**References**

[1] E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der Quadratischen Reste*, Dissertation, Berlin 1906.

[2] Thomas Storer, *Cyclotomy and difference sets*, in *Lectures in Advanced Math.*, vol. 2, Markham, Chicago 1967, vii + 134 pp.

[3] A. L. Whiteman, *A family of symmetric block designs*, J. Combin. Theory, Sec. A, 47 (1988), 153–156.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
Berkeley, California 94720
U.S.A.

*Received on 26.8.1988*
*and in revised form on 16.11.1988* (1861)

ACTA ARITHMETICA
LIII (1990)

# On unit equations with rational coefficients

by

B. BRINDZA* (Sydney) and K. GYŐRY* (Debrecen)

*To the memory of Professor V. G. Sprindžuk*

**1. Introduction.** Let $K$ be an algebraic number field of degree $n$ with ring of integers $O_K$ and unit group $U_K$. Many numbertheoretical problems lead to equations of the types

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

or more generally

$$ax+by=c \quad \text{in } x, y\in O_K\setminus\{0\} \quad \text{with } \max\{|N_{K/Q}(x)|, |N_{K/Q}(y)|\} \leqslant N \tag{2}$$

where $a$, $b$ and $c$ are given non-zero elements of $K$ and $N \geqslant 1$ is a given integer. For surveys on equations (1) and (2) and their applications we refer to [15], [8], [9], [10], [20], [11], [18], [6] and [12]. Equation (1) is called a *unit equation*. For $N = 1$, equation (2) becomes equation (1). Further, for $N \geqslant 1$, equation (2) can be reduced to finitely many unit equations. The number of solutions of (1) can be estimated from above by a bound which depends only on $n$ (cf. Evertse [3]). Moreover, most of the unit equations have considerably fewer solutions (cf. Győry [7] and Evertse, Győry, Stewart and Tijdeman [5]). These and other related results will be referred to in more detail at the beginnings of Sections 2 and 3.

The main purpose of the present paper is to considerably refine the results of [7] and [5] in the important special case when the coefficients $a$, $b$, $c$ in (1) are rational numbers. Furthermore, we shall establish our results for the more general equation (2) having rational coefficients $a$, $b$, $c$. In this situation (2) cannot be reduced in general to equations of type (1) with rational coefficients. It will be enough to deal with the case when, in (1) and (2), $a$, $b$ and $c$ are pairwise relatively prime positive integers (cf. Section 2). We shall show (cf. Section 2, Theorem 1) that for all but finitely many triples $(a, b, c)\in N^3$ with coprime $a, b, c$, equation (2) has at most one, so-called trivial, solution.

* Research supported in part by Grant 273 from the Hungarian National Foundation for Scientific Research.

Further, for fixed coprime $a, b \in N$ we shall obtain a more precise result (cf. Section 2, Theorem 2). It will be proved that for all but finitely many positive integers $c$ with $(ab, c) = 1$, equation (2) has a trivial solution $(x, y)$ if and only if $a = b = 1$, $c = x+y$ and $x, y$ are conjugate elements in some real quadratic subfield of $K$.

Theorems 1 and 2 are ineffective in the sense that their proofs do not enable one to determine the finitely many exceptional equations which have a non-trivial solution or more than one trivial solutions. This is due to the fact that in the proofs the Thue–Siegel–Roth–Schmidt method is involved. By using an effective lower bound of Loxton [13] for simultaneous linear forms in logarithms we shall also establish (cf. Section 3, Theorem 3) a weaker but effective version of Theorem 2. Moreover, we shall give (cf. Section 3, Theorem 4) a quantitative version of Theorem 3 by deriving an effective upper bound for the minima of the sizes of the components of solutions $(x, y)$ of (2). This bound has the property that it tends to zero as $c$ tends to infinity. This implies that under appropriate conditions, equation (2) has no solution.

The ineffective results are formulated in Section 2. Section 3 is devoted to the effective results. Theorems 1 and 2 are proved in Section 4, Theorem 4 in Section 5.

**2. Ineffective results.** We shall use the same notation as above. Consider first equations (1) and (2) in the general case when $a, b, c$ are not necessarily rational elements of $K$. Denote by $v_1(a, b, c)$ and $v_N(a, b, c)$ the number of solutions of (1) and (2), respectively. Every solution of (1) is also a solution of (2), hence $v_1(a, b, c) \leqslant v_N(a, b, c)$. It was proved by Evertse [3] that

$$v_1(a, b, c) \leqslant 3 \times 7^{n+2(r+1)}$$

where $r$ denotes the unit rank of $K$. Equation (2) can be reduced to $\psi^2(N)$ equations of type (1) where $\psi(N)$ is the maximal number of pairwise non-associate non-zero elements $\alpha$ in $O_K$ with $|N_{K/Q}(\alpha)| \leqslant N$. Hence

$$v_N(a, b, c) \leqslant 3\psi^2(N) \times 7^{n+2(r+1)}.$$

It follows from certain explicit estimates of Sunley [22] that

$$\psi(N) < e^{20n^2}|D_K|^{1/(n+1)}(\log|2D_K|)^n N.$$

Here $D_K$ denotes the discriminant of $K$.

Two triples $(a, b, c)$ and $(a', b', c')$ in $(K^*)^3$ (1) (and the corresponding unit equations) are called *K-equivalent* if

$$a' = \lambda\varepsilon_1 a, \quad b' = \lambda\varepsilon_2 b, \quad c' = \lambda\varepsilon_3 c$$

with some $\lambda \in K^*$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in U_K$. It is easy to check that if $(a, b, c)$ and $(a', b', c')$ are $K$-equivalent then $v_N(a, b, c) = v_N(a', b', c')$ for all $N \geqslant 1$.

(1) $K^*$ denotes the set of non-zero elements of $K$.



Obviously, the same holds for $Q$-equivalent triples from $(Q^*)^3$. Evertse, Győry, Stewart and Tijdeman [5] showed that $v_1(a, b, c) \leqslant 2$ for all but finitely many $K$-equivalence classes of triples $(a, b, c) \in (K^*)^3$(*). Further, they pointed out (see [6], § 1) that, for $r > 0$, the upper bound "two" cannot be improved, because there are infinitely many $K$-equivalence classes of triples $(a, b, c) \in (K^*)^3$ with $v_1(a, b, c) = 2$. However, the method of proof used in [5] and [6] does not provide any more information about the equations of type (1) having at most two solutions. Our Theorem 1 below characterizes, with at most finitely many exceptions, both the $Q$-equivalence classes of triples $(a, b, c) \in (Q^*)^3$ for which equation (2) is solvable and all the solutions of these equations.

In the remainder of this section we assume that in (1) and (2) the coefficients $a, b, c$ are rational numbers. Before stating Theorem 1 we make some remarks. If $(x, y)$ is a solution of (2) then so is $(x', y')$ for all those conjugates $x', y'$ of $x, y$ which belong to $K$. We shall not distinguish between conjugate solutions.

A solution $(x, y)$ of (1) or (2) will be called *trivial* if $x$ and $y$ belong to $Q$ or a real quadratic subfield of $K$. It is clear that there are infinitely many $Q$-equivalence classes of triples $(a, b, c) \in (Q^*)^3$ for which equations (1) and (2) have a trivial solution in $Q$. Further, if $K$ contains a real quadratic subfield, $L$ say, with ring of integers $O_L$ then, for any non-zero $x, y \in O_L$ with $\max\{|N_{K/Q}(x)|, |N_{K/Q}(y)|\} \leqslant N$ for which $x, y$ and 1 are pairwise linearly independent over $Q$, $(x, y)$ is a trivial solution of some equation of type (2) with rational coefficients.

Equations (1) and (2) with rational coefficients can have relatively many solutions. Nagell [15] showed that for $n \geqslant 5$ there exists an algebraic number field $K$ of degree $n$ such that $v_1(1, 1, 1) \geqslant 3(2n-3)$. Furthermore, equation (2) can have many trivial solutions if $N$ is sufficiently large. Indeed, let $a, b$ and $c$ be positive rational integers with coprime $a$ and $b$. Then all solutions of the equation $ax+by = c$ in $x, y \in Z$ can be given in the form

$$x = x_0 + at, \quad y = y_0 - bt, \quad t = 0, \pm 1, \pm 2, \ldots$$

where $(x_0, y_0)$ is a particular solution with $\max(|x_0|, |y_0|) \leqslant A := \max(a, b, c)$. It is easy to see that if now $N > A^n$ then at least $N^{1/n}/A$ of the solutions in question satisfy (2), i.e. $v_N(a, b, c) \geqslant N^{1/n}/A$.

THEOREM 1. *Apart from finitely many $Q$-equivalence classes of triples $(a, b, c) \in (Q^*)^3$, equation (2) with non-zero rational coefficients has at most one solution (up to conjugacy) which is a trivial solution.*

All those equations of type (2) with rational coefficients which have solution in some real quadratic subfield $L$ of $K$ can be parametrized (provided that the fundamental unit and a maximal set of pairwise non-associate integers

(*) Added in proof. Recently, Evertse and Győry proved (J. Reine Angew. Math. 399 (1989), 60–80) the same assertion for $v_N(a, b, c)$.

