Invent. math. 75, 561–584 (1984)

Inventiones mathematicae
© Springer-Verlag 1984

On equations in S-units and the Thue-Mahler equation

J.-H. Evertse

University of Leiden, Department of Mathematics and Computer Science,
Wassenaarseweg 80, Postbus 9512, NL-2300 RA Leiden, The Netherlands

§ 1. Introduction

Several classes of diophantine equations, such as the Thue-Mahler equation and certain generalisations of the Ramanujan-Nagell equation, can be reduced to certain linear equations in two S-units. Here S is a finite set of equivalence classes of valuations on a given algebraic number field K and an S-unit is an element $\alpha \in K$ with the property that the only valuations on K which assume a value $\neq 1$ for α belong to equivalence classes from S. In this section we shall state a general result on the number of solutions of linear equations in two S-units. Before we can state it, we have to introduce some notions on valuations. In § 2 we shall discuss the consequences of our general result for generalisations of the Ramanujan-Nagell equation and in §§ 3–4 we shall deal with the Thue-Mahler equation.

Let K be an algebraic number field. By a *prime* on K we shall mean an equivalence class of non-trivial valuations on K. Usually we shall denote primes on $\mathbb{Q}$ by the letter p, on a given algebraic number field K by v and on an extension of K by V. The completion of K at the prime v is denoted by K_v. We distinguish between *finite primes*, containing non-archimedean valuations, and *infinite primes*, containing archimedean valuations. Furthermore, an infinite prime is called *real* if $K_v = \mathbb{R}$ and *complex* if $K_v = \mathbb{C}$. Finally, the set of primes on K is denoted by M_K.

Let L be a finite extension of K and let v, V be primes on K, L respectively. If all valuations in V are continuations of the valuations in v to L we say that V *lies above* v. Then L_V is a finite extension of K_v and we have

$$\sum_{V|v} [L_V : K_v] = [L : K]. \tag{1}$$

(Here $\sum_{V|v}$ means that the sum is taken over all $V \in M_L$ lying above v. $\prod_{V|v}$ has a similar meaning.) As a consequence, there are at most $[L:K]$ primes on L lying above v.

On $\mathbb{Q}$ we have only one infinite prime, p_∞, which is represented by the ordinary absolute value. There exists a one-to-one correspondence between finite primes on $\mathbb{Q}$ and the prime numbers. We shall not make a clear distinction between prime numbers and finite primes and the finite prime corresponding to the prime number p is also denoted by p. If p is a prime on $\mathbb{Q}$ we define $|.|_p$ to be the absolute value on $\mathbb{Q}$ if $p=p_\infty$ and the ordinary p-adic valuation if p is a prime number.

Let v be a prime on the algebraic number field K. Then it lies above a prime p on $\mathbb{Q}$. In v we choose a valuation $|.|_v$ such that

$$|\alpha|_v=|\alpha|_p^{[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]} \qquad \text{for } \alpha\in\mathbb{Q}. \tag{2}$$

By our choice of the valuations we have the so-called *product formula*

$$\prod_{v\in M_K} |\alpha|_v=1 \qquad \text{for } \alpha\in K\setminus\{0\}. \tag{3}$$

As is well-known, there is a one-to-one correspondence between finite primes and prime ideals on K and similarly to $\mathbb{Q}$, we shall not make a clear distinction between them.

Let S be a finite set of primes on K, containing the infinite primes. An element α of K is called an *S-unit* if

$$|\alpha|_v=1 \qquad \text{for } v\notin S. \tag{4}$$

Our general result is as follows:

Theorem 1. *Let K be an algebraic number field of degree m, let λ, μ be non-zero elements of K and let S be a finite set of primes on K of cardinality s containing the infinite primes. Then the equation*

$$\lambda x+\mu y=1 \qquad \text{in } S\text{-units } x, y \tag{5}$$

has at most

$$3\times 7^{m+2s}$$

solutions.

The proof of Theorem 1 is based on an approximation result (cf. §7, Lemma 8), dealing with the approximation of cube roots of unity by numbers from a fixed algebraic number field. This approximation result is derived by applying a modification of a method of Thue and Siegel, in which hypergeometric functions are used [20, 25]. Very recently, J. Silverman [23] showed independently, but by a different method, that (5) has at most $C\times 2^{20s}$ solutions in case that $\lambda=\mu=1$. Here C is some absolute constant.

In 1961, Lewis and Mahler [11] proved that the equation

$$p_{11}^{x_{11}}\dots p_{1r}^{x_{1r}}+p_{21}^{x_{21}}\dots p_{2s}^{x_{2s}}=p_{31}^{x_{31}}\dots p_{3t}^{x_{3t}} \qquad \text{in } x_{11},\dots,x_{3t}\in\mathbb{N}\cup\{0\} \tag{6}$$

has at most

$$\left(c_1(r+s)\frac{\log Q}{\log P}\right)^{r+s}+c_2^{r+s+t+1}$$

solutions, where $p_{11}, \ldots, p_{3t}$ are prime numbers of which the smallest is P and the largest is Q and where c_1, c_2 are solute constants. The disadvantage of this bound is that it depends on $p_{11}, \ldots, p_{3t}$. It follows easily from theorem 1 that the number of solutions of (6) can be estimated from above in terms of r, s, t only.

Corollary 1. (6) *has at most* $3 \times 7^{2(r+s+t)+3}$ *solutions.*

We mention that in certain special cases, Theorem 1 can be essentially improved. For instance, Györy [10] proved the following:

let β be an algebraic integer such that $\beta\lambda := \alpha_1$, $\beta\mu := \alpha_2$ are algebraic integers. Let S be a finite set of primes on K consisting of all infinite primes (of which the number equals r) and t finite primes. Suppose the finite primes of S ly above prime numbers of which the largest equals P. Let ε be a real number with $0 < \varepsilon \leqq 1$. Put

$$M_i := \prod_{v \in S} |\alpha_i|_v \quad \text{for } i = 1, 2, \qquad M := \prod_{v \in S} |\beta|_v. \tag{7}$$

If $\min_i M_i \leqq M^{1-\varepsilon}$ *and* $\log M > C$, *where C is an effectively computable constant depending on ε, P, K, t only, then* (5) *has at most* $r + 4t$ *solutions.*

Györy gives an explicit, but very complicated expression for C. The reader is warned, that Györy uses valuations $\|\cdot\|_v$ which are exactly the m-th powers of our valuations $|\cdot|_v$.

As we already mentioned, § 2 will be devoted to a generalisation of the Ramanujan-Nagell equation. In §§ 3–4 we shall deal with the Thue-Mahler equation. In § 5 we shall give some properties of height functions and in §§ 6–8 we shall prove Theorem 1.

§ 2. A generalisation of the Ramanujan-Nagell equation

In his collected works ([19], p. 327, question 464), Ramanujan poses the following question: $2^n - 7$ *is a perfect square for the values* 3, 4, 5, 7, 15 *of* n. *Find other values.* In 1948, Nagell [17] showed, that other values for n do not exist. Beukers [1–3] generalised this in the following way: *let D be an integer with $D \neq 0$ and let p be a prime number which does not divide D. Then the equation*

$$x^2 + D = p^n \quad \text{in } x, n \in \mathbb{N} \tag{8}$$

has at most five *solutions.*

We shall give a further generalisation of Beukers' result. Let K be an algebraic number field. The ring of integers of K is denoted by $\mathcal{O}_K$ and the ideal (i.e. finitely generated $\mathcal{O}_K$-module) generated by $\alpha_1, \ldots, \alpha_r$ is denoted by $\langle \alpha_1, \ldots, \alpha_r \rangle$. We have the following result:

Theorem 2. *Let K be an algebraic number field of degree m with r infinite primes, let $f(X) \in \mathcal{O}_K[X]$ be a quadratic polynomial of non-zero discriminant and* *let* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ *be a (possibly empty) set of distinct prime ideals. Then the equation*

$$\langle f(x)\rangle = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\mathfrak{p}_t^{k_t} \quad \text{in } x\in\mathcal{O}_K, k_1, k_2, \ldots, k_t\in\mathbb{Z} \tag{9}$$

has at most

$$3\times 7^{2m+4r+4t}$$

solutions.

It follows that for every non-zero rational integer D and for every set of prime numbers $\{p_1, \ldots, p_t\}$ the equation

$$x^2+D=p_1^{k_1}\ldots p_t^{k_t} \tag{10}$$

has at most $3\times 7^{4t+6}$ solutions. In case that $t=1$ this is weaker than Beukers' result, but our bound also has the property that it does not depend on D and the prime number involved.

We shall now prove Theorem 2 under assumption of Theorem 1. We have

$$f(X)=\beta(X-\alpha)(X-\tilde{\alpha}), \tag{11}$$

where $\beta\in\mathcal{O}_K$ and where $\alpha, \tilde{\alpha}$ are distinct numbers, being algebraic over K. Put $L=K(\alpha)$ and let S be the set of primes on L lying above the infinite primes on K and $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Then

$$[L:\mathbb{Q}]\leqq 2\text{m}, \quad \#(S)\leqq 2(r+t). \tag{12}$$

There are integral ideals $a, \tilde{a}$ such that $a\langle\alpha\rangle, \tilde{a}\langle\tilde{\alpha}\rangle$ are integral ideals in L and $\beta\in a\tilde{a}$. Solutions of (9) are shortly denoted by x. If x is a solution of (9), then the ideals $a<x-\alpha\rangle, \tilde{a}\langle x-\tilde{\alpha}\rangle$ are integral and solely composed of prime ideals in S. Assume that (9) is solvable and let x_0 be a fixed solution of (9). Then we have for every other solution x of (9) that $(x-\alpha)/(x_0-\alpha)$, $(x-\tilde{\alpha})/(x_0-\alpha)$ are S-units. Moreover, by a straightforward computation,

$$\frac{x_0-\alpha}{\tilde{\alpha}-\alpha}\,\frac{x-\alpha}{x_0-\alpha}-\frac{x_0-\tilde{\alpha}}{\tilde{\alpha}-\alpha}\,\frac{x-\tilde{\alpha}}{x_0-\tilde{\alpha}}=1. \tag{13}$$

