.$$

Proof Assume that $\underline{x} \in \mathbb{Z}^3$ is a solution of (1). Then there exist by Proposition 1 and by Theorem 1 integers $j_1, j_2, v \in \mathbb{Z}$ for which (3), (4) and (5) hold.

If $m \equiv 2, 3$ (mod 4) then (3) has the form

$$x_3^2 - mx_4^2 = j_1.$$

Hence there exist $\beta \in \mathcal{B}, n \in \mathbb{Z}$ with

$$x_3 + \sqrt{m}x_4 = \beta\varepsilon^n.$$

This implies that x_3 and x_4 are of the form given in the theorem.

Analogously, as we derived (20) of [4] we obtain

$$\frac{(mA_3 + A_4 + A_{34}\sqrt{m})\beta^2\varepsilon^{2n} + (mA_3 + A_4 - A_{34}\sqrt{m})\beta'^2\varepsilon'^{2n}}{4m} =$$

$$= y_1^2 + A_0 - \frac{j_1(mA_3 - A_4)}{2m}. \tag{7}$$

where (since we have $g = 0, h = 2$ in the actual case), the constants in (7) are

$$\begin{aligned} A_3 &= 4m(c^2e + d^2me + 2cdfm) \\ A_4 &= 4m^2(c^2e + d^2me + 2cdfm) = mA_3 \\ A_{34} &= 8m^2(c^2f + d^2mf + 2cde) \\ A_0 &= 32mv. \end{aligned}$$

Because of $A_4 = mA_3$, the third summand on the right side of (7) is 0, and further

$$mA_3 + A_4 + A_{34}\sqrt{m} = 8m^2(e + f\sqrt{m})(c + d\sqrt{m})^2.$$

Thus (7) can be written as

$$2m\left[(e + f\sqrt{m})(c + d\sqrt{m})^2\beta^2\varepsilon^{2n} + (e - f\sqrt{m})(c - d\sqrt{m})^2\beta'^2\varepsilon'^{2n}\right] = y_1^2 + 32mv.$$

As in the actual case e and f are even and m is square-free, $2m$ divides y_1, say $y_1 = 2my$. Dividing the last equation by $4m$ we get (6).

If $m \equiv 1$ (mod 4) then the proof is similar and is left to the reader. □

3 Some properties of recurrence sequences

Let $P, Q \in \mathbb{Z}$ such that $P^2 + 4Q \neq 0$ and denote by α, β the (distinct) zeros of $x^2 - Px - Q$. For $n \in \mathbb{Z}^{\geq 0}$ and in case $|Q| = 1$ even for $n \in \mathbb{Z}$ we set

$$\begin{aligned} V_n(P,Q) &= \alpha^n + \beta^n, \\ U_n(P,Q) &= \frac{\alpha^n - \beta^n}{\alpha - \beta}, \end{aligned}$$

and

$$W_n(P,Q) = \begin{cases} V_n(P,Q) & \text{if P is odd} \\ V_n(P,Q)/2 & \text{otherwise.} \end{cases}$$

It is easy to see that for P even also V_n is even and for P odd the number V_n is even if and only if $n \equiv 0 \pmod 3$. The following properties are easily proved for $n, l \in \mathbb{Z}^{\geq 0}$ ($n, l \in \mathbb{Z}$, if $|Q| = 1$) :

$$\begin{aligned} 2U_{n+l} &= U_n V_l + U_l V_n && (8) \\ 2V_{n+l} &= V_n V_l + (\alpha - \beta)^2 U_n U_l && (9) \\ V_{2n} &= V_n^2 - 2(-Q)^n && (10) \\ U_{2n} &= U_n V_n && (11) \\ V_n &\mid V_{nm} \quad \text{for all odd m.} && (12) \end{aligned}$$

Lemma 1 *Let $|Q| = 1$ and $n = 2^k m \in \mathbb{Z}$ with $k \geq 1$. Additionally, if P is odd let $m \not\equiv 0$ (mod 3) and if $Q = 1$ let m be even. Then the congruences*

$$\begin{aligned} U_{n+l} &\equiv -U_l \pmod{W_{2^{k-1}m}}, && (13) \\ V_{n+l} &\equiv -V_l \pmod{W_{2^{k-1}m}} && (14) \end{aligned}$$

hold for all $l \in \mathbb{Z}$.

Proof We only prove (13) because the proof of the other congruence is similar. By (8),(11) and (10) we obtain

$$\begin{aligned} 2U_{n+l} &= U_n V_l + U_l V_n \equiv U_l V_n \pmod{V_{n/2}} \\ &\equiv -2U_l(-Q)^{n/2} \pmod{V_{n/2}}. \end{aligned}$$

If $Q = -1$ or if $Q = 1$ and m is even we get

$$2U_{n+l} \equiv -2U_l \pmod{V_{n/2}}.$$

If P is even then $V_{n/2}$ is also even, otherwise $(2, V_{n/2}) = 1$ because $3 \not| m$. Dividing the last congruence by 2 we get (13). □

This lemma can be generalized to all second order linear recurrence sequences. If all terms of a sequence $\{G_n\}_{n=0}^{\infty}$ satisfy the equation

$$G_{n+2} = PG_{n+1} + QG_n$$

then $x^2 - Px - Q$ is called the characteristic polynomial of $\{G_n\}$.

