*Publ. Math. Debrecen*
**56 / 3-4** (2000), 251–262

# On the number of solutions of index form equations

By A. BÉRCZES (Debrecen)

*To Professor K. Győry on his 60th birthday*

**Abstract.** In Evertse and Győry [3], [4] and Evertse [2] explicit upper bounds have been established for the numbers of solutions of index form equations. In the case when the Galois group of the splitting field of the index form is triply transitive, recently Győry [11] has considerably improved the bounds of [3] and [2]. The purpose of the present paper is to give, under the same assumption concerning the Galois group, a significant improvement of the bound in [4], which is valid for all but at most finitely many possible values of the constant term of the equation.

## 1. Introduction

Let $K$ be an algebraic number field of degree $n \geq 3$ with discriminant $D_K$ and ring of integers $\mathcal{O}_K$. Let $\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n$ denote the $\mathbb{Q}$-isomorphisms of $K$ in $\mathbb{C}$. For any $\alpha \in K$, put $\alpha^{(i)} = \sigma_i(\alpha)$. Consider an integral basis $\{1, \alpha_2, \dots, \alpha_n\}$ in $\mathcal{O}_K$, and the linear forms $l^{(i)}(\boldsymbol{X}) = X_1 + \alpha_2^{(i)} X_2 + \dots + \alpha_n^{(i)} X_n$ for $i = 1, \dots, n$, with the convention that $l^{(1)}(\boldsymbol{X}) = l(\boldsymbol{X})$. Putting $l_{ij}(\boldsymbol{X}) = l^{(i)}(\boldsymbol{X}) - l^{(j)}(\boldsymbol{X})$,

$$D_{K/\mathbb{Q}}(l(\boldsymbol{X})) := \prod_{1 \leq i < j \leq n} l_{ij}^2(\boldsymbol{X}) \tag{1.1}$$

*Mathematics Subject Classification*: 11D57, 11D61.
*Key words and phrases*: diophantine equation, number of solutions index forms.
Research supported in part by the Hungarian Academy of Sciences, by OTKA 023800, by the Soros Foundation and by the Universitas Foundation.

is a decomposable form with coefficients in $\mathbb{Z}$. It can be written in the form

$$D_{K/\mathbb{Q}}(l(\boldsymbol{X})) = (I(\boldsymbol{X}))^2 D_K, \tag{1.2}$$

where $I(\boldsymbol{X}) = I(X_2, \dots, X_n)$ is a decomposable form of degree $n(n-1)/2$ with coefficients in $\mathbb{Z}$. If $\alpha$ is a primitive integral element of $K$ and $\alpha = x_1 + x_2\alpha_2 + \dots + x_n\alpha_n$ with $x_1, \dots, x_n \in \mathbb{Z}$, then $|I(x_2, \dots, x_n)|$ is precisely the index $I(\alpha)$ of $\alpha$, i.e. the index of the subgroup $\mathbb{Z}^+[\alpha]$ in the additive group $\mathcal{O}_K^+$ of $\mathcal{O}_K$. Hence $I(\boldsymbol{X})$ is called the *index form* of the basis $\{1, \alpha_2, \dots, \alpha_n\}$.

Let $I$ denote a positive rational integer, and $S = \{p_1, \dots, p_s\}$ a finite set of $s \geq 0$ distinct rational primes. Consider the *index form equation*

$$\begin{aligned} I(x_2, \dots, x_n) = \pm I p_1^{z_1} \dots p_s^{z_s} & \\ & \text{in} \quad x_2, \dots, x_n \in \mathbb{Z}, \\ & \text{and} \quad z_1, \dots, z_s \in \mathbb{Z}_{\geq 0} \\ & \text{with} \quad (x_2, \dots, x_n, p_1 \dots p_s) = 1 \text{ if } s > 0. \end{aligned} \tag{1.3}$$

We may and shall assume that $I$ is relatively prime to $p_1, \dots, p_s$. For $s = 0$, the assumption $(x_2, \dots, x_n, p_1 \dots p_s) = 1$ is omitted. We identify the solutions $\boldsymbol{x} = (x_2, \dots, x_n), z_1, \dots, z_s$ and $\boldsymbol{x}' = (x_2', \dots, x_n'), z_1', \dots, z_s'$ of (1.3) if $\boldsymbol{x}' = \pm\boldsymbol{x}$.

