On the Resolution of Index Form Equations in Dihedral Quartic Number Fields

István Gaál, Attila Pethő and Michael Pohst

CONTENTS

Gaál is grateful 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 his stay there as a Humboldt fellow.

Pethő was supported by Hungarian National Foundation for Scientific Research Grant 1641/90.

Pohst was supported by the Deutsche Forschungsgemeinschaft.

We describe a new algorithm, based on sieving procedures, for determining the minimal index and all elements with minimal index in a class of totally real quartic fields with Galois group D_8. It is not universally applicable, but its applicability is easily checked for any particular example, and it is very fast when applicable. We include several tables demonstrating the potential of the method. (A more general approach for quartic fields, described in [Gaál et al.], requires much more computation time for each field.)

Finally, we present a family of totally real quartic fields with Galois group D_8 and having minimal index 1 (that is, a power integral basis).

1. INTRODUCTION

Let K be a totally real quartic number field with Galois group D_8. Such fields can be obtained in the form $K = \mathbb{Q}(\sqrt{\mu})$, with an algebraic integer $\mu = \frac{1}{2}(e + f\sqrt{m})$, where e, m, f are integers, m is square-free, and μ is totally positive and not a square in the quadratic subfield $L = \mathbb{Q}(\sqrt{m})$.

Fixing the notation above, set

$$\begin{cases} g = h = 1 & \text{if } m \equiv 1 \bmod 4, \\ g = 0 \text{ and } h = 2 & \text{if } m \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

so that for $\omega = \frac{1}{2}(g + h\sqrt{m})$ the pair $\{1, \omega\}$ is an integral basis of L. We assume that K/L has a relative integral basis. Hence, a basis of K over $\mathbb{Q}$ is of the form $\{1, \omega, \psi, \omega\psi\}$, with

$$\psi = \tfrac{1}{4}(a + b\sqrt{m} + (c + d\sqrt{m})\sqrt{\mu})$$

for suitable $a, b, c, d \in \mathbb{Z}$ (see [Pohst 1975], for example). We know that K has such an integral basis

1058-6458/96 \$0.50 per page

if L has class number one. We recall [Gaál et al. 1991a, eq. (2)] that the discriminant of K is

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

where $\omega' = \frac{1}{2}(g - h\sqrt{m})$ and $\psi_1, \dots, \psi_4$ are the conjugates of $\psi \in K$ over $\mathbb{Q}$ ordered in correspondence with $\sqrt{\mu}$, $\sqrt{\mu'}$, $-\sqrt{\mu}$, $-\sqrt{\mu'}$, where $\mu' = \frac{1}{2}(e - f\sqrt{m})$. (In general we will use a prime $'$ to denote the nontrivial $\mathbb{Q}$-automorphism of L.)

For $1 \le i \le 4$, let $l_i(\underline{X}) = l_i(X_2, X_3, X_4)$ be the conjugates of the linear form $l(\underline{X}) = \omega X_2 + \psi X_3 + \omega\psi X_4$. Then we obtain forms $l_{ij}(\underline{X}) := l_i(\underline{X}) - l_j(\underline{X})$, for $1 \le i, j \le 4$, $i \ne j$. We list them for $i < j$:

$$\begin{aligned}
l_{12}(\underline{X}) &= (\omega - \omega')X_2 + (\psi_1 - \psi_2)X_3 + (\omega\psi_1 - \omega'\psi_2)X_4,\\
l_{23}(\underline{X}) &= (\omega' - \omega)X_2 + (\psi_2 - \psi_3)X_3 + (\omega'\psi_2 - \omega\psi_3)X_4,\\
l_{34}(\underline{X}) &= (\omega - \omega')X_2 + (\psi_3 - \psi_4)X_3 + (\omega\psi_3 - \omega'\psi_4)X_4,\\
l_{14}(\underline{X}) &= (\omega - \omega')X_2 + (\psi_1 - \psi_4)X_3 + (\omega\psi_1 - \omega'\psi_4)X_4,\\
l_{13}(\underline{X}) &= (\psi_1 - \psi_3)(X_3 + \omega X_4),\\
l_{24}(\underline{X}) &= (\psi_2 - \psi_4)(X_3 + \omega' X_4).
\end{aligned}$$

