Exponential Diophantine Equations and the Irrationality of Certain Real Numbers

PAUL-GEORG BECKER

Mathematisches Institut der Universität zu Köln,
Weyertal 86-90, D-5000 Köln 41, Germany

Communicated by M. Waldschmidt
Received September 10, 1990; revised October 15, 1990

We apply Schlickewei's recent result on the S-unit equation to show that certain purely exponential diophantine equations have only finitely many solutions. This yields a generalization of irrationality results of Mahler, Bundschuh, Shan, and Wang.

COPYRIGHT © 1991 BY ACADEMIC PRESS, INC.

INTRODUCTION

K. Mahler [4] proved the irrationality of the decimal fraction
\[ 0.1(g)(g^2)\ldots, \]
where \( g \geq 2 \) is a fixed integer and \( (g^n) \) denotes the number \( g^n \) written in decimal form. Later this was generalized by Bundschuh [1], Shan [8], Niederreiter [5], and Shan and Wang [9]. In [9], the most general of these results is established: Let \( g, h \geq 2 \) be fixed integers and let \( (n_k)_{k \in \mathbb{N}} \) be a strictly increasing sequence of nonnegative integers. Then the positive real number (written in base \( h \))
\[ 0.(g^{n_1})_h (g^{n_2})_h (g^{n_3})_h \ldots \]
is irrational if we denote by \( (a)_h \) the number \( a \) written in base \( h \).

From the proof in [1, 9], it could be seen that there is a strong connection between the problem of the irrationality of these numbers and the question of whether certain diophantine equations have only a finite number of solutions. In this paper, we show how the recent result of Schlickewei [7] on the number of solutions of the S-unit equation can be applied to give a further generalization of the theorem of Shan and Wang.

In Part I we study exponential diophantine equations of the type
\[ a_1 u_1^{x_{11}} \ldots u_1^{x_{1l}} + \ldots + a_n u_n^{x_{n1}} \ldots u_n^{x_{nl}} = b, \]
where \( b \) is an algebraic number and \( a_1, \ldots, a_n, u_{11}, \ldots, u_{1l}, \ldots, u_{nl}, \ldots, u_{nl_n} \) are
nonzero algebraic numbers from an algebraic number field $K$. We show that under suitable conditions on the $u_{ij}$, the number of integer solutions $x_{ij}$ of Eq. (1) is less than a bound depending only on $n$, the numbers $u_{ij}$, and the degree of $K$ over $\mathbb{Q}$. This generalizes earlier results of Gel'fond [2, 3], Revuz [6], and Tijdeman and Wang [10].

In Part II we prove the irrationality of numbers $\theta_h(f)$ which have (written in base $h$) the form

$$\theta_h(f) = 0.(f_1)_h (f_2)_h (f_3)_h \cdots,$$

where $f = (f_n)_{n \in \mathbb{N}}$ denotes a sequence generalizing the above-mentioned sequence $(g^n)_{k \in \mathbb{N}}$. This applies, for example, to the number $\theta(f)$, where $f$ is a subsequence of the Fibonacci sequence $1, 1, 2, 3, 5, \ldots$.

These results, which are consequences of Theorem 1 and Theorem 2 of Part I, are given as irrationality measures for the numbers in consideration.

PART I: EXPONENTIAL DIOPHANTINE EQUATIONS

In this section we show that the number of integer solutions of Eq. (1) can be bounded from above if a certain condition on the multiplicative independence of the $u_{ij}$ holds (Theorem 1). This condition can be weakened if we consider exponential diophantine equations of a more special type than Eq. (1) (Theorem 2).

**Theorem 1.** Let $K$ be an algebraic number field, let $n$, $l_1, \ldots, l_n$, be natural numbers, and let $a_1, \ldots, a_n$, $u_{i1}, \ldots, u_{ih}$, $u_{n1}, \ldots, u_{nl_n}$ be nonzero elements from $K$. Let $b \in K$ and suppose that for $i, j \in \{1, \ldots, n\}$ with $i \neq j$ the numbers $u_{i1}, \ldots, u_{ih}$, $u_{j1}, \ldots, u_{jl_j}$ are multiplicatively independent. Then there exists an effectively computable number $C$ depending only on $K$, $n$, and the $u_{ij}$ such that Eq. (1) has at most $C$ solutions in rational integers $x_{i1}, \ldots, x_{ih}$, $x_{n1}, \ldots, x_{nl_n}$.