In the most interesting case when $s = 0$, Győry [7] proved that (1.3) has only finitely many solutions, and gave an effective upper bound for the solutions. Later, this theorem was extended to the case $s > 0$ by Trelina [13] and Győry and Papp [12]. For surveys presenting further generalizations, we refer to [8], [9], [6].

The first explicit upper bound for the number of solutions of (1.3) was derived by Evertse and Győry [3]. They showed as a consequence of a more general result that (1.3) has at most

$$\left(4 \cdot 7^{g(2s+2\omega(I)+3)}\right)^{n-2} \tag{1.4}$$

solutions. Here $\omega(I)$ denotes the number of distinct prime factors of $I$, and $g$ is the degree of the normal closure of $K$ over $\mathbb{Q}$. Hence $n \leq g \leq n!$.

It follows from a result of Evertse [2] on decomposable form equations that the number of solutions of (1.3) does not exceed

$$\left(2^{33} r^2\right)^{(n-1)^3(s+\omega(I)+1)}, \tag{1.5}$$

where $r = n(n-1)/2$. When $n$ is large and $g$ is large with respect to $n$, this bound is better than (1.4).

Put

$$\Psi(I) = \binom{r}{n-2}^{\omega(I)} \prod_{\substack{p|I \\ p \text{ prime}}} \binom{\mathrm{ord}_p(I)+n-2}{n-2}$$

with $r = n(n-1)/2$, where the product is taken over all distinct prime factors of $I$ and $\mathrm{ord}_p(I)$ denotes the greatest rational integer $a$ for which $p^a$ divides $I$ in $\mathbb{Z}$. As a consequence of a more general theorem concerning decomposable form equations, Evertse and Győry [4] derived in 1997 the upper bound

$$\left(2^{33}r^2\right)^{e(n)(s+1)}\Psi(I) \tag{1.6}$$

for the number of solutions of (1.3). Here $e(n) = \frac{1}{3}(n-1)n(2n-1)-2$. The bound (1.6) is better than (1.5) when all the exponents $\mathrm{ord}_p(I)$ are small.

An important special case is when the Galois group, $\mathcal{G}$, of the normal closure of $K$ over $\mathbb{Q}$ is triply transitive. In other words, for any ordered subsets $\{i_1, i_2, i_3\}$ and $\{i'_1, i'_2, i'_3\}$ of $\{1,\dots,n\}$ there is a $\sigma \in \mathcal{G}$ such that if $\alpha \in K$ then $\sigma(\alpha^{(i_k)}) = \alpha^{(i'_k)}$ for $k = 1,2,3$. For example, $\mathcal{G}$ is triply transitive if $n \geq 5$ and $\mathcal{G} = S_n$ or $A_n$. Under this assumption concerning $\mathcal{G}$ Győry [11] has recently showed that for $s = 0$, equation (1.3) has at most

$$2^{4n(n-1)(\omega(I)+1)+8}$$

solutions*. This is a considerable improvement of (1.4) and (1.5) for $s = 0$. The purpose of our paper is to improve (1.6) under the same assumption concerning $\mathcal{G}$.

**Theorem 1.** *Suppose that the Galois group $\mathcal{G}$ is triply transitive. Then apart from finitely many values of $I$, equation* (1.3) *has at most*

$$2\Psi(I)$$

*solutions. Further, the number of the exceptional $I$'s is at most*

$$e^{30^{20}n^2(s+1)}.$$

*For simplicity, this result was proved in [11] for $s = 0$ only, but the same arguments work for $s > 0$ as well and give the same upper bound with $\omega(I) + s$ instead of $\omega(I)$.

This means that under the assumption of Theorem 1 and apart from finitely many values of $I$, the factor $(2^{33}r^2)^{e(n)(s+1)}$ in (1.6) can be replaced by 2.

For $s = 0$, we obtain as a special case the following result for the equation

$$I(x_2, \dots, x_n) = \pm I \quad \text{in} \quad x_2, \dots, x_n. \tag{1.7}$$

**Theorem 2.** *Suppose again that the Galois group $\mathcal{G}$ is triply transitive. Then apart from at most $e^{30^{20}n^2}$ values of $I$, equation* (1.7) *has at most $2\Psi(I)$ solutions.*

In the proof of Theorem 1 we shall combine some methods from [8] and [11] with some recent results from [10], [1], [4] and [6].