The discriminant form

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

can be written as

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

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

In a series of papers [Gaál et al. 1991a; 1991b; 1995] we considered the problem of the resolution of the index form equation

$$I(x_2, x_3, x_4) = J \quad \text{with } x_2, x_3, x_4 \in \mathbb{Z} \tag{1.1}$$

for a given nonzero integer J. For $J = \pm 1$ the solutions yield all power integral bases of K. In the case of quartic fields containing a quadratic subfield we gave in [Gaál et al. 1991a] a "fast" algorithm for determining the "small" solutions of (1.1), that is, solutions with $\max(|x_2|, |x_3|, |x_4|) < 10^{20}$, say. The computation time was a few seconds per example on an HP 9000/433 workstation. Methods for the complete resolution of (1.1) have so far been developed only for quartic fields with Galois group C_4 [Gaál et al. 1991b] and V_4 [Gaál et al. 1995]. These methods produce all solutions of (1.1), but the computation time can be several minutes (and more) per example.

This paper describes an algorithm for the fast computation of all solutions of (1.1) in quartic fields of Galois group D_8. The algorithm is based on suitable sieving methods. It reduces the problem of solving (1.1) to the solution of equations of type

$$G_n = x^2 + D \quad \text{for } n, x \in \mathbb{Z}, \tag{1.2}$$

where G_n is a second-order linear recurrence sequence and D is a given integer. The method is successful only for a subset of the fields of interest, which we characterize later (Corollary 6.3); it turns out that this subset includes about 70% of the totally real quartic fields of Galois group D_8 having discriminant less than 10^6. Table 1 in Section 8 gives some statistics. When successful, the method produces all solutions fast, say in a few seconds. It allows the determination of the minimal index of K and all integers of K with minimal index.

The last section of this paper presents an infinite family of totally real quartic fields of Galois group D_8 with minimal index 1.

2. FROM INDEX FORM EQUATIONS TO LINEAR RECURRENCE SEQUENCES

In this section we show how the resolution of the index form equation (1.1) can be reduced to that of an equation of type (1.2). We keep all the notation of the previous section. We excerpt the following two statements from [Gaál et al. 1991a].

Proposition 2.1. *Let J be a nonzero integer. Then $\boldsymbol{x} = (x_2, x_3, x_4) \in \mathbb{Z}^3$ is a solution of* (1.1) *if and only if there exist $j_1, j_2 \in \mathbb{Z}$ satisfying $j_1 j_2 = J$,*

$$x_3^2 + (\omega + \omega')x_3x_4 + \omega\omega' x_4^2 = j_1, \tag{2.1}$$

and

$$l_{12}(\boldsymbol{x})l_{23}(\boldsymbol{x})l_{34}(\boldsymbol{x})l_{41}(\boldsymbol{x}) = j_2(\omega - \omega')^2. \qquad (2.2)$$

Theorem 2.2. *If the system of equations* (2.1) *and* (2.2) *has a solution* $\boldsymbol{x} \in \mathbb{Z}^3$, *there exists a rational integer* v *such that*

$$v^2 = j_1^2\mu\mu'\big(\tfrac{1}{4}(c^2 - d^2m)\big)^2 + 4j_2h^2m. \qquad (2.3)$$

We use these results to prove:

Theorem 2.3. *Let* $\varepsilon > 1$ *be the fundamental unit of* L, *and let* $\mathcal{B}$ *be a maximal set of nonassociate elements of* $\mathbb{Z} + \mathbb{Z}\omega$ *with norm* j_1. *If the system of equations* (2.1) *and* (2.2) *has a solution* $\boldsymbol{x} \in \mathbb{Z}^3$, *there exist* $\beta \in \mathcal{B}$ *and* $y, n, v \in \mathbb{Z}$ *such that* v *satisfies* (2.3) *and*

$$\mu(c+d\sqrt{m})^2\beta^2\varepsilon^{2n}+\mu'(c-d\sqrt{m})^2\beta'^2\varepsilon'^{2n} = my^2+8v. \qquad (2.4)$$

Moreover, possibly after replacing $\boldsymbol{x}$ *with* $-\boldsymbol{x}$, *we have*

$$x_3 = \tfrac{1}{2}(\beta\varepsilon^n + \beta'\varepsilon'^n),$$
$$x_4 = \tfrac{1}{2}(\beta\varepsilon^n - \beta'\varepsilon'^n)/\sqrt{m},$$
$$x_2 = \tfrac{1}{8}(-2(bx_3 + ax_4) + y)$$

if $m \equiv 2$ *or* 3 mod 4, *and*

$$x_3 = (-w'\beta\varepsilon^n + w\beta'\varepsilon'^n)/\sqrt{m},$$
$$x_4 = (\beta\varepsilon^n - \beta'\varepsilon'^n)/\sqrt{m},$$
$$x_2 = \tfrac{1}{4}(-2bx_3 - (a+b)x_4 + y)$$

if $m \equiv 1$ mod 4.

