ACTA ARITHMETICA
XXVII (1975)

Reduction of an arbitrary diophantine equation to one in 13 unknowns

by

YURI MATIJASEVIČ (Leningrad) and JULIA ROBINSON (Berkeley, Calif.)

A diophantine equation is a polynomial equation in some *parameters* $a_1, \ldots, a_\mu$ and some *unknowns* $z_0, \ldots, z_\nu$. That is, an equation of the form

$$P(a_1, \ldots, a_\mu, z_0, \ldots, z_\nu) = 0 \tag{1}$$

where P is a polynomial with integer coefficients (μ and ν are particular natural numbers). Both parameters and unknowns will be restricted to the natural numbers $N = \{0, 1, \ldots\}$. The distinction between parameters and unknowns will be clear if we consider Mordell's equation

$$y^2 = x^3 + a. \tag{2}$$

Here x and y are unknowns and a is a parameter. The problem is to find the values of the parameter a for which (2) has a solution for the unknowns x and y. A trivial problem would result if x and a were unknowns and y the parameter. (For every y, we can find x and a satisfying (2).) Thus, it is convenient to think of P as a polynomial in $z_0, \ldots, z_\nu$ with coefficients which are polynomials in $a_1, \ldots, a_\mu$ with integer coefficients. We then write $P(z_0, \ldots, z_\nu)$ and speak of $a_1, \ldots, a_\mu$ as the *parameters of* P and $z_0, \ldots, z_\nu$ as the *variables of* P.

Given a polynomial P, we shall construct another polynomial $\overline{P}$ such that

$$P(a_1, \ldots, a_\mu, z_0, \ldots, z_\nu) = 0 \tag{3}$$

for some $z_0, \ldots, z_\nu$ if and only if

$$\overline{P}(a_1, \ldots, a_\mu, b, c, d, e, f, g, h, i, j, k, l, m, n) = 0 \tag{4}$$

for some $b, c, d, e, f, g, h, i, j, k, l, m, n$.

We say that (3) is a *diophantine definition* with $\nu+1$ unknowns of the relation among $a_1, \ldots, a_\mu$ which holds if and only if (3) has a solution, while (4) is a diophantine definition of the same relation with 13 unknowns.

We shall also speak of the equation $P = 0$ being *reduced* to the equation $\bar{P} = 0$. Two equations with the same parameters are *equivalent* if they are solvable for exactly the same values of the parameters.

In 1970, it was shown that every recursively enumerable relation has a diophantine definition [7]. From this and the existence of a universal recursively enumerable relation, it follows that for some δ and ν, there is a polynomial U of degree δ in $z_0, \ldots, z_\nu$ such that

$$U(a, n, z_0, \ldots, z_\nu) = 0$$

for some $z_0, \ldots, z_\nu$ if and only if $a \in \mathscr{D}_n$, where $\mathscr{D}_0, \mathscr{D}_1, \ldots$ is a list of all diophantine sets, i.e. sets which have a diophantine definition. By the use of pairing functions, this result can be extended to the case of any number of parameters leaving δ and ν unchanged. Hence every diophantine equation is equivalent to an equation with the same parameters of degree δ in $\nu+1$ unknowns. Before 1970, the existence of such a ν was widely disbelieved.

Our proof that the number of unknowns needed for a diophantine definition is $\leqslant 13$ is virtually self-contained, using only familiar or easily proved facts from elementary number theory.

Skolem [11] showed that every diophantine equation is equivalent to an equation of total degree 4. To see this we can replace (1) by an equation of the form $A = B$ where A and B are polynomials with positive integer coefficients. We then make up a system of equations $A_i = B_i$ of the forms $\alpha+\beta = \gamma$ and $\alpha\cdot\beta = \gamma$ where each α, β, γ is either a natural number, a parameter or variable of P, or a new variable introduced to represent an expression in the stepwise calculation of A and B, making sure to represent A and B by the same variable. Then $P = 0$ for some $z_0, \ldots, z_\nu$ if and only if $\sum(A_i-B_i)^2 = 0$ has a solution. Since A_i-B_i is of at most the second degree, the resulting equation will be of at most the fourth degree. Skolem's reduction increases the number of unknowns according to the number of steps needed to calculate P. Neither his result nor ours shows that both the degree (with respect to the unknowns) and the number of unknowns can be bounded simultaneously, although this is clear from the existence of U.

Now a diophantine equation $F(a, u_1, \ldots, u_\nu) = 0$ has a solution for $u_1, \ldots, u_\nu$ if and only if

$$(u_0+1)\big(1-F^2(u_0, \ldots, u_\nu)\big)-1 = a$$

has a solution for $u_0, \ldots, u_\nu$ (see Putnam [9]). Thus, our theorem shows that *every diophantine set is the non-negative part of the range on* $\boldsymbol{N}$ *of a polynomial with* 14 *variables.*

On the other hand, if we consider the range on $\boldsymbol{N}$ of a polynomial with positive coefficients, we cannot put a bound on the number of variables needed as the following example of R. M. Robinson shows. Let

$$F = x_1^n + 2x_2^n + 4x_3^n + \ldots + 2^{k-1}x_k^n.$$

Then F assumes the values $0, 1, \ldots, 2^k-1$ and no other values less than 2^n. We shall show that for n sufficiently large, the range (on $\boldsymbol{N}$) of F is not the same as the range of any polynomial with positive coefficients and fewer variables.