$\alpha$ in $L$ with $|N_{K/\mathbf{Q}}(\alpha)| \leqslant N$ are given). For simplicity, let us consider the particular case $N = 1$. Suppose that $K$ has a real quadratic subfield $L$ with unit group $U_L$. Then $L = \mathbf{Q}(\sqrt{d})$ for some squarefree rational integer $d > 0$. Further, $\{1, w\}$ is an integral basis for $L$ with $w = (1+\sqrt{d})/2$ or $w = \sqrt{d}$ according as $d \equiv 1 \pmod 4$ or $d \equiv 2, 3 \pmod 4$. If $(x, y)$ is a solution of (1) with $x, y$ belonging to $L$ then

$$x = \pm\varepsilon^u, \quad y = \pm\varepsilon^v \quad \text{with some } u, v \in \mathbf{Z}$$

where $\varepsilon$ denotes the fundamental unit of $L$ with $\varepsilon > 1$. We have

$$\varepsilon^u = \varepsilon'_u + \varepsilon''_u w, \quad \varepsilon^v = \varepsilon'_v + \varepsilon''_v w$$

with appropriate rational integers $\varepsilon'_u, \varepsilon''_u, \varepsilon'_v, \varepsilon''_v$ where $\varepsilon''_u \neq 0$ for $u \neq 0$ and $\varepsilon''_v \neq 0$ for $v \neq 0$. If $x$ and $y$ are rational (i.e. $x, y \in \{1, -1\}$) then

$$a(\operatorname{sign} x) + b(\operatorname{sign} y) = c.$$

For not rational $x, y$ we have $uv \neq 0$ and $u \neq v$. Then it follows from (1) that up to a proportional factor, the coefficients $a, b$ and $c$ are determined by

$$a = (\operatorname{sign} y)\varepsilon''_v, \quad b = -(\operatorname{sign} x)\varepsilon''_u, \quad c = (\operatorname{sign} x)(\operatorname{sign} y)(\varepsilon'_u\varepsilon''_v - \varepsilon''_u\varepsilon'_v).$$

These numbers $a, b, c$ are non-zero rational integers for all distinct non-zero $u, v \in \mathbf{Z}$. Further, when $u, v$ with $u \neq v$ run through the rational integers these triples provide all the equations of type (1) with rational coefficients which have a solution in $U_L \backslash \{1, -1\}$.

In the next theorem we deal with equations (1) and (2) for fixed coefficients $a$ and $b$. Every $\mathbf{Q}$-equivalence class of $(\mathbf{Q}^*)^3$ contains a representative $(a, b, c)$ with relatively prime positive integers $a, b$ and $c$. Hence we may assume without loss of generality that in (1) and (2) $a, b$ and $c$ are positive integers, that $(a, b) = 1$ and that, in case of (1), $a, b$ and $c$ are pairwise relatively prime. This latter assumption may be made for equation (2), too. Indeed, if $(x, y)$ is a solution of (2) then the greatest common divisors $(a, c)$ and $(b, c)$ divide in $O_K$ $y$ and $x$, respectively. After dividing in (2) $a, c$ and $y$ by $(a, c)$ and $b, c$ and $x$ by $(b, c)$ the new coefficients will be pairwise relatively prime.

It follows from Theorem 1 that for all but finitely many positive integers $c$, the equation

$$(2') \quad x + y = c \quad \text{in } x, y \in O_K \backslash \{0\} \quad \text{with } \max\{|N_{K/\mathbf{Q}}(x)|, |N_{K/\mathbf{Q}}(y)|\} \leqslant N$$

has at most one, trivial solution (up to conjugacy). But if $(x, y)$ is a solution of (2') then so is $(y, x)$. Hence either $x = y$ (when $x, y \in \mathbf{Z}$) or $x$ and $y$ must be conjugate real quadratic integers in $K$. On the other hand, if $K$ has a real quadratic subfield then there are infinitely many positive integers $c$ which can be represented in the form (2') with conjugate integers $x, y$ from the subfield under consideration.



THEOREM 2. *Let $a$ and $b$ be relatively prime positive rational integers. There exists a number $C_1(K, N)$, depending only on $K$ and $N$, with the following property. For all but at most $C_1(K, N)$ positive integers $c$ with $(ab, c) = 1$, equation (2) is solvable if and only if $a = b = 1$ and $c$ can be represented in the form (2') with some conjugate real quadratic integers $x, y$ in $O_K$. In this case $(x, y)$ is the only solution of (2).*

Clearly, Theorems 1 and 2 yield the same assertions for equations of type (1) by choosing $N = 1$. An interesting consequence of Theorem 2 is that if $a$ and $b$ are coprime positive integers with $ab > 1$ then $ax + by$ can assume at most $2C_1(K, 1)$ rational integer values whenever $x, y$ run through the units of $K$.

In Theorems 1 and 2 the situation becomes much simpler when $K$ contains no real quadratic subfield. Then we have as immediate consequences the following corollaries.

COROLLARY 1. *Assume that $K$ has no real quadratic subfield. Then apart from finitely many $\mathbf{Q}$-equivalence classes of triples $(a, b, c) \in (\mathbf{Q}^*)^3$, equation (2) with non-zero rational coefficients has at most one solution $(x, y)$ in which $x, y$ are rational integers.*

COROLLARY 2. *Let $a, b$ be coprime positive integers and assume that $K$ has no real quadratic subfield. Then apart from at most $C_1(K, 1)$ positive integers $c$, equation (1) with positive integer coefficient $c$ has no solution.*

The proofs of Theorems 1 and 2 can be found in Section 4. They are based on a combination of the above-mentioned result of [5] with a recent theorem of Evertse and Győry [4] on unit equations in more than two unknowns. The results utilized from [5] and [4] are ineffective, hence our above theorems are also ineffective. Our method of proof does not make it possible to determine the finitely many equivalence classes of equations having a non-trivial solution or more than one trivial solutions.

**3. Effective results.** We keep the notation of Sections 1 and 2. First consider again equations (1) and (2) in the general case when $a, b$ and $c$ are arbitrary elements of $K^*$. For an algebraic integer $\alpha$ we denote by $|\overline{\alpha}|$ the *size* of $\alpha$, that is the maximum of the absolute values of the conjugates of $\alpha$. By means of Baker's method effective upper bounds can be derived for the sizes of $x$ and $y$ where $(x, y)$ is an arbitrary solution of (1) or (2). Assuming that $a, b, c \in O_K \backslash \{0\}$ (which is no restriction), the best known bound (cf. [8]) for the solutions $(x, y)$ of (2) is of the form

$$(3) \quad \max(|\overline{x}|, |\overline{y}|) < \exp\{(5(n+1))^{30(n+1)} |D_K|^{3/2} (\log |2D_K|)^{3n} \log AN\}$$

where $A := \max(|\overline{a}|, |\overline{b}|, |\overline{c}|, 3)$.

As was mentioned in the preceding section, $v_1(a, b, c) \leqslant 2$ for all but finitely many $K$-equivalence classes of triples $(a, b, c) \in (K^*)^3$. This result is, however, ineffective, its proof does not enable one to determine all triples

$(a, b, c)$ for which $v_1(a, b, c) > 2$. Some weaker but effective results have also been established in this direction by using Baker's method. Győry [7] showed in 1979 that $v_1(a, b, c) \leqslant r+1$ for infinitely many and effectively determinable $K$-equivalence classes of $(a, b, c) \in (K^*)^3$. More precisely, it was proved in [7] that this bound is valid for every triple $(a, b, c) \in (O_K \setminus \{0\})^3$ which satisfies for some $\varrho > 0$ the inequality

$$|N_{K/\dot{Q}}(c)| > \max\{C_2(K, \varrho), \left(\min(|N_{K/Q}(a)|, |N_{K/Q}(b)|)\right)^{1+\varrho}\}$$

where $C_2(K, \varrho)$ is an effectively computable number (which was given explicitly in [7]). There are, however, infinitely many $K$-equivalence classes which have no such a representative $(a, b, c)$. Later, Evertse, Győry, Stewart and Tijdeman [5] showed that $v_1(a, b, c) \leqslant r+2$ for all but finitely many $K$-equivalence classes of triples $(a, b, c) \in (K^*)^3$ which can be effectively determined(*).

In the remaining part of this section we shall deal with equations (1) and (2) in the case when the coefficients $a$, $b$ and $c$ are rational numbers. As we have shown in Section 2, in this case we may suppose without loss of generality that $a$, $b$ and $c$ are pairwise relatively prime positive rational integers. Further, we assume that $\max(a, b, c) = c$. In case of equation (1) this is no restriction, because this situation can be achieved by multiplying (1) by $x^{-1}$ or $y^{-1}$ if necessary.

If $K$ is a normal extension of $\boldsymbol{Q}$ then any solution of (1) yields further solutions by taking conjugates. Then, subject to appropriate conditions concerning $a$, $b$, $c$ and $K$, the above-quoted upper bounds for $v_1(a, b, c)$ lead to a contradiction. The following theorem gives, however, a much more precise result.