Proof. We assume that $\boldsymbol{x} \in \mathbb{Z}^3$ is a solution of (1.1). Then, by Proposition 2.1 and Theorem 2.2, there exist integers $j_1, j_2, v \in \mathbb{Z}$ satisfying (2.1)–(2.3).

For $m \equiv 2$ or 3 mod 4, equation (2.1) has the form

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

Hence there exist $\beta \in \mathcal{B}$ and $n \in \mathbb{Z}$ 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, and the same holds for x_2 because of (2.2). As in the derivation of [Gaál et al. 1991a, eq. (20)], we obtain

$$\begin{aligned}\big((mA_3 + A_4 + A_{34}\sqrt{m})\beta^2\varepsilon^{2n} \\ + (mA_3 + A_4 - A_{34}\sqrt{m})\beta'^2\varepsilon'^{2n}\big)/(4m) \\ = y_1^2 + A_0 - j_1(mA_3 - A_4)/(2m) \end{aligned} \qquad (2.5)$$

with $y_1 \in \mathbb{Z}$ and

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

From these expressions we get

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

Recalling that $\mu = \frac{1}{2}(e + f\sqrt{m})$, we can write (2.5) as

$$\begin{aligned} 4m(\mu(c+d\sqrt{m})^2\beta^2\varepsilon^{2n} + \mu'(c-d\sqrt{m})^2\beta'^2\varepsilon'^{2n}) \\ = y_1^2 + 32mv. \end{aligned}$$

Since e and f are even and m is square-free, $2m$ divides y_1. Putting $y = y_1/(2m)$ we get (2.4).

For $m \equiv 1$ mod 4 the proof is analogous. □

We note that the left-hand side of (2.4) is a sequence in n that obeys a second-order linear recurrence. Hence, the resolution of (1.1) is reduced to solving an equation of type (2.4). For this we develop sieving procedures for general second-order linear recurrence sequences in Sections 3 to 7.

3. USEFUL PROPERTIES OF RECURRENCE SEQUENCES

Take $P, Q \in \mathbb{Z}$ such that $P^2 + 4Q \neq 0$, and let α, β be the (distinct) zeros of $x^2 - Px - Q$. For $n \in \mathbb{Z}^{\geq 0}$ (or for $n \in \mathbb{Z}$ if $|Q| = 1$), set

$$V_n = \alpha^n + \beta^n, \quad U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

$$W_n = \begin{cases} V_n & \text{if } P \text{ is odd,} \\ \frac{1}{2}V_n & \text{otherwise.} \end{cases}$$

It is easy to see that V_n is odd if and only if P is odd and 3 does not divide n. The following properties are easily proved for $n, l \in \mathbb{Z}$:

$$2U_{n+l} = U_n V_l + U_l V_n \tag{3.1}$$

$$2V_{n+l} = V_n V_l + (\alpha - \beta)^2 U_n U_l \tag{3.2}$$

$$V_{2n} = V_n^2 - 2(-Q)^n \tag{3.3}$$

$$U_{2n} = U_n V_n \tag{3.4}$$

$$V_n \mid V_{nm} \quad \text{for } m \text{ odd.} \tag{3.5}$$

Lemma 3.1. *Let $|Q| = 1$ and $n = 2^k m \in \mathbb{Z}$ with $k \geq 1$. Additionally, if P is odd let $m \not\equiv 0 \bmod 3$ and if $Q = 1$ let m be even. Then*

$$U_{n+l} \equiv -U_l \bmod W_{2^{k-1}m},$$
$$V_{n+l} \equiv -V_l \bmod W_{2^{k-1}m}$$

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

Proof. We only prove the first congruence because the proof of the second is similar. By (3.1), (3.4) and (3.3) we obtain

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

If P is even, so is $V_{n/2}$. Otherwise $V_{n/2}$ is odd because 3 does not divide m. Dividing the last congruence by 2 we get the desired result. □

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

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

we call $x^2 - Px - Q$ the characteristic polynomial of that sequence.