## 2. Auxiliary results

Let $G \subset \mathbb{C}^*$ be a finitely generated subgroup of the multiplicative group $\mathbb{C}^*$, and let $a$, $b$, $a'$, $b'$ be non-zero complex numbers. Then the equations

$$ax + by = 1 \quad \text{in } x, y \in G \tag{2.1}$$

and

$$a'x' + b'y' = 1 \quad \text{in } x', y' \in G$$

are called *equivalent* if $\frac{a}{a'} \in G$ and $\frac{b}{b'} \in G$. Equivalent equations have obviously the same number of solutions.

The number of solutions of the equation

$$x_1 + \dots + x_n = 1 \quad \text{in} \quad x_1, \dots, x_n \in G \tag{2.2}$$

$$\text{with} \sum_{i \in I} x_i \neq 0 \text{ for each non-empty subset } I \text{ of } \{1, \dots, n\}$$

is finite. Denote by $\nu_n = \nu_{n,G}$ this number.

**Lemma 1.** *The number of equivalence classes of equations of the form* (2.1) *which have more than two solutions is at most*

$$\nu_5 + 12\nu_3 + 30\nu_2^2.$$

Proof. See [10]. This lemma is a quantitative version of the main result of [5]. □

**Lemma 2.** *Let $G$ be a finitely generated subgroup of $\mathbb{C}^*$ with rank $r$. Then equation* (2.2) *has at most*

$$e^{(r+2)(6n)^{4n}}$$

*solutions.*

Proof. Lemma 2 is a special case of Theorem 2 of [6]. □

For $n = 2$, a better bound has been obtained in [1].

**Lemma 3.** *Let $G$ be a finitely generated subgroup of $(\mathbb{C}^*)^2$ with rank $r$. Then the number of solutions of the equation*

$$x + y = 1 \quad \text{in } (x, y) \in G$$

*is bounded by $2^{8r+8}$.*

Proof. This is a special case of Theorem 1.1 of [1]. □

Lemmas 1 and 2 give the following

**Lemma 4.** *The number of equivalence classes of equations* (2.1) *having more than two solutions is at most*

$$2e^{(r+2)30^{20}}.$$

As in Section 1, let $S = \{p_1, \dots, p_s\}$ be a set of $s \geq 0$ rational primes. Let $\mathbb{Z}_S$ denote the ring of $S$-integers, and $\mathbb{Z}_S^*$ the group of $S$-units in $\mathbb{Q}$. For any algebraic number field $L$, denote by $\mathcal{O}_L$ the ring of integers and by $\mathcal{O}_L^*$ the group of units in $L$. Further, denote by $M_L$ the set of all places of $L$, and by $S_L$ the subset of $M_L$ consisting of all infinite places of $L$ and of those finite places of $L$ which correspond to prime ideals of $\mathcal{O}_L$ lying above rational primes from $S$. Consider the ring of $S_L$ integers $\mathcal{O}_{S_L}$ and the group of $S_L$-units $\mathcal{O}_{S_L}^*$ in $L$.

Suppose that $L$ is of degree $l$ over $\mathbb{Q}$. Let $\mathcal{M}$ denote a finitely generated $\mathbb{Z}_S$-module in $L$. By the dimension of $\mathcal{M}$ we mean the dimension of the $\mathbb{Q}$-vector space $\mathcal{M}\mathbb{Q}$. Assume that $\mathcal{M}$ has dimension $k$ over $\mathbb{Q}$. Let $\alpha_1, \dots, \alpha_m$ be a set of generators of $\mathcal{M}$ and let $l(\boldsymbol{X}) := \alpha_1 X_1 + \dots + \alpha_m X_m$. Then

$\mathcal{M} = \{x = l(\boldsymbol{x}) : \boldsymbol{x} \in \mathbb{Z}_S^m\}$. Fix an element $c \in \mathbb{Q}^*$ for which $cN_{L/\mathbb{Q}}(l(\boldsymbol{X}))$ has its coefficients in $\mathbb{Z}_S$. Consider the equation

$$cN_{L/\mathbb{Q}}(x) \in I \cdot \mathbb{Z}_S^* \quad \text{in } x \in \mathcal{M}, \tag{2.3}$$

where $I$ denotes a fixed positive rational integer which is relatively prime to $p_1, \dots, p_s$ if $s > 0$.

