数理解析研究所講究録
958巻 1996年 62-78

APPLICATIONS OF UNIT EQUATIONS

K. GYŐRY (Debrecen, Hungary)
Univ.

INTRODUCTION

Unit equations have a lot of applications. The purpose of this paper is to give a short overview of unit equations and their applications. For more detailed surveys on the subject, we refer to Shorey and Tijdeman (1986), Evertse, Győry, Stewart and Tijdeman (1988a) and Győry (1992).

In Sections I and IV, the most important results are formulated for unit equations in $k = 2$ and $k \geq 2$ unknowns, respectively. Sections II and V are devoted to some applications. Finally, in Section III some conjectures and their implications are presented. At the end of the paper only those references are listed which are not included in the works mentioned above.

I. UNIT EQUATIONS IN TWO UNKNOWNS

First we introduce some notation which will be used throughout the paper. Let K be an algebraic number field, O_K the ring of integers of K, O_K^* the unit group of O_K, and $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ $(s \geq 0)$ a finite set of prime ideals in O_K. Then

$$O_S = \{a \in K : \mathrm{ord}_{\mathfrak{p}}(a) \geq 0 \text{ for all prime ideals } \mathfrak{p} \notin S\}$$

is a subring of K which is called the ring of S-integers. It contains O_K as a subring and, for $s = 0$ it is just O_K. The unit group O_S^* of O_S is called the group of S-units. As is known, it is finitely generated.

Let a_1, a_2 be non-zero elements of K. The equation

$$(1.1) \qquad a_1 u_1 + a_2 u_2 = 1 \quad \text{in } u_1, u_2 \in O_S^*$$

is called an S-unit equation. If $s = 0$, we speak simply about unit equation. Since O_S^* is finitely generated, (1.1) can be regarded as an exponential diophantine equation.

THEOREM A (Siegel (1921), Mahler (1933)). Equation (1.1) has only finitely many solutions.

This classical theorem was implicitly proved by Siegel for ordinary units, and by Mahler for S-units. They used their profound results on approximations of algebraic numbers.

The proof of Theorem A was ineffective, i.e. it did not provide any algorithm for determining the solutions of (1.1). Baker's method concerning linear forms in logarithms of algebraic numbers and its p-adic version made it possible to give an effective proof for Theorem A. We present now an effective and quantitative version of Theorem A.

Let $n = [K : \mathbb{Q}]$, let P be the maximum of the rational primes in $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ (with $P = 3$ if $s = 0$), and let $A = \max\{H(a_1), H(a_2), 3\}$ (where $H(a)$ denotes the ordinary height of an algebraic number a, i.e. the maximum of the absolute values of the coefficients of the minimal defining polynomial of a over $\mathbb{Z}$).

THEOREM B (Győry (1979)). Every solution of (1.1) satisfies

$$(1.2) \qquad \max_i H(u_i) < \exp\{(c_1(s+1))^{c_2(s+1)} P^{n+1} \log A\}$$

where $c_i = c_i(K)$ $(i = 1, 2)$ depend only on K and can be given explicitly.

This implies that, at least in principle, all solutions of (1.1) can be determined.

The bound in (1.2) is already best possible in terms of A. In 1979, I gave the constants c_1, c_2 explicitly. Recently, these values of c_1 and c_2 have been substantially improved by Bugeaud and Győry (199?).

EXAMPLE. When $K = \mathbb{Q}$ and $S = \{p_1, \dots, p_s\}$ is a finite set of primes, then $O_S = \mathbb{Z}[(p_1 \dots p_s)^{-1}]$ and

equation (1.1) takes the form

$$(1.3)\qquad a_1 p_1^{x_1} \cdots p_s^{x_s} + a_2 p_1^{y_1} \cdots p_s^{y_s} = 1 \quad \text{in } x_i, y_i \in \mathbb{Z}.$$

It follows from the recent explicit version of Theorem B that then every solution of (1.3) satisfies

$$\max\{|x_i|, |y_i|\} < (3(s+1))^{5(s+5)} p (\log p)^{s+1} \log A.$$

We note that recently Bombieri (1993) developed a new method for deriving explicit bounds for the solutions of unit equations. The above-mentioned bounds are, however, better than those obtained by Bombieri's method.

The following theorem was proved by a combination of a method of Mahler with hypergeometric functions.

THEOREM C (Evertse (1984)). Equation (1.1) has at most $3 \times 7^{3n+2s}$ solutions.

