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

I. Gaál
Kossuth Lajos University, Mathematical Institute,
Debrecen, Pf 12, H-4010 Hungary,

A. Pethő
Laboratory for Computer Science
University Medical Schoole of Debrecen
Nagyerdei krt. 98, H-4028 Debrecen Hungary

and

M. Pohst
Mathematisches Institut
Heinrich Heine Universit"at D"usseldorf
Universit"atsstra"se 1, 4000 D"usseldorf 1, Germany

November 28, 2009

1 Introduction

Let $\mathbb{K}$ be a quartic number field with Galois group D_8 and denotes $\mathbb{L} = \mathbf{Q}(\sqrt{m})$ its quadratic subfield. As in the paper [2] we assume that the extension $\mathbb{K}/\mathbb{L}$ has a relative integral basis and $\mathbb{K}$ is given in the form $\mathbb{K} = \mathbf{Q}(\sqrt{\mu})$, with $\mu = \frac{e+f\sqrt{m}}{2}$ beeing a squre free integer in $\mathbb{L}$.

Extending and making more explicite the results of [2] we are given in this paper a method for the resolution of the index form equation

$$I_{\mathbf{K}/\mathbf{Q}}(x_1, x_2, x_3) = J, \tag{1}$$

where J denotes a given non-zero integer. We are given also an algorithm for establishing the minimal index of the field $\mathbb{K}$.

Our method is based on an algorithm, which solves diophantine equations of type

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

where D is a given integer and G_n denotes the $n-$th term of a linear recurrence sequence of order two. The presented method does not work for all equations of form (2), but we are able to characterise the cases when it can be applied successfully.

Our notations will be the same as in [2], if needed we refer equation 'x' of [2] as (1.x).

2 Translation of (1) to (2)

The proof of the following two statements are essentially the same as the proof of Proposition 1 and Theorem 1 of [2]. In the sequel α' denotes the conjugate of $\alpha \in \mathbb{L}$.

Proposition 1 *Let $J \in \mathbb{Z}$. $\underline{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ 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*

$$x_3^2 + (w + w')x_3x_4 + ww'x_4^2 = j_1 \tag{3}$$

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.

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 $\mathbb{Z}_{\mathbb{L}}$ and $\mathcal{B}$ be a maximal set of non-associated elements of $\mathbb{Z}_{\mathbb{L}}$ with norm j_1. Then there exist $\beta \in \mathcal{B}; y, n, v \in \mathbb{Z}; v$ satisfying (5) such that*

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

holds. Further, if $m \equiv 2, 3 \pmod 4$ then

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

and if $m \equiv 1 \pmod 4$ then

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

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 $m \equiv 2, 3 \pmod 4$ 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 have the form given in the theorem.
Inserting x_3 and x_4 into (1.19) we obtain

$$\frac{(mA_3 + A_4 + A_{34}\sqrt{m})\beta^2\varepsilon^{2n} + (mA_3 + A_4 - A_{34}\sqrt{m})\beta'^2\varepsilon'^{2n}}{4m} = y_1^2 + A_0 - \frac{j_1(mA_3 - A_4)}{2m}. \tag{7}$$

Using that we have $g = 0, h = 2$ in the actual case, the constants appearing in 7 become

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

Hence the third summand staying on the right hand side of 7 is 0, and

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

Thus 7 has the form

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

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) at once.
If $m \equiv 2, 3 \pmod 4$ then the proof is similar and is left to the reader. □

3 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 even $n \in \mathbb{Z}$ in case $|\mathbf{Q}| = 1$ 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 even P also V_n is even and for odd P the number V_n is even if and only if $n \equiv 0 \ (mod\ 3)$. The following properties can be proved for $n, l \in \mathbb{Z}$ without difficulties:

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

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*

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

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

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

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

$$2U_{n+l} \equiv -2U_l \ (mod\ V_{n/2}).$$

If P is even then $V_{n/2}$ is even too, 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 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 recurrence sequence of integers with characteristic polynomial $x^2 - Px - Q$. Let n, k and m be as in Lemma 1. Then the congruence*

$$G_{n+l} \equiv -G_l \ (mod\ W_{2^{k-1}m}) \qquad (14)$$

is satisfied 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 calculation yields

$$G_n = G_1 U_n + Q G_0 U_{n-1}. \tag{15}$$

Using (13) we get (14) immediately. □

4 Background of the first sieving procedure

In the sequel $\left(\frac{x}{m}\right)$ denotes the Jacobi symbol for $x, m \in \mathbb{Z}, m > 0$. For an integer m fix an 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 $r(m)$. This time 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 $a, b \in \mathbb{Z}$ $[a, b]$ will denote the least common multiple of a and 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 $0 \le m_1 < m_2 < ... < m_s < R$. If there exists for all $m \in \mathcal{M}$ an $1 \le i \le t$ such that*

$$\left(\frac{G_m - D}{p_i}\right) = -1 \tag{16}$$

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

$$\left(\frac{G_n - D}{p}\right) = 1 \quad \text{or} \quad 0 \tag{17}$$

by (2) for all primes p.
On the other hand there exists by the assumption of the lemma a $p_i \in S$ with (16). As $n \equiv m \pmod R$ 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 (17) and (16) are contradictory. □

The idea to use modular method for the resolution of (2) goes back to Wunderlich [8]. The combination of it with effective upper bound for the solutions was applied by Pethő for establishing the cubes [5] and the fifth powers [6] in the Fibonacci sequence. An "intelligent" implementation is described in Nemes [4].