Theorem 3 *Let $\{G_n\}$ be a second order linear recurrence sequence of integers with characteristic polynomial $x^2 - Px - Q,\ |Q| = 1$. Let n, k and m be as in Lemma 1. Then the congruence*

$$G_{n+l} \equiv -G_l \pmod{W_{2^{k-1}m}} \tag{15}$$

holds for every $l \in \mathbb{Z}$.

Proof It is well known that

$$G_n = \frac{a\alpha^n - b\beta^n}{\alpha - \beta}$$

for $a = G_1 - \beta G_0, b = G_1 - \alpha G_0$ and $n \in \mathbb{Z}$. Hence a short calculation yields

$$G_n = G_1 U_n + QG_0 U_{n-1}. \tag{16}$$

Using (13) we get (15) immediately. □

4 The first sieving procedure

In the sequel $\left(\frac{x}{m}\right)$ denotes the Jacobi symbol for $x, m \in \mathbb{Z}^{\geq 0}, m > 0$. For an integer m fix a complete residue system mod m and let $r(m)$ denote the length of the minimal period of the sequence $\{U_n \mod m\}$. It follows from (10) that if $\{G_n\}$ denotes a recurrence sequence with the same characteristic polynomial, as $\{U_n\}$ then the minimal period of $\{G_n \mod m\}$ divides $r(m)$. In this case Q is arbitrary.

The following lemma can be used very efficiently to prove that (2) is not solvable or to localize its solutions in a few residue classes with respect to an appropriate module. For $a, b \in \mathbb{Z}$ we denote the least common multiple of a and b by $[a, b]$.

Lemma 2 *Let $D \in \mathbb{Z}$, $S = \{p_1, ..., p_t\}$ a set of prime numbers, $R = [r(p_1), ..., r(p_t)]$ and $\mathcal{M} = \{m_1, ..., m_s\}$ with $0 \leq m_1 < m_2 < ... < m_s < R$. If there exists for all $m \in \mathcal{M}$ an i $(1 \leq i \leq t)$ such that*

$$\left(\frac{G_m - D}{p_i}\right) = -1 \tag{17}$$

then all solution $n, x \in \mathbb{Z}$ of (2) satisfy $n \not\equiv m \pmod{R}$, for all $m \in \mathcal{M}$.

Proof Assume that $n, x \in \mathbb{Z}$ is a solution of (1) with $n \pmod{R} \in \mathcal{M}$. We have

$$\left(\frac{G_n - D}{p}\right) = 1 \quad \text{or} \quad 0 \tag{18}$$

by (2) for all primes p.

On the other hand by assumption there exists a $p_i \in S$ satisfying (17). Because of $n \equiv m \pmod{R}$ and $r(p_i)$ divides R we have $n \equiv m \pmod{r(p_i)}$. Thus $G_n \equiv G_m \pmod{p_i}$ and the equations (18) and (17) are contradictory. □

The idea to use modular methods for the resolution of (2) goes back to Wunderlich [15]. Its combination with an effective upper bound for the solutions was applied by Pethő for determining all cubes [10] and fifth powers [11] in the Fibonacci sequence. An ”intelligent“ implementation of those ideas is described in Nemes [9].

5 The second sieving procedure.

The disadventage of the first sieving procedure is that if (2) has a solution $n, x \in \mathbb{Z}$ then we are not able to localize it in its residue class mod R. Therefore we need another method to prove that for all but one element of the mod R_1 residue class containing n equation (2) is not solvable. Here R_1 denotes another module, which is (we hope) not much bigger as R.

Such a method was invented by Cohn [3] and applied also by Ribenboim [14]. In the next lemma we formulate the background of the algorithm. In the sequel we assume that the recurrence sequences under consideration satisfy $|Q| = 1$.

Lemma 3 *Let $m, D \in \mathbb{Z}$, $S = \{p_1, ..., p_t\}$ a set of prime numbers with $p_i > 3, 1 \le i \le t$. Assume that there exist $a, b_1, ..., b_t \in \mathbb{Z}^{>0}$ such that there exist for every $\alpha \ge a$ integers $\beta_1, ..., \beta_t \in \mathbb{Z}$ such that $0 \le \beta_i \le b_i, i = 1, ..., t$ and*

$$\left(\frac{-G_m - D}{W_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}}\right) = -1. \tag{19}$$

Then (2) has at most one solution $n, x \in \mathbb{Z}$ with

$$n \equiv m \pmod{2^{a+1} p_1^{b_1} \cdots p_t^{b_t}} \tag{20}$$

and this is $n = m$.

Proof Let $n, x \in \mathbb{Z}$ be a solution of (2) satisfying (20) and such that $n \ne m$. Then there exists a $h \in \mathbb{Z}$ such that $n = m + 2^{a+1} sh$, where $s = p_1^{b_1} \cdots p_t^{b_t}$. Let

$h = \pm 2^c h_1$ with h_1 odd. Then $V_{2^{a+c+1}s}$ divides $V_{2^{a+c+1}sh_1}$ because of (12) hence $W_{2^{a+c+1}s}$ divides $W_{2^{a+c+1}sh_1}$ and Lemma 1 yields

$$G_n - D \equiv -G_m - D \pmod{W_{2^{a+c}s}}.$$

Put $\alpha = a + c \geq a$. Then by assumption there exist $\beta_1, ..., \beta_t \in \mathbb{Z}$ with $0 \leq \beta_i \leq b_i, i = 1, ..., t$ satisfying (19). By (12) $V_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}$ divides $V_{2^\alpha p_1^{b_1} \cdots p_t^{b_t}}$, hence the last congruence implies

$$G_n - D \equiv -G_m - D \pmod{W_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}}.$$

This and (19) make it impossible that n, x is a solution of (2). □

How do we apply this lemma?

