9

S-UNIT EQUATIONS AND THEIR APPLICATIONS

J.-H. Evertse[1], K. Győry[2], C. L. Stewart[3], R. Tijdeman

Contents

§0. Introduction.

This paper gives a survey of the remarkable results on S-unit equations and their applications which have been obtained, mainly in the

[1] Research supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.)

[2] Research supported in part by the Hungarian National Foundation for Scientific Research Grant 273

[3] Research supported in part by Grant $A3528$ from the Natural Sciences and Engineering Research Council of Canada

last five years. It is impossible to cover all applications within the scope of this paper, but the wide range of applications illustrates how fundamental these developments are. The developments are still going on and several of the mentioned results are new.

In §1 we introduce notation which will be used throughout the paper. In §§2–5 five theorems on S-unit equations are treated. The Main Theorem on S-Unit Equations (Theorem 1), which deals with general S-unit equations

$$x_0 + x_1 + \ldots + x_n = 0 \quad \text{in } S\text{-units } x_0, x_1, \ldots, x_n, \tag{0.1}$$

is stated in §2 and its deduction from the Subspace Theorem is sketched in §4. Theorem 1′ is a version of Theorem 1 dealing with arbitrary finitely generated multiplicative subgroups of $\mathbf{C} \setminus \{0\}$. Theorems 2–5 stated in §3 deal with S-unit equations in two variables,

$$\alpha_1 x_1 + \alpha_2 x_2 = 1 \quad \text{in } S\text{-units } x_1, x_2 \tag{0.2}$$

where α_1 and α_2 are constants. Theorem 2 gives an upper bound for the number of solutions of (0.2). A proof of it, this time not derived from the theory of hypergeometric functions, but from a variant of Roth's theorem, is given in §4. Theorem 3 was proved during the conference in Durham. It says that apart from finitely many equivalence classes of equations only, equation (0.2) has at most two solutions. Its proof is sketched in §5. Theorems 1–3 are ineffective and hence the methods do not yield upper bounds for the sizes of the solutions. In contrast, Theorems 4 and 5 are effective. They are based on Baker's method concerning linear forms in logarithms of algebraic numbers. Theorem 4 gives an upper bound for the sizes of the solutions of (0.2). Theorem 5, which is new, is an effective, but weaker version of Theorem 3. The proofs of Theorems 4 and 5 in the rational case are given in §5. The formulations of Theorems 1–5 in the case of rational integers are given as Corollaries 1.3 and 2–5. Both §5 and §6 deal with rational integers and can be read independently of the rest of the paper. They are meant for those readers who want to understand and apply the results on S-unit equations for rational integers only.

In §§6–9 applications of Theorems 1–5 are given which are more or less straightforward. Theorems 6 and 7 in §6 are new. Theorem 7 resolves a conjecture of D. Newman on the number of representations of an integer in the form $2^\alpha 3^\beta + 2^\gamma + 3^\delta$ where α, β, γ and δ are non-negative integers. Theorem 8 in §7 is also new. It gives a result on groups which has been applied in the study of ellipticity problems in group theory.

Theorem 9 in §8 is an extension of a result of Evertse [20]. It implies several known results on recurrence sequences as is shown in §§8, 9.

The more classical applications of S-unit equations are mentioned in §§10–12. There is a strong connection between the theory of S-unit equations and the theory of decomposable form equations (which covers the Thue-Mahler equations). The two theories are in fact equivalent (cf. §11). Siegel proved the finiteness of the number of solutions of unit equations in two variables via Thue equations. The opposite approach has also proved applicable, even for decomposable form equations in more than two unknowns. There are several consequences of unit equations which can be deduced via complicated systems of unit equations. All these results can be proved by using the same "intermediate" results, Theorems 10 and 11, which are applications of Theorems 4 and 2 and are presented in §10. The versions of Theorems 10 and 11 presented here had only appeared in Hungarian [42] before. These results are improvements of results in Győry [35]. Theorem 12 in §10 is an application of Theorem 11 to irreducibility of polynomials. Theorems 13–15 in §11 provide general finiteness results for decomposable form equations which imply several known results on Thue equations, Thue-Mahler equations, norm form equations, discriminant form equations and index form equations. Theorems 16–18 in §12 give finiteness results for algebraic integers and polynomials with a given non-zero discriminant. They have many applications in algebraic number theory.

Finally, in §13, a remarkable application of the Main Theorem on S-unit Equations to algebraic independence of function values due to Nishioka [60, 61] is mentioned. Nishioka solved in this way a conjecture of D. W. Masser and a more general problem which had been open for several years.

For more information on S-unit equations and their applications, see [25], [36], [51] and [77].

The authors thank the organisers of the conference in Durham, A. Baker and R. C. Mason, for the excellent opportunity offered to the authors to discuss mathematics and to work together. They further thank F. Beukers and P. Erdös for valuable discussions and Lianxiang Wang for remarks on an early draft of the paper.

§1. Notation and simple observations

The notation introduced in this paragraph will be used throughout the paper without further mention. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. Let d, h_K, r_K and R_K denote the degree, class

number, unit rank and regulator of K, respectively. Let M_K be the set of *places* on K (i.e. equivalence classes of multiplicative valuations on K). A place v is called *finite* if v contains only non-archimedean valuations and *infinite* otherwise. K has only finitely many infinite places. The rational number field $\mathbf{Q}$ has only one infinite place ∞, containing the ordinary absolute value, and a finite place for each prime number p. In ∞ we choose a representative $|\,.\,|_\infty$ which is equal to the ordinary absolute value. In the place corresponding to p (which is also denoted by p) we choose the valuation $|\,.\,|_p$ such that $|p|_p = p^{-1}$ as representative. In each place v of M_K we choose a valuation $|\,.\,|_v$ as follows. Let $p \in M_{\mathbf{Q}}$ be such that $v|p$ (i.e. the restrictions to $\mathbf{Q}$ of the valuations in v belong to p; in particular v is infinite if and only if $v|\infty$). We put $d_v = [K_v : \mathbf{Q}_p]$, where K_v and $\mathbf{Q}_p$ denote the completions of K at v and $\mathbf{Q}$ at p, respectively. In v we choose the valuation $|\,.\,|_v$ satisfying

$$|\alpha|_v = |\alpha|_p^{d_v/d} \quad \text{for each } \alpha \text{ in } \mathbf{Q}. \tag{1.1}$$

By these choices for the valuations we have the *Product Formula*

$$\prod_{v \in M_K} |\alpha|_v = 1 \quad \text{for } \alpha \in K^*. \tag{1.2}$$

Here and elsewhere we put $V^* = V \setminus \{0\}$ for any set V. Put

$$s(v) = \begin{cases} 0 & \text{if } v \text{ is a finite place,} \\ 1/d & \text{if } K_v = \mathbf{R}, \\ 2/d & \text{if } K_v = \mathbf{C}. \end{cases}$$

Then $\sum_{v \in M_K} s(v) = 1$ and

$$|\alpha_1 + \ldots + \alpha_r|_v \le r^{s(v)} \max(|\alpha_1|_v, \ldots, |\alpha_r|_v) \tag{1.3}$$
$$\text{for } \alpha_1, \ldots, \alpha_r \in K \text{ and } v \in M_K.$$

The *height function* $h(\,.\,)$ on K is defined by

$$h(\alpha) = \prod_{v \in M_K} \max(1, |\alpha|_v) \qquad \text{for } \alpha \in K.$$

This height depends only on α, and not on the choice of the algebraic number field K. The following elementary properties of h can be proved.

$$\begin{aligned} h(\alpha^{-1}) &= h(\alpha) \qquad \text{for } \alpha \in K^*, \\ h(\alpha_1 \ldots \alpha_r) &\le h(\alpha_1) \ldots h(\alpha_r) \qquad \text{for } \alpha_1, \ldots, \alpha_r \in K, \\ h(\alpha_1 + \ldots + \alpha_r) &\le r h(\alpha_1) \ldots h(\alpha_r) \qquad \text{for } \alpha_1, \ldots, \alpha_r \in K, \\ h(\alpha) &= 1 \qquad \text{if and only if } \alpha = 0 \text{ or a root of unity.} \end{aligned} \tag{1.4}$$

Other heights of algebraic numbers α which are often used in diophantine approximation, are $\overline{|\alpha|}$ (the maximum of the absolute values of the conjugates of α over $\mathbb{Q}$) and $H(\alpha)$ (the maximum of the absolute values of the coefficients of the minimal polynomial of α over $\mathbb{Z}$). If α is an algebraic number of degree m, then

$$\begin{aligned} \overline{|\alpha|} \le \big(h(\alpha)\big)^m \le \overline{|\alpha|}^m, &\quad \text{if } \alpha \text{ is an algebraic integer,} \\ 2^{1-m}H(\alpha) \le \big(h(\alpha)\big)^m \le \sqrt{m+1}\,H(\alpha), &\quad \text{if } \alpha \text{ is an arbitrary algebraic number.} \end{aligned} \tag{1.5}$$

The first inequality is obvious, while the second follows from Lang [51] Ch. 3, Theorem 2.8. Consequently, for each positive number C there are only finitely many α in K with $h(\alpha) \le C$ and these belong to an effectively determinable finite subset of K.

Let S_∞ be the set of all infinite places on K, and let S be a finite subset of M_K containing S_∞. Let s denote the cardinality of S. An element α of K is called an *S-unit* if $|\alpha|_v = 1$ for each $v \notin S$ (i.e. $v \in M_K \setminus S$). The S-units form a finitely generated multiplicative group of rank $s-1$ which is denoted by U_S. If S contains no finite places, then U_S is just the group of units, U_K, of $\mathcal{O}_K$. Note that if $\alpha \in U_S$, then, by (1.2) and (1.4),

$$\prod_{v\in S} |\alpha|_v = 1, \qquad h(\alpha) = \prod_{v\in S} \max(1, |\alpha|_v). \tag{1.6}$$

Suppose that the finite places in S correspond to the prime ideals $\wp_1, \dots, \wp_t$ and that these prime ideals lie above rational primes not exceeding $P(\ge 2)$. An element α of K is called an *S-integer* if $|\alpha|_v \le 1$ for all $v \notin S$. The S-integers form a ring which is denoted by $\mathcal{O}_S$. If $\alpha \in K$ then the principal ideal (α) can be written uniquely as a product of two ideals $\mathcal{A}_1$, $\mathcal{A}_2$ where $\mathcal{A}_1$ is composed of $\wp_1, \dots, \wp_t$ and $\mathcal{A}_2$ is composed solely of prime ideals different from $\wp_1, \dots, \wp_t$. We define $N_S(\alpha)$, which is sometimes called the *S-norm* of α, by $N_S(\alpha) = N_{K/\mathbb{Q}}(\mathcal{A}_2)$. This function N_S has several useful properties. We have

$$N_S(\alpha) = \Big(\prod_{v\in S} |\alpha|_v\Big)^d \qquad \text{for all } \alpha \text{ in } K.$$

Further N_S is multiplicative, $N_S(\alpha) \ge 1$ if $\alpha \in \mathcal{O}_S$, and $N_S(\alpha) = 1$ if $\alpha \in U_S$. Finally we note that if $S = S_\infty$, then $N_S(\alpha) = \big|N_{K/\mathbb{Q}}(\alpha)\big|$.

We shall deal with the (*general homogeneous*) *S-unit equation*

$$\alpha_0 x_0 + \ldots + \alpha_n x_n = 0 \quad \text{in } x_0, x_1, \ldots, x_n \in U_S \tag{1.7}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_n \in K^*$. In the study of this equation we can identify pairwise linearly dependent non-zero points in K^{n+1}, that is, consider solutions in the n-dimensional projective space $\mathbf{P}^n(K)$. Points in $\mathbf{P}^n(K)$, so-called *projective points*, are denoted by $X = (x_0 : x_1 : \ldots : x_n)$, where the homogeneous coordinates are in K, and are determined up to a multiplicative factor in K. Alternatively we can divide all coefficients α_i by α_0 and all variables x_i by $-x_0$ and study the *inhomogeneous* S-unit equation

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 1 \qquad \text{in } x_1, x_2, \ldots, x_n \in U_S.$$

Since U_S is finitely generated, S-unit equations are in fact exponential diophantine equations. Most of our attention will be focussed on the (*inhomogeneous*) *S-unit equation in two variables*,

$$\alpha_1 x + \alpha_2 y = 1 \qquad \text{in } x, y \in U_S. \tag{1.8}$$

It is implicit in the work of Mahler [56] and explicitly stated by Lang [50] that (1.8) has only finitely many solutions. Denote the number of solutions of (1.8) by $\nu(\alpha_1, \alpha_2)$.

In §3 we shall give upper bounds for $\max\big(h(x), h(y)\big)$ and for $\nu(\alpha_1, \alpha_2)$ when x, y satisfy (1.8). In view of the symmetry in (1.7) we can distinguish equivalence classes of equations such that the sets of solutions of two equations from the same class are isomorphic: two tuples $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ and $(\beta_0, \beta_1, \ldots, \beta_n)$ in $(K^*)^{n+1}$ (resp. the corresponding homogeneous S-unit equations) are called *S-equivalent* if there is a permutation σ of $\{0, 1, \ldots, n\}$, a $\lambda \in K^*$ and S-units $\epsilon_0, \epsilon_1, \ldots, \epsilon_n$ such that

$$\beta_i = \lambda \epsilon_i \alpha_{\sigma(i)} \qquad \text{for } i = 0, , \ldots, n.$$

Observe that the solution $(\epsilon_{\sigma^{-1}(0)}\tilde{x}_0 : \epsilon_{\sigma^{-1}(1)}\tilde{x}_1 : \ldots : \epsilon_{\sigma^{-1}(n)}\tilde{x}_n)$ of $\alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_n x_n = 0$ corresponds to the solution $(\tilde{x}_{\sigma(0)} : \tilde{x}_{\sigma(1)} : \ldots : \tilde{x}_{\sigma(n)})$ of $\beta_0 x_0 + \beta_1 x_1 + \ldots + \beta_n x_n = 0$ so that there is indeed a simple bijection between the solutions of both equations. Transferring the concept of S-equivalence to the inhomogeneous case, we find that the S-equivalence class of equation (1.8) consists of the following six classes of inhomogeneous S-unit equations:

$$\alpha_1 \epsilon_1 x + \alpha_2 \epsilon_2 y = 1,$$

$$\begin{aligned}
\alpha_1^{-1}\alpha_2\epsilon_1 x + \alpha_1^{-1}\epsilon_2 y &= 1,\\
\alpha_2^{-1}\epsilon_1 x + \alpha_1\alpha_2^{-1}\epsilon_2 y &= 1,\\
\alpha_2\epsilon_1 x + \alpha_1\epsilon_2 y &= 1,\\
\alpha_1^{-1}\epsilon_1 x + \alpha_1^{-1}\alpha_2\epsilon_2 y &= 1,\\
\alpha_1\alpha_2^{-1}\epsilon_1 x + \alpha_2^{-1}\epsilon_2 y &= 1,
\end{aligned} \tag{1.9}$$

where ϵ_1 and ϵ_2 are arbitrary S-units.

We now show that if U_S is infinite (which is the case if $s > 1$), then there are infinitely many S-equivalence classes of S-unit equations with at least two distinct solutions. Let $\xi \in U_S$, $\xi \neq 1$. For each η in U_S with $\eta \neq \xi$, $\eta \neq 1$ we define α_1, α_2 by

$$\alpha_1 = \frac{\eta - 1}{\eta - \xi}, \qquad \alpha_2 = \frac{\xi - 1}{\xi - \eta}.$$

Then (1.1) and (ξ, η) are distinct solutions of $\alpha_1 x + \alpha_2 y = 1$ in $x, y \in U_S$. The equations $\alpha_1 x + \alpha_2 y = 1$ constructed in this way must belong to infinitely many S-equivalence classes, since the number of equations constructed in this way is infinite, but each S-equivalence class contains only finitely many equations with solution (1,1). This last fact follows from applying Lang's result to (1.9) with $x = y = 1$, α_1 and α_2 fixed and ϵ_1, $\epsilon_2 \in U_S$ variables.

§2. The General Case: The Main Theorem on S-Unit Equations

In this paragraph we deal with equations (1.7). The results in this paragraph are all based on p-adic versions of the Thue-Siegel-Roth-Schmidt method. Both Schlickewei [68], [69], [70] and Dubois and Rhin [14] gave such a p-adic version and used it to prove that, for any given set of prime numbers $T = \{p_1, \ldots, p_t\}$, the equation

$$x_0 + x_1 + \ldots + x_n = 0 \qquad \text{in } x_0, x_1, \ldots, x_n \in \mathbf{Z} \tag{2.1}$$

has only finitely many solutions x_0, x_1, $\ldots$, x_n each composed of primes from T such that

$$\gcd(x_i, x_j) = 1 \qquad \text{for } i \neq j. \tag{2.2}$$

Actually they proved the following more general result. Let Δ, δ be real constants with $\Delta > 0$, $0 \leq \delta < 1$. Then the number of solutions of (2.1) satisfying (2.2) and

$$\prod_{k=0}^{n}\Big(|x_k| \prod_{p \in T} |x_k|_p\Big) \leq \Delta\big(\max(|x_0|, |x_1|, \ldots, |x_n|)\big)^{\delta} \tag{2.3}$$

is finite. The restriction of pairwise coprimality may be too severe, but some restriction is needed in view of the equation $x_0 + x_1 + \ldots + x_5 = 0$ with $T = \{2, 3\}$ which has the solution $x_0 = 2^{k+1}$, $x_1 = 2^k$, $x_2 = -3 \cdot 2^k$, $x_3 = 2^3 3^\ell$, $x_4 = 3^\ell$, $x_5 = -3^{\ell+2}$ for all positive integers k, ℓ.

Van der Poorten and Schlickewei [67] proved that (2.1) has only finitely many solutions $x_0, x_1, \ldots, x_n$ each composed of primes from T such that

$$\gcd(x_0, \ldots, x_n) = 1 \text{ and no proper non-empty subsum}$$
$$x_{i_1} + \ldots + x_{i_k} \text{ of } x_0 + x_1 + \ldots + x_n \text{ vanishes.} \quad (2.4)$$

Condition (2.4) is necessary and sufficient. Their result holds for algebraic number fields (cf. Corollary 1.1) and even for finitely generated subgroups of $\mathbf{C}^*$ (cf. Theorem 1'), but they have not yet published the complete proofs of their claim. Independently of van der Poorten and Schlickewei, Evertse [20] proved that (2.1) has only finitely many solutions satisfying (2.3) and (2.4) and extended this result to algebraic number fields. By using these results of van der Poorten and Schlickewei and Evertse, a further extension for subgroups of $\mathbf{C}^*$ of finite rank was given by Laurent [52].

To state Evertse's result in full generality we need some more notation. For any projective point $\mathbf{x} = (x_0 : x_1 : \ldots : x_n)$ in $\mathbf{P}^n(K)$ and for any $v \in M_K$ we put $|\mathbf{x}|_v = \max(|x_0|_v, \ldots, |x_n|_v)$. We define the *projective height*[1] of $\mathbf{x}$ as

$$\mathcal{H}(\mathbf{x}) = \prod_{v \in M_K} |\mathbf{x}|_v. \quad (2.5)$$

This height is well-defined, since it is independent of the multiplicative factor by the Product Formula. There is a simple relation between the height h and the projective height $\mathcal{H}$, namely

$$h(\alpha) = \mathcal{H}(1 : \alpha) \qquad \text{for } \alpha \in K. \quad (2.6)$$

Let, as always, S be a finite subset of M_K containing all infinite places. Let Δ, δ be real constants with $\Delta > 0$, $\delta \geq 0$. A projective point $\mathbf{x} \in \mathbf{P}^n(K)$ is called (Δ, δ, S)-*admissible*[1] if its homogeneous coordinates can be chosen such that

[1] The valuation $\|.\|_v$ in [20] is not the same as the valuation $|.|_v$. The relation between them is given by $\|\alpha\|_v = |\alpha|_v^d$ for $\alpha \in K$. Hence the notation of (Δ, δ, S)-admissibility here corresponds with (Δ^d, δ, S)-admissibility in Evertse's paper.

(i) all x_k are S-integers

and

(ii) $\prod_{v\in S}\prod_{k=0}^{n}|x_k|_v \leq \Delta(\mathcal{H}(\mathbf{x}))^{\delta}$.

Clearly the homogeneous coordinates of $(1,0,S)$-admissible projective points can all be chosen to be S-units.

Theorem 1. (The Main Theorem on S-Unit Equations for Algebraic Number Fields) (Evertse [20]).

Let $\Delta > 0$, $0 \leq \delta < 1$. *There are only finitely many* (Δ,δ,S)-*admissible projective points* $\mathbf{x} = (x_0 : x_1 : \ldots : x_n) \in \mathbf{P}^n(K)$ *satisfying*

$$x_0 + x_1 + \ldots + x_n = 0 \tag{2.7}$$

but

$x_{i_1} + \ldots + x_{i_k} \neq 0$ *for each proper, non-empty subset*

$$\{i_1,\ldots,i_k\} \text{ of } \{0,1,\ldots,n\} \tag{2.8}$$

We express (2.8) succinctly by saying that no subsum of $x_0 + \ldots + x_n$ vanishes. When we use the word 'subsum' we exclude the full and empty sum.

For general homogeneous S-unit equations (1.7) we derive the following consequence of Theorem 1.

Corollary 1.1. *Let* $\alpha_0, \alpha_1, \ldots, \alpha_n \in K^*$. *There are only finitely many projective points* $\mathbf{x} = (x_0 : x_1 \ldots : x_n) \in \mathbf{P}^n(K)$ *with* $x_0, x_1, \ldots, x_n \in U_S$ *such that* $\alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_n x_n = 0$, *but no subsum of* $\alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_n x_n$ *vanishes.*

This implies for inhomogeneous S-unit equations:

Corollary 1.2. *Let* $\alpha_1, \alpha_2, \ldots, \alpha_n \in K^*$. *There are only finitely many tuples* $(x_1,\ldots,x_n) \in U_S^n$ *such that* $\alpha_1 x_1 + \ldots + \alpha_n x_n = 1$, *but no subsum of* $\alpha_1 x_1 + \ldots + \alpha_n x_n$ *vanishes.*

By a specialisation argument, Theorem 1 can be extended as follows.

