

REDUCTION OF UNKNOWNNS IN DIOPHANTINE REPRESENTATIONS*

SUN ZHI-WEI (孙智伟)

(Department of Mathematics, Nanjing University, Nanjing 210008, PRC)

Received December 10, 1990.

ABSTRACT

The hardest step to solve Hilbert's tenth problem is to prove that the exponential relation is Diophantine. In the study of decision problems concerning the solvability of Diophantine equations with few unknowns, reducing unknowns in Diophantine representations plays an important role. In this paper, we give Diophantine representations of $C = \psi_B(A, 1)$ (where $\psi_0(A, 1) = 0$, $\psi_1(A, 1) = 1$, $\psi_{m+1}(A, 1) = A\psi_m(A, 1) - \psi_{m-1}(A, 1)$) and $W = V^B \wedge A_1, \dots, A_k \in \square \wedge S|T \wedge R > 0$ with only 3 and 5 natural number unknowns respectively, $C = \psi_B(A, 1)$ (on the condition $1 < |B| < \frac{|A|}{2} - 1$) and $W = V^B \wedge A_1, \dots, A_k \in \square \wedge S|T$ with 4 and 6 integer unknowns respectively.

Keywords: Hilbert's tenth problem, Diophantine representation, Lucas sequence, exponential relation, combination of relations.

I. INTRODUCTION

Hilbert's tenth problem asks an algorithm to test polynomial Diophantine equations (with integer coefficients) for solvability in integers. By Lagrange's theorem, this is equivalent to the question whether there is an algorithm to test polynomial Diophantine equations for solvability in natural numbers. In 1961, M. Davis, H. Putnam and J. Robinson^[1] proved that any r.e. (recursively enumerable) set W is exponential Diophantine, i.e. W can be represented in the form

$$x \in W \iff \exists x_1, \dots, x_n \in \mathbb{N} (P(x, x_1, \dots, x_n, 2^{x_1}, \dots, 2^{x_n}) = 0),$$

where P is a polynomial (with integer coefficients) and \mathbb{N} denotes the set of natural numbers (nonnegative integers). For this reason, to find a Diophantine function with exponential growth becomes the key to solving Hilbert's tenth problem. In 1970, Ju. V. Matijasevič^[2] successfully showed that $y = F_{2x}$ is Diophantine where $\{F_n\}$ is the well-known Fibonacci sequence ($F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$). Since then, instead of F_{2n} , $\phi_A(n)$ has been widely used. Here $\phi_A(n)$ denotes the n th y -solution (in order of the size of $y \geq 0$) of the Pell equation

$$X^2 - (A^2 - 1)Y^2 = 1 \quad (A > 0).$$

* Project supported by the National Natural Science Foundation of China.

As a matter of fact, both $\{F_{2n}\}_{n \in \mathbb{N}}$ and $\{\phi_A(n)\}_{n \in \mathbb{N}}$ are Lucas sequences of a special kind.

Definition. Let A and B be integers. $\{\phi_n\}(\{\phi_n(A, B)\})$ and $\{\chi_n\}(\{\chi_n(A, B)\})$ given by

$$\phi_0 = 0, \phi_1 = 1, \phi_{n+1} = A\phi_n - B\phi_{n-1} \quad (n = 1, 2, \dots)$$

and

$$\chi_0 = 2, \chi_1 = A, \chi_{n+1} = A\chi_n - B\chi_{n-1} \quad (n = 1, 2, \dots)$$

are called the Lucas sequences.

By induction on n , one can easily prove $\chi_n(A, B) = 2\phi_{n+1}(A, B) - A\phi_n(A, B)$, $F_{2n} = \phi_n(3, 1)$ and $\phi_A(n) = \phi_n(2A, 1)$.

If we take into account the number of unknowns, then it is natural to ask that for what n there does not exist an algorithm to test (polynomial) Diophantine equations with n unknowns for solvability in integers (resp. natural numbers). After more than ten years' hard work, it is shown that we can take $n=27$ (resp. $n=9$). (cf. [3] and [4]). These are the best results at present. Here we claim that we can take $n=11$ in the case of integer unknowns. The purpose of this paper is to provide a basis for the claim. In fact from [3] and this paper, we already see that n can be taken less than 27.

In the process of reducing unknowns, the key point is to reduce unknowns in Diophantine representations of functions with exponential growth, and to give a Diophantine representation of the conjunction of some relations with unknowns as few as possible. In this paper, we obtain the results mentioned in the abstract, and discuss the upper and lower bounds of solutions. In the case of natural number unknowns, our results are stronger than the known ones; in the case of integer unknowns, our results are much better than those obtained by the usual method (using $n \geq 0 \iff \exists u \exists v \exists w (4n + 1 = u^2 + v^2 + w^2)$ (cf. [4] and [5])).

Throughout this paper, polynomial refers to polynomial with integer coefficients, \mathbb{Z} (resp. \mathbb{N}) denotes the set of integers (resp. natural numbers), Latin letters represent integers, bounded variables are written in lower case, \square stands for the set of squares, and (A, B) denotes the greatest common divisor of A and B .

II. SOME LEMMAS ON LUCAS SEQUENCES

The general form of second-order (linear) recurrences is

$$\tau_0 = C_0, \tau_1 = C_1, \tau_{n+1} = A\tau_n - B\tau_{n-1} \quad (n = 1, 2, \dots).$$

One can easily prove $\tau_n = C_0\phi_{n+1}(A, B) + (C_1 - AC_0)\phi_n(A, B)$, and this shows that the Lucas sequence $\{\phi_n\}$ is fundamental. Here are some examples of Lucas sequences:

$$\phi_n(0, 1) = \begin{cases} 0 & \text{if } 2|n, \\ \left(\frac{-1}{2}\right)^{\frac{n-1}{2}} & \text{if } 2 \nmid n. \end{cases} \quad \chi_n(0, 1) = \begin{cases} 0 & \text{if } 2 \nmid n, \\ 2(-1)^{\frac{n}{2}} & \text{if } 2|n. \end{cases}$$

$$\phi_n(1, 1) = \begin{cases} 1 & \text{if } n \equiv 1, 2 \pmod{6}, \\ 0 & \text{if } 3|n, \\ -1 & \text{if } n \equiv 4, 5 \pmod{6}. \end{cases} \quad \chi_n(1, 1) = \begin{cases} 2 & \text{if } n \equiv 0 \pmod{6}, \\ 1 & \text{if } n \equiv 1, 5 \pmod{6}, \\ -1 & \text{if } n \equiv 2, 4 \pmod{6}, \\ -2 & \text{if } n \equiv 3 \pmod{6}. \end{cases}$$

$$\phi_n(2, 1) = n, \quad \chi_n(2, 1) = 2.$$

In the following lemmas, ϕ_n and χ_n are short for $\phi_n(A, B)$ and $\chi_n(A, B)$ respectively.