**Lemma 5.** *The set of solutions of* (2.3) *is contained in some union* $x_1\mathcal{O}_{S_L}^* \cup \dots \cup x_q\mathcal{O}_{S_L}^*$, *where*

$$q \le \binom{l}{k-1}^{\omega(I)} \cdot \prod_{\substack{p|I \\ p \text{ prime}}} \binom{\operatorname{ord}_p(I) + k - 1}{k-1}$$

*and where* $x_1, \dots, x_q$ *are solutions of* (2.3).

Proof. This is a special case of Lemma 4 of [4] □

## 3. Proof of Theorem 1

We shall use Lemma 5 and Győry's method (see e.g. [8, Ch. IV] and [11, Section 5]) to reduce equation (1.3) to an appropriate system of unit equations. Then we shall apply Lemmas 3 and 4 concerning unit equations.

First we introduce some further notation and make some preliminary observations. Let $\xi$ be a primitive integral element of $K$. Denote by $d$ the index of $\xi$ in $\mathcal{O}_K$. Then $D_{K/\mathbb{Q}}(\xi) = d^2 \cdot D_K$. In view of (1.1) and (1.2) it follows that each solution $\boldsymbol{x} \in \mathbb{Z}^{n-1}$, $z_1, \dots, z_s \in \mathbb{Z}_{\ge 0}$ of (1.3) satisfies

$$\prod_{1 \le i < j \le n} l_{ij}^2(\boldsymbol{x}) = D_K I^2 p_1^{2z_1} \dots p_s^{2z_s},$$

whence

$$c \prod_{1 \le i < j \le n} \frac{d \cdot l_{ij}(\boldsymbol{x})}{\xi^{(i)} - \xi^{(j)}} = \pm I p_1^{z_1} \dots p_s^{z_s} \tag{3.1}$$

where $c = d^{1 - \frac{n(n-1)}{2}}$.

Let $K^{(i)} := \mathbb{Q}(\xi^{(i)})$ for $i = 1, \dots, n$. For any distinct $i$, $j$ in $\{1, \dots, n\}$ consider the subfield $K_{ij} = \mathbb{Q}(\xi^{(i)} + \xi^{(j)}, \xi^{(i)} \cdot \xi^{(j)})$ of the field $K^{(i)}K^{(j)}$.

By assumption $\mathcal{G}$, the Galois group of the normal closure of $K$ over $\mathbb{Q}$, is triply transitive. Hence the field $K^{(i)}K^{(j)}$ is of degree $n(n-1)$ over $\mathbb{Q}$. Each $\sigma \in \mathcal{G}$ permutes the elements of $\{1, \dots, n\}$ where $\sigma(i)$ is defined by $\sigma(\xi^{(i)}) = \xi^{\sigma(i)}$. This implies a Galois action on the ordered pairs $(i, j)$. Each $\sigma \in \mathcal{G}$ for which $\sigma(i, j) = (j, i)$ leaves fixed the elements of $K_{ij}$. Therefore $K_{ij}$ is a proper subfield of $K^{(i)}K^{(j)}$. More precisely, $K^{(i)}K^{(j)}$ is a quadratic extension of $K_{ij}$, and hence $K_{ij}$ is of degree $n(n-1)/2$ over $\mathbb{Q}$. Denote by $\lambda^{(i,j)}$ the conjugate of any $\lambda = \lambda^{(1,2)} \in K_{1,2}$ corresponding to $\xi^{(i)} + \xi^{(j)}$, $\xi^{(i)}\xi^{(j)}$ $(1 \le i < j \le n)$ and for simplicity we let $\lambda^{(i,j)} = \lambda^{(j,i)}$.

Since $d\mathcal{O}_K \subseteq \mathbb{Z}[\xi]$, it follows that for every $\alpha \in \mathcal{O}_K$ and each different $i, j$ from $\{1, \dots, n\}$, $\frac{d(\alpha^{(i)} - \alpha^{(j)})}{\xi^{(i)} - \xi^{(j)}}$ is an integer in $K_{ij}$. Denote by $\mathcal{M}$ the $\mathbb{Z}_S$-module in $K_{1,2}$, generated by the coefficients of the linear form $\frac{d \cdot l_{1,2}(\boldsymbol{X})}{\xi^{(1)} - \xi^{(2)}}$. The module $\mathcal{M}$ is of rank at most $n-1$. For any solution $\boldsymbol{x}, z_1, \dots, z_s$ of (1.3), put

$$\delta = \delta^{(1,2)} = \frac{d \cdot l_{1,2}(\boldsymbol{x})}{\xi^{(1)} - \xi^{(2)}}.$$