Theorem 3.2. *Let $\{G_n\}$ be a second-order linear recurrence sequence of integers with characteristic polynomial $x^2 - Px - Q$. Let n, k and m be as in Lemma 3.1. Then $G_{n+l} \equiv -G_l \bmod W_{2^{k-1}m}$ 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

$$G_n = G_1 U_n + QG_0 U_{n-1}. \tag{3.6}$$

Using the first congruence in Lemma 3.1 we immediately get the desired result. □

4. THE FIRST SIEVING PROCEDURE

In the sequel, $\left(\frac{x}{m}\right)$ denotes the Jacobi symbol for $x, m \in \mathbb{Z}^{>0}$. We maintain the notation for recurrence sequences introduced in the previous section.

For an integer m we fix a complete residue system modulo m, and we denote by $r(m)$ the length of the minimal period of the sequence $\{U_n \bmod m\}$. It follows from (3.6) that the minimal period of $\{G_n \bmod m\}$ divides $r(m)$ for any recurrence sequence $\{G_n\}$ with the same characteristic polynomial as $\{U_n\}$. In this case Q is an arbitrary integer.

The following lemma can be used very efficiently for proving that (1.2) is not solvable or for localizing the solutions of (1.2) in a few residue classes with respect to an appropriate module.

Lemma 4.1. *Let D be an integer, $S = \{p_1, \ldots, p_t\}$ a set of prime numbers, R the least common multiple of $r(p_1), \ldots, r(p_t)$, and $\mathcal{M} = \{m_1, \ldots, m_s\}$ with $0 \leq m_1 < m_2 < \cdots < m_s < R$. If there exists for all $m \in \mathcal{M}$ an index $i \in [1, t]$ such that*

$$\left(\frac{G_m - D}{p_i}\right) = -1, \tag{4.1}$$

then all solutions $n, x \in \mathbb{Z}$ of (1.2) satisfy $n \not\equiv m \bmod R$ for all $m \in \mathcal{M}$.

Proof. Assume that $n, x \in \mathbb{Z}$ is a solution of (1.2) with $n \cong m_i \bmod R$ for some $m_i \in \mathcal{M}$. Then

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

for all primes $p \in S$ because of (1.2).

On the other hand, by assumption there exists $p_i \in S$ satisfying (4.1). Because $n \equiv m \bmod R$ and $r(p_i)$ divides R, we have $n \equiv m \bmod r(p_i)$. Thus $G_n \equiv G_m \bmod p_i$ which together with (4.1) contradicts the previous paragraph. □

The idea of using modular methods for the resolution of (1.2) goes back to [Wunderlich 1963]. Its combination with an effective upper bound for the solutions was applied in [Pethő 1993; 1991] for determining all cubes and fifth powers, respectively, in the Fibonacci sequence. An "intelligent" implementation of those ideas is described in [Nemes 1991].

5. THE SECOND SIEVING PROCEDURE

The disadvantage of the first sieving procedure is that a solution $n, x \in \mathbb{Z}$ of (1.2) cannot be located in its residue class modulo R. Therefore we develop another method that allows us to prove that, for another appropriate module R_1, expected to be not much larger than R, and for all but one element of the residue classes modulo R_1 containing n, equation (1.2) is not solvable.

Such an idea was invented by Cohn [1964] and applied also by Ribenboim [1989]. 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 5.1. *Let m and D be integers, and $S = \{p_1, \dots, p_t\}$ a set of prime numbers greater than 3. Assume that there exist $a, b_1, \dots, b_t \in \mathbb{Z}^{>0}$ such that for every $\alpha \geq a$ there exist nonnegative integers $\beta_1 \leq b_1, \dots, \beta_t \leq b_t$ satisfying*

$$\left(\frac{-G_m - D}{W_{2^\alpha p_1^{\beta_1} \dots p_t^{\beta_t}}}\right) = -1. \tag{5.1}$$

Then (1.2) *has at most one solution $n, x \in \mathbb{Z}$ with $n \equiv m \bmod 2^{a+1} p_1^{b_1} \dots p_t^{b_t}$, namely $n = m$.*