Suppose G is a polynomial with positive integer coefficients in $k-1$ variables with the same range as F. The G must assume some value less than 2^k with some variable $x > 1$. We may assume that when the other variables are fixed then G depends on x and hence has the form

$$H(x) = c_{k-1}x^{k-1} + \ldots + c_1x + c_0$$

where $c_1, \ldots, c_{k-1}$ are not all zero and $H(2) < 2^k$. But then,

$$2^k \leqslant H(2^k) \leqslant (2^k)^{k-1}H(2) < 2^{k^2} \leqslant 2^n$$

for $n \geqslant k^2$. Hence G assumes some value g with $2^k \leqslant g < 2^n$ while F does not which contradicts the assumption that F and G have the same range. Nevertheless for any n and k, the range of the corresponding F is the non-negative part of the range of a polynomial G in 14 variables with integer coefficients.

We believe that the minimum number of unknowns necessary is less than 13, possibly as small as 3, but new methods will be needed to obtain the optimum result. In a companion paper [12] written with Martin Davis, we give a direct construction of a universal polynomial as well as applications of this paper to the theory of diophantine equations.

Notation. Lower-case Latin letters will stand for natural numbers; upper-case Latin letters will stand for integers or particular polynomials with integer coefficients; lower case Greek letters will be used in various ways with their range given at the time or clear from the context. We will use the following notation for familiar relations of number theory: $x|y$ for 'x divides y'; $x \perp y$ for 'x is prime to y'; $[\sigma]$ for the greatest integer $\leqslant \sigma$ where σ is real; $\langle\sigma\rangle$ for the nearest integer to σ – we consider $\langle\sigma\rangle$ is undefined if σ is an integer plus a half; $\mathrm{Rem}(x, y)$ for 'the remainder when x is divided by y'; and $x = \square$ for 'x is a square'.

The paper is organized in two parts as follows:

Part I. Definition of the exponential function.

1. The Relation-combining Theorem.
2. Lucas sequences and Pell equations.
3. Definition of the nth solution of a Pell equation.
4. The exponential function.

Part II. Reduction to 13 unknowns.

5. The code.
6. Diophantine equation with coded unknowns.
7. Reduction to the positiveness of a polynomial.
8. Reduction to binomial coefficients.
9. Reduction to a partial binomial expansion.
10. Definition of a partial binomial expansion.
11. Completion of the proof.

Section 4 is not needed for the rest of the paper but contains a diophantine definition with just 5 unknowns of the relation $y = x^n$. We might say that the cost of "polynomializing exponentiation" is not more than 5 unknowns. It also provides a good introduction to the similar but more complicated Section 10. Part I is not used in Part II until Section 9 where the two lemmas of exponential size from Section 2 are needed. Thus, a reader familiar with some account of the negative solution to Hilbert's tenth problem (any of the expository articles by Davis [3], Manin [6], Matijasevič [8], etc. or the original papers by Davis, Putnam, and Robinson [4], Matijasevič [7], and Robinson [10]) may wish to begin with Part II and return to Part I as needed.

Construction of $\bar{P}$. We define a polynomial Q with parameters $a_1, \ldots, a_\mu$ and variables b, c, t such that $P(z_0, \ldots, z_\nu) = 0$ has a solution if and only if there are b and c such that $Q(b, c, t) > 0$ for all t. Q is completely defined by the 14 *-formulas in Sections 5, 6, and 7.

Next we consider an arbitrary polynomial Q in one variable with positive leading coefficient. We find a polynomial $\bar{Q}$ with 11 variables and the same parameters as Q such that $Q(t) > 0$ for all t if and only if $\bar{Q} = 0$ has a solution. We apply this result to $Q(b, c, t)$, treating b and c as parameters, and let $\bar{P}$ be the corresponding $\bar{Q}$. There are 24 **-formulas in Sections 1, 2, 3, 8, 9, and 10 which completely define $\bar{P}$ given Q.

We wish to thank R. M. Robinson for several ideas and suggestions made during the course of this work (some of these have been superseded and others incorporated) and to thank Craig Smorynski who read the manuscript and made helpful comments.

PART I

Definition of the exponential function

1. The Relation-combining Theorem. Certain combinations of relations can be defined more cheaply than by defining each separately by an equation and then combining the equations. For example, let D and E be integers. Then $D > 0$ and $E \neq 0$ both hold if and only if $DE^2 = 1 + x$ for some natural number x. The direct method of combining the equations $D = 1 + x$ and $E^2 = 1 + y$ gives $(D - 1 - x)^2 + (E^2 - 1 - y)^2 = 0$ which has two unknowns. The Relation-combining Theorem will permit us to save 2 unknowns in the definition of the exponential function and 7 unknowns in the reduction of an arbitrary diophantine equation.