Lemma 1. (i) $(\alpha - \beta)\phi_n = \alpha^n - \beta^n$, $\chi_n = \alpha^n + \beta^n$ ($n \geq 0$), where

$$\alpha = \frac{A + \sqrt{A^2 - 4B}}{2} \quad \text{and} \quad \beta = \frac{A - \sqrt{A^2 - 4B}}{2}$$

are the two roots of the equation $\theta^2 - A\theta + B = 0$.

(ii) $\chi_n^2 - (A^2 - 4B)\phi_n^2 = 4B^n$, $\phi_{n+1}^2 - A\phi_{n+1}\phi_n + B\phi_n^2 = B^n$ ($n \geq 0$).

The proof is simple. (Note that $\chi_n = 2\phi_{n+1} - A\phi_n$.)

Lemma 2. $\phi_{k+n+r} = \sum_{i=0}^n \binom{n}{i} (\phi_{k+1} - A\phi_k)^{n-i} \phi_k^i \phi_{r+i}$ ($k, n, r \in \mathbb{N}$).

Proof. First we show it in the case $n = 1$ (by induction on k), then we proceed by induction on n using $k(n+1) + r = kn + (k+r)$, $(k+r) + i = k + (r+i)$ and $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$, ($i \geq 1$).

Lemma 3. Let $(A, B) = 1$. Then $(\phi_m, \phi_n) = |\phi_{(m,n)}|$ ($m, n \in \mathbb{Z}^+$).

Proof. By part (ii) of Lemma 1, $(\phi_{n+1}, \phi_n) | B^n$. Since $\phi_{n+1} \equiv A^n \pmod{B}$, we have $(\phi_{n+1}, \phi_n) = 1$ and hence $(\phi_{k+n+r}, \phi_n) = ((\phi_{n+1} - A\phi_n)^k \phi_r, \phi_n) = (\phi_r, \phi_n)$. From this, we can easily prove $(\phi_m, \phi_n) = |\phi_{(m,n)}|$ by Euclid's algorithm.

Lemma 4. Suppose $\Delta = A^2 - 4B \geq 0$. For $\{\phi_n\}_{n \in \mathbb{N}}$ to be nondecreasing, it is necessary and sufficient that A is not less than 1. If $A \geq 1$ then $\phi_{n+1} = \phi_n \iff A = 1 \wedge n > 0 \wedge (n-1)B = 0$. Hence $\{\phi_n\}_{n \in \mathbb{N}}$ is strictly increasing if and only if $A \geq 2$.

Proof. Use $\phi_{n+1} - \alpha\phi_n = \beta^n$ if $B > 0$.

Lemma 5. Suppose $\Delta = A^2 - 4B \geq 0$. For $\{\chi_n\}_{n \in \mathbb{N}}$ to be nondecreasing, it is necessary and sufficient that A is not less than 2. If $A \geq 2$, then $\chi_{n+1} = \chi_n \iff A = 2 \wedge n(B-1) = 0$. Thus $\{\chi_n\}_{n \in \mathbb{N}}$ is strictly increasing if and only if $A \geq 3$.

Proof. By Lemma 1 (ii) and Lemma 4.

Lemma 6. Let $M \neq 0$. Then $(B, M) = 1$ if and only if for some positive integer λ , $\phi_\lambda \equiv 0 \pmod{M}$ and $\phi_{\lambda+1} \equiv 1 \pmod{M}$.

Proof. For the "if" part, observe that

$$\phi_{\lambda+1}^2 - A\phi_{\lambda+1}\phi_\lambda + B\phi_\lambda^2 \equiv B^\lambda \pmod{M}.$$

As to the "only if" part, we suppose $(B, M) = 1$. For $\zeta \in \mathbb{Z}$, we use $\bar{\zeta}$ to denote the

residue of ζ modulo $|M|$. Since

$$\{\langle \bar{\phi}_i, \bar{\phi}_{i+1} \rangle : i = 0, 1, \dots, M^2\} \subseteq \{\langle s, t \rangle : s, t = 0, 1, \dots, |M| - 1\},$$

there exist i, j with $0 \leq i < j \leq M^2$ such that $\langle \bar{\phi}_i, \bar{\phi}_{i+1} \rangle = \langle \bar{\phi}_j, \bar{\phi}_{j+1} \rangle$. Let λ be the smallest positive integer j such that $\langle \bar{\phi}_i, \bar{\phi}_{i+1} \rangle = \langle \bar{\phi}_j, \bar{\phi}_{j+1} \rangle$ for some $i < j$ ($i \geq 0$). Then λ is not more than M^2 and the corresponding i equals 0. (If $i > 0$, then

$$\langle \overline{B\phi_{i-1}}, \overline{B\phi_i} \rangle = \langle \overline{A\phi_i - \phi_{i+1}}, \overline{B\phi_i} \rangle = \langle \overline{A\phi_\lambda - \phi_{\lambda+1}}, \overline{B\phi_\lambda} \rangle = \langle \overline{B\phi_{\lambda-1}}, \overline{B\phi_\lambda} \rangle$$

and hence $\langle \bar{\phi}_{i-1}, \bar{\phi}_i \rangle = \langle \bar{\phi}_{\lambda-1}, \bar{\phi}_\lambda \rangle$ (since $(B, M) = 1$), which contradicts the minimality of λ .)

Lemma 7. Suppose $A \neq 0, (A, B) = 1$ and $\Delta = A^2 - 4B \geq 0$. Then $\phi_k^2 | \phi_m$ if and only if $k\phi_k | m$ ($k, m \in \mathbb{N}$) unless $|A| = 1, (k-2)B = 0$ and $k \nmid m$.

Proof. We have $\phi_{kn} \equiv n\phi_{k+1}^{-1}\phi_k \pmod{\phi_k^2}$ and $|\phi_n| = |\phi_n(|A|, B)| = \phi_n(|A|, B)$. If $|A| = 1 \wedge (k-2)B = 0 \wedge k \nmid m$ does not hold, then $\phi_k | \phi_m$ implies $k | m$.

Lemma 8. Let $A > B \geq 0$. Then $(A-B)^n \leq \phi_{n+1} \leq A^n$ ($n \in \mathbb{N}$).