We can apply Jacobi's reciprocity law almost automatically because for any $n \in \mathbb{Z}$ not divisible by 3 we have

$$W_{4n}(P, Q) \equiv \begin{cases} -1 \pmod 4 & \text{if P is odd} \\ 1 \pmod 4 & \text{if P is even} \end{cases}$$

The proof of this property is a simple application of (12). Choosing $\alpha \geq 2$ and combining the last congruence with (19) we get

$$\left(\frac{-G_m - D}{W_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}} \right) = \pm \left(\frac{W_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}}{G_m + D} \right),$$

where the sign on the right hand side depends only on the sign of $G_m + D$ and on the parity of P. To be able to apply Lemma 3 we have to analyze the sequence V_n more carefully. This is done in the next Section.

6 Analysis of the second sieving procedure

For fixed $t, M \in \mathbb{Z}^{>0}$ define

$$v(t, M, n) \equiv V_{t2^n} \pmod M$$

for every $n \in \mathbb{Z}$, where we take the smallest non-negative residues $\pmod M$. It is obvious that the sequence $\{v(t, M, n)\}_{n=0}^\infty$ is periodic. Let $e(t, M)$ and $r(t, M)$ be the length of the minimal preperiod and of the minimal period of $\{v(t, M, n)\}_{n=0}^\infty$, respectively, normalized such that $e(t, M) \geq 1$.

Lemma 4 *Let t be odd and $M > 1$ then*

$$r(t, M) | r(1, M) \quad \textit{and} \quad e(t, M) \leq e(1, M). \tag{21}$$

Proof We prove (21) by induction on t. It is obviously true for $t = 1$. Assume that it is true for any u with $1 \leq u < t$. Put $e = e(1, M)$ and $r = r(1, M)$. Then

$$v(u, M, e) \equiv v(u, M, r + e) \pmod{M} \tag{22}$$

immediately follows by the induction hypothesis for all odd value of $u, (1 \leq u < t)$. Further, to prove (21) for t, it is sufficient to prove (22) for $u = t$. For $u = 1$ equation (22) means

$$\alpha^{2^e} + \beta^{2^e} \equiv \alpha^{2^{e+r}} + \beta^{2^{e+r}} \pmod{M}. \tag{23}$$

because of the definition of V_n. Taking the t-th power of (23), using the binomial theorem and the identity $\binom{t}{j} = \binom{t}{t-j}$ we get

$$\begin{aligned} &\sum_{j=0}^{(t-1)/2} \binom{t}{j} \left(\alpha^{j2^e}\beta^{(t-j)2^e} + \alpha^{(u-j)2^e}\beta^{j2^e}\right) \\ \equiv &\sum_{j=0}^{(t-1)/2} \binom{t}{j} \left(\alpha^{j2^{e+r}}\beta^{(t-j)2^{e+r}} + \alpha^{(u-j)2^{e+r}}\beta^{j2^{e+r}}\right) \qquad \pmod{M} \end{aligned} \tag{24}$$

We have $j < t - j, \alpha\beta = -Q = \pm 1$ and $e \geq 1$, hence

$$\begin{aligned} \alpha^{j2^e}\beta^{(t-j)2^e} &= \beta^{(t-2j)2^e} \\ \alpha^{(t-j)2^e}\beta^{j2^e} &= \alpha^{(t-2j)2^e}. \end{aligned}$$

Analogous identities hold if we replace e by $e + r$. Thus (24) implies

$$\sum_{j=0}^{(t-1)/2} \binom{t}{j} \left(V_{(t-2j)2^e} - V_{(t-2j)2^{e+r}}\right) \equiv 0 \qquad \pmod{M}.$$

As $t - 2j < t$ for $j > 0$ and $t - 2j$ is always odd, all the summands with $j > 0$ on the left hand side of the last congruence are 0 by the induction hypothesis. The remaining congruence is exactly (22) with $u = t$, and the lemma is proved. □

We can now characterize those values of n, D for which the result of Lemma 4 can be successfully applied. We remark that if m and D are fixed then $-G_m - D$ is a fixed integer, say M.

Theorem 4 *Let $|M| > 1$ be an odd integer. If there exist integers m_1, m_2 such that $e(1, M) < m_1, m_2 \leq e(1, M) + r(1, M)$ and*

$$\left(\frac{W_{2^{m_1}}}{M}\right)\left(\frac{W_{2^{m_2}}}{M}\right) = -1,$$

then for all k, ε such that $e(1,M) < k \leq e(1,M) + r(1,M)$ and $\varepsilon \in \{1,-1\}$ there exists a prime $p > 3$ satisfying

$$\left(\frac{W_{2^k p}}{M}\right) = \varepsilon \quad .$$

Proof Set $e = e(1,M)$ and $r = r(1,M)$ for abbrevation. Denote by $R = R(M)$ the minimal length of the period of the sequence $\{V_n \bmod M\}_{n=-\infty}^{\infty}$. We remark that this sequence is purely periodic for all M because of $|Q| = 1$. Let $R = 2^s u$, with an odd u. Starting, if necessary, with a longer preperiod than the minimal one, we may assume without loss of generality that