We will need a bound on the absolute values of the complex zeros of a polynomial $F(z) = \varphi_a z^a + \ldots + \varphi_1 z + \varphi_0$ where the φ's are complex numbers and $|\varphi_a| \geqslant 1$. Suppose $F(\tau) = 0$ and $|\tau| \geqslant 1$. Then

$$|\tau^a| \leqslant |\varphi_a \tau^a| \leqslant \sum_{i=0}^{a-1} |\varphi_i| \cdot |\tau|^{a-1}$$

so $|\tau| < 1 + \sum_{i=0}^{a-1} |\varphi_i|$. In particular, if the φ_i are integers then all zeros of $F(z)$ will lie in a circle of radius $1 + \sum_{i=0}^{a-1} \varphi_i^2$.

THEOREM 1. *Suppose $A_1, \ldots, A_q$ are integers. Then $A_1 = \square, \ldots, A_q = \square$ if and only if*

$$J_q(A_1, \ldots, A_q, X) = 0 \quad \text{for some integer } X \tag{1}$$

where

$$J_q(A_1, \ldots, A_q, X) = \prod (X \pm \sqrt{A_1} \pm \sqrt{A_2}\, W \pm \ldots \pm \sqrt{A_q} W^{q-1}), \tag{2}$$

$$W = 1 + \sum_{i=1}^{q} A_i^2, \tag{3}$$

and the product in (2) extends over all combinations of signs.

Proof. Clearly, (1) has a solution if all the A's are squares. On the other hand, we will show by induction on q that (1) implies that all the A's are squares. Obvious for $q = 1$. Suppose it is true for $q = j$. If $A_{j+1} = \square$, then $J_{j+1}(A_1, \ldots, A_{j+1}, X) = 0$ for some integer X if and only if $J_j(A_1, \ldots, A_j, Y) = 0$ for some integer Y. Hence the assertion holds for $q = j + 1$. Suppose $A_{j+1} \neq \square$ and some factor ξ of $J_{j+1}(A_1, \ldots, A_{j+1}, X)$ is 0 for X. Let p be a prime which divides A_{j+1} to an odd power and $\bar{\xi}$ be the conjugate of ξ with respect to $\sqrt{p}$. Then

$$\xi - \bar{\xi} = 0 = \pm 2(\sqrt{A_{j+1}}\, W^j \pm \ldots)$$

where ... stands for similar terms of lower degree in W. But this is impossible because $W \geqslant 1 + \sum_{i=1}^{j} |\sqrt{A_i}|$.

Remark. Actually (1) has a solution with X a natural number whenever it has an integer solution. In Theorem 3, we will make use of the fact that in this theorem we ask for integer solutions of (1).

THEOREM 2. *Let $F(X) = F_a X^a + \ldots + F_1 X + F_0$ where $F_a \neq 0$. There is a polynomial H such that if $F_a \perp B$ and $B \neq 0$ then*

$$B \mid C, \quad D > 0, \quad F(X) = 0$$

for some integer X if and only if

$$H(B^2x+C^2) = 0$$

for some natural number x.

Proof. Choose $\overline{F}$ so large that all the integer zeros of F are greater than $-\overline{F}$. Let $G(Y) = F(Y-\overline{F}-C^2)$ then the integer zeros of $G(Y)$ are all greater than C^2. Let $H(Z) = J^qG(Z/J)$. Then the zeros of $H(Z)$ are J times the zeros of $G(Y)$. If $J \perp F_a$ (F_a is the leading coefficient of $G(Y)$) then the integer zeros of $H(Z)$ correspond to integer zeros of $G(Y)$ since the remaining rational zeros of $G(Y)$ have denominators which divide F_a. Also if $J > 0$ the integer zeros of $H(Z)$ will all be positive; otherwise they will all be negative. Now let $J = B^2(2DF_a^2-1)$. Then $J > 0$ if and only if $D > 0$. (Obviously, $J \neq 0$.)

Suppose $H(B^2x+C^2) = 0$. Then $D > 0$ since B^2x+C^2 is positive. Also $B \mid C$ since B^2x+C^2 is a multiple of J and hence of B^2. By the argument above, $F(X) = 0$ for some integer X. On the other hand, suppose $B \mid C$, $D > 0$, and $F(X) = 0$. Then $H(B^2x+C^2) = 0$ has a solution if

$$B^2(2DF_a^2-1)(X+\overline{F}+C^2) = B^2x+C^2$$

has. It does, since the left side is a multiple of B^2 and greater than C^2.

Notice that we cannot apply Theorem 2 again since $H(B^2T+C^2) = 0$ will always have an integer solution for T if $B \mid C$ and $F(X) = 0$.

Theorem 3. (The Relation-combining Theorem.) *For every q there is a polynomial M_q with integer coefficients such that for all integers $A_1, \ldots, A_q, B, C, D$ with $B \neq 0$ the conditions*

$$A_1 = \square, \quad \ldots, \quad A_q = \square, \quad B \mid C, \quad D > 0$$

all hold if and only if

$$M_q(A_1, \ldots, A_q, B, C, D, n) = 0$$

for some natural number n.