Theorem 1' (The Main Theorem on S-Unit Equations for Groups) (Van der Poorten and Schlickewei [67]).

Let G be a finitely generated multiplicative subgroup of $\mathbf{C}^*$. There are only finitely many projective points $\mathbf{x} = (x_0 : x_1 : \ldots : x_n) \in \mathbf{P}^n(G)$ satisfying (2.7) *and* (2.8).

Laurent [52] proved Theorem 1′ in the more general case of multiplicative subgroups of $\mathbf{C}^*$ of finite rank. He used it to prove a special case of a conjecture of S. Lang which is an assertion on commutative algebraic groups.

§3. Upper bounds in the two variables case

In this section we deal with the S-unit equation in two variables

$$\alpha_1 x + \alpha_2 y = 1 \qquad \text{in } x, y \in U_S, \tag{1.8}$$

where $\alpha_1, \alpha_2 \in K^*$. It is implicit in the work of Siegel [78, 79] that equations of the form (1.8) have only finitely many solutions in units x, y, and implicit in the work of Mahler [56] that (1.8) has only finitely many solutions (in S-units x, y). As remarked before, Lang [50] proved this result explicitly. Siegel developed the so-called Thue-Siegel method involving hypergeometric functions. By combining his method with ideas of Mahler about p-adic approximation of algebraic numbers, Evertse proved the following result on the number of solutions $\nu(\alpha_1, \alpha_2)$ of (1.8).

Theorem 2. (Evertse [19]).

$$\nu(\alpha_1, \alpha_2) \leq 3 \times 7^{d+2s}.$$

This bound has the remarkable feature of being dependent only on the degree of K and the cardinality of S. Theorem 2 is a considerable improvement and generalisation of a result of Lewis and Mahler [54] who derived an upper bound for $\nu(1,1)$ in the rational case which depends on the primes involved in S and not only on their number. Independently of Evertse, and by a different method, Silverman [81] showed $\nu(1,1) \leq C \times 2^{20s}$. Here and elsewhere C is a constant, the value of which may be different at each occurrence. Later, Evertse and Győry [22] derived an upper bound for the number of solutions of (1.8) independent of α_1 and α_2 in the general case that the variables x, y belong to a finitely generated multiplicative subgroup of $\mathbf{C}^*$.

The dependence of Evertse's bound on the degree of K and the cardinality of S is necessary. Nagell [59] proved that for $d \geq 5$ there exists a number field K of degree d such that $x + y = 1$ has at least

$3(2d-3)$ solutions in units x, y of K. Erdős, Stewart and Tijdeman [17] proved that in the case $K = \mathbb{Q}$ the equation $x + y = 1$ can have more than $\exp(Cs^{1/2}/\log s)$ solutions x, $y \in U_S$. This implies that the best improvement of Theorem 2 one can hope for is $\nu(\alpha_1, \alpha_2) \leq \exp(s^{1/2})$. According to a conjecture which Stewart presented during the conference, the exponent $\frac{1}{2}$ should be replaced by $\frac{2}{3}$. In great contrast to this result is the observation made during the conference that for most pairs α_1, α_2 we have $\nu(\alpha_1, \alpha_2) \leq 2$.

Theorem 3 (Evertse, Győry, Stewart, Tijdeman [26]).

There are only finitely many S-equivalence classes of equations (1.8) *with more than two solutions.*

As observed at the end of §1 there are infinitely many S-equivalence classes of equations (1.8) with two solutions. The proof of Theorem 3 is based on Corollary 1.1. Its principle will be explained in §5. Theorem 3 can be extended to finitely generated multiplicative subgroups of $\mathbb{C}^*$.

Up to now all the upper bounds we have mentioned were proved by ineffective methods. This has the important disadvantage that it is impossible to derive upper bounds for the solutions themselves or to decide from the proof that for given α_1, α_2 (1.8) has no more than two solutions. Skolem [83], using Skolem's method, and Cassels [9], using Gelfond's results, showed how certain classes of S-unit equations in rationals can be solved effectively, at least in principle. The important breakthrough was Baker's method for estimating linear forms in logarithms and its p-adic analogue by Coates. Implicitly in Coates' work on the Thue-Mahler equation [11] there are S-unit equations in two variables and upper bounds for their solutions. The first explicit mention of such an application is in Sprindzhuk [84]. Győry [34] worked out an explicit upper bound for the heights of the solutions of (1.8). We state his result in a slightly different and less precise form. To state his result we transform (1.8) into an equivalent equation. By multiplying α_1 and α_2 by the product of their denominators, (1.8) transforms into an equivalent equation of the form

$$\alpha_1 x + \alpha_2 y = \alpha_0 \qquad \text{in } x, y \in U_S \tag{3.1}$$

where $\alpha_1, \alpha_2, \alpha_0 \in \mathcal{O}_K \setminus \{0\}$.

Theorem 4 (Győry [34]). *Let $\epsilon > 0$. Every solution (x, y) of* (3.1) *satisfies*

$$\max\big(h(x), h(y)\big) < \exp\big(s^{C(K,\epsilon)s} P^{d+\epsilon} \log A\big) \tag{3.2}$$

where $A = \max\bigl(h(\alpha_1), h(\alpha_2), h(\alpha_0), 3\bigr)$ *and* $C(K, \epsilon)$ *is an expression, explicitly given in* [34], *involving the parameters* d, h_K, r_K *and* R_K *of* K *and* ϵ.

It is most likely that the right-hand side of (3.2) cannot be improved on in an essential way when we use the presently available estimates for linear forms in logarithms of algebraic numbers. However, if we assume that (3.1) has at least $s + 2$ solutions, then it is possible, after having replaced $(\alpha_1, \alpha_2, \alpha_0)$ by an appropriate S-equivalent triple, to derive a result similar to (3.2) with a bound independent of A. A first step in this direction was made by Győry. Recall the definition of $N_S(\alpha)$ given in §1. Győry [34] proved the following statement in a more precise form. Here and in the sequel we use $C(K)$ for an effectively computable number depending only on K which may have a different value at each occurrence.

Let $0 < \epsilon < 1$. *For each triple* $(\alpha_1, \alpha_2, \alpha_0)$ *of elements in* $\mathcal{O}_K \setminus \{0\}$ *with*

$$\min\bigl(N_S(\alpha_1), N_S(\alpha_2)\bigr) \leq N_S(\alpha_0)^{1-\epsilon} \tag{3.3}$$

such that (3.1) *has at least* $s + 3t + 1$ *solutions, we have*

$$N_S(\alpha_0) \leq \exp\left\{\epsilon^{-1} s^{C(K)s} P^{d+1} \log\frac{2}{\epsilon}\right\}.$$

An upper bound for $N_S(\alpha_0)$ *of the same form can be given if* $\max\bigl(\log N_S(\alpha_1), \log N_S(\alpha_2)\bigr) \leq \bigl(\log N_S(\alpha_0)\bigr)^{1-\epsilon}$ *and there are at least* $s + t + 1$ *solutions.*

There are infinitely many S-equivalence classes which have a representative satisfying (3.3), but there are also infinitely many S-equivalence classes which do not have such a representative. (If $p_1, \ldots, p_t$ are the rational primes in $\wp_1, \ldots, \wp_t$ and $P = p_1 \ldots p_t$, then for all sufficiently large positive integers a the triples $(Pa + 1, 2Pa - 1, 2Pa + 1)$ will be pairwise S-inequivalent and they do not satisfy (3.3).)

Recently we considerably relaxed Győry's conditions and moreover slightly improved upon the bound for the number of required solutions.

Theorem 5 (Evertse, Győry, Stewart, Tijdeman [26]). *For each* $(\alpha_1, \alpha_2, \alpha_0) \in (\mathcal{O}_K \setminus \{0\})^3$ *such that* (3.1) has at least $s + 2$ *solutions, there exists an* S*-equivalent triple* $(\beta_1, \beta_2, \beta_0) \in (\mathcal{O}_K \setminus \{0\})^3$ *such that*

$$\max\bigl(h(\beta_1), h(\beta_2), h(\beta_0)\bigr) \leq \exp\{s^{C(K)s} P^{d+1}\}. \tag{3.4}$$

Since there are only finitely many S-equivalence classes which have a representative satisfying (3.4) (cf. (1.5)), this result implies that (3.1)

has at most $s+1$ solutions for all but the finitely many S-equivalence classes determined by (3.4). It follows from Theorem 4 that the solutions of $\beta_1 x + \beta_2 y = \beta_0$ in $x, y \in U_S$ subject to (3.4) satisfy

$$\max\big(h(x), h(y)\big) \leq \exp\{s^{C(K)s} P^{2(d+1)}\}. \tag{3.5}$$

§4. On the proofs of Theorems 1 and 2

In this section we shall describe some ideas behind the proofs of Theorems 1 and 2.

Theorem 1 (the Main Theorem on S-Unit Equations) is a consequence of the Subspace Theorem of Schmidt and Schlickewei, stated below. We use the notation introduced in §§1, 2. By a *projective subspace* we shall mean a set of the type

$$\big\{\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbf{P}^n(K) : \ell_1(\mathbf{x}) = \ldots = \ell_r(\mathbf{x}) = 0\big\}$$

where $\ell_1, \ldots, \ell_r$ are linear forms in $K[X_0, \ldots, X_n]$.

Subspace Theorem. *Let K be an algebraic number field, S a finite set of places on K with $S_\infty \subseteq S$, and $n \geq 1$ an integer. For each v in S, let $\{\ell_{iv}\}_{i=0}^{n_v}$ be a collection of linear forms in $K[X_0, \ldots, X_n]$ of rank $n_v + 1$; thus $n_v \leq n$ for $v \in S$. Then for every $c > 0$ and $\epsilon > 0$, the solutions of the inequality*

$$\prod_{v \in S} \prod_{i=0}^{n_v} \frac{|\ell_{iv}(\mathbf{x})|_v}{|\mathbf{x}|_v} \leq c\mathcal{H}(\mathbf{x})^{-n-1-\epsilon} \quad \text{in } \mathbf{x} \in \mathbf{P}^n(K) \tag{4.1}$$

are contained in finitely many proper, projective subspaces of $\mathbf{P}^n(K)$.

This theorem was proved by Schmidt [73, 74] in case that S contains only infinite places, and by Schlickewei [69] in full generality.

We remark that Schlickewei's formulation of the Subspace Theorem is different from ours. Schlickewei considered the inequality

$$\prod_{v \in S} \prod_{i=0}^{n_v} \big|\ell_{iv}(\mathbf{x})\big|_v \leq c\|x\|^{-\epsilon} \quad \text{in } \mathbf{x} \in \mathcal{O}_K^{n+1} \tag{4.2}$$

where $\|\mathbf{x}\| = \max_{i,j} |\sigma_j(x_i)|$ and $\sigma_1, \ldots, \sigma_d$ are the different $\mathbb{Q}$-isomorphisms of K. Inequality (4.1) is easily reduced to an inequality

of type (4.2) and vice versa, by observing that there are positive integers c_1, c_2, c_3 depending on K only, such that each $\mathbf{x} \in \mathbf{P}^n(K)$ can be represented by homogeneous coordinates $(x_0 : x_1 : \ldots : x_n)$ for which

$$\begin{aligned} x_0, \ldots, x_n &\in \mathcal{O}_K, \\ N_{K/\mathbb{Q}}\big((x_0, \ldots, x_n)\big) &\leq c_1, \\ c_2\|\mathbf{x}\| \leq \mathcal{H}(\mathbf{x}) &\leq c_3\|\mathbf{x}\|. \end{aligned}$$

Sketch of proof of Theorem 1. We shall proceed by induction on n. For $n = 1$, Theorem 1 is trivial. Suppose that Theorem 1 has been proved for equations $x_0 + \ldots + x_{n'} = 0$ with $n' < n$ (induction hypothesis). Consider the equation

$$x_0 + x_1 + \ldots + x_n = 0 \text{ in } S\text{-integers } x_0, x_1, \ldots, x_n \tag{4.3}$$

satyisfying

$$\prod_{v \in S} \prod_{i=0}^{n} |x_i|_v \leq \Delta \mathcal{H}(\mathbf{x})^{1-\epsilon}, \tag{4.4}$$

where S is a finite subset of M_K containing all infinite places, $\Delta > 0$ and $\epsilon = 1 - \delta$. Now (4.4) can be rewritten as

$$\prod_{v \in S} \left(\frac{|x_0|_v \ldots |x_{n-1}|_v |x_0 + \ldots + x_{n-1}|_v}{|\tilde{\mathbf{x}}|^{n+1}} \right) \leq c\mathcal{H}(\tilde{\mathbf{x}})^{-n-\epsilon} \tag{4.5}$$

where $\tilde{\mathbf{x}} = (x_0 : \ldots : x_{n-1}) \in \mathbf{P}^{n-1}(K)$ and $c = n\Delta$. Consider the solutions of (4.5) with $|\tilde{\mathbf{x}}|_v = |x_{i(v)}|_v$, where $\big(i(v)\big)_{v \in S}$ is any fixed tuple of subscripts taken from $\{0, 1, \ldots, n-1\}$. For $v \in S$, let $\{\ell_{iv}\}_{i=0}^{n-1}$ be the set of linear forms

$$\{X_0, X_1, \ldots, X_{n-1}, X_0 + X_1 + \ldots + X_{n-1}\} \setminus \{X_{i(v)}\}.$$

Then (4.5) can be written as

$$\prod_{v \in S} \prod_{i=0}^{n-1} \frac{|\ell_{iv}(\tilde{\mathbf{x}})|_v}{|\tilde{\mathbf{x}}|_v} \leq c\mathcal{H}(\tilde{\mathbf{x}})^{-n-\epsilon}. \tag{4.6}$$

By the subspace Theorem, the solutions of (4.6) in $\tilde{\mathbf{x}} \in \mathbf{P}^{n-1}(K)$ are contained in finitely many proper projective subspaces of $\mathbf{P}^{n-1}(K)$. This

implies that the solutions of (4.3) satisfying (4.4) are contained in finitely many linear subspaces of K^{n+1} of the type

$$\{x \in K^{n+1} : \alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_{n-1} x_{n-1} = 0\}$$

where $\alpha_0, \ldots, \alpha_{n-1} \in K$ and $(\alpha_0, \ldots, \alpha_{n-1}) \neq (0, \ldots, 0)$. Fix $\alpha_0, \ldots, \alpha_{n-1}$, fix a non-empty subset J of $\{0, \ldots, n-1\}$, and consider all solutions of (4.3) satisfying

$$\sum_{j \in J} \alpha_j x_j = 0, \quad \text{but no subsum of } \sum_{j \in J} \alpha_j x_j \text{ vanishes.}$$

By the induction hypothesis, there is a finite number of tuples $(\beta_j)_{j \in J}$ such that each x_j $(j \in J)$ can be written as $x_j = \xi \beta_j$ where ξ is some S-integer. By substituting this into (4.3) we obtain

$$\Big(\sum_{j \in J} \beta_j\Big)\xi + \sum_{j \in \{0,\ldots,n\} \setminus J} x_j = 0.$$

By applying the induction hypothesis again we conclude that there are only finitely many possible projective solutions $(\xi : x_{i_1} : \ldots : x_{i_t})$ where $\{i_1, \ldots, i_t\} = \{0, \ldots, n\} \setminus J$. Combining this with the facts that the numbers of possible tuples $(\alpha_0, \ldots, \alpha_{n-1})$, sets J and tuples β_j $(j \in J)$ are finite, we obtain that the total number of solutions of (4.3) subject to (4.4) is finite. ∎

We shall now sketch the ideas behind the proof of Theorem 2. We use the notation of §§1–3. For $i = 1, 2, \ldots$ let $c_i(\ldots)$ denote effectively computable numbers depending only on the parameters written within the parentheses. Hence c_6 and c_{13} are absolute constants.

Equation (1.8) can be rewritten as

$$y_0 + y_1 + y_2 = 0 \text{ in } (y_0 : y_1 : y_2) \in \mathbf{P}^2(K) \quad \text{with } y_i/\nu_i \text{ } S\text{-units for } i = 0, 1, 2, \tag{4.7}$$

where $\nu_0, \nu_1, \nu_2 \in K^*$ are fixed. Put

$$A = \prod_{v \in S} |\nu_0 \nu_1 \nu_2|_v \times \prod_{v \notin S} \{\max(|\nu_0|_v, |\nu_1|_v, |\nu_2|_v)\}^3.$$

A straightforward computation shows

$$\prod_{v \in S} \frac{|y_0 y_1 y_2|_v}{\{\max(|y_0|_v, |y_1|_v, |y_2|_v)\}^3} = A\mathcal{H}(\mathbf{y})^{-3},$$

where $\mathbf{y} = (y_0 : y_1 : y_2)$. Let $\big(i(v)\big)_{v\in S}$ be subscripts such that $|y_{i(v)}|_v = \min\big(|y_0|_v, |y_1|_v, |y_2|_v\big)$. If $|y_{i(v)}|_v \le |y_{j(v)}|_v \le |y_{k(v)}|_v$ with $\big\{i(v), j(v), k(v)\big\} = \{1,2,3\}$, then $|y_{k(v)}|_v \le 2^{s(v)}|y_{j(v)}|_v$ by (1.3). Hence

$$\prod_{v\in S} \frac{|y_{i(v)}|_v}{|\mathbf{y}|_v} \le 2A\mathcal{H}(\mathbf{y})^{-3}. \tag{4.8}$$

One possible way to deal with inequalities of type (4.8) is to use a quantitative version of Roth's theorem of the type below. If $\ell(X_0, X_1) = \alpha_0 X_0 + \alpha_1 X_1$, we put $|\ell|_v = \max\big(|\alpha_0|_v, |\alpha_1|_v\big)$.

Roth's Theorem. *Let K be an algebraic number field of degree d. Let $S \subset M_K$ be a finite set of cardinality s, containing all infinite places. Let $C \ge 1$ be a constant. Let $F(X_0, X_1) \in \mathbf{Z}[X_0, X_1]$ be a binary form of degree m, of which the absolute values of the coefficients are at most M. Finally, let $\{\ell_v\}_{v\in S}$ be a set of linear forms in $K[X_0, X_1]$, all dividing F. Then the number of solutions of the inequality*

$$\prod_{v\in S} \frac{|\ell_v(\mathbf{x})|_v}{|\ell_v|_v |\mathbf{x}|_v} \le c\mathcal{H}(\mathbf{x})^{-2-\epsilon} \tag{4.9}$$

in $\mathbf{x} \in \mathbf{P}^1(K)$ with $\mathcal{H}(\mathbf{x}) \ge c_1(d, m, \epsilon)(C + M + 1)^{C_2(d,m,\epsilon)}$ is at most $c_3(d, m, \epsilon) \times \big(c_4(\epsilon)\big)^s$.

As far as we know, no explicit proof of this result has been published. In [51] Ch. 7, Lang proved that (4.9) has only finitely many solutions. It is possible to prove Roth's theorem above by making explicit all arguments in Lang's proof, and combining this with ideas of Davenport and Roth [13]. In [82] Theorem 2.1, Silverman stated and sketched a proof of a result which is equivalent to Roth's Theorem stated above.

Roth's Theorem is a quantitative version of the Subspace Theorem in the special case $n = 1$, $n_v = 0$ for $v \in S \setminus S_\infty$. It would be of great interest to derive a quantitative version of the same type for the general Subspace Theorem.

Using Roth's Theorem with $F(X_0, X_1) = X_0 X_1(-X_0 - X_1)$, it follows that inequality (4.8) has at most $c_5(d) \times c_6^s$ solutions with

$$\mathcal{H}(\mathbf{y}) \ge c_7(d)(2A)^{c_8(d)}.$$

Our purpose is to obtain an upper bound for the number of solutions of (4.8) which is independent of A. Below we state a "gap principle"

which enables us to derive such a bound. First we reduce (4.8) to a finite number of systems of inequalities

$$\frac{|y_{i(v)}|_v}{|\mathbf{y}|_v} \leq \left(2A\mathcal{H}(\mathbf{y})^{-3}\right)^{\Gamma_v} \qquad \text{for } v \in S, \tag{4.10}$$

where $\Gamma_v \geq 0$ for $v \in S$, $\sum_{v\in S}\Gamma_v = B$ for some B with $\frac{2}{3} < B < 1$, and the tuple $(\Gamma_v)_{v\in S}$ can be chosen from a set of cardinality at most $\left(c_7(B)\right)^s$. This can be achieved by taking a sufficiently fine grid of Γ_v's (cf. [19] Lemma 4).