$$\left(\frac{W_{2^{m_1}}}{M}\right) = \varepsilon,$$

$e = m_1 \geq s$ and $m_1 \leq k$. By Dirichlet's theorem on primes in arithmetical progressions there exists a prime $p > 3$ which satisfies the congruence $p2^k \equiv 2^{m_1} \pmod{R}$. This implies $V_{2^k p} \equiv V_{2^{m_1}} \pmod{M}$ and as M is odd we get $W_{2^k p} \equiv W_{2^{m_1}} \pmod{M}$ from which the assertion of the theorem follows. □

Combining the results of Theorem 2 and Lemma 4 we immediately get

Corollary 1 *Let $\{G_n\}$ be a recurrence sequence with $|Q| = 1$, $D \in \mathbb{Z}$ and take $M = G_m + D$. Let $\{V_n\}$ be the recurrence sequence defined by the zeros of the characteristic polynomial of $\{G_n\}$. Assume that there exist integers m_1, m_2 such that $e(1,M) < m_1, m_2 \leq e(1,M) + r(1,M)$ and*

$$\left(\frac{W_{2^{m_1}}}{M}\right)\left(\frac{W_{2^{m_2}}}{M}\right) = -1,$$

then there exist an integer $a \leq e(1,M) + r(1,M) + 1$ and primes $p_1, \ldots, p_t > 3$ such that (2) has at most one solution $n, x \in \mathbb{Z}$ with $n \equiv m \pmod{2^a p_1 \cdots p_t}$ and this is $n = m$.

7 The algorithm

In this Section we describe a practical algorithm for the resolution of (1).

The first step is to apply the assertions of Section 1 in order to reduce (1) to (2). In solving (2) we apply the two sieving procedures, called **Sieve 1** and **Sieve 2** in the following.

Sieve 1 means the application of Lemma 2 of Section 4.

Sieve 2 is the following: Let $m \in \mathbb{Z}$ be an index, which survived **Sieve 1**, i.e $m \in [0, R-1] \backslash \mathcal{M}$. Let M be the square free part of $G_m + D$.
Compute the sequence $\left\{ \left(\dfrac{v(1,M,n)}{M} \right) \right\}$. If it is ultimately constant then by Theorem 4. we can not rule out the index m. Try in this case an other index.

If the test was successful, compute the sequences $\left\{ \left(\dfrac{v(p,M,n)}{M} \right) \right\}_{n=0}^{r+e}$ for $p \in \{1, 5, 7, ..\}$ so until you find for any $n \geq e$ a p such that $\left(\dfrac{v(p,M,n)}{M} \right) = \pm 1$. The right side one gets from Lemma 3. For given P, Q and small M one can naturally precompute the suitable sieving moduls, that is the product of the convenient primes.

The proposed method consists of three steps:

Step 1. Choose a modul R_0, and find all solutions of (2) in n modulo R_0. For this purpose use **Sieve 1** so that the absolute smallest representatives of the surviving residue classes correspond to the actual solutions. Denote by $n_i, i = 1, ..., t$ these representatives.

Step 2. Let $1 \leq i \leq t$. By using **Sieve 2** find, if possible, a number $R_i = 2^{k_i} p_{i1} ... p_{is_i}$ with the property that if n is a solution of (2) with $n \equiv n_i \pmod{R_i}$ then $n = n_i$.

Step 3. Prove for each $i(1 \leq i \leq t)$ that if n is a solution of (2) then there is a $j(1 \leq j \leq t)$ with $n \equiv n_j \pmod{R_i}$. Here use again **Sieve 1**.

In Section 9 we are given an elaborated example for the application of the algorithm. Moreover we present the results of a computation, where we applied the algorithm for all totally real quartic fields with discriminant at most 10^6.

8 An attempt for applying the Baker–Davenport reduction method

In this section we demonstrate why is it very important to have such fast methods, like the one described above, that computes all solutions but is not always usable, or the one described in [4] that computes the "small" solutions (that is e.g. the solutions with absolute value $< 10^{20}$) in any case.

In the following we report on the difficulties occurring by an attempt of applying Baker's method combined with an analogue of the reduction algorithm of Baker and Davenport [1] for the complete resolution of index form equations in quartic fields with Galois group D8. The reduction of the equation to a unit equation in two variables and the application of Baker's method and a numerical reduction algorithm due originally to Baker and Davenport is until today the only general method for the complete resolution of some types of decomposable form equations. Unfortunately (as it is shown by our experiments) the complexity of the computations involved grows about exponentially with the unit rank of the splitting field of the equation. That is the reason why a similar method was usable in the case of index form equations in cyclic quartic fields [5], and why it can not be performed in our case within a reasonable time. For the purposes of practical applications it is more worthy e.g. to build up an extensive table of "small" solutions then to waste some weeks of CPU time by proving for a single example that there are really no "large" solutions, only the "small" ones that we have known after the first 10 seconds.