Proof. Let $F(X) = J_q(A_1, \ldots, A_q, X)$ of Theorem 1. Then $a = 2^q$ and $F_a = 1$. Hence the hypothesis of Theorem 2 is satisfied so we can take for M_q the corresponding polynomial $H(B^2n+C^2)$.

In order to construct M_q explicitly we need to choose $\overline{F}$ and then carry out the steps in the proof of Theorem 2. From the factored form of J_q given by (2), we see that all integer zeros of J_q are greater than $-W^q$. Hence we can put $\overline{F} = W^q$. Also $J = B^2(2D-1)$. Therefore

$$** \quad M_q(A_1, \ldots, A_q, B, C, D, n) = \prod \left(B^2n+C^2-B^2(2D-1)(C^2+W^q \pm \sqrt{A_1} \pm \sqrt{A_2}W \pm \ldots \pm \sqrt{A_q}W^{q-1})\right)$$

where the product is over all sets of signs and

$$** \quad W = 1+\sum_{i=1}^{q} A_i^2$$

will satisfy Theorem 3. Notice that the parameters of M_q are $A_1, \ldots, A_q, B, C, D$ and the only variable is n. (W is used only as an abbreviation for the sum.)

2. Lucas sequences and Pell equations. A *Lucas sequence* is a sequence of integers generated by

$$(1) \qquad X_0 = A, \quad X_1 = B, \quad X_{n+2} = CX_{n+1}+DX_n$$

where A, B, C, and D are integers. For example, if $A = 0$, $B = 1$, $C = 3$, $D = -2$ then $X_n = 2^n-1$.

The ultimate tool in both the definition of exponentiation and the reduction to 13 unknowns is a diophantine definition of the nth term of a special type of Lucas sequences. In this section, we give some elementary facts about Lucas sequences and their relation to Pell equations.

A diophantine equation of the form

$$(2) \qquad x^2-dy^2 = 1$$

where d is a parameter is called a Pell equation. The basic result about solutions of Pell equations is:

If $d > 0$ and not a square then (2) has infinitely many solutions in natural numbers; if d is a positive square, then the only solution is $x = 1$ and $y = 0$; if $d = 0$, then the solutions are $x = 1$ and $y = 0, 1, \ldots$

We shall be concerned with a special type of Pell equation — those of the form

$$(3) \qquad x^2-(a^2-1)y^2 = 1 \quad \text{for} \quad a > 0.$$

In this case, let the solutions in order of the size of y be

$$x = \chi_a(n), \quad y = \psi_a(n).$$

In particular, $\chi_1(n) = 1$ and $\psi_1(n) = n$.

There are two convenient ways of generating the solutions of (3): as Lucas sequences and algebraically in terms of the powers of the unit $a+\sqrt{a^2-1}$.

Recurrence equations. For $a > 0$,

$$(4) \qquad \chi_a(0) = 1, \quad \chi_a(1) = a, \quad \chi_a(n+2) = 2a \cdot \chi_a(n+1)-\chi_a(n),$$

$$(5) \qquad \psi_a(0) = 0, \quad \psi_a(1) = 1, \quad \psi_a(n+2) = 2a \cdot \psi_a(n+1)-\psi_a(n).$$

Algebraic characterization. For $a > 1$,

$$(6) \qquad (a+\sqrt{a^2-1})^n = \chi_a(n)+\psi_a(n)\sqrt{a^2-1}.$$

For the proof of these results, see any elementary number theory book which treats the Pell equation. With this background, we can easily derive the properties of χ and ψ which will be needed. The reader may also wish to consult the derivations in expository articles on Hilbert's tenth problem.

For every $a > 0$ and $b > 0$, there are infinitely many n such that $b \mid \psi_a(n)$ since $x^2 - (a^2-1)b^2y^2 = 1$ has infinitely many solutions.

Also for $a > 0$, $n \leqslant \psi_a(n)$ by the definition of $\psi_a(n)$ and the fact that (3) has infinitely many solutions.

Congruence rule. For $a > 0$ and $b > 0$, if $a \equiv b \pmod m$ then

$$\chi_a(n) \equiv \chi_b(n), \quad \psi_a(n) \equiv \psi_b(n) \pmod m.$$

This is clear since $\chi_a(n)$ and $\psi_a(n)$ for fixed n are polynomials in a by (4) and (5). The special case of the congruence rule which we use over and over is obtained when $b = 1$ and $m = a-1$ so

$$\psi_a(n) \equiv n \pmod{a-1}.$$

Bounds on ψ. For $a > 0$,

$$(2a-1)^n \leqslant \psi_a(n+1) \leqslant (2a)^n.$$

To check this, note that $\psi_a(1) = 1$ and $\psi_a(2) = 2a$. Since $\psi_a(n+1)$ is obtained from $\psi_a(n)$ by multiplying by $2a$ and subtracting something, the upper limit is verified by induction. Similarly, the lower limit can be checked since $\psi_a(n+1)$ is obtained by multiplying by $2a$ and subtracting something less than $\psi_a(n)$, i.e. multiplying by something greater than $2a-1$.