Proof. Since $A \geq B + 1 \geq 2\sqrt{B}$, by Lemma 4 we have

$$(A-B)\phi_{n+1} \leq \phi_{n+2} = A\phi_{n+1} - B\phi_n \leq A\phi_{n+1}.$$

Lemma 9. Suppose $A \geq 2$. Then

$$Y^2 = (A^2 - 4)X^2 + 4 \wedge X \geq 0 \wedge Y \geq 0 \iff \exists n \in \mathbb{N} (X = \phi_n(A, 1) \wedge Y = \chi_n(A, 1)),$$

$$X^2 - AXY + Y^2 = 1 \wedge Y \geq X \geq 0 \iff \exists n \in \mathbb{N} (X = \phi_n(A, 1) \wedge Y = \phi_{n+1}(A, 1)).$$

Proof. “ \Leftarrow ”: By Lemmas 1, 4, 5.

“ \Rightarrow ”: First we prove the following for $X \geq 0$ (by induction):

$$Y^2 = (A^2 - 4)X^2 + 4 \wedge Y \geq 0 \Rightarrow \exists n \in \mathbb{N} (X = \phi_n(A, 1) \wedge Y = \chi_n(A, 1)). \quad (*)$$

It is obvious if $X = 0$ (since $0 = \phi_0(A, 1), 2 = \chi_0(A, 1)$).

Let $X > 0$ and assume that $(*)$ holds for smaller X . Suppose $Y \geq 0$ satisfies $Y^2 = (A^2 - 4)X^2 + 4$. Obviously $Y \equiv AX \pmod{2}$, $A^2X^2 \geq Y^2$, $A^2Y^2 \geq (A^2 - 4)^2X^2$, hence both $X' = \frac{AX - Y}{2}$ and $Y' = \frac{AY - (A^2 - 4)X}{2} = 2X - AX'$ are natural numbers. Clearly $X' < X$ (since $Y^2 > (A - 2)^2X^2$), $(A^2 - 4)X'^2 + 4 - Y'^2 = (A^2 - 4)X^2 + 4 - Y^2 = 0$. By the inductive hypothesis, for some $n \in \mathbb{N}$ we have $X' = \phi_n(A, 1)$ and $Y' = \chi_n(A, 1)$, therefore

$$X = \frac{1}{2}(AX' + Y') = \frac{1}{2}(A\phi_n(A, 1) + \chi_n(A, 1)) = \phi_{n+1}(A, 1),$$

$$\begin{aligned} Y &= AX - 2X' = A\phi_{n+1}(A, 1) - 2\phi_n(A, 1) = 2\phi_{n+2}(A, 1) - A\phi_{n+1}(A, 1) \\ &= \chi_{n+1}(A, 1). \end{aligned}$$

By the above, $(*)$ holds for all $X \geq 0$. This proves the first “ \Rightarrow ” part.

Now suppose $X^2 - AXY + Y^2 = 1$ and $Y \geq X \geq 0$. Clearly $AY \geq AX \geq 2X$,

$(AY - 2X)^2 = (A^2 - 4)Y^2 + 4$, thus there exists a $k \in \mathbb{N}$ such that

$$\begin{cases} AY - 2X = \chi_k(A, 1) = 2\phi_{k+1}(A, 1) - A\phi_k(A, 1), \\ Y = \phi_k(A, 1), \end{cases}$$

i.e.

$$\begin{cases} X = A\phi_k(A, 1) - \phi_{k+1}(A, 1), \\ Y = \phi_k(A, 1). \end{cases}$$

Since $X \geq 0$, we have $k > 0$. Let $n = k - 1$, then $X = \phi_n(A, 1)$ and $Y = \phi_{n+1}(A, 1)$. This concludes the proof.

Remark 1. Let $B \neq 0, 1$ then B^n varies with n . For a fixed $n \in \mathbb{N}$, provided that $A^2 - 4B \in \mathbb{N} \setminus \square$, the equation $y^2 - (A^2 - 4B)x^2 = 4B^n$ has infinitely many solutions (including $x = \phi_n(A, B)$, $y = \chi_n(A, B)$), however, it is very difficult for us to give the general solution explicitly.

We point out that, in some special cases (e.g. the case $2|A \wedge A > 0 \wedge B = 1$), Lemmas 1—9 have been investigated more or less (see [6] and [7]).

III. MAIN RESULTS

By Lemma 9 and Remark 1, the Lucas sequences $\{\phi_n(A, 1)\}_{n \geq 0}$ are of great importance in Diophantine representations. In such case $B = 1$, we can extend $\{\phi_n\}_{n \in \mathbb{N}}$ (resp. $\{\chi_n\}_{n \in \mathbb{N}}$) to $\{\phi_n\}_{n \in \mathbb{Z}}$ (resp. $\{\chi_n\}_{n \in \mathbb{Z}}$) by the same recursion formula. If $A \neq 0$, $\phi_k = \phi_k(A, 1)$ and $\chi_k = \chi_k(A, 1)$ ($k \in \mathbb{Z}$) can also be determined as follows:

$$\phi_{-1} = 1, \phi_1 = 1, \phi_{m-1} + \phi_{m+1} = A\phi_m \quad (m = 0, \pm 1, \pm 2, \dots);$$

$$\chi_{-1} = \chi_1 = A, \chi_{m-1} + \chi_{m+1} = A\chi_m \quad (m = 0, \pm 1, \pm 2, \dots).$$

By induction, for $n \in \mathbb{N}$ one has $\phi_{-n}(A, 1) = -\phi_n(A, 1) = (-1)^n \phi_n(-A, 1)$ and $\chi_{-n}(A, 1) = \chi_n(A, 1) = (-1)^n \chi_n(-A, 1)$, so $\phi_m(|A|, 1) = \phi_m(A, 1)$ or $\phi_{-m}(A, 1)$ ¹⁾. From this and Lemma 9, we obtain $(A^2 - 4)X^2 + 4 \in \square \iff \exists m(X = \phi_m(A, 1))$.