THEOREM 3. *There exists an effectively computable positive number* $C_3 = C_3(n, |D_K|)$ *with the following property. If*

$$c > \exp\{\max((2N)^{C_3}, (\log 3a)^2 (\log 3b)^2)\}$$

*then* (2) *has at most one solution (up to conjugacy). Further, if* $ab > 1$ *or* $n = [K:\boldsymbol{Q}]$ *is odd then* (2) *has no solution.*

Theorem 3 is a weaker but effective version of Theorem 2. Theorem 3 should also be compared with the above-quoted result of [7]. For triples $(a, b, c) \in \boldsymbol{N}^3$, Theorem 3 provides a more precise result on equation (1). On the other hand, in the case $a = b = 1$, $N = 1$ and $n$ odd, the assertion of Theorem 3 can also be deduced from the result of [7].

As we have seen in Section 2, if $a = b = 1$ and $K$ has a real quadratic subfield (when $n$ is even) then (2) has a solution $(x, y)$ for infinitely many $c \in \boldsymbol{N}$ and $\min(|\overline{x}|, |\overline{y}|)$ can be arbitrarily large, provided that $c$ is sufficiently large. This shows that in this case there does exist an exceptional solution in

(*) Added in proof. Recently, Evertse and Győry (J. Reine Angew. Math. 399 (1989), 60–80) extended this result to $v_N(a, b, c)$.



Theorem 3 and Theorem 4 below. Further, the examples given in Section 2 show that Theorem 3 does not remain valid for those $c$ which are not large enough relative to $N$ or $\max(a, b)$.

Theorem 3 is a consequence of the following quantitative version.

THEOREM 4. *There exists an effectively computable number* $C_4 = C_4(n, |D_K|)$ *with the following property. If* $c > \exp\{(2N)^{C_4}\}$ *then apart from at most one exception (up to conjugacy), each solution of equation* (2) *satisfies*

$$\min(|\overline{x}|, |\overline{y}|) < \frac{\exp\{((\log 3a)(\log 3b)(\log c))^{2/3}\}}{c}. \tag{4}$$

*Further, if* $ab > 1$ *or* $n$ *is odd then each solution of* (2) *satisfies* (4).

This bound in (4) has the property that if $c$ is large enough with respect to $a$ and $b$ then the bound becomes less than 1. However, for any non-zero algebraic integers $x$, $y$, $\min(|\overline{x}|, |\overline{y}|) \geqslant 1$ holds, hence Theorem 3 immediately follows from Theorem 4.

It is interesting to compare the estimates (4) and (3). From equation (2) and estimate (4) one can easily deduce an upper bound also for $\max(|\overline{x}|, |\overline{y}|)$ and, for $c$ large, this gives a better estimate than (3). In the case when $a, b, c \in \boldsymbol{N}$ and $ab > 1$ or $n$ is odd, for large $c$ Theorem 4 can be considered as a considerable refinement of the result (3).

**4. Proofs of Theorems 1 and 2.** We adopt the notation of Sections 1 and 2. To prove Theorems 1 and 2 we shall need two lemmas.

For any $\alpha \in K^*$ and any prime ideal $\mathfrak{p}$ in $O_K$, we denote by $\mathrm{ord}_{\mathfrak{p}}\alpha$ the exponent of $\mathfrak{p}$ in the prime ideal decomposition of the principal ideal $(\alpha)$. Let $S$ be a finite (possibly empty) set of prime ideals in $O_K$. An element $\alpha$ of $K^*$ is said to be an *$S$-unit* if $\mathrm{ord}_{\mathfrak{p}}\alpha = 0$ for all prime ideals $\mathfrak{p}$ not contained in $S$. The $S$-units form a group under multiplication which is denoted by $U_S$. This group $U_S$ contains $U_K$ as a subgroup and if $S$ is empty then $U_S = U_K$. Consider the so-called $S$-unit equation

$$ax + by = c \quad \text{in } x, y \in U_S, \tag{5}$$

where $a, b, c \in K^*$. Equation (5) is a generalization of equation (1).

The triples $(a, b, c)$, $(a', b', c')$ in $(K^*)^3$ will be said to be *$(K, S)$-equivalent* if there are $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in U_S$ and $\lambda \in K^*$ such that $a' = \lambda\varepsilon_1 a$, $b' = \lambda\varepsilon_2 b$, $c' = \lambda\varepsilon_3 c$. Obviously, the number of solutions of (5) remains unchanged when $(a, b, c)$ is replaced by a $(K, S)$-equivalent triple. The result of [5] quoted in Section 2 was proved in the following more general form.

LEMMA 1 (Evertse, Győry, Stewart and Tijdeman [5]). *Equation* (5) *has at most two solutions for all but finitely many* $(K, S)$*-equivalence classes of triples* $(a, b, c) \in (K^*)^3$.

Proof. This is Theorem 1 in [5].

Let $k \geqslant 2$ be an integer, and let $a_0, a_1, \ldots, a_k$ be non-zero elements of $K$.

The equation

$$a_1x_1+\ldots+a_kx_k=a_0 \quad \text{in } x_1,\ldots,x_k\in U_S \tag{6}$$

is a generalization of equation (5). A solution $(x_1,\ldots,x_k)$ of (6) is called *non-degenerate* if

$$\sum_{j\in J} a_jx_j\neq 0 \quad \text{for each non-empty subset } J \text{ of } \{1,\ldots,k\}$$

and *degenerate* otherwise. It is clear that if $U_S$ is infinite and if (6) has a degenerate solution then (6) has infinitely many degenerate solutions. Evertse [2] and van der Poorten and Schlickewei [16] proved independently of each other that (6) has only finitely many non-degenerate solutions. The next lemma is a refinement of this result.

LEMMA 2 (Evertse and Győry [4]). *The number of non-degenerate solutions of* (6) *is at most* $C_5(k, U_S)$, *where* $C_5$ *is a number depending only on* $k$ *and* $U_S$.

Proof. This is a special case of Theorem 1 in [4]. For $k=2$, an explicit expression for $C_5(2, U_S)$ can be found in Evertse [3].

In what follows, $C_6, C_7, \ldots, C_{22}$ will denote positive numbers which depend only on $K$ and $N$.

Proof of Theorem 1. Every prime ideal $\mathfrak{p}$ of $O_K$ divides some rational prime $p$ for which $N(\mathfrak{p})=p^{f_\mathfrak{p}}$ with some positive integer $f_\mathfrak{p}\leqslant n$. Denote by $S$ the set of those prime ideals in $O_K$ which are divisors of rational primes not exceeding $N$. Then $S$ is finite and $U_S$, the corresponding $S$-unit group, depends only on $K$ and $N$. Further, $x$ and $y$ are $S$-units for each solution $(x, y)$ of (2).

We can choose from every $Q$-equivalence class of $(Q^*)^3$ a uniquely determined representative $(a, b, c)$ with relatively prime positive rational integers $a$, $b$ and $c$. Hence it suffices to prove the theorem for equations of type (2) with relatively prime positive integer coefficients. Further, we note that if $(x, y)$ is a solution of (2) then (2) implies that $(a, b)=1$, $(a, c)\mid y$ and $(b, c)\mid x$ in $O_K$. So the absolute values of $(a, c)$ and $(b, c)$ do not exceed $N^{1/n}$.

Suppose that equation (2) with relatively prime coefficients $a, b, c\in N$ has at least three solutions. Then it follows from Lemma 1 that

$$a=\lambda\varepsilon_1a', \quad b=\lambda\varepsilon_2b', \quad c=\lambda\varepsilon_3c' \tag{7}$$

where $\lambda\in K^*$, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are $S$-units and $(a', b', c')$ belongs to a finite subset of $(K^*)^3$ of cardinality at most $C_6$ which is independent of $a$, $b$ and $c$. Further, we can write

$$a=e_1a_1, \quad b=e_2b_1, \quad c=e_3c_1 \tag{8}$$

where $e_1, e_2, e_3, a_1, b_1, c_1$ are positive integers such that $e_1, e_2, e_3$ are divisible only by primes not exceeding $N$ and that $a_1, b_1, c_1$ have no prime factor $\leqslant N$. Since, by assumption, $a, b, c$ are relatively prime hence so are both $e_1, e_2, e_3$ and $a_1, b_1, c_1$. Furthermore, $e_1, e_2, e_3$ are $S$-units.