Addition equations. For $a > 0$,

$$\chi_a(n \pm m) = \chi_a(n)\chi_a(m) \pm (a^2-1)\psi_a(n)\psi_a(m), \tag{7}$$

$$\psi_a(n \pm m) = \pm\chi_a(n)\psi_a(m) + \psi_a(n)\chi_a(m). \tag{8}$$

Trivial for $a = 1$. The proof for $a > 1$ is immediate from the algebraic characterization of χ and ψ together with the fact that $(a+\sqrt{a^2-1})^{-1} = a-\sqrt{a^2-1}$. In particular,

$$\chi_a(2n) = 2\chi_a(n)^2 - 1, \tag{9}$$

$$\psi_a(2n) = 2\chi_a(n)\psi_a(n). \tag{10}$$

In general, we will be interested in the ψ-sequence rather than the χ-sequence. For $a > 0$,

$$(a^2-1)y^2 + 1 = \square$$

if and only if $y = \psi_a(n)$ for some n.

Next we prove two lemmas which are used in the next section in the definition of $\psi_A(B) = C$.

First step-down lemma. *For $a > 0$, if $\psi_a(m)^2 \mid \psi_a(n)$ then $\psi_a(m) \mid n$.*

Proof. For convenience, we will drop the subscript a throughout. Trivial for $m = 0$. For $m > 0$ by the addition equation for ψ,

$$\psi(m+k) \equiv \chi(m)\psi(k) \pmod{\psi(m)}.$$

But by (3), $\chi(m) \perp \psi(m)$. Hence $\psi(m) \mid \psi(m+k)$ if and only if $\psi(m) \mid \psi(k)$. If $0 < k < m$, then $0 < \psi(k) < \psi(m)$ and $\psi(m) \nmid \psi(k)$. Hence $\psi(m) \mid \psi(n)$ if and only if $m \mid n$. Now

$$\left(\chi(m) + \psi(m)\sqrt{a^2-1}\right)^k = \chi(km) + \psi(km)\sqrt{a^2-1}.$$

Using the binomial expansion and taking the irrational part, we obtain

$$\psi(km) = \sum_{j \leqslant k,\, j \text{ odd}} \binom{k}{j} \chi(m)^{k-j} \psi(m)^j (a^2-1)^{(j-1)/2}.$$

Hence

$$\psi(km) \equiv k\chi(m)^{k-1}\psi(m) \pmod{\psi(m)^3}.$$

Since $\chi(m) \perp \psi(m)$, we conclude that if $\psi(m)^2 \mid \psi(km)$ then $\psi(m) \mid k$. The lemma follows.

Remark. This lemma also follows from the classical laws of apparition and repetition of primes in Lucas sequences beginning with $0, 1, \ldots$ We call it a step-down lemma since the conclusion is obtained from the hypothesis by reducing the power of $\psi(m)$ by 1 and replacing $\psi(n)$ by its index n. Thus a particular divisibility condition on $\psi(n)$ implies a corresponding divisibility condition on n.

Second step-down lemma. *For $a > 1$ and $n > 0$, if $\psi_a(j) \equiv \psi_a(i) \pmod{\chi_a(n)}$ then $j \equiv i$ or $j \equiv -i \pmod{2n}$.*

Proof. Here again we omit the subscript a. From the addition equations (8), (9), and (10),

$$\psi(2n \pm m) \equiv \mp\psi(m) \pmod{\chi(n)}.$$

Hence

$$\psi(4n \pm m) \equiv -\psi(2n \pm m) \equiv \pm\psi(m) \pmod{\chi(n)}.$$

Hence $\psi \pmod{\chi(n)}$ has a period of length $4n$. For $m \leqslant n$, we have $\pmod{\chi(n)}$,

$$\begin{aligned} \psi(m) &\equiv \psi(m), \\ \psi(2n-m) &\equiv \psi(m), \\ \psi(2n+m) &\equiv -\psi(m), \\ \psi(4n-m) &\equiv -\psi(m). \end{aligned}$$

In order to prove the lemma, we need to show that

$$\psi(m) \not\equiv \pm\psi(m') \pmod{\chi(n)} \quad \text{for} \quad m < m' \leqslant n. \tag{11}$$

It would be sufficient to show that

$$\psi_a(n) < \tfrac{1}{2}\chi_a(n) \quad \text{for} \quad n > 0. \tag{12}$$

This is true for $a > 2$, since

$$4\psi_a(n)^2 < (a^2-1)\psi_a(n)^2 + 1 = \chi_a(n)^2.$$

Thus the absolutely least residue of $\psi \pmod{\chi(n)}$ is 0 at 0, increases to a maximum of $\psi(n)$ at n, decreases to a minimum of $-\psi(n)$ at $3n$, and increases to 0 at $4n$.