**Remarks.** (1) From the proof of Theorem 1 we see that the number $C$ does depend only on $d := [K : \mathbb{Q}]$, $n$, and the number $N$ of prime divisors occurring in the prime ideal decompositions of the ideals generated by the numbers $u_{ij}$. It can be shown that $C \leq (4Nd!)^{2[\mathbb{N}]}$. Similar remarks apply to the constants appearing in Theorem 2 and Lemma 2, which are stated below.

(2) Gel'fond studied Eq. (1) in the case $n = 3$ and $b = 0$. In [2], he showed that it has only finitely many integer solutions, if one assumes that $l_1, l_2, l_3 = 1$ and $a_1, a_2, a_3 = \pm 1$. Furthermore [3, Theorem VIII, p. 37], he proved the number of nonnegative integer solutions of (1) to be finite, if the $u_{ij}$ are assumed to be integers in $K$. 
Revuz [6, Theorem II] also treated Eq. (1) only in the case \( n = 3, b = 0, l_1, l_2, l_3 = 1 \) and showed the finiteness of the set of integer solutions. Tijdeman and Wang [10, Theorem VI] proved for arbitrary \( n \) that the number of integer solutions of (1) without vanishing subsums is finite. It should be remarked that the methods used in the above-mentioned papers cannot be applied to give explicit bounds for the number \( C \).

The following theorem, which concerns equations less general than (1), is used in Part II for the treatment of recursive sequences.

**Theorem 2.** Let \( K \) be an algebraic number field, let \( n \geq 2 \) be a natural number, and let \( a_1, ..., a_n, u_1, ..., u_n \) be nonzero elements from \( K \). Suppose that \( u_1, ..., u_n \) and for \( i, j \in \{1, ..., n-1\} \) with \( i \neq j \) the numbers \( u_i u_j^{-1} \) are no roots of unity. Then there exists an effectively computable number \( C \), depending only on \( K, n \), and the \( u_i \), such that the equation

\[
\sum_{i=1}^{n-1} a_i u_i x_1 + a_n u_n x_2 = 1
\]

has at most \( C \) solutions in rational integers \( x_1, x_2 \).

Our proofs of Theorems 1 and 2 make essential use of Schlickewei's result on the \( S \)-unit equation over number fields. To state his result we have to introduce the following definitions. Let \( K \) be an algebraic number field of degree \( d \). Denote by \( M(K) \) the set of places of \( K \) and write \( M_{\infty}(K) \) for the set of archimedian places of \( K \). For \( v \in M(K) \) denote by \( \| \cdot \|_v \) the associated absolute value. Let \( S \) be a finite subset of \( M(K) \) containing \( M_{\infty}(K) \) and having \( s \) elements. We call an element \( y \in K \) an \( S \)-unit, if \( \| y \|_v = 1 \) for \( v \notin S \).

Now we are able to state Schlickewei's result.

**Lemma 1** [7, Theorem 1.1]. Let \( \alpha_1, ..., \alpha_m \) be nonzero elements of \( K \). Then the equation

\[
\alpha_1 y_1 + \cdots + \alpha_m y_m = 1
\]

has not more than

\[
\gamma(m) := (4sd!)^{2(4md)^{s+6}}
\]

solutions in \( S \)-units \( y_1, ..., y_m \) such that no proper subsum \( \alpha_{i_1} y_{i_1} + \cdots + \alpha_{i_k} y_{i_k} \) vanishes.

**Proof of Theorem 1.** We assume that the conditions of Theorem 1 are fulfilled and define \( L := l_1 + \cdots + l_n \) and for \( i = 1, ..., n \), \( u_i := (u_{i1}, ..., u_{id}) \), \( x_i := (x_{i1}, ..., x_{id}) \).
Furthermore, if the $x_{ij}$ are integers we set
\[ u_i^{x_i} := \prod_{j=1}^{l_i} u_{ij}^{x_{ij}}. \]

By $S$ we denote the smallest subset of $M(K)$ containing $M_\infty(K)$ and all the places $v$ from $M(K)$ with $\|u_{ij}\|_v \neq 1$ for at least one pair $(i, j)$ with $1 \leq i \leq n$ and $1 \leq j \leq l_n$.

It is easy to see that we have to consider only the cases $b = 0$ and $b = 1$. We prove the assertion by induction on $n$. The case $n = 1$ follows immediately from the assumption that the numbers $u_{11}, \ldots, u_{1l_1}$ are multiplicatively independent.