It is interesting to observe that this bound is independent of the coefficients a_1, a_2 . Erdős, Stewart and Tijdeman. (1988) showed that the above bound is not far from being best possible. Namely, they proved that if $K = \mathbb{Q}$, $a_1 = a_2 = 1$, p_i denotes the ith prime and s is large enough then (1.1) has more than $\exp\{(s/\log s)^{1/2}\}$ solutions.

Equation (1.1) and equation

$$a_1' u_1' + a_2' u_2' = 1 \quad \text{in } u_i' \in O_S^*$$

are called S-equivalent if $a_i'/a_i \in O_S^*$ for $i = 1, 2$. For given S , there are infinitely many S-equivalence classes of S-unit equations in two unknowns. S-equivalent equations have obviously the same number of solutions.

THEOREM D (Evertse, Győry, Stewart and Tijdeman (1988b)). Apart from finitely many S-equivalence classes, equation (1.1) has at most 2 solutions.

This bound is already sharp in the sense that if $s > 0$ then there are infinitely many S-equivalence classes with 2 solutions.

The above Theorems A, C and D were generalized (by Lang, Evertse, Győry, Stewart, Tijdeman and others) to the case

when O_S^* is replaced by an arbitrary finitely generated subgroup or a subgroup of finite rank of $\mathbb{C}^*$, the multiplicative group of non-zero complex numbers.

Some analogue results have also been established (by Győry, Mason, Evertse, Silverman and others) over function fields.

II. APPLICATIONS

Applications of S-unit equations in two unknowns led to the resolution of several open problems. We present some of these applications.

1. Polynomials diophantine equations

Let $F \in O_S[X,Y]$ be a binary form of degree $d \geq 3$ with distinct linear factors over $\mathbb{C}$, and let $b \in O_S \setminus \{0\}$. Consider the equation

$$F(x,y) = b \quad \text{in} \quad x, y \in O_S. \tag{2.1}$$

For $O_S = \mathbb{Z}$, Thue (1909) proved, in an ineffective way, that the number of solutions of (2.1) is finite. Hence (2.1) is called a Thue-equation. The first effective proof for this theorem was given by Baker (1968). In the proof he used his deep method concerning linear forms in logarithms of algebraic numbers. The results of Thue and Baker were generalized by several people.

The use of unit equations made it possible to generalize these results to equations in an arbitrary number of unknowns. We may assume without loss of generality that K is the splitting field of F. This can be achieved by a suitable extension of the ground field. Denote by H_b the height of b and by H_F the maximum of the heights of the coefficients of F. Using Theorem B, I proved in 1981 the following result as a spacial case of a more general theorem. If F has K as its splitting field, then for every solution of (2.1)

$$(2.2)\quad \max\{H(x),H(y)\} < \exp\{d^{6}(c_1(s+1))^{c_2(s+1)}P^{n+1}\log(H_F H_b)\}$$

where the constants $c_i = c_i(K)$ $(i=1,2)$ depend only on K and can be given explicitly.

This bound is already sharp in terms of H_F and H_b. In 1981, I expressed c_1 and c_2 explicitly. Recently, this bound has been considerably improved in Győry (199?) in terms of d and the parameters of K involved in c_1 and c_2.

Using his Theorem C on unit equations, Evertse (1984) proved that equation (2.1) has at most $7d^3(3n+2s)$ solutions. We note that other upper bounds have also been obtained by Silverman (1983), Bombieri (1994) and Fujimori (1994) without using unit equations. Bombieri's bound is of the form $(12d)^{12(n+s)}$.

The above-presented quantitative result concerning Thue equations was proved in a more general form, for decomposable form equations (including norm form equations, discriminant form equations and index form equations). For further effective results concerning these equations we refer to the papers of Győry, Győry and Papp, Trelina, Kotov, Evertse and Győry, and Evertse, respectively, quoted in Győry (198o), Evertse, Győry, Stewart and Tijdeman (1988a) and Evertse and Győry (1988a).

The above-mentioned results concerning polynomial equations have various further applications to superelliptic equations, algebraic number theory, irreducible polynomials, finite arithmetic progressions and so on.