Proof. Let $n, x \in \mathbb{Z}$ be a solution of (1.2) satisfying $n \equiv m \bmod 2^{a+1} p_1^{b_1} \dots p_t^{b_t}$ and $n \neq m$. Then there exists $h \in \mathbb{Z}$ such that $n = m + 2^{a+1} sh$, where $s = p_1^{b_1} \dots p_t^{b_t}$. 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 (3.5) and therefore $W_{2^{a+c+1}s}$ divides $W_{2^{a+c+1}sh_1}$. Hence, Lemma 3.1 yields

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

We put $\alpha = a + c \geq a$. By assumption there exist nonnegative integers $\beta_1 \leq b_1, \dots, \beta_t \leq b_t$ satisfying satisfying (5.1). Because of (3.5), $V_{2^\alpha p_1^{\beta_1} \dots p_t^{\beta_t}}$ divides $V_{2^\alpha p_1^{b_1} \dots p_t^{b_t}}$, so the last congruence implies

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

This and (5.1) contradict the assumption that n, x give a solution of (1.2). □

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

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

The proof of this property is a simple application of (3.5). Choosing $\alpha \geq 2$ and combining the last congruence with (5.1), we get

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

where the sign on the right depends only on the sign of $G_m + D$ and on the parity of P. To be able to apply Lemma 5.1 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

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

for every $n \in \mathbb{Z}$, where we take the smallest nonnegative residues mod M. It is obvious that the sequence $\{v(t, M, n)\}_{n=0}^{\infty}$ is eventually periodic. Let $e(t, M)$ be its minimal preperiod (or 1 if the preperiod is 0), and $r(t, M)$ its minimal period.

Lemma 6.1. *Assume that t is odd and $M > 1$. Then $r(t, M)$ divides $r = r(1, M)$ and $e(t, M) \leq e = e(1, M)$.*

Proof. We use induction on t. The case $t = 1$ is trivial. We assume that the result is true for any odd u with $1 \leq u < t$. Then the congruence

$$v(u, M, e) \equiv v(u, M, r+e) \bmod M \tag{6.1}$$

immediately follows for all such u. To complete the induction step it is sufficient to prove (6.1) for $u = t$. For $u = 1$ equation (6.1) means

$$\alpha^{2^{e+r}} + \beta^{2^{e+r}} \equiv \alpha^{2^e} + \beta^{2^e} \bmod M$$

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

$$\sum_{j=0}^{(t-1)/2} \binom{t}{j} (\alpha^{j2^{e+r}} \beta^{(t-j)2^{e+r}} + \alpha^{(u-j)2^{e+r}} \beta^{j2^{e+r}})$$
$$\equiv \sum_{j=0}^{(t-1)/2} \binom{t}{j} (\alpha^{j2^e} \beta^{(t-j)2^e} + \alpha^{(u-j)2^e} \beta^{j2^e}) \bmod M.$$

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

$$\alpha^{j2^e} \beta^{(t-j)2^e} = \beta^{(t-2j)2^e}, \quad \alpha^{(t-j)2^e} \beta^{j2^e} = \alpha^{(t-2j)2^e}.$$

Analogous identities hold if we replace e by $e + r$. Thus the above congruence of sums implies

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

Because $t-2j < t$ for $j > 0$ and $t-2j$ is always odd, the induction hypothesis means that all summands on the left with $j > 0$ vanish. The remaining congruence is exactly (6.1) for $u = t$. This proves the induction step. □

We can now characterize those pairs n, D for which the result of Lemma 6.1 can be successfully applied. We remark that if m and D are fixed then $-G_m - D$ is a fixed integer, which we call M.

Theorem 6.2. *Let M be an odd integer with $|M| > 1$, and let $e = e(1, M)$ and $r = r(1, M)$. If there exist integers m_1, m_2 such that $e \leq m_1, m_2 \leq e + r$ and*

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

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

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

Proof. Let $R = R(M)$ be the minimal period of the sequence $\{V_n \bmod M\}_{n=-\infty}^{\infty}$. (This sequence is purely periodic for all M because $|Q| = 1$.) Let $R = 2^s u$ with u odd. Starting with a longer preperiod than the minimal one, if necessary, we can 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 an arithmetic progression there exists a prime p such that $p2^k \equiv 2^{m_1} \bmod R$. This implies $V_{2^k p} \equiv V_{2^{m_1}} \bmod M$, and since M is odd we get $W_{2^k p} \equiv W_{2^{m_1}} \bmod M$, hence the theorem. □