Now we suppose that the theorem is true for all positive integers $n'$ less than $n$. We denote by $C(n')$ the upper bound for the number of solutions of (1), which may depend also on $d$ and $s := |S|$. We assume that $n \geq 2$ and denote for $b = 0, 1$ by $\mathcal{L}_b$ the set of all solutions $x = (x_1, \ldots, x_n) \in \mathbb{Z}^L$ of the equation
\[ \sum_{i=1}^{n} a_i u_i^{x_i} = b. \]

We treat the cases $b = 0$ and $b = 1$ simultaneously and define

(a) if $b = 0$,
\[
 m := n - 1, \quad \alpha_i := -a_i a_n^{-1}, \quad \text{and} \quad y_i = y_i(x) := \prod_{j=1}^{l_i} u_j^{-x_{ij}} \quad \text{for} \quad i = 1, \ldots, m;
\]

(b) if $b = 1$
\[
 m := n, \quad \alpha_i := a_i, \quad \text{and} \quad y_i = y_i(x) := u_i^{x_i} \quad \text{for} \quad i = 1, \ldots, m.
\]

By the assumption that for $i \neq j$ the numbers $u_{i1}, \ldots, u_{il_i}, u_{j1}, \ldots, u_{jl_j}$ are multiplicatively independent, it follows that the mapping $y(x) := (y_1(x), \ldots, y_m(x))$ from $\mathbb{Z}^L$ to $K^m$ is injective. Hence we have at least $|\mathcal{L}_b|$ solutions of the $S$-unit equation
\[ \alpha_1 y_1 + \cdots + \alpha_m y_m = 1. \]

By Lemma 1 we know that the number of nondegenerate solutions of (3) (i.e., solutions without vanishing proper subsums) is bounded above by $\gamma(m)$. Therefore we have only to deduce an upper bound for the number of degenerate solutions of (3). Let $x \in \mathcal{L}_b$ be such that $y(x)$ is a degenerate solution of (3). Then there exists a nonempty set $J_{\neq} \{1, \ldots, m\}$ with
\[
 \sum_{j \in J} \alpha_j y_j = 0 \quad \text{and} \quad \sum_{j \notin J} \alpha_j y_j = 1.
\]
This implies that \( x \) is a solution of the following system of exponential diophantine equations:

\[
\sum_{j \in J} a_j u_j^x = 0, \quad \sum_{j \notin J} a_j u_j^x + (1 - b) a_n u_n^x = b.
\]

But we have assumed that Theorem 1 is true for \( n' < n \) and hence the number of such \( x \in \mathbb{Z}^L \) is at most \( C(|J|) \cdot C(n - |J|) \). This gives

\[
|\mathcal{L}_b| \leq \gamma(n) + 2^n \max_{n' = 1, \ldots, n - 1} C(n')^2,
\]

which completes the proof of Theorem 1.

The proof of Theorem 2 is based on the following lemma.

**Lemma 2.** Let \( K \) be an algebraic number field, let \( n \) be a natural number, and let \( a_1, \ldots, a_n, u_1, \ldots, u_n \) be nonzero elements from \( K \). Suppose that for \( i, j \in \{1, \ldots, n\} \) with \( i \neq j \) the numbers \( u_i u_j^{-1} \) are no roots of unity.

Then there exists an effectively computable number \( C \), depending only on \( K, n, \) and the \( u_i \), such that the equation

\[
\sum_{i=1}^{n} a_i u_i^x = 0
\]

has at most \( C \) rational integer solutions \( x \).

**Proof.** We may argue in exactly the same way as in the proof of Theorem 1. For \( i = 1, \ldots, n - 1 \) we define \( \alpha_i := -a_i a_n^{-1} \) and \( y_i := u_i u_n^{-x} \). Hence there is a one-to-one correspondence between the solutions of (4) and a subset of all the solutions of the \( S \)-unit equation

\[
\alpha_1 y_1 + \cdots + \alpha_{n-1} y_{n-1} = 1.
\]

By Lemma 1 the number of solutions of (4) leading to nondegenerate solutions of (5) is at most \( \gamma(n - 1) \). If a solution \( x \) of (4) leads to a degenerate solution of (5), there exists a nonempty set \( J \subseteq \{1, \ldots, n - 1\} \) with

\[
\sum_{j \in J} a_j u_j^x = 0.
\]

Again, an induction argument completes the proof.