2. Algebraic number theory

Unit equations have many applications to algebraic number theory. It was an old problem going back to Dedekind and Kronecker to determine power integral bases in O_K. An integral basis for O_K is called a power integral basis if it takes the form

$$\{1,\alpha,\dots,\alpha^{n-1}\} \Leftrightarrow O_K = \mathbb{Z}[\alpha] \Leftrightarrow D_{K/\mathbb{Q}}(\alpha) = D_K \quad (\alpha \in O_K)$$

where D_K denotes the discriminant of K. If K is quadratic or cyclotomic then O_K contains a power integral basis. However, as was showed by Dedekind, this is not the case in general. Several people, including Dedekind, Kronecker, Hensel,

Hasse and Nagell studied the question of existence and determination of power integral bases. If $O_K = \mathbb{Z}[\alpha]$ then $O_K = \mathbb{Z}[\alpha + a]$ for all $a \in \mathbb{Z}$. Using a version of Theorem B, I proved in 1976 in a quantitative form that up to translation by elements of $\mathbb{Z}$, there are only finitely many $\alpha \in O_K$ with $O_K = \mathbb{Z}[\alpha]$ and all these can be effectively determined.

I generalized this to the case when the ground ring is an arbitrary finitely generated integral domain over $\mathbb{Z}$ and proved also several related theorems. These results led to the resolution of some problems of Nagell, Narkiewicz, and Delone and Faddeev, respectively, on algebraic integers and polynomials of given discriminant (for references, cf. Győry (198o, 1984)).

Using Theorem C on unit equations, we proved with Evertse (1985) that up to translation by elements of $\mathbb{Z}$, the number of $\alpha \in O_K$ with $O_K = \mathbb{Z}[\alpha]$ is at most $(4 \times 7^{3n!})^{n-2}$.

3. Binary forms with given discriminant

The binary forms $F, G \in \mathbb{Z}[X,Y] = \mathbb{Z}[\underline{X}]$ are called equivalent if $F(\underline{X}) = G(U\underline{X})$ for some $U \in SL_2(\mathbb{Z})$. In this case they have the same discriminant. It is a classical theorem that for $n \geq 2$ and $D \neq 0$, there are only finitely many equivalence classes of binary forms $F \in \mathbb{Z}[\underline{X}]$ with degree n and discriminant D.

This theorem was proved

for $n = 2$ by Lagrange (1773) in an effective way,
for $n = 3$ by Hermite (1851) in an effective way,
for $n \geq 4$ by Birch and Merriman (1972) in an ineffective way,
for $n \geq 4$ and for the monic case (when $F(1,0) = 1$) by Győry (1973) in an effective way.

Further, I proved in 1974 that if $n = \deg F$ and $D = D(F) \neq 0$ then

$$n \leq 3 + \frac{2}{\log 3} \log |D|$$

and this is already sharp.

Using Theorem B on unit equations, Evertse and myself (1991) proved that there are only finitely many equivalence classes of binary forms $F \in \mathbb{Z}[\underline{X}]$ with discriminant $D \neq 0$ and

all them can be effectively determined.

We proved this in a quantitative and more general form, over O_S instead of $\mathbb{Z}$. In 1992, we generalized our result for decomposable forms over O_S. These results were applied by Evertse and Győry (1991, 1992) to the geometry of numbers and algebraic number theory, and by Brindza, Evertse and Győry (1991) and Thunder (1994) to diophantine equations.

4. Prime factors of sums of integers

Denote by $|A|$ the cardinality of a finite set A, and by $\omega(a)$ the number of distinct prime factors of a positive integer a. Let A, B be finite subsets of $\mathbb{N}$, the set of positive integers. It was conjectured by Erdős and Turán in the thirties that if $k = |A| = |B| \geq 2$ then

$$\omega\Big(\prod_{a\in A, b\in B}(a+b)\Big) \to \infty \quad \text{as} \quad k \to \infty.$$

They confirmed their conjecture for $A = B$.

Using Theorem C, Győry, Stewart and Tijdeman (1986) proved the conjecture in a more general and more precise form by showing that if $k = |A| \geq |B| \geq 2$ then

$$\omega\Big(\prod_{a\in A, b\in B}(a+b)\Big) > c \log k$$

with an effectively computable absolute constant $c > 0$.
As was proved by Erdős, Stewart and Tijdeman (1988), this lower bound is not far from the best possible.

Recently, Győry, Sárközy and Stewart (199?) have proved an analogue of the above result. They showed that if $k = |A| \geq |B| \geq 2$ then

$$\omega\Big(\prod_{a\in A, b\in B}(ab+1)\Big) > c' \log k$$

where $c' > 0$ is an effectively computable absolute constant. Further, they obtained a common generalization of the above results concerning numbers of the form $a+b$ and $ab+1$, respectively.