Note that x is completely determined by the pair $((x-\alpha)/(x_0-\alpha), (x-\alpha)/(x_0-\tilde{\alpha}))$. Hence by (13), (12) and Theorem 1, Eq. (9) has at most

$$3\times 7^{[L:\mathbb{Q}]+2\#(S)}\leqq 3\times 7^{2m+4r+4t}$$

solutions. □

§ 3. The Thue-Mahler equation

Let K be an algebraic number field, let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a (possibly empty) set of prime ideals in K and let F be a binary form of degree $\geqq 3$ with coefficients in

$\mathcal{O}_K$. We shall deal with the *generalised Thue-Mahler equation*

$$\langle F(x, y)\rangle = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_t^{k_t} \quad \text{in } x, y \in \mathcal{O}_K, \; k_1, \ldots, k_t \in \mathbb{Z}. \tag{14}$$

If (14) is solvable and if $t > 0$ or K is not equal to $\mathbb{Q}$ or an imaginary quadratic field, then it has infinitely many solutions. For if $(x, y, k_1, \ldots, k_t)$ is a solution of (14) then infinitely many other solutions can be found by multiplying x, y with the same S-unit in $\mathcal{O}_K$, where S consists of the infinite primes on K and of $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. It therefore makes sense, to identify solutions of (14) which have the same ratio $x : y$. Every point on the projective line $\mathbb{P}^1(K)$ can be given by homogeneous coordinates $(x : y)$, which are determined up to a multiplicative constant. We call $(x : y)$ a *projective solution* of (14) if x, y can be chosen such that $x, y \in \mathcal{O}_K$ and (14) holds for certain rational integers $k_1, \ldots, k_t$.

Theorem 3. *Let K be an algebraic number field of degree m with r infinite primes, let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a (possibly empty) set of distinct prime ideals, and let $F(X, Y) \in \mathcal{O}_K[X, Y]$ be a binary form of degree $n \geqq 3$ which is divisible by at least three pairwise linearly independent linear forms in some extension of K. Then* (14) *has at most*

$$7^{n^3(m + 2r + 2t)}$$

projective solutions.

Corollary 2. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geqq 3$ which is divisible by at least three pairwise linearly independent linear forms in some algebraic number field and let $\{p_1, \ldots, p_t\}$ be a (possibly empty) set of distinct prime numbers. Then the equation*

$$|F(x, y)| = p_1^{k_1} \ldots p_t^{k_t} \quad \textit{in } x, y, k_1, \ldots, k_t \in \mathbb{Z} \quad \textit{with} \quad (x, y) = 1 \tag{15}$$

has at most

$$2 \times 7^{n^3(2t + 3)}$$

solutions.

Corollary 2 follows from Theorem 3 by observing that there are exactly two pairs of rational integers (x, y) with $(x, y) = 1$ corresponding to the same projective point $(x : y) \in \mathbb{P}^1(\mathbb{Q})$.

The upper bounds in Theorem 3 and Corollary 2 have the remarkable property that they do not depend on the coefficients of F or the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, the prime numbers $p_1, \ldots, p_t$ respectively. Already in 1933, Mahler [12, 13] gave an upper bound for the number of solutions of (15) depending on F and t only in case that F is irreducible. In 1961, Lewis and Mahler [11] derived the more explicit bound

$$c_1 (an)^{c_2 \sqrt{n}} + (c_3 n)^{t+1}$$

in case that F has non-zero discriminant, that $F(1, 0) F(0, 1) \neq 0$ and that F has integral coefficients with absolute values not exceeding a. Here c_1, c_2, c_3 are absolute constants. For large values of n, the bound of Lewis and Mahler is better than ours, but it has the disadvantage of being dependent on the coefficients of F.

Our Theorem 3 is a more explicit version of a result of Parry [18]. In fact, he showed the following:

let K be an algebraic number field of discriminant D_K, let $F(X, Y) \in \mathcal{O}_K[X, Y]$ be a binary form of degree $n \geqq 3$ and non-zero discriminant and let $\{p_1, \ldots, p_t\}$ be a (possibly empty) set of distinct prime numbers. Call two solutions $(x', y', k'_1, \ldots, k'_t)$, $(x'', y'', k''_1, \ldots, k''_t)$ of the equation

$$|N_{K/\mathbb{Q}}(F(x, y))| = p_1^{k_1} \ldots p_t^{k_t} \quad \text{in } x, y \in \mathcal{O}_K,\ k_1, \ldots, k_t \in \mathbb{Z} \tag{16}$$

associated if $x'' = \varepsilon x'$, $y'' = \varepsilon y'$ for some unit ε in $\mathcal{O}_K$. Then (16) has at most c^{t+1} pairwise non-associated solutions for which the norm of the ideal $\langle x, y \rangle$ does not exceed $|D_K|^{1/2}$. Here c is a positive constant depending on F and K only.

As a consequence of Theorem 3 we can choose c such that c depends on n and K only. For the sake of completeness, we mention that in Chap. 6 of [8] we derived an upper bound for the number of projective solutions of (14) which is sharper for large values of t than the one derived in Theorem 3, namely

$$7^{15\left(\binom{n}{3}m+1\right)^2} + 6 \times 7^{2\binom{n}{3}(r+t)}.$$

We shall prove Theorem 3 by applying Theorem 1 to a certain equation of S-units.

It is also possible to derive upper bounds for the number of solutions of the Thue equation

$$F(x, y) = \gamma \quad \text{in } x, y \in \mathcal{O}_K, \tag{17}$$

where $\gamma \in \mathcal{O}_K \backslash \{0\}$ and F is as in Theorem 3. For every projective point $P \in \mathbb{P}^1(K)$ there are at most n solutions (x, y) of (17) with $(x : y) = P$. For if (x_1, y_1), (x_2, y_2) are solutions of (17) with $(x_1 : y_1) = (x_2 : y_2)$ then $x_2 = \delta x_1$, $y_2 = \delta y_1$ for some $\delta \in K$, hence

$$\gamma = F(x_2, y_2) = \delta^n F(x_1, y_1) = \delta^n \gamma,$$

i.e. $\delta^n = 1$. This implies the following

Corollary 3. (17) *has at most $n \times 7^{n^3(m+2r+2t)}$ solutions, where m, r are the degree and the number of infinite primes of K respectively and where t is the number of distinct prime ideals dividing $\langle \gamma \rangle$.*

The bound in Corollary 3 depends on n, m, r, t only. Already in 1974, Choodnovsky [4] claimed that such an upper bound exists for the number of solutions of (17), but as far as I know, he never published a proof of his claim.

Very recently, Faltings [9] proved the conjecture of Mordell, which states that if $G(X, Y)$ is a polynomial with algebraic coefficients such that the curve $C: G(X, Y) = 0$ has genus $\geqq 2$, then C contains at most finitely many points (x, y) with x, y belonging to the algebraic number field K. As a consequence, (17) has at most finitely many solutions in $x, y \in K$ if F has non-zero discriminant and degree $n \geqq 4$.

Now suppose that F is an irreducible binary form of degree $n \geqq 3$ with coefficients in $\mathbb{Z}$. From Corollary 3 it follows that the equation

$$F(x, y) = 1 \quad \text{in } x, y \in \mathbb{Z} \tag{18}$$

has at most $n \times 7^{3n^3}$ solutions. For $n=3$ much better results are known. Delone [5] and Nagell [16] independently proved that (18) has at most *five* solutions if $n=3$ and F has negative discriminant and the author [7] proved that the number of solutions of (18) is at most *twelve* in case that $n=3$ and F has positive discriminant. In 1969, Tartakovskii [24] stated without proof that (18) has at most $235n^6$ solutions if $n \geqq 4$.

We now deal with the Thue equation

$$F(x, y)=c \quad \text{in } x, y \in \mathbb{Z} \quad \text{with} \quad (x, c)=(y, c)=(x, y)=1, \ y \neq 0, \tag{19}$$

where F is as in (18) and where c is a non-zero integer. We call two solutions (x_1, y_1), (x_2, y_2) of (19) *congruent* $\bmod c$ if $x_1 y_2 - x_2 y_1 \equiv 0 (\bmod c)$. Then the number of congruence classes of solutions of (19) is at most equal to the number of congruence classes $U (\bmod c)$ satisfying

$$F(U, 1) \equiv 0 (\bmod c). \tag{20}$$

In order to estimate the number of solutions of (19) in a fixed congruence class, we apply a reduction method of Lagrange (cf. [15], Chap. 18). Let (x_0, y_0) be a solution in a given congruence class. For every other solution (x, y) in the same class, put $X = kx - ly$, $Y = (-y_0 x + x_0 y)/c$, where k, l are fixed rational integers with $kx_0 - ly_0 = 1$. Then X, Y are rational integers. Put

$$G(X, Y) = c^{-1} F(x_0 X + lcY, y_0 X + kcY).$$

Since $G(1, 0) = F(x_0, y_0)/c = 1$, G has integral coefficients and

$$G(X, Y) = c^{-1} F(x, y) = 1.$$

In view of the upper bound for the number of solutions of (18) this proves the following

Corollary 4. *Let* $v(c)$ *be the number of congruence classes* $U (\bmod c)$ *with* $F(U, 1) \equiv 0 (\bmod c)$. *Then* (19) *has at most*

$$n \times 7^{3n^3} v(c)$$

solutions.

Very recently, Mahler [14] showed, that this can be improved to $32nv(c)$ if

$$|c| \geqq (450 n^4 a^4)^{n/(n-2)},$$

where a is the maximum of the absolute values of the coefficients of F.