We deduce from (7) and (8) that

$$\left(\frac{a_1}{b_1}\right)^n=\left(\frac{e_2}{e_1}\right)^n N_{K/Q}\left(\frac{\varepsilon_1}{\varepsilon_2}\right)N_{K/Q}\left(\frac{a'}{b'}\right). \tag{9}$$

The primes in the prime decomposition of $N_{K/Q}(\varepsilon_1/\varepsilon_2)$ do not exceed $N$. But $a_1$ and $b_1$ are not divisible by primes $\leqslant N$, hence (9) implies that $(a_1/b_1)^n$ and so $a_1/b_1$ are uniquely determined by $N_{K/Q}(a'/b')$. Further, $(a_1, b_1)=1$ and $N_{K/Q}(a'/b')$ assumes at most $C_7$ distinct values. Thus the number of possible values of $a_1$ and $b_1$ is at most $C_7$. We can proceed in the same way with $a_1$ and $c_1$, and in view of $|(a_1, c_1)|\leqslant|(a, c)|\leqslant N^{1/n}$ we obtain that $(a_1, b_1, c_1)$ belongs to a finite subset of $N^3$ of cardinality at most $C_8$ which is independent of $a, b$ and $c$.

Fix now such a triple $(a_1, b_1, c_1)$. Then it follows from (2) and (9) that

$$a_1\left(\frac{e_1x}{e_3}\right)+b_1\left(\frac{e_2y}{e_3}\right)=c_1 \quad \text{with } \frac{e_1x}{e_3}, \frac{e_2y}{e_3}\in U_S.$$

By Lemma 2, $e_1x/e_3$ and $e_2y/e_3$ and hence their norms

$$\left(\frac{e_1}{e_3}\right)^n N_{K/Q}(x) \quad \text{and} \quad \left(\frac{e_2}{e_3}\right)^n N_{K/Q}(y)$$

can assume at most $C_9$ distinct values. Since

$$\max\{|N_{K/Q}(x)|, |N_{K/Q}(y)|\}\leqslant N,$$

this implies that $e_1/e_3$ and $e_2/e_3$ can assume at most $C_{10}$ distinct values. But $(e_1, e_3)\mid(a, c)$ and $(e_2, e_3)\mid(b, c)$, hence we can proceed in a similar way as above to show that each of the $e_1, e_2, e_3$ can assume at most $C_{11}$ values. Consequently, excluding at most $C_{12}$ triples $(a, b, c)\in N^3$ with relatively prime $a, b, c$, each of the remaining equations (2) has at most two solutions.

If (2) has two solutions with rational components $x, y$ then, by Cramer's rule, we get that $\max(a, b, c)\leqslant C_{13}$. This implies that excluding again at most $C_{14}$ further triples $(a, b, c)\in N^3$ with relatively prime $a, b, c$, each of the remaining equations (2) has at most two solutions, and at most one solution with rational components $x, y$.

Let now $(a, b, c)\in N^3$ be one of the remaining triples, and suppose that for this triple (2) has a solution $(x, y)$. Put $L=Q(x)=Q(y)$ and $l=[L:Q]$. Since the $l$ conjugates of $(x, y)$ are also solutions of (2), hence we have $l\leqslant 2$. Thus $L$ is either the rational field or a quadratic field. Further, it follows that (up to conjugacy) $(x, y)$ is the only solution of (2). If $L$ is $Q$ or a real quadratic field then our proof is completed. It remained the case when $l=2$ and $L$ is an imaginary quadratic field. Denoting by $\bar{x}, \bar{y}$ the complex conjugates of $x, y$, we get from (2) that

$$a(x-\bar{x})=-b(y-\bar{y}).$$

By taking norms of both sides and using the fact that $(a, b) = 1$, we see that $\max(a, b) \leqslant C_{15}$. Then (2) implies that $c \leqslant C_{16}$. Consequently, apart from at most $C_{17}$ further triples $(a, b, c)$, $L$ cannot be imaginary and this completes the proof.

Proof of Theorem 2. Let $a, b$ be given coprime positive integers. The number of non-zero rational integers $x$ with $|x|^n \leqslant N$ is at most $2N^{1/n}$. So there are at most $(2N^{1/n})^2$ rational integers $c$ for which (2) is soluble in rational integers $x, y$. This together with Theorem 1 imply that for all but at most $C_{18}$ rational integers $c$ with $(ab, c) = 1$, equation (2) has the following property. If (2) is solvable and $(x, y)$ is a solution of (2) then, up to conjugacy, this is the only solution and $x, y$ are non-rational integers in a real quadratic subfield, $L$ say, of $K$. We denote by $x', y'$ the conjugates of $x, y$, respectively. Then (2) implies that

$$ax + by = ax' + by',$$

whence

$$1 = x'/x + (b/a)\, y'/x - (b/a)\, y/x.$$

Let $S$ and $U_S$ have the same meaning as in the above proof of Theorem 1. Then $x, x', y, y'$ are $S$-units and $(x'/x, y'/x, y/x)$ is a solution of the equation

$$z_1 + (b/a) z_2 - (b/a) z_3 = 1 \quad \text{in } z_1, z_2, z_3 \in U_S. \tag{10}$$

We show that if $ab > 1$ then $(x'/x, y'/x, y/x)$ is a non-degenerate solution of (10).

The relations

$$(b/a)\, y'/x - (b/a)\, y/x = 0, \quad x'/x = 1$$

cannot hold because $x' \neq x$. If

$$x'/x - (b/a)\, y/x = 0, \quad (b/a)\, y'/x = 1$$

then $by = ax'$. Hence it follows from (2) that $a(x + x') = c$. Since $x + x' \in \boldsymbol{Z}$, this implies that $a|c$ in $\boldsymbol{Z}$. Similarly, $b|c$ in $\boldsymbol{Z}$. But $a, b, c$ are coprime so $a = b = 1$. Finally, if

$$x'/x + (b/a)\, y'/x = 0, \quad -(b/a)\, y/x = 1$$

then $ax + by = 0$ which is impossible by (2). Thus, if $ab > 1$, $(x'/x, y'/x, y/x)$ is indeed a non-degenerate solution of (10). It follows now from Lemma 2 that $x'/x$, $y'/x$ and $y/x$ belong to a finite subset of $K^*$ of cardinality at most $C_{19}$. But $xx' = N_{L/\boldsymbol{Q}}(x) = 1$ or $-1$ and similarly $yy' = 1$ or $-1$. Therefore $x^2, x'^2, y^2, y'^2$ and hence $x, x', y, y'$ also belong to a subset of $K^*$ of cardinality at most $C_{20}$. The integers $a$ and $b$ being fixed, $ax + by$ can assume now at most $C_{21}$ distinct values. Consequently, apart from at most $C_{22}$ further values of $c$ with $(ab, c) = 1$, (2) has no solution if $ab > 1$.



Finally, we consider the case when $a = b = 1$ and $c = x + y$. Since $x, y$ are not rational, $x \neq y$. Further, $y$ must be a conjugate of $x$ since otherwise $(y, x)$ would be a third solution of (2) which is impossible. This completes the proof of the theorem.

**5. Proof of Theorem 4.** To prove Theorem 4 we need several lemmas. We shall keep the notation of the previous sections.

For any algebraic number $\alpha$, we denote by $H(\alpha)$ its (usual) height, that is the maximum of the absolute values of the coefficients of the minimal polynomial of $\alpha$ over $\boldsymbol{Z}$. Notice that

$$H(1/\alpha) = H(\alpha) \quad \text{and} \quad |\overline{\alpha}| \leqslant \deg(\alpha)\, H(\alpha).$$

Further, if $\alpha$ is an algebraic integer then

$$H(\alpha) \leqslant (2|\overline{\alpha}|)^{\deg(\alpha)} \quad \text{and} \quad |\overline{\alpha^{-1}}| \leqslant |\overline{\alpha}|^{\deg(\alpha)-1}.$$

For algebraic numbers $\alpha, \beta$ of degree at most $n$, $H(\alpha+\beta)$ and $H(\alpha\beta)$ do not exceed $\left(\max(2, H(\alpha), H(\beta))\right)^{C_{23}}$ where $C_{23}$ is an effectively computable number which depends only on $n$. For these and other properties of the height we refer to [18].

In what follows, $C_{24}, C_{25}, \ldots$ will denote effectively computable numbers $> 1$ which, unless otherwise stated, depend at most on $n$ and on $|D_K|$. We shall use frequently the fact that the class number $h_K$ of $K$ and the regulator $R_K$ of $K$ can be estimated from above by effectively computable numbers depending only on $n$ and $|D_K|$. This follows from an upper bound for $h_K R_K$ obtained by Siegel [19] and a lower bound for $R_K$ due to Zimmert [23].

Let $\sigma_1, \ldots, \sigma_n$ be the distinct $\boldsymbol{Q}$-isomorphisms of $K$ in $\boldsymbol{C}$, and put $\sigma_i(\alpha) = \alpha^{(i)}$ for $\alpha \in K$. Suppose that there are $r_1$ real conjugate fields to $K$ and $2r_2$ complex conjugates to $K$ and that they are ordered in the usual manner: $\sigma_i(K)$ is real for $i = 1, \ldots, r_1$ and $\sigma_{i+r_2}(K)$ is the complex conjugate of $\sigma_i(K)$ for $i = r_1 + 1, \ldots, r_1 + r_2$.

Lemma 1. *If $r \geqslant 1$, then there exist multiplicatively independent units $\varepsilon_1, \ldots, \varepsilon_r$ in $O_K$ with heights not exceeding $C_{24}$ such that the entries of the inverse of the matrix $\left(\log|\varepsilon_j^{(i)}|\right)_{\substack{1 \leqslant j \leqslant r \\ 1 \leqslant i \leqslant r}}$ have absolute values at most $C_{25}$.*

Proof. See e.g. [10] or [18].