Then $\delta \in K_{1,2}$, and the numbers $\delta^{(i,j)} = \frac{d \cdot l_{ij}(\boldsymbol{x})}{\xi^{(i)} - \xi^{(j)}}$ are the conjugates of $\delta$ with respect to $K_{1,2}/\mathbb{Q}$. Hence equation (3.1) leads to the equation

$$cN_{K_{1,2}/\mathbb{Q}}(\delta) \in I\mathbb{Z}_S^* \quad \text{in } \delta \in \mathcal{M}. \tag{3.2}$$

By Lemma 5 we deduce that there are solutions $\delta_1, \dots, \delta_q$ of (3.2) such that any solution $\delta$ of (3.2) is contained in $\delta_1 \mathcal{O}^*_{S_{K_{1,2}}} \cup \dots \cup \delta_q \mathcal{O}^*_{S_{K_{1,2}}}$ and that $q \le \Psi(I)$ with the $\Psi(I)$ introduced in Section 1.

Consider now those solutions $\boldsymbol{x}, z_1, \dots, z_s$ of (1.3) for which the corresponding $\delta$ belong to the same coset, say $\delta_1 \mathcal{O}^*_{S_{K_{1,2}}}$. Let $i, j, k$ be arbitrary, but fixed and pairwise distinct elements of $\{1, \dots, n\}$. Then we have

$$l_{ij}(\boldsymbol{x}) + l_{jk}(\boldsymbol{x}) + l_{ki}(\boldsymbol{x}) = 0 \tag{3.3}$$

for any solution $\boldsymbol{x}, z_1, \dots, z_s$ under consideration. We can write $\delta = \delta^{(1,2)} = \delta_1^{(1,2)} \varepsilon^{(1,2)}$ with an appropriate $\varepsilon^{(1,2)} \in \mathcal{O}^*_{S_{K_{1,2}}}$. Now we infer from (3.3) that

$$\rho_1 \frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}} + \rho_2 \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}} = 1 \tag{3.4}$$

where

$$\rho_1 = \frac{\delta_1^{(i,j)}(\xi^{(i)} - \xi^{(j)})}{\delta_1^{(i,k)}(\xi^{(i)} - \xi^{(k)})} \quad \text{and} \quad \rho_2 = \frac{\delta_1^{(j,k)}(\xi^{(j)} - \xi^{(k)})}{\delta_1^{(i,k)}(\xi^{(i)} - \xi^{(k)})}.$$

Observe that (3.4) is a unit equation in the unknowns $\left(\frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}}, \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}}\right)$. For given $i$, $k$, let $\{\varepsilon_1, \dots, \varepsilon_t\}$ be a fundamental system of $S_{K_{ik}}$-units in the field $K_{ik}$. Then

$$t \le \frac{n(n-1)}{2}(s+1).$$

Further, we have

$$\varepsilon^{(i,k)} = \theta \varepsilon_1^{b_1} \dots \varepsilon_t^{b_t},$$

where $\theta$ is a root of unity of $K_{ik}$ and $b_1, \dots, b_t$ are rational integers. The $\varepsilon^{(i,j)}$ and $\varepsilon^{(j,k)}$ being conjugates of $\varepsilon^{(i,k)}$, there exist $\mathbb{Q}$-isomorphisms $\varphi$ and $\chi$ of $K_{ik}$ such that $\varepsilon^{(i,j)} = \varphi(\varepsilon^{(i,k)})$ and $\varepsilon^{(j,k)} = \chi(\varepsilon^{(i,k)})$. Then (3.4) can be written in the form

$$\rho_1 \frac{\varphi(\theta)}{\theta} \left(\frac{\varphi(\varepsilon_1)}{\varepsilon_1}\right)^{b_1} \dots \left(\frac{\varphi(\varepsilon_t)}{\varepsilon_t}\right)^{b_t} + \rho_2 \frac{\chi(\theta)}{\theta} \left(\frac{\chi(\varepsilon_1)}{\varepsilon_1}\right)^{b_1} \dots \left(\frac{\chi(\varepsilon_t)}{\varepsilon_t}\right)^{b_t} = 1.$$