**Proof of Theorem 2.** As before we consider the "corresponding" \( S \)-unit equation

\[
a_1 y_1 + \cdots + a_n y_n = 1.
\]
The number of solutions of (2) leading to a nondegenerate solution of (6) is bounded by $\gamma(n)$. If a solution $(x_1, x_2)$ of (2) leads to a degenerate solution of (6), there exists a nonempty set $J \subset \{1, \ldots, n-1\}$ and a $b \in \{0, 1\}$ with

$$\sum_{j \in J} a_j x_j = b. \quad (7)$$

If $b = 0$ it follows from Lemma 2 that Eq. (7) has only a bounded number of solutions $x_1 \in \mathbb{Z}$. If $b = 1$ an induction argument applies to (7), since it is of the same form as Eq. (2). But to each $x_1$ there exists at most one $x_2$ such that $(x_1, x_2)$ solves (2). Hence in both cases the number of solutions $(x_1, x_2)$ is bounded, which proves Theorem 2.

**PART II: IRRATIONALITY RESULTS**

In this section we show how the results of Part I can be applied to prove the irrationality of real numbers which are given by their $h$-adic expansion.

Let $h \geq 2$ be a natural number and $f = (f_k)_{k \in \mathbb{N}}$ be a sequence of natural numbers. For a nonnegative integer $x$ we define $T(x) = T_{h,f}(x)$ to be the total number of digits of

$$(f_1)_h (f_2)_h \cdots (f_x)_h.$$

Now we can state our irrationality result.

**THEOREM 3.** Let $h$ and $f$ be as above and suppose that there exists a natural number $C_0$ with the following property:

For all nonzero rational numbers $q_1, q_2$ the equation $f_k = q_1 h^r + q_2$ has at most $C_0$ solutions $(k, r) \in \mathbb{N} \times \mathbb{Z}$. \( (8) \)

Then there exists a positive real number $C_f$ depending only on $h$ and $f$, such that for all $(p, q) \in \mathbb{Z} \times \mathbb{N}$ the following inequality holds:

$$\left| \theta_h(f) - \frac{p}{q} \right| > h^{-\gamma(C_f w^2)}. \quad (9)$$

**Remark.** It follows from Theorem 3 that $\theta_h(f)$ is irrational.

**COROLLARY.** Let $h \geq 2$ be a natural number, and let $a_1, \ldots, a_n, u_1, \ldots, u_n$ be nonzero algebraic numbers. Suppose that $u_1, \ldots, u_n$ and for $i, j \in \{1, \ldots, n\}$ with $i \neq j$ the numbers $u_i u_j^{-1}$ are no roots of unity. Let $(n_k)_{k \in \mathbb{N}}$ be a strictly
increasing sequence of natural numbers with the property that for \( k = 1, 2, \ldots \) the number

\[ f_k := \sum_{i=1}^{n} a_i u_i^n \]

is a natural number.

Then \( \theta_h(f) \) is irrational.

**Proof.** The Corollary follows directly from Theorem 3, since condition (8) can be checked by applying Theorem 2.

**Remarks.** (1) A result similar to the Corollary can be deduced from the combination of Theorems 1 and 3.

(2) The result of Shan and Wang [9] is a special case of the Corollary. It follows by choosing \( n = 1, a_1 = 1 \) and taking a natural number \( u_1 = g \geq 2 \).

(3) The Corollary also yields the irrationality of \( \theta_h(f) \) for a certain type of recursive sequences \( f_k \). Thus we have, for example, the irrationality of the "Fibonacci decimal" 0.11235813... and similar numbers which are constructed using subsequences of the Fibonacci sequence \( f_k \).

**Proof of Theorem.** We assume that the conditions of Theorem 3 are fulfilled. For a nonnegative integer \( y \) we define \( \hat{T}(y) \) to be the smallest natural number \( k \) with the property that the number \((f_1)_h \cdots (f_k)_h\) has at least \( y \) digits. It is easily checked that \( T(x) \) and \( \hat{T}(y) \) are nondecreasing functions with the property

\[ x \geq \hat{T}(y) \iff T(x) \geq y \quad (x, y \geq 0). \quad (9) \]

Now, we suppose that \( \theta := \theta_h(f) \) satisfies the inequality

\[ \left| \frac{\theta - p}{q} \right| \leq h^{-\tau} \quad (10) \]

for some natural number \( \tau \) and some \((p, q) \in \mathbb{Z} \times \mathbb{N}\).