§ 4. Proof of Theorem 3

In this section we shall derive Theorem 3 from Theorem 1. The same notations are used as in §§ 1-3. Thus K is an algebraic number field of degree m with r infinite primes, F is a binary form of degree $n \geqq 3$ with coefficients in $\mathcal{O}_K$ which is divisible by at least three pairwise linearly independent linear forms in some extension of K and $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a (possibly empty) set of distinct prime ideals. We have to show, that the number of projective solutions of the equation

$$\langle F(x, y)\rangle = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_t^{k_t} \quad \text{in } x, y \in \mathcal{O}_K,\ k_1, \ldots, k_t \in \mathbb{Z} \tag{14}$$

is at most

$$7^{n^3(m+2r+2t)}.$$

The first step is to show that it suffices to prove this in case that $F(1,0)=1$. Suppose that (14) is solvable. Let $(x_0, y_0, \ldots)$ be a solution of (14) and put $F(x_0, y_0)=\varepsilon$. Let δ be a generator of the principal ideal $\langle x_0, y_0\rangle^h$, where h is the class number of K. Then $\langle\delta\rangle$ is solely composed of prime ideals from $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ and since $\delta \in \langle x_0, y_0\rangle$ there are $\alpha, \beta \in \mathcal{O}_K$ such that $\beta y_0 - \alpha x_0 = \delta$. Put

$$G(x, y) = F(x_0 x - \beta y, y_0 x - \alpha y), \qquad H(x, y) = \varepsilon^{n-1} G(\varepsilon^{-1} x, y).$$

Then $G(x, y)$ has coefficients in $\mathcal{O}_K$ and since $G(1,0)=\varepsilon$, $H(x, y)$ also has. Moreover, $H(1,0)=1$. It is easy to check, that the mapping

$$(x : y) \mapsto (\varepsilon(-\alpha x + \beta y) : -y_0 x + x_0 y)$$

defines an injection of the set of projective solutions of (14) into the set of projective solutions of the equation

$$\langle H(x, y)\rangle = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_t^{k_t} \quad \text{in } x, y \in \mathcal{O}_K,\ k_1, \ldots, k_t \in \mathbb{Z}.$$

(In fact we have a bijection here but since we do not need this, the proof of this fact is left to the reader). This shows indeed that it suffices to prove Theorem 3 in case that $F(1,0)=1$.

From now on we assume that $F(1,0)=1$, i.e.

$$F(x, y) = (x - \alpha_1 y)(x - \alpha_2 y) \ldots (x - \alpha_n y), \tag{21}$$

where $\alpha_1, \ldots, \alpha_n$ are algebraic integers in some extension of K among which are three distinct numbers, $\alpha_1, \alpha_2, \alpha_3$ say. Put $L = K(\alpha_1, \alpha_2, \alpha_3)$ and let S be the set of primes on L which $1y$ above the infinite primes on K and $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Then

$$d := [L : \mathbb{Q}] \leqq mn(n-1)(n-2), \qquad s := \#(S) \leqq n(n-1)(n-2)(r+t). \tag{22}$$

Put

$$\Lambda = \frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha_3}, \qquad M = \frac{\alpha_2 - \alpha_3}{\alpha_1 - \alpha_3}$$

and define for every projective solution $(x : y)$ of (14)

$$X = \frac{x - \alpha_3 y}{x - \alpha_2 y}, \qquad Y = \frac{x - \alpha_1 y}{x - \alpha_2 y}.$$

Then X, Y do not depend on the choice of the homogeneous coordinates $(x : y)$. Moreover, the projective point $(x : y)$ is completely determined by X, Y. Note that X, Y are S-units in view of (21) and that, by an easy computation,

$$(23) \qquad \Lambda X + M Y = 1.$$

Together with Theorem 1 and (22) this implies that the number of projective solutions of (14) is at most

$$3 \times 7^{d+2s} \leqq 3 \times 7^{n(n-1)(n-2)(m+2r+2t)} \leqq 7^{n^3(m+2r+2t)}. \quad \square$$

§ 5. Some properties of height functions

Let K be an algebraic number field of degree m and let M_K be the set of primes on K. The *absolute height* of $\alpha \in K \backslash \{0\}$ is defined by

$$h(\alpha) = \prod_{v \in M_K} \max(1, |\alpha|_v). \tag{24}$$

It is easy to check that $h(\alpha)$ depends on α but does not depend on K. For let $k = \mathbb{Q}(\alpha)$. If v is a prime on K lying above the prime w on k then, by the definition of our valuations in § 1,

$$|\alpha|_v = |\alpha|_w^{[K_v:k_w]/[K:k]}. \tag{25}$$

Hence by (1), if $\prod_{v|w}$ denotes the product taken over all $v \in M_K$ lying above w,

$$\begin{aligned}\prod_{w \in M_k} \max(1, |\alpha|_w) &= \prod_{w \in M_k} \prod_{v|w} \max(1, |\alpha|_w^{[K_v:k_w]/[K:k]}) \\ &= \prod_{v \in M_K} \max(1, |\alpha|_v).\end{aligned}$$

By the product formula we have for $\xi, \eta \in K \backslash \{0\}$,

$$h(\xi/\eta) = \prod_{v \in M_K} \max(|\xi|_v, |\eta|_v) \tag{26}$$

and hence

$$h(\alpha) = h(\alpha^{-1}) \quad \text{for } \alpha \in K \backslash \{0\}. \tag{27}$$

It is easy to check that, more generally,

$$h(\alpha^n) = h(\alpha)^{|n|} \quad \text{for } \alpha \in K \backslash \{0\}, \quad n \in \mathbb{Z}. \tag{28}$$

This implies that roots of unity have absolute height equal to 1. If α is not a root of unity, then $h(\alpha) > 1$.

In the sequel we shall use the notations below. Put

$$\begin{aligned} s(v) &= 1/m && \text{if } v \text{ is a real prime,} \\ &= 2/m && \text{if } v \text{ is a complex prime,} \\ &= 0 && \text{if } v \text{ is a finite prime.} \end{aligned}$$

Then

$$\sum_{v \in S} s(v) = 1 \quad \text{for sets of primes } S \text{ containing the infinite primes} \tag{29}$$

and

$$|\alpha_1 + \alpha_2 + \ldots + \alpha_r|_v \leqq r^{s(v)} \max(|\alpha_1|_v, |\alpha_2|_v, \ldots, |\alpha_r|_v) \quad \text{for } \alpha_1, \ldots, \alpha_r \in K \text{ and } v \in M_K. \tag{30}$$

Lemma 1. *Let θ be a non-zero algebraic number, not necessarily in K and let $C \geqq 1$ be a constant. Then the number of $z \in K \backslash \{0\}$ with*

$$h(\theta z) \leqq C \tag{31}$$

is at most

$$5(2C^3)^m.$$

Proof. Let N be an integer with $N \geqq 5$ and suppose that a set $\mathscr{S}$ exists, which contains N numbers $z \in K \backslash \{0\}$ satisfying (31). Let w be a fixed infinite prime on K. Primes denoted by capitals V or W will always belong to $M_{K(\theta)}$. Put $M = \prod_{W|w} |\theta|_W$, where $\prod_{W|w}$ means that the product is taken over all W lying above w. We shall use frequently that

$$\prod_{W|w} |\alpha|_W = |\alpha|_w \quad \text{for } \alpha \in K, \quad \sum_{W|w} s(W) = s(w). \tag{32}$$

First of all, we assume that w is complex. Then we may assume that $K \subset \mathbb{C}$ and that $|\,.\,|_w^{m/2}$ can be extended to the ordinary absolute value on $\mathbb{C}$. By (32) we have for $z \in \mathscr{S}$,

$$\begin{aligned} |z| = |z|_w^{m/2} = (\prod_{W|w} |z|_W)^{m/2} &= (M^{-1} \prod_{W|w} |\theta z|_W)^{m/2} \\ &\leqq (M^{-1} h(\theta z))^{m/2} \leqq (C/M)^{m/2}. \end{aligned}$$

Hence all elements of $\mathscr{S}$ belong to the square in the complex plane with sides of length $2(C/M)^{m/2}$, centered around the origin. Divide this square into d^2 small squares, each having sides of length $2(C/M)^{m/2}/d$, where d is the integer defined by $d^2 < N \leqq (d+1)^2$. By the box principle, at least one of these squares contains two distinct elements of $\mathscr{S}$, z_1, z_2 say. Clearly, $|z_1 - z_2| \leqq 2\sqrt{2}(C/M)^{m/2}/d$. Together with (32) and $d \geqq 2$ this implies that

$$\prod_{W|w} |\theta(z_1 - z_2)|_W = M|z_1 - z_2|_w \leqq 2^{s(w)}(2/d^2)^{1/m} C \leqq 2^{s(w)} C(5/N)^{1/m}. \tag{33}$$

If w is real, then one can show in a similar way that (33) holds for certain $z_1, z_2 \in \mathscr{S}$ with $z_1 \neq z_2$, by dividing the interval $[-(C/M)^m, (C/M)^m]$ into $N-1$ subintervals of equal length. A combination of (33), the right-hand side of (32), (29) and the product formula on $K(\theta)$ yields that

$$\begin{aligned} 1 &= \prod_{W|w} |\theta(z_1 - z_2)|_W \cdot \prod_{V \nmid w} |\theta(z_1 - z_2)|_V \\ &\leqq (\prod_{W|w} 2^{s(W)})\, C(5/N)^{1/m} \prod_{V \nmid w} (2^{s(V)} \max(1, |\theta z_1|_V) \max(1, |\theta z_2|_V)) \\ &\leqq 2(5/N)^{1/m}\, C h(\theta z_1) h(\theta z_2) \leqq 2C^3(5/N)^{1/m}, \end{aligned}$$

hence $N \leqq 5(2C^3)^m$. This proves Lemma 1. □

§ 6. Preliminaries to the proof of theorem 1

We shall use the same notations as in the preceding sections. Thus K is an algebraic number field of degree m, S is a finite set of primes on K of cardinality s containing the infinite primes and λ, μ are non-zero elements of K. We shall consider the equation

$$\lambda x + \mu y = 1 \qquad \text{in } S\text{-units } x, y. \tag{5}$$

Let ρ be a fixed, primitive third root of unity and put $L = K(\rho)$. We introduce the following notations:

$$\begin{gathered} \xi = \xi(x, y) = \lambda x - \rho \mu y, \qquad \eta = \eta(x, y) = \lambda x - \rho^2 \mu y, \\ \zeta(x, y) = \xi(x, y)/\eta(x, y) \qquad \text{for } x, y \in K. \end{gathered} \tag{34}$$

x, y can be expressed in terms of ξ, η as follows:

$$\lambda x = \frac{\rho^2 \xi - \rho \eta}{\rho^2 - \rho}, \qquad \mu y = \frac{\xi - \eta}{\rho^2 - \rho}.$$