In the special case $B = 1$, we also have

Lemma 10. Suppose $|A| > 2$, $n > 3$ and $2|\chi_n(A, 1)$. Then

$$\phi_s(A, 1) \equiv \phi_t(A, 1) \left(\text{mod } \frac{\chi_n(A, 1)}{2} \right) \iff s \equiv t \pmod{4n} \vee s + t \equiv 2n \pmod{4n}.$$

Proof. By induction on k , we can easily prove $\phi_{k+r}(A, 1) = \phi_r(A, 1)\chi_k(A, 1) + \phi_{k-r}(A, 1)$ ($k \in \mathbb{N}$). Hence for any r we have

$$\begin{aligned} \phi_{n+r}(A, 1) &\equiv \phi_{n-r}(A, 1), \quad \phi_{2n+r}(A, 1) \equiv \phi_{-r}(A, 1) \equiv -\phi_r(A, 1), \\ \phi_{4n+r}(A, 1) &\equiv -\phi_{2n+r}(A, 1) \equiv \phi_r(A, 1) \pmod{\chi_n(A, 1)}. \end{aligned}$$

Therefore $\phi_{4nq+r}(A, 1) \equiv \phi_r(A, 1) \left(\text{mod } \frac{\chi_n(A, 1)}{2} \right)$, and the integers $\phi_0(A, 1)$,

1) $\phi_m(-A, 1) = (-1)^m \phi_{-m}(A, 1) = (-1)^{m-1} \phi_m(A, 1)$.

$\phi_1(A, 1), \dots, \phi_{n-1}(A, 1)$ are congruent to the following numbers (modulo $\frac{\chi_n(A, 1)}{2}$) respectively:

$$0, \phi_{-1}(A, 1), \dots, \phi_{n-1}(A, 1), \phi_n(A, 1), \phi_{n-1}(A, 1), \dots, \phi_1(A, 1),$$

$$0, -\phi_1(A, 1), \dots, -\phi_{n-1}(A, 1), -\phi_n(A, 1), -\phi_{n-1}(A, 1), \dots, -\phi_1(A, 1).$$

Since $|\chi_n(A, 1)| = |\chi_n(|A|, 1)|$, $\{\phi_i(A, 1), -\phi_i(A, 1)\} = \{\phi_i(|A|, 1), -\phi_i(|A|, 1)\}$, it suffices to prove, in the case $A = |A| > 2$, that the numbers $0, \phi_1, -\phi_1, \phi_2, -\phi_2, \dots, \phi_n, -\phi_n$ have distinct residues modulo $\frac{\chi_n}{2}$, where $\phi_i = \phi_i(A, 1)$ and $\chi_i = \chi_i(A, 1)$.

The residues of $0, \phi_1, \phi_2, \dots, \phi_n \pmod{\frac{\chi_n}{2}}$ are distinct because

$$0 < \phi_1 < \phi_2 < \dots < \phi_n$$

and

$$\chi_n > \left(\frac{A + \sqrt{A^2 - 4}}{2}\right)^n - \left(\frac{A - \sqrt{A^2 - 4}}{2}\right)^n = \sqrt{A^2 - 4} \phi_n \geq \sqrt{5} \phi_n > 2\phi_n.$$

If $1 \leq s, t < n$, then $\phi_s + \phi_t \not\equiv 0 \pmod{\frac{\chi_n}{2}}$ for

$$\begin{aligned} \phi_n &= \frac{A + \sqrt{A^2 - 4}}{2} \phi_{n-1} + \left(\frac{A - \sqrt{A^2 - 4}}{2}\right)^{n-1} > \frac{A + \sqrt{A^2 - 4}}{2} \phi_{n-1} \\ &\geq \frac{3 + \sqrt{5}}{2} \phi_{n-1}, \end{aligned}$$

$$0 < \phi_s + \phi_t \leq 2\phi_{n-1} \leq \frac{4}{3 + \sqrt{5}} \phi_n < \frac{4}{3 + \sqrt{5}} \cdot \frac{\chi_n}{\sqrt{5}} \leq \frac{\chi_n}{2}.$$

Let $1 \leq r \leq n$. Since $0 < \phi_n + \phi_r \leq 2\phi_n < \chi_n$, we have

$$\phi_n + \phi_r \equiv 0 \pmod{\frac{\chi_n}{2}} \Rightarrow \phi_n + \phi_r = \frac{\chi_n}{2}.$$

If $1 \leq r < n - 2$, then $\phi_n + \phi_r \not\equiv 0 \pmod{\frac{\chi_n}{2}}$ because

$$\phi_n > \frac{3 + \sqrt{5}}{2} \phi_{n-1} > \left(\frac{3 + \sqrt{5}}{2}\right)^2 \phi_{n-2} > \left(\frac{3 + \sqrt{5}}{2}\right)^3 \phi_{n-3},$$

$$\phi_n + \phi_r \leq \phi_n + \phi_{n-3} < \left(1 + \left(\frac{3 + \sqrt{5}}{2}\right)^{-3}\right) \phi_n \leq \frac{\sqrt{5}}{2} \phi_n < \frac{\chi_n}{2}.$$

By the above, we need only to prove (a) $\phi_n + \phi_n \neq \frac{\chi_n}{2}$, (b) $\phi_n + \phi_{n-1} \neq \frac{\chi_n}{2}$ and

(c) $\phi_n + \phi_{n-2} \neq \frac{\chi_n}{2}$.

Since $|(20 - A^2)\phi_n^2| \geq \phi_n^2 \geq \phi_2^2 = A^2 > 4$, (a) holds, for we have $4 \neq (20 -$

$A^2)\phi_n^2 = (4\phi_n)^2 - (A^2 - 4)\phi_n^2$ and thus $\chi_n \neq 4\phi_n$. If (b) fails, then $\chi_n = 2\phi_n + (A\phi_n - \chi_n)$, $(A + 2)^2\phi_n^2 = 4(A^2 - 4)\phi_n^2 + 16$ and hence $(3A - 10)(A + 2)\phi_n^2 + 16 = 0$ which is impossible. Suppose (c) does not hold, then $(A^2\phi_n)^2 = (A + 1)^2 \cdot ((A^2 - 4)\phi_n^2 + 4)$ (because $\chi_n = 2A\phi_{n-1} = A(A\phi_n - \chi_n)$), and so

$$((2A + 1)(A + 1)(A - 3) - 1)\phi_n^2 + 4(A + 1)^2 = 0,$$

which is not true since $\phi_n > \phi_3 = A^2 - 1 \geq 8$ (no matter whether $A=3$ or $A > 3$).

The proof of Lemma 10 is now finished.

Lemma 11. $K > 0 \wedge M \in \square \setminus \{0\} \iff \exists z > 0((z - KM)^2 = K^2M)$. Furthermore z can be required to satisfy $KM \leq z \leq 2KM$.