Let $\varepsilon_1, \ldots, \varepsilon_r$ be a fixed system of independent units in $O_K$ with the properties specified in Lemma 1, and denote by $U$ the multiplicative group generated by them.

Lemma 2. *Let $\alpha \in K^*$. Then there exists an $\varepsilon \in U$ such that*

$$|\overline{\varepsilon\alpha}| \leqslant C_{26} |N_{K/\boldsymbol{Q}}(\alpha)|^{1/n}.$$

Proof. See e.g. [10] or [18].

Let $S$ be a set of at most $t$ prime ideals which lie above rational primes not

exceeding $P$ ($\geqslant 2$). Denote by $\mathscr{N}$ the set of $\alpha \in O_K \setminus \{0\}^*$ with $|N_{K/\mathbb{Q}}(\alpha)| \leqslant N$.

LEMMA 3. *Let $\alpha_1, \alpha_2, \alpha_3$ be non-zero elements of $O_K$ with $\max_{1 \leqslant k \leqslant 3} |\overline{\alpha_k}| \leqslant A$ ($A \geqslant 3$). If $x_1, x_2$ and $x_3$ are non-zero elements of $O_K$ satisfying*

$$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 0 \quad \text{and} \quad x_1, x_2, x_3 \in \mathscr{N}(U_S \cap O_K)$$

*then for some $\eta \in U_S \cap O_K$, we have $\eta^{-1} x_k \in O_K$ ($k = 1, 2, 3$) and*

$$\max_{1 \leqslant k \leqslant 3} |\overline{\eta^{-1} x_k}| < \exp\{(C_{27}(t+1)\log P)^{C_{28}(t+1)} P^n \log(AN)\}. \tag{11}$$

Proof. See Lemma 6 in [7]. We note that the proof of this lemma involves the effective theory of linear forms in logarithms and its $p$-adic analogue.

LEMMA 4. *Let $\alpha_1, \alpha_2, \alpha_3$ be as in Lemma 3, and let $a_1, \ldots, a_r, b_1, \ldots, b_r$ be rational integers with*

$$\alpha_1 \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r} + \alpha_2 \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r} = \alpha_3.$$

*Then*

$$\max(|a_1|, \ldots, |a_r|, |b_1|, \ldots, |b_r|) < C_{29} \log A. \tag{12}$$

Remark. Lemma 4 was implicitly proved in [7], in the proof of the above Lemma 3. For convenience of the reader, we deduce here Lemma 4 from Lemmas 3 and 1.

Proof of Lemma 4. Put

$$x_1 = \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}, \quad x_2 = \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r}, \quad x_3 = -1.$$

By applying Lemma 3 with the choice $t = 0$, $P = 2$ we deduce that there is an $\eta \in U_K$ such that (11) holds with $t = 0$, $P = 2$, $N = 1$. But $|\overline{\eta^{-1}}| \leqslant |\overline{\eta}|^{n-1}$, hence it follows from (11) that $\max_{i,k}(|x_k^{(i)}|, 1/|x_k^{(i)}|) \leqslant C_{30} A^{C_{31}}$ whence

$$-C_{32} \log A \leqslant a_1 \log|\varepsilon_1^{(i)}| + \ldots + a_r \log|\varepsilon_r^{(i)}| \leqslant C_{32} \log A \quad \text{for } i = 1, \ldots, n. \tag{13}$$

By Lemma 1, the entries of the inverse of the matrix $(\log|\varepsilon_j^{(i)}|)_{\substack{1 \leqslant j \leqslant r \\ 1 \leqslant i \leqslant r}}$ have absolute values at most $C_{25}$. Thus (13) implies that

$$\max(|a_1|, \ldots, |a_r|) \leqslant C_{33} \log A.$$

A similar upper bound can be derived for $\max(|b_1|, \ldots, |b_r|)$ and (12) follows.

The next lemma is due to Loxton and van der Poorten [14].

LEMMA 5. *Let $\eta_1, \ldots, \eta_s$ be multiplicatively dependent numbers in $K$. Let $w(K)$ denote the number of roots of unity in $K$. Then there are rational integers $m_1, \ldots, m_s$, not all zero, such that*



$$\eta_1^{m_1} \ldots \eta_s^{m_s} = 1$$

*and*

$$|m_j| \leqslant C_{34} w(K) \prod_{i \neq j} \log H(\eta_i) \quad \text{for} \quad j = 1, \ldots, s. \tag{14}$$

Proof. This is in fact Theorem 3 of [14], apart from the fact that in [14] the absolute logarithmic height $h(\eta_i)$ occurs instead of $\log H(\eta_i)$. But

$$C_{35} \log H(\eta_i) \leqslant h(\eta_i) \leqslant C_{36} \log H(\eta_i) \tag{15}$$

(cf. [11], p. 60) hence (14) also holds.

We observe that the roots of unity generate a subfield of degree $\varphi(w(K))$ in $K$ where $\varphi(\,)$ denotes the Euler function. Hence $\varphi(w(K))$ divides $n$, that is

$$w(K) \leqslant C_{37}. \tag{16}$$

Consider the numbers

$$\Lambda_j = \eta_1^{q_{j1}} \ldots \eta_s^{q_{js}} - 1, \quad j = 1, \ldots, l,$$

where $s \geqslant 2$, the $\eta$'s are elements of $K^*$ and the $q$'s are rational integers. We assume that the $\eta$'s are multiplicatively independent, and that the matrix $(q_{ji})$ formed by the $q$'s has rank $l$. Further, we suppose that the height of $\eta_i$ is at most $A_i$ ($\geqslant 4$), and that $q_i$ has absolute value at most $Q$ ($\geqslant 4$). We set

$$\Omega = \log A_1 \ldots \log A_s.$$

The following lemma is an easy consequence of Theorem 4 of Loxton [13] on simultaneous linear forms in logarithms. It will play a crucial rôle in the proof of Theorem 4. We note that the best known effective lower bound for a single linear form in logarithms would not be sharp enough in terms of $\Omega$ to prove our Theorem 4.

LEMMA 6. *Under the above assumption we have*

$$\max_{1 \leqslant j \leqslant l} |\Lambda_j| > \exp\{-C_{38}(\Omega \log \Omega)^{1/l} \log(Q\Omega)\} \tag{17}$$

*where $C_{38}$ is an effectively computable positive number depending only on $s$ and $n$.*

Proof. For a deduction of Lemma 6 from Theorem 4 of [13], see [1]. In [1], the Mahler height $M(\eta_i)$ is used instead of $H(\eta_i)$. However, we have

$$C_{39} \log H(\eta_i) \leqslant \log M(\eta_i) \leqslant C_{40} \log H(\eta_i)$$

(cf. (15) and [11], p. 54), hence (17) holds.

Proof of Theorem 4. Denote by $G$ the normal closure of $K/\mathbb{Q}$, and by $O_G$, $g$ and $D_G$ the ring of integers, the degree and the discriminant of $G$, respectively. At some points of our proof we shall work in $G$. We shall use the inequalities $|D_G| \leqslant |D_K|^g$ (cf. [21], Lemma 7) and $g \leqslant n!$.

Let $(x, y)$ be an arbitrary but fixed solution of (2). If $r_G$, the unit rank of $O_G$ is equal to zero then the assertion easily follows. In this case $\max(a, b) \geqslant c/(2N)$, since otherwise (2) would not have any solution. If now $c > \max\{(4N)^2, e^{27}\}$ then $c/(2N) > c^{1/2}$ and the bound occurring in Theorem 4 is greater than $N$. But $\min(|\overline{x}|, |\overline{y}|) \leqslant N$ hence (4) is proved.

Next we suppose that $r_G \geqslant 1$ when $n \geqslant 2$. Then, from (2) we get

$$ax^{(i)} + by^{(i)} = c \quad \text{for} \quad i = 1, \dots, n. \tag{18}$$

Let $i_0$ be an index for which $|x^{(i_0)}|$ is minimal among the numbers $|x^{(1)}|, \dots, |x^{(n)}|$. We may assume without loss of generality that $|y|$ is minimal among the numbers $|y^{(1)}|, \dots, |y^{(n)}|$. Then it follows from (18) that

$$\left|\frac{ax}{c} - 1\right| = \frac{b|y|}{c} \tag{19}$$

and

$$\left|\frac{by^{(i_0)}}{c} - 1\right| = \frac{a|x^{(i_0)}|}{c}. \tag{20}$$

Let $\{\varepsilon_1, \dots, \varepsilon_{r_G}\}$ be a fixed system of multiplicatively independent units in $O_G$ with the properties specified in Lemma 1. Then, by Lemma 2, there are $\alpha, \beta, x', y' \in O_G$ such that

$$x = \alpha x', \quad y = \beta y' \quad \text{and hence} \quad y^{(i_0)} = \beta^{(i_0)} y'^{(i_0)}, \tag{21}$$

where

$$x' = \varepsilon_1^{a_1} \dots \varepsilon_{r_G}^{a_{r_G}}, \quad y'^{(i_0)} = \varepsilon_1^{b_1} \dots \varepsilon_{r_G}^{b_{r_G}} \tag{22}$$

with appropriate rational integers $a_j, b_j$, and

$$\max(|\alpha|, |\beta|) \leqslant C_{41} N^{1/n}. \tag{23}$$

By (2) we have

$$(a\alpha)x' + (b\beta)y' = c \tag{24}$$

where, by (23), $|a\alpha| \leqslant C_{41} aN^{1/n}$, $|b\beta| \leqslant C_{41} bN^{1/n}$. Then (24) together with (22) and Lemma 4 imply that

$$\max(|a_1|, \dots, |a_{r_G}|) \leqslant C_{42} \log(AN) \tag{25}$$

where $A = \max(a, b, c)$ (which is by assumption equal to $c$). Similarly, by taking the $i_0$th conjugate of (24) and applying again Lemma 4

$$\max(|b_1|, \dots, |b_{r_G}|) \leqslant C_{42} \log(AN) \tag{26}$$

follows.