Therefore, in view of (30), (34) and $|\rho^2 - \rho|_V = |3|_V^{1/2}$ for $V \in M_L$,

$$\begin{aligned} 2^{-s(V)} \max(|\xi|_V, |\eta|_V) &\leqq \max(|\lambda x|_V, |\mu y|_V) \\ &\leqq |3|_V^{-1/2} 2^{s(V)} \max(|\xi|_V, |\eta|_V) \qquad \text{for } V \in M_L. \end{aligned} \tag{35}$$

This implies by (26), (29) and the product formula, that

$$\begin{aligned} h(\lambda x/\mu y) &= \prod_{V \in M_L} \max(|\lambda x|_V, |\mu y|_V) \\ &\leqq \Big(\prod_{V \in M_L} |3|_V\Big)^{-1/2} 2 \prod_{V \in M_L} \max(|\xi|_V, |\eta|_V) = 2h(\zeta(x, y)). \end{aligned} \tag{36}$$

In the sequel we shall also use the following notations. $\mathscr{V}^0$ is the set of those $\zeta \in L$ for which a solution (x, y) of (5) exists, with $\lambda x/\mu y$ not a root unity, such that $\zeta = \zeta(x, y)$. Let T be the set of primes on L lying above the primes from S and put

$$A = \Big(\prod_{V \in T} |3|_V\Big)^{1/2} \prod_{V \in T} |\lambda \mu|_V \Big(\prod_{V \notin T} \max(|\lambda|_V, |\mu|_V)\Big)^3.$$

Since $|\lambda \mu|_V \leqq \max(|\lambda|_V, |\mu|_V)^2$ for $V \in M_L$, we have by the product formula that $A \geqq \prod_{V \notin T} \max(|\lambda|_V, |\mu|_V)$. If (5) is solvable in S-units x, y, then $\max(|\lambda|_V, |\mu|_V) \geqq 1$ for $V \notin T$. Hence it is no restriction to assume that $A \geqq 1$ and we shall do so in the remainder of this article.

Lemma 2. *We have*

$$\prod_{V \in T} |1 - \zeta^3|_V \cdot \prod_{V \in T} \max(1, |\zeta|_V^3) \leqq \Big(\prod_{V \in T} |3|_V\Big) A \qquad \textit{for } \zeta \in \mathscr{V}^0 \tag{37}$$

and

$$\prod_{V \in T} \frac{|\zeta_1 - \zeta_2|_V}{\max(1, |\zeta_1|_V) \max(1, |\zeta_2|_V)} \geqq \frac{A}{3h(\zeta_1) h(\zeta_2)} \qquad \textit{for } \zeta_1, \zeta_2 \in \mathscr{V}^0,\ \zeta_1 \neq \zeta_2. \tag{38}$$

Proof. Note that $\xi^3-\eta^3=\pm 3\sqrt{-3}\,\lambda\mu(\lambda x+\mu y)$. Together with (35) this implies for every solution (x,y) of (5), on putting $\zeta=\zeta(x,y)$.

$$\prod_{V\in T}|\xi^3-\eta^3|_V\cdot\prod_{V\notin T}\max(|\xi|_V^3,|\eta|_V^3)$$
$$\leqq\Big(\prod_{V\in T}|3|_V\Big)^{3/2}\prod_{V\in T}|\lambda\mu|_V\cdot\prod_{V\notin T}\max(|\lambda|_V^3,|\mu|_V^3)=\Big(\prod_{V\in T}|3|_V\Big)A.$$

Together with the product formula this implies (37).

We now prove (38). Let $\xi_i=\xi(x_i,y_i)$, $\eta_i=\eta(x_i,y_i)$, $\zeta_i=\xi_i/\eta_i$ for $i=1,2$, where (x_1,y_1), (x_2,y_2) are distinct solutions of (5). Let $V\notin T$. Then

$$|\lambda(x_1y_2-x_2y_1)|_V=|y_2(1-\mu y_1)-y_1(1-\mu y_2)|_V=|y_2-y_1|_V\leqq 1$$

and

$$|\mu(x_1x_2-x_2y_1)|_V=|x_1(1-\lambda x_2)-x_2(1-\lambda x_1)|_V=|x_1-x_2|_V\leqq 1.$$

Hence

$$\max(|\lambda|_V,|\mu|_V)|x_1y_2-x_2y_1|_V\leqq 1\qquad\text{for } V\notin T.$$

Therefore, by the product formula,

$$\prod_{V\in T}|x_1y_2-x_2y_1|_V\geqq\prod_{V\in M_L}|x_1y_2-x_2y_1|_V\cdot\prod_{V\notin T}\max(|\lambda|_V,|\mu|_V)$$
$$=\prod_{V\notin T}\max(|\lambda|_V,|\mu|_V).$$

Since $\xi_1\eta_2-\xi_2\eta_1=(\rho^2-\rho)\lambda\mu(x_1y_2-x_2y_1)$, this implies that

$$\prod_{V\in T}|\xi_1\eta_2-\xi_2\eta_1|_V\geqq\Big(\prod_{V\in T}|3|_V\Big)^{1/2}\prod_{V\in T}|\lambda\mu|_V\cdot\prod_{V\notin T}\max(|\lambda|_V,|\mu|_V).\tag{39}$$

Moreover, by (35) with $V\notin T$ and the fact that x_i,y_i $(i=1,2)$ are S-units,

$$\prod_{V\notin T}\max(|\xi_i|_V,|\eta_i|_V)\geqq\Big(\prod_{V\notin T}|3|_V\Big)^{1/2}\prod_{V\notin T}\max(|\lambda|_V,|\mu|_V)$$
$$\geqq 3^{-1/2}\prod_{V\notin T}\max(|\lambda|_V,|\mu|_V).$$

Together with (24), the product formula and (39), this implies that

$$\prod_{V\in T}\frac{|\zeta_1-\zeta_2|_V}{\max(1,|\zeta_1|_V)\max(1,|\zeta_2|_V)}$$
$$=\prod_{V\in T}|\zeta_1-\zeta_2|_V\cdot\prod_{V\notin T}(\max(1,|\zeta_1|_V)\max(1,|\zeta_2|_V))/h(\zeta_1)h(\zeta_2)$$
$$=\prod_{V\in T}|\xi_1\eta_2-\xi_2\eta_1|_V\cdot\prod_{V\notin T}(\max(|\xi_1|_V,|\eta_1|_V)\max(|\xi_2|_V,|\eta_2|_V))/h(\zeta_1)h(\zeta_2)$$
$$\geqq\Big(\prod_{V\in T}|3|_V\Big)^{1/2}\prod_{V\in T}|\lambda\mu|_V\Big(\prod_{V\notin T}\max(|\lambda|_V,|\mu|_V)\Big)^3/3h(\zeta_1)h(\zeta_2)$$
$$=A/3h(\zeta_1)h(\zeta_2).\quad\square$$

In the sequel we shall not refer to ξ,η. In fact, the inequalities (37), (38) will suffice for most of our arguments.

Lemma 3. *Put*

$$m_V(\zeta)=\min_{i=0,1,2}(1,\max(|1-\rho^i\zeta|_V,|1-\rho^{-i}\zeta^{-1}|_V)\quad \textit{for } V\in M_L,\ \zeta\in L.$$

Then

$$\prod_{V\in T} m_V(\zeta)\leqq 8Ah(\zeta)^{-3}\quad \textit{for } \zeta\in\mathscr{V}^0.$$

Proof. Let $V\in T$ and $\zeta\in\mathscr{V}^0$. Choose $\zeta_0\in\{\zeta,\rho\zeta,\rho^2\zeta\}$ such that $|1-\zeta_0|_V\leqq |1-\rho^i\zeta_0|_V$ for $i=1,2$. Then, by (30),

$$\begin{aligned}|1-\rho^i\zeta_0|_V&=\max(|1-\rho^i\zeta_0|_V,|1-\zeta_0|_V)\\&=\max(|\rho^{-i}-\zeta_0|_V,|1-\zeta_0|_V,|1-\rho^i\zeta_0|_V)\\&\geqq 2^{-s(V)}\max(|1-\rho^{-i}|_V,|(1-\rho^i)\zeta_0|_V)=2^{-s(V)}|3|_V^{1/2}\max(1,|\zeta_0|_V)\end{aligned}$$

for $i=1,2$. Therefore,

$$|1-\zeta_0^3|_V\geqq 2^{-2s(V)}|3|_V\max(1,|\zeta_0|_V^2)|1-\zeta_0|_V. \tag{40}$$

Now we have either $|\zeta_0|_V\leqq 2^{s(V)}$, which implies that $2^{-s(V)}\max(1,|\zeta_0|_V)\leqq 1$; or $|\zeta_0|_V>2^{s(V)}$ in which case we have by (30),

$$\begin{aligned}2^{-s(V)}|\zeta_0|_V=|\zeta_0|_V2^{-s(V)}|1|_V&\leqq|\zeta_0|_V\max(|\zeta_0^{-1}|_V,|1-\zeta_0^{-1}|_V)\\&=\max(1,|1-\zeta_0|_V)=|1-\zeta_0|_V.\end{aligned}$$

Hence by (40),

$$|1-\zeta_0^3|_V\geqq 2^{-3s(V)}|3|_V\max(1,|\zeta_0|_V^3)\min(1,|1-\zeta_0|_V). \tag{41}$$

By a similar argument it is possible to derive inequality (41) with ζ_0 replaced by ζ_0^{-1}, on noting that $|1-\zeta_0^{-1}|_V=|\zeta_0|_V^{-1}|1-\zeta_0|_V\leqq|\zeta_0|_V^{-1}|1-\rho^i\zeta_0|_V=|1-\rho^{-i}\zeta_0^{-1}|_V$ for $i=1,2$. Hence,

$$\begin{aligned}|1-\zeta_0^3|_V&=|\zeta_0^3|_V|1-\zeta_0^{-3}|_V\\&\geqq 2^{-3s(V)}|3|_V|\zeta_0^3|_V\max(1,|\zeta_0|_V^{-3})\min(1,|1-\zeta_0^{-1}|_V)\\&=2^{-3s(V)}|3|_V\max(1,|\zeta_0|_V^3)\min(1,|1-\zeta_0^{-1}|_V).\end{aligned}$$