Gap Principle. *Let* $\mathbf{y}^{(1)}$, $\mathbf{y}^{(2)}$ *be different solutions of* (4.7) *satisfying the same system of inequalities* (4.10), *and suppose that* $\mathcal{H}(\mathbf{y}^{(1)}) \leq \mathcal{H}(\mathbf{y}^{(2)})$. *Then*

$$\mathcal{H}(\mathbf{y}^{(2)}) \geq 2^{-B-1}A^{1-B}\left(\mathcal{H}(\mathbf{y}^{(1)})\right)^{3B-1}. \tag{4.11}$$

Proof. Let $\mathbf{y}^{(1)} = (y_0^{(1)} : y_1^{(1)} : y_2^{(1)})$, $\mathbf{y}^{(2)} = (y_0^{(2)} : y_1^{(2)} : y_2^{(2)})$. Put

$$\Delta_v = \frac{|y_i^{(1)}y_j^{(2)} - y_j^{(1)}y_i^{(2)}|_v}{|\mathbf{y}^{(1)}|_v \times |\mathbf{y}^{(2)}|_v} \qquad \text{for } v \in M_K,$$

where i, j are distinct elements of $\{0,1,2\}$. Obviously, Δ_v is independent of the choice of i, j. For $v \in S$, take $i = i(v)$, $j \neq i(v)$. Then, by (4.10), for $v \in S$,

$$\begin{aligned}\Delta_v &\leq 2^{s(v)} \max\left(\frac{|y_{i(v)}^{(1)}|_v}{|\mathbf{y}^{(1)}|_v}, \frac{|y_{i(v)}^{(2)}|_v}{|\mathbf{y}^{(2)}|_v}\right)\\ &\leq 2^{s(v)}\left(2A\mathcal{H}(\mathbf{y}^{(1)})^{-3}\right)^{\Gamma_v}.\end{aligned}$$

Hence

$$\begin{aligned}\prod_{v\in S}\Delta_v &\leq 2\left(2A\mathcal{H}(\mathbf{y}^{(1)})^{-3}\right)^{\sum_{v\in S}\Gamma_v} \qquad (4.12)\\ &= 2\left(2A\mathcal{H}(\mathbf{y}^{(1)})^{-3}\right)^{B}.\end{aligned}$$

For $v \notin S$ we have, on choosing i, j such that $|\nu_i|_v \leq |\nu_j|_v \leq |\nu_k|_v$ for $k \neq i, j$,

$$\begin{aligned}\Delta_v &\leq \frac{|\nu_i\nu_j|_v}{\{\max(|\nu_0|_v, |\nu_1|_v, |\nu_2|_v)\}^2}\\ &= \frac{|\nu_0\nu_1\nu_2|_v}{\{\max(|\nu_0|_v, |\nu_1|_v, |\nu_2|_v)\}^3}.\end{aligned}$$

Together with the Product Formula this shows that

$$\prod_{v \in M_K \setminus S} \Delta_v \leq A^{-1}.$$

By combining this with (4.12) and the Product Formula we obtain

$$\frac{1}{\mathcal{H}(\mathbf{y}^{(1)})\mathcal{H}(\mathbf{y}^{(2)})} = \prod_{v \in M_K} \Delta_v \leq 2^{1+B} A^{B-1} \mathcal{H}(\mathbf{y}^{(1)})^{-3B}.$$

This implies (4.11). ∎

Since in (4.11) the exponent of A is positive and that of $\mathcal{H}(\mathbf{y}^{(1)})$ is greater than one, the number of solutions of (4.10) with

$$\mathcal{H}(\mathbf{y}) < c_7(d)(2A)^{c_8(d)}$$

is bounded above by $c_9(B,d)$. We infer that the total number of solutions of (4.8) is at most $c_{10}(B,d)\big(c_{11}(B)\big)^s$. By choosing B appropriately and observing that equation (4.7) can be reduced to at most 3^s different inequalities (4.8), we conclude that the number of solutions of (4.7) is at most $c_{12}(d) \times c_{13}^s$.

We remark that it is possible to prove that (4.8) has at most $c_5(d) \times c_6^s$ solutions with $\mathcal{H}(\mathbf{y}) \geq c_7(d)(2A)^{c_8(d)}$ by techniques which are less powerful than Roth's (cf. [19], [21]).

§5. The rational case

We specialise the theorems of §§2, 3 to the case $K = \mathbb{Q}$. This paragraph can be read independently of §§1–4. The text between square brackets indicates the connection with the preceding paragraphs.

For any prime number p and any rational number α we define $|\alpha|_p = p^{-k}$ if $p^{-k}\alpha$ is the quotient of two rational integers both coprime to p. Let M denote the set of valuations on $\mathbb{Q}$ consisting of the absolute value $|.|$ and the valuation $|.|_p$ just defined for each prime number p. Then we have the *Product Formula*

$$\prod_{v \in M} |\alpha|_v = 1 \qquad \text{for all } \alpha \in \mathbb{Q}^*. \tag{5.1}$$

Here and elsewhere we put $V^* = V \setminus \{0\}$ for any set V. Furthermore, we define the height $h(\alpha)$ of α by

$$h(\alpha) = \prod_{v \in M} \max(1, |\alpha|_v). \tag{5.2}$$

Hence, if $\alpha = a/b$ with $a, b \in \mathbf{Z}$ and $\gcd(a,b) = 1$, then $h(\alpha) = \max(|a|, |b|)$. Note that, by (5.1),

$$h(\alpha) = h(\alpha^{-1}) = \prod_{v \in M} \min(1, |\alpha|_v)^{-1}. \tag{5.3}$$

Let $t \geq 2$. Let $T = \{p_1, \ldots, p_t\}$ be a set of prime numbers not exceeding P. Let S be the set of valuations $|.|, |.|_{p_1}, \ldots, |.|_{p_t}$. [Hence $s = t + 1$, the number of valuations in S.] By $v \notin S$ we mean $v \in M \setminus S$. For $\alpha \in \mathbf{Q}^*$ we write $\alpha = [\alpha]_S \{\alpha\}_S$ where $[\alpha]_S := \prod_{p \in T} |\alpha|_p^{-1}$ is the *T-part* of α and $\{\alpha\}_S := |\alpha| \prod_{p \in T} |\alpha|_p = \prod_{v \in S} |\alpha|_v$ is the *T-free part* of α. The set U_S of S-units consists of the rational numbers α with $\{\alpha\}_S = 1$. Hence every α in U_S is of the form $\pm p_1^{k_1} \ldots p_t^{k_t}$ with $k_1, \ldots, k_t \in \mathbf{Z}$. Put $\mathcal{S} = U_S \cap \mathbf{Z}$.

Since there are exactly two tuples $(x_0, \ldots, x_n)$ of rational integers with gcd 1 which correspond with a given projective point in $\mathbf{P}^n(\mathbf{Q})$, we have the following consequence of Theorem 1.

Corollary 1.3. *Let Δ, δ be real constants with $\Delta > 0$, $0 \leq \delta < 1$. Then there are only finitely many tuples $x = (x_0, x_1, \ldots, x_n)$ of rational integers such that*

$$x_0 + x_1 + \ldots + x_n = 0, \tag{5.4}$$

$$x_{i_1} + \ldots + x_{i_k} \neq 0 \tag{5.5}$$

for each proper, non-empty subset $\{i_1, \ldots, i_k\}$ of $\{0, 1, \ldots, n\}$,

$$\gcd(x_0, x_1, \ldots, x_n) = 1, \tag{5.6}$$

and

$$\prod_{j=0}^{n} \{x_j\}_S \leq \Delta \big(\max_{j=0,\ldots,n} |x_j| \big)^{\delta}. \tag{5.7}$$

We express (5.5) succinctly by saying that no subsum of $x_0 + x_1 + \ldots x_n$ vanishes. Taking $\Delta = 1$, $\delta = 0$ means requiring that $x_0, x_1, \ldots, x_n$ are all elements of $\mathcal{S}$. Obviously Corollary 1.3 generalises the result of Schlickewei [70] and Dubois and Rhin [14], mentioned at the beginning of §2, who required pairwise coprimality instead of (5.5) and (5.6).

The subsequent results deal with the case $n = 2$. Let $\nu(a, b, c)$ denote the number of solutions of the equation

$$ax + by = cz \quad \text{in } x, y, z \in \mathcal{S} \text{ with } \gcd(x, y, z) = 1, \tag{5.8}$$

where $a, b, c \in \mathbf{Z}^*$. Since every solution $x_1, x_2 \in U_S$ of $ax_1 + bx_2 = c$ corresponds to exactly two solutions of (5.8), the following result follows from Theorem 2.

Corollary 2. $\nu(a, b, c) \leq 6 \times 7^{2t+3}$.

Erdős, Stewart and Tijdeman [17] have proved that there exist sets S of arbitrarily large cardinality t for which $\nu(1, 1, 1) > \exp(Ct^{1/2} \log t)$. Here and elsewhere C is a constant, but the constant may have a different value at each occurrence.

We call a triple $(a, b, c) \in (\mathbf{Z}^*)^3$ *S-normalised* if a, b, c, p_1, ..., p_t are pairwise relatively prime and $0 < a \leq b \leq c$. [Then each S-equivalence class in $(\mathbf{Z}^*)^3$ contains exactly one S-normalised triple: Suppose $(a_0, a_1, a_2) \in (\mathbf{Z}^*)^3$. Put $\lambda = \gcd(a_0, a_1, a_2)$. Then (a_0, a_1, a_2) is S-equivalent with $(\{a_0/\lambda\}_S, \{a_1/\lambda\}_S, \{a_2/\lambda\}_S)$. Arrange the three numbers in the latter tuple in increasing order and call them a, b, c, respectively. Then (a, b, c) is the unique S-normalised triple in the S-equivalence class of (a_0, a_1, a_2).] The following result is an immediate consequence of Theorem 3.

Corollary 3. *There are only finitely many S-normalised triples $(a, b, c) \in (\mathbf{Z}^*)^3$ for which* (5.8) *has more than two solutions with positive z.*

Corollary 3 can be derived from Corollary 1.3 as follows. Let $(a, b, c) \in (\mathbf{Z}^*)^3$ be an S-normalised triple and suppose there are three distinct triples $(x_i, y_i, z_i) \in \mathcal{S}^3$ satisfying (5.8) and $z_i > 0$ for $i = 1, 2, 3$. Then we obtain

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix} = 0. \tag{5.9}$$

Note that the expression on the left-hand side does not change value if we permute x, y, z or subscripts 1, 2, 3 consistently. Furthermore, if $x_1y_2z_3 = x_2y_1z_3$, then $x_1y_2 = x_2y_1$, hence $x_1 = \pm x_2$, $y_1 = \pm y_2$ and therefore $z_1 = \pm z_2$. Since z_1 and z_2 are positive, we obtain

$$x_1y_2z_3 \neq x_2y_1z_3. \tag{5.10}$$

We first prove that there are only finitely many possible values for x_1z_2/x_2z_1 and y_1z_2/y_2z_1. To do so we apply Corollary 1.3 with $\Delta = 1$, $\delta = 0$ in the following way. If all conditions with the possible exception of (5.5) are satisfied, then there are only finitely many possibilities for the quotients x_i/x_j $(0 \leq i \leq j \leq n)$. If no (proper, non-empty) subsum of (5.9) vanishes, then Corollary 1.3 implies that there are only finitely many possibilities for $x_1y_3z_2/x_2y_3z_1 = x_1z_2/x_2z_1$ and $x_3y_1z_2/x_3y_2z_1 = y_1z_2/y_2z_1$. In this case our claim is correct, but we cannot be certain that no subsum vanishes. Suppose that there is a vanishing subsum. Then the complementary subsum vanishes too and we can apply Corollary 1.3 to both subsums. There are a great many cases to be considered, but, by using the symmetry and (5.10), their number can be brought down to five. The most difficult one is $x_1y_2z_3 + x_2y_3z_1 + x_3y_1z_2 = 0$, $x_2y_1z_3 + x_3y_2z_1 + x_1y_3z_2 = 0$. By Corollary 1.3 there are only finitely many possibilities for the quotients $x_3y_1z_2/x_1y_2z_3$, $x_2y_3z_1/x_1y_2z_3$, $x_1y_3z_2/x_2y_1z_3$ and $x_3y_2z_1/x_2y_1z_3$, hence for $x_1^2y_2z_2/x_2^2y_1z_1$ and $x_1y_2^2z_1/x_2y_1^2z_2$, whence for $x_1^3z_2^3/x_2^3z_1^3$ and $y_1^3z_2^3/y_2^3z_1^3$, whence for x_1z_2/x_2z_1 and y_1z_2/y_2z_1. The other cases can be treated similarly. We conclude that there are only finitely many possible values of x_1z_2/x_2z_1 and y_1z_2/y_2z_1, hence of x_1y_2/x_2y_1. Since (x_1, y_1, z_1) and (x_2, y_2, z_2) satisfy (5.8), we have

$$\frac{a}{c} = \frac{y_1z_2 - y_2z_1}{x_2y_1 - x_1y_2}, \qquad \frac{b}{c} = \frac{x_1z_2 - x_2z_1}{x_1y_2 - x_2y_1},$$

hence

$$\frac{ax_1}{cz_1} = \frac{y_1z_2/y_2z_1 - 1}{x_2y_1/x_1y_2 - 1}, \qquad \frac{by_1}{cz_1} = \frac{x_1z_2/x_2z_1 - 1}{x_1y_2/x_2y_1 - 1}.$$

Since a, b, c, $p_1, \ldots, p_t$ are pairwise coprime and x_1, y_1, z_1 are composed of $p_1, \ldots, p_t$, we obtain that there are only finitely many possible values for ax_1/cz_1 and by_1/cz_1, whence for a, b and c. Thus there are only finitely many normalised triples $(a, b, c) \in (\mathbb{Z}^*)^3$ for which (5.8) has more than two solutions.

Corollaries 1.3, 2 and 3 do not provide any upper bounds for the solutions themselves. We shall show how such bounds can be derived from results on linear forms in logarithms of algebraic numbers.

Lemma 1. *Let $\gamma_1, \ldots, \gamma_n \in \mathbb{Q}^*$ with $h(\gamma_i) \leq \Gamma_i$ where $\Gamma_i \geq 3$ for $i = 1, \ldots, n$ and $n \geq 2$. Let $B \geq 2$ and $b_i \in \mathbb{Z}$ with $|b_i| \leq B$ for $i = 1, \ldots, n$. Put*

$$\Lambda = \gamma_1^{b_1} \ldots \gamma_n^{b_n} - 1,$$

$$\Omega = \prod_{i=1}^{n} \log \Gamma_i,$$

$$\Omega' = \prod_{i=1}^{n-1} \log \Gamma_i.$$

a) *Then either* $\Lambda = 0$ *or* $|\Lambda| \geq \exp(-n^{Cn}\Omega \log \Omega' \log B)$.

b) *Let* p *be any prime number. Then either* $\Lambda = 0$ *or*

$$|\Lambda|_p \geq \exp\bigl(-n^{Cn} p \Omega (\log B)^2\bigr).$$

The proofs of Lemma 1a) and 1b) can be found in Baker [3] and van der Poorten [65], respectively. For defects in the latter proof, see Yu [91], [92].

Győry [34] proved the Corollary below by applying a variation on Lemma 1.

Corollary 4. *If the triple* $a, b, c \in (\mathbf{Z}^*)^3$ *is* S*-normalised, then each solution* (x, y, z) *of* (5.8) *satisfies*

$$\max\bigl(|x|, |y|, |z|\bigr) < \exp(t^{Ct} P^{4/3} \log A)$$

where $A = \max(a, b, c, 3)$.

We shall give a simple proof of a slightly weaker assertion, namely with $\log A$ replaced by $\log A (\log \log A)^2$:

Let $(x, y, z) \in \mathcal{S}^3$ satisfy (5.8). Put $Z = \max\bigl(|x|, |y|, |z|\bigr)$. Then each of x, y, z is of the form $\pm p_1^{k_1} \ldots p_t^{k_t}$ with $k_1, \ldots, k_t \in \mathbf{Z}$. Observe that $|k_i| \leq C \log p_i^{k_i} \leq C \log Z$. Let $p \in T$. Suppose $|z|_p \neq 1$. Then $|x|_p = |y|_p = 1$ and

$$|z|_p = |cz|_p = |ax + by|_p = \left| -\frac{ax}{by} - 1 \right|_p.$$

Hence, by Lemma 1b),

$$|z|_p \geq \exp\bigl(-t^{Ct} P (\log P)^t \log A (\log B)^2\bigr), \tag{5.11}$$

where $B = \max\bigl(|k_1|, \ldots, |k_t|\bigr) \leq C \log Z$. Inequality (5.11) is also valid if $|z|_p = 1$. It follows that

$$\begin{aligned} |z| &= \prod_{p \in T} |z|_p^{-1} \\ &\leq \exp\bigl(t^{Ct} P (\log P)^t \log A (\log \log Z)^2\bigr). \end{aligned}$$

By the symmetry of (5.8), the right-hand side is also an upper bound for $|x|$ and $|y|$. (We have not used the fact that $0 < a \leq b \leq c$.) Hence

$$\frac{\log Z}{(\log\log Z)^2} \leq t^{Ct} P (\log P)^t \log A.$$

By transferring secondary factors we obtain

$$\log Z \leq t^{Ct} P (\log P)^{t+3} \log A (\log\log A)^2.$$

If $\log P \leq t^4$ then $(\log P)^{t+3} \leq t^{Ct}$, otherwise

$$\begin{aligned}(\log P)^{t+3} &\leq (\log P)^{3t} \\ &\leq \exp\bigl(3(\log P)^{1/4} \log\log P\bigr) \\ &\leq C P^{1/3}.\end{aligned}$$

Thus

$$\log Z \leq t^{Ct} P^{4/3} \log A (\log\log A)^2$$

which is our claim.

An upper bound depending on P and t only can be given for the coefficients and the solutions of those S-normalised S-unit equations which have more than $t+2$ solutions. This follows from the following consequence of Theorems 4 and 5. (Observe that for each triple $(a', b', c') \in (\mathbb{Q}^*)^3$ we have $\max\bigl(h(a'), h(b'), h(c')\bigr) \geq \max\bigl(|a|, |b|, |c|\bigr)$ where (a, b, c) is an S-normalised triple of non-zero integers which is S-equivalent to (a', b', c').)

Corollary 5. *Each S-normalised triple $(a, b, c) \in (\mathbb{Z}^*)^3$ such that* (5.8) *has at least $t+3$ solutions (x, y, z) with $z > 0$ satisfies*

$$\max\bigl(|a|, |b|, |c|\bigr) \leq \exp(t^{Ct} P^2)$$

and each solution of such an equation satisfies

$$\max\bigl(|x|, |y|, |z|\bigr) \leq \exp(t^{Ct} P^3).$$

Proof. Put $\alpha = a/c$, $\beta = b/c$, $A = c = \max(a, b, c)$. Then $0 \leq \alpha \leq \beta \leq 1$. If (5.8) has $t+3$ solutions with $z > 0$, then the equation

$$\alpha x + \beta y = 1 \tag{5.12}$$

has $t+3$ solutions, $(x_0, y_0), (x_1, y_1), \ldots, (x_{t+2}, y_{t+2}) \in U_S^2$, say. Without loss of generality we may assume

$$h(x_0) \leq \ldots \leq h(x_{t+2}). \tag{5.13}$$

We shall prove that

$$\log A \leq t^{Ct} P^{4/3}. \tag{5.14}$$

By Corollary 4, this suffices to prove Corollary 5. In the sequel we shall assume $A > 2^{10}$.

First we prove that for $i = 1, \ldots, t+2$ there exists a valuation $|\ |_v \in S = \{|\cdot|, |\cdot|_{p_1}, \ldots, |\cdot|_{p_t}\}$ such that

$$|\alpha x_i|_v \leq A^{-1/5(t+1)}. \tag{5.15}$$

We write $v \in S$. We distinguish two cases.

Case 1. $\alpha \leq A^{-1/4}$.

(This condition is equivalent to $a < c^{3/4}$. Essentially this is the case treated by Győry [34], cf. §3 above. In this case the solution (x_0, y_0) is not used so that the conclusion of the theorem can be reached when there are only $t+2$ solutions.)

We have $[\alpha]_S = 1$ and $\{x_i\}_S = 1$. Hence

$$\prod_{v \in S} |\alpha x_i|_v = \prod_{v \in S} |\alpha|_v = \alpha \leq A^{-1/4}.$$

Since S has $t+1$ elements, there is some v in S such that (5.15) holds.

Case 2. $\alpha > A^{-1/4}$. (This part contains the new argument.) We have $\beta \geq \alpha > A^{-1/4}$, $b \geq a > A^{3/4}$ and, by (5.12),

$$\alpha(x_i - x_0) = \beta(y_0 - y_i) \qquad \text{for } i = 1, \ldots, t+2.$$

Since $x_0, x_i, y_0, y_i \in U_S$, we obtain for any prime $p \notin T$ that

$$\big|\alpha(x_i - x_0)\big|_p \leq \min\big(|\alpha|_p, |\beta|_p\big).$$

Hence, by (5.1) and $[\alpha]_S = [\beta]_S = 1$,

$$\begin{aligned}
\prod_{v \in S} \big|\alpha(x_i - x_0)\big|_v &= \prod_{p \notin T} \big|\alpha(x_i - x_0)\big|_p^{-1} \\
&\geq \prod_{p \notin T} \big(\min(|\alpha|_p, |\beta|_p)\big)^{-1} \\
&= \Big(\prod_p \min\big(|\alpha|_p, |\beta|_p\big)\Big)^{-1}.
\end{aligned}$$

By the coprimality condition on a, b, c we have $\min(|a|_p, |b|_p) = |\mathrm{lcm}(a,b)|_p = |ab|_p$. Hence

$$\min(|\alpha|_p, |\beta|_p) = \frac{\min(|a|_p, |b|_p)}{|c|_p} = \left|\frac{ab}{c}\right|_p.$$

By the Product Formula we obtain

$$\Big(\prod_p \min(|\alpha|_p, |\beta|_p)\Big)^{-1} = \frac{ab}{c}.$$

Therefore

$$\prod_{v\in S} |\alpha(x_i - x_0)|_v \geq ab/c > A^{3/4}A^{3/4}A^{-1} = A^{1/2}.$$

On the other hand, by $0 \leq \alpha \leq 1$ and (5.13),

$$\begin{aligned}\prod_{v\in S} |\alpha(x_i - x_0)|_v &\leq \alpha \prod_{v\in S} |x_i - x_0|_v \\ &\leq 2\prod_{v\in S} \max(|x_0|_v, |x_i|_v) \\ &\leq 2\Big(\prod_{v\in S} \max(1, |x_0|_v)\Big)\Big(\prod_{v\in S} \max(1, |x_i|_v)\Big) \\ &= 2h(x_0)h(x_i) \leq 2\big(h(x_i)\big)^2.\end{aligned}$$

It follows that

$$h(x_i) \geq \left(\tfrac{1}{2}A^{1/2}\right)^{1/2} > A^{1/5}.$$

We infer from (5.2) and (5.3) that

$$\begin{aligned}\prod_{v\in S} \min(1, |x_i|_v) &= \Big(\prod_{v\in S} \max(1, |x_i|_v)\Big)^{-1} \\ &= \big(h(x_i)\big)^{-1} < A^{-1/5}.\end{aligned}$$

Since $0 \leq \alpha \leq 1$ and $[\alpha]_S = 1$, there is some v in S such that

$$|\alpha x_i|_v \leq |x_i|_v < A^{-1/(5(t+1))}.$$

This proves (5.15) in the second case.