5. Arihmetic graphs

Using Theorems B, C and D, Győry (198o, 199o, 1992) proved finiteness theorems for some arithmetic graphs which led to further applications to algebraic number theory and irreducible polynomials. It should also be mentioned the results of Leutbecher and Niklasch(1989) on these graphs and their applications to Euclidean number fields.

6. Polynomials of given number of terms

Using Theorems C and D, Győry and Schinzel (1994) solved a problem of Posner and Rumsey (1965) on polynomials of given number of terms.

7. Finitely generated groups

Finally, we mention an interesting result of Chaltin (1992) on finitely generated groups in the proof of which Theorem B was utilized on unit equations.

III. CONDITIONAL RESULTS

In the special case $K = \mathbb{Q}$, $a_1 = a_2 = 1$, unit equation (1.1) can be written in the form

$$A + B = C$$

where A, B, C are positive integers composed of primes $p_1, \dots, p_s$.

The Oesterlé-Masser or ABC conjecture asserts that for any given $\varepsilon > 0$, there is an effectively computable $c = c(\varepsilon)$ such that

$$C < c(p_1 \dots p_s)^{1+\varepsilon}.$$

A similar conjecture has been formulated by Vojta (1987) over number fields. This suggests that the bound in Theorem B is still far from the best possible.

The ABC conjecture and its analogue over number fields have profound implications:

1. Fermat's conjecture

Suppose that there exist positive integers x, y, z and $n \geq 4$ such that

$$x^n + y^n = z^n.$$

Then, by the ABC conjecture, we have

$$z^n < c \Big(\prod_{p \mid x^n y^n z^n} p \Big)^{1+\varepsilon} = c \Big(\prod_{p \mid xyz} p \Big)^{1+\varepsilon} \leq$$

$$\leq c\,(xyz)^{1+\varepsilon} < c\, z^{3(1+\varepsilon)}$$

whence $z^{n-3(1+\varepsilon)} < c$. This implies that if ε is small then x, y, z and n are bounded and they can be effectively determined.

2. Faltings' theorem (Mordell's conjecture)

Elkies (1991) deduced from the ABC conjecture over number fields Faltings' finiteness theorem on rational points of curves of genus > 1.

3. Roth's approximation theorem

Recently Bombieri and Langevin showed independently of each other that the ABC conjecture over number fields implies an effective version of Roth's theorem on approximation of algebraic numbers.

4. "Siegel zeros" of L-functions

Using the ABC conjecture over number fields, Granville and Stark (199?) have recently proved that there are no "Siegel zeros" for any L-functions of characters associated to imaginary quadratic number fields.

IV. UNIT EQUATIONS IN $k \geq 2$ UNKNOWNS

Let $a_1, \ldots, a_k$ be non-zero elements of K, and consider the following generalization of equation (1.1) :

$$(4.1) \qquad a_1 x_1 + \ldots + a_k x_k = 1 \quad \text{in } x_1, \ldots, x_k \in O_S^*.$$

This equation is called an S-unit (unit) equation in k unknowns. The solution $x_1, \ldots, x_k$ is called degenerate if the left hand side of (4.1) has a vanishing subsum $\sum_{i \in I} a_i x_i = 0$ for some $I \subseteq \{1, \ldots, k\}$. In this case there exist infinitely many degenerate solutions (provided that O_S^* is infinite).

Van der Poorten and Schlickewei and, independently, Evertse proved the following.

THEOREM E (van der Poorten and Schlickewei (1982), Evertse (1984)). Equation (4.1) has only finitely many non-degenerate solutions.

For $k = 2$, this gives Theorem A. In the proof, the authors used the deep Thue-Siegel-Roth-Schmidt method, more precisely an appropriate version of the Subspace Theorem.

Bounds for the number of non-degenerate solutions which are independent of $a_1, \ldots, a_k$ were obtained by Evertse and Győry (1988) and Schlickewei (199o). The best known bound is due to Evertse.

THEOREM F (Evertse (199?)). Equation (4.1) has at most

$$\{2^{34}(k+1)^2\}^{k^3(n+s)} \qquad (n = [K:\mathbb{Q}],\ s = |S|)$$

non-degenerate solutions.