Proof. Suppose $z > 0$ satisfies $(z - KM)^2 = K^2M$. Clearly $K \neq 0, M \neq 0, K|z$ and $M = \left(\frac{z}{K} - M\right)^2 \in \square$. If $K < 0$, then $M \geq (-1 - M)^2 > M^2 \geq M$.

Take $z = K(m^2 + m)$ if $K > 0$ and $M = m^2$ ($m > 0$).

Now we are ready to present

Theorem 1. Let $A \geq 2$ and $B \geq 0$. Then

$$\begin{aligned} C = \phi_B(A, 1) &\iff C \geq B \wedge \exists x > 0 \exists y > 0 (DFI \in \square) \\ &\iff \exists x, y, z > 0((x - DFI(C - B + 1))^2 \\ &= DFI(C - B + 1)^2), \end{aligned}$$

where $D = (A^2 - 4)C^2 + 4, E = C^2Dx, F = 4(A^2 - 4)E^2 + 1, G = 1 + CDF - 2(A + 2)(A - 2)^2E^2, H = C + BF + (2y - 1)CF$ and $I = (G^2 - 1)H^2 + 1$. When $B \neq 0$, for any $N > 0$ we may require x, y, z to satisfy

$$N \leq x \leq A^{16N^2C^4D^2-1}, N \leq y \leq (2CDF)^{B+2GNF^2-1}, N \leq z \leq 2CDFI \text{ and } N^2 \leq DFI.$$

*Proof.*¹⁾ a) Suppose $x \neq 0$ and y satisfy $DFI \in \square$. Since $|A| > 2$, we have $D \geq 4 > 0, F > 0, G \neq 0$ (since $G \equiv 1 \pmod{D}$), $I > 0; F \equiv G \equiv I \equiv 1 \pmod{D}$, $(D, F) = (D, I) = 1; H \equiv C, 2G \equiv A, 4I = ((2G)^2 - 4)H^2 + 4 \equiv (A^2 - 4)C^2 + 4 = D \pmod{F}$, $(4I, F) = (D, F) = 1$. Thus D, F, I are pairwise relatively prime, and hence $D, F, I \in \square$ follow from $DFI \in \square$.

Since $(A^2 - 4)C^2 + 4, (A^2 - 4)(4E)^2 + 4, ((2G)^2 - 4)H^2 + 4 \in \square$, there are integers m, s, t satisfying $C = \phi_s(A, 1), 4E = \phi_m(A, 1)$ and $H = \phi_t(2G, 1)$.

Assume $C \neq 0$. Let $n = |m|$ then $n > 3$, for

$$\begin{aligned} |4E| = 4C^2D|x| &\geq D \geq A^2 - 4 + 4 > A^2 - 1 = |\phi_3(A, 1)| \\ &> |\phi_2(A, 1)| > |\phi_1(A, 1)| > 0. \end{aligned}$$

Clearly $4F = (A^2 - 4)\phi_m^2(A, 1) + 4 = (A^2 - 4)\phi_n^2(A, 1) + 4 = \chi_n^2(A, 1)$, so $2|\chi_n(A, 1)$. By $2G \equiv A, H \equiv C \pmod{F}$ and Lemma 10, we have

$$\phi_s(A, 1) \equiv \phi_t(2G, 1) \equiv \phi_t(A, 1) \pmod{\frac{\chi_n(A, 1)}{2}}, s \equiv t \text{ or } -t \pmod{2n}.$$

1) To prove Theorem 2 similarly and conveniently, we proceed first on looser conditions (e.g. $|A| > 2$).

Since $C^2|E$, $\phi_{|s|}^2(A,1)|\phi_n(A,1)$. Applying Lemma 7, we get $\phi_s(A,1)|n$ and hence $s \equiv t$ or $-t \pmod{2\phi_s(A,1)}$. Because $F \equiv 1$, $2G \equiv 2$, $H \equiv B \pmod{2C}$, we have

$$B \equiv \phi_t(2G,1) \equiv \phi_t(2,1) = t \equiv s \text{ or } -s \pmod{2\phi_s(A,1)}.$$

If $|B| \leq |C|$, then $|s| = |B|$, for

$$|s| \neq |B| \Rightarrow 0 < |B \pm s| \leq |B| + |s| < 2|\phi_s(A,1)|.$$

By the above, if $C \geq B$ (≥ 0) and $DFI \in \square$ for some $x, y > 0$, then $C = \phi_B(A,1)$. (When $C=0$, $C=B=0 = \phi_B(A,1)$; when $C \neq 0$, $C > 0$ and $0 < s \neq -B$. (Note that $A > 2$, $B \geq 0$.)

b) Suppose $C = \phi_B(A,1) \neq 0$. Since $|A| > 2$, $D > 0$. Let $N > 0$, by Lemma 6 there is an n for which $0 < n \leq (4NC^2D)^2$ and $\phi_n(A,1) \equiv \phi_0(A,1) = 0 \pmod{4NC^2D}$. Take $x = \frac{\phi_n(A,1)}{4C^2D}$, then $N|x$ and $x \neq 0$ (since $|\phi_n(A,1)| = \phi_n(|A|$,

$1) \geq n > 0$). Let

$$E = C^2Dx = \frac{\phi_n(A,1)}{4}, \quad F = 4(A^2 - 4)E^2 + 1 = \frac{\chi_n^2(A,1)}{4}$$

and

$$G = 1 + CDF - 2(A+2)(A-2)^2E^2.$$

By Lemma 6, there exists a positive integer $\lambda \leq F^2$ such that $\phi_\lambda(A,1) \equiv 0$, $\phi_{\lambda+1}(A,1) \equiv 1 \pmod{F}$, thus for any i, j , we have

$$i \equiv j \pmod{\lambda} \Rightarrow \phi_i(A,1) \equiv \phi_j(A,1) \pmod{F}.$$

Put $\bar{\lambda} = \lambda N$ if $\lambda > F$ or $\bar{\lambda} = \lambda NF$ if $\lambda \leq F$. Let $j = B + 2\bar{\lambda}C$ and $H = \phi_j(2G,1)$. Since $2G \equiv A \pmod{F}$, $G \equiv 1 \pmod{C}$ and $F \equiv 1 \pmod{2C}$, we have

$$H \equiv \phi_j(A,1) \equiv \phi_B(A,1) = C \equiv C + (B-C)F \pmod{F},$$

$$H \equiv \phi_j(2,1) = j \equiv B \equiv C + (B-C)F \pmod{2C},$$

$$2CF | H - (C + (B-C)F).$$

Take $y = \frac{H - C - (B-C)F}{2CF}$, then $H = C + BF + (2y-1)CF$. Let $I = (G^2 - 1)H^2 + 1$, we then have

$$D = (A^2 - 4)\phi_B^2(A,1) + 4 = \chi_B^2(A,1), \quad F = \left(\frac{\chi_n(A,1)}{2}\right)^2,$$

$$I = \frac{1}{4} \left(((2G)^2 - 4)\phi_j^2(2G,1) + 4 \right) = \left(\frac{\chi_j(2G,1)}{2}\right)^2,$$

and therefore $DFI \in \square$.