Since $|S| = t+1$, there are i, j in $\{1,\dots,t+2\}$ with $i<j$ such that, for the same valuation $v \in S$,

$$|\alpha x_i|_v \le A^{-1/(5(t+1))}, \qquad |\alpha x_j|_v \le A^{-1/(5(t+1))}.$$

Hence, by (5.12),

$$|\beta y_j|_v = |1-\alpha x_j|_v \ge \frac{1}{2},$$
$$\big|\beta(y_i-y_j)\big|_v = \big|\alpha(x_j-x_i)\big|_v \le 2A^{-1/(5(t+1))}.$$

We obtain

$$\left|\frac{y_i}{y_j}-1\right|_v \le 4A^{-1/(5(t+1))}. \tag{5.16}$$

We apply Lemma 1a) if v is the absolute value and Lemma 1b) otherwise. Note that $y_i/y_j = \pm p_1^{k_1}\dots p_t^{k_t}$ with $|k_h| \le C\log\max\big(h(y_i),h(y_j)\big)$. Hence

$$\left|\frac{y_i}{y_j}-1\right|_v \ge \exp\Big(-t^{Ct}P(\log P)^{t+1}\big(\log\log\max\big(h(y_i),h(y_j)\big)\big)^2\Big). \tag{5.17}$$

Corollary 4 implies that

$$\log\max\big(h(y_i),h(y_j)\big) \le t^{Ct}P^{4/3}\log A. \tag{5.18}$$

Combining (5.16), (5.17) and (5.18) we obtain

$$\log A \le t^{Ct}P(\log P)^{t+3}(\log\log A)^2.$$

This implies, by transferring secondary factors,

$$\log A \le t^{Ct}P(\log P)^{t+5}.$$

As in the proof of Corollary 4 we have $(\log P)^{t+5} \le t^{Ct}P^{1/3}$. Hence $\log A \le t^{Ct}P^{4/3}$ as claimed in (5.14). ∎

It is clear from the proofs that, in Corollaries 4 and 5, $P^{4/3}$ and P^2 can be replaced by $P^{1+\epsilon}$ and P^3 by $P^{2+\epsilon}$ for any positive ϵ, provided that the constants C are allowed to depend on ϵ.

§6. Applications to sums of products of given primes

Let $T = \{p_1, \ldots, p_t\}$ be a set of prime numbers not exceeding P (≥ 2). Let $\mathcal{S}$ be the set of rational integers of which each prime divisor belongs to T. We consider representations $x_1 + \ldots + x_n$ with $x_1, \ldots, x_n \in \mathcal{S}$, so-called *$\mathcal{S}$-representations*. We call two representations $x_1 + \ldots + x_n$ and $y_1 + \ldots + y_n$ *distinct* if $(x_1, \ldots, x_n)$ is not a permutation of $(y_1, \ldots, y_n)$. The representations $x_1 + \ldots + x_{n_1}$ and $y_1 + \ldots + y_{n_2}$ are called *relatively prime* if $\gcd(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) = 1$. They are called *disjoint* if $x_i \neq y_j$ for $i = 1, \ldots, n_1$ and $j = 1, \ldots, n_2$, and *totally disjoint* if there are no equal subsums, that means there are no non-empty proper subsets $\{i_1, \ldots, i_k\}$ of $\{1, \ldots, n_1\}$ and $\{j_1, \ldots, j_\ell\}$ of $\{1, \ldots, n_2\}$ such that $x_{i_1} + \ldots + x_{i_k} = y_{j_1} + \ldots + y_{j_\ell}$. If $n_1 = n_2 = 2$, then there is no difference between the notions distinct, disjoint and totally disjoint.

In this paragraph we give some applications of Corollaries 1.3 and 2–5. By C we shall denote absolute constants, by $C(T, n)$ numbers depending only on T and n, and so on.

Theorem 6. *Let n, n_1 and n_2 be positive integers.*

a) *There is a number $C(T, n)$ such that every integer m has at most $C(T, n)$ representations as sums of n pairwise relatively prime elements from $\mathcal{S}$.*

b) *There are only finitely many integers which admit a representation $x_1 + \ldots + x_{n_1}$ of pairwise relatively prime elements of $\mathcal{S}$ and a representation $y_1 + \ldots + y_{n_2}$ of pairwise relatively prime elements of $\mathcal{S}$ such that the representations are disjoint.*

c) *There are only finitely many integers which admit an $\mathcal{S}$-representation $x_1 + \ldots + x_{n_1}$ and an $\mathcal{S}$-representation $y_1 + \ldots + y_{n_2}$ such that the representations are relatively prime and totally disjoint.*

Proof. c) Suppose m admits the two described representations. Then $x_1 + \ldots + x_{n_1} - y_1 - \ldots - y_{n_2} = 0$. We may assume $m \neq 0$. We apply Corollary 1.3. Conditions (5.6) and (5.7) are satisfied (with $\Delta = 1$, $\delta = 0$). If (5.5) is not fulfilled, then $x_1 + \ldots + x_{n_1} - y_1 - \ldots - y_{n_2}$ has a vanishing subsum. The complementary subsum vanishes too. Since $m \neq 0$, one of both subsums involves both x's and y's. This leads to a contradiction with the supposition that the representations are totally disjoint. Thus (5.5) holds. By Corollary 1.3 we find that there exists a finite set of $(n_1 + n_2)$-tuples depending only on T, n_1 and n_2 to which $(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})$ belongs. Thus $m = x_1 + \ldots + x_{n_1}$ satisfies $m < C(T, n_1, n_2)$.

b) Suppose m admits the two described representations. We may assume that $m \neq 0$ and that we do not have $x_i = -x_j = 1$ for some i, j in $\{1, \ldots, n_1\}$ or $y_i = -y_j = 1$ for some i, j in $\{1, \ldots, n_2\}$. Observe that $x_1 + \ldots + x_{n_1} - y_1 - \ldots - y_{n_2}$ can be split into a number of vanishing subsums so that none of these subsums has a vanishing subsum. The number of possible splittings is $C(n_1 + n_2)$. By the conditions of b) each subsum has at least three terms, hence involves at least two x's or two y's. By applying Corollary 1.3 to each of the possible splittings we obtain that there are only finitely many possibilities for the terms in each subsum, since these terms have no common prime factor. It follows that there is a finite set of $(n_1 + n_2)$-tuples depending only on T, n_1 and n_2 to which $(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})$ belongs. Thus $|m| = |x_1 + \ldots + x_{n_1}| < C(T, n_1, n_2)$.

a) It suffices to prove that there are at most $C(T, n)$ distinct representations. If $m = 0$ then we apply the argument to the $\mathcal{S}$-representations $x_1 + \ldots + x_n$ of m which we applied to $x_1 + \ldots + x_{n_1} - y_1 - \ldots - y_{n_2}$ in the proof of b). It follows that there is a finite set of n-tuples depending only on T and n to which $(x_1, \ldots, x_n)$ belongs.

Now assume $m \neq 0$. If m admits two representations of the described form, then, after permutation, they can be written as $x_1 + \ldots + x_n$ and $y_1 + \ldots + y_{n_1} + x_{n_1+1} + \ldots + x_n$ with $x_i \neq y_j$ for $i = 1, \ldots, n_1$ and $j = 1, \ldots, n_1$. According to b) there are only $C_1(T, n)$ integers m_1 which admit two disjoint representations $x_1 + \ldots + x_{n_1}$ and $y_1 + \ldots + y_{n_1}$ of pairwise relatively prime elements of $\mathcal{S}$ for some $n_1 \leq n$. Moreover, it follows from the proof of b) that there is a finite set of $2n_1$-tuples depending only on T and n_1 to which $(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_1})$ belongs, that is, each m_1 admits at most $C_2(T, n_1)$ pairwise disjoint $\mathcal{S}$-representations of pairwise relatively prime integers. Similarly $m - m_1$ admits at most $C_2(T, n - n_1)$ pairwise disjoint $\mathcal{S}$-representations of pairwise relatively prime integers $x_{n_1+1} + \ldots + x_n$. Hence there are at most $C_1(T, n)C_2(T, n_1)$ possibilities for the distinct part $(x_1, \ldots, x_{n_1})$ and $C_2(T, n - n_1)$ possibilities for the remaining common part $(x_{n_1+1}, \ldots, x_n)$. Thus the total number of representations as sums of n pairwise relatively prime elements from $\mathcal{S}$ is bounded by $C(T, n) := C_1(T, n) \sum_{n_1=1}^{n} C_2(T, n_1)C_2(T, n - n_1)$. ∎

It is not hard to see that the restrictions in b) and c) cannot be omitted. Let $T = \{2, 3, 5\}$. In b) we require disjointness, since there are infinitely many integers with representations $5^k + 2^2 + 1 = 5^k + 3 + 2$. We require pairwise coprimality in view of the representations $2^{k+1} + 3 + 2$ and $2^k + 2^k + 5$. In c) we require total disjointness to exclude representations $2^{k+2} + 2^k + 2 + 1$ and $2^k \cdot 3 + 2^{k+1} + 3$. We require that the representations are relatively prime, since otherwise we may

have $2^{k+2}+2^k$ and $2^k \cdot 3+2^{k+1}$ as representations. The restriction in a) is necessary, since 1 has infinitely many representations of the form $3 \cdot 2^k-2^{k+1}-2^k+1$. However, Tijdeman and Wang [90] have proved that there is a number $C_1(T,n)$ such that every integer has at most $C_1(T,n)$ representations as sums of n positive elements from $\mathcal{S}$.

In a letter to one of us, P. Erdős drew our attention to the following conjecture of D. Newman (cf. [16] p. 80). The number of representations $m=2^\alpha 3^\beta+2^\gamma+3^\delta$ in non-negative integers α, β, γ, δ is bounded. Erdős wondered whether this could be solved by Corollary 1.3. We show that he is right, and that there are only finitely many integers which have more than two disjoint representations. Any pair of coprime integers greater than 1 could be taken in place of the bases 2 and 3.

Theorem 7. a) *There is a constant C such that every integer has at most C representations of the form $2^\alpha 3^\beta+2^\gamma+3^\delta$ with α, β, γ and δ non-negative integers.*

b) *There are only finitely many integers which admit more than two pairwise disjoint representations of the form $2^\alpha 3^\beta+2^\gamma+3^\delta$ with α, β, γ and δ non-negative integers.*

Proof. Put $T=\{2,3\}$. By N-representation we shall mean a representation of the form $2^\alpha 3^\beta+2^\gamma+3^\delta$. By Theorem 6c) there are only finitely many integers m which admit two totally disjoint N-representations. Let M_0 be the maximum of such numbers m.

We now assume that $m>M_0$ has two distinct N-representations, $m=2^\alpha 3^\beta+2^\gamma+3^\delta=2^\varepsilon 3^\zeta+2^\eta+3^\theta$. Hence these representations are not totally disjoint. Since the representations are distinct, $2^\alpha 3^\beta+2^\gamma+3^\delta-2^\varepsilon 3^\zeta-2^\eta-3^\theta$ has exactly two vanishing subsums (which are complementary).

Suppose first that each vanishing subsum has three terms. By using the symmetry, also with respect to the bases 2 and 3, we may assume without loss of generality that we have one of the following cases:

(i) $\quad 2^\alpha 3^\beta+2^\gamma-2^\varepsilon 3^\zeta=0, \qquad 3^\delta-2^\eta-3^\theta=0.$

(ii) $\quad 2^\alpha 3^\beta+2^\gamma-2^\eta=0, \qquad 3^\delta-2^\varepsilon 3^\zeta-3^\theta=0.$

(iii) $\quad 2^\alpha 3^\beta+2^\gamma-3^\theta=0, \qquad 3^\delta-2^\varepsilon 3^\zeta-2^\eta=0.$

(iv) $\quad 2^\gamma+3^\delta-2^\varepsilon 3^\zeta=0, \qquad 2^\alpha 3^\beta-2^\eta-3^\theta=0.$

We treat the cases separately and apply Corollary 1.3 to both subsums.

Case (i). It follows that there are only finitely many possibilities for δ, η and θ. The numbers $2^\alpha 3^\beta$, 2^γ and $2^\epsilon 3^\zeta$ belong to a finite set apart from a common factor 2^k ($k \in \mathbb{Z}$, $k \geq 0$).

Case (ii). The numbers $2^\alpha 3^\beta$, 2^γ, 2^η belong to a finite set apart from a common factor 2^k. The numbers 3^δ, $2^\epsilon 3^\zeta$, 3^θ belong to a finite set apart from a common factor 3^ℓ.

Cases (iii) and (iv). There are only finitely many possibilities for the exponents.

We conclude that m is both of the form $2^k(2^{k_1}3^{\ell_1} + 2^{k_2}) + 3^{\ell+\ell_2}$ and of the form $2^{k+k_3} + 3^\ell(2^{k_4}3^{\ell_3} + 3^{\ell_4})$ where $k_1, \ldots, k_4, \ell_1, \ldots, \ell_4$ belong to a certain finite set.

Suppose next that one vanishing subsum has two elements and the other four. This implies that the representations are not disjoint and hence we are not in situation b). Without loss of generality we may assume that we have one of the following cases:

$$\text{(v)} \qquad 2^\alpha 3^\beta - 2^\epsilon 3^\zeta = 0, \qquad 2^\gamma + 3^\delta - 2^\eta - 3^\theta = 0.$$

$$\text{(vi)} \qquad 2^\gamma - 2^\eta = 0, \qquad 2^\alpha 3^\beta + 3^\delta - 2^\epsilon 3^\zeta - 3^\theta = 0.$$

Case (v). By applying Corollary 1.3 to the second sum we obtain that $(\gamma, \delta, \eta, \theta)$ belongs to a finite set of quadruples.

Case (vi). By applying Corollary 1.3 to the second sum we find that $(2^\alpha 3^\beta, 3^\delta, 2^\epsilon 3^\zeta, 3^\theta)$ belongs to a finite set of quadruples apart from a common factor 3^ℓ.

To prove a) we observe that each N-representation of m is either of the form $a2^k + b3^\ell$ or of the form $2^k 3^\ell + a + b$ where in each case (a, b) belongs to a finite set. Put $M_1 = \max(a + b)$ where (a, b) runs over this finite set. The number of representations of m of the form $a2^k + b3^\ell$ is bounded by Corollary 2. For representations of the form $2^k 3^\ell + a + b$ we remark that it follows from Corollary 1.3 that the distance between numbers of the form $2^k 3^\ell$ exceeds $2M_1$ when $2^k 3^\ell > M_2$. Hence if $m > M_1 + M_2$ and $m = 2^k 3^\ell + a + b$, then k and ℓ are uniquely determined by m. It follows that for $m > M_0 + M_1 + M_2$ the number of N-representations of the second type is also bounded. We conclude that the total number of N-representations of any number $m > M_0 + M_1 + M_2$ is bounded. It is obvious that the number of N-representations of numbers $m \leq M_0 + M_1 + M_2$ can be bounded. This proves a).

To prove b) we recall that if $m > M_0$ admits two disjoint N-representations then each representation is of the form $a \,.\, 2^k + b \,.\, 3^\ell$ where

(a, b) belongs to some finite set and either $a = 2^{k_1}3^{\ell_1} + 2^{k_2}$, $b = 3^{\ell_2}$ (the first type) or $a = 2^{k_3}$, $b = 2^{k_4}3^{\ell_3} + 3^{\ell_4}$ (the second type). We define T_1 as the set consisting of $2, 3$ and all the prime divisors of a and b where (a, b) runs over the finite set. Denote by $\mathcal{S}_1$ the set of rational integers of which each prime divisor belongs to T_1. Let M_3 be so large that if m has two totally disjoint, relatively prime $\mathcal{S}_1$-representations $x_1 + x_2$ and $y_1 + y_2$, then $m < M_3$. This number M_3 exists by Theorem 6c).

Suppose $m > \max(M_0, M_3)$ admits three pairwise disjoint N-representations. Then there are two disjoint representations of the same type. Since $m > M_3$, these representations as sum of two elements of $\mathcal{S}_1$, are not totally disjoint. It follows that the corresponding N-representations are not totally disjoint. If the representations are of the first type,

$$2^k(2^{k_1}3^{\ell_1} + 2^{k_2}) + 3^{\ell+\ell_2}$$

and

$$2^{k'}(2^{k_3}3^{\ell_3} + 2^{k_4}) + 3^{\ell'+\ell_4}$$

say, then

$$2^k(2^{k_1}3^{\ell_1} + 2^{k_2}) = 3^{\ell'+\ell_4}$$

and

$$2^{k'}(2^{k_3}3^{\ell_3} + 2^{k_4}) = 3^{\ell+\ell_2},$$

since the N-representations are disjoint. It follows that k and ℓ are bounded, hence $m < M_4$. If the representations are of the second type, then we obtain similarly $m < M_5$. Thus no m greater than $\max(M_0, M_3, M_4, M_5)$ admits more than two disjoint N-representations. ∎

There exist infinitely many integers with two disjoint N-representations in view of $2^a.3^1 + 2^a + 3^{b+2} = 2^3 3^b + 2^{a+2} + 3^b$ for any positive integers a, b. There are infinitely many integers m which admit four distinct N-representations, namely, for $a \geq 2$, $b \geq 2$,

$$\begin{aligned}(2^a + 3^b) &= 2^{a-1}3^0 + 2^{a-1} + 3^b \\ &= 2^{a-2}3^1 + 2^{a-2} + 3^b \\ &= 2^1 3^{b-1} + 2^a + 3^{b-1} \\ &= 2^3 3^{b-2} + 2^a + 3^{b-2}.\end{aligned}$$

Tijdeman and Wang [90] have proved that apart from the numbers of the form $2^a + 3^b$ there are only finitely many positive integers m which admit at least four N-representations.

It follows from Corollary 2 that the number of representations of a non-zero integer m as difference of two elements of $\mathcal{S}$ is bounded (in terms of t). This was the clue to the solution of an old problem of Erdős and Turán.

Let $a_1 < a_2 < \ldots < a_k$ and $b_1 < b_2 < \ldots < b_\ell$ be positive integers. Assume that the prime factors of

$$P_{k,l} := \prod_{1 \le i \le k, 1 \le j \le \ell} (a_i + b_j)$$

are given by $p_1, \ldots, p_t$. Erdős and Turán (cf. [15] p. 36) conjectured that if $\ell = k$ and k tends to infinity then $t \to \infty$. They had settled the special case $b_j = a_j$ for $j = 1, \ldots, k$ in their first joint paper [18]. Győry, Stewart and Tijdeman [47] observed that a stronger assertion follows from Corollary 2. Since, for any non-zero c, the number of solutions of $x - y = c$ in integers x, y composed of given primes $p_1, \ldots, p_t$ is at most $6 \times 7^{2t+3}$, the number of positive integers a such that both $a + b_1$ and $a + b_2$ are composed of $p_1, \ldots, p_t$ is at most $6 \times 7^{2t+3}$. It follows that $\ell \ge 2$ already implies $t \ge \frac{1}{4} \log k - 2$, hence $t \to \infty$ as $k \to \infty$. An elementary solution of the problem of Erdős and Turán was presented in [88]. Erdős also posed the problem of investigating the number of distinct prime factors of $\prod(a_i + b_j)$ if the product extends over a given set of pairs (i, j). Results in this direction can be found in Győry, Stewart and Tijdeman [48].

There are several related results involving $P := \max_{i=1,\ldots,t} p_i$. We henceforth assume that P is fixed and that $a_1 + b_1, \ldots, a_1 + b_\ell$, $a_2 + b_1, \ldots, a_k + b_\ell$ have no prime factor in common. In [47] we showed that if $k \ge 2$, $\ell \ge 2$, then $a_k + b_\ell$ is bounded. This follows by applying Corollary 1.3 to $(a_1 + b_1) + (a_2 + b_2) - (a_1 + b_2) - (a_2 + b_1) = 0$. By applying Corollary 5 to $x - y = b_\ell - b_1$, we obtain the following refinement of [47, Theorem 2]:

If $k \ge t + 3$ and $\ell \ge 2$, then $a_k + b_\ell \le \exp(t^{Ct} P^3)$ where C is some effectively computable absolute constant. Surveys on these and related results are given by Stewart [87] and Stewart and Tijdeman [88].

§7. Applications to finitely generated groups

In a letter to one of us A. Rhemtulla and S. Sidki asked to show that not every rational integer r is of the form $r_1 + r_2 + \ldots + r_{n'}$, $n' \le n$, where

each r_i belongs to G, where G is a fixed multiplicative group generated by algebraic integers $\alpha_1, \ldots, \alpha_t$. They needed this result for their study of ellipticity problems in group theory. An application of Theorem 1 yielded a positive answer. In fact, if n is a positive integer and $\alpha_1, \ldots, \alpha_t$ are non-zero algebraic numbers (not necessarily integers), then there exists a positive integer m which is not representable as the sum of at most n power products $\alpha_1^{b_1} \ldots \alpha_t^{b_t}$ $(b_1, \ldots, b_t \in \mathbb{Z})$. This assertion follows from the following theorem by letting G be the group generated by $\alpha_1, \ldots, \alpha_t$ and H the group generated by a prime number p of which no power belongs to G. We namely infer from the theorem that only finitely many powers of p can be represented as the sum of at most n power products of $\alpha_1, \ldots, \alpha_t$.