Combining Theorem 2.3 and Lemma 6.1 we immediately get the following corollary:

Corollary 6.3. *Let $\{G_n\}$ be a recurrence sequence with $|Q| = 1$, let $D \in \mathbb{Z}$, and set $M = G_m + D$. Let $\{V_n\}$ be the recurrence sequence defined by the zeros of the characteristic polynomial of $\{G_n\}$. 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*

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

there exist an integer $a \leq e(1, M) + r(1, M) + 1$ and primes $p_1, \ldots, p_t > 3$ such that (1.2) has at most one solution $n, x \in \mathbb{Z}$ with $n \equiv m \bmod 2^a p_1 \cdots p_t$, namely $n = m$.

7. THE ALGORITHM

We are ready to summarize our results and spell out a practical algorithm for the resolution of (1.1).

In a first step we reduce that problem to that of calculating all solutions of (1.2), as described in Section 2. In the sequel we fix D and the sequence $\{G_n\}$. To solve (1.2) we then apply two sieving procedures, called Sieve 1 and Sieve 2 in the sequel.

Sieve 1. This amounts to an application of Lemma 4.1. Choose enough prime numbers $p_1, \dots, p_t$ so that the least common multiple R of $r(p_1), \dots, r(p_t)$ is not much larger than $\max_{1 \le i \le t} r(p_i)$. Using the lemma, determine a subset $\mathcal{M}_0$ of $\{0, 1, \dots, R-1\}$ that is as large as possible. Note that $\mathcal{M}_0$ necessarily contains all solutions of (1.2).

Sieve 2. Let $m \in \{0, 1, \dots, R-1\} \setminus \mathcal{M}_0$ be an index of the output of Sieve 1. Let M be the square-free part of $G_m + D$. Compute the sequences

$$\Big\{ \Big(\frac{v(p, M, n)}{M} \Big) \Big\}_{n=1}^{r(1,M)+e(1,M)}$$

until finding a prime number p such that

$$\Big(\frac{v(p, M, n)}{M} \Big) = \varepsilon$$

for all $n \in \{1, 2, \dots, e(1, M) + r(1, M)\}$, where ε is 1 or -1 depending only on M (see the end of Section 5).

For given P, Q and small M we will of course precompute the appropriate sieving modules, that is, a product of convenient primes.

Algorithm. Step 1. Choose a module R as described above and calculate all solutions of (1.2) in n modulo R. For this use Sieve 1 so that the absolute smallest representatives of the remaining residue classes correspond to the actual solutions. Denote these representatives by n_i, for $1 \le i \le t$. If $t = 0$ there are no solutions to (1.2) and the algorithm terminates.

Step 2. Let $1 \le i \le t$. Using Sieve 2, try to determine a number $M_i = 2^{k_i} p_{i1} \dots p_{is_i}$ with the property that a solution n of (1.2) with $n \equiv n_i \bmod M_i$ satisfies $n = n_i$. According to Corollary 6.3 this is not always possible.

Step 3. For each $i = 1, \dots, t$, try to prove—possibly by enlarging the initial set of prime numbers—that for a solution n of (1.2) subject to $n \equiv n_i \bmod R$ there exists an index $j \in [1, t]$ with $n \equiv n_j \bmod M_i$. For this use Sieve 1 again. This procedure is not deterministic.

The next section illustrates the algorithm with a detailed example. We also present the results of a computation where we applied the algorithm to all totally real quartic fields with Galois group D_8 and discriminant $< 10^6$.

8. APPLICATION OF THE SIEVE METHOD

To exemplify the algorithm, we use the following input data, in the notation of Sections 1–5: $D_K = 725$, $m = 5$, $a = 2$, $b = 0$, $c = 2$, $d = 0$, $g = h = J = 1$, $e = 14$, $f = 4$. Equation (2.3) 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 (2.4), namely

$$\begin{aligned} G_n &:= 5(7 - 2\sqrt{5})\Big(\frac{3+\sqrt{5}}{2}\Big)^n + 5(7 + 2\sqrt{5})\Big(\frac{3-\sqrt{5}}{2}\Big)^n \\ &= y_0^2 + 10v \end{aligned} \tag{8.1}$$

for $v = \pm 3, \pm 7$, where we multiplied (2.4) by $\frac{5}{4}$ and set $y_0 = \frac{5}{2} y$. We want integer solutions n, y_0.