This implies a weaker version of Theorem C.

For given k, equivalence of equations of the form (4.1) can be defined in the same way as in the case $k = 2$.

THEOREM G (Evertse and Győry (1988)). Let $k \geq 2$. Apart from finitely many equivalence classes of equations (4.1), the solutions of (4.1) are contained in the union of fewer than $2^{(k+1)!}$ $(k-1)$-dimensional linear subspaces of K^k.

Evertse (1992) improved the bound $2^{(k+1)!}$ to $(k!)^{2k+2}$. For $k = 2$, these results give Theorem D in a weaker form.

Theorems E, F (with other bounds) and G were generalized (by van der Poorten and Schlickewei, Laurent, Evertse and Győry, Győry, Schlickewei and others) to the case when $\mathcal{O}_S^*$ is replaced by an arbitrary finitely generated subgroup or a subgroup of finite rank of $\mathbb{C}^*$. Analogue results have also been established (by Mason, Brownawell and Masser, Voloch, Noguchi and others) over function fields.

V. APPLICATIONS

In what follows, we present some applications of Theorems E, F and G.

1. Decomposable form equations

Let $F \in \mathbb{Z}[X_1, \ldots, X_m]$ be a decomposable form, i.e. a homogeneous polynomial which is a product of linear forms with algebraic coefficients. The equation

$$(5.1) \qquad F(x_1, \ldots, x_m) = b \quad \text{in} \quad x_1, \ldots, x_m \in \mathbb{Z}$$

is called a decomposable form equation.

When $m = 2$, i.e. F is a binary form, (5.1) is just a Thue equation.

When $m \geq 2$ and $F = N_{K/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_m X_m)$ is a norm form where $\alpha_1, \ldots, \alpha_m$ are given elements of K, (5.1) is called a norm form equation. In this case Schmidt (1971,1972) proved a finiteness criterion for (5.1) and gave a description of the set of solutions. In fact he showed that all solutions are contained in finitely many so-called families of solutions. Later Schlickewei and Laurent extended this to the case of more general ground rings. They deduced their results from the Subspace Theorem, and did not use unit equations.

The use of unit equations made it possible to obtain

finiteness results on decomposable form equations in full generality and over more general ground rings. Using Theorem E, we gave with Evertse (1988b) a general finiteness criterion. Further, we proved that unit equations and decomposable form equations are equivalent in the sense that any unit equation can be reduced to finitely many decomposable form equations and conversely, any decomposable form equation can be reduced to finitely many unit equations over an appropriate extension of the ground ring.

In Győry (1993a) I showed in full generality that the set of solutions of a decomposable form equation is the union of finitely many families of solutions. Further, using an earlier version of Theorem F, I gave an explicit upper bound for the number of families of solutions which is independent of the coefficients of F. In case of finitely many solutions, this provided an explicit upper bound for the number of solutions as well. These implied all former (ineffective) finiteness results on decomposable form equations and led to several further applications.

Recently Evertse (199?) proved that if the number of solutions of (5.1) is finite, then this number is at most

$$(2^{34}d^2)^{m^3(t+1)}$$

where $d = \deg F$ and t denotes the number of distinct prime factors of b.

With the help of Theorem F we have recently derived with Evertse (199?) improved bounds for the number of families of solutions of decomposable form equations over O_S. This enabled us to prove that if (5.1) has infinitely many solutions then the number of solutions with $\max_i |x_i| \le N$ is

$$c \log^+ N + O((\log N)^{r-1}) \quad (c>0)$$

where r denotes the maximum of the ranks of the families of solutions. This gives as a special case some results of Pethő and myself (1977) on norm form equations.

2. Resultant equations (with one unknown polynomial)

Let $P \in O_S[X]$ be a polynomial of degree $m \ge 2$ without multiple zero and consider the resultant equation

(5.2) $\mathrm{Res}(P,Q) \in \mathcal{O}_S^*$ in $Q \in \mathcal{O}_S[X]$.

If Q is a solution then so is εQ for every $\varepsilon \in \mathcal{O}_S^*$. The solutions Q, εQ are called proportional.

In the case when $K = \mathbb{Q}$, Wirsing, Fujiwara, Schmidt and Schlickewei obtained finiteness results on resultant equations. In their proofs, they used various versions of the Subspace Theorem.

