Publ. Math. Debrecen
68/1-2 (2006), 225–242

Index form equations in biquadratic fields: the *p*-adic case

By ISTVÁN GAÁL (Debrecen) and GÁBOR NYUL (Debrecen)

Abstract. We give an efficient algorithm for determining elements of index divisible by fixed primes only in biquadratic number fields. In other words, we solve the p-adic version of the index form equation in such fields.

1. Introduction

Let m, n be distinct square-free integers, $l = \gcd(m, n)$, and define m_1, n_1 by $m = lm_1, n = ln_1$. In this case the quartic field $K = \mathbb{Q}(\sqrt{m}, \sqrt{n}\,)$ has Galois group V_4 (the Klein four group). Several aspects of the very nice special properties and structure of these fields are described in the literature (for a summary see I. Gaál [3]).

We recall that if $\{1, \omega_2, \omega_3, \omega_4\}$ is an integral basis of a biquadratic field K with ring of integers $\mathbb{Z}_K$ and discriminant D_K, then the corresponding index form is given by

$$I(x_2, x_3, x_4)$$
$$= \frac{1}{\sqrt{|D_K|}} \prod_{1\le i<j\le 4} \left(\left(\omega_2^{(i)} - \omega_2^{(j)}\right) x_2 + \left(\omega_3^{(i)} - \omega_3^{(j)}\right) x_3 + \left(\omega_4^{(i)} - \omega_4^{(j)}\right) x_4 \right)$$

Mathematics Subject Classification: 11Y50, 11D57, 11R04.
Key words and phrases: biquadratic fields, index form equations, p-adic case.
Research supported in part by Grants T 037367 and T 042985 from the Hungarian National Foundation for Scientific Research.
Research supported in part by Grant T 037367 from the Hungarian National Foundation for Scientific Research and by the PRCH Student Science Foundation.

and the elements $\alpha \in \mathbb{Z}_K$ of given index $I(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha]) = m$ are of the form $\alpha = x_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4$ where $x_1 \in \mathbb{Z}$ is arbitrary and $x_2, x_3, x_4 \in \mathbb{Z}$ are solutions of the index form equation $I(x_2, x_3, x_4) = \pm m$ (cf. [3]).

T. Nakahara [10] showed that infinitely many of these fields are monogene but the minimal index of such fields can be arbitrary large. I. Gaál, A. Pethő and M. Pohst [5] characterized the field index of biquadratic fields. M. N. Gras and F. Tanoe [7] gave necessary and sufficient conditions for the monogenity of these fields. In the totally real case I. Gaál, A. Pethő and M. Pohst [6] gave an efficient algorithm for determining all generators of power integral bases of biquadratic fields. G. Nyul [11] described all monogene totally complex biquadratic fields and gave explicitely all generators of power integral bases in them.

The purpose of the present paper is to solve the p-adic analogue of the index form equation in biquadratic fields. Let $p_1, \dots, p_s$ be given distinct primes. Consider the solutions $x_2, x_3, x_4 \in \mathbb{Z}$, $\gcd(x_2, x_3, x_4) = 1$, $0 \le t_1, \dots, t_s \in \mathbb{Z}$ of the equation

$$I(x_2, x_3, x_4) = \pm p_1^{t_1} \cdots p_s^{t_s}. \qquad (1)$$

By a general result of K. Győry [8] this equation has only finitely many solutions and effective upper bounds (far too large for practical applications) can be given for the solutions.

The solutions give all elements of index divisible by $p_1, \dots, p_s$ only. Note that except from an example solved by N. P. Smart [12] (in a very simple totally complex cyclic quartic field, using two primes) no p-adic index form equations have been solved so far.

2. Preliminaries

The integral basis and discriminant of K was described by K. S. Williams [15] according to the following five cases. We add also the corresponding index forms:

Case 1. $m \equiv 1 \pmod 4$, $n \equiv 1 \pmod 4$, $m_1 \equiv 1 \pmod 4$, $n_1 \equiv 1 \pmod 4$
integral basis: $\{1, (1+\sqrt{m})/2, (1+\sqrt{n})/2, (1+\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1})/4\}$,
discriminant: $D_K = (l m_1 n_1)^2$

$$I(x_2,x_3,x_4)=\left(l\left(x_2+\frac{x_4}{2}\right)^2-\frac{n_1}{4}x_4^2\right)\left(l\left(x_3+\frac{x_4}{2}\right)^2-\frac{m_1}{4}x_4^2\right)$$
$$\times\left(n_1\left(x_3+\frac{x_4}{2}\right)^2-m_1\left(x_2+\frac{x_4}{2}\right)^2\right).$$

Case 2. $m\equiv 1 \pmod 4$, $n\equiv 1 \pmod 4$, $m_1\equiv 3 \pmod 4$, $n_1\equiv 3 \pmod 4$
integral basis: $\{1,(1+\sqrt{m})/2,(1+\sqrt{n})/2,(1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1})/4\}$,
discriminant: $D_K=(lm_1n_1)^2$

$$I(x_2,x_3,x_4)=\left(l\left(x_2-\frac{x_4}{2}\right)^2-\frac{n_1}{4}x_4^2\right)\left(l\left(x_3+\frac{x_4}{2}\right)^2-\frac{m_1}{4}x_4^2\right)$$
$$\times\left(n_1\left(x_3+\frac{x_4}{2}\right)^2-m_1\left(x_2-\frac{x_4}{2}\right)^2\right).$$

Case 3. $m\equiv 1 \pmod 4$, $n\equiv 2 \pmod 4$
integral basis: $\{1,(1+\sqrt{m})/2,\sqrt{n},(\sqrt{n}+\sqrt{m_1n_1})/2\}$, discriminant:
$D_K=(4lm_1n_1)^2$

$$I(x_2,x_3,x_4)=\left(lx_2^2-n_1x_4^2\right)\left(l\left(x_3+\frac{x_4}{2}\right)^2-\frac{m_1}{4}x_4^2\right)$$
$$\times\left(4n_1\left(x_3+\frac{x_4}{2}\right)^2-m_1x_2^2\right).$$

Case 4. $m\equiv 2 \pmod 4$, $n\equiv 3 \pmod 4$
integral basis: $\{1,\sqrt{m},\sqrt{n},(\sqrt{m}+\sqrt{m_1n_1})/2\}$, discriminant:
$D_K=(8lm_1n_1)^2$

$$I(x_2,x_3,x_4)=\left(\frac{l}{2}(2x_2+x_4)^2-\frac{n_1}{2}x_4^2\right)$$
$$\times\left(2lx_3^2-\frac{m_1}{2}x_4^2\right)\left(2n_1x_3^2-\frac{m_1}{2}\left(2x_2+x_4\right)^2\right).$$

Case 5. $m\equiv 3 \pmod 4), n\equiv 3 \pmod 4$
integral basis: $\{1,\sqrt{m},(\sqrt{m}+\sqrt{n})/2,(1+\sqrt{m_1n_1})/2\}$, discriminant:
$D_K=(4lm_1n_1)^2$

$$I(x_2,x_3,x_4)=\left(l(2x_2+x_3)^2-n_1x_4^2\right)\left(lx_3^2-m_1x_4^2\right)\left(\frac{n_1}{4}x_3^2-m_1\left(x_2+\frac{x_3}{2}\right)^2\right).$$

Note that for integer x_2,x_3,x_4 all factors attain integer values.