Together with (41) and the fact that $\max(\min(a,b),\min(a,c))=\min(a,\max(b,c))$ for real numbers a,b,c this implies that

$$|1-\zeta_0^3|_V\geqq 2^{-3s(V)}|3|_V\max(1,|\zeta_0^3|_V)\min(1,\max(|1-\zeta_0|_V,|1-\zeta_0^{-1}|_V)).$$

Hence, by our choice of ζ_0,

$$m_V(\zeta)\leqq 2^{3s(V)}|3|_V^{-1}\max(1,|\zeta|_V)^{-3}|1-\zeta^3|_V.$$

Together with (37) and (29) this implies that

$$\begin{aligned}\prod_{V\in T} m_V(\zeta)&\leqq 8(\prod_{V\in T}|3|_V)^{-1}(\prod_{V\in T}|3|_V)A(\prod_{V\in T}\max(1,|\zeta|_V)\cdot\prod_{V\notin T}\max(1,|\zeta|_V))^{-3}\\&=8Ah(\zeta)^{-3}.\quad\square\end{aligned}$$

Lemma 4. *Let B be a real number with $0<B<1$, let $q \geqq 1$ be an integer and put $R(B)=(1-B)^{-1}B^{B/(B-1)}$. Then there exists a set $\mathscr{W}$ of cardinality at most $\max(1,(2B)^{-1})R(B)^{q-1}$ consisting of tuples $(\Gamma_1,\ldots,\Gamma_q)$ with $\Gamma_j \geqq 0$ for $j=1,\ldots,q$ and $\sum_{j=1}^{q}\Gamma_j=B$ with the following property: for any set of reals $F_1,\ldots,F_q$, Λ with $0<F_j \leqq 1$ for $j=1,\ldots,q$ and $\prod_{j=1}^{q}F_j \leqq \Lambda$ there exists a tuple $(\Gamma_1,\ldots,\Gamma_q)\in\mathscr{W}$ such that*

$$F_j \leqq \Lambda^{\Gamma_j} \quad \textit{for } j=1,\ldots,q. \tag{42}$$

Proof. We assume that $q \geqq 2$ which is clearly no restriction. Note that for $\Lambda \geqq 1$ any set $\mathscr{W}$ will satisfy the statement in the lemma. Hence it is no restriction to assume that $\Lambda<1$ and we shall do so in the sequel.

Let $F_1,\ldots,F_q,\Lambda$ be reals with $0<F_j \leqq 1$ for $j=1,\ldots,q$, $\Lambda<1$ and $\sum_{j=1}^{q}F_j \leqq \Lambda$. Then there are non-negative reals ϕ_j such that

$$F_j=\Lambda^{\phi_j}, \qquad \sum_{j=1}^{q}\phi_j \geqq 1. \tag{43}$$

Define the integer u by

$$(q-1)B/(1-B) \leqq u < (q-1)B/(1-B)+1. \tag{44}$$

Then $u \geqq 1$. For $j=1,\ldots,q$ define integers g_j by

$$u\phi_j/B-1 < g_j \leqq u\phi_j/B. \tag{45}$$

Then $g_j \geqq 0$ and by the right-hand side inequality of (43) and by (44),

$$\sum_{j=1}^{q} g_j > uB^{-1}\left(\sum_{j=1}^{q}\phi_j\right)-q \geqq uB^{-1}-q \geqq u-1.$$

Hence $\sum_{j=1}^{q} g_j \geqq u$. Now there are integers $f_j (j=1,\ldots,q)$ with $0 \leqq f_j \leqq g_j$ and $\sum_{j=1}^{q} f_j = u$. Therefore, by the left-hand side inequality of (43) and (45), since $\Lambda<1$,

$$F_j=\Lambda^{\phi_j} \leqq \Lambda^{g_jB/u} \leqq \Lambda^{f_jB/u}.$$

Hence (42) is satisfied by some tuple $(\Gamma_1,\ldots,\Gamma_q)$ belonging to the set

$$\mathscr{W}=\left\{(\Gamma_1,\ldots,\Gamma_q)\,\middle|\,\Gamma_j=f_jB/u, f_j\in\mathbb{Z}, f_j \geqq 0 \text{ for } j=1,\ldots,q, \sum_{j=1}^{q} f_j=u\right\}.$$

We shall now estimate the cardinality of $\mathscr{W}$ from above. Note that $\mathscr{W}$ has by (44) cardinality at most

$$\binom{u+q-1}{q-1} \leqq \binom{(q-1)B/(1-B)+q}{q-1}.$$

Note also that $R(B)=T(B/(1-B))$, where $T(x)=(1+x)^{1+x}x^{-x}$. Hence it suffices to show, on putting $x=B/(1-B)$, $h=q-1$,

$$\binom{h(1+x)+1}{h}\leqq\tfrac{1}{2}(1+x^{-1})\,T(x)^h \quad \text{for } x>0,\ h\in\mathbb{N}. \tag{46}$$

The proof of this fact is based on the inequality

$$\binom{\xi}{g}\leqq\frac{\xi^\xi}{(\xi-g+1)^{\xi-g}g^g} \quad \text{for } \xi\in\mathbb{R},\ g\in\mathbb{N} \ \text{ with } \ \xi\geqq g. \tag{47}$$

It is not difficult to prove (47) by induction on g, on using that the function $(\eta/(\eta+1))^\eta$ decreases monotonically for $\eta>0$. For (47) is trivial for $g=1$ and if (47) has been proved for $g=p(p\geqq 1)$, then, for $\xi\geqq p+1$,

$$\binom{\xi}{p+1}=\frac{\xi}{p+1}\binom{\xi-1}{p}\leqq\frac{\xi}{p+1}\,\frac{(\xi-1)^{\xi-1}}{(\xi-p)^{\xi-p-1}p^p}$$
$$=\frac{((\xi-1)/\xi)^{\xi-1}}{(p/(p+1))^p}\,\frac{\xi^\xi}{(\xi-p)^{\xi-p-1}(p+1)^{p+1}}\leqq\frac{\xi^\xi}{(\xi-p)^{\xi-p-1}(p+1)^{p+1}}.$$

We shall now prove (46). Note that $h\,x\geqq x>0$, that the function $(\eta/(\eta+1))^{\eta+1}$ increases for $\eta>0$ and that the function $(\eta/(\eta+1))^\eta$ decreases for $\eta>0$. Together with (47) these facts imply that

$$\binom{h(1+x)+1}{1}T(x)^{-h}\leqq\frac{(h(1+x)+1)^{h(1+x)+1}}{(h\,x+2)^{hx+1}\,h^h}\cdot x^{hx}(1+x)^{-h(1+x)}$$
$$=\left(\frac{h(1+x)+1}{h(1+x)}\right)^{h(1+x)+1}\left(\frac{h\,x}{h\,x+1}\right)^{hx+1}\left(\frac{h\,x+1}{h\,x+2}\right)^{hx+1}\frac{1+x}{x}$$
$$\leqq\left(\frac{h(1+x)+1}{h(1+x)}\right)^{h(1+x)+1}\left(\frac{h(1+x)}{h(1+x)+1}\right)^{h(1+x)+1}$$
$$\cdot\left(\frac{h\,x+1}{h\,x+2}\right)^{hx+1}(1+x^{-1})$$
$$=\left(\frac{h\,x+1}{h\,x+2}\right)^{hx+1}(1+x^{-1})\leqq\tfrac{1}{2}(1+x^{-1}).\quad\square$$

Let ζ be a fixed number in $\mathscr{V}^0$. Choose for every prime $V\in T$ $\rho_V\in\{1,\rho,\rho^2\}$ such that

$$m_V(\zeta)=\min(1,\max(|1-\rho_V\,\zeta|_V,|1-\rho_V^{-1}\,\zeta^{-1}|_V)).$$

Note that there are at most two primes on $L=K(\rho)$ lying above each v in S. Suppose that V, V' are primes on L lying above a given $v\in S$. Then $[L\colon K]=2$. If σ is the K-automorphism of L mapping ρ onto $\rho^2=\rho^{-1}$, then

$$|\alpha|_{V'}=|\sigma(\alpha)|_V \quad \text{for } \alpha\in L.$$

Hence, on noting that ζ can be written as $(\lambda x-\rho\mu y)/(\lambda x-\rho^2\mu y)$ for certain $x, y\in K$,

$$|1-\rho^i\zeta|_{V'}=|1-\sigma(\rho^i\zeta)|_V=|1-\rho^{-i}\zeta^{-1}|_V, \qquad |1-\rho^{-i}\zeta^{-1}|_{V'}=|1-\rho^i\zeta|_V.$$

for $i=0,1,2$. Therefore, we may assume that

$$\rho_{V'}=\rho_V, \qquad m_{V'}(\zeta)=m_V(\zeta). \tag{48}$$

Let B be a real with $\frac{1}{2}\leqq B<1$. By Lemmas 3 and 4, there exists a tuple $(\Gamma_v)_{v\in S}$, belonging to a set $\mathscr{W}$ of cardinality at most $R(B)^{s-1}$, not depending on ζ, such that

$$\prod_{V|v} m_V(\zeta)\leqq(8Ah(\zeta)^{-3})^{\Gamma_v} \qquad \text{for } v\in S.$$

(Here the product is taken over all primes on L lying above v.) For $v\in S$, let $n(v)$ be the number of primes on L lying above v and put $\Gamma_V=\Gamma_v/n(v)$ for every prime V on L lying above v. Then we obtain, in view of (48) and the fact that $m_V(\zeta)\geqq\min(1,|1-\rho_V\zeta|_V)$ for $V\in T$,

$$\min(1,|1-\rho_V\zeta|_V)\leqq(8\,\mathrm{A\,h}(\zeta)^{-3})^{\Gamma_v} \qquad \text{for } V\in T. \tag{49}$$

By (48), the tuple $(\rho_V)_{V\in T}$ can be chosen from a set of cardinality at most 3^s and clearly, the tuple $(\Gamma_V)_{V\in T}$ belongs to a set of cardinality at most $R(B)^{s-1}$. Moreover, $\Gamma_V\geqq 0$ for $V\in T$ and $\sum_{V\in T}\Gamma_V=\mathrm{B}$. Thus we arrive at

Lemma 5. *Let B be a real number with $\frac{1}{2}\leqq B<1$. Then there exists a set $\mathscr{W}_0$ of cardinality at most $3^s R(B)^{s-1}$ (where $R(B)=(1-B)^{-1}B^{B/(B-1)}$), consisting of tuples $((\rho_V)_{V\in T},(\Gamma_V)_{V\in T})$ with $\rho_V^3=1$ and $\Gamma_V\geqq 0$ for $V\in T$ and $\sum_{V\in T}\Gamma_V=B$ with the following property: for every $\zeta\in\mathscr{V}^0$ there is a tuple $((\rho_V)_{V\in T},(\Gamma_V)_{V\in T})\in\mathscr{W}_0$ such that ζ satisfies* (49).