The numbers $c, \varepsilon_1, \dots, \varepsilon_{r_G}$ and $a$ (if $a > 1$), $b$ (if $b > 1$) are multiplicatively independent. Let $\{\eta_1, \dots, \eta_s\}$ be a maximal subset of multiplicatively independent elements of

$$\mathscr{A} = \{c, \varepsilon_1, \dots, \varepsilon_{r_G}, a, b, \alpha, \beta^{(i_0)}\}$$

which contains $c, \varepsilon_1, \dots, \varepsilon_{r_G}$ and $a$ (if $a > 1$), $b$ (if $b > 1$). Obviously $2 \leqslant s \leqslant r_G + 5 \leqslant n! + 5$. Here, by Lemma 1, $H(\varepsilon_j) \leqslant C_{43}$ for $j = 1, \dots, r_G$ and, by (23), $H(\alpha) \leqslant C_{44} N$ and $H(\beta^{(i_0)}) \leqslant C_{44} N$. Hence we have

$$\Omega := \prod_{j=1}^{s} \log\left(\max(H(\eta_j), 4)\right) \leqslant C_{45} (\log 3N)^2 (\log 3a)(\log 3b)(\log 3c). \tag{27}$$

The elements of $\mathscr{A}$ belong to the field $G$. The set $\mathscr{A} \setminus \{\eta_1, \dots, \eta_s\}$ can contain at most two elements different from 1, namely the elements $\alpha$ and $\beta^{(i_0)}$. If $\alpha \neq 1$ and if it is not contained in $\{\eta_1, \dots, \eta_s\}$ then, by Lemma 5, (16), (23) and (27), there are a positive integer $m$ and rational integers $m_1, \dots, m_s$ which are not all zero, such that

$$\alpha^m = \eta_1^{m_1} \dots \eta_s^{m_s}$$

and

$$\max(m, |m_1|, \dots, |m_s|) \leqslant C_{46} (\log 3N)^3 (\log 3a)(\log 3b)(\log 3c).$$

A similar assertion holds for $\beta^{(i_0)}$ if $\beta^{(i_0)} \neq 1$ and if $\beta^{(i_0)} \notin \{\eta_1, \dots, \eta_s\}$. In view of (21), (22), (25) and (26) it follows now that there is a positive integer $M$ with

$$M < C_{47} (\log 3N)^6 \left((\log 3a)(\log 3b)(\log 3c)\right)^2 \tag{28}$$

such that

$$\left(\frac{ax}{c}\right)^M = \eta_1^{p_1} \dots \eta_s^{p_s}, \quad \left(\frac{by^{(i_0)}}{c}\right)^M = \eta_1^{q_1} \dots \eta_s^{q_s} \tag{29}$$

with some rational integers $p_1, \dots, p_s, q_1, \dots, q_s$ satisfying

$$\begin{aligned} Q &:= \max(|p_1|, \dots, |p_s|, |q_1|, \dots, |q_s|, 4) \\ &\leqslant C_{48} (\log AN)(\log 3N)^6 \left((\log 3a)(\log 3b)(\log 3c)\right)^2. \end{aligned} \tag{30}$$

Put

$$\Lambda_1 = \eta_1^{p_1} \dots \eta_s^{p_s} - 1 \quad \text{and} \quad \Lambda_2 = \eta_1^{q_1} \dots \eta_s^{q_s} - 1.$$

We shall first derive an upper bound for $\max(|\Lambda_1|, |\Lambda_2|)$ in terms of $\max(|x^{(i_0)}|, |y|)$. Then, by using Lemma 6 we shall give a lower bound for $\max(|\Lambda_1|, |\Lambda_2|)$, provided that

$$\operatorname{rank}\begin{pmatrix} p_1 \dots p_s \\ q_1 \dots q_s \end{pmatrix} = 2. \tag{31}$$

Estimate (4) will then follow at once by comparing the lower and upper bounds.

For any complex number $z$, we have

$$|z^M-1| \leqslant M|z-1|\max(|z|^M, 1).$$

Using this together with (29), (19) we obtain that

$$|\Lambda_1| = \left|\left(\frac{ax}{c}\right)^M - 1\right| \leqslant M\left|\frac{ax}{c}-1\right|\max\left(\left|\frac{ax}{c}\right|^M, 1\right) \leqslant M\frac{b|y|}{c}\left(\frac{b|y|}{c}+1\right)^M. \tag{32}$$

We may suppose that

$$\min(|\overline{x}|, |\overline{y}|) > \frac{N(abM)^{n-1}}{c^{n-1}}$$

since otherwise, if $c > C_{49}N$, estimate (4) follows immediately. But we have

$$\prod_{i=1}^{n}|x^{(i)}| = |N_{K/\mathbf{Q}}(x)| \leqslant N \quad \text{and} \quad \prod_{i=1}^{n}|y^{(i)}| = |N_{K/\mathbf{Q}}(y)| \leqslant N. \tag{33}$$

Thus

$$|y| \leqslant \frac{c}{bM}, \quad \text{whence} \quad \frac{b|y|}{c} < \frac{1}{M}.$$

Hence, in view of (28) we deduce from (32) that

$$|\Lambda_1| \leqslant C_{50}\frac{(\log 3N)^6((\log 3a)(\log 3b)(\log 3c))^2}{c}\cdot b|y|.$$

We can estimate from above $|\Lambda_2|$ in a similar manner and we obtain

$$\max(|\Lambda_1|, |\Lambda_2|) \leqslant C_{50}\frac{(\log 3N)^6((\log 3a)(\log 3b)(\log 3c))^2}{c}\max(a|x^{(i_0)}|, b|y|). \tag{34}$$

We are now going to derive a lower bound for $\max(|\Lambda_1|, |\Lambda_2|)$. Assume that (31) holds. Then Lemma 6 together with (27), (30) and $c > C_{49}N$ imply that

$$\max(|\Lambda_1|, |\Lambda_2|) > \exp\{-C_{51}(\Omega\log\Omega)^{1/2}\log(Q\Omega)\} > \exp\{-C_{52}(\log 3N)((\log 3a)(\log 3b)(\log 3c))^{1/2}(\log\log 3c)^{3/2}\}.$$

Comparing now this inequality with (34) we infer that

$$\max(|x^{(i_0)}|, |y|) > c\exp\{-C_{53}(\log 3N)((\log 3a)(\log 3b)(\log 3c))^{1/2}(\log\log 3c)^{3/2}\}. \tag{35}$$



But (33) gives

$$|\overline{x}| \leqslant \frac{N}{|x^{(i_0)}|^{n-1}} \quad \text{and} \quad |\overline{y}| \leqslant \frac{N}{|y|^{n-1}};$$

hence, if $c > \exp\{C_{54}(\log 3N)^7\}$ with a sufficiently large $C_{54}$, (35) implies immediately inequality (4) of Theorem 4.

It remained the case when

$$\operatorname{rank}\begin{pmatrix} p_1 \cdots p_s \\ q_1 \cdots q_s \end{pmatrix} \leqslant 1.$$

In case $c > N$, neither the $p$'s nor the $q$'s can be all zero. Indeed, if $p_j = 0$ for all $j$ then taking norms in (29) $a^n|N_{K/\mathbf{Q}}(x)| = c^n$ follows. But $(a, c) = 1$ hence $c \leqslant |N_{K/\mathbf{Q}}(x)| \leqslant N$. Similarly, if $q_j = 0$ for all $j$ then it follows that $c \leqslant |N_{K/\mathbf{Q}}(y)| \leqslant N$. Assuming that $c > N$, the tuples $(p_1, \ldots, p_s)$ and $(q_1, \ldots, q_s)$ are therefore proportional. Thus, by (29), there exist coprime non-zero rational integers $p$, $q$ such that

$$\left(\frac{ax}{c}\right)^{Mp} = \left(\frac{by^{(i_0)}}{c}\right)^{Mq}. \tag{36}$$

First consider the case when $p$ and $q$ are distinct. We may assume without loss of generality that $p > q$ and that $p > 0$. Next we distinguish two subcases.