As example we take the totally real quartic field with Galois group D8 and smallest discriminant, that is the field $K = Q(\sqrt{7+2\sqrt{5}})$ with discriminant $D_K = 725$. We set $\mu = 7 + 2\sqrt{5}$, $\mu' = 7 - 2\sqrt{5}$. An integral basis of the field is $\{1, \omega, \psi, \omega\psi\}$ with $\omega = (1+\sqrt{5})/2, \psi = (1+\sqrt{\mu})/2$. Observe that in this case the coefficients of the linear forms $l_{ij}(\underline{X})$ are divisible by the algebraic integers $\gamma_{ij} = \psi_i - \psi_j$. These satisfy $|\gamma_{12}\gamma_{23}\gamma_{34}\gamma_{41}\gamma_{13}\gamma_{24}| = \sqrt{D_K}$ and taking $l^*_{ij}(\underline{X}) = l_{ij}(\underline{X})/\gamma_{ij}$ we can write the index form equation corresponding to the above basis of the field in the form

$$\prod_{1\le i<j\le 4} l^*_{ij}(x_2, x_3, x_4) = \pm 1 \quad (x_2, x_3, x_4 \in \mathbb{Z}). \tag{25}$$

In the following let $x_2, x_3, x_4 \in \mathbb{Z}$ be a solution of (25). In order to obtain a unit equation we use the identity

$$l_{12}(x_2, x_3, x_4) + l_{23}(x_2, x_3, x_4) - l_{13}(x_2, x_3, x_4) = 0$$

that is

$$\gamma_{12} l^*_{12}(x_2, x_3, x_4) + \gamma_{23} l^*_{23}(x_2, x_3, x_4) - \gamma_{13} l^*_{13}(x_2, x_3, x_4) = 0 \quad . \tag{26}$$

By (25) the factors $l_{ij}^*(x_2,x_3,x_4)$ (having algebraic integer coefficients) of the index form equation must be units, however not in K but in the normal closure of K that we shall denote in the following by F.

The field F has discriminant $D_F = 442050625 = 725^2 \cdot 29^2$ and is generated by a root ρ of the polynomial

$$f(x) = x^8 - 6x^7 + 2x^6 + 32x^5 - 33x^4 - 38x^3 + 55x^2 - 13x - 1 \quad .$$

An LLL reduced integral basis $\{\theta_1 = 1, \theta_2, \ldots, \theta_8\}$ in F can be obtained in the form

$$\theta_i = \frac{1}{a_{i9}} \left(\sum_{j=1}^{8} a_{ij} \rho^{j-1} \right) \quad (i = 1, \ldots, 8)$$

where a_{ij} are the entries of the $8 \cdot 9$ matrix

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
-12 & -11 & 6 & 70 & -39 & -18 & 14 & -2 & 7 \\
-9 & 109 & 22 & -203 & 46 & 53 & -21 & 2 & 21 \\
24 & -55 & -40 & -7 & 71 & 1 & -21 & 4 & 21 \\
-4 & 316 & -509 & 28 & 225 & -62 & -14 & 4 & 21 \\
5 & 235 & -230 & -392 & 354 & 67 & -98 & 16 & 21 \\
-32 & 15 & 114 & -147 & 43 & 43 & -28 & 4 & 21 \\
1 & 21 & 9 & -42 & 16 & 10 & -7 & 1 & 3
\end{pmatrix}$$

Considering the conjugates of the elements in the integral basis one observes that

$$\theta_2 = \frac{-1+\sqrt{5}}{2}, \quad \theta_4 = \frac{1+\sqrt{\mu}}{2}, \quad \theta_5 = \frac{1-\sqrt{\mu'}}{2}$$

that is the coefficients occurring in equation (26) are easily expressed in terms of the basis of F:

$$\gamma_{12} = \psi_1 - \psi_2 = \frac{\sqrt{\mu} - \sqrt{\mu'}}{2} = -\theta_1 + \theta_4 + \theta_5$$

$$\gamma_{23} = \psi_2 - \psi_3 = \frac{\sqrt{\mu} + \sqrt{\mu'}}{2} = \theta_4 - \theta_5$$

$$\gamma_{13} = \sqrt{\mu} = -\theta_1 + 2\theta_4 \quad .$$

The field F is totally real with unit rank 7. Its fundamental units are

$$\eta_i = \sum_{j=1}^{8} b_{ij} \theta_j \quad (i = 1, \ldots, 7)$$

where b_{ij} are the entries of the $7 \cdot 8$ matrix

$$\begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & -1 & -2 & 1 & 0 & 0 & -1 \end{pmatrix}$$

We remark, that the integral basis and the fundamental units of F were computed with the KANT system [16].

We can now return to our basic equation (26). Rewrite it in the form

$$\frac{\gamma_{12}}{\gamma_{13}} \frac{l_{12}^*(x_2, x_3, x_4)}{l_{13}^*(x_2, x_3, x_4)} + \frac{\gamma_{23}}{\gamma_{13}} \frac{l_{23}^*(x_2, x_3, x_4)}{l_{13}^*(x_2, x_3, x_4)} = 1 \quad . \tag{27}$$