In order to be able to deal with all cases in a unique way introduce integer parameters u_1, u_2, u_3, a, b, c, d, f, g, t and new variables x, y, z according to the following table:

Case	u_1	u_2	u_3	a	b	c	d	f	g	t	x	y	z
1.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2+x_4$	$2x_3+x_4$
2.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2-x_4$	$2x_3+x_4$
3.	m_1	$4n_1$	l	n_1	1	m_1	4	n_1	1	1	x_4	x_2	$2x_3+x_4$
4.	m_1	n_1	l	n_1	2	$m_1/2$	1	$2n_1$	1	2	x_4	$2x_2+x_4$	x_3
5.	m_1	n_1	$4l$	n_1	1	m_1	1	n_1	4	1	x_4	$2x_2+x_3$	x_3

Note that m_1 is even in Case 4.

Denote by $F_i = F_i(x_2, x_3, x_4)$ the absolute value of the i-th factor of the index form. It is easily seen by direct calculations (see [6]) that

Lemma 1. *The following relation holds:*

$$\pm u_1 F_1 \pm u_2 F_2 = \pm u_3 F_3. \tag{2}$$

For the quadratic factors F_1, F_2, F_3 of the index form we have

$$\begin{aligned}(ax)^2 - ny^2 &= \pm abF_1\\ (cx)^2 - mz^2 &= \pm cdF_2\\ (fz)^2 - m_1n_1y^2 &= \pm fgF_3.\end{aligned} \tag{3}$$

These equations split into linear factors in the quadratic fields $M_1 = \mathbb{Q}(\sqrt{n})$, $M_2 = \mathbb{Q}(\sqrt{m})$, $M_3 = \mathbb{Q}(\sqrt{m_1n_1})$, respectively, which are the three quadratic subfields of K. The linear factors of the left hand sides of (3) are connected according to the identity

$$tc(ax - \sqrt{n}y) - ta(cx - \sqrt{m}z) = \sqrt{m}(fz - \sqrt{m_1n_1}y). \tag{4}$$

3. Representation

In the following we assume that $x_2, x_3, x_4 \in \mathbb{Z}$, $\gcd(x_2, x_3, x_4) = 1$, $0 \le t_1, \dots, t_s \in \mathbb{Z}$ is an arbitrary but fixed solution of equation (1), hence $F_i(x_2, x_3, x_4) \in \mathbb{Z}$ for $i = 1, 2, 3$. Now $I(x_2, x_3, x_4) = \pm F_1F_2F_3$ implies that F_1, F_2, F_3 is a solution of the S-unit equation over $\mathbb{Z}$

$$\begin{aligned}&\pm u_1F_1 \pm u_2F_2 = \pm u_3F_3\\ &F_i = p_1^{\alpha_{i1}} \cdots p_s^{\alpha_{is}} \quad (i = 1, 2, 3).\end{aligned} \tag{5}$$

We are going to find the primitive solutions $f_1, f_2, f_3 \in \mathbb{N}$ of (5), that is those with $\gcd(f_1, f_2, f_3) = 1$. Then all solutions of (5) are of the form

$$F_i = f_i \cdot p_1^{a_1} \cdots p_s^{a_s} \quad (i = 1, 2, 3) \tag{6}$$

with arbitrary $0 \leq a_1, \dots, a_s \in \mathbb{Z}$. Set

$$f_i = p_1^{a_{i1}} \cdots p_s^{a_{is}} \quad (1 \leq i \leq 3). \tag{7}$$

Further, for $j = 1, \dots, s$ let

$$a'_{ij} = a_{ij} + \mathrm{ord}_{p_j}(u_i) \quad (i = 1, 2, 3). \tag{8}$$

Then $\pm u_1 f_1 \pm u_2 f_2 = \pm u_3 f_3$ can be written in the form

$$\pm u'_1 p_1^{a'_{11}} \cdots p_s^{a'_{1s}} \pm u'_2 p_1^{a'_{21}} \cdots p_s^{a'_{2s}} = \pm u'_3 p_1^{a'_{31}} \cdots p_s^{a'_{3s}} \tag{9}$$

where u'_1, u'_2, u'_3 are relatively prime to $p_1, \dots, p_s$. In this equation we again simplify with the possible common $p_1, \dots, p_s$ factors coming from u_1, u_2, u_3 and assume that at most one of a'_{1j}, a'_{2j}, a'_{3j} is positive ($1 \leq j \leq s$). Having determined a'_{ij} we have to multiply with the same factors again to get the original a'_{ij}, then by (8) we obtain a_{ij} and (7) gives (f_1, f_2, f_3).

4. Sketch of the algorithm

In this section we briefly sketch the main steps of our procedure to make it easier to follow the arguments below.

Step I. Solving the S-unit equation (9) over $\mathbb{Z}$. This is done in Section 5. The procedure involves application of p-adic linear form estimates giving an upper bound of magnitude $10^{18} - 10^{28}$ for the exponents in our examples. We use a reduction procedure to reduce these bounds to about 5–23 in the examples. Then we can calculate the values of a'_{ij} explicitely using direct testing.

Step II. The common factor of F_1, F_2, F_3 is $p_1^{a_1} \cdots p_s^{a_s}$, cf. (6). In Section 6 we show that in fact in most of the cases the exponents $a_1, \dots, a_s$ attain only very small values. The exceptional case occurs only when there is a prime p_i which splits into the product of two distinct prime ideals in all the three quadratic subfields of K.

Step III. If p_i splits into the product of two distinct prime ideals in all the three quadratic subfields of K, then in order to determine the corresponding a_i we have to solve an S-unit equation over K (see Example 2). This is done in Section 7. This procedure involves p-adic and complex linear form estimates (giving an upper bound 10^{32} for the unknown exponents) as well as repeated application of reduction procedures both in the p-adic and complex cases (which are used to reduce the bound to 28 in Example 2).