If $q < 0$ then (36) implies

$$(ax)^{Mp}(by^{(i_0)})^{M(-q)} = c^{M(p-q)}.$$

By taking norms on both sides with respect to $G/\mathbf{Q}$ and using the transitivity of the norm and the fact that $(ab, c) = 1$ we infer that $a = b = 1$ and that

$$|N_{K/\mathbf{Q}}(x)|^{Mp}|N_{K/\mathbf{Q}}(y)|^{M(-q)} = c^{nM(p-q)}$$

which is impossible if $c > N^{1/n}$.

Suppose now that $q > 0$. Taking norms on both sides of (36) we get

$$|a^n N_{K/\mathbf{Q}}(x)|^{Mp} = |b^n N_{K/\mathbf{Q}}(y)|^{Mq}c^{nM(p-q)}.$$

Since by assumption $a$, $b$ and $c$ are coprime, this implies that any rational prime factor of $b$ and $c$ divides $N_{K/\mathbf{Q}}(x)$ and any rational prime factor of $a$ divides $N_{K/\mathbf{Q}}(y)$ in $\mathbf{Z}$. Consequently, the product of distinct rational prime factors of $abc$ is at most $N^2$. Denote by $t$ the number of distinct prime factors of $abc$, and by $p_1, \ldots, p_t$ the first $t$ prime numbers. Then it follows that $p_1 \ldots p_t \leqslant N^2$. As is known (cf. [17]), we have

$$t\log t < p_t \quad \text{and} \quad \frac{1}{C_{55}}p_t < \sum_{j=1}^{t}\log p_j.$$

Hence

$$t < C_{56}\log 3N/\log\log 3N.$$

We can now apply Lemma 3 to equation (2). Let $S$ be the set of distinct prime ideal divisors of $abc$ in $O_K$. The cardinality of $S$ is at most $nC_{56}\log 3N/\log\log 3N$. Further, these prime ideals lie above rational primes not exceeding $N$. It follows from Lemma 3 that there is an $\eta\in O_K\setminus\{0\}$ with the following properties: If

$$(\eta)=\prod_{\mathfrak{p}\mid\eta}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}\eta} \tag{37}$$

is the prime ideal decomposition of $\eta$ then $\mathfrak{p}\mid abc$ and hence $N(\mathfrak{p})\leqslant N^n$ for each $\mathfrak{p}$. Further, $ax/\eta$, $by/\eta$, $c/\eta$ belong to $O_K$ and

$$\max\left(\left|\overline{\frac{ax}{\eta}}\right|,\left|\overline{\frac{by}{\eta}}\right|,\left|\overline{\frac{c}{\eta}}\right|\right)<\exp\exp\{C_{57}\log N\}. \tag{38}$$

Since $(a, b)=1$, it follows that for any prime ideal factor $\mathfrak{p}$ of $\eta$, $\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}\eta}$ divides $x$ or $y$. Consequently, taking norms we get that $\mathrm{ord}_{\mathfrak{p}}\eta\leqslant\log N$. Thus we infer from (37) that

$$|N_{K/\mathbf{Q}}(\eta)|=\prod_{\mathfrak{p}\mid\eta}N(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}\eta}\leqslant\exp\{C_{58}(\log N)^3\}. \tag{39}$$

Further, by (38) it follows that

$$\frac{c^n}{|N_{K/\mathbf{Q}}(\eta)|}=\left|N_{K/\mathbf{Q}}\left(\frac{c}{\eta}\right)\right|\leqslant\left|\overline{\frac{c}{\eta}}\right|^n\leqslant\exp\exp\{C_{59}\log N\}$$

which together with (39) imply

$$c<\exp\exp\{C_{60}\log N\}.$$

Hence, if

$$c>\exp\{(2N)^{C_{61}}\} \tag{40}$$

with a sufficiently large $C_{61}$ then $p\neq q$ cannot hold.

It remained the case when $p=q=1$. Then, by (36), $(ax)/(by^{(i_0)})$ is a root of unity, say $\zeta$. In view of (21) we have then

$$a\alpha x'=\zeta b\beta^{(i_0)}y'^{(i_0)}. \tag{41}$$

Since, by assumption, $(a, b)=1$ hence we deduce from (41) that $b\mid\alpha$ and $a\mid\beta^{(i_0)}$ in $O_G$. However, this implies that $a\mid\beta$. Hence $b\mid x$, $a\mid y$ and so, by (2), $ab\mid c$ follows. But $(ab, c)=1$, thus $a=b=1$ and, by (41) and (21), $x=\zeta y^{(i_0)}$. Further, it follows from (2) that

$$c=x+y=\zeta y^{(i_0)}+y. \tag{42}$$

We show that $\zeta=1$. We recall that $x^{(i_0)}$ and $y$ are minimal in absolute values among their conjugates. Thus from (33) we get $|x^{(i_0)}|\leqslant N^{1/n}$, $|y|\leqslant N^{1/n}$. Hence, by (42) we have



$$\left|\frac{\zeta y^{(i_0)}}{c}-1\right|=\left|\frac{x}{c}-1\right|\leqslant\frac{N^{1/n}}{c},\qquad\left|\frac{y^{(i_0)}}{c}-1\right|\leqslant\frac{N^{1/n}}{c}.$$

By (35), this implies that

$$\frac{|y^{(i_0)}|}{c}>\frac{1}{2}\quad\text{and}\quad\left|\frac{\zeta y^{(i_0)}-y^{(i_0)}}{c}\right|\leqslant\frac{2N^{1/n}}{c}.$$

It follows now that

$$\tfrac{1}{2}|\zeta-1|<\frac{|y^{(i_0)}|}{c}|\zeta-1|\leqslant\frac{2N^{1/n}}{c}$$

whence

$$|\zeta-1|<\frac{4N^{1/n}}{c}. \tag{43}$$

Denote by $k$ the greatest positive integer for which $\varrho=e^{2\pi i/k}\in G$. For $k=2$ we have $\zeta\in\{1,-1\}$ and, by (43) and (40), $\zeta=1$. Hence we may suppose that $k\geqslant 3$. By (16) we have $k\leqslant C_{62}$. Further, it is easy to verify that

$$2\sin\frac{2\pi}{2k}=|\varrho-1|,\qquad\frac{2\pi}{2k}<\tan\frac{2\pi}{2k}$$

and that

$$\cos\frac{2\pi}{2k}\geqslant\cos\frac{2\pi}{6}=\frac{1}{2}.$$

If now $\zeta\neq 1$ then

$$|\zeta-1|\geqslant|\varrho-1|\geqslant 2\frac{2\pi}{2k}\cos\frac{2\pi}{2k}\geqslant\frac{2\pi}{2k}\geqslant\frac{1}{C_{63}}$$

which contradicts (43) if in (40) $C_{61}$ is large enough. Thus $\zeta=1$ and $x=y^{(i_0)}$.

For large $c$ we have now from (42)

$$y+y^{(i_0)}=c. \tag{44}$$

Denote by $l$ the degree of $y$ over $\mathbf{Q}$. We show that $l$ is even. If $y^{(i_0)}=y$ then (44) gives $c=2y$ and $c^n=2^n|N_{K/\mathbf{Q}}(y)|\leqslant 2^nN$ which is impossible if $c>2N^{1/n}$. Hence, in (44), $y^{(i_0)}\neq y$ and so $l>1$. Suppose that $l=2h+1$ for some positive integer $h$. Consider a conjugate $y^{(i)}$ of $y$ which is different from $y$ and $y^{(i_0)}$. Then taking the $i$th conjugate of (44) we get

$$y^{(i)}+y^{(i_0')}=c$$

for some $i_0'$ where, by (44) and the choice of $y^{(i)}$, $y^{(i_0')}$ differs from $y$, $y^{(i_0)}$ and $y^{(i)}$.

After repeating this argument $h$ times we obtain $h$ conjugates of (44) in which $2h$ distinct conjugates of $y$ will occur. The sum of these $2h$ conjugates is equal to $hc$ which is a rational integer. But the sum of all the conjugates of $y$ is also a rational integer, hence there must exist a conjugate of $y$ which is rational. This is, however, impossible and thus $l$ is even. Since $l$ divides $n$ (the degree of $K$) hence $n$ is also even.

We have shown above that if $c$ is large enough and if $ab > 1$ or $n$ is odd then (36) cannot hold. In this case each solution of (2) satisfies inequality (4) in Theorem 4.

In what follows, we suppose that $a = b = 1$, that $n$ is even and that (40) holds. Assume that (2) has another solution $(u, v)$ which is not conjugate to the solution $(x, y)$. Then neither $u$ nor $v$ is conjugate to $x$ or $y$. We shall show that at least one of the solutions $(x, y)$ and $(u, v)$ satisfies inequality (4) in Theorem 4.