In Győry (1993b), a more general finiteness theorem was established for equation (5.2) whose proof depends on Theorem E on unit equations. In Győry (1994) I proved the following quantitative version of this theorem. Let k be a positive integer with $2k < m$. Then up to a proportional factor from $\mathcal{O}_S^*$, the number of solutions $Q(X)$ of (5.2) with degree k is at most

$$(2^{34} m^2)^{k^3(n+s)} \qquad (n = [K:\mathbb{Q}],\ s = |S|).$$

Further, in case of solutions $Q(X)$ with leading coefficients in $\mathcal{O}_S^*$, the assumption $2k < m$ can be replaced by $2k \leq m$.

The assumptions concerning P and k are necessary.

Recently, Hirata-Kohno generalized Schmidt's Subspace Theorem in a quantitative form. From this one can deduce bounds for the number of solutions of resultant inequalities as well.

3. Resultant equations (with two unknown polynomials)

Using Theorems E and F, Győry and Evertse and Győry have obtained general finiteness results for (5.2) in the case when both P and Q are unknowns, but their splitting field is fixed. For references, cf. Győry (1993c).

4. Irreducible polynomials of the form $P(X)+b$

Many people (including Pólya, Tatuzawa, A.Brauer, Ore, Weisner, Seres and Győry) published irreducibility results of Schur's type which assert that if $P \in \mathbb{Z}[X]$ with "many" distinct integer zeros and $b \in \mathbb{Z}$ with "small" absolute value then $P(X)+b$ is irreducible.

In the general case when $P \in \mathbb{Z}[X]$ is arbitrary, Hilbert's irreducibility theorem implies the irreducibility of $P(X)+b$ for infinitely many $b \in \mathbb{Z}$.

Szegedy (1984) proposed the following problem. Does there exist a constant $c = c(m)$ (depending only on m) such that for any $P \in \mathbb{Z}[X]$ of degree m, $P(X)+b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \le c$?

With the help of my above-stated quantitative result on resultant equations I proved in Győry (1994) the following. Let $P \in \mathbb{Z}[X]$ be a polynomial of degree m and let ω denote the number of distinct prime factors of the leading coefficient of P. There is a $b \in \mathbb{Z}$ with absolute value at most

$$\exp\{(\omega+1)^2 (2^{17} m)^{m^3}\}$$

such that $P(X)+b$ is irreducible over $\mathbb{Q}$.

For monic polynomials $P(X)$, this gives an affirmative answer to Szegedy's problem. It would be interesting to remove here the dependence on ω and obtain a bound which is polynomial in terms of m.

5. Irreducible polynomials of the form $g(f(X))$

Using Theorems B, C and E, I established irreducibility theorems of Schur's type for polynomials of the form $g(f(X))$ where g is a given irreducible polynomial and the polynomials $f(X)$ possess a fixed splitting field. These generalized several earlier results on the subject. For references, we refer to Győry (1992).

6. Sums of products of given primes

Denote by $w(n)$ the number of solutions of the equation

$$n = 2^x \cdot 3^y + 2^z + 3^v \quad \text{in non-negative integers } x, y, z, v.$$

By means of Theorem E Evertse, Győry, Stewart and Tijdeman (1988a)

proved that $w(n)$ is bounded. This confirmed a conjecture of D. Newman. In fact we proved this in a more general form, when 2 and 3 are replaced by finitely many given primes. Further, Tijdeman and L. Wang showed that for sufficiently large n we have $w(n) \geq 4$ and this bound is already sharp.

7. Transcendental number theory

Let $f(z) = \sum_{k=1}^{\infty} z^{k!}$. It is known that if $\alpha \in \bar{\mathbb{Q}}$ with $0 < |\alpha| < 1$ then $f(\alpha)$ is transcendental. Using Theorem E, Nishioka (1986) proved the following theorem. Suppose that $\alpha_1, \ldots, \alpha_n \in \bar{\mathbb{Q}}$ with $0 < |\alpha_i| < 1$ $(1 \leq i \leq n)$ and that no α_i/α_j $(1 \leq i < j \leq n)$ is a root of unity. Then the numbers $f^{(l)}(\alpha_i)$ $(1 \leq i \leq n, l \geq 0)$ are algebraically independent.

This confirmed a conjecture of Masser. Later Nishioka (1987, ...) proved some generalizations, p-adic analogues and several related results as well.

8. Recurrence sequences

The use of Theorems E, F and G enabled van der Poorten, Evertse, Győry, Stewart, Tijdeman, Laurent, Schlickewei and Schmidt to get some general theorems on recurrence sequences.