Now suppose that equation (1.3) has two different solutions $\boldsymbol{x}, z_1, \dots, z_s$ and $\boldsymbol{x}', z_1', \dots, z_s'$ for which the corresponding solutions $\left(\frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}}, \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}}\right)$ and $\left(\frac{\varepsilon'^{(i,j)}}{\varepsilon'^{(i,k)}}, \frac{\varepsilon'^{(j,k)}}{\varepsilon'^{(i,k)}}\right)$ of (3.4) coincide, that is

$$\frac{\varepsilon^{(i,j)}}{\varepsilon^{(i,k)}} = \frac{\varepsilon'^{(i,j)}}{\varepsilon'^{(i,k)}} \quad \text{and} \quad \frac{\varepsilon^{(j,k)}}{\varepsilon^{(i,k)}} = \frac{\varepsilon'^{(j,k)}}{\varepsilon'^{(i,k)}},$$

and thus

$$\frac{\varepsilon^{(i,j)}}{\varepsilon'^{(i,j)}} = \frac{\varepsilon^{(k,i)}}{\varepsilon'^{(k,i)}} = \frac{\varepsilon^{(j,k)}}{\varepsilon'^{(j,k)}}.$$

Put $\beta^{(i,j)} = \frac{\varepsilon^{(i,j)}}{\varepsilon'^{(i,j)}}$. Then $\beta^{(i,j)}$ is an $S_{K_{ij}}$-unit in the field $K_{ij}$. Since $\mathcal{G}$ is triply transitive, $K^{(i)}K^{(j)}$ has a $\mathbb{Q}$-isomorphism which lives $\xi^{(i)}$ fixed and moves $\xi^{(j)}$ to $\xi^{(l)}$ for arbitrary $l \in \{1, 2, \dots, n\} \setminus \{i\}$. Among the conjugates of $\beta^{(i,j)}$ there are at least two, namely $\beta^{(i,j)} = \beta^{(k,i)}$, which are equal. But $\beta^{(i,j)}$ and $\beta^{(k,i)}$ are conjugates over $K^{(i)}$, too. Furthermore, $\mathcal{G}$ being triply transitive, $K^{(i)}K^{(j)}$ is a primitive extension of $K^{(i)}$. Together with $\beta^{(i,j)} = \beta^{(k,i)}$ this means that all conjugates of $\beta^{(i,j)}$ over $K^{(i)}$ are equal. Thus $\beta^{(i,j)} \in K^{(i)}$, and similarly $\beta^{(k,i)} \in K^{(k)}$. But $\beta^{(i,j)} = \beta^{(k,i)}$, hence we get $\beta^{(i,j)} \in K^{(i)} \cap K^{(k)}$. It follows from the triply transitivity of $\mathcal{G}$ that $[K^{(i)}K^{(k)} : K^{(i)}] = n-1$ and thus $K^{(i)} \neq K^{(k)}$. Further $K^{(i)}$ is a primitive extension of $\mathbb{Q}$ (because of the doubly transitivity of $\mathcal{G}$), hence we get $K^{(i)} \cap K^{(k)} = \mathbb{Q}$ and so $\beta^{(i,j)} \in \mathbb{Q}$. But $\beta^{(i,j)}$ is an $S_{K_{ij}}$-unit, thus we get $\beta^{(i,j)} \in \mathbb{Z}_S^*$.

The above arguments lead us to the conclusion that $\underline{\varepsilon} = \eta\underline{\varepsilon'}$, with some $\eta \in \mathbb{Z}_S^*$, where $\underline{\varepsilon} = \left(\varepsilon^{(i,j)}\right)_{1\le i\ne j\le n}$ and $\underline{\varepsilon}' = \left({\varepsilon'}^{(i,j)}\right)_{1\le i\ne j\le n}$. Thus $l_{ij}(\boldsymbol{x}) = \eta l_{ij}(\boldsymbol{x}')$ for $1 \le i,j \le n$ with $i \ne j$ and so

$$(\alpha_2 - \alpha_2^{(2)})(x_2 - \eta x_2') + \cdots + (\alpha_n - \alpha_n^{(2)})(x_n - \eta x_n') = 0.$$

Since $K$ is a primitive extension of $\mathbb{Q}$ and $\alpha_2, \dots, \alpha_n$ are $\mathbb{Q}$-linearly independent, it follows that $\alpha_2 - \alpha_2^{(2)}, \dots, \alpha_n - \alpha_n^{(2)}$ are also $\mathbb{Q}$-linearly independent. Hence we infer that $\boldsymbol{x} = \eta\boldsymbol{x}'$ with $\eta \in \mathbb{Z}_S^*$. But by assumption $(x_2, \dots, x_n, p_1 \dots p_s) = 1$ and $(x_2', \dots, x_n', p_1 \dots p_s) = 1$, hence $\eta = \pm 1$ follows. Thus we have shown that different solutions of (1.3) lead to different solutions of the unit equation (3.4).