As we have already seen, all the $l_{ij}^*(x_2, x_3, x_4)$ are units in F. Hence it holds also for their quotiens, that is we can write

$$\frac{l_{12}^*(x_2, x_3, x_4)}{l_{13}^*(x_2, x_3, x_4)} = \pm \prod_{i=1}^{7} \eta_i^{y_i} = \epsilon_1$$

and

$$\frac{l_{23}^*(x_2, x_3, x_4)}{l_{13}^*(x_2, x_3, x_4)} = \pm \prod_{i=1}^{7} \eta_i^{z_i} = \epsilon_2$$

where $y_i, z_i \in \mathbb{Z}$ $(i = 1, \ldots, 7)$ and put $Y = \max_{1 \leq i \leq 7} |y_i|$, $Z = \max_{1 \leq i \leq 7} |z_i|$. In the following we have to consider two cases according as $Y \geq Z$ or $Z \geq Y$. We assume here $Y \geq Z$, the other case should be considered similarly. Further, we set

$$\alpha = \frac{\gamma_{12}}{\gamma_{13}}, \quad \beta = \frac{\gamma_{23}}{\gamma_{13}} \quad .$$

Then equation (27) obtains the form

$$\alpha\epsilon_1 + \beta\epsilon_2 = 1 \tag{28}$$

which is a unit equation over F.

At this point it is important to remark, that $l_{13}^*(x_2, x_3, x_4)$ is a unit in the quadratic subfield $\mathbf{Q}(\sqrt{5})$ and hence if we determine ϵ_1 and ϵ_2, then using the properties of the field and equation (25) it is easy the determine the values of all the forms $l_{ij}^*(x_2, x_3, x_4)$ and from those the values of x_2, x_3, x_4.

Denote by J the conjugate of ϵ_2 for which $|\epsilon_2^{(J)}|$ is maximal. From the system of equations

$$\log|\epsilon_2^{(j)}| = \sum_{i=1}^{7} z_i \log|\eta_i^{(j)}| \quad (j = 1, \ldots, 8)$$

we conclude, that

$$Z \le c_1 |\log|\epsilon_2^{(J)}||$$

where c_1 is the row–norm of the inverse matrix of a matrix obtained from the matrix with $\log|\eta_j^{(i)}|$ in the ith row and jth column, by omitting a row. (For our example we obtained $c_1 = 2.098$.) Taking into consideration, that ϵ_2 is a unit, from the avobe estimate we conclude, that there must be an s for which

$$\log|\epsilon_2^{(s)}| \le \frac{-Z}{7c_1} \quad . \tag{29}$$

We have to consider in our computations all the eight possibilities for s. If Z is not very small (the "small" values can be tested directly) then from (28), (29) and $Y \ge Z$ we obtain

$$\Lambda = |\log|\alpha^{(s)}| + y_1 \log|\eta_1^{(s)}| + \ldots + y_7 \log|\eta_7^{(s)}|| \le$$

$$\le 2|\alpha^{(s)}\epsilon_1^{(s)} - 1| = 2|\beta^{(s)}\epsilon_2^{(s)}| \le c_2 \exp\left(\frac{-Z}{7c_1}\right) \le c_2 \exp\left(\frac{-Y}{7c_1}\right) \tag{31}$$

where $c_2 = 2|\beta^{(s)}|$. (The values of c_2 in cases $s = 1, \ldots, 8$ were between 0.53 and 3.13). On the other hand by applying the estimate of [2] we obtain a lower bound

$$\exp(-c_3(\log Y + c_4)) < \Lambda \quad .$$

Comparing it with (31) we get an upper bound for Y_U for Y, which lays between 10^{75} and 10^{76} in the eight cases.

Divide inequality (31) by $|\log|\eta_7^{(s)}||$ to get

$$|y_1\xi_1 + \ldots + y_6\xi_6 + y_7 + \xi_8| \le c_2 c_5^{-X} \tag{32}$$

with

$$\xi_i = \frac{\log|\eta_i^{(s)}|}{\log|\eta_7^{(s)}|} \quad (i = 1, \ldots, 6), \quad \xi_8 = \frac{\log|\alpha^{(s)}|}{\log|\eta_7^{(s)}|}$$

and $c_5 = \exp(1/7c_1)$. By using the following generalization of the Baker–Davenport method it is possible to reduce the bound Y_U obtained for Y.

Lemma 5 *(Pethő and Schulenberg [12]) Let Q_1, Q_2, Q_3 be positive real numbers with $Q_2 \ge 1, Q_1 > 2^{r-1}((r-1)Q_2+1)$, and let d_1, d_2 be given positive constants.. If q is an integer satisfying*

$$1 \le q \le Q_1 Q_3$$

$$||q\xi_i|| \leq Q_2(Q_1Q_3)^{-1/(r-1)} \quad (i = 1, \ldots, r-1)$$

and

$$||q\xi_{r+1}|| \geq ((r-1)Q_2 + 1)Q_1^{-1/(r-1)}$$

then there is no solution $y_1, \ldots, y_r \in \mathbb{Z}$ *of the inequality*

$$|y_1\xi_1 + \ldots + y_{r-1}\xi_{r-1} + y_r + \xi_{r+1}| \leq d_1 d_2^{-Y}$$

with

$$\frac{\log(Q_1^{r/(r-1)}Q_3d_1)}{\log d_2} < Y \leq Q_3^{1/(r-1)}$$

where $||.||$ *denotes the distance from the nearest integer and* $Y = \max|y_i|$.