The binary recursive sequence $\{G_n\}$ is defined by the initial values $G_0 = 70$, $G_1 = 55$ and by the difference equation $G_{n+2} = 3G_{n+1} - G_n$ for $n \ge 0$ or $n < 0$, that is, $P = 3$ and $Q = -1$. Considering (8.1) modulo the primes in the set $S = \{3, 7, 11, 13, 29, 31, 41, 61, 71, 83, 167, 211, 241, 281, 421, 911, 1427\}$, we see by Lemma 4.1 that the solutions of (8.1) modulo 840 are the following, where j denotes the least positive remainder of n modulo 840:

v	j	y_0	$y = \frac{2}{5} y_0$
3	1	5	2
-3	4	25	10
-3	0	10	4
7	2	5	2
7	0	0	0
-7	-1	15	6

Now we apply Sieve 2 six times. We have

$$W_k = V_k = \Big(\frac{3+\sqrt{5}}{2}\Big)^k + \Big(\frac{3-\sqrt{5}}{2}\Big)^k.$$

By the remark at the end of Section 5 we also have $V_k \equiv -1 \bmod 4$ if k is not divisible by 3. For $j=1$, $v=3$, $D=30$ we obtain $-G_j - D = -85 = -5\cdot 17$. Let k be an integer not divisible by 3. Then

$$\Big(\frac{-G_j - D}{V_k}\Big) = \Big(\frac{-5\cdot 17}{V_k}\Big) = -\Big(\frac{V_k}{5}\Big)\Big(\frac{V_k}{17}\Big) = \Big(\frac{V_k}{17}\Big),$$

because

$$\Big(\frac{V_k}{5}\Big) = -1$$

for all k. We also have:

$$\begin{array}{cccccccc} k & = & 0 & 1 & 2 & 3 & 4 \\ \Big(\frac{V_{2^k}}{17}\Big) & = & -1 & -1 & 1 & -1 & -1 \\ \Big(\frac{V_{5\cdot 2^k}}{17}\Big) & = & 1 & -1 & -1 & 1 & -1 \end{array}$$

The period length of both sequences is three and by Lemma 5.1 we obtain $n=1$ for $n \equiv 1 \bmod 20$, hence there exists only one solution that is divisible by 840. In four more of the six cases similar computations lead to the same result, with new period lengths equal to 1540, 56, 16 and 20 for $(v,j) = (-3,4)$, $(7,2)$, $(7,0)$ and $(-7,-1)$, respectively.

Unfortunately our method does not work in the case $j=0$, $v=-3$, $D=-30$. There we have $-G_j - D = -40 = -2^3\cdot 5$, but Lemma 5.1 is not applicable since

$$\Big(\frac{-2^3\cdot 5}{V_k}\Big) = \Big(\frac{2}{V_k}\Big) = 1$$

for all $k \ge 0$ not divisible by 3.

This method was implemented in Maple [Char et al. 1991] by J. Sajtos of the Mathematical Institute, Kossuth Lajos University, Debrecen. We tested the method for all totally real number fields of Galois group D_8 with discriminants up to 10^6 containing a quadratic subfield of class number one. In each case we computed the minimal index and, if the method worked, all elements with minimal index. Table 1 gives some statistics about these computations.

Hence, the algorithm succeeds for about 85% of the equations (1.2). The rate of success seems to grow rapidly with the size of the discriminant of K.

9. AN INFINITE FAMILY OF FIELDS WITH A POWER INTEGRAL BASIS

We now describe an infinite family of totally real quartic fields with Galois group D_8 and minimal index one.