For $a = 2$, (11) holds but not (12). However we can easily check that

$$\tfrac{1}{2}\chi_2(n) \geqslant \chi_2(n) - \psi_2(n) > \psi_2(n-1) \quad \text{for} \quad n > 0,$$

since the recurrence equations yield

$$2\psi_2(n) - \chi_2(n) = \psi_2(n-1) \geqslant 0$$

and

$$\chi_2(n) - \psi_2(n) - \psi_2(n-1) = \chi_2(n-1) > 0.$$

Remark. From the relation in the hypothesis among the terms of Lucas sequences, we obtain almost the same relation among the corresponding indices. Hence we also call this a step-down lemma. It should be compared with Lemma 6 used to define the Fibonacci sequence in [7] as well as similar lemmas used by Kosovskii [5], Čudnovskii [1], and Davis [2] in their definitions of the nth solution of the special Pell equation. All of the definitions used the first step-down lemma.

Next we will prove two lemmas which can be used to force one unknown to be exponentially larger than another. These lemmas will be used only in Section 9.

First lemma of exponential size. *There is a polynomial U with integer coefficients such that*

$$U(x, y) = \square \tag{13}$$

implies that $y > x^x$ and furthermore, for every x and $m > 0$, there is a y satisfying (13) *such that $m \mid y+1$.*

Proof. By the basic result on Pell equations, for every $d > 1$ and $m > 0$ there are infinitely many z satisfying

$$(d^2-1)(d-1)^2 m^2 (z+1)^2 + 1 = \square.$$

We can put $y+1 = m(z+1)$. Hence there are infinitely many solutions for y of

$$(d^2-1)(d-1)^2(y+1)^2 + 1 = \square \tag{14}$$

such that $m \mid y+1$. Also $(d-1)(y+1)$ is $\psi_d(w)$ for some w by (14) and $w \equiv (d-1)(y+1) \pmod{d-1}$ by the congruence rule. Since $(d-1)(y+1) \neq 0$, w is a positive multiple of $d-1$ and $\psi_d(w) \geqslant \psi_d(d-1)$. Hence $(d-1)(y+1) \geqslant (2d-1)^{d-2}$ for $d > 2$. If we put $d = x+3$, then

$$(x+2)(y+1) \geqslant (2x+5)^{x+1}$$

so

$$y > x^x.$$

Thus, we can take

$$U(x, y) = \left((x+3)^3 - 1\right)(x+2)^2(y+1)^2 + 1 \tag{**15}$$

to satisfy the lemma.

Second lemma of exponential size. *There is a polynomial V with integer coefficients such that*

$$V(x, y, m) = \square \tag{16}$$

implies $y > x^x$ and furthermore, for every x there exists y satisfying (16) *in every residue class* $\pmod{m+1}$.

Proof. Consider the equation

$$\left((d(m+1)+1)^2 - 1\right)d^2(y+1)^2 + 1 = \square \tag{17}$$

where $d > 1$. Now by the congruence rule,

$$\psi_{d(m+1)+1}(d(k+1)) \equiv d(k+1) \pmod{d(m+1)}$$

so there is a y satisfying (17) and such that

$$d(y+1) \equiv d(k+1) \pmod{d(m+1)},$$

i.e. $y \equiv k \pmod{m+1}$. Also if y satisfies (17), then $d(y+1) = \psi_{d(m+1)+1}(w)$ for some $w \equiv d(y+1) \pmod{d(m+1)}$. Since $d(y+1) > 0$, we must have $w > 0$ so $\psi_{d(m+1)+1}(w) \geqslant \psi_{d(m+1)+1}(d)$. Hence

$$d(y+1) \geqslant (2d(m+1)+1)^{d-1}$$

and so

$$y \geqslant (2d+1)^{d-2}.$$

If we put $d = x+3$, we will have $y > x^x$ as required. Thus, we can take

$$V(x, y, m) = \left(((m+1)(x+3)+1)^2 - 1\right)(x+3)^2(y+1)^2 + 1. \tag{**18}$$

Remark. Notice that the second lemma does not include the first since V is a function of m while U is not.

3. Definition of the nth solution of a Pell equation. In this section, we will give a diophantine definition of the relation $\psi_A(B) = C$ for $A > 1$, $B > 0$, and $C > 0$. The definition is more economical with respect to the number of unknowns (three) than the previously known definitions given by Kosovskii [5], Čudnovskii [1], and Davis [2].

Let $\mathscr{A}$ be the following system of conditions:

A1 $DFI = \square$, $F \mid H - C$, $B \leqslant C$,

**A2 $D = (A^2-1)C^2+1$,

**A3 $E = 2(i+1)D(e+1)C^2$,

**A4 $F = (A^2-1)E^2+1$,

**A5 $G = A+F(F-A)$,

**A6 $H = B+2jC$,

**A7 $I = (G^2-1)H^2+1$.

The parameters of $\mathscr{A}$ are e, A, B, C and the unknowns are i, j, D, E, F, G, H, I. We shall say that $\mathscr{A}$ can be satisfied if there are natural numbers i, j and integers D, E, F, G, H, I such that A1, ..., A7 hold. Of course whether $\mathscr{A}$ can be satisfied depends on the values of the parameters e, A, B, C and hence $\mathscr{A}$ defines a relation among them.

THEOREM 4. *Suppose $A > 1$, $B > 0$, $C > 0$. Then $\psi_A(B) = C$ if and only if $\mathscr{A}$ can be satisfied.* [*Furthermore,* A3 *and* A4 *imply* $e+1 \perp F$.]