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 elements of the residue class mod R_1 containing n equation (2) is not soluble. Here R_1 denotes an other module, which is (at least we hope) not much bigger as R.
Such a method was found by Cohn [1] and applied also by Ribenboim [7]. In the next lemma we formulate the background of the algorithm. We assume in the sequel that for the occouring recurrence sequences $|Q| = 1$.

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

$$\left(\frac{-G_m - D}{W_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}} \right) = -1. \tag{18}$$

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

$$n \equiv m \ (mod\ 2^{a+1} p_1^{b_1} \cdots p_t^{b_t}) \tag{19}$$

and this is $n = m$.

Proof Let $n, x \in \mathbb{Z}$ be a solution of (2) with (19). Then there exists a $h \in \mathbb{Z}$ such that $n = m2^{a+1}sh$, 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 $V_{2^{a+c+1}sh_1}$ by (12) and

$$G_n - D \equiv -G_m - D \ (mod\ W_{2^{a+c}s})$$

by Lemma 1. Put $\alpha = a + c \geq a$. Then there exist by the assumption $\beta_1, ..., \beta_t \in \mathbb{Z}$ with $0 \leq \beta_i \leq b_i, i = 1, ..., t$ satisfying (18). As by (12) we have $V_{2^\alpha p_1^{\beta_1} \cdots p_t^{\beta_t}}$ divides $V_{2^\alpha p_1^{b_1} \cdots p_t^{b_t}}$ the last congruence implies

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

This together with (18) contradicts that n, x is a solution of (2). □

How to use this lemma?
We can apply Jacobi's reciprocity law almost automatically because of the following property of the sequence W_n.

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

is true for any $n \in \mathbb{Z}$, which is not divisible by 3. The proof is a simple application of (12). Choosing $\alpha \geq 2$ and combining the last congruence with (18) 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 of 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

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

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 $r(t, M)$ the length of the minimal preperiod, normalized such that $e \geq 1$, and the minimal period of $\{v(t, M, n)\}_{n=0}^{\infty}$ respectively. Then we have

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

$$r(t, M) | r(1, M) \quad \textit{and} \quad e(t, M) \leq e(1, M). \tag{20}$$

Proof We prove (20) by induction on t. It is obviously true for $t = 1$. Assume that it is true for any all u with $1 \leq u < t$. Put $e = e(1, M)$ and $r = r(1, M)$. Then

$$v(u, M, e) \equiv v(u, M, r + e) \ (mod\ M) \tag{21}$$

immediately follows by the induction hypothesis for all $1 \leq u < t, u$ odd. Furthermore to prove (20) for t, it is sufficient to prove (21) for $u = t$. For $u = 1$ equation (21) means by the definition of V_n

$$\alpha^{2^e} + \beta^{2^e} \equiv \alpha^{2^{e+r}} + \beta^{2^{e+r}} \ (mod\ M). \tag{22}$$

Taking the t-th power of (22), using the binomial theorem and the identity $\binom{t}{j} = \binom{t}{t-j}$ we get

$$\begin{aligned} & \sum_{j=0}^{(t-1)/2} \binom{t}{j} \left(\alpha^{j2^e} \beta^{(t-j)2^e} + \alpha^{(u-j)2^e} \beta^{j2^e}\right) \\ \equiv & \sum_{j=0}^{(t-1)/2} \binom{t}{j} \left(\alpha^{j2^{e+r}} \beta^{(t-j)2^{e+r}} + \alpha^{(u-j)2^{e+r}} \beta^{j2^{e+r}}\right) \qquad (\text{mod } M). \end{aligned} \tag{23}$$

We have $j < t-j, \alpha\beta = -Q$ 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 (23) implies

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

As $t-2j < t$ for $j > 0$ and $t-2j$ is always odd, all the summands with $j > 0$ staying on the left hand side of the last congruence, are 0 by the inductions hypothesis. The remaining congruence is exactly (21) with $u = t$, and the lemma is proved. □

We are now in the position to be able to characterize those values of n, D for which the result of Lemma 4 can be applied successfuly. We remark that if n and D are fixed then $-G_n - D$ 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 $e(1,M) \leq m_1, m_2 \leq e(1,M) + r(1,M)$ and*

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

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

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

holds.

Proof Take $e = e(1,M)$ and $r = r(1,M)$ for simplicity. Denotes $R = R(M)$ the minimal length of period of the sequence $\{V_n \bmod M\}_{n=-\infty}^{\infty}$. We remark that this sequence is for all M purelly periodic because $|Q| = 1$. Let $R = 2^s u$, where u is odd. Starting, if necessary, with a longer preperiod as 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 $m_1 \leq m$. There exists by Dirichlet's theorem on primes in arithmetical progressions a prime p which satisfies the congruence $p2^m \equiv 2^{m_1}\ (mod\ R)$. This implies $V_{2^m p} \equiv V_{2^{m_1}}\ (mod\ M)$ and as M is odd we get $W_{2^m p} \equiv W_{2^{m_1}}\ (mod\ M)$ from which the assertion of the theorem follows at once. □

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

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 recursive sequence defined by the zeros of the characteristic polynomial of $\{G_n\}$. Assume that there exist integers m_1, m_2 such that $e(1, M) \leq m_1, m_2 \leq e(1, M) + r(1, M)$ 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 $n = m$.

References

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

[2] 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.

[3] 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.

[4] 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.

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

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

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

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