Step IV. From the explicit values of F_1, F_2, F_3 we determine the values of x, y, z in (3) and from those the values of x_2, x_3, x_4 either by using the procedure of [6] (totally real case) or [11] (totally complex case).

5. Solving the S-unit equation over Z

5.1. P-adic linear form estimates.

Consider equation (9). For any j the exponent a'_{1j} is either zero or

$$\begin{aligned} 0 < a'_{1j} &= \mathrm{ord}_{p_j}\left(\pm u'_2 p_1^{a'_{21}} \cdots p_s^{a'_{2s}} \pm u'_3 p_1^{a'_{31}} \cdots p_s^{a'_{3s}}\right) \\ &= \mathrm{ord}_{p_j}\left(1 \pm \frac{u'_2}{u'_3} p_1^{a'_{21}-a'_{31}} \cdots p_s^{a'_{2s}-a'_{3s}}\right) \end{aligned} \tag{10}$$

since the right hand side contains no p_j factor.

Using the estimates of K. Yu [16] (see also [13]) we obtain

$$\begin{aligned} a'_{1j} &= \mathrm{ord}_{p_j}\left(\log_{p_j}\frac{u'_2}{u'_3} + (a'_{21}-a'_{31})\log_{p_j} p_1 + \cdots + (a'_{2s}-a'_{3s})\log_{p_j} p_s\right) \\ &< C_1 \log H \end{aligned} \tag{11}$$

where $H = \max a'_{ij}$. Observe that again the j-th term is missing and only one of a'_{2k}, a'_{3k} can be positive. A similar upper bound can be derived for a'_{2j}, a'_{3j} by interchanging their roles for $j = 1, \ldots, s$, whence $H < C_1 \log H$, which implies an upper bound for H.

To simplify the calculations, if $u'_1 u'_2 u'_3$ have only a few prime factors, then we can extend the set of primes with these primes (see Example 2). Then by symmetry we have less cases to consider.

5.2. ***P*-adic reduction.**

The reduction procedure is based on B. M. M. DE WEGER's ideas [14]. A variant of it was formulated by I. GAÁL, I. JÁRÁSI and F. LUCA [4] which we can use here, as well. Lemma 4.1 of [4] can be used to (11) to reduce the bound for H in several steps (see the Examples).

6. GCD calculations

Using a primitive solution f_1, f_2, f_3 of (5) by (6) we can write (3) in the form

$$\begin{aligned}(ax)^2 - ny^2 &= \pm s_1\, P\\ (cx)^2 - mz^2 &= \pm s_2\, P\\ (fz)^2 - m_1 n_1 y^2 &= \pm s_3\, P\end{aligned} \tag{12}$$

with $s_1 = abf_1$, $s_2 = cdf_2$, $s_3 = fgf_3$ and $P = p_1^{a_1} \cdots p_s^{a_s}$. By our assumption $\gcd(x_2, x_3, x_4) = 1$ and by the definition of x, y, z we get $\gcd(x, y, z) = 1$ or 2. In the following we assume $2 \in \{p_1, \dots, p_s\}$ (we may extend the set of primes otherwise).

The two lemmas below play an important role in our calculations. Their proofs can be given by elementary means, just using divisibility arguments. For this reason we only detail the proof of one characteristic case.

Lemma 2. (i) *If $p \notin \{p_1, \dots, p_s\}$ is a prime then $p \nmid \gcd(x, y)$, $p \nmid \gcd(x, z)$, $p \nmid \gcd(y, z)$.*

(ii) *if* $p_i \in \{p_1, \dots, p_s\} \setminus \{2\}$ *then*	(iii) *if* $p_i = 2$ *then*
$\mathrm{ord}_{p_i}(\gcd(x,y)) \le \mathrm{ord}_{p_i}(s_1)/2$	$\mathrm{ord}_{p_i}(\gcd(x,y)) \le (\mathrm{ord}_2(s_1)+3)/2$
$\mathrm{ord}_{p_i}(\gcd(x,z)) \le (\mathrm{ord}_{p_i}(s_2)+1)/2$	$\mathrm{ord}_{p_i}(\gcd(x,z)) \le (\mathrm{ord}_2(s_2)+3)/2$
$\mathrm{ord}_{p_i}(\gcd(y,z)) \le \mathrm{ord}_{p_i}(s_3)/2$	$\mathrm{ord}_{p_i}(\gcd(y,z)) \le (\mathrm{ord}_2(s_3)+2)/2$

PROOF OF LEMMA 2. As an example we prove the first statement of (ii). Let α be a positive exponent with $p_i^\alpha \mid x, y$. By $\gcd(x, y, z) \le 2$ and $p_i \ne 2$ we obtain $p_i \nmid z$. Then $p_i^{2\alpha} \mid s_1 P$ follows from the first equation of (12).

Indirectly suppose $2\alpha > \mathrm{ord}_{p_i}(s_1)$. Then $p_i \mid P$, hence by the second and third equations of (12) $p_i \mid mz^2$ and $p_i \mid f^2z^2$. By $p_i \nmid z$ it is easy to see that $p_i \mid m$ and $p_i \mid f$. Further, $p_i \mid f$, $p_i \neq 2$ implies $p_i \mid n_1$, hence from $\gcd(m_1, n_1) = 1$ we get $p_i \nmid m_1$. But $p_i \mid m$ implies $p_i \mid l$ whence $p_i^2 \mid n_1 l = n$. This contradicts to n being square-free. □

Let $x, y, z \in \mathbb{Z}$ be an arbitrary but fixed solution of (12). Then for $i = 1, 2, 3$ we set

i	α_i	β_i	φ_{i1}	φ_{i2}	D_{1i}	D_{2i}
1	a	$\sqrt{n}$	$ax - \sqrt{n}y$	$ax + \sqrt{n}y$	0	3
2	c	$\sqrt{m}$	$cx - \sqrt{m}z$	$cx + \sqrt{m}z$	1	3
3	f	$\sqrt{m_1 n_1}$	$fz - \sqrt{m_1 n_1}y$	$fz + \sqrt{m_1 n_1}y$	0	2

We recall that we have $M_1 = \mathbb{Q}(\sqrt{n})$, $M_2 = \mathbb{Q}(\sqrt{m})$, $M_3 = \mathbb{Q}(\sqrt{m_1 n_1})$. There are three possible ways for a rational prime p to split in a quadratic field. According to these possibilities we have the following statement.