Range of D_K (in units of 10^5)	$(0,1]$	$(1,2]$	$(2,3]$	$(3,4]$	$(4,5]$	$(5,6]$	$(6,7]$	$(7,8]$	$(8,9]$	$(9,10]$	Total
# of fields (or of index form equations)	379	428	449	442	451	449	431	450	447	453	4379
# of recurrence equations (1.2)	1036	1223	1400	1404	1340	1490	1268	1436	1366	1304	13267
# without solutions after Step 1	406	590	691	709	705	806	650	767	701	670	6595
# of equivalence classes left after Step 1	839	792	856	825	742	799	722	778	770	727	7850
# of solutions isolated by Step 2	574	568	640	610	569	617	545	615	611	570	5919
# of algorithm failures	265	224	216	215	173	182	177	163	159	157	1931

TABLE 1. Frequency data resulting from the application of the algorithm of Section 7 to all totally real number fields K of Galois group D_8 with $D_K \le 10^6$. For each range of values of D_K (first row) we give: the number of equations (1.1) for fields in that range (second row); the number of resulting recurrence equations of the form (1.2), possibly several to a field, according to Theorem 2.3 (third row); the number of such equations that have no solution, as given by Step 1 of the algorithm (fourth row); the number of equivalence classes remaining after Step 1, possibly several to each recurrence equation (fifth row); number of successes, that is, solutions of recurrence equations isolated by Step 2 (sixth row); and number of failures, that is, equivalence classes for which Step 2 does not isolate the solution (last row). Note that the rate of success seems to grow with the size of the discriminant of K.

Theorem 9.1. *There are infinitely many positive integers k such that $K = \mathbb{Q}(\sqrt{2k+\sqrt{2}})$ is a noncyclic quartic field with minimal index one.*

Proof. Let $k \geq 1$ be an integer, and consider $\mu = 2k+\sqrt{2}$ with norm $N(\mu) = 2(2k^2-1)$. Obviously, this norm is not divisible by 2^2. It follows from [Nagell 1922] that there are infinitely many positive integers k such that $2k^2-1$ is not divisible by the square of a prime number. For all such k the field $\mathbb{Q}(\sqrt{\mu})$ is of degree four over $\mathbb{Q}$ and has minimal index one. Indeed, an integral basis of K is

$$\{1, \sqrt{2}, \sqrt{\mu}, \sqrt{2}\sqrt{\mu}\}$$

[Pohst 1975]. Because $\sqrt{2} = (\sqrt{\mu})^2 - 2k$, the elements 1, $\sqrt{\mu}$, μ, $\mu\sqrt{\mu}$ form a power integral basis of K. □

We note that the discriminant of K is $2^{10}(4k^2-2)$, and by Proposition 2.1 the index form equation $I(x_2, x_3, x_4) = \pm 1$ for the integral basis $\{1, \sqrt{2}, \sqrt{\mu}, \sqrt{2}\sqrt{\mu}\}$ is tantamount to the system of equations

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

with the obvious solution $(x_2, x_3, x_4) = (0, 1, 0)$.

ACKNOWLEDGEMENT

We thank the referees for their detailed comments, which were of great help in improving the clarity of the paper.

REFERENCES

[Buchmann and Ford 1989] J. Buchmann and D. Ford, "On the computation of totally real quartic fields of small discriminant", *Math. Comp.* **52** (1989), 161–174.

[Char et al. 1991] B. W. Char et al., *Maple V Language Reference Manual* and *Maple V Library Reference Manual*, Springer, New York, 1991.

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

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

[Gaál et al. 1991b] 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.

[Gaál et al. 1995] I. Gaál, A. Pethő and M. Pohst, "On the resolution of index form equations in biquadratic number fields, III: The bicyclic biquadratic case", to appear in *J. Number Theory.*

[Gaál et al.] I. Gaál, A. Pethő and M. Pohst, "Simultaneous representation of integers by a pair of ternary quadratic forms, with an application to index form equations in quartic number fields", submitted to *J. Number Theory.*

[Nagell 1922] T. Nagell, "Zur Arithmetik der Polynome", *Abh. Math. Sem. Univ. Hamburg* **1** (1922), 179–194.

[Nemes 1991] I. Nemes, "On the solution of the diophantine equation $G_n = P(x)$ with sieve algorithm", pp. 303–312 in *Computational Number Theory* (edited by A. Pethő et al.), de Gruyter, Berlin, 1991.

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

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

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

[Pohst 1993] M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser, Boston and Basel, 1993.

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

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

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

Attila Pethő, University Medical School of Debrecen, Laboratory for Informatics, Nagyerdei krt. 98, H-4028 Debrecen, Hungary (pethoe@peugeot.dote.hu)

Michael Pohst, Fachbereich 3 Mathematik, MA 8-1, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany (pohst@math.tu-berlin.de)

Received February 7, 1994; accepted in revised form November 25