Now suppose that equation (1.3) has more than two solutions corresponding to the same $\delta_1$. Then for every fixed $i$, $j$, $k$, equation (3.4) has also at least three solutions. Equation (3.4) can be considered as an equation of the type (2.1), where $G$ is the subgroup of $\mathbb{C}^*$ generated by

$$\left\{ \frac{\varphi(\theta)}{\theta}, \frac{\varphi(\varepsilon_1)}{\varepsilon_1}, \dots, \frac{\varphi(\varepsilon_t)}{\varepsilon_t}, \frac{\chi(\theta)}{\theta}, \frac{\chi(\varepsilon_1)}{\varepsilon_1}, \dots, \frac{\chi(\varepsilon_t)}{\varepsilon_t} \right\}.$$

Thus by Lemma 4 there exists a finite set $\mathcal{C}_1$ of pairs $(\kappa_1, \kappa_2) \in (\mathbb{C}^*)^2$ which is independent of $I$ such that

$$\rho_1 = \kappa_1\eta_1 \quad \text{and} \quad \rho_2 = \kappa_2\eta_2$$

with $(\kappa_1, \kappa_2) \in \mathcal{C}_1$ and with some fixed $\eta_1, \eta_2 \in G$. Furthermore, by Lemma 4

$$\#\mathcal{C}_1 \le 2 \cdot e^{(2t+4)30^{20}} \le 2 \cdot e^{(n(n-1)(s+1)+4)30^{20}} := c_1(n,s).$$

For the moment fix $(\kappa_1,\kappa_2)\in(\mathbb{C}^*)^2$. Then $\left(\eta_1\frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}},\eta_2\frac{\varepsilon^{(j,k)}}{\varepsilon^{(k,i)}}\right)$ is a solution of the equation

$$\kappa_1 u'+\kappa_2 v'=1 \quad \text{in } u',v'\in G. \tag{3.5}$$

But equation (3.5) leads to the equation

$$u''+v''=1 \quad \text{in } (u'',v'')\in G' \tag{3.6}$$

where $G'$ is the subgroup of $(\mathbb{C}^*)^2$ generated by

$$\begin{aligned}\Big\{(\kappa_1,1),\left(\frac{\varphi(\theta)}{\theta},1\right),\left(\frac{\varphi(\varepsilon_1)}{\varepsilon_1},1\right),\dots,\left(\frac{\varphi(\varepsilon_t)}{\varepsilon_t},1\right),\\ \left(\frac{\chi(\theta)}{\theta},1\right),\left(\frac{\chi(\varepsilon_1)}{\varepsilon_1},1\right),\dots,\left(\frac{\chi(\varepsilon_t)}{\varepsilon_t},1\right),\\ (1,\kappa_2),\left(1,\frac{\varphi(\theta)}{\theta}\right),\left(1,\frac{\varphi(\varepsilon_1)}{\varepsilon_1}\right),\dots,\left(1,\frac{\varphi(\varepsilon_t)}{\varepsilon_t}\right),\\ \left(1,\frac{\chi(\theta)}{\theta}\right),\left(1,\frac{\chi(\varepsilon_1)}{\varepsilon_1}\right),\dots,\left(1,\frac{\chi(\varepsilon_t)}{\varepsilon_t}\right)\Big\}.\end{aligned}$$

Then $\left(\kappa_1\eta_1\frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}},\kappa_2\eta_2\frac{\varepsilon^{(j,k)}}{\varepsilon^{(k,i)}}\right)$ is a solution of equation (3.6), which by Lemma 3 has at most

$$2^{8(4t+6)+8}\le 2^{8(2n(n-1)(s+1)+6)+8}:=c_2(n,s)$$

solutions. Thus, allowing now $(\kappa_1,\kappa_2)$ to vary through $\mathcal{C}_1$, $\rho_1\frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}=\kappa_1\eta_1\frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}$ can assume at most $c(n,s):=c_1(n,s)\cdot c_2(n,s)$ different values and so does $\frac{\delta_1^{(i,j)}}{\delta_1^{(k,i)}}\cdot\frac{\varepsilon^{(i,j)}}{\varepsilon^{(k,i)}}$.