Lemma 3.

(i) *Let* $p_j \in \{p_1, \ldots, p_s\} \setminus \{2\}$. *If* (p_j) *is a prime ideal in* M_i $(i = 1, 2, 3)$, *then* $a_j \leq 2\max(\mathrm{ord}_{p_j}(2\alpha_i), \mathrm{ord}_{p_j}(2\beta_i)) + D_{1i}$.

(ii) *Let* $p_j = 2$. *If* (2) *is a prime ideal in* M_i $(i = 1, 2, 3)$, *then* $a_j \leq 2\max(\mathrm{ord}_2(2\alpha_i), \mathrm{ord}_2(2\beta_i)) + D_{2i}$.

(iii) *Let* $p_j \in \{p_1, \ldots, p_s\} \setminus \{2\}$. *If* $(p_j) = \wp^2$ *for some prime ideal* $\wp$ *in* M_i, *then* $a_j \leq \max(\mathrm{ord}_\wp(2\alpha_i), \mathrm{ord}_\wp(2\beta_i)) + D_{1i}$.

(iv) *Let* $p_j = 2$. *If* $(2) = \wp^2$ *for some prime ideal* $\wp$ *in* M_i, *then* $a_j \leq \max(\mathrm{ord}_\wp(2\alpha_i), \mathrm{ord}_\wp(2\beta_i)) + D_{2i}$.

(v) *Let* $p_j \in \{p_1, \ldots, p_s\} \setminus \{2\}$. *If* $(p_j) = \wp \cdot \overline{\wp}$ *for some prime ideal* $\wp$ *in* M_i, *then, assuming* $\wp^k \mid (\varphi_{i1})$ *and* $\overline{\wp}^k \mid (\varphi_{i1})$, *we have* $k \leq \max(\mathrm{ord}_{p_j}(2\alpha_i), \mathrm{ord}_{p_j}(2\beta_i)) + (\mathrm{ord}_{p_j}(s_i) + D_{1i})/2$ *where for any* $\sigma \in \mathbb{Z}_{M_i}$ *by* $\mathrm{ord}_{p_j}(\sigma)$ *we mean* $\min(\mathrm{ord}_\wp(\sigma), \mathrm{ord}_{\overline{\wp}}(\sigma))$.

(vi) *Let* $p_j = 2$. *If in* M_i *we have* $(2) = \wp \cdot \overline{\wp}$ *for some prime ideal* $\wp$, *then assuming* $\wp^k \mid (\varphi_{i1})$ *and* $\overline{\wp}^k \mid (\varphi_{i1})$ *we have* $k \leq \max(\mathrm{ord}_2(2\alpha_i), \mathrm{ord}_2(2\beta_i)) + (\mathrm{ord}_2(s_i) + D_{2i})/2$ *where for any* $\sigma \in \mathbb{Z}_{M_i}$ *by* $\mathrm{ord}_2(\sigma)$ *we mean* $\min(\mathrm{ord}_\wp(\sigma), \mathrm{ord}_{\overline{\wp}}(\sigma))$.

Proof of Lemma 3. As an example we prove (i). Assume that (p_j) is a prime ideal in M_1 and set $\overline{a_j} = a_j + \mathrm{ord}_{p_j}(s_1)$. The first equation of (12) implies

$$p_j^{\overline{a_j}} \parallel (ax)^2 - ny^2 = \varphi_{11} \cdot \varphi_{12}.$$

Since φ_{11} and φ_{12} are conjugates over M_1, hence $p_j^{b_j} | \varphi_{11}$ if and only if $p_j^{b_j} | \varphi_{12}$ for a non-negative b_j. If b_j is the greatest possible value with this property, then $\overline{a_j} = 2b_j$, $p_j^{b_j} \mid \varphi_{11} + \varphi_{12} = 2ax$ and $p_j^{b_j} \mid \varphi_{12} - \varphi_{11} = 2\sqrt{n}y$ also hold. These imply $b_j \leq \mathrm{ord}_{p_j}(2a) + \mathrm{ord}_{p_j}(x)$ and $b_j \leq \mathrm{ord}_{p_j}(2\sqrt{n}\,) + \mathrm{ord}_{p_j}(y)$. By Lemma 2 $\min(\mathrm{ord}_{p_j}(x), \mathrm{ord}_{p_j}(y)) \leq \mathrm{ord}_{p_j}(s_1)/2$. Combining these inequalities we obtain $b_j \leq \max(\mathrm{ord}_{p_j}(2a), \mathrm{ord}_{p_j}(2\sqrt{n}\,)) + \mathrm{ord}_{p_j}(s_1)/2$, which proves the proposition since $\overline{a_j} = 2b_j$. □

Using the above lemma if $p_j \in \{p_1, \ldots, p_s\}$ remains prime or is the square of a prime ideal in one of the quadratic subfields of K, then we can derive a small upper bound for a_j. If this can be done for all primes on the right hand side of (1), then there are altogether just a few possibilities for F_1, F_2, F_3. In such cases (3) can be solved in the totally real case by using the method of I. Gaál, A. Pethő and M. Pohst [6] by solving systems of simultaneous Pellian equations (see Example 1), or in the totally complex case by the help of the method of G. Nyul [11] using that one of the quadratic factors of the index form is definite.

On the other hand, if there are primes among $p_1, \ldots, p_s$ which split into the product of two distinct prime ideals in all quadratic subfields of K, then we have to proceed by solving an S-unit equation over the quartic field K.

7. S-unit equation over the quartic field

In this section we apply the identity (4). Using standard arguments (see e.g. K. Győry [8]) we derive from (4) an S-unit equation over the quartic field K. Note that there are effective upper bounds for the solutions of S-unit equations (see e.g. K. Győry [9]) but direct calculations utilizing the properties of our specific S-unit equation give much sharper bounds. This also prepares the application of the reduction procedure.

We detail the totally real case only, which is the most interesting one. In the totally complex case we have to simplify some formulas in a straightforward way.