Remarks. We can write $\mathscr{A}$ as a system with only two unknowns i and j since we can eliminate D, E, F, G, H, I in order by means of A2, ..., A7. To see this is possible, notice that the letters on the right side of an equation of $\mathscr{A}$ are either parameters, unknowns defined by earlier equations, i, or j. We have had to put in the extraneous conditions about e in order to apply the theorem later. In Section 11, we will need to combine the condition $F \mid H - C$ of A1 with another divisibility condition with divisor $e+1$ which we can do provided $e+1 \perp F$. If we only want to define $\psi_A(B) = C$, we can put $e = 0$ throughout. The reason we use integer parameters A, B, C and then suppose they are positive is again for applications of the theorem. In general, A, B, C, will be assigned values which are polynomials (with integer coefficients) in parameters and unknowns. We must check in each case that the hypothesis concerning A, B, C is satisfied before substituting $\mathscr{A}$ for $\psi_A(B) = C$ in another system as well as be sure that the set of unknowns of $\mathscr{A}$ is disjoint from the set of unknowns in the other system.

Proof. Suppose $A > 1$, $B > 0$, $C > 0$, and A1, ..., A7 hold. We see immediately that in fact $D, \ldots, I$ are all positive. ($F > A$ since $F = (A+1)(A-1)E^2+1$ and $A > 1$.) We will first show that D, F, and I are co-prime and hence each is a square by A1. We obtain in turn

(1) $$E \equiv 0, \quad F \equiv 1, \quad G \equiv 1, \quad I \equiv 1 \pmod{D}$$

by A3, A4, A5, A7 respectively. Next we get

(2) $$G \equiv A, \quad H \equiv C, \quad I \equiv D \pmod{F},$$

the first two congruences by A5, A1 respectively and then use them to obtain the third. Then both $F \perp D$ and $I \perp D$ by (1), and $I \perp F$ since $I \equiv D \pmod{F}$ and $F \perp D$. Hence D, F, and I are all squares so there are p, q, r such that

$$C = \psi_A(p), \quad D = \chi_A(p)^2,$$
$$E = \psi_A(q), \quad F = \chi_A(q)^2,$$
$$H = \psi_G(r), \quad I = \chi_G(r)^2.$$

Now G was chosen in such a way that $\psi_G(r)$ acts as a bridge between r and B on one hand and between r and p on the other, allowing us to conclude that $p = B$ and $C = \psi_A(B)$. Indeed, $G \equiv 1 \pmod{2C}$ by A3, A4, A5 so that $H = \psi_G(r) \equiv r \pmod{2C}$ by the congruence rule and $H \equiv B \pmod{2C}$ by A6 so

(3) $$r \equiv B \pmod{2C}.$$

On the other hand, $G \equiv A \pmod{F}$ by A5 so that $H = \psi_G(r) \equiv \psi_A(r) \pmod{F}$ by the congruence rule and $H \equiv C \pmod{F}$ by A1. Hence

(4) $$\psi_A(r) \equiv \psi_A(p) \pmod{\chi_A(q)}$$

since $C = \psi_A(p)$ and $F = \chi_A(q)^2$. Now $C^2 \mid \psi_A(q)$ by A3 so by the first step-down lemma, $C \mid q$. Hence by (4) and the second step-down lemma,

(5) $$r \equiv \pm p \pmod{2C}.$$

By (3) and (5), we have $B \equiv \pm p \pmod{2C}$. Also $B \leqslant C$ by A1 and $p \leqslant \psi_A(p) = C$ so $B = p$ and $\psi_A(B) = C$ as required.

We still need to show that if $\psi_A(B) = C$ and $A > 1, B > 0, C > 0$ then we can choose natural numbers i, j and integers $D, \ldots, I$ satisfying $\mathscr{A}$. Put $D = \chi_A(B)^2$, then D will satisfy A2. Choose $q > 0$ so that $2D(e+1)C^2 \mid \psi_A(q)$. This is possible since $D > 0$, $C > 0$, and we can always choose a solution ψ of a Pell equation to be a multiple of any positve integer (see Section 2). Put $E = \psi_A(q)$ and choose i satisfying A3. Let F and G be given by A4 and A5. Put $H = \psi_G(B)$. Since A2, ..., A5 have already been satisfied, $G \equiv 1 \pmod{2C}$. Hence $\psi_G(B) \equiv B \pmod{2C}$ and $\psi_G(B) \geqslant B$, so we can choose j satisfying A6. Let I be given by A7. Finally, D, F, and I are all squares by the hypothesis and the choice of E and H; $G \equiv A \pmod{F}$ so $H = \psi_G(B) \equiv \psi_A(B) \pmod{F}$; and $B \leqslant C$. Hence A1 is satisfied and the theorem is proved.