Since $A > 2$ and $B \geq 0$, $C = \phi_B(A,1) \geq B$. If $B = 0$, let $x = y = N$ then $DFI = 4 \times 1 \times 1 = 2^2$. Now assume $B \neq 0$, clearly $C \geq B > 0$. Choose x and y as the above, then $DFI \in \square$. Obviously

$$0 < N \leq x \leq \phi_n(A,1) \leq A^{n-1} \leq A^{16N^2C^4D^2-1}.$$

Clearly $E \neq 0$, $F > 1$, $1 \leq G \leq CDF$, $1 < \lambda \leq F^2$, $NF < \bar{\lambda} \leq NF^2$, $H \geq j \geq B +$

$2(NF + 1)C, y \leq \frac{H + CF}{2CF} < H + 1$, so we have

$$0 < N \leq y \leq H = \phi_j(2G, 1) \leq (2G)^{j-1} \leq (2CDF)^{B+2CNF^2-1}.$$

Since $A > 2, 2G \geq 2, B > 0$ and $j \geq 0$, we also have

$$\begin{aligned} \chi_B(A, 1) \cdot \frac{\chi_n(A, 1)}{2} \cdot \frac{\chi_j(2G, 1)}{2} &\geq \chi_0(A, 1) \cdot \frac{\chi_n(A, 1)}{2} \cdot \frac{\chi_0(2G, 1)}{2} = \chi_n(A, 1) \\ &> \left(\frac{A + \sqrt{A^2 + 4}}{2}\right)^n - \left(\frac{A - \sqrt{A^2 - 4}}{2}\right)^n = \sqrt{A^2 - 4} \phi_n(A, 1) \\ &\geq \phi_n(A, 1) \geq x \geq N, \end{aligned}$$

hence $DFI \geq N^2 > 0$. By Lemma 11, there is a positive integer z which satisfies

$$(z - DFI(C - B + 1))^2 = DFI(C - B + 1)^2$$

and

$$N^2 \leq DFI(C - B + 1) \leq z \leq 2DFI(C - B + 1) \leq 2CDFI.$$

Combining a) and b) and applying Lemma 11, we see that Theorem 1 is proved.

Remark 2. Let $A > 2$ and $B \geq 0$. Matijasevič once tried to give a Diophantine representation of $C = \phi_B(A, 1)$, but his method was much more complicated and involved a lot of unknowns. In the case that A is even, Matijasevič and Robinson^[8] proved theoretically that there is a Diophantine representation of $C \parallel \phi_B(A, 1)$ with three natural number unknowns. Our Theorem 1 gives an explicit Diophantine representation of $C = \phi_B(A, 1)$ (A need not be even) with only three positive integer unknowns. (For natural number unknowns, we may replace x, y, z by $x + 1, y + 1, z + 1$ respectively.) Furthermore, Theorem 1 indicates that there is a Kalmár elementary function ϕ such that whenever $B \neq 0$ for any $N > 0$ we may require $N \leq x, y, z \leq \phi(A, B, C, N)$.

For convenience, D, F, I mentioned below are expressed as in Theorem 1.

Lemma 12. (i) If $K \neq 0$, then $K | L \wedge M \in \square \iff \exists z((Kz + L)^2 = K^2M)$;
 (ii) $X \neq 0 \iff \exists u \exists v (X = (2u - 1)(3v - 1))$.

Proof. (i) is obvious. For (ii), one may consult [4].

Theorem 2. Suppose $1 < |B| < \frac{|A|}{2} - 1$. Then

$$\begin{aligned} C = \phi_B(A, 1) &\iff A - 2 | C - B \wedge \exists x \neq 0 \exists y (DFI \in \square), \\ &\iff \exists u, v, y, z (((A - 2)z + C - B)^2 = (A - 2)^2 DF'I'), \end{aligned}$$

where F' and I' are obtained from F and I by substituting $(2u - 1)(3v - 1)$ for x .

Proof. By Lemma 2, it suffices to prove the first necessity and sufficiency.

“ \Rightarrow ” : Let $C = \phi_B(A, 1)$, then $C \equiv \phi_B(2, 1) = B \pmod{A - 2}$. Since $1 < |B| < |A| - 2 \leq |A - 2|$, C is nonzero. Choose x and y as in part b) of the proof of Theorem 1, then $x \neq 0$ and $DFI \in \square$.

“ \Leftarrow ” : Suppose $A - 2 | C - B$ and $DFI \in \square$ for some $x \neq 0$ and y . By part a) of the proof of Theorem 1, there exists an s such that $C = \phi_s(A, 1)$. Clearly we have

$$0 < |B| - 1 < |B| < |B| + 1 < 2|B| < |A| - 2 \leq |A - 2|,$$

$$B \equiv C \equiv \phi_s(2,1) = s \pmod{A-2}, \quad C \neq 0, \quad |s| > 1, \quad s \neq -B,$$

$$|B| < |A| = |\phi_2(A,1)| \leq |\phi_s(A,1)| = |C|.$$

Again by part a) of the proof of Theorem 1, we get $|s| = |B|$ and thus $s = B$, $C = \phi_B(A,1)$.

Remark 3. No one else has given a direct Diophantine representation of $C = \phi_B(A,1)$ with integer unknowns.

To cope with the exponential relation, we need

Lemma 13. *If $B > 0$ then*

$$V^{B-1}\phi_B(A,1) \equiv 1 + V^2 + \dots + V^{2(B-1)} \pmod{AV - V^2 - 1}.$$

Proof. By induction on B .