7.1. Constructing the S-unit equation.
For our purpose we first factorize φ_{i1} in the corresponding quadratic subfield M_i. For $i = 1, 2, 3$, let I_{i1}, I_{i2}, I_{i3} be pairwise disjoint subsets of $\{1, 2, \ldots, s\}$ with $\{1, 2, \ldots, s\} = I_{i1} \cup I_{i2} \cup I_{i3}$ so that in M_i

I. (p_j) is prime for $j \in I_{i1}$

II. $(p_j) = \wp_{ji}^2$ for $j \in I_{i2}$

III. $(p_j) = \wp_{ji1} \cdot \wp_{ji2}$ for $j \in I_{i3}$

with suitable prime ideals $\wp_{ji}$, $\wp_{ji1}$, $\wp_{ji2}$ of M_i. We have

$$\varphi_{i1} \cdot \varphi_{i2} = \pm s_i \cdot p_1^{a_1} \cdots p_s^{a_s} \quad (i = 1, 2, 3).$$

Note that there are small upper bounds for a_j for $j \in \bigcup_{i=1}^{3}(I_{i1} \cup I_{i2})$, hence the corresponding factors can be dealt with as constants. This reduces the number of variables in the S-unit equation considerably. If the bound for a_j is not very small, then it can be dealt with as a variable in a straightforward way as well, if the total number of variables in the S-unit equation does not become too large and this way we can spare to consider a couple of cases. Sometimes these variables cancel from the S-unit equation (see the Example 2).

Denote by h_i the class number of M_i and let ε_i be a fundamental unit of M_i $(i = 1, 2, 3)$. Set $h = \mathrm{lcm}(h_1, h_2, h_3)$. For $j \in I_{i3}$ there are distinct (coprime, conjugated) prime ideals $\wp_{ji1}$ and $\wp_{ji2}$ in M_i such that $(p_j) = \wp_{ji1} \cdot \wp_{ji2}$. There are integral elements π_{ji1} and π_{ji2} in M_i with $\wp_{ji1}^h = (\pi_{ji1})$, $\wp_{ji2}^h = (\pi_{ji2})$.

Let $I = I_{13} \cap I_{23} \cap I_{33}$. To simplify our notation we use the representation

$$\varphi_{i1} = \pm\delta_i \cdot \varepsilon_i^{e_i} \cdot \prod_{j \in I} \pi_{jik_{ji}}^{d_j}$$

where δ_i is an integer in M_i, whose few possible values can be determined easily, $k_{ji} = 1$ or 2 and $d_j = [a_j/h]$. By calculating the values of d_j we can determine a_j for $j \in I$. Using standard arguments by (4) we have

$$\pm\rho_1\varepsilon_1^{e_1}\varepsilon_3^{-e_3}\prod_{j\in I}\left(\frac{\pi_{j1k_{j1}}}{\pi_{j3k_{j3}}}\right)^{d_j} \pm \rho_2\varepsilon_2^{e_2}\varepsilon_3^{-e_3}\prod_{j\in I}\left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}}\right)^{d_j} = 1, \qquad (13)$$

where $\rho_1 = (tc\cdot\delta_1)/(\sqrt{m}\cdot\delta_3)$, $\rho_2 = (ta\cdot\delta_2)/(\sqrt{m}\cdot\delta_3)$.

Let $E = \max(|e_1|,|e_2|,|e_3|)$, $E_1 = \max(|e_1|,|e_3|)$, $E_2 = \max(|e_2|,|e_3|)$, $D = \max_{j\in I} d_j$, $H = \max(E,D)$, $H_1 = \max(E_1,D)$, and $H_2 = \max(E_2,D)$. Using the arguments of [9] we deduce now from (13) inequalities in e_i and d_j to which p-adic and complex linear form estimates can be applied.

7.2. P-adic upper bounds.

We are going to derive an upper bound for D. Fix $j \in I$. Observe that for $i = 1,2,3$, $k = 1,2$ we have $\mathrm{ord}_{p_j}(\pi_{jik}) = 0$ or h, more exactly, it is h for $k = 1$ and 0 for $k = 2$, or conversely. Moreover, these elements π_{ji1} and π_{ji2} can be chosen to be conjugated of each other over M_i. This means, that for any fixed k_{j1} and k_{j3} in (13) there is a conjugation $\gamma \mapsto \gamma^*$ ($\gamma \in K$) of K such that $\mathrm{ord}_{p_j}(\pi^*_{j1k_{j1}}) = h$ and $\mathrm{ord}_{p_j}(\pi^*_{j3k_{j3}}) = 0$. We apply such a suitable conjugation to equation (13) but omit the $(.)^*$ for simplifying the notation. Remark that the ε_i are p_j-adic units as well as the other $\pi_{j'ik}$ for $j' \neq j$. Then the p_j-adic value of the first term of (13) is $h\cdot d_j + \mathrm{ord}_{p_j}(\rho_1)$ which is positive except if d_j is very small which case can be considered separately. We have

$$\begin{aligned}0 &< h\cdot d_j + \mathrm{ord}_{p_j}(\rho_1)\\ &= \mathrm{ord}_{p_j}\left(\pm 1 \pm \rho_2\, \varepsilon_2^{e_2}\varepsilon_3^{-e_3}\prod_{j\in I}\left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}}\right)^{d_j}\right).\end{aligned} \qquad (14)$$

Appling the estimates of K. Yu [16] (see also [13]) we confer $h\cdot d_j + \mathrm{ord}_{p_j}(\rho_1) < C_2'\log H_2$ with a huge constant C_2'. By performing the same arguments for each $j \in I$, this implies

$$D < C_2\ \log H_2. \qquad (15)$$

Similarly, we obtain

$$D < C_3\ \log H_1. \qquad (16)$$

7.3. Upper bounds for the exponents of the units.
Using standard arguments we obtain, that there is a conjugate η_1^* of $\eta_1 = \varepsilon_1^{e_1}\varepsilon_3^{-e_3}$ such that $|\eta_1^*| < \exp(-c_3\ E_1)$. Similarly, there is a conjugate η_2^{**} of $\eta_2 = \varepsilon_2^{e_2}\varepsilon_3^{-e_3}$ such that $|\eta_2^{**}| < \exp(-c_3\ E_2)$. We have

$$\left|\rho_1^*\ \eta_1^* \prod_{j\in I}\left(\frac{\pi^*_{j1k_{j1}}}{\pi^*_{j3k_{j3}}}\right)^{d_j}\right| < c_4\ \exp(-c_3\ E_1)\ c_5^D, \tag{17}$$

and similarly,

$$\left|\rho_2^{**}\ \eta_2^{**} \prod_{j\in I}\left(\frac{\pi^{**}_{j2k_{j2}}}{\pi^{**}_{j3k_{j3}}}\right)^{d_j}\right| < c_4\ \exp(-c_3\ E_2)\ c_5^D, \tag{18}$$

where the constant c_5 is straightforward to calculate. Let $c_6 = c_3/(2\log c_5)$. If we choose c_5 large enough, we have $0 < c_6 < 1$.