9. Linear equations in integers with bounded sums of digits

Using some versions of Theorems E and F, Schlickewei, Pethő and Tichy obtained finiteness results for linear equations in integers with bounded sums of digits.

10. Modular forms

With the help of Theorem E Odoni (1988) gave an affirmative answer to a question of Serre concerning modular forms.

11. Finitely generated and finitely presented groups

By means of Theorem E Evertse, Győry, Stewart and Tijdeman (1988a) solved a problem of Rhemtulla and Sidki on fintely generated groups. In this direction, further applications of unit equations were given by Tijdeman and L. wang, and Wilson.

Acknowledgements. The author would like to express his gratitude to the organizers of the conference and to the financial supporters, to the Nihon University, and to the Hungarian National Foundation for Scientific Research, who made possible his visit to Japan.

References

E. Bombieri (1993), Effective diophantine approximation on G_m, Ann.Scuola Norm.Sup.Pisa (IV) 2o, 61-89.

E. Bombieri (1994), On the Thue-Mahler equation II, Acta Arith. 67, 69-96.

B. Brindza, J.H. Evertse and K. Győry (1991), Bounds for the solutions of some diophantine equations in terms of discriminants, J.Austral.Math.Soc., (Ser A), 51, 8-26.

Y. Bugeaud and K. Győry (199?), Bounds for the solutions of unit equations, to appear.

H. Chaltin (1992), Groupes de Coxeter à torsion (II), C.R.Acad. Sci.Paris, 315 Série I, 175-178.

N. Elkies (1991), ABC implies Mordell, Int.Math.Res.Nat. 7, 99-109.

J.H. Evertse (1992), Decomposable form equations with a small linear scattering, J.Reine Angew.Math. 432, 177-217.

J.H. Evertse (199?), The number of solutions of decomposable form equations, to appear.

J.H. Evertse and K. Győry (1988a), Decomposable form equations, in "New Advances in Transcendence Theory" (A.Baker ed.), pp. 175-202. Cambridge University Press.

J.H. Evertse and K. Győry (1988b), Finiteness criteria for decomposable form equations, Acta Arith. 50, 357-379.

J.H. Evertse, K. Győry, C.L. Stewart and R. Tijdeman (1988a), S-unit equations and their applications, in "New Advances in Transcendence Theory" (A.Baker ed.), pp. 110-174. Cambridge University Press.

J.H. Evertse, K. Győry, C.L. Stewart and R. Tijdeman (1988b), On S-unit equations in two unknowns, Invent.Math. 92,461-477.

M. Fujimori (1994), On the solutions of Thue equations, Tôhoku Math.J. 46, 523-539.

A.Granville and H.M.Stark (199?), ABC implies no "Siegel zeros", to appear.

K. Győry (198o), Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers in Pure and Applied Math., No. 56. Kingston, Canada.

K. Győry (1984), Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains, J.Reine Angew.Math. 346, 54-1oo.

K. Győry (1992), Some recent applications of S-unit equations, Journées Arithmétiques de Genève (1991), (D.F.Coray, Y.-F.S. Pétermann eds.), Astérisque, 2o9, 17-38.

K. Győry (1993a), On the numbers of families of solutions of systems of decomposable form equations, Publ.Math.Debrecen 42, 65-1o1.

K. Győry (1993b), Some applications of decomposable form equations to resultant equations, Colloq.Math. 65, 267-275.

K. Győry (1993c), Some new results connected with resultants of polynomials and binary forms, Grazer Math.Ber. 318, 17-27.

K. Győry (1994), On the irreducibility of neighbouring polynomials, Acta Arith. 67, 283-294.

K. Győry (199?), Bounds for the solutions of decomposable form equations, to appear.

K. Győry and A. Schinzel (1994), On a conjecture of Posner and Rumsey, J.Number Theory 47, 63-78.

K. Győry, A. Sárközy and C.L. Stewart (199?), On the number of prime factors of integers of the form $ab+1$, to appear.

T.N. Shorey and R. Tijdeman (1986), Exponential diophantine equations, Cambridge University Press.

J.F. Thunder (1994), The number of solutions to cubic Thue inequalities, Acta Arith. 66, 237-243.

P. Vojta (1987), Diophantine approximations and value distribution theory, Lecture Notes in Math. 1239. Springer Verlag.