Lemma 14. *Let $B > 0$ and $|V| > 1$. We have $W = V^B$ if there is an A satisfying $|A| \geq \max\{V^{4B}, W^4\}$ and*

$$(V^2 - 1)W\phi_B(A,1) \equiv V(W^2 - 1) \pmod{AV - V^2 - 1}. \quad (**)$$

Proof. Suppose $|A| \geq \max\{V^{4B}, W^4\}$ and $(**)$ holds. By Lemma 13, we have

$$V^B(W^2 - 1) \equiv V^{B-1}(V^2 - 1)W\phi_B(A,1) \equiv W(V^{2B} - 1) \pmod{AV - V^2 - 1},$$

$$(V^B W + 1)(W - V^B) \equiv 0 \pmod{AV - V^2 - 1}.$$

Since $|A|^{\frac{1}{4}} \geq |V|^B > 2$, $1 + |A|^{\frac{1}{4}} + |A|^{\frac{1}{2}} \leq |A|^{\frac{3}{4}} - 1 < |A|^{\frac{3}{4}}$, we also have

$$|(V^B W + 1)(W - V^B)| \leq 2|A|^{\frac{1}{4}}(1 + |A|^{\frac{1}{4} + \frac{1}{2}}) < 2|A|^{\frac{1}{4}}(|A|^{\frac{3}{4}} - |A|^{\frac{1}{4}})$$

$$= 2|A| - 2|A|^{\frac{1}{2}} \leq |V||A| - 2V^2 \leq |AV| - (V^2 + 1)$$

$$\leq |AV - V^2 - 1|,$$

and hence $(V^B W + 1)(W - V^B) = 0$. Obviously $W \neq 0$, $|V^B W| \geq 2$, so $W = V^B$.

This concludes the proof.

Remark 4. The first result similar to Lemma 14 is obtained by Robinson and Jones. (On the basis of an idea of J. Robinson, Jones^[9] proved that for $B, V, W > 0$, $W = V^B$ holds if and only if there exists an even $A > \max\{2V^{3B}, 2W^3\}$ which satisfies $(**)$.)

Lemma 15. *Let $MX > 0$ and $Q(x, y, m) = 4m(mx + 2)x^3y^2 + 1$.*

(i) *If $Q(X, Y, M) \in \square$ then $Y = 0$ or $|Y| > |X|^{|X|}$;*

(ii) *for any given $N > 0$ there is a Y satisfying*

$$Q(X, Y, M) \in \square, \quad Y \equiv L \pmod{M} \quad \text{and} \quad N \leq Y \leq (2MX + 2)^{2(|M|+N)|X|^{-1}}.$$

Proof. i) Suppose $Y \neq 0$ satisfies $Q(X, Y, M) \in \square$, then for some $n > 0$ we have

$$2|XY| = \phi_n(2MX + 2, 1), \quad 0 \equiv \phi_n(2, 1) = n \pmod{2X}, \quad n \geq 2|X|.$$

(Observe that $((2MX + 2)^2 - 4)(2|XY|)^2 + 4 \in \square$.) If $|X| = 1$, then $2|Y| \geq$

$\phi_2(2MX + 2, 1) > 2$; if $|X| \geq 2$, then $2|XY| \geq (2MX + 1)^{n-1} > (2|X|)^{|X|+1} \geq 2|X| \cdot |X|^{|X|}$. This gives $|Y| > |X|^{|X|}$.

ii) Take $Y = \phi_{2KX}(2MX + 2, 1)/(2X)$ where K satisfies $M|K-L$ and $N \leq K < N + |M|$ (Notice that $\phi_{2KX}(2MX + 2, 1) \equiv \phi_{2KX}(2, 1) = 2KX \equiv 2LX \pmod{2MX}$.)

Remark 5. Lemma 15 is analogous to the second lemma of exponential size^[8]. Our polynomial Q is much simpler than the polynomial V in [8].

Lemma 16. For $S \neq 0$, we have

$$A_1, \dots, A_k \in \square \wedge S|T \wedge R > 0 \iff \exists n \geq 0 (M_k(A_1, \dots, A_k, S, T, R, n) = 0),$$

where

$$M_k(A_1, \dots, A_k, S, T, R, n) = \Pi(S^2n + T^2 - (2R - 1)S^2(T^2 + W^k \pm \sqrt{A_1}W^0 \pm \dots \pm \sqrt{A_k}W^{k-1}))$$

(W denotes $1 + \sum_{i=1}^k A_i^2$ and the product extends over all combinations of signs.)

Furthermore, we can require n to satisfy

$$W^k \leq n \leq (2R - 1)(T^2 + W^k + A_1 + A_2W + \dots + A_kW^{k-1}).$$

Proof. The first half is just the relation-combining theorem of [8], and the second half is obvious.

For the combination of some relations including the exponential relation, we have

Theorem 3. There exists a polynomial P_k and a Kalmar elementary function ϕ_k such that whenever $B > 1$, $S \neq 0$ and $|V| > 1$, we have

$$W = V^B \wedge A_1, \dots, A_k \in \square \wedge S|T \wedge R > 0 \iff \exists n, w \geq 0 \exists x, y, z > 0 (P_k(A_1, \dots, A_k, S, T, R, W, V, B, n, w, x, y, z) = 0).$$

Giving $N > 0$, we may require further that

$$N \leq n, w, x, y, z \leq \phi_k(A_1, \dots, A_k, |S|, |T|, R, |W|, |V|, B, N).$$

Proof. Let Q and M_i be polynomials given by Lemmas 15 and 16. Put

$$P_k(A_1, \dots, A_k, S, T, R, W, V, B, n, w, x, y, z) = M_{k+2}(DFI, Q(X, A, M), A_1, \dots, A_k, (AV - V^2 - 1)S, U, R, n),$$

where $X = 2B + V^2 + W^2$, $M = S^2V^2$, $A = V + zM$, $U = ((V^2 - 1)WC - V(W^2 - 1))S + (AV - V^2 - 1)T$, $C = B + w$. (For D, F, I , consult Theorem 1.) Below we will show that P_k has the desired property. (The existence of ϕ_k is implied by the following proof.)

Suppose $B > 1$, $S \neq 0$ and $|V| > 1$. Since $S \neq 0$ and $AV - V^2 = zS^2V^3 \neq 1$, we have $(AV - V^2 - 1)S \neq 0$ and $(AV - V^2 - 1, S) = 1$. Hence

$$(AV - V^2 - 1)S|U \iff S|T \wedge AV - V^2 - 1|(V^2 - 1)WC - V(W^2 - 1).$$

Note that $A \neq 0$, $B > 1$. Applying part (i) of Lemma 15, we get

$$Q(X, A, M) \in \square \Rightarrow |A| > X^X \geq \max\{V^{4B}, W^4\}.$$

This, together with Lemma 16, Theorem 1 and Lemma 14, proves the “ \Leftarrow ” part.