Since each conjugate of $(u, v)$ is also a solution of (2) in $G$, we may choose that conjugate as solution for which $|u^{(i_1)}|$ and $|v|$ are minimal among the absolute values of the conjugates of $u$ and $v$, respectively. Repeating the above argument for $(u, v)$ instead of $(x, y)$ we see that if $u \neq v^{(i_1)}$ then $\min(\overline{|u|}, \overline{|v|})$ is less than the bound occurring in (4) and the proof is completed. Hence it suffices to deal with the case when

$$x = y^{(i_0)}, \quad u = v^{(i_1)}.$$

We shall now repeat some part of the above arguments for $x$ and $u$ instead of $x$ and $y$. We can see in the same way as above that

$$\left|\frac{u}{c} - 1\right| = \frac{|v|}{c}$$

and that

$$u = \vartheta \varepsilon_1^{d_1} \dots \varepsilon_{r_G}^{d_{r_G}}$$

with some rational integers $d_1, \dots, d_{r_G}$ satisfying

$$\max(|d_1|, \dots, |d_{r_G}|) \leqslant C_{64} \log(AN)$$

and with some non-zero $\vartheta \in O_G$ for which $\overline{|\vartheta|} \leqslant C_{65} N^{1/n}$. Let now $\{\eta'_1, \dots, \eta'_t\}$ be a maximal subset of multiplicatively independent elements of

$$\mathscr{A}' = \{c, \varepsilon_1, \dots, \varepsilon_{r_G}, \alpha, \vartheta\}$$

which contains $c, \varepsilon_1, \dots, \varepsilon_{r_G}$. Then we have $2 \leqslant t \leqslant n! + 3$. We can define $\Omega$ in the same way as in (27) and inequality (27) follows for the $\eta$'s. Further, we can see that there is a positive integer $M'$ which is less than the bound occurring in (28), such that

$$\left(\frac{x}{c}\right)^{M'} = \eta_1'^{p'_1} \dots \eta_t'^{p'_t}, \quad \left(\frac{u}{c}\right)^{M'} = \eta_1'^{q'_1} \dots \eta_t'^{q'_t} \tag{45}$$



with some rational integers $p'_1, \dots, p'_t, q'_1, \dots, q'_t$ for which

$$Q' := \max(|p'_1|, \dots, |p'_t|, |q'_1|, \dots, |q'_t|, 4) \leqslant C_{66} (\log AN)(\log 3N)^6 (\log 3c)^2.$$

By (40), neither the $p'_j$ nor the $q'_j$ can be all zero. Put

$$\Lambda'_1 = \eta_1'^{p'_1} \dots \eta_t'^{p'_t} - 1 \quad \text{and} \quad \Lambda'_2 = \eta_1'^{q'_1} \dots \eta_t'^{q'_t} - 1.$$

We may suppose that both $\overline{|y|}$ and $\overline{|v|}$ are greater than $N(M')^{n-1}/c^{n-1}$ since otherwise estimate (4) of Theorem 4 immediately follows for the solution $(x, y)$ or $(u, v)$. Following again the above argument we get

$$\max(|\Lambda'_1|, |\Lambda'_2|) \leqslant C_{67} \frac{(\log 3N)^6 (\log 3c)^2}{c} \max(|y|, |v|).$$

Further, if

$$\operatorname{rank} \begin{pmatrix} p'_1 & \dots & p'_t \\ q'_1 & \dots & q'_t \end{pmatrix} = 2,$$

then

$$\max(|\Lambda'_1|, |\Lambda'_2|) > \exp\{-C_{68} (\log 3N)(\log 3c)^{1/2} (\log\log 3c)^{3/2}\}$$

follows. Now comparing the upper bound with the lower bound we obtain for $\min(\overline{|y|}, \overline{|v|})$ the upper bound occurring in (4) and the assertion follows.

Finally, consider the case when

$$\operatorname{rank} \begin{pmatrix} p'_1 & \dots & p'_t \\ q'_1 & \dots & q'_t \end{pmatrix} = 1.$$

Then there are coprime non-zero rational integers $p'$, $q'$ such that $p' > 0$ and that

$$\left(\frac{x}{c}\right)^{M'p'} = \left(\frac{u}{c}\right)^{M'q'}. \tag{46}$$

If $q' < 0$ then (46) gives

$$x^{M'p'} u^{-M'q'} = c^{M'(p'-q')}.$$

But taking norms we see that this contradicts (40). Hence $q' > 0$. Taking norms again on both sides of (46) we get

$$|N_{K/\mathbf{Q}}(x)|^{M'p'} = |N_{K/\mathbf{Q}}(u)|^{M'q'} c^{nM'(p'-q')}.$$

This shows that any rational prime factor $p$ of $c$ divides $N_{K/\mathbf{Q}}(x)$ in $\mathbf{Z}$ and hence $p \leqslant N$. But then Lemma 3 can be applied to equation (2) in the same way as we did before and we arrive at a contradiction with (40) for sufficiently large $C_{61}$. This completes the proof of Theorem 4.

## References


[1] B. Brindza, *On Thue's equations*, in preparation.
[2] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. 53 (1984), 225–244.
[3] — *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.
[4] J.-H. Evertse and K. Győry, *On the numbers of solutions of weighted unit equations*, Compositio Math. 66 (1988), 329–354.
[5] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *On S-unit equations in two unknowns*, Invent. Math. 92 (1988), 461–477.
[6] — — — — *S-unit equations and their applications*, in *New Advances in Transcendence Theory*, Cambridge, 1980, pp. 110–174.
[7] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. 54 (1979), 583–600.
[8] — *On the solutions of linear diophantine equations in algebraic integers of bounded norm*, Ann. Univ. Budapest. Eötvös, Sect. Math. 22–23 (1979–80), 225–233.
[9] — *On certain graphs composed of algebraic integers of a number field and their applications I*, Publ. Math. Debrecen 27 (1980), 229–242.
[10] — *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Applied Math., No. 56, Kingston, Canada, 1980.
[11] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, 1983.
[12] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, Lecture Notes in Math., 1380, 1989, pp. 150–178.
[13] J. H. Loxton, *Some problems involving powers of integers*, Acta Arith. 46 (1986), 113–123.
[14] J. H. Loxton and A. J. van der Poorten, *Multiplicative dependence in number fields*, ibid. 42 (1983), 291–302.
[15] T. Nagell, *Quelques problèmes relatifs aux unités algébriques*, Arkiv för Mat. 8 (1969), 115–127.
[16] A. J. van der Poorten and H. P. Schlickewei, *The growth conditions for recurrence sequences*, Macquarie Univ. Math. Rep. 82–0041, North Ryde, Australia, 1982.
[17] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
[18] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge 1986.
[19] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II, 71–86, 1969.
[20] V. G. Sprindžuk, *Classical diophantine equations in two unknowns* (Russian), Nauka, Moskva 1982.
[21] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.
[22] J. S. Sunley, *Class numbers of totally imaginary quadratic extensions of totally real fields*, Trans. Amer. Math. Soc. 175 (1973), 209–232.
[23] R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. 62 (1981), 367–380.



SCHOOL OF MATHEMATICS AND PHYSICS
MACQUARIE UNIVERSITY
North Ryde, N.S.W., 2113, Australia

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 Debrecen, Hungary


*Received on 13.9.1988* (1867)

ACTA ARITHMETICA
LIII (1990)

# Über eine Klasse von gleichverteilten Folgen

von

EDMUND HLAWKA (Wien)

*Dem Andenken an V. G. Sprindžuk gewidmet*

Es seien $p_1, \dots, p_s$ verschiedene ganzrationale Primzahlen von der Gestalt $4k+1$. Jede dieser Primzahlen besitzt im Gaußschen Zahlring $Z[i]$ die Zerlegung in Primzahlen

$$p_j = \pi_j \bar{\pi}_j \tag{1}$$

wobei $\pi_j$, $\bar{\pi}_j$ Primzahlen in $Z[i]$ sind, dabei ist noch $\bar{\pi}_j$ nicht zu $\pi_j$ assoziiert, d.h. es ist $\pi_j$ zu $\bar{\pi}_j$ teilerfremd. Es ist nun für $j = 1, \dots, s$

$$\frac{\pi_j}{|\pi_j|} = e(\varphi_j) \tag{2}$$

wobei $e(\alpha) = e^{i\alpha}$ sein soll. Wir setzen noch

$$\varphi_j = 2\pi\psi_j \tag{3}$$

und betrachten die Folgen

$$\varphi = (\varphi_1, \dots, \varphi_s), \tag{4}$$

bzw.

$$\psi = (\psi_1, \dots, \psi_s) \tag{5}$$

und fassen sie als Koordinaten des Punkte $\varphi$ bzw. $\psi$ in $R^s$ auf.

**1.** Wir behaupten nun

SATZ 1. *Es sind $\psi_1, \dots, \psi_s$ über $Z$ linear unabhängig: Sind $h_1, h_2, \dots, h_{s+1}$ ganze Zahlen, so daß*

$$h_1\psi_1 + \dots + h_s\psi_s + h_{s+1} = 0 \tag{6}$$

*so folgt*

$$h_1 = h_2 = \dots = h_{s+1} = 0.$$