The next step in the proof of Theorem 1 is to apply an approximation method to systems of inequalities of type (49). The following section will be devoted to this.

§ 7. Application of the approximation method

In the study of systems of inequalities of type (49) we shall use certain auxiliary polynomials of which some properties are stated in the lemma below. As in § 6, we put $L=K(\rho)$, where K is an algebraic number field of degree m and ρ is a primitive cube root of unity.

Lemma 6. *For every $r\in\mathbb{N}$ there are polynomials $A_r(X)$, $B_r(X)$, $V_r(X)\in\mathbb{Z}[X]$ of degree r with the following properties:*

$$A_r(X^3)-XB_r(X^3)=(1-X)^{2r+1}V_r(X); \tag{50}$$

$$A_{r+1}(\alpha)B_r(\alpha)\neq A_r(\alpha)B_{r+1}(\alpha) \qquad \textit{for } \alpha\in L\backslash\{1\}; \tag{51}$$

$$\begin{aligned}&|A_r(\alpha)|_V \leqq \left(\tfrac{1}{4}(12\sqrt{3})^r\right)^{s(V)}\max(1,|\alpha|_V)^r,\\ &|B_r(\alpha)|_V \leqq \left(\tfrac{1}{4}(12\sqrt{3})^r\right)^{s(V)}\max(1,|\alpha|_V)^r \quad \textit{for } \alpha\in L,\ V\in M_L;\end{aligned} \tag{52}$$

$$\begin{aligned}&|A_r(\alpha^3)|_V \leqq \left(\tfrac{1}{4}(96\sqrt{3})^r\right)^{s(V)}, |B_r(\alpha^3)|_V \leqq \left(\tfrac{1}{4}(96\sqrt{3})^r\right)^{s(V)},\\ &|V_r(\alpha)|_V \leqq \left(\tfrac{1}{2}(96\sqrt{3})^r\right)^{s(V)} \quad \textit{for } \alpha\in L \ \ \textit{with} \ \ |1-\alpha|_V\leqq 1, \ \ V\in M_L.\end{aligned} \tag{53}$$

Proof. The polynomials $A_1(X)=1+2X$, $B_1(X)=2+X$, $V_1(X)=1+X$ satisfy the lemma for $r=1$. Therefore we shall restrict ourselves to the case $r\geqq 2$. Put $q_r=(3^r, r!)\,3^r$ and

$$A_r(X)=q_r\sum_{m=0}^{r}\binom{r+1/3}{m}\binom{r-1/3}{r-m}X^m, \qquad B_r(X)=q_r\sum_{m=0}^{r}\binom{r-1/3}{r}\binom{r+1/3}{r-m}X^m. \tag{54}$$

In Lemma 8 of [6] we showed that the polynomials $G_r(X):=A_r(1-X)$ and $H_r(X):=B_r(1-X)$ have rational integral coefficients. Hence $A_r(X)$, $B_r(X)\in\mathbb{Z}[X]$. Moreover, we showed there, using results from the theory of hypergeometric functions, that we have the identity in formal power series

$$U_r(X):=A_r(1-X)-(1-X)^{1/3}B_r(1-X)=X^{2r+1}F_r(X), \tag{55}$$

where $(1-X)^{1/3}=\sum_{k=0}^{\infty}\binom{1/3}{k}(-X)^k$ and where $F_r(X)$ is a formal power series with rational coefficients. By eliminating $(1-X)^{1/3}$ from (55) and from (55) with $r+1$ instead of r and by replacing $1-X$ by X, we obtain

$$A_{r+1}(X)\,B_r(X)-A_r(X)\,B_{r+1}(X)=(1-X)^{2r+1}P_r(X) \tag{56}$$

for some rational function $P_r(X)$ which has a Taylor expansion around $X=1$. Since the degree of the left-hand side of (56) is at most $2r+1$, $P_r(X)$ must be a constant, c_r say. An easy computation shows that $c_r\neq 0$. This shows (51).

In order to show (50) we put $W_r(X):=A_r(X^3)-XB_r(X^3)$, $Y=1-X^3$. It is easy to check, by induction on k, that

$$\frac{d^k}{dX^k}W_r(X)=\sum_{j=0}^{k}f_{jk}(X)\frac{d^j}{dY^j}U_r(Y) \quad \text{for } k\in\mathbb{N}\cup\{0\},$$

where the functions $f_{jk}(X)$ are polynomials with coefficients in $\mathbb{Z}$. Hence

$$W_r^{(k)}(1)=\sum_{j=0}^{k}f_{jk}(1)\,U_r^{(j)}(0)$$

for $k\in\mathbb{N}\cup\{0\}$. Since $U_r^{(k)}(0)=0$ for $k=0,1,\dots,2r$ this implies that $W_r^{(k)}(1)=0$ for $k=0,1,\dots,2r$, i.e. that the polynomial $W_r(X)$ is divisible by $(1-X)^{2r+1}$. This shows that (50) holds true for some polynomial $V_r(X)$ and by Gauss' lemma, $V_r(X)$ has rational integral coefficients.

In the proof of (52), (53) we shall use the following inequality:

$$q_r\binom{2r}{r}\leqq\tfrac{1}{4}(12\sqrt{3})^r. \tag{57}$$

(57) can be proved as follows. Note that $r \geqq 2$ (by the restriction made at the beginning of the proof) and $(3^r, r!) = 3^{\delta(r)}$, where

$$\delta(r) = \sum_{j=1}^{\infty} [r/3^j] < \sum_{j=1}^{\infty} r/3^j = r/2,$$

i.e. $\delta(r) \leqq \frac{1}{2}(r-1)$. Moreover, the sequence $\left\{\binom{2r}{r} 4^{-r}\right\}_{r=1}^{\infty}$ decreases. Hence

$$q_r \binom{2r}{r} = 3^r (3^r, r!) \binom{2r}{r} \leqq 3^r (\sqrt{3})^{r-1} 4^r \cdot \binom{2r}{r} 4^{-r} \leqq \frac{1}{\sqrt{3}} \frac{3}{8} (12\sqrt{3})^r$$
$$\leqq \tfrac{1}{4}(12\sqrt{3})^r.$$

For every polynomial $f(X) = b_0 + b_1 X + \ldots + b_d X^d \in \mathbb{Z}[X]$ we put

$$\|f\| := |b_0| + |b_1| + \ldots + |b_d|.$$

Then

$$|f(\alpha)|_V \leqq \|f\|^{s(V)} \max(1, |\alpha|_V)^d \quad \text{for } \alpha \in L,\ V \in M_L. \tag{58}$$

In case that V is finite this is almost trivial; in case that V is infinite this follows from the fact that the valuation $|\,.\,|_V^{1/s(V)}$ satisfies the triangle inequality and is equal to the ordinary absolute value on $\mathbb{Q}$.

By comparing the coefficients of X^r in the identity of power series $(1+X)^{2r} = (1+X)^{r+1/3}(1+X)^{r-1/3}$ we obtain $\binom{2r}{r} = \sum_{m=0}^{r} \binom{r+1/3}{m}\binom{r-1/3}{r-m}$. Hence by (57),

$$\|A_r\| = \|B_r\| = q_r \binom{2r}{r} \leqq \tfrac{1}{4}(12\sqrt{3})^r. \tag{59}$$

In view of (58) this proves (52).

The inequalities of (53) with A_r, B_r follow immediately from (52), on noting that $|\alpha^3|_V \leqq 2^{3s(V)}$ if $|1-\alpha|_V \leqq 1$. In order to derive the inequality with V_r we shall estimate $\|V_r^*\|$ from above, where $V_r^*(X) = V_r(1-X)$. For convenience, we put $\binom{a}{m} = 0$ if $m \in \mathbb{Z}$, $m < 0$ or $a, m \in \mathbb{Z}$, $a < m$. Then

$$\begin{aligned}
V_r^*(X) &= X^{-2r-1}(A_r((1-X)^3) - (1-X)B_r((1-X)^3)) \\
&= X^{-2r-1} q_r \left(\sum_{m=0}^{r} \binom{r+1/3}{m}\binom{r-1/3}{r-m}(1-X)^{3m}\right. \\
&\quad \left. - \sum_{m=0}^{r} \binom{r-1/3}{m}\binom{r+1/3}{r-m}(1-X)^{3m+1}\right) \\
&= X^{-2r-1} q_r \sum_{m=0}^{r} \binom{r+1/3}{m}\binom{r-1/3}{r-m}\left(\sum_{j=0}^{3m}\binom{3m}{j}(-X)^j\right) \\
&\quad - X^{-2r-1} q_r \sum_{m=0}^{r} \binom{r+1/3}{m}\binom{r-1/3}{r-m}\left(\sum_{j=0}^{3(r-m)+1}\binom{3(r-m)+1}{j}(-X)^j\right)
\end{aligned}$$

$$=X^{-2r-1}q_r\sum_{j=2r+1}^{3r+1}\left(\sum_{m=0}^{r}\binom{r+1/3}{m}\binom{r-1/3}{r-m}\left(\binom{3m}{j}\right.\right.$$
$$\left.\left.-\binom{3(r-m)+1}{j}\right)\right)(-1)^j X^j.$$

This implies by (57) that

$$\begin{aligned}\|V_r^*\| &\leqq q_r\sum_{j=2r+1}^{3r+1}\sum_{m=0}^{r}\binom{r+1/3}{m}\binom{r-1/3}{r-m}\left|\binom{rm}{j}-\binom{3(r-m)+1}{j}\right|\\ &\leqq q_r\sum_{j=2r+1}^{3r+1}\binom{3r+1}{j}\left(\sum_{m=0}^{r}\binom{r+1/3}{m}\binom{r-1/3}{r-m}\right)\\ &\leqq q_r\binom{2r}{r}2^{3r+1}\leqq\tfrac{1}{2}(96\sqrt{3})^r.\end{aligned}$$

By (58) this completes the proof of our lemma. □

Let T be the set of primes on L lying above the primes in S, let $(\rho_V)_{V\in T}$ be a tuple of cube roots of unity and let $(\Gamma_V)_{V\in T}$ a tuple of non-negative real numbers with $\sum_{V\in T}\Gamma_V=\mathrm{B}$. Here B is a positive real number. We shall consider the system of inequalities

$$\min(1,|1-\rho_V\zeta|_V)\leqq(8Ah(\zeta)^{-3})^{\Gamma_V}\quad\text{for } V\in T \tag{49}$$

in the variable $\zeta\in\mathscr{V}^0$.