Below we assume $W=V^B$, $A_1, \dots, A_k \in \square$, $S|T$ and $R>0$. Giving $N>0$, we have $K=V+(B+N)S^2V^2>0$. By part (ii) of Lemma 15, there is an integer z for which

$$Q(X, A, M) \in \square, K \leq A \leq (2MX+2)^{2(M+K)X-1}$$

and

$$2 < B+N \leq z \leq A \leq (2MX+2)^{2(M+K)X-1}.$$

Let $w = \phi_B(A, 1) - B$, then $N \leq w \leq A^{B-1}$ (since $B+N \leq A = \phi_2(A, 1) \leq \phi_B(A, 1) \leq A^{B-1}$). By Theorem 1, DFI is square for some $x, y > 0$ satisfying

$$N \leq x \leq A^{16N^2C^4D^2-1}, N \leq y \leq (2CDF)^{B+2CNF^2-1} \text{ and } N^2 \leq DFI$$

(where $C = B+w = \phi_B(A, 1) \leq A^{B-1}$). Since $S|T$ and $W=V^B$, using Lemma 13 we get $(AV - V^2 - 1)S|U$. By Lemma 16, there exists an $n \geq 0$ such that

$$M_{k+2}(DFI, Q(X, A, M), A_1, \dots, A_k, (AV - V^2 - 1)S, U, R, n) = 0$$

and

$$N \leq N^2 \leq DFI \leq \bar{W}^{k+2} \leq n \leq (2R-1)(U^2 + \bar{W}^{k+2} + DFI + Q(X, A, M)\bar{W} + A_1\bar{W}^2 + \dots + A_k\bar{W}^{k+1}),$$

where $\bar{W} = 1 + D^2F^2I^2 + Q^2(X, A, M) + \sum_{i=1}^k A_i^2$. This concludes the proof.

Remark 6. It is known^[8,9] that there is a Diophantine representation of $W=V^B$ (where $B, V > 1$ and $W > 0$) with only 5 natural number unknowns, however the two former methods cannot be used to prove Theorem 3. Namely, if we do not employ more unknowns, the method of [8] (respectively, the method of [9] pointed out by Robinson) will not allow $R>0$ (resp., $S|T$) to be a term of the conjunction, for we already have an inequality E_2 (resp., for if V is odd and A is even, then $AV - V^2 - 1$ is even and hence not relatively prime to even S).

Lemma 17. *There exists a polynomial H_k such that whenever $S \neq 0$ we have*

$$A_1, \dots, A_k \in \square \wedge S|T \iff \exists z (H_k(A_1, \dots, A_k, S, T, z) = 0).$$

Proof. Let

$$J_k(A_1, \dots, A_k, x) = \prod (x \pm \sqrt{A_1} \pm \sqrt{A_2}W \pm \dots \pm \sqrt{A_k}W^{k-1}) \\ = X^{2k} + C_1X^{2k-1} + \dots + C_{2k-1}X + C_{2k},$$

where $W = 1 + \sum_{i=1}^k A_i^2$ and the product is over all sets of signs. Put

$$H_k(A_1, \dots, A_k, S, T, z) = (Sz + T)^{2k} + C_1S(Sz + T)^{2k-1} + \dots \\ + C_{2k-1}S^{2k-1}(Sz + T) + C_{2k}S^{2k}.$$

Clearly all the rational zeros of $J_k(A_1, \dots, A_k, x)$ are integers, so when $S \neq 0$ we have

$$A_1, \dots, A_k \in \square \wedge S|T \stackrel{[8]}{\iff} \exists x (J_k(A_1, \dots, A_k, x) = 0) \wedge S|T \\ \iff \exists z (H_k(A_1, \dots, A_k, S, T, z) = 0).$$

Theorem 4. *There is a polynormial Q_k such that whenever $B > 1$, $S \neq 0$ and $|V| > 1$ we have*

$$\begin{aligned} W = V^B \wedge A_1, \dots, A_k \in \square \wedge S|T \\ \Leftrightarrow \exists x \neq 0 \exists m, w, y, z (Q_k(A_1, \dots, A_k, S, T, W, V, B, m, w, x, y, z) = 0) \\ \Leftrightarrow \exists m, w, u, v, y, z (Q_k(A_1, \dots, A_k, S, T, W, V, B, m, w, (2u - 1) \\ \times (3v - 1), y, z) = 0). \end{aligned}$$

(By letting $A_1 = \dots = A_k = S = T = 1$, we obtain a Diophantine representation of $W = V^B$ with only 6 integer unknowns.)

Proof. Let Q and H_i be polynomials given by Lemmas 15 and 17. Put

$$\begin{aligned} Q_k(A_1, \dots, A_k, S, T, W, V, B, m, w, x, y, z) \\ = H_{k+2}(DFI, Q(X, A, M), A_1, \dots, A_k, (AV - V^2 - 1)S, U, m), \end{aligned}$$

where X, A, M, D, F, I, U are expressed as in the proof of Theorem 3 except that $C = B + w(A - 2)$. Since $|A| > X^X$ implies $|A| > \max\{V^{4B}, W^4\} \wedge 2 < 2B < |A| - 2$, by Theorem 2 and Lemmas 12, 17, we can easily show the required property for Q_k .

Remark 7. It is the first time to give directly a Diophantine representation of the exponential relation with integer unknowns. By the usual method of [4], we need at least 15 integer unknowns.

The author is indebted to Prof. Moh Shawkwei for his guidance.

REFERENCES

- [1] Davis, M., Putnam, H. & Robinson, J., The decision problem for exponential Diophantine equations, *Ann. Math.*, **74**(1961), 425.
- [2] Matijasevič, Ju. V., Enumerable sets are Diophantine, *Soviet Math. Doklady*, **11**(1970), 354.
- [3] Jones, J. P., Universal diophantine equation, *J. Symbolic, Logic*, **47**(1982), 549.
- [4] Tung Shih Ping, On weak number theories, *Japan. J. Math.*, **11**(1985), 203.
- [5] Robinson, R. M., Arithmetical definitions in the ring of integers, *Proc. Amer. Math. Soc.*, **2**(1951), 279.
- [6] Davis, M., Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly*, **80**(1973), 233.
- [7] 莫绍揆, 递归论, 科学出版社, 北京, 1987, 97—106.
- [8] Matijasevič, Ju. V. & Robinson, J., Reduction of an arbitrary diophantine equation to one in 13 unknowns, *Acta Arith.*, **27**(1975), 521.
- [9] Jones, J. P., Diophantine representation of Mersenne and Fermat primes, *ibid.*, **35**(1979), 209.