Theorem 8. *Let n_1 and n_2 be positive integers. Let G, H be finitely generated multiplicative subgroups of $\mathbb{C}^*$ with $G \cap H = \{1\}$. There are only finitely many complex numbers α which can be written both as*

$$\alpha = \epsilon_1 + \ldots + \epsilon_{n_1} \quad \text{with } \epsilon_1, \ldots, \epsilon_{n_1} \in G \tag{7.1}$$

and as

$$\alpha = \eta_1 + \ldots + \eta_{n_2} \quad \text{with } \eta_1, \ldots, \eta_{n_2} \in H. \tag{7.2}$$

Proof. We use induction on $n = n_1 + n_2$. We denote by $N(n)$ the number of complex numbers α which can be written both in the form (7.1) and in the form (7.2) with $n_1 + n_2 \leq n$. Further we denote by $N_0(n)$ the number of complex numbers which are of the forms (7.1) and (7.2) with $n_1 + n_2 \leq n$ such that no subsum of $\epsilon_1 + \ldots + \epsilon_{n_1}$ equals any subsum of $\eta_1 + \ldots + \eta_{n_2}$. Obviously $N(2) = 1$. Suppose $N(n-1) < \infty$. If α is of the forms (7.1) and (7.2) with $n_1 + n_2 = n$, then

$$\epsilon_1 + \ldots + \epsilon_{n_1} - \eta_1 \ldots - \eta_{n_2} = 0,$$

$$\epsilon_1, \ldots, \epsilon_{n_1} \in G, \ \eta_1, \ldots, \eta_{n_2} \in H. \tag{7.3}$$

If no subsum of the left-hand side vanishes, then we obtain, by applying Theorem 1′ to $G_0 = G^{n_1} \times H^{n_2}$, that there are only finitely many possibilities for $(\epsilon_1 : \ldots : \epsilon_{n_1} : \eta_1 : \ldots : \eta_{n_2})$. If $(\epsilon_1', \ldots, \epsilon_{n_1}', \eta_1', \ldots, \eta_{n_2}')$ and $(\epsilon_1'', \ldots, \epsilon_{n_1}'', \eta_1'', \ldots, \eta_{n_2}'')$ are two solutions corresponding to the same projective point, then $\epsilon_1'/\epsilon_1'' = \eta_1'/\eta_1'' \in G \cap H = \{1\}$. Thus there are only finitely many solutions of (7.3) without vanishing subsums, whence $N_0(n) < \infty$. If some subsum vanishes, then α can be written as $\beta + \gamma$ where both β and γ are of the forms (7.1) and (7.2), but in both cases $n_1 + n_2 \leq n - 1$. The number of numbers α representable in this way is at most $\big(N(n-1)\big)^2$. Thus $N(n) \leq N_0(n) + \big(N(n-1)\big)^2 < \infty$. This proves the induction hypothesis. ∎

§8. Applications to recurrence sequence of complex numbers

By a *recurrence sequence* we mean an infinite sequence of complex numbers $U = \{u_m\}_{m=0}^{\infty}$ satisfying a relationship of the type

$$u_{m+k} = c_1 u_{m+k-1} + \ldots + c_k u_m \qquad \text{for } m = 0, 1, 2, \ldots \tag{8.1}$$

where $c_1, \ldots, c_k$ are complex numbers. The sequence U satisfies several recurrence relations of type (8.1); among these there is a unique recurrence relation for which k is minimal. Supposing that (8.1) is the recurrence with minimal k satisfied by U, we put

$$F(X) = X^k - c_1 X^{k-1} \ldots - c_{k-1} X - c_k. \tag{8.2}$$

F is called the *companion polynomial* of U. Obviously $F(0) \neq 0$. Let

$$F(X) = (X - \omega_1)^{e_1} \ldots (X - \omega_r)^{e_r}$$

where $e_1, \ldots, e_r$ are positive integers and $\omega_1, \ldots, \omega_r$ non-zero distinct complex numbers. Then there are polynomials $f_1, \ldots, f_r \in \mathbb{C}[X]$, of degrees at most $e_1 - 1, \ldots, e_r - 1$ respectively, such that

$$u_m = f_1(m)\omega_1^m + \ldots + f_r(m)\omega_r^m \qquad \text{for } m = 0, 1, 2, \ldots. \tag{8.3}$$

We call k the *order* and r the *rank* of U. We say that U is *non-degenerate* if ω_i/ω_j is not a root of unity for $1 \leq i < j \leq r$, and *degenerate* otherwise. If U is degenerate, then there exists a positive integer v such that each sequence $\{u_{\ell+mv}\}_{m=0}^{\infty}$ $(0 \leq \ell < v)$ is either non-degenerate and of rank less than r or identically zero.

The following theorem can be derived from the Main Theorem on S-Unit Equations.

Theorem 9. *Let R be a subring of $\mathbb{C}$ which is finitely generated over $\mathbb{Z}$ and let $U = \{u_m\}_{m=0}^{\infty}$ be a non-degenerate recurrence sequence in $\mathbb{C}$ of rank at least 2. Then there are only finitely many pairs of integers (m, n) for which a $\zeta_{m,n} \in R \setminus \{0\}$ exists such that*

$$\zeta_{m,n} u_m = u_n, \qquad m > n \geq 0. \tag{8.4}$$

This is a slight generalisation of Theorem 3 of Evertse [20] which gives the result when R is a finitely generated multiplicative subgroup of the field of algebraic numbers.

Before discussing the proof, we state some consequences of Theorem 9.

Corollary 9.1 (Skolem, Mahler, Lech [53]). *Let $U = \{u_m\}_{m=0}^{\infty}$ be a recurrence sequence in $\mathbb{C}$ for which the set $\mathcal{M} = \{m : u_m = 0\}$ is infinite. Then $\mathcal{M}$ is ultimately periodic (i.e. there are positive integers m_0 and v such that $m \in \mathcal{M}$ implies $m + v \in \mathcal{M}$ for all $m \geq m_0$).*

Proof. It is easy to check that $\mathcal{M}$ is finite if U has rank 1. Suppose U has rank at least 2 and $\mathcal{M}$ is infinite. Then U is degenerate by Theorem 9. Hence there exists an integer v such that each sequence $\{u_{\ell+mv}\}_{m=0}^{\infty}$ is either non-degenerate, whence has only finitely many zeros, or is identically zero. ∎

The following statement was made by Glass, Loxton and van der Poorten [27].

Corollary 9.2. *Let $U = \{u_m\}_{m=0}^{\infty}$ be a non-periodic non-degenerate recurrence sequence in $\mathbb{C}$. Then there are only finitely many pairs of integers m, n with $m > n \geq 0$ and $u_m = u_n$.*

Proof. If U has rank 1, then $u_m = u_n$ implies

$$f_1(m)\omega_1^m = f_1(n)\omega_1^n.$$

If f_1 is constant, then ω_1 is a root of unity and U is periodic, which contradicts our assumption. If f_1 is non-constant, then, by $m > n$, $|f_1(m)| > |f_1(n)|$ for m sufficiently large. Hence $|\omega_1| < 1$. Put $f_1(X) = a_0X^\ell + a_1X^{\ell-1} + \ldots + a_\ell$ with $a_0 \neq 0$. Then

$$1 < |\omega_1|^{-1} \leq |\omega_1|^{n-m} < \frac{|a_0| + \frac{1}{m}\sum_{j=1}^{\ell}|a_j|}{|a_0| - \frac{1}{n}\sum_{j=1}^{\ell}|a_j|} = \frac{1 + c/m}{1 - c/n}$$

for some $c > 0$. This implies that n is bounded. Since $u_m \neq 0$ for m large, we have $u_n \neq 0$, hence $|f_1(n)\omega_1^n|$ is bounded from below by a positive constant. We have $f_1(m)\omega_1^m \to 0$ as $m \to \infty$. Thus m is bounded.

If U has rank at least 2, then Corollary 9.2 follows at once from Theorem 9. ∎

The next result was proved by Pólya [64] in 1921 in the case that all the u_m are rational.

Corollary 9.3. *Let G be a finitely generated multiplicative subgroup of $\mathbb{C}^*$ and let $U = \{u_m\}_{m=0}^{\infty}$ be a recurrence sequence such that $u_m \in G \cup \{0\}$ for $m = 0, 1, 2, \ldots$. Then the formal power series $\sum_{m=0}^{\infty} u_m X^m$ is equal to*

$$\sum_{j=1}^{\ell} \frac{\beta_j X^{j-1}}{1 - \alpha_j X^{\ell}},$$

where $\ell \geq 1$ is an integer and $\alpha_1, \ldots, \alpha_\ell, \beta_1, \ldots, \beta_\ell$ are complex numbers with $\alpha_1, \ldots, \alpha_\ell \neq 0$.

Proof. We first prove Corollary 9.3 in the case when U has rank 1, that is $u_m = f(m)\alpha^m$ where $\alpha \in \mathbb{C}^*$ and $f \in \mathbb{C}[X]$. Suppose that $u_m \in G \cup \{0\}$ for $m = 0, 1, 2, \ldots$. Let G' be the multiplicative group generated by G and α. Then $f(m) \in G' \cup \{0\}$ for $m = 0, 1, 2, \ldots$. We shall prove that f is constant.

There exist complex numbers $c_1, \ldots, c_k$ such that

$$f(X + k) = c_1 f(X + k - 1) + \ldots + c_k f(X) \quad \text{identically in } X.$$

We suppose that k is minimal, hence $c_k \neq 0$. Choose m_0 such that $f(m_0) \neq 0$ for $m > m_0$. By assumption, we have for $m > m_0$ that $\big(f(m + k), f(m + k - 1), \ldots, f(m)\big)$ is a solution of the equation

$$c_0 x_k + c_1 x_{k-1} + \ldots + c_k x_0 = 0$$

$$\text{in } x_0, \ldots, x_k \in G' \text{ (where } c_0 = -1). \quad (8.5)$$

For each proper non-empty subset J of $\{0, \ldots, k\}$, there are only finitely many m with $\sum_{j \in J} c_j f(m + k - j) = 0$, since the polynomial $\sum_{j \in J} c_j f(X + k - j)$ does not vanish identically in X. Hence there is an m_1 such that for $m \geq m_1$, $\big(f(m+k), \ldots, f(m)\big)$ is a solution of (8.5) with $\sum_{j \in J} c_j x_{k-j} \neq 0$ for each proper non-empty subset J of $\{0, 1, \ldots, k\}$. We obtain from Theorem 1′ that $f(m + k)/f(m)$ assumes only finitely many values for $m = 0, 1, 2, \ldots$. Since $f(m + k)/f(m) \to 1$ as $m \to \infty$, this implies that f is constant. Hence $u_m = \beta\alpha^m$ for $m = 0, 1, 2, \ldots$ and therefore

$$\sum_{m=0}^{\infty} u_m X^m = \frac{\beta}{1 - \alpha X}.$$

Now suppose that U has order at least 2. By Theorem 9, U is degenerate. Hence there is a v such that the sequences $U_\ell = \{u_{\ell+mv}\}_{m=0}^{\infty}$

$(0 \leq \ell < v)$ are either non-degenerate or identically zero. But the non-degenerate sequences among the U_ℓ must have order 1. Now Corollary 9.3 follows by applying the result for recurrence sequences of rank 1. ■

Recently, Bézivin [6] proved the following result by applying Theorem 1'.

Let G be a finitely generated multiplicative subgroup of $\mathbb{C}^*$ and let $F(X) = \sum_{m=0}^{\infty} u_m X^m \in \mathbb{C}[[X]]$ be a formal power series with the following properties:

(a) there are polynomials $f_0, \ldots, f_k \in \mathbb{C}[X]$ such that

$$\sum_{i=0}^{k} f_i(m) u_{m+i} = 0 \quad \text{for } m = 0, 1, 2, \ldots \tag{8.6}$$

and

(b) there are sequences $\{c_j(m)\}_{m=0}^{\infty}$ $(1 \leq j \leq \ell)$, with entries in $G \cup \{0\}$ such that

$$u_m = \sum_{j=1}^{\ell} c_j(m) \quad \text{for } m = 0, 1, 2, \ldots. \tag{8.7}$$

Then $F(X)$ is the Taylor expansion around the origin of a rational function with only simple zeros.

Using Bezivin's result, Pólya's result can be extended to a recurrence sequence $\{u_m\}_{m=0}^{\infty}$ satisfying a relationship of type (8.6). A relation of type (8.6) is satisfied if $F(X)$ is the Taylor expansion of an algebraic function around the origin.

We now turn to the proof of Theorem 9, which resembles the proof of Theorem 3 of [20]. We shall only work out in detail the new ideas. The lemma below is used to reduce Theorem 9 to the case that R is contained in the field of algebraic numbers $\mathbb{A}$.

Lemma 2. *Let $R \subset \mathbb{C}$ be a ring which is finitely generated over $\mathbb{Z}$ and let V be a finite subset of R such that V does not contain 0 or a root of unity. Then there exists a ring homomorphism $\phi : R \to \mathbb{A}$ ("specialisation") such that ϕ is invariant on $R \cap \mathbb{Q}$ and, for each α in V, $\phi(\alpha) \neq 0$ and $\phi(\alpha)$ is not a root of unity.*

Proof. Let K be the quotient field of R. Then K is finitely generated over $\mathbb{Q}$, whence $K = \mathbb{Q}(\mathbf{x}; y)$ where $\mathbf{x} = (x_1, \ldots, x_t)$ is a tuple of numbers which are algebraically independent over $\mathbb{Q}$ and y is integral over the ring

$\mathbf{Z}[\mathbf{x}] = \mathbf{Z}[x_1, \ldots, x_t]$. Thus y is a zero of a polynomial $F(\mathbf{x}; Y)$ which is irreducible in $\mathbf{Z}[\mathbf{x}, Y]$ and has leading coefficient 1. Thus R can be written as

$$R = \mathbf{Z}\left[\frac{f_1(\mathbf{x}; y)}{p(\mathbf{x})}, \ldots, \frac{f_\ell(\mathbf{x}; y)}{p(\mathbf{x})}\right]$$

where $f_1, \ldots, f_\ell \in \mathbf{Z}[\mathbf{x}; Y]$ and $p \in \mathbf{Z}$. Hence R is contained in the ring

$$\tilde{R} = \left\{\frac{f(\mathbf{x}; y)}{p^n(\mathbf{x})} : f \in \mathbf{Z}[\mathbf{x}; Y], n \in \mathbf{Z}, n \geq 0\right\}.$$

Each pair $\tilde{\mathbf{x}}$, $\tilde{y}$ with $\tilde{\mathbf{x}} = (\tilde{x}_1, \ldots, \tilde{x}_t) \in \mathbf{Z}^t$ with $p(\tilde{\mathbf{x}}) \neq 0$ and $F(\tilde{\mathbf{x}}, Y)$ not identically zero in Y and $\tilde{y}$ a zero of $F(\tilde{\mathbf{x}}, Y)$, defines a ring homomorphism $\phi : \tilde{R} \to \mathbf{A}$ with

$$\phi\left(\frac{f(\mathbf{x}, y)}{p^n(\mathbf{x})}\right) = \frac{f(\tilde{\mathbf{x}}, \tilde{y})}{p^n(\tilde{\mathbf{x}})}.$$

The image of ϕ is contained in the algebraic number field $\mathbf{Q}(\tilde{y})$ of which the degree is bounded by $[K : \mathbf{Q}(\mathbf{x})]$. Hence there is an integer $m > 0$, independent of $\tilde{\mathbf{x}}$ and $\tilde{y}$, such that every root of unity ρ in $\phi(\tilde{R})$ satisfies $\rho^m = 1$.

Let $G_1, \ldots, G_v$ denote the minimal polynomials in $\mathbf{Z}[\mathbf{x}; Y]$ of the elements of V. Choose $\tilde{\mathbf{x}} \in \mathbf{Z}^t$ such that $p(\tilde{\mathbf{x}}) \neq 0$, $F(\tilde{\mathbf{x}}; Y)$ is not identically zero and $G_i(\tilde{\mathbf{x}}; \alpha) \neq 0$ for each i in $\{1, \ldots, v\}$ and $\alpha \in \{0\} \cup \{\rho : \rho^m = 1\}$. (Note that no $G_i(\mathbf{X}, \alpha)$ is identically zero). Let $\tilde{y}$ be a zero of $F(\tilde{\mathbf{x}}; Y)$. It is now obvious that ϕ, defined by $\tilde{\mathbf{x}}$ and $\tilde{y}$, satisfies the assertion of Lemma 2. ∎

Proof of Theorem 9. Let $U = \{u_m\}_{m=0}^{\infty}$ be a non-degenerate recurrence sequence of rank $r \geq 2$. Then there are non-zero polynomials $f_i \in \mathbf{C}[X]$ and $\omega_i \in \mathbf{C}^*$ for $i = 1, \ldots, r$ such that

$$u_m = \sum_{i=1}^{r} f_i(m)\omega_i^m \qquad \text{for } m = 0, 1, 2, \ldots$$

and ω_i/ω_j is not a root of unity for $1 \leq i < j \leq r$. Let $R \subset \mathbf{C}$ be a ring which is finitely generated over $\mathbf{Z}$, and let K be the smallest subfield of $\mathbf{C}$ which contains R, $\omega_1, \ldots, \omega_r$ and the coefficients of $f_1, \ldots, f_r$.

We first show that it suffices to show Theorem 9 in the algebraic case, i.e. when $K \subseteq \mathbf{A}$. So suppose that Theorem 9 holds in the algebraic case and that $K/\mathbf{Q}$ is transcendental. Let $\hat{R}$ be the ring generated by R,

the coefficients of $f_1, \ldots, f_r$ and $\omega_1, \ldots, \omega_r$, $\omega_1^{-1}, \ldots, \omega_r^{-1}$. By Lemma 2 there is a specialisation $\phi : \hat{R} \to \mathsf{A}$ such that ϕ maps non-zero coefficients of the f_i on non-zero numbers, and all quotients ω_i/ω_j $(i \neq j)$ on numbers different from 0 and roots of unity. Then ϕ maps U on the sequence $\tilde{U} := \{\tilde{u}_m\}_{m=0}^{\infty} := \{\phi(u_m)\}_{m=0}^{\infty}$ where

$$\tilde{u}_m = \sum_{i=1}^{r} \tilde{f}_i(m)\tilde{\omega}_i^m \qquad \text{for } m = 0, 1, 2, \ldots,$$

$\tilde{f}_i \in \mathsf{A}[X]$ and $\tilde{\omega}_i = \phi(\omega_i) \in \mathsf{A}^*$. Obviously $\tilde{U}$ is a non-degenerate recurrence sequence of rank $r \geq 2$. Let (m, n) be a pair of integers with

$$\begin{aligned} &m > n \geq 0, \qquad \zeta_{m,n} u_m = u_n, \\ &\zeta_{m,n} \in R \setminus \{0\}, \qquad \zeta_{m,n} = 1 \quad \text{if } u_n = 0. \end{aligned} \tag{8.8}$$

Then, on putting $\tilde{R} = \phi(R)$, $\tilde{\zeta}_{m,n} = \phi(\zeta_{m,n})$, we obtain

$$\tilde{\zeta}_{m,n} \tilde{u}_m = \tilde{u}_n, \qquad \tilde{\zeta}_{m,n} \in \tilde{R}. \tag{8.9}$$

$\tilde{R}$ is finitely generated over $\mathbf{Z}$, but $\tilde{\zeta}_{m,n}$ may be 0. However, from Theorem 9 in the algebraic case it follows that there is an n_0 such that $\tilde{u}_n \neq 0$ for $n \geq n_0$, whence (8.9) is satisfied by at most finitely many pairs m, n with $m > n \geq n_0$. We infer that (8.8) is satisfied by only finitely many pairs m, n with $m > n \geq n_0$. To prove that (8.8) holds for only finitely many pairs with $n < n_0$, take a specialisation ϕ' having the same properties as ϕ and the additional property that $\phi'(u_n) \neq 0$ for each $n < n_0$ with $u_n \neq 0$, and repeat the arguments given above.

We shall now prove Theorem 9 in the algebraic case. Henceforth, the field K is an algebraic number field and S a finite set of places on K containing the infinite places, such that all non-zero coefficients of the polynomials f_i and all ω_i $(i = 1, \ldots, r)$ are S-units, and such that all elements of R are S-integers.

We shall need two other lemmas.

Lemma 3. *Let $p \in \mathsf{A}(X)$ be a rational function with no poles outside the disc $\{z \in \mathbf{C} : |z| \leq A\}$ and let $\alpha \in \mathsf{A}^*$. If there are infinitely many pairs of integers m, n with*

$$m > n \geq A, \qquad p(m)\alpha^m = p(n)\alpha^n$$

then p is constant and α is a root of unity.

Proof (cf. [77] pp. 84–85). We assume that

$$p(X) = \frac{X^k + a_{k-1}X^{k-1} + \ldots + a_1X + a_0}{X^\ell + b_{\ell-1}X^{\ell-1} + \ldots + b_1X + b_0}$$

which is no restriction. Let $\overline{p}(z)$ be the rational function obtained from $p(z)$ by replacing all coefficients of p by their complex conjugates. If $k \neq \ell$ we put $F(X) = p(X)\overline{p}(X)(\alpha\overline{\alpha})^X$ and if $k = \ell$ and α is a root of unity of order q say, we define $F(X)$ to be a non-constant function from $\{p(X)^q + \overline{p}(X)^q,\ i(p(X)^q - \overline{p}(X)^q)\}$. In both cases $p(m)\alpha^m = p(n)\alpha^n$ implies $F(m) = F(n)$, and there is an x_0 such that $F(x)$ is monotone for $x \geq x_0$. We conclude that $p(m)\alpha^m = p(n)\alpha^n$ for at most finitely many pairs of integers m, n with $m > n$.