Lemma 7. *Assume that $2/3<B<1$. Let $\zeta_1,\zeta_2,\dots,\zeta_{k+1}$ be distinct elements of $\mathscr{V}^0$ which are ordered such that $h(\zeta_1)\leqq h(\zeta_2)\leqq\dots\leqq h(\zeta_{k+1})$ and which satisfy* (49). *Then*

$$h(\zeta_{k+1})\geqq\left(\frac{A^{1-B}}{6\times 8^B}\right)^{((3B-1)^k-1)/(3B-2)}h(\zeta_1)^{(3B-1)^k}. \tag{60}$$

Proof. We shall prove (60) only for $k=1$. Then the lemma follows easily by induction on k. Let $V\in T$. First of all, we have by (30),

$$E_V:=\frac{|\zeta_1-\zeta_2|_V}{\max(1,|\zeta_1|_V)\max(1,|\zeta_2|_V)}\leqq 2^{s(V)}.$$

By (30) we also

$$E_V\leqq|\zeta_1-\zeta_2|_V\leqq 2^{s(V)}\max(|1-\rho_V\zeta_1|_V,|1-\rho_V\zeta_2|_V).$$

Note that $\min(a,\max(b,c))=\max(\min(a,b),\min(a,c))$ for $a,b,c\in\mathbb{R}$. Together with (49) this yields

$$\begin{aligned}E_V&\leqq 2^{s(V)}\max(\min(1,|1-\rho_V\zeta_1|_V),\min(1,|1-\rho_V\zeta_2|_V))\\ &\leqq 2^{s(V)}\max(8Ah(\zeta_1)^{-3},8Ah(\zeta_2)^{-3})^{\Gamma_V}=2^{s(V)}(8Ah(\zeta_1)^{-3})^{\Gamma_V}.\end{aligned}$$

Therefore, by (38) (cf. Lemma 2) and (29),

$$\frac{A}{3h(\zeta_1)h(\zeta_2)} \leqq \prod_{V\in T} E_V \leqq 2(8Ah(\zeta_1)^{-3})^B,$$

which immediately implies that

$$h(\zeta_2) \geqq \frac{A^{1-B}}{6\times 8^B} h(\zeta_1)^{3B-1}. \quad \square$$

The following lemma will be proved by means of an approximation method. We have to impose a further restriction on B.

Lemma 8. *Assume that* $5/6<B<1$. *Let* r_0 *be an integer with* $r_0>\dfrac{2+2B-3B^2}{B(6B-5)}$, *let* k *be an integer with* $(3B-1)^{k+1}>3r_0+4$ *and put*

$$f_1(B,r_0)=\frac{(2r_0+1)B(3B-1)+B}{3B(6B-5)r_0-(6+6B-9B^2)},$$

$$f_2(B,r_0)=\frac{3B(r_0+1)}{3B(6B-5)r_0-(6+6B-9B^2)},$$

$$g_1(B,k,r_0)=\frac{B+(B-1)(3B-1)((3B-1)^k-1)/(3B-2)}{(3B-1)^{k+1}-3r_0-4},$$

$$g_2(B,k,r_0)=\frac{r_0+1+(3B-1)((3B-1)^k-1)/(3B-2)}{(3B-1)^{k+1}-3r_0-4}.$$

Then there are at most k *numbers* $\zeta\in\mathscr{V}^0$ *satisfying* (49) *and*

$$h(\zeta)\geqq \max((8A)^{f_1(B,r_0)}(96\sqrt{3})^{f_2(B,r_0)}, (8A)^{g_1(B,k,r_0)}(96\sqrt{3})^{g_2(B,k,r_0)}). \tag{61}$$

Proof. We assume that there are at least $k+1$ numbers $\zeta\in\mathscr{V}^0$ satisfying (49) and (61), $\zeta_1,\zeta_2,\ldots,\zeta_{k+1}$ say, ordered such that $h(\zeta_1)\leqq h(\zeta_3)\leqq h(\zeta_4)\ldots\leqq h(\zeta_k)$ $\leqq h(\zeta_{k+1})\leqq h(\zeta_2)$. We shall show that this assumption leads to a contradiction. Put $h_i=h(\zeta_i)$ for $i=1,2$. Then

$$h_2\geqq h_1\geqq (8A)^{1/3}>1. \tag{62}$$

For $A\geqq 1$, $f_2(B,r_0)>0$ and $f_1(B,r_0)$ decreases to $2(3B-1)/3(6B-5)$ if $r_0\to\infty$. Since $5/6<B<1$ the latter expression is larger than $1/3$.

In the first step of the proof we shall show that an integer l with $l\geqq r_0+1$ exists such that

$$(93\sqrt{3})^l(8A)^B h_1^{3l+1}<h_2^{3B-1}\leqq (96\sqrt{3})^{l+1}(8A)^B h_1^{3l+4}. \tag{63}$$

To prove this, it suffices to show that

$$h_2^{3B-1}>(96\sqrt{3})^{r_0+1}(8A)^B h_1^{3r_0+4}.$$

In view of Lemma 7 and the fact that $A^{1-B}/(6\times 8^{B})=(8A)^{1-B}/48>(8A)^{1-B}/96\sqrt{3}$, it is even sufficient to show that

$$\begin{aligned}\left(\frac{(8A)^{1-B}}{96\sqrt{3}}\right)^{((3B-1)^{k}-1)(3B-1)/(3B-2)} & \times h_1^{(3B-1)^{k+1}}\\ &\geqq (96\sqrt{3})^{r_0+1}(8A)^{B}h_1^{3r_0+4}.\end{aligned}$$

But this is equivalent to $h_1\geqq(8A)^{g_1(B,k,r_0)}(96\sqrt{3})^{g_2(B,k,r_0)}$ which is true by (61).

Put

$$U_n=\zeta_2 A_n(\zeta_1^3)-\zeta_1 B_n(\zeta_1^3)\qquad \text{for } n\in\mathbb{N},$$

where $A_n(X), B_n(X)$ are the polynomials from Lemma 6. Note that $l\geqq r_0+1\geqq 2$. Put $r=l$ if $U_l\neq 0$, $r=l-1$ otherwise. Then $r\geqq r_0$. From (62) and (28) it follows that $h(\zeta_1^3)>1$. Hence $\zeta_1^3\neq 1$. Together with (51) this implies that $U_r\neq 0$.

Let T' be the set of those $V\in T$ for which $\Gamma_V>0$. For $V\in T'$ we have firstly that $|1-\rho_V\zeta_i|_V\leqq 1$ for $i=1,2$ (cf. (62)) and secondly, by (50), (53), (30) and (49),

$$\begin{aligned}|U_r|_V&=|\rho_V\zeta_2 A_r(\zeta_1^3)-\rho_V\zeta_1 B_r(\zeta_1^3)|_V\\ &=|(\rho_V\zeta_2-1)A_r(\zeta_1^3)+(1-\rho_V\zeta_1)^{2r+1}V_r(\rho_V\zeta_1)|_V\\ &\leqq 2^{s(V)}(\tfrac{1}{2}(96\sqrt{3})^{r})^{s(V)}\max(|1-\rho_V\zeta_2|_V,|1-\rho_V\zeta_1|_V^{2r+1})\\ &\leqq (96\sqrt{3})^{rs(V)}\max(8Ah_2^{-3},(8A)^{2r+1}h_1^{-3(2r+1)})^{\Gamma_V}.\end{aligned}$$

Hence

$$\prod_{V\in T'}|U_r|_V\leqq\Big(\prod_{V\in T'}(96\sqrt{3})^{rs(V)}\Big)\max((8A)^{B}h_2^{-3B},(8A)^{(2r+1)B}h_1^{-3B(2r+1)}).\tag{64}$$

For $V\notin T'$ we have, by (30) and (52),

$$\begin{aligned}|U_r|_V&\leqq 2^{s(V)}\max(|\zeta_2|_V|A_r(\zeta_1^3)|_V,|\zeta_1|_V|B_r(\zeta_1^3)|_V)\\ &\leqq(96\sqrt{3})^{rs(V)}\max(1,|\zeta_1|_V)^{3r+1}\max(1,|\zeta_2|_V).\end{aligned}$$

Therefore,

$$\prod_{V\notin T'}|U_r|_V\leqq\Big(\prod_{V\notin T'}(96\sqrt{3})^{rs(V)}\Big)h_1^{3r+1}h_2.$$

Together with the product formula, (64) and (29) this implies that

$$1\leqq\max((96\sqrt{3})^{r}(8\mathrm{A})^{B}h_1^{3r+1}h_2^{1-3B},(96\sqrt{3})^{r}(8A)^{(2r+1)B}h_2h_1^{3r+1-3B(2r+1)}).\tag{65}$$

By the left inequality of (63) we have, since $r\geqq l$,

$$(96\sqrt{3})^{r}(8A)^{B}h_1^{3r+1}h_2^{1-3B}<1.\tag{66}$$

By the right inequality of (63), by (61), by $r_0\leqq r$, by $l\leqq r+1$ and by the fact that the functions$f_1(B,x), f_2(B,x)$ are decreasing in x for $x>(2+2B-3B^2)/B(6B-5)$

we have

$$\begin{aligned}
&(96\sqrt{3})^r (8A)^{(2r+1)B} h_2 h_1^{3r+1-3B(2r+1)}\\
&\quad \leqq ((96\sqrt{3})^{r(3B-1)+r+2} (8A)^{(2r+1)B(3B-1)+B} h_1^{3r+7+(3B-1)(3r+1-3B(2r+1))})^{\frac{1}{3B-1}}\\
&\quad < ((8A)^{(2r+1)B(3B-1)+B} (96\sqrt{3})^{3Br+3} h_1^{-3B(6B-5)r+6+6B-9B^2})^{\frac{1}{3B-1}}\\
&\quad = ((8A)^{f_1(B,r)} (96\sqrt{3})^{f_2(B,r)} h_1^{-1})^{(3B(6B-5)r-(6+6B-9B^2))/(3B-1)} \leqq 1.
\end{aligned}$$

Together with (66) this inequality contradicts (65). Hence the assumption made at the beginning of the proof of this lemma, i.e. that there are at least $k+1$ numbers $\zeta \in \mathscr{V}^0$ satisfying (49) and (61), must be false. □

§ 8. Proof of Theorem 1

First of all, we shall count the numbers $\zeta \in \mathscr{V}^0$ which satisfy a fixed system (49). We apply Lemma 8 with $B=0.846$, $r_0=34$, $k=10$ and Lemma 7 with $B=0.846$. When speaking of (49) or of B we implicitly assume that $B=0.846$.