Now if $c_6E_1 \le D$ then by (16) we have $H_1 \le \frac{C_3}{c_6}\ \log H$. Similarly, if $c_6E_2 \le D$, by (15) we obtain $H_2 < \frac{C_2}{c_6}\ \log H$.

If $D < c_6E_1$, then $H_1 = E_1$. Using equation (13) by (18) we have

$$\left|\log|\rho_2^*| + e_2\log|\varepsilon_2^*| - e_3\log|\varepsilon_3^*| + \sum_{j\in I} d_j \log\left|\frac{\pi^*_{j2k_{j2}}}{\pi^*_{j3k_{j3}}}\right|\right| < 2c_4\ \exp\left(-\frac{c_3}{2}\ H_1\right). \tag{19}$$

Applying the lower bounds of Baker and Wüstholz [2] (see also [13]) to the linear forms in the logarithms of algebraic numbers in (19) we obtain an inequality of type $H_1 < \frac{2}{c_3}\,(\log(2c_4) + C_3\log H)$.

Similarly, if $D < c_6E_2$ then using (18) and

$$\left|\log|\rho_1^{**}| + e_1\log|\varepsilon_1^{**}| - e_3\log|\varepsilon_3^{**}| + \sum_{j\in I} d_j \log\left|\frac{\pi^{**}_{j1k_{j1}}}{\pi^{**}_{j3k_{j3}}}\right|\right| < 2c_4\ \exp\left(-\frac{c_3}{2}\ H_2\right) \tag{20}$$

we get an upper bound of the same type for H_2.

Hence, combining all possible cases, we conclude $H < C_4\log H$ which implies an upper bound for H. Denote this upper bound by H_0.

7.4. P-adic reduction.
In the present situation we have to perform both reduction concerning $d_1, \dots, d_s$ (p-adic reduction) and the exponents e_1, e_2, e_3 of the units (usually called complex reduction) to diminish the upper bound H_0 obtained for H.

The p-adic reduction step is based on the equation (14) (where we had to take a suitable conjugate of the equation). By (14) we have

$$\begin{aligned} h \cdot d_j &+ \mathrm{ord}_{p_j}(\rho_1) \\ &= \mathrm{ord}_{p_j}\left(\log_{p_j}\rho_2 + e_2\log_{p_j}\varepsilon_2 - e_3\log_{p_j}\varepsilon_3 + \sum_{j\in I} d_j \log_{p_j}\left(\frac{\pi_{j2k_{j2}}}{\pi_{j3k_{j3}}}\right)\right). \end{aligned}$$

Using $D \le H < H_0$ we apply Lemma 4.1 of [4] for each $j \in I$. Then we achieve a reduced bound D_R for D which is much smaller than H_0 (in the first reduction step it is about the logarithm of H_0).

In the further reduction procedure we also have to consider all possible cases we considered at deriving the initial upper bound for H. If $c_6E_1 \le D$ then similarly we obtain that D_R/c_6 is an upper bound for H_1. Similarly, if $c_6E_2 \le D$ then D_R/c_6 is an upper bound for H_2.

7.5. Reduction of the bound for the exponents of units.
Assume $D < c_6E_1$. We apply Lemma 2.2.2 of [3] to the linear form inequality (19). Using the bound $H_2 < H_0$ we can derive an upper bound H_1' for H_1.

Similarly, if $D < c_6E_2$ then using $H_1 < H_0$ the application of the lemma to (20) gives a bound H_2' for H_2.

We put $H_0' = \max(H_1', H_2', D_R/c_6)$ in place of H_0 and repeat the p-adic reduction step and the reduction for the exponents of units as long as the reduced bound is less than the original one.

8. Examples

8.1. Example 1. A totally real biquadratic field.
Consider the totally real field $K = \mathbb{Q}(\sqrt{5}, \sqrt{2})$. We have $m = m_1 = 5$, $n = n_1 = 2$, $l = 1$ and K belongs to Case 3. Denote by $I(x_2, x_3, x_4)$

the index form corresponding to the integral basis in Case 3, let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ in equation (1). Yu's theorem gives the upper bound 10^{18} for the exponents in equation (5) which is then reduced by Lemma 4.1 of [4] according to

step	$H <$	$\|b_1\| >$	μ	new bound
I.	10^{18}	$0.2 \cdot 10^{19}$	125	126
II.	126	252	17	18
III.	$18,\ p = 2$	36	11	12
III.	$18,\ p = 3$	36	8	8
III.	$18,\ p = 5$	36	5	5

We obtain 99 primitive solutions f_1, f_2, f_3.

The quadratic subfields of K are $M_1 = \mathbb{Q}(\sqrt{2})$, $M_2 = \mathbb{Q}(\sqrt{5})$ and $M_3 = \mathbb{Q}(\sqrt{10})$. The ideal (2) is a square in M_1 and M_3 and prime in M_2. The ideal (3) is prime in M_1 and M_2. The ideal (5) is prime in M_1 and square in M_2 and M_3. Hence by applying Lemma 3 we obtain $a_1 \le 5$, $a_2 = a_3 = 0$. The $99 \cdot 6 = 594$ possible triples F_1, F_2, F_3 were considered by the method of I. Gaál, A. Pethő and M. Pohst [6]. There are 140 solutions of (1).