We would like to find out, how far were it possible to reduce Y_U by using the lemma. For applying the Lemma we have to take $r = 7,\ d_1 = c_2,\ d_2 = c_5$. The constant Q_3 schould be chosen such that $Q_3^{1/(r-1)} = Y_U$.The best reduction is obtained if we choose Q_1 and Q_2 as small as possible. The Lemma allows to take $Q_2 = 1$ and $Q_1 = 2^{r-1}((r-1)Q_2+1)$. If we could compute such a q and we could repeat again and again the reduction step until the new bound does not decrease any more, then we could reduce Y_U to Y_R which is the maximum of the bounds obtained in the eight cases (the maximum of 704, 729, 666, 672, 690, 669, 699 and 756) that is $Y_R = 756$. These bounds (that can not be diminished any further by this method) we could reach in five reduction steps. (A typical sequence is 10^{75}, 15375, 998, 757, 732, 729.) It would yield, that with the known methods we had to test al least

$$2^7 \cdot 756^7 = 18066022141228700663808 \approx 1.8 \cdot 10^{22}$$

possible vectors $(y_2, ..., y_7)$. The amount of these possibilities is unfortunately too much to test within a reasonable CPU time.

9 Application of the sieve method

For comparison we apply the algorithm of Section 7. to the same problem discussed in the last section. We adopt the notations from Sections 1–5.
The input data we need are: $D_K = 725, m = 5, a = 2, b = 0, c = 2, d = 0, g = h = J = 1, e = 14$ and $f = 4$. Equation (5) has four solutions: $(j_1, j_2, v) = (1, -1, \pm 3)$ and $(1, 1, \pm 7)$. Thus we have to solve four equations of type (6) in integers n, y_1, which are

$$G_n = 5(7+2\sqrt{5})\left(\frac{3+\sqrt{5}}{2}\right)^n + 5(7-2\sqrt{5})\left(\frac{3-\sqrt{5}}{2}\right)^n = y_1^2 + 10v. \qquad (33)$$

The binary recursive sequence $\{G_n\}$ is defined by the initial terms $G_0 = 70$, $G_1 = 55$ and by the difference equation $G_{n+2} = 3G_{n+1} - G_n$ for $n \geq 0$ or $n < 0$. Considering (1) modulo the primes belonging to the set $S = \{3, 7, 11, 13, 29, 31, 41, 61, 71, 83, 167, 211, 241, 281, 421, 911, 1427\}$ we realize by means of Lemma 2 that the solutions of (33) modulo 840 are as listed in table 1.

v	m	y_1	$y = 2y_1/5$
3	1	5	2
-3	4	25	10
-3	0	10	4
7	2	5	2
7	0	0	0
-7	-1	15	6

Table 1.

We apply now the second sieving procedure six times. We have $P = 3, Q = -1$ and $W_k = V_k = \left(\frac{3+\sqrt{5}}{2}\right)^k + \left(\frac{3-\sqrt{5}}{2}\right)^k$. By the remark at the end of Section 5 we have $V_k \equiv -1 \pmod 4$, if k is not divisible by 3.
Let $m = 1, v = 3, D = 30$, then $-G_m - D = -85 = -5 \cdot 17$. Let k be an integer which is not divisible by 3. Then we have

$$\left(\frac{-G_m - D}{V_k}\right) = \left(\frac{-5 \cdot 17}{V_k}\right) = -\left(\frac{V_k}{5}\right)\left(\frac{V_k}{17}\right) = \left(\frac{V_k}{17}\right),$$

as $\left(\frac{V_k}{5}\right) = -1$ for all k. In table 2 we listed the values of $\left(\frac{V_{2^k}}{17}\right)$ and $\left(\frac{V_{5\cdot 2^k}}{17}\right)$ for $k = 0, \ldots, 4$.

k	0	1	2	3	4
$\left(\frac{V_{2^k}}{17}\right)$	-1	-1	1	-1	-1
$\left(\frac{V_{5\cdot 2^k}}{17}\right)$	1	-1	-1	1	-1

Table 2.

The period length of both sequences is 3 and by means of Lemma 3 we get that if $n \equiv 1 \pmod{20}$ then $n = 1$, hence there exist only one solution which is congruent 1 modulo 840.

In five of the six cases similar computation leads to the same result. The new period lengths are $(v, m, NP) = (-3, 4, 1540), (7, 2, 56), (7, 0, 16), (-7, -1, 20)$. Unfortunatelly our method does not work in the last case, namely when $m = 0, v = -3$ and $D = -30$. We have now $-G_m - D = -40 = -2^3 \cdot 5$ but as $\left(\frac{-2^3 \cdot 5}{V_k}\right) = \left(\frac{2}{V_k}\right) = 1$ holds for all $k \geq 0$, which are not divisible by 3, we can not apply Lemma 3.

The above method was implemented in the computer algebra package MAPLE. We tested the method for all totally real number fields of Galois group D_8 with discriminants less then 10^6, and such that their quadratic subfield has class number one. We computed in each case the minimal index and if the method worked all elements with minimal index. In the following table we displayed a statistic of our computation. The numbers in the columns have the following meaning:

$D_{\mathbb{K}}$ Range of discriminants.