We now consider the remaining case: $k = \ell$ and α is not a root of unity. We suppose $|\alpha| \leq 1$ which is no restriction. By $c_1, c_2, \ldots$ we denote (effectively computable) numbers depending only on α and p. We have $|p(m) - 1| \leq c_1/m$ for $m \geq m_0$. Hence, for $m > n \geq m_0$ with $p(m)\alpha^m = p(n)\alpha^n$,

$$|\alpha^{m-n} - 1| \leq |\alpha|^{m-n}|1 - p(m)| + |p(n) - 1| \leq \frac{c_2}{n}.$$

On the other hand, by Baker's theorem [3] (which is the analogue of Lemma 1a) for algebraic numbers) we have, noting that α is not a root of unity,

$$|\alpha^{m-n} - 1| \geq |m - n|^{-c_3}.$$

Hence

$$n \leq c_4(m - n)^{c_5}. \tag{8.10}$$

By assumption, α is not a root of unity. Hence there is a valuation $|\,.\,|_v$ on the smallest number field K containing α and the coefficients of p with $|\alpha|_v := c_6 > 1$. Therefore

$$c_6^{m-n} = |\alpha|_v^{m-n} = \left|\frac{p(n)}{p(m)}\right|_v \leq c_7 m^{c_8}$$

which implies $m - n \leq c_9 \log m$. Together with (8.10) this shows that

$$m = n + m - n \leq c_4(m - n)^{c_5} + m - n \leq c_{10}(\log m)^{c_{11}}.$$

Hence m is bounded. ∎

The next lemma was already stated in van der Poorten and Schlickewei [67].

Lemma 4. *Let T be a finite set of places on K, containing S. Then for every ϵ with $0 < \epsilon < 1$ there is an m_0 depending only on ϵ and T such that for all $m \geq m_0$,*

$$\prod_{v \in T} |u_m|_v \geq \Big\{ \prod_{v \in S} \max\big(|\omega_1|_v, \ldots, |\omega_r|_v\big) \Big\}^{m(1-\epsilon)} > 0. \tag{8.11}$$

Proof. We shall prove Lemma 4 by induction on r. For $r = 1$, Lemma 4 is obvious. Suppose that (8.11) holds for all non-degenerate recurrence sequences of rank less than r where $r \geq 2$ (induction hypothesis). We have the identity

$$u_m - \sum_{i=1}^{r} f_i(m)\omega_i^m = 0 \quad \text{for } m = 0, 1, 2, \ldots. \tag{8.12}$$

By the induction hypothesis, there is an m_1 such that no proper, non-empty subsum of this sum vanishes for $m \geq m_1$. Let $0 < \epsilon < 1$. Let H_m be the projective height of the projective point $(u_m : -f_1(m)\omega_1^m : \ldots : -f_r(m)\omega_r^m)$. It is easy to show that there is an $m_2 = m_2(\epsilon, T) > m_1$ such that

$$H_m \geq \Big\{ \prod_{v \in S} \max\big(|\omega_1|_v, \ldots, |\omega_r|_v\big) \Big\}^{m(1-\epsilon/5)}$$

for all $m \geq m_2$. Moreover, there is an $m_3 = m_3(\epsilon, T) > m_2$ such that for all $m \geq m_3$,

$$\prod_{v \in T} \prod_{i=1}^{r} |f_i(m)\omega_i^m|_v \leq H_m^{\epsilon/5},$$

since all ω_i are S-units. If $m > m_3$ does not satisfy (8.11) then

$$\prod_{v \in T} \Big(|u_m|_v \prod_{i=1}^{r} |f_i(m)\omega_i^m|_v \Big) \leq H_m^{\frac{\epsilon}{5} + \frac{1-\epsilon}{1-\epsilon/5}} \leq H_m^{1-\epsilon/2}.$$

Recall that u_m and the $f_i(m)\omega_i^m$ are all T-integers. Together with the Main Theorem on S-Unit Equations this implies that there are only finitely many projective points $P_m = (u_m : f_1(m)\omega_1^m : \ldots : f_r(m)\omega_r^m)$ such that (8.11) is not satisfied. For each projective point $\underline{\alpha}$, there are only finitely many m with $P_m = \underline{\alpha}$. For if there were infinitely many such m, then there would be infinitely many pairs (m, n) with $m > n$ and

$$\frac{f_1(m)\omega_1^m}{f_1(n)\omega_1^n} = \frac{f_2(m)\omega_2^m}{f_2(n)\omega_2^n},$$

whence

$$\frac{f_1(m)}{f_2(m)}\left(\frac{\omega_1}{\omega_2}\right)^m = \frac{f_1(n)}{f_2(n)}\left(\frac{\omega_1}{\omega_2}\right)^n.$$

The latter is impossible by Lemma 3. This completes the proof of Lemma 4. ∎

Suppose that there are infinitely many pairs m, n with $m > n \geq 0$ for which a $\zeta_{m,n} \in R\setminus\{0\}$ exists such that $\zeta_{m,n}u_m = u_n$, i.e.

$$\sum_{i=1}^{r} \zeta_{m,n} f_i(m)\omega_i^m - \sum_{i=1}^{r} f_i(n)\omega_i^n = 0.$$

Then there are pairs of subsets (I_j, J_j) of $\{1,\dots,r\}$, for $j = 1,\dots,\ell$, such that $\bigcup_{j=1}^{\ell} I_j = \bigcup_{j=1}^{\ell} J_j = \{1,\dots,r\}$, the sets I_j and the sets J_j are pairwise disjoint, at least one of I_j, J_j is non-empty, there is an infinite set V of pairs (m,n) for which

$$m > n \geq 0, \quad \sum_{i\in I_j} \zeta_{m,n} f_i(m)\omega_i^m + \sum_{i\in J_j} \left(-f_i(n)\omega_i^n\right) = 0 \tag{8.13}$$

and no proper, non-empty subsum of this sum is 0.

We shall show that the cardinality of each I_j is at most 1. Suppose I_j contains two subscripts, which, for convenience, are taken equal to 1 and 2. Let $P_{m,n}$ be the projective point with entries $\zeta_{m,n}f_i(m)\omega_i^m$ $(i \in I_j)$ and $-f_i(n)\omega_i^n$ $(i \in J_j)$. Then the entries of $P_{m,n}$ are all S-integers. Moreover there are infinitely many different points among the $P_{m,n}$ with $(m,n) \in V$, for the sequence of m with $(m,n) \in V$ is unbounded, and by Lemma 3 there are only finitely many pairs (m_1, m_2) with $m_1 < m_2$, $(m_1, n_1) \in V$, $(m_2, n_2) \in V$ and

$$P_{m_1,n_1} = P_{m_2,n_2},$$

whence

$$\frac{f_1(m_1)}{f_2(m_1)}\left(\frac{\omega_1}{\omega_2}\right)^{m_1} = \frac{f_1(m_2)}{f_2(m_2)}\left(\frac{\omega_1}{\omega_2}\right)^{m_2}.$$

Let $H_{m,n}$ denote the height of $P_{m,n}$. It is easy to check that for m sufficiently large,

$$H_{m,n} \geq C^{4m/5} \tag{8.14}$$

where

$$C = \prod_{v\in S} \max(|\omega_1|_v, |\omega_2|_v).$$

By enlarging S if necessary, we may assume that $\prod_{v\in S}|u_n|_v \le C_1^{n(1+\kappa/10r)}$ for all $n \ge 0$ where $\kappa = \log C/\log C_1$ and $C_1 = \prod_{v\in S}\max(|\omega_1|_v,\dots,|\omega_r|_v)$. By Lemma 4 we have for m sufficiently large, that

$$\prod_{v\in S}|u_m|_v \ge C_1^{m(1-\kappa/10r)}.$$

Hence

$$\prod_{v\in S}|\zeta_{m,n}|_v = \prod_{v\in S}\left|\frac{u_n}{u_m}\right|_v \le C_1^{(m+n)\kappa/10r} \le C^{m/5r}.$$

This shows that for m sufficiently large, in view of (8.14)

$$\prod_{v\in S}\Big(\prod_{i\in I_j}|\zeta_{m,n}f_i(m)\omega_i^m|_v\prod_{i\in J_j}|f_i(n)\omega_i^n|_v\Big) \le C^{m/5} < H_{m,n}^{1/2}.$$

By Theorem 1, we obtain that there are only finitely many projective points $P_{m,n}$ and this yields a contradiction. Therefore no set I_j or J_j can have cardinality larger than 1.

We infer that there is a permutation σ of $(1,\dots,n)$ such that for all (m,n) in V

$$\zeta_{m,n}f_i(m)\omega_i^m = f_{\sigma(i)}(n)\omega_{\sigma(i)}^n. \tag{8.15}$$

If σ is the identity, then there are infinitely many pairs (m,n) with

$$\frac{f_1(m)}{f_2(m)}\left(\frac{\omega_1}{\omega_2}\right)^m = \frac{f_1(n)}{f_2(n)}\left(\frac{\omega_1}{\omega_2}\right)^n,$$

which is impossible in view of Lemma 3. If σ is not the identity, we derive a contradiction as follows (cf. [20] pp. 242–243). Let $i\in\{1,\dots,n\}$ such that $i\ne\sigma(i)$, and put

$$\theta_\ell = \omega_{\sigma^\ell(i)}/\omega_{\sigma^{\ell+1}(i)}, \quad q_\ell = f_{\sigma^{\ell+1}(i)}(n)/f_{\sigma^\ell(i)}(m).$$

Then, by (8.15),

$$\theta_\ell^m = \frac{q_\ell}{q_{\ell+1}}\theta_{\ell+1}^n \quad \text{for } \ell = 0,1,2\dots. \tag{8.16}$$

Let μ be the order of σ. Then $\theta_\mu = \theta_0$, $q_\mu = q_0$. By starting with $\theta_0^{m^\mu}$ and applying (8.16) μ times, we find

$$\theta_0^{m^\mu-n^\mu} = q_0^{m^{\mu-1}-n^{\mu-1}}q_1^{m^{\mu-2}n-m^{\mu-1}}q_2^{m^{\mu-3}n^2-m^{\mu-2}n}\dots q_{\mu-1}^{n^{\mu-1}-mn^{\mu-2}}. \tag{8.17}$$

All exponents are divisible by $m-n$. Choose a valuation $|.|_v$ with $|\theta_0|_v \geq c > 1$. Then the v-adic valuation of the left-hand side of (8.17) is bounded from below by $c^{m^{\mu-1}(m-n)}$, while the v-adic valuation of the right-hand side is bounded from above by $m^{c_1 m^{\mu-2}(m-n)}$ for some constant c_1. This shows that m is bounded. Thus the proof of Theorem 9 is complete. ∎

Lewis and Turk [55] studied the solubility of equation $u_m = au_n$ in integers $m > n$ where $U = \{u_m\}_{m=0}^{\infty}$ is a non-degenerate recurrence sequence and a some complex number. They gave various upper bounds which should be treated with care, since not all results are well stated. The methods are however correct and some of them are quite interesting, but they do not involve S-unit equations.

§9. Applications to recurrence sequences of algebraic numbers

We shall use the notation of §8 and consider recurrence sequences of algebraic numbers $U = \{u_m\}_{m=0}^{\infty}$. We assume that U is non-degenerate. It then follows that the coefficients c_i of the minimal recurrence relation (8.2), the roots ω_i of the companion polynomial and the coefficients of the polynomials f_i are all algebraic (cf. [77] Ch. R). Let K be an algebraic number field which contains all these algebraic numbers. By an argument similar to that employed in the proof of Lemma 4 in §8, van der Poorten and Schlickewei [67] proved that for every positive ϵ there exists a positive number C_1 depending only on U and ϵ such that

$$|u_m| > C_1\big(\max_{i=1,\ldots,r} |\omega_i|\big)^{(1-\epsilon)m} \tag{9.1}$$

for $m = 1, 2, \ldots$. This inequality should be compared with the opposite inequality

$$|u_m| < C_2\big(\max_{i=1,\ldots,r} |\omega_i|\big)^{(1+\epsilon)m}$$

for some effectively computable number C_2 depending only on U and ϵ, which follows directly from (8.3). Inequality (9.1) says that cancellation of terms in the sum on the right-hand side of (8.3) can occur only to a very limited extent (in the algebraic case).

For $\alpha \in K^*$ we define $P_K(\alpha)$ ($P_K^+(\alpha)$, respectively) to be the maximum of the norms of prime ideals $\wp$ such that for valuations v corresponding to $\wp$ one has $|\alpha|_v \neq 1$ ($|\alpha|_v < 1$ respectively) if such prime ideals $\wp$ exist and $P_K(\alpha) = 1$ ($P_K^+(\alpha) = 1$, respectively) otherwise. Further we put $P_K(0) = P_K^+(0) = 0$. We assume that U is non-degenerate

and of rank at least 2. Van der Poorten [66] noticed that Theorem 1 implies that $P_K(u_m) \to \infty$ as $m \to \infty$. Evertse [20] generalised this by proving

$$\lim_{\substack{m\to\infty \\ m>n \\ u_n\neq 0}} P_K(u_m/u_n) = \infty. \tag{9.2}$$

Theorem 9 implies the following stronger result.

Corollary 9.4.

$$\lim_{\substack{m\to\infty \\ m>n \\ u_n\neq 0}} P_K^+(u_m/u_n) = \infty.$$

Proof. It follows from Corollary 9.1 that $u_m u_n \neq 0$ for $m > n \geq n_0$. Put $\zeta_{m,n} = u_n/u_m$ for these values of m and n. Suppose there are infinitely many pairs (m,n) with $m > n \geq n_0$ such that $P_K^+(u_m/u_n)$ is bounded from above by M. Let S be the union of all infinite places on K and all finite places corresponding to prime ideals on K with norms at most M. Then the cardinality of S is finite. Further, $\zeta_{m,n}$ is an S-integer for infinitely many pairs m, n with $m > n \geq n_0$. The S-integers form a finitely generated subring of $\mathbf{C}$. Thus Theorem 9 implies that there are only finitely many pairs m, n with $m > n \geq n_0$ such that $\zeta_{m,n}$ is an S-integer, a contradiction. ∎

Since the proof of Theorem 1 is ineffective, it is impossible to derive lower bounds for $P_K(u_m)$ or $P_K^+(u_m/u_n)$ from the proof of Theorem 1.

If $k = r = 2$, then (8.3) becomes

$$u_m = \alpha\omega_1^m + \beta\omega_2^m \qquad (m = 0, 1, \ldots) \tag{9.3}$$

and it is possible to apply Theorems 2–5. We assume

$$\begin{gathered} \omega_1 \neq \omega_2, \qquad \omega = |\omega_1| \geq |\omega_2| > 0, \\ \omega_1/\omega_2 \text{ not a root of unity.} \end{gathered} \tag{9.4}$$

Let S be the smallest set of places on K containing all infinite places such that α, β, ω_1 and ω_2 are all S-units. Theorem 2 implies that for any non-zero complex number A the equation $u_m = A$ has at most $3 \times 7^{d+2s}$ solutions where d is the degree of K and s the cardinality of S. Theorem 3 implies that for given roots ω_1 and ω_2 there are only finitely many equivalence classes of recurrence sequences such that $u_m = A$ has more than two solutions m. If $u_m \in \mathbf{Z}$ for $m = 0, 1, \ldots$, then results of Kubota

[49] and Beukers [4] imply that $u_m = A$ has at most four solutions m. Upper bounds for the number of subscripts m with $u_m = A$ in the case that (9.3) yields a sequence of rational numbers, or even just algebraic numbers, are contained in the papers of Kubota [49] and Beukers and Tijdeman [5].

Since the proofs of Theorems 4 and 5 are effective, it is possible to derive effective bounds for sequences (9.3). First we state some results in case $u_m \in \mathbb{Z}$ for all m. Stewart [85] proved by Baker's method that there exist effectively computable numbers C_3 and m_1 depending *only on* α *and* β such that

$$|u_m| \geq \omega^{m - C_3 \log m} \qquad (m \geq m_1).$$

Parnami and Shorey [62] used this result to prove that $u_m = u_n$ with $m > n$ implies that m is bounded by an effectively computable constant and Shorey [76] even derived lower bounds for $|u_m - u_n|$. In the latter paper Shorey also proved that

$$P^+(u_m/u_n) \geq C_4 \left(\frac{m}{\log m}\right)^{1/(d_1+1)}$$

where $d_1 = [\mathbb{Q}(\omega_1) : \mathbb{Q}]$ and C_4 is an effectively computable number depending only on U. Stewart [86] and Shorey [75] also considered lower bounds for the greatest squarefree factor of u_m.

It is possible to generalise most of the above mentioned results to arbitrary algebraic recurrence sequences in K. Further Mignotte, Shorey and Tijdeman [58] have extended some results to the case $r = 3$. Their main result is that there exist effectively computable numbers C_5 and m_2 such that

$$|u_m| \geq \omega^m \exp\bigl(-C_5(\log m)^2\bigr) \qquad (m \geq m_2).$$

It seems impossible to prove such a result by Baker's method for r larger than 3. For these and related results, see Shorey and Tijdeman [77] Ch. R, 2, 3, 4.

§10. Applications to irreducible polynomials and arithmetic graphs

Let K be an algebraic number field, and S a finite set of places on K containing S_∞. Let N be a positive integer. For any finite subset

$\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ of $\mathcal{O}_S$ with $m \geq 3$, we denote by $\mathcal{G}_K(\mathcal{A}, S, N)$ the graph whose vertex set is $\mathcal{A}$ and whose edges are the unordered pairs α_i, α_j such that $N_S(\alpha_i - \alpha_j) = \prod_{v \in S} |\alpha_i - \alpha_j|_v^{[K:\mathbb{Q}]} > N$. If in particular $S = S_\infty$, then we shall denote this graph simply by $\mathcal{G}_K(\mathcal{A}, N)$. Many diophantine problems, for instance related to irreducibility of polynomials (see Theorem 12), decomposable form equations (see §11) or algebraic number theory (see §12), can be reduced to the study of connectedness properties of graphs $\mathcal{G}_K(\mathcal{A}, S, N)$. Such properties are stated in Theorems 10 and 11 below and these theorems can be used to solve the diophantine problems mentioned. Before stating Theorem 10, we introduce some terminology. If $\mathcal{G}$ is a graph, then, as usual, $|\mathcal{G}|$ and $\overline{\mathcal{G}}$ denote the order (the number of vertices) and the complement of $\mathcal{G}$, respectively. The *triangle hypergraph* $\mathcal{G}^T$ of $\mathcal{G}$ is that hypergraph whose vertices are the edges of $\mathcal{G}$ and whose edges are the triples of edges of $\mathcal{G}$ that form a triangle.

Theorem 10 (Győry [35], [42]). *Let $m \geq 3$ be a rational integer, $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ a subset of $\mathcal{O}_S$ and $\mathcal{G}_1, \ldots, \mathcal{G}_\ell$ the connected components of $\mathcal{G} = \mathcal{G}(\mathcal{A}, S, N)$ such that $|\mathcal{G}_1| \geq |\mathcal{G}_2| \geq \ldots \geq |\mathcal{G}_\ell|$. Then at least one of the following cases holds:*

i) *$\ell = 1$ and $\overline{\mathcal{G}}$ or $\overline{\mathcal{G}}^T$ is not connected;*

ii) *$\ell = 2$, $|\mathcal{G}_2| = 1$ and $\overline{\mathcal{G}}_1$ is not connected;*

iii) *$\ell = 2$, $2 \leq |\mathcal{G}_2| \leq |\mathcal{G}_1|$ and both $\mathcal{G}_1$ and $\mathcal{G}_2$ are complete;*

iv) *there is an $\epsilon \in U_S$ and for every pair i, j with $1 \leq i < j \leq m$ there is an $\alpha_{ij} \in \mathcal{O}_S$ such that*

$$\alpha_i - \alpha_j = \epsilon \alpha_{ij}$$

and

$$\max_{i,j} h(\alpha_{ij}) \leq \exp\{(c_1 s)^{c_2 s} P^{2d} \log 2N\}$$

where c_1, c_2 are effectively computable numbers depending only on m, d and D_K.

Except for certain trivial situations, each of the cases i) to iv) can occur (cf. [35]). The graphs $\mathcal{G}_K(\epsilon\mathcal{A} + \beta, S, N)$ have obviously the same structure for every $\epsilon \in U_S$ and $\beta \in \mathcal{O}_S$. It follows from Theorem 10 that apart from translation by elements of $\mathcal{O}_S$ and multiplication by elements of U_S, there are only finitely many m-tuples $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$ for which $\mathcal{G}_K(\mathcal{A}, S, N)$ is not of the type i), ii) or iii) and all those $\mathcal{A}$ can be, at least in principle, effectively determined.

Theorem 10 is proved by repeatedly applying Theorem 4. We sketch some ideas behind the proof of Theorem 10:

Suppose i), ii) and iii) do not hold. Then one can prove that

a) $\overline{\mathcal{G}}$ and its triangle hypergraph $\overline{\mathcal{G}}^T$ are connected; or

b) $\mathcal{G}$ has two connected components of order ≥ 2 of which at least one is not complete.