A straightforward computation shows that

$$\begin{aligned}
f_1(B,r_0)&=47.111\ldots, & f_2(B,r_0)&=46.178\ldots,\\
g_1(B,k,r_0)&=-3.964\ldots, & g_2(B,k,r_0)&=30.871\ldots.
\end{aligned}$$

Since $f_1(B,r_0)\log 8 + f_2(B,r_0)\log(96\sqrt{3}) < 335$ and $A \geqq 1$ it follows from Lemma 8 that there are at most *ten* numbers $\zeta \in \mathscr{V}^0$ which satisfy a fixed system (49) and

$$h(\zeta) \geqq e^{335} A^{48}. \tag{67}$$

We now count the numbers $\zeta \in \mathscr{V}^0$ satisfying a fixed system (49) and

$$e^8/2 \leqq h(\zeta) < e^{335} A^{48}. \tag{68}$$

Suppose that there are t of such numbers, $\zeta_1, \zeta_2, \ldots, \zeta_t$ say, ordered such that $h(\zeta_1) \leqq h(\zeta_2) \ldots \leqq h(\zeta_t)$. Then, by Lemma 7,

$$\begin{aligned}
&\left(\frac{A^{1-B}}{6\times 8^B}\right)^{1/(3B-2)} e^{335} A^{48} > \left(\frac{A^{1-B}}{6\times 8^B}\right)^{1/(3B-2)} h(\zeta_t)\\
&\quad \geqq \left(\left(\frac{A^{1-B}}{6\times 8^B}\right)^{1/(3B-2)} h(\zeta_1)\right)^{(3B-1)} \geqq \left(\left(\frac{A^{1-B}}{6\times 8^B}\right)^{1/(3B-2)} \frac{e^8}{2}\right)^{(3B-1)^{t-1}}.
\end{aligned} \tag{69}$$

Together with $A \geqq 1$ this implies that

$$\begin{aligned}
1.538^{t-1} = (3B-1)^{t-1} &< \frac{335 - \dfrac{\log 6 + B\log 8}{3B-2} + \left(48 + \dfrac{1-B}{3B-2}\right)\log A}{8 - \log 2 - \dfrac{\log 6 + B\log 8}{3B-2} + \dfrac{1-B}{3B-2}\log A}\\
&\leqq \frac{328.4 + 48.29\log A}{0.7 + 0.2\log A} \leqq \frac{328.4}{0.7} \leqq 469.2.
\end{aligned}$$

Therefore, $t<1+\log 469.2/\log\ 1.538=15.28\ldots$, i.e. $t\leqq 15$. We infer that the total number of $\zeta\in\mathscr{V}^0$ which satisfy a fixed system (49) and for which $h(\zeta)\geqq e^8/2$ is at most 25.

By Lemma 5, every $\zeta\in\mathscr{V}^0$ satisfies one of at most

$$3^s R(0.846)^{s-1}\leqq 3^s(49/3)^{s-1}\leqq \tfrac{2}{25}\times 7^{2s}$$

systems (49). Moreover, every solution (x,y) of (5) is completely determined by $\zeta(x,y)$. Together with (36) and the fact that roots of unity have absolute height equal to 1, this implies the following lemma, which might have some interest in itself.

Lemma 9. *Let K be an algebraic number field, let λ,μ be non-zero elements of K and let S be a finite set of primes on K of cardinality s which contains the infinite primes. Then the equation*

$$\lambda x+\mu y=1 \quad \textit{in } S\textit{-units } x,y \tag{5}$$

has at most

$$2\times 7^{2s}$$

solutions with $h(\lambda x/\mu y)\geqq e^8$.

We shall now give an upper estimate for the number of solutions of (5) with $h(\lambda x/\mu y)<e^8$. Here λ,μ and also K,S,s have the same meaning as in Lemma 9. Moreover, K has degree m.

As is well-known, the group of S-units is the direct product of s multiplicative cyclic groups, $G_1,\ldots,G_s$ say, one of which is finite. Let n be a positive integer which will be specified later. Then each factor group G_i/G_i^n has order at most n. Hence for every S-unit ε there are S-units $\varepsilon',\varepsilon''$ with $\varepsilon=\varepsilon'\varepsilon''^n$, where ε' can be chosen from a set of cardinality at most n^s. We infer that for every solution (x,y) of (5) there are an S-unit z and an element ω of K belonging to a fixed set of cardinality at most n^s which does not depend on x,y such that $\lambda x/\mu y=\omega z^n$. Let ω be a fixed element of this set and let θ be a fixed n-th root of ω. By Lemma 1, the number of non-zero z in K with $h(\theta z)<e^{8/n}$ is at most $5(2e^{24/n})^m$. Since every solution (x,y) of (5) is completely determined by ω and z, this implies that (5) has at most

$$5n^s(2e^{24/n})^m \tag{70}$$

solutions with $h(\lambda x/\mu y)<e^8$. By a combination of (70) with $n=49$ and Lemma 9, we obtain that the total number of solutions of (5) is at most

$$(5(2e^{24/49})^m+2)\,7^{2s}\leqq 3\times 7^{m+2s}.$$

References

1. Beukers, F.: The generalised Ramanujan-Nagell equation. Thesis, Leiden 1979
2. Beukers, F.: On the generalized Ramanujan-Nagell equation. I. Acta Arith. **38**, 389–410 (1980/81)
3. Beukers, F.: On the generalized Ramanujan-Nagell equation. II. Acta Arith. **39**, 113–123 (1981)
4. Choodnovsky, G.V.: The Gel'fond-Baker method in problems of diophantine approximation. Coll. Math. Soc. János Bolyai **13**, 19–30 (1974)

5. Delone, B.N.: Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante. Math. Z. **31**, 1-26 (1930)
6. Evertse, J.H.: On the equation $a x^n - b y^n = c$. Compositio Math. **47**, 289-315 (1982)
7. Evertse, J.H.: On the representation of integers by binary cubic forms of positive discriminant. Invent. Math. **73**, 117-138 (1983)
8. Evertse, J.H.: Upper bounds for the numbers of solutions of diophantine equations. MC-tract, Mathematisch Centrum, Amsterdam 1983
9. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349-366 (1983)
10. Györy, K.: On the number of solutions of linear equations in units of an algebraic number field. Comm. Math. Helv. **54**, 583-600 (1979)
11. Lewis, D.J., Mahler, K.: Representation of integers by binary forms. Acta Arith. **6**, 333-363 (1960/61)
12. Mahler, K.: Zur Approximation algebraischer Zahlen. I. Über den größten Primteiler binärer Formen. Math. Ann. **107**, 691-730 (1933)
13. Mahler, K.: Zur Approximation algebraischer Zahlen. II. Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen. Math. Ann. **108**, 37-55 (1933)
14. Mahler, K.: On Thue's theorem. Austral. Nat. Un. Math. Res. Rep. **24**, (1982); Math. Scand. in press (1984)
15. Mordell, L.J.: Diophantine equations. London: Academic Press 1969
16. Nagell, T.: Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante. Math. Z. **28**, 10-29 (1928)
17. Nagell, T.: The diophantine equation $x^2 + 7 = 2^n$, Norsk Mat. Tidsskr. **30**, 62-64 (1948); Ark. Mat. **4**, 185-187 (1960)
18. Parry, C.J.: The p-adic generalisation of the Thue-Siegel theorem. Acta Math. **83**, 1-99 (1950)
19. Ramanujan, S.: Collected papers: p. 327. Chelsea Publ. Co., New York (1962)
20. Siegel, C.L.: Die Gleichung $ax^n - by^n = c$. Math. Ann. **114**, 57-68 (1937); Gesammelte Abhandlungen, vol. 2. pp. 8-19. Berlin-Heidelberg-New York: Springer 1966
21. Silverman, J.H.: Integer points and the rank of Thue elliptic curves. Invent. Math. **66**, 395-404 (1982)
22. Silverman, J.H.: The Thue equation and height functions. In: Bertrand, D., Waldschmidt, M. eds. Approximations diophantienne et nombres transcendents. Coll. Luminy 1982, pp. 259-270. Boston-Basel-Stuttgart: Birkhäuser 1983
23. Silverman, J.H.: Quantitative results in diophantine geometry. Preprint, Massachusetts Inst. of Techn.
24. Tartakovskii, V.A.: A uniform estimate of the number of representations of unity by a binary form of degree $n \geqq 3$. Dokl. Akad. Nauk. SSSR **193**: (1970) (Russian); Soviet Math. Dokl. **11**, 1026-1027 (1970)
25. Thue, A.: Berechnung aller Lösungen gewisser Gleichungen von der Form $a x^r - b y^r = f$, Vid. Selsk. Skrifter I. mat-naturv. Kl., Christiania 1918, Nr. 4; Selected Mathematical Papers of Axel Thue, pp. 565-572. Oslo, Bergen, Tromsø (1977)

Oblatum 25-VIII-1983