2 Number of fields, i.e. the number of index form equations, in the above range.

3 Number of the resulting reccurrence equations of form (1).

4 Number of recurrence equations without solutions, i.e. for which sieve 1. terminated successfull.

5 Number of equivalence classes including solutions of the recurrence equations, detected by sieve 1.

6 Number of solutions of recurrence equations isolated by sieve 2.

7 Number of equivalence classes for which sieve 2. was not able to isolate the solution.

$D_{\mathbb{K}}$	2	3	4	5	6	7
1–100000	379	1036	406	839	574	265
100001–200000	428	1223	590	792	568	224
200001–300000	449	1400	691	856	640	216
300001–400000	442	1404	709	825	610	215
400001–500000	451	1340	705	742	569	173
500001–600000	449	1490	806	799	617	182
600001–700000	431	1268	650	722	545	177
700001–800000	450	1436	767	778	615	163
800001–900000	447	1366	701	770	611	159
900001–1000000	453	1304	670	727	570	157
1–1000000	4379	13267	6595	7850	5919	1931

Table 3.

10 An infinite family of fields with minimal index 1

In this section we describe an infinite family of totally real biquadratic fields with Galois group D8 and minimal index 1.

Theorem 5 *There are infinitely many positive integers k, such that $K = \sqrt{2k+\sqrt{2}}$ is a totally real biquadratic field with minimal index 1.*

Proof Let $k \geq 1$ be integer, and set $\mu = 2k + \sqrt{2}$. The norm of μ (in $\mathbf{Q}(\sqrt{2})$) is

$$N(\mu) = 2(2k^2 - 1) \quad .$$

Obviously, this norm is not divisible by 2^2. It follows from the assertions of Nagel [8] that there are infinitely many positive integers k, such that $2k^2 - 1$ is not divisible by the square of any prime number. For all these values of k the field $\mathbf{Q}(\sqrt{\mu})$ is biquadratic, because μ is square–free. We show, that for all these values of k the field $K = \mathbf{Q}(\sqrt{\mu})$ has minimal index 1.

An integral basis of the field is $\{1, \sqrt{2}, \sqrt{\mu}, \sqrt{2}\sqrt{\mu}\}$ (cf. [13]). Obviously, $\sqrt{2} = (\sqrt{\mu})^2 - 2k$, hence for $\alpha = \sqrt{\mu}$ the system $\{1, \alpha, \alpha^2, \alpha^3\}$ is a power integral basis of K. □

We remark, that the discriminant of the field K involved in Theorem 5 is $D_K = 2^{10}(4k^2 - 2)$. By Proposition 1 in the integral basis $\{1, \sqrt{2}, \sqrt{\mu}, \sqrt{2}\sqrt{\mu}\}$ the index form equation $I(x_2, x_3, x_4) = \pm 1$ is equivalent with the system of equations

$$\begin{aligned} x_3^2 - 2x_4^2 &= \pm 1 \\ 8x_2^4 - 8kx_2^2x_3^2 - 16x_2^2x_3x_4 - 16kx_2^2x_4^2 + x_3^4 + 8kx_3^3x_4 + 4x_3^2x_4^2 + & \\ 16k^2x_3^2x_4^2 + 16kx_3x_4^3 + 4x_4^4 &= \pm 1 \end{aligned}$$

a solution of which is $(x_2, x_3, x_4) = (0, 1, 0)$, which yields the same result.

References

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

[2] J.Blass, A.M.W.Glass, D.K.Manski, D.B.Meronk and R.P.Steiner, *Constants for lower bounds for linear forms in logarithms of algebraic numbers II., The homogeneous rational case*, Acta Arith., **55**, (1990), 15–22.

[3] J.H.E. Cohn, *On square Fibonacci numbers,* J. London Math. Soc. **39** (1964) 537–540.

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

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

[6] I.Gaál, A.Pethő and M.Pohst, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case*, J.Number Theory, to appear.

[7] K. Győry, *On the solutions of linear diophantine equations in algebraic integers of bounded norm,* Ann. Univ. Sci. Eötvös , Sect. Math., **22-23** (1979-1980), 225-233.

[8] T.Nagel, *Zur Arithmetik der Polynome*, Abhandlungen Math. Sem. Hamburg, **1** (1922), 179–194.

[9] I. Nemes, *On the solution of the diophantine equation* $G_n = P(x)$ *with sieve algorithm,* in:Computational Number Theory, Eds.:A. Pethő, M. Pohst, H.C. Williams and H.G. Zimmer, Walter de Gruyter Publ. Co. (1991) pp 303-312.

[10] A. Pethő, *Full cubes in the Fibonacci sequence,* Publ. Math. Debrecen, **30** (1983) 117–127.

[11] A. Pethő, *Perfect powers in second order recurrences,* in:Topics in Classical Number Theory, Eds.: G. Halász, Akadémiai Kiadó, Budapest (1981) pp 1217–1227.

[12] A.Pethő und R.Schulenberg , *Effektives Lösen von Thue Gleichungen*, Publ. Math. (Debrecen), **34** (1987), 189–196.

[13] M.Pohst, *Berechnung unabhängiger Einheiten und Klassenzahlen in total reellen biquadratischen Zahlkörpern*, Computing **14** (1975), 67–78.

[14] P. Ribenboim, *Square classes of Fibonacci and Lucas numbers,* Portugaliae Math. **46** (1989), 159-175.

[15] M.C. Wunderlich, *On the existence of Fibonacci squares,* Math. Comp. **17** (1963) 455–457.

[16] M.Pohst, Computational Algebraic Number Theory, Birkhäuser Verlag, to appear.