We show that this is impossible as soon as \( \tau \) is larger than some constant depending on \( q \). It means no restriction to assume that \( 0 < p/q < 1 \) and it is a direct consequence of (10) that the \( h \)-adic expansions of \( \theta \) and \( p/q \) are closely related. We assume that there is a natural number \( \lambda \) with the following properties: (i) the first \( \lambda - 1 \) digits of both expansions are identical, (ii) the digits at position \( \lambda \) are different, and (iii) there is a digit of \( \theta \) at position \( \lambda' > \lambda \) not equal to zero or to \( h - 1 \). This gives us the inequality

\[ |\theta - p/q| \geq h^{-\lambda}, \]

which by (10) implies that there exists a natural number \( \lambda \)
such that the first $\lambda - 1$ digits are identical and the digits of $\theta$ from position $\lambda + 1$ up to position $\tau - 1$ are either all zero or all equal to $h - 1$. We now have to distinguish two cases.

(i) $\hat{T}(\tau) - \hat{T}(\lambda) \geq C_0 + 3$. Hence, there exist at least $C_0 + 1$ numbers $f_k$ with an $h$-adic expansion of the form $(f_k)_h = (dd\ldots d)$, where $d = 0$ or $d = h - 1$. Here $d = 0$ is impossible, since $f_k \in \mathbb{N}$. Therefore we have at least $C_0 + 1$ numbers $k \in \mathbb{N}$ with $f_k = h^r - 1$ with some $r_k \in \mathbb{N}$. But this contradicts condition (8) and we only have to study the remaining case.

(ii) $\hat{T}(\tau) - C_0 - 3 < \hat{T}(\lambda)$. Let us denote the $h$-adic expansion of the rational number $p/q$ by $0.t_1t_2\ldots t_{l-1}d_1d_2\ldots d_l$, where $l$ is the minimal period length. Since the first $\lambda - 1$ digits of $p/q$ and $\theta$ are identical, we know that there are at least $\hat{T}(\lambda) - \tau - 2$ numbers $f_k$ of the form

$$
(f_k)_h = d_s d_{s+1} d_1 d_i d_1 d_i d_1 d_i d_1 d_i d_i \ldots d_i (11)
$$

with $s, t \in \{1, \ldots, l\}$. We now assume

$$
\hat{T}(\tau) \geq C_0(q - 1)^2 + \nu + C_0 + 5, \tag{12}
$$

which yields $\hat{T}(\lambda) > C_0(q - 1)^2 + \nu + 2$. Since $l \leq q - 1$, we can find $s, t \in \{1, \ldots, l\}$ such that there exist more than $C_0$ numbers $f_k$ having an $h$-adic expansion of the form in (11) with fixed $s$ and $t$. Without loss of generality, we can assume $s = 1$. Then we get from Eq. (11)

$$
f_k = \sum_{i=1}^{l} d_i h^{i-1} + \sum_{i=1}^{l} d_i h^{i+l-1} \frac{h^{\omega_k l} - 1}{h^l - 1},
$$

where $\omega_k \in \mathbb{N}$ denotes the number of occurrences of the complete period $d_1 \ldots d_l$ in expansion (11).

We set

$$
q_1 := \frac{h^l - 1}{h^l - 1} \sum_{i=1}^{l} d_i h^{i-1},
$$

$$
q_2 := -q_1 + \sum_{i=1}^{l} d_i h^{i-1},
$$

and $r_k := \omega_k l$. Thus we have

$$
f_k = q_1 h^{r_k} + q_2. \tag{13}
$$

But $q_1$ is trivially nonzero and $q_2$ is nonzero, since $h^l(h^l-1)$ $(d_1 h^{l-1} + \ldots + d_l)$. Thus we have found more than $C_0$ solutions $(k, r_k)$ of
Eq. (13), which contradicts property (8). Hence our assumption (10) is false as soon as \( \tau \) fulfills (12), which by (9) is equivalent to

\[
\tau \geq T(C_0(q - 1)^2 + v + C_0 + 5).
\]

But this is a consequence of \( \tau \geq T(2C_0q^2) \). Hence Theorem 3 is correct if we choose \( C_1 = 2C_0 \).

**REFERENCES**

2. A. O. Gel'fond, Sur la divisibilité de la différence des puissances de deux nombres entiers par un puissance d’un idéal premier, *Mat. Sb.* 7 (1940), 7–25.