$(x_2, x_3, x_4, 2^{t_1}3^{t_2}5^{t_3}) = (1,-1,1,3^1), (-1,-1,1,3^1), (1,0,1,3^1), (-1,0,1,3^1),$
$(7,-8,5,3^1), (7,3,5,3^1), (-7,3,5,3^1), (-7,-8,5,3^1), (-1,1,0,3^1), (1,1,0,3^1),$
$(2,1,1,2^2), (0,-1,1,2^2), (0,0,1,2^2), (-2,-2,1,2^2), (2,-2,1,2^2), (-2,1,1,2^2),$
$(0,-2,1,2^23^2), (2,0,1,2^23^2), (2,-1,1,2^23^2), (-2,0,1,2^23^2), (-2,-1,1,2^23^2),$
$(0,1,1,2^23^2), (4,2,3,2^23^2), (-4,2,3,2^23^2), (4,-5,3,2^23^2), (-4,-5,3,2^23^2),$
$(2,1,2,2^43^1), (-2,1,0,2^43^1), (2,1,0,2^43^1), (-2,-3,2,2^43^1), (-2,1,2,2^43^1),$
$(2,-3,2,2^43^1), (-3,-4,2,2^23^3), (-3,2,2,2^23^3), (3,-4,2,2^23^3), (3,2,2,2^23^3),$
$(1,2,0,2^23^3), (-1,2,0,2^23^3), (-3,-4,3,3^25^2), (3,1,3,3^25^2), (-3,1,3,3^25^2),$
$(3,-4,3,3^25^2), (3,-1,2,3^25^2), (-3,-1,2,3^25^2), (1,2,1,3^25^2), (1,-3,1,3^25^2),$
$(-1,2,1,3^25^2), (-1,-3,1,3^25^2), (41,-47,29,3^25^2), (41,18,29,3^25^2),$
$(-41,18,29,3^25^2), (-41,-47,29,3^25^2), (0,1,2,2^8), (0,-3,2,2^8), (48,21,34,2^8),$
$(-48,-55,34,2^8), (-48,21,34,2^8), (48,-55,34,2^8), (-4,-4,3,2^23^15^2),$
$(2,2,1,2^23^15^2), (-2,-3,1,2^23^15^2), (-2,2,1,2^23^15^2), (2,-3,1,2^23^15^2),$
$(4,1,3,2^23^15^2), (4,-4,3,2^23^15^2), (-4,1,3,2^23^15^2), (-4,1,2,2^73^1), (4,-3,2,2^73^1),$
$(4,1,2,2^73^1), (-4,-3,2,2^73^1), (6,3,4,2^45^2), (-6,3,4,2^45^2), (-6,-7,4,2^45^2),$
$(6,-7,4,2^45^2), (-2,-1,2,2^45^2), (2,-1,2,2^45^2), (0,2,1,2^25^3), (0,-3,1,2^25^3),$

$(-10,4,7,2^2 5^3), (10,-11,7,2^2 5^3), (10,4,7,2^2 5^3), (-10,-11,7,2^2 5^3), (4,3,0,2^7 3^2),$
$(-4,3,0,2^7 3^2), (-4,1,0,2^7 3^2), (4,1,0,2^7 3^2), (-12,-13,8,2^7 3^2), (-12,5,8,2^7 3^2),$
$(12,-13,8,2^7 3^2), (12,5,8,2^7 3^2), (5,4,0,2^4 3^1 5^2), (-5,4,0,2^4 3^1 5^2),$
$(-8,-9,6,2^8 3^2), (-8,3,6,2^8 3^2), (8,-9,6,2^8 3^2), (8,3,6,2^8 3^2), (-4,-1,2,2^7 5^2),$
$(4,-1,2,2^7 5^2), (0,-4,3,2^2 3^2 5^3), (0,1,3,2^2 3^2 5^3), (-4,3,4,2^7 3^1 5^2),$
$(-4,-7,4,2^7 3^1 5^2), (4,3,4,2^7 3^1 5^2), (4,-7,4,2^7 3^1 5^2), (6,5,0,2^4 3^2 5^3),$
$(-6,5,0,2^4 3^2 5^3), (-14,5,10,2^4 3^2 5^3), (-14,-15,10,2^4 3^2 5^3), (14,5,10,2^4 3^2 5^3),$
$(14,-15,10,2^4 3^2 5^3), (2,5,0,2^4 3^2 5^3), (-2,5,0,2^4 3^2 5^3), (8,3,4,2^8 3^1 5^2),$
$(8,-7,4,2^8 3^1 5^2), (-8,-7,4,2^8 3^1 5^2), (-8,3,4,2^8 3^1 5^2), (0,3,4,2^8 5^3),$
$(0,-7,4,2^8 5^3), (4,5,0,2^7 3^1 5^3), (-4,5,0,2^7 3^1 5^3), (0,-13,8,2^{10} 3^4), (0,5,8,2^{10} 3^4),$
$(24,-29,18,2^9 3^2 5^2), (24,11,18,2^9 3^2 5^2), (-24,-29,18,2^9 3^2 5^2),$
$(-24,11,18,2^9 3^2 5^2), (8,-3,6,2^9 3^2 5^2), (-8,-3,6,2^9 3^2 5^2), (8,5,0,2^9 3^1 5^3),$
$(-8,5,0,2^9 3^1 5^3), (-28,15,20,2^7 3^3 5^4), (28,-35,20,2^7 3^3 5^4), (28,15,20,2^7 3^3 5^4),$
$(-28,-35,20,2^7 3^3 5^4), (-16,5,0,2^{11} 3^3 5^3), (16,5,0,2^{11} 3^3 5^3), (0,-29,18,2^{10} 3^4 5^3),$
$(0,11,18,2^{10} 3^4 5^3), (32,25,0,2^{13} 3^1 5^5), (-32,25,0,2^{13} 3^1 5^5).$

8.2. Example 2. An example for solving the S-unit equation over K.

Consider the field $K = \mathbb{Q}(\sqrt{19}, \sqrt{7})$. This field belongs to Case 5 and we have $m = m_1 = 19$, $n = n_1 = 7$, $l = 1$. Let $p_1 = 2$, $p_2 = 3$. According to the remark at the end of Section 5.1 we extended this set of primes with 7 and 19. Denote by $I(x_2, x_3, x_4)$ the index form corresponding to the integral basis given in Case 5. Yu's theorem implies an upper bound 10^{28} for the exponents in equation (5), which is then reduced according to the following table.

Step	$H <$	$\|b_1\| >$	μ	newbound
I.	10^{28}	$0.35 \cdot 10^{29}$	300	301
II.	301	1043	34	35
III.	35	122	23	24
IV.	$24, p = 2$	84	22	23
IV.	$24, p = 3$	84	16	16

We obtain six primitive solutions f_1, f_2, f_3.

In $M_1 = \mathbb{Q}(\sqrt{7})$ the class number is 1, 2 is the square of a prime ideal, 3 is the product of two distinct prime ideals. Similarly in $M_2 = \mathbb{Q}(\sqrt{19})$. In $M_3 = \mathbb{Q}(\sqrt{133})$ the class number is 1, 2 is prime, 3 is the product of two distinct prime ideals. Using Lemma 3 we get $a_1 \le 5$ for the exponent of 2 in (6). Since a_1 is even, this implies that only $a_1 = 0, 2, 4$ is possible. To determine a_2 we have to solve an S-unit equation over the quartic field. By using the p-adic linear form estimates we get $a_2 < 0.65 \cdot 10^{28} \log H_1$, $a_2 < 0.65 \cdot 10^{28} \log H_2$. If $a_2 < 0.807 E_i$, the linear form estimates for the exponents of units (application of the estimates of Baker–Wüstholz) imply $H < 10^{32}$. Otherwise, if $a_2 \ge 0.807 E_i$ then $H < 10^{30}$. Hence we conclude $H < 10^{32}$. Using this bound we applied the p-adic reduction and reduction for the exponents of units (application of Lemma 2.2.2 of [3]). The following table summarizes the reduction procedure showing characteristic values that we mostly had in the several possible cases. In the table "p-adic μ" and "Digits" refers to the accuracy used by the p-adic reduction and the application of Lemma 2.2.2 of [3], respectively.