Taking $k=1$ this yields that for every distinct $i$, $j$,

$$\delta_1^{(i,j)}\varepsilon^{(i,j)}=\mu_{ij}\delta_1^{(1,i)}\varepsilon^{(1,i)},$$

where $\mu_{i,j}$ can assume at most $c(n,s)$ values. Put $i:=2$, $j:=3$, $L:=K^{(1)}K^{(2)}K^{(3)}$ and $l:=[L:K_{2,3}]$. Taking the $L/\mathbb{Q}$-norm of the above equation and using (3.2) we have

$$(I/c)^l\,\mathbb{Z}_S^*\ni N_{L/\mathbb{Q}}(\delta_1^{(2,3)}\varepsilon^{(2,3)})=N_{L/\mathbb{Q}}(\delta_1^{(1,2)})\cdot N_{L/\mathbb{Q}}(\varepsilon^{(1,2)})\cdot N_{L/\mathbb{Q}}(\mu_{2,3}).$$

However, $c$ and $\delta_1$ are fixed and $N_{L/\mathbb{Q}}(\mu_{2,3})$ can take at most $c(n,s)$ distinct values. So it follows that apart from a factor from $\mathbb{Z}_S^*$, $I$ can assume also at most $c(n,s)$ distinct values. Now a simple computation proves the bound for the number of exceptional $I$'s, given in Theorem 1.

If $I$ does not take any of these values, then the number of solutions of (1.3) is at most the product of the number of solutions of (3.4) and the number of the possibilities for $\delta_1$. Because of the choice of $I$ (3.4) has at most 2 solutions. Further, by Lemma 5 we have at most $\Psi(I)$ choices for $\delta_1$. This completes the proof of Theorem 1.

*Acknowledgements.* I would like to thank my supervisor, Professor K. Győry, for his help in writing this paper, and the referees, for their valuable remarks.

### References

[1] F. Beukers and H. P. Schlickewei, The equation $x+y=1$ in finitely generated groups, *Acta Arith.* **78** (1996), 189–199.

[2] J. -H. Evertse, The number of solutions of decomposable form equations, *Invent. Math.* **122** (1995), 559–601.

[3] J. -H. Evertse and K. Győry, On unit equations and decomposable form equations, *J. Reine Angew. Math.* **358** (1985), 6–19.

[4] J. -H. Evertse and K. Győry, The number of families of solutions of decomposable form equations, *Acta Arith.* **80** (1997), 367–394.

[5] J. -H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, $S$-unit equations in two unknowns, *Invent. Math.* **92** (1988), 461–477.

[6] J. -H. Evertse and H. P. Schlickewei, The absolute subspace theorem and linear equations with unknowns from a multiplicative group, Number Theory in Progress (K. Győry, H. Iwaniec and J. Urbanowicz, eds.), *Walter de Gruyter*, *Berlin – New York*, 1999, 121–142.

[7] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné III, *Publ. Math. Debrecen* **23** (1976), 141–165.

[8] K. Győry, Résultats effectifs sur la représentation des entiers par des formes décomposables, *Queen's Papers in Pure and Applied Math.* No. 56, *Kingston, Canada*, 1980.

[9] K. Győry, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta Math. Hungar.* **42** (1983), 45–80.

[10] K. Győry, Upper bounds for the number of solutions of unit equations in two unknowns, *Lithuanian Math. J.* **32** (1992), 40–44.

[11] K. Győry, Discriminant form and index form equations, Proceedings of the Number Theory Conference, *Graz*, 1998 (*to appear*).

[12] K. Győry and Z. Z. Papp, On discriminant form and index form equations, *Studia Sci. Math. Hungar.* **12** (1977), 47–60, (1980).

[13] L. A. Trelina, On the greatest prime factor of an index form, *Dokl. Akad. Nauk BSSR* **21** (1977), 975–976. (in *Russian*)

A. BÉRCZES
INSTITUTE OF MATHEMATICS AND INFORMATICS
LAJOS KOSSUTH UNIVERSITY
H–4010 DEBRECEN, P.O. BOX 12
HUNGARY

*E-mail*: berczesa@math.klte.hu

*(Received August 16, 1998; revised December 11, 1999)*