We shall sketch the proof that iv) holds in case a). Let $\{\alpha_i, \alpha_j, \alpha_k\}$ be an edge of $\overline{\mathcal{G}}^T$. Then

$$N_S(\alpha_i - \alpha_j) \leq N, \quad N_S(\alpha_j - \alpha_k) \leq N, \quad N_S(\alpha_k - \alpha_i) \leq N.$$

This implies that $\alpha_i - \alpha_j$, $\alpha_j - \alpha_k$, $\alpha_k - \alpha_i$ are $\tilde{S}$-units where $\tilde{S}$ is a finite set of places which contains S and depends only on N, K and S. Moreover,

$$\frac{\alpha_i - \alpha_j}{\alpha_i - \alpha_k} + \frac{\alpha_j - \alpha_k}{\alpha_i - \alpha_k} = 1.$$

By Theorem 4 this implies that there are only finitely many possible values for the quotient $(\alpha_i - \alpha_j)/(\alpha_j - \alpha_k)$, which can all be effectively determined. If $\{\alpha_j, \alpha_k, \alpha_\ell\}$ is another edge of $\overline{\mathcal{G}}^T$, then $(\alpha_j - \alpha_k)/(\alpha_k - \alpha_\ell)$ belongs to a finite, effectively determinable set, and so $(\alpha_i - \alpha_j)/(\alpha_k - \alpha_\ell)$ must belong to such a set. By continuing this argument, it follows that for any two connected pairs (α_i, α_j), (α_p, α_q) in $\overline{\mathcal{G}}^T$, $(\alpha_i - \alpha_j)/(\alpha_p - \alpha_q)$ belongs to a finite effectively determinable set. But $\overline{\mathcal{G}}^T$ is connected, hence for each quadruple $(\alpha_i, \alpha_j, \alpha_p, \alpha_q)$ for which $[\alpha_i, \alpha_j]$ and $[\alpha_p, \alpha_q]$ are edges in $\overline{\mathcal{G}}$, the quotient $(\alpha_i - \alpha_j)/(\alpha_p - \alpha_q)$ can assume only finitely many values which can be effectively determined. Fix p and q. Since $\overline{\mathcal{G}}$ is connected, each pair (α_a, α_b) can be connected by a path in $\overline{\mathcal{G}}$. By summing over all terms $(\alpha_i - \alpha_j)/(\alpha_p - \alpha_q)$ for the edges in this path we obtain that for each pair (a, b) the quotient $(\alpha_a - \alpha_b)/(\alpha_p - \alpha_q)$ can assume only finitely many values which can be determined effectively. Since $N_S(\alpha_p - \alpha_q) \leq N$, we have $\alpha_p - \alpha_q = \alpha_{pq}\epsilon$ where $\epsilon \in U_S$ and α_{pq} belongs to a finite set which can be effectively determined. From these facts it follows easily that $\alpha_a - \alpha_b = \alpha_{ab}\epsilon$ for each pair (α_a, α_b), where $\epsilon \in U_S$, and each α_{ab} belongs to a finite set which can be effectively determined. This proves (iv).

If the order of $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, S, N)$ is large enough then $\mathcal{G}$ cannot have property iii). This fact plays a crucial role in some applications to irreducible polynomials (see below and [41]) and polynomials of given discriminant (cf. §12 and [38]). Győry [35], [42] proved the following

theorem but with a weaker estimate for $|\mathcal{G}|$ than (10.1), since he used a weaker version of Theorem 2.

Theorem 11. *Let $\mathcal{A}$ be a finite subset of $\mathcal{O}_S$ and let $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, S, N)$. There exists an effectively computable positive number c_3, depending only on d and D_K, such that if*

$$|\mathcal{G}| > c_3 7^{2s} N^2 \tag{10.1}$$

then $\mathcal{G}$ has at most two connected components, and one of them is of order at least $|\mathcal{G}| - 1$.

For certain more general (but ineffective) versions of Theorems 10 and 11, see Győry [40]. Theorems 10 and 11 are slightly modified versions of Theorems 1, 2 of [35].

Theorems 10 and 11 have applications to irreducible polynomials. Here we shall present a consequence of Theorem 11. I. Schur and later A. Brauer, R. Brauer and H. Hopf investigated the reducibility of polynomials of the form $g(f(X))$ where f, g are monic polynomials in $\mathbf{Z}[X]$, g is irreducible over $\mathbf{Q}$ and the zeros of f are distinct elements of $\mathbf{Z}$. For a survey of results in this direction, see [29], [41]. Győry [28], [29], [41] extended these investigations to the case that the zeros of f are in an arbitrary totally real algebraic number field K of degree d. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\} \in \mathcal{O}_K^m$ be the set of zeros of such a monic polynomial $f \in \mathbf{Z}[X]$ and suppose that $g \in \mathbf{Z}[X]$ is an irreducible monic polynomial whose splitting field is a totally imaginary quadratic extension of a totally real number field. Consider the graph $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, N)$ with the choice $N = 2^d |g(0)|^{d/\deg(g)}$. Győry [28] proved that if this graph $\mathcal{G}$ has a connected component with k vertices, then the number of irreducible factors of $g(f(X))$ over $\mathbf{Q}$ is not greater than $\deg(f)/k$. This estimate is in general best possible (cf. [29]). Therefore, Theorem 11 implies the following

Theorem 12. *Let $f, g \in \mathbf{Z}[X]$ with the properties specified above. There is an effectively computable number c_4, depending only on d, h_K and D_K, such that if*

$$\deg(f) > c_4 |g(0)|^{2/\deg(g)}$$

then $g(f(X))$ is irreducible over $\mathbf{Q}$.

This theorem was proved by Győry [41] with a slightly weaker but explicit lower bound for $\deg(f)$ and in the more general case that the ground field is an arbitrary totally real number field (instead of $\mathbf{Q}$).

§11. Applications to decomposable form equations

Decomposable form equations form a very important class of polynomial diophantine equations. Many problems in number theory can be reduced to such equations. The most important types of decomposable form equations are Thue equations, norm form equations, discriminant form equations and index form equations. There is an extensive literature of equations of these types, and this will be the theme of the next memoir [25] in these Proceedings. Here we shall restrict ourselves to the application of unit equations to decomposable form equations. As will be seen, finiteness problems for decomposable form equations are in fact equivalent to finiteness questions concerning unit equations.

Let $F(X_1, X_2)$ be a binary form with coefficients in $\mathcal{O}_K$ and splitting field G over K. Let $\beta \in \mathcal{O}_K \setminus \{0\}$. By using their results on approximations of algebraic numbers, Thue [89] (in the case $K = \mathbb{Q}$) and Siegel [78], [80] showed that if

(a) F has at least three pairwise linearly independent linear factors in its factorisation over G

then the equation

$$F(x_1, x_2) = \beta \qquad \text{in } x_1, x_2 \in \mathcal{O}_K \tag{11.1}$$

has only finitely many solutions. Equation (11.1) is called a *Thue equation over* K. Further, as was (implicitly) pointed out by Siegel [79], [80], any unit equation in two variables (over K) can be reduced to a finite number of Thue equations (over K) and conversely, any Thue equation over K leads to a finite number of unit equations in two variables (over an appropriate extension of K). Indeed, since U_K is finitely generated, every solution of

$$\alpha_1 u + \alpha_2 v = 1 \qquad \text{in } u, v \in U_K \tag{11.2}$$

(where $\alpha_1, \alpha_2 \in K^*$) can be written in the form $u = u' x_1^n$, $v = v' x_2^n$ where $n \geq 3$ is a given positive integer, $x_1, x_2 \in U_K$, and $u', v' \in U_K$ can assume only finitely many values. Hence (11.2) reduces to finitely many Thue equations

$$(\alpha_1 u') x_1^n + (\alpha_2 v') x_2^n = 1 \qquad \text{in } x_1, x_2 \in \mathcal{O}_K.$$

We shall now show how the finiteness of the number of solutions of (11.1) follows from the fact that any equation of the form (11.2) has

only finitely many solutions. After multiplying (11.1) by an appropriate rational integer, (11.1) takes the form

$$\ell_1(\mathbf{x})\dots\ell_n(\mathbf{x}) = \beta' \quad \text{in } \mathbf{x} = (x_1, x_2) \in \mathcal{O}_K^2 \tag{11.3}$$

where the $\ell_i(\mathbf{X})$ $(i = 1, \dots, n)$ are linear forms in X_1, X_2 with coefficients in the ring of integers $\mathcal{O}_G$ of G. For every solution $\mathbf{x}$ of (11.3), each $\ell_i(\mathbf{x})$ divides β' in $\mathcal{O}_G$, and hence lies in a finite number of cosets of G^* with respect to the unit group U_G. If now e.g. ℓ_1, ℓ_2, ℓ_3 are pairwise linearly independent, then

$$\lambda_1 \frac{\ell_1(\mathbf{X})}{\ell_3(\mathbf{X})} + \lambda_2 \frac{\ell_2(\mathbf{X})}{\ell_3(\mathbf{X})} = 1$$

for appropriate $\lambda_1, \lambda_2 \in G^*$. The numbers $\ell_1(\mathbf{x})/\ell_3(\mathbf{x})$ and $\ell_2(\mathbf{x})/\ell_3(\mathbf{x})$ are contained in a finite number of cosets of G^* with respect to U_G, hence (11.3) yields a finite number of unit equations

$$\lambda_1' u + \lambda_2' v = 1 \qquad \text{in } u, v \in U_G.$$

For every solution u, v of this equation, $\ell_1(\mathbf{x})/\ell_3(\mathbf{x}) = u$, $\ell_2(\mathbf{x})/\ell_3(\mathbf{x}) = v$ determine $\ell_1(\mathbf{x})$, $\ell_2(\mathbf{x})$, $\ell_3(\mathbf{x})$ and hence $\mathbf{x}$, up to a proportional factor which can be determined from (11.3). There is a similar relationship between *Thue equations over* $\mathcal{O}_S$, i.e. equations of the type

$$F(x_1, x_2) = \beta \qquad \text{in } x_1, x_2 \in \mathcal{O}_S \tag{11.1'}$$

and S-unit equations in two variables (with not necessarily the same ground field and set of places S). Cf. Mahler [56] and Parry [63].

Thanks to Baker [1] and others, it turns out that the above arguments can be made effective and Theorem 4 (as well as its other versions) can be applied to obtain effective results for Thue equations. Baker [1], [2] proved (implicitly) the first version of Theorem 4 (for ordinary units) and used it to make effective Thue's and Siegel's finiteness theorems mentioned above by giving explicit upper bounds for the heights of the solutions of (11.1). Coates [11], [12], in the case $K = \mathbb{Q}$, and Győry [37], [39], in the general case, extended these results to equation (11.1'). By using (a more explicit version of) Theorem 4, it was shown in [37], [39] that all solutions x_1, x_2 of (11.1') satisfy

$$\max\{h(x_1), h(x_2)\} < \exp\{(c_1 s)^{c_2 s} P^{d+1}\}$$

where c_1 and c_2 are positive numbers depending only on β, F and K (which were given explicitly in [39]).

By means of (a generalisation of) Theorem 2, Evertse [19] and later Evertse and Győry [22] derived explicit upper bounds for the numbers of solutions of (11.1) and (11.1′) which are independent of the coefficients of F. In [22], the bound

$$4n \times 7^{2g(d+s+w(\beta))}$$

has been obtained for the number of solutions of (11.1′) where $n = \deg(F)$, $g = [G : K]$ (hence $1 \leq g \leq n!$) and $w(\beta)$ denotes the number of distinct prime ideal divisors of (β).

As a generalisation of (11.1) and (11.1′), consider the *decomposable form equations*

$$F(x_1, \ldots, x_m) = \beta \qquad \text{in } x_1, \ldots, x_m \in \mathcal{O}_K \tag{11.4}$$

or, more generally,

$$F(x_1, \ldots, x_m) = \beta \qquad \text{in } x_1, \ldots, x_m \in \mathcal{O}_S \tag{11.4′}$$

where $F(\mathbf{X}) = F(X_1, \ldots, X_m)$ is a *decomposable form* in $m \geq 2$ variables with coefficients in $\mathcal{O}_K$, i.e. a homogeneous polynomial which factorises into linear factors, $\ell_1(\mathbf{X}), \ldots, \ell_n(\mathbf{X})$ say, over some finite extension G of K.

In the case that F is a norm form and $K = \mathbb{Q}$, Schmidt [72] and Schlickewei [71] gave finiteness criteria for (11.4) and (11.4′), repectively. Their proofs are based on Schmidt's Subspace Theorem and its p-adic generalisation (cf. §4) and are ineffective. For generalisations to norm form equations over arbitrary finitely generated domains over $\mathbb{Z}$, see Laurent [52].

(11.4) and (11.4′) can be reduced to unit equations in a similar way as in the case $m = 2$ described above. Any linear relation $\lambda_{i_1}\ell_{i_1} + \ldots + \lambda_{i_r}\ell_{i_r} = 0$ with $\lambda_{i_1}, \ldots, \lambda_{i_r} \in G^*$ leads to finitely many inhomogeneous unit equations in $r - 1$ variables. But in contrast to the case $m = 2$, where one linear relation with $r = 3$ was enough, in general several linear relations are needed to prove the finiteness of the number of solutions of (11.4) and (11.4′). Győry (partly with Papp) extended the above method of reducing Thue equations to unit equations to all decomposable form equations in m (≥ 2) variables whose system of linear factors $\mathcal{L}_0 = \{\ell_1, \ldots, \ell_n\}$ satisfies the following conditions:

(b) $\operatorname{rank} \mathcal{L}_0 = m$;

(c) $\mathcal{L}_0$ can be divided into subsets $\mathcal{L}_1, \ldots, \mathcal{L}_h$ such that if $|\mathcal{L}_j| \geq 2$ for some j, then for each i, i' with $\ell_i, \ell_{i'} \in \mathcal{L}_j$ there exists a sequence

$\ell_i = \ell_{i_1}, \ldots, \ell_{i_r} = \ell_{i'}$ in $\mathcal{L}_j$ with the property that for $q = 1, \ldots, r-1$ there is a linear combination of ℓ_{i_q} and $\ell_{i_{q+1}}$, with coefficients in G^*, which also belongs to $\mathcal{L}_j$;

(d) There is a k with $1 \leq k \leq m$ such that X_k can be expressed as a linear combination of the forms from $\mathcal{L}_j$ for each j in $\{1, \ldots, h\}$.

By using Theorem 10, Győry [37], [39] showed that under assumptions (b), (c), (d), equation (11.4′) has only finitely many solutions with $x_k \neq 0$ and he gave an effective bound for the heights of the solutions. The condition $x_k \neq 0$ is necessary in general, but if $h = 1$ in (c) then conditions (d) and $x_k \neq 0$ can be dropped. This is always the case for Thue equations. Then $h = 1$ and (b), (c) are equivalent to condition (a).

Important special types of decomposable form equations are the *discriminant form equation*

$$D_{M/K}(\alpha_1 x_1 + \ldots + \alpha_m x_m) = \beta \quad \text{in } x_1, \ldots, x_m \in \mathcal{O}_S, \tag{11.5}$$

and the *norm form equation*

$$N_{M/K}(\alpha_0 x_0 + \ldots + \alpha_m x_m) = \beta \quad \text{in } x_0, \ldots, x_m \in \mathcal{O}_S, \tag{11.6}$$

where $\alpha_0 = 1$, $M = K(\alpha_1, \ldots, \alpha_m)$ is a finite extension of K, $1, \alpha_1, \ldots, \alpha_m$ are linearly independent over K, and $D_{M/K}$ and $N_{M/K}$ denote the discriminant and norm over K, respectively. As an application of his result on decomposable form equations with properties (b),(c),(d), Győry [39] gave explicit upper bounds for the heights of the solutions of (11.5) and (11.6), where in (11.6) he assumed that

$$[K(\alpha_0, \ldots, \alpha_{i+1}) : K(\alpha_0, \ldots, \alpha_i)] \geq 3 \quad \text{for } i = 0, \ldots, m-1.$$

Győry [36], [39] derived several results on index form equations and algebraic number theory from his result on (11.5).

Recently, Evertse and Győry [25] replaced conditions (b),(c),(d) by the slightly weaker condition (e) of Theorem 13. To state this theorem we need some further notation. Let $\mathcal{L}^*$ be a maximal set of pairwise linearly independent linear factors of $\mathcal{L}_0$. For any subspace V of K^m, let $r(V, \mathcal{L}^*)$ denote the minimum of all positive integers r for which there are $\ell_{i_1}, \ldots, \ell_{i_r}$ in $\mathcal{L}^*$ whose restrictions to V are linearly dependent, but pairwise linearly independent. If this minimum exists, then $r(V, \mathcal{L}^*) \geq 3$. Otherwise we put $r(V, \mathcal{L}^*) = 2$. Let $\mathcal{L} \supseteq \mathcal{L}^*$ be a finite set of pairwise linearly independent linear forms in $X_1, \ldots, X_m$ with coefficients in G. By applying Theorem 4 the following result can be proved.

Theorem 13. (Evertse and Győry [25]). *Suppose that*

(e) *for every subspace V of K^m of dimension ≥ 2 on which none of the forms in $\mathcal{L}$ vanishes identically, we have $r(V, \mathcal{L}^*) = 3$.*

Then there exists an effectively computable number c_3, depending only on K, S, F and *β, such that all solutions of the equation*

$$F(\mathbf{x}) = F(x_1, \ldots, x_m) = \beta \text{ in } \mathbf{x} \in \mathcal{O}_S^m \quad \text{with } \ell(\mathbf{x}) \neq 0 \text{ for all } \ell \in \mathcal{L} \tag{11.7}$$

satisfy $\max_i h(x_i) < c_3$.

If in particular $\mathcal{L} = \mathcal{L}^*$, then equation (11.7) reduces to (11.4′) and Theorem 13 provides an effective bound for the solutions of (11.4′). In [25], Theorem 13 is proved under a slightly weaker assumption which involves only a finite and effectively determinable collection of subspaces V of K^m.

The next result can be deduced from Theorem 2.

Theorem 14 (Evertse and Győry [22]). *With the above notation and under assumption* (e), *the number of solutions of* (11.7) *is at most*

$$n(4 \times 7^{2g(d+s+w(\beta))})^{m-1}.$$

It is a remarkable fact that this bound is independent of the coefficients of F. As a consequence of Theorem 14, Evertse and Győry [22] derived also explicit bounds for the numbers of solutions of (11.5) and (11.6), with similar conditions as for the effective results.

An application of Corollary 1.2 led to the following general finiteness criterion for decomposable form equations.

Theorem 15 (Evertse and Győry [24]). *The following two statements are equivalent*:

(f) *For every subspace V of K^m of dimension ≥ 2 on which none of the forms in $\mathcal{L}$ vanishes identically, we have $r(V, \mathcal{L}^*) \geq 3$;*

(g) *For every $\beta \in K^*$ and every finite subset S of M_K containing all infinite places,* (11.7) *has only finitely many solutions.*

Condition (f) is obviously weaker than (e). Theorem 15 implies, in an ineffective form, all the above-mentioned finiteness results for decomposable form equations (cf. [24]). In [57] Mason gave an analogous result for decomposable form equations over function fields which he derived from his own effective analogue of Corollary 1.2 over function fields.

As was pointed out in [24], Corollary 1.2 is a consequence of implication (f)$\Longrightarrow$(g) of Theorem 15. Indeed, let $\alpha_1, \ldots, \alpha_m \in K^*$ and consider the unit equation

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m = 1 \quad \text{in } x_1, x_2, \ldots, x_m \in U_S \tag{11.8}$$

with $\alpha_{i_1} x_{i_1} + \ldots + \alpha_{i_r} x_{i_r} \neq 0$ for all non-empty subsets $\{i_1, \ldots, i_r\}$ of $\{1, \ldots, m\}$. Put $F(\mathbf{X}) = X_1 \ldots X_m(\alpha_1 X_1 + \ldots + \alpha_m X_m)$, $\mathcal{L}^* = \{X_1, \ldots, X_m, \alpha_1 X_1 + \ldots + \alpha_m X_m\}$ and let $\mathcal{L}$ be the set of linear forms of the type $\alpha_{i_1} X_{i_1} + \ldots + \alpha_{i_r} X_{i_r}$ where $\{i_1, \ldots, i_r\}$ is a non-empty subset of $\{1, \ldots, m\}$. Since $F(\mathbf{x}) \in U_S$ for every solution $\mathbf{x} = (x_1, \ldots, x_m) \in U_S^m$ of (11.8), we have $F(\mathbf{x}) = \beta \epsilon^{m+1}$ where β, $\epsilon \in U_S$ and β can assume only finitely many values. This means that, with the notation $\mathbf{x}' = \mathbf{x}/\epsilon$, (11.8) reduces to finitely many equations of the type

$$F(\mathbf{x}') = \beta \quad \text{in } \mathbf{x}' = (x_1', \ldots, x_m') \in U_S^m$$
$$\text{with } \ell(\mathbf{x}') \neq 0 \text{ for all } \ell \in \mathcal{L}. \tag{11.9}$$

It was, however, shown in [24] that these $\mathcal{L}^*$ and $\mathcal{L}$ satisfy assumption (f) of Theorem 15. Therefore, by Theorem 15, equation (11.9) has only finitely many solutions $\mathbf{x}'$. This implies that (11.8) has indeed only finitely many solutions. In other words, Corollary 1.2 on unit equations is equivalent to the implication (f)$\Longrightarrow$(g) of Theorem 15. This contains as a special case the relationship observed by Siegel between Thue equations and unit equations in two variables.

Finally, we note that Theorems 14, 15 were proved in [22], [24], respectively, in the more general form when the ground ring is an arbitrary finitely generated extension ring of $\mathbf{Z}$. In the proofs the authors used Theorem 1′ and the general version of Theorem 2, respectively. Győry's effective results on decomposable form equations in [37], [39] have been extended to this more general situation in [43], [44].