Step	$H <$	p−adic μ	complex Digits	new bound
I.	10^{32}	400	200	445
II.	445	32	50	36
III.	36	25	30	28

Finally we got $a_2 \le 28$, $e_1, e_2, e_3 \in [-28, 28]$ which bounds are valid in all cases. We also have $a_1 = 0, 2, 4$. We substituted these possible exponents into the corresponding representation of φ_{i1} $(i = 1, 2, 3)$. We calculated the corresponding x, y, z, then x_2, x_3, x_4 and checked whether $\gcd(x_2, x_3, x_4) = 1$ and the index of the corresponding element in K is a product of powers of 2 and 3 only. There are 52 solutions of equation (1) which are listed below.

$(x_2, x_3, x_4, 2^{t_1}3^{t_2}) = (1, -1, 0, 3^1), (0, 1, 0, 3^1), (-1, 5, -1, 2^2 3^1), (4, -5, -1, 2^2 3^1),$
$(-4, 5, -1, 2^2 3^1), (1, -5, -1, 2^2 3^1), (3, -4, -1, 3^4), (-1, 4, -1, 3^4), (1, -4, -1, 3^4),$
$(-3, 4, -1, 3^4), (-12, 61, -14, 3^4), (49, -61, -14, 3^4), (-49, 61, -14, 3^4),$
$(12, -61, -14, 3^4), (0, -1, 1, 2^2 3^4), (-1, 1, 1, 2^2 3^4), (1, -1, 1, 2^2 3^4), (0, 1, 1, 2^2 3^4),$
$(3, -4, 0, 2^6 3^2), (-1, 4, 0, 2^6 3^2), (0, -4, -1, 2^4 3^4), (-4, 4, -1, 2^4 3^4), (4, -4, -1, 2^4 3^4),$
$(0, 4, -1, 2^4 3^4), (-13, 16, -4, 2^6 3^5), (3, -16, -4, 2^6 3^5), (-3, 16, -4, 2^6 3^5),$
$(13, -16, -4, 2^6 3^5), (-3, 7, -2, 3^{10}), (4, -7, -2, 3^{10}), (-4, 7, -2, 3^{10}), (3, -7, -2, 3^{10}),$
$(3, -4, 4, 2^7 3^7), (-1, 4, 4, 2^7 3^7), (1, -4, 4, 2^7 3^7), (-3, 4, 4, 2^7 3^7), (15, -8, -8, 2^9 3^{11}),$
$(7, 8, -8, 2^9 3^{11}), (-7, -8, -8, 2^9 3^{11}), (-15, 8, -8, 2^9 3^{11}), (24, -29, -11, 2^2 3^{16}),$
$(-5, 29, -11, 2^2 3^{16}), (5, -29, -11, 2^2 3^{16}), (-24, 29, -11, 2^2 3^{16}),$

$(147,-748,172,2^7 3^{13}),(-601,748,172,2^7 3^{13}),(601,-748,172,2^7 3^{13}),$
$(-147,748,172,2^7 3^{13}),(-60,32,-13,2^4 3^{22}),(-28,-32,-13,2^4 3^{22}),$
$(28,32,-13,2^4 3^{22}),(60,-32,-13,2^4 3^{22}).$

9. Computational experiences

We implemented our algorithm in Maple and executed the routines on a PC (1GHz CPU) under Linux.

The resolution of the S-unit equations over $\mathbb{Z}$ took just a few minutes. Also, the further computations in Example 1 were fast.

In Example 2 the resolution of the S-unit equation in K took a few hours. This was mainly because of the tedious calculation of the p-adic logarithms with high accuracy. Further, the enumeration of the remaining small values of the exponents, testing all possible values of γ_1, γ_2, γ_3 and checking the prime factors of the candidate elements $x_2\omega_2 + x_3\omega_3 + x_4\omega_4$ took again about couple of hours of CPU time. Note that these procedures can be made much faster by implementing an efficient routine for calculating p-adic logarithms of algebraic numbers (this is missing in Maple) and by using a sieve in testing.

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] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.

[3] I.Gaál, Diophantine equations and power integral bases, *Birkhäuser Boston*, 2002.

[4] I. Gaál, I. Járási and F. Luca, A remark on prime divisors of lengths of sides of Heron triangles, *Experimental Mathematics* **12** (2003), 303–310.

[5] I. Gaál, A. Pethő and M. Pohst, On the indices of biquadratic number fields having Galois group V_4, *Arch. Math.* **57** (1991), 357–361.

[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,* **53** (1995), 100–114.

[7] M. N.Gras and F. Tanoe, Corps biquadratiques monogénes, *Manuscripta Math.* **86** (1995), 63–79.

[8] K. Győry, On polynomials with integer coefficients and given discriminant V. p-adic generalizations, *Acta Math. Acad. Sci. Hungar.* **32** (1978), 175–190.

[9] K. Győry, On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.* **54** (1979), 583–600.

[10] T. Nakahara, On the indices and integral bases of non-cyclic but abelian biquadratic fields, *Archiv. der Math.* **41** (1983), 504–508.

[11] G. Nyul, Power integral bases in totally complex biquadratic number fields, *Acta Acad. Paed. Agriensis, Sectio Mathematicae,* **28** (2001), 79–86.

[12] N. P.Smart, Solving a quartic discriminant form equation, *Publ. Math. Debrecen,* **43** (1993), 29–39.

[13] N. P.Smart, The algorithmic resolution of diophantine equations, London Math. Soc., Student Texts 41, *Cambridge University Press*, 1998.

[14] B. M. M. de Weger, Algorithms for diophantine equations, CWI Tracts 65, *Amsterdam*, 1989.

[15] K. S. Williams, Integers of biquadratic fields, *Canad. Math. Bull.* **13** (1970), 519–526.

[16] K. Yu, Linear forms in p-adic logarithms, *Acta Arith.* **53** (1989), 107–186.

ISTVÁN GAÁL
MATHEMATICAL INSTITUTE
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: igaal@math.klte.hu

GÁBOR NYUL
MATHEMATICAL INSTITUTE
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: gnyul@math.klte.hu

(Received November 17, 2004, revised July 8, 2005)