§12. Applications to algebraic number theory

Several diophantine problems in algebraic number theory can be reduced to the study of the equations

$$D_{K/\mathbf{Q}}(\alpha) = D_0 \quad \text{in } \alpha \in \mathcal{O}_K \tag{12.1}$$

and

$$D(f) = D_0 \quad \text{in monic polynomials } f \in \mathbf{Z}[X] \tag{12.2}$$

where K is now an algebraic number field of degree $d \geq 2$, $D(f)$ and $D_{K/\mathbf{Q}}(\alpha)$ denote the discriminant of f and α, respectively, and $D_0 \in \mathbf{Z} \setminus \{0\}$. If α satisfies (12.1) then its minimal defining polynomial over $\mathbf{Z}$ satisfies (12.2). Equation (12.2) can have, however, other (not necessarily irreducible) solutions without zeros in K. Hence (12.2) is more general than (12.1). If α is a solution of (12.1) then so is $\alpha + a$ for all $a \in \mathbf{Z}$. Elements α, α' of $\mathcal{O}_K$ with $\alpha - \alpha' \in \mathbf{Z}$ are called $\mathbf{Z}$-*equivalent*. Similarly, if f is a solution of (12.2), then so is $f^*(X) = f(X + a)$ for every $a \in \mathbf{Z}$. Polynomials f, f^* of this kind are called $\mathbf{Z}$- *equivalent*. By repeatedly applying an earlier version of Theorem 4, Győry proved, in 1973, the following

Theorem 16 (Győry [30]). *Every solution α of* (12.1) *is $\mathbf{Z}$-equivalent to a solution $\alpha' \in \mathcal{O}_K$ for which*

$$H(\alpha') < c_1$$

where c_1 is an effectively computable number depending only on d, D_K and D_0.

In other words, there are only finitely many pairwise $\mathbf{Z}$- inequivalent elements in $\mathcal{O}_K$ with discriminant D_0, and a full set of representatives of such elements can be, at least in principle, effectively determined. This finiteness assertion was independently proved in a non-effective form by Birch and Merriman [7] in 1972.

We shall now sketch how (12.1) can be reduced to a finite system of unit equations. Let G be the normal closure of $K/\mathbf{Q}$ with degree g (over $\mathbf{Q}$) and let $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(d)}$ denote the conjugates of α with respect to $K/\mathbf{Q}$. If $d \geq 3$ then

$$\frac{\alpha^{(1)} - \alpha^{(i)}}{\alpha^{(1)} - \alpha^{(2)}} + \frac{\alpha^{(i)} - \alpha^{(2)}}{\alpha^{(1)} - \alpha^{(2)}} = 1 \quad \text{for } i = 3, \ldots, d. \tag{12.3}$$

Further, the numbers $\alpha^{(1)} - \alpha^{(2)}$, $\alpha^{(1)} - \alpha^{(i)}$, $\alpha^{(i)} - \alpha^{(2)}$ divide D_0 in $\mathcal{O}_G$, whence they belong to finitely many cosets of G^* with respect to U_G. Thus (12.3) reduces indeed to finitely many unit equations in two variables and, by Theorem 4, $\alpha^{(1)} - \alpha^{(i)}$, $\alpha^{(2)} - \alpha^{(i)}$ and so $\alpha^{(i)} - \alpha^{(j)}$ can be determined up to the common factor $\alpha^{(1)} - \alpha^{(2)}$ which is however determinable from (12.1), and Theorem 16 follows.

In fact Theorem 16 is an immediate consequence of Theorem 10. Let $\mathcal{A} = \{\alpha^{(1)}, \ldots, \alpha^{(d)}\}$ and $N = |D_0|^g$. By (12.1) we have

$$\left|N_{G/\mathbf{Q}}(\alpha^{(i)} - \alpha^{(j)})\right| \leq N \quad \text{for } 1 \leq i < j \leq d,$$

hence the graph $\mathcal{G}_G(\mathcal{A}, N)$ (cf. §10) has only isolated vertices. Therefore case iv) of Theorem 10 applies and the differences $\alpha^{(i)} - \alpha^{(j)}$ can assume only finitely many effectively determinable values, up to a common factor, while this common factor can be derived from (12.1).

If (12.1) is solvable then $D_K | D_0$. Denote by w the number of distinct prime factors of D_0/D_k. By means of Theorem 2 one can prove the following

Theorem 17 (Evertse and Győry [23]). *Equation* (12.1) *has at most* $7^{g(d-1)(2w+3)}$ *pairwise* $\mathbf{Z}$*-inequivalent solutions.*

We note that $d \leq g \leq d!$.

In view of a theorem of Minkowski d can be estimated from above explicitly in terms of D_K. Further, (12.1) implies $|D_K| \leq |D_0|$. Hence the dependence of c_1 on d and D_K in Theorem 16 can be dropped (cf. [30]). For irreducible polynomials $f \in \mathbf{Z}[X]$ this implies the following

Theorem 18 (Győry [30]). *Every solution* f *of* (12.2) *is* $\mathbf{Z}$*-equivalent to a solution* $f^* \in \mathbf{Z}[X]$ *for which*

$$\deg(f^*) \leq c_2, \qquad H(f^*) \leq c_3$$

where c_2, c_3 *are effectively computable numbers depending only on* D_0, *and* $H(f^*)$ *denotes the maximum absolute value of the coefficients of* f^*.

The 'reducible' case can be reduced to the 'irreducible' one by using the relation

$$D(F) = \prod_{i=1}^{k} D(f_i) \prod_{1 \leq i < j \leq k} \left(\mathrm{Res}(f_i, f_j)\right)^2$$

where $f = \prod_{i=1}^{k} f_i$ in $\mathbf{Z}[X]$ and $\mathrm{Res}(f_i, f_j)$ denotes the resultant of f_i and f_j. We note that in Theorem 18 an upper bound for $\deg(f^*)$ can also be derived by means of Theorem 11.

Theorem 18 implies that up to $\mathbf{Z}$-equivalence, there are only finitely many monic polynomials $f \in \mathbf{Z}[X]$ with discriminant $D_0 \neq 0$ and a full set of representatives of such polynomials can be effectively determined. For binary forms of given degree and given non-zero discriminant, a similar but ineffective finiteness theorem was independently proved by Birch and Merriman [7].

We present one consequence of Theorems 16 and 17 here. For other applications we refer to [32], [33], [36], [23]. As is known, there exist algebraic number fields K having *power integral bases* (i.e. integral bases

of the form $\{1, \alpha, \ldots, \alpha^{d-1}\}$ where $d = [K : \mathbb{Q}]$), but this is not the case in general. For references to results concerning power integral bases, see [46]. It is known that $\alpha \in \mathcal{O}_K$ generates a power integral basis if and only if $D_{K/\mathbb{Q}}(\alpha) = D_K$. If α is a generator then so are all $\alpha' \in \mathcal{O}_K$ which are $\mathbb{Z}$-equivalent to α. By applying Theorem 16 with $D_0 = D_K$, we have

Corollary 16.1 (Győry [32]). *If $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis of K, then there is an $\alpha' \in \mathcal{O}_K$ which is $\mathbb{Z}$-equivalent to α such that*

$$H(\alpha') < c_4$$

where c_4 is an effectively computable number depending only on d and D_K.

Thus, up to $\mathbb{Z}$-equivalence, there are only finitely many elements in $\mathcal{O}_K$ which generate a power integral basis and they can be effectively determined. In particular, one can decide at least in principle, whether K has a power integral basis or not.

Corollary 17.1 (Evertse and Győry [23]). *Up to $\mathbb{Z}$-equivalence there are at most $7^{3g(d-1)}$ elements $\alpha \in \mathcal{O}_K$ for which $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis for K.*

Since $g \leq d!$, this implies an upper bound depending only on d.

For explicit expressions for c_1 to c_4 and for references, see Győry [31], [33]. The results presented above have various generalisations; for references see [45], [46], [23].

§13. Applications to transcendental number theory

Let $g(z) = \sum_{k=1}^{\infty} z^{k!}$. Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers with $0 < |\alpha_i| < 1$ for $i = 1, \ldots, n$. D. W. Masser conjectured that if α_i/α_j is not a root of unity for $1 \leq i < j \leq n$, then $g(\alpha_1), \ldots, g(\alpha_n)$ are algebraically independent. Nishioka [60] used Theorem 1 to prove the stronger assertion that under the above conditions all numbers $g^{(\ell)}(\alpha_i)$ $(1 \leq i \leq n, \ell \geq 0)$ are algebraically independent.

Nishioka generalised the above result to more general gap series f. Let K be an algebraic number field. Let $f(z) = \sum_{k=0}^{\infty} a_k z^{e_k}$ be a power series with non-zero coefficients $a_k \in K$, positive convergence radius R and increasing non-negative exponents e_k satisfying

$$\lim_{k \to \infty} (e_k + \log M_k + \log A_k)/e_{k+1} = 0$$

where $A_k = \max(1, |a_0|, \ldots, |a_k|)$ and M_k is a positive integer such that $M_k a_0, \ldots, M_k a_k$ are algebraic integers. Cijsouw and Tijdeman [10] proved that $f(\alpha)$ is transcendental for any algebraic number α with $0 < |\alpha| < R$. Bundschuh and Wylegala [8] proved the remarkable result that $f(\alpha_1), \ldots, f(\alpha_n)$ are algebraically independent for any algebraic numbers $\alpha_1, \ldots, \alpha_n$ with $0 < |\alpha_1| < \ldots < |\alpha_n| < R$. There are several other papers on the algebraic independence of values of gap series, but nobody could handle the case of α_i of equal absolute values until Nishioka [61] applied Theorem 1. She proved the following general result.

Theorem 19. *Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers with $0 < |\alpha_i| < 1$ for $i = 1, \ldots, n$. Then the following three properties are equivalent.*

(i) *The numbers $f^{(\ell)}(\alpha_i)$ $(1 \le i \le n, \ell \ge 0)$ are algebraically dependent over the rationals.*

(ii) *The numbers 1, $f(\alpha_1)$, ..., $f(\alpha_n)$ are linearly dependent over the algebraic numbers.*

(iii) *There is a non-empty subset $\{i_1, \ldots, i_m\}$ of $\{1, \ldots, n\}$, a number γ, roots of unity $\zeta_1, \ldots, \zeta_m$ and algebraic numbers $d_1, \ldots, d_m$, not all zero, such that*

$$\alpha_{i_j} = \zeta_j \gamma \quad (1 \le j \le m) \qquad \text{and} \qquad \sum_{j=1}^{m} d_j \zeta_j^{e_k} = 0$$

for all sufficiently large k.

References

[1] A. Baker, Contributions to the theory of diophantine equations, *Philos. Trans. Roy. Soc. London* A **263** (1967/68), 173–208.

[2] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.

[3] A. Baker, The theory of linear forms in logarithms, *Transcendence Theory: Advances and Applications*, Academic Press, London, 1977, pp. 1–27.

[4] F. Beukers, The multiplicity of binary recurrences, *Compositio Math.* **40** (1980), 251–267.

[5] F. Beukers and R. Tijdeman, On the multiplicities of binary complex recurrences, *Compositio Math.* **51** (1984), 193–213.

[6] J.-P. Bézivin, Sur un Théorème de G. Pólya, *J. Reine Angew. Math.* **364** (1986), 60–68.

[7] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* (3) **24** (1972), 385–394.

[8] P. Bundschuh and F.-J. Wylegala, Über algebraische Unabhängigkeit bei gewissen nichtfortsetzbaren Potenzreihen, *Arch. Math.* **34** (1980), 32–36.

[9] J. W. S. Cassels, On a class of exponential equations, *Ark. Mat.* **4** (1961), 231–233.

[10] P. L. Cijsouw and R. Tijdeman, On the transcendence of certain power series of algebraic numbers, *Acta Arith.* **23** (1973), 301–305.

[11] J. Coates, An effective p-adic analogue of a theorem of Thue, *Acta Arith.* **15** (1968/69), 279–305.

[12] J. Coates, An effective p-adic analogue of a theorem of Thue II: The greatest prime factor of a binary form, *Acta Arith.* **16** (1969/70), 399–412.

[13] H. Davenport and K. F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 160–167.

[14] E. Dubois and G. Rhin, Sur la majoration de formes linéaires à coefficients algébriques réels et p-adiques, Démonstration d'une conjecture de K. Mahler, *C. R. Acad. Sci. Paris* **A 282** (1976), 1211–1214.

[15] P. Erdős, Problems in number theory and combinatorics, Proc. 6th Manitoba Conference on Numerical Math., *Congress Numer. 18, Utilitas Math., Winnipeg, Man.*, 1977.

[16] P. Erdős and R. L. Graham, Old and new problems and results in combinatorial theory: van der Waerden's theorem and related topics, *Enseign. Math.* (2) **25** (1979), 325–344.

[17] P. Erdős, C. L. Stewart and R. Tijdeman, On the number of solutions of the equation $x + y = z$ in S-units, *Compositio Math.*, to appear.

[18] P. Erdős and P. Turán, On a problem in the elementary theory of numbers, *Amer. Math. Monthly* **41** (1934), 608–611.

[19] J.-H. Evertse, On equations in S-units and the Thue-Mahler equation, *Invent. Math.* **75** (1984), 561–584.

[20] J.-H. Evertse, On sums of S-units and linear recurrences, *Compositio Math.* **53** (1984), 225–244.

[21] J.-H. Evertse, On equations in two S-units over function fields of characteristic 0, *Acta Arith.* **47** (1986), 233–253.

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

[23] J.-H. Evertse and K. Győry, On the number of polynomials and integral elements of given discriminant, *Acta Math. Hungar.*, to appear.

[24] J.-H. Evertse and K. Győry, Finiteness criteria for decomposable form equations, *Acta Math.*, to appear.

[25] J.-H. Evertse and K. Győry, Decomposable form equations, *New Advances in Transcendence Theory* (A. Baker ed.), Cambridge Univ. Press, 1988, Chapter 10.

[26] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, On S-unit equations in two unknowns, *Invent Math.*, to appear.

[27] J. P. Glass, J. H. Loxton and A. J. van der Poorten, Identifying a rational function, *C. R. Math. Rep. Acad. Sci. Canada* **3** (1981), 279–284. Corr. 4 (1982), 309–314.

[28] K. Győry, Sur l'irréductibilité d'une classe des polynômes I, *Publ. Math. Debrecen* **18** (1971), 289–307.

[29] K. Győry, Sur l'irréducibilité d'une classe des polynômes II, *Publ. Math. Debrecen* **19** (1972), 293–326.

[30] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, *Acta Arith.* **23** (1973), 419–426.

[31] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné II, *Publ. Math. Debrecen* **21** (1974), 125–144.

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

[33] K. Győry, On polynomials with integer coefficients and given discriminant IV, *Publ. Math. Debrecen* **25** (1978), 155–167.

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

[35] K. Győry, On certain graphs composed of algebraic integers of a number field and their applications I, *Publ. Math. Debrecen* **27** (1980), 229–242.

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

[37] K. Győry, On the representation of integers by decomposable forms in several variables, *Publ. Math. Debrecen* **28** (1981), 89–98.

[38] K. Győry, On discriminants and indices of integers of an algebraic number field, *J. Reine Angew. Math.* **324** (1981), 114–126.

[39] K. Győry, On S-integral solutions of norm form, discriminant form and index form equations, *Studia Sci. Math. Hungar.* **16** (1981), 149–161.

[40] K. Győry, On certain graphs associated with an integral domain and their applications to Diophantine problems, *Publ. Math. Debrecen* **29** (1982), 79–94.

[41] K. Győry, On the irreducibility of a class of polynomials III, *J. Number Theory* **15** (1982), 164–181.

[42] K. Győry, Effective finiteness theorems for Diophantine problems and their applications (in Hungarian), Academic doctor's thesis, Debrecen, 1983.

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

[44] K. Győry, On norm form, discriminant form and index form equations, *Coll. Math. Soc. J. Bolyai* **34**, Topics in Classical Number Theory, Budapest, 1981, North-Holland, Amsterdam etc., 1984, pp. 617–676.

[45] K. Győry, Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains, *J. Reine Angew. Math.* **346** (1984), 54–100.

[46] K. Győry, Sur les générateurs des ordres monogènes des corps de nombres algébriques, *Sém. Théorie des Nombres* 1983–84, Univ. Bordeaux, No. 32, 1984, 12 pp.

[47] K. Győry, C. L. Stewart and R. Tijdeman, On prime factors of sums of integers I, *Compositio Math.* **59** (1986), 81–88.

[48] K. Győry, C. L. Stewart and R. Tijdeman, On prime factors of sums of integers III, *Acta Arith.*, to appear.

[49] K. K. Kubota, On a conjecture of Morgan Ward, *Acta Arith.* **33** (1977), 11–48, 99–109.

[50] S. Lang, Integral points on curves, *Publ. Math. I.H.E.S.* **6** (1960), 27–43.

[51] S. Lang, Fundamentals of Diophantine Geometry, *Springer-Verlag*, Berlin, Heidelberg, New York, 1983.

[52] M. Laurent, Équations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299–327.

[53] C. Lech, A note on recurring series, *Ark. Mat.* **2** (1953), 417–421.

[54] D. J. Lewis and K. Mahler, On the representation of integers by binary forms, *Acta Arith.* **6** (1960/61), 333–363.

[55] D. J. Lewis and J. Turk, Repetitiveness in binary recurrences, *J. Reine Angew. Math.* **356** (1985), 19–48.

[56] K. Mahler, Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen, *Math. Ann.* **107** (1933), 691–730.

[57] R. C. Mason, Norm form equations IV; rational functions, *Mathematika* **33** (1986), 204–211.

[58] M. Mignotte, T. N. Shorey and R. Tijdeman, The distance between terms of an algebraic recurrence sequence, *J. Reine Angew. Math.* **349** (1984), 63–76.

[59] T. Nagell, Quelques problèmes relatifs aux unités algébriques, *Ark. Mat.* **8** (1969), 115–127.

[60] K. Nishioka, Proof of Masser's conjecture on the algebraic independence of values of Liouville series, *Proc. Japan Acad. Ser.* **A 62** (1986), 219–222.

[61] K. Nishioka, Conditions for algebraic independence of certain power series of algebraic numbers, *Compositio Math.*, **62** (1987), 53–61.

[62] J. C. Parnami and T. N. Shorey, Subsequences of binary recursive sequences, *Acta Arith.* **40** (1981/82), 193–196.

[63] C. J. Parry, The $\wp$-adic generalisation of the Thue-Siegel theorem, *Acta Math.* **83** (1950), 1–100.

[64] G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. Reine Angew. Math.* **151** (1921), 1–31.

[65] A. J. van der Poorten, Linear forms in logarithms in the p-adic case, *Transcendence Theory: Advances and Applications*, Academic Press, London, 1977, pp. 29–57.

[66] A. J. van der Poorten, Some problems of recurrent interest, *Coll. Math. Soc. János Bolyai* **34**, Topics in Classical Number Theory, North-Holland, Amsterdam, 1984, pp. 1265–1294.

[67] 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.

[68] H. P. Schlickewei, Linearformen mit algebraischen Koeffizienten, *Manuscripta Math.* **18** (1976), 147–185.

[69] H. P. Schlickewei, The $\wp$-adic Thue-Siegel-Roth-Schmidt theorem, *Arch. Math.* **29** (1977), 267–270.

[70] H. P. Schlickewei, Über die diophantische Gleichung $x_1 + x_2 + \ldots + x_n = 0$, *Acta Arith.* **33** (1977), 183–185.

[71] H. P. Schlickewei, On norm form equations, *J. Number Theory* **9** (1977), 370–380.

[72] W. M. Schmidt, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191** (1971), 1–20.

[73] W. M. Schmidt, Simultaneous approximation to algebraic numbers by elements of a number field, *Monatsh. Math.* **79** (1975), 55–66.

[74] W. M. Schmidt, *Diophantine Approximation*, Lect. Notes Math. **785**, Springer-Verlag, Berlin, Heidelberg, New York, 1980.

[75] T. N. Shorey, The greatest square free factor of a binary recursive sequence, *Hardy Ramanujan J.* **6** (1983), 23–36.

[76] T. N. Shorey, Linear forms in members of a binary recursive sequence, *Acta Arith.* **43** (1984), 317–331.

[77] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.

[78] C. L. Siegel, Approximation algebraischer Zahlen, *Math. Z.* **10** (1921), 173–213.

[79] C. L. Siegel, The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$, *J. London Math. Soc.* **1** (1926), 66–68.

[80] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss., Phys.-Math. Kl.*, **1929**, No. 1.

[81] J. H. Silverman, Quantitative results in diophantine geometry, Preprint, M. I. T., Cambridge, Mass., 1983.

[82] J. H. Silverman, A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves, *J. Reine Angew. Math.* **378** (1987), 60–100.

[83] Th. Skolem, A method for the solution of the exponential equation $A_1^{x_1} \dots A_m^{x_m} - B_1^{y_1} \dots B_n^{y_n} = C$ (Norwegian), *Norsk Mat. Tidsskr.* **27** (1945), 37–51.

[84] V. G. Sprindzhuk, Effective estimates in 'ternary' exponential diophantine equations (Russian), *Dokl. Akad. Nauk BSSR* **13** (1969), 777–780.

[85] C. L. Stewart, Divisor Properties of Arithmetical Sequences, Ph.D. Thesis, Univ. of Cambridge, Cambridge, 1976.

[86] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers III, *J. London Math. Soc.* (2) **28** (1983), 211–217.

[87] C. L. Stewart, Some remarks on prime divisors of sums of integers, Séminaire de Théorie des Nombres, Paris, 1984–85, *Progress in Mathematics* **63**, Birkhäuser, Boston etc., 1986, pp. 217–223.

[88] C. L. Stewart and R. Tijdeman, On prime factors of sums of integers II, in *Diophantine Analysis*, edited by J. H. Loxton and A. J. van der Poorten, Cambridge Univ. Press, 1986, pp. 83–98.

[89] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. Reine Angew. Math.* **135** (1909), 284–305.

[90] R. Tijdeman and L. Wang, Sums of products of powers of given prime numbers, *Pacific J. Math.* to appear.

[91] K. R. Yu, Linear forms in logarithms in the p-adic case, *New Advances in Transcendence Theory* (A. Baker ed.), Cambridge Univ. Press, 1988, Chapter 26.

[92] K. R. Yu, *Linear forms in the p-adic logarithms*, Max-Planck-Institut für Mathematik MPI/87–20, Bonn, F. R. Germany, 1986.