COROLLARY. *There is a polynomial Z such that if $A > 1$, $B > 0$, $C > 0$ then $\psi_A(B) = C$ if and only if there are i, j, and k such that $Z(A, B, C, i, j, k) = 0$.*

Proof. Take Z to be the polynomial obtained from

$$M_1(DFI, F, H-C, C-B+1, k)$$

by putting $e=0$ and eliminating $D, \ldots, I$ by A2, ..., A7. Here M_1 is the polynomial satisfying the Relation-combining Theorem for one square condition. Since $F>0$ by A4 and the hypothesis, we can apply the Relation-combining Theorem to see that $Z=0$ has a solution if and only if $\mathscr{A}$ can be satisfied. Hence the corollary follows from the theorem.

4. The exponential function. In this section, we will show that the relation $y=x^n$ can be defined by a diophantine equation in 5 unknowns. We do not use the exponential function in Part II but it seems worthwhile to give the definition — both as an introduction to Section 10 and for its own sake.

Consider the case $x>0$ and $n>0$. The bounds on ψ given in Section 2 yield

$$\psi_A(B) \sim (2A)^{B-1} \quad \text{as} \quad A\to\infty.$$

Hence

$$\frac{\psi_{Mx}(n+1)}{\psi_M(n+1)} \to x^n \quad \text{as} \quad M\to\infty. \tag{1}$$

Let

$$\varrho = \frac{\psi_{Mx}(n+1)}{\psi_M(n+1)}. \tag{2}$$

We wish to find a lower bound M_0 such that for $M>M_0$,

$$\langle \varrho \rangle = x^n. \tag{3}$$

To make the necessary estimates, we will use the elementary inequalities

(i) $$(1-\alpha)^q \geqslant 1-q\alpha > 0 \quad \text{for} \quad 0\leqslant \alpha < 1/q;$$

(ii) $$(1-\alpha)^{-1} \leqslant 1+2\alpha \quad \text{for} \quad 0\leqslant \alpha \leqslant \tfrac{1}{2}.$$

Then for $M\geqslant n$,

$$\varrho \leqslant \frac{(2Mx)^n}{(2M-1)^n} = x^n\left(1-\frac{1}{2M}\right)^{-n} \leqslant x^n\left(1-\frac{n}{2M}\right)^{-1} \leqslant x^n\left(1+\frac{n}{M}\right) \tag{4}$$

and

$$\varrho \geqslant \frac{(2Mx-1)^n}{(2M)^n} = x^n\left(1-\frac{1}{2Mx}\right)^n \geqslant x^n\left(1-\frac{n}{2Mx}\right). \tag{5}$$

Hence if M is so large that

$$\frac{nx^n}{M} < \frac{1}{2}, \tag{6}$$

then $|x^n-\varrho| < \frac{1}{2}$ and $\langle\varrho\rangle = x^n$. Also if $M>n$, then

$$\varrho > \tfrac{1}{2}x^n \tag{7}$$

by (5). If $y=\langle\varrho\rangle$, that is

$$(\varrho-y)^2 < \tfrac{1}{4}, \tag{8}$$

then $y=x^n$ provided $M>4n(y+1)$.

We have used two terms of Lucas sequences in obtaining y. This would lead to a definition of exponentiation with nine unknowns. Next we will show that only one term of a Lucas sequence is necessary.

Let $\mathscr{E}$ be the following system:

E0 $C=\psi_A(B)$,
E1 $(M^2-1)L^2+1=\square$,
E2 $\left(\frac{C}{L}-y\right)^2 < \frac{1}{4}$, $xyn>0$,
(or $\left(L^2-4(C-Ly)^2\right)xyn>0$ since $L>0$ by E3, E4),
E3 $M=4n(y+1)+x+2$,
E4 $L=n+1+l(M-1)$,
E5 $A=Mx$,
E6 $B=n+1$,
E7 $C=k+B$.

The parameters of $\mathscr{E}$ are x, y, n and the variables are k, l, M, L, A, B, C.

LEMMA. *$x>0$, $n>0$, and $y=x^n$ if and only if $\mathscr{E}$ can be satisfied.* [E2, E3, E5, E6, *and* E7 *imply* $A>1$, $B>0$, $C>0$.]

Remark. We repeat for emphasis one remark after Theorem 4. Whether $\mathscr{E}$ can be satisfied depends on the values of the parameters x, y, n and our assertion is that $\mathscr{E}$ can be satisfied exactly when $y=x^n$ and x, y, n are all positive. The values of the unknowns k, l must be natural numbers while those of M, L, A, B, C must be integers. Furthermore we could use E3, ..., E7 to eliminate M, L, A, B, C in turn and obtain a system with the same parameters and with only two variables k and l.

Proof. Suppose E0, ..., E7 hold. E2 implies $x>0$, $y>0$, and $n>0$. Also $L>0$ by E3 and E4 so there is an integer L' such that

$$L = \psi_M\left(n+1+L'(M-1)\right)$$

by E1, E4, and the congruence rule. Also $L'\geqslant 0$ since $M-1>n+1$ by E3. We will first show that $L'=0$ by contradiction. For $L'>0$,

$$\frac{\psi_{Mx}(n+1)}{\psi_M\left(n+1+L'(M-1)\right)} \leqslant \frac{\psi_{Mx}(n+1)}{\psi_M(n+1+M-1)} \leqslant \frac{(2Mx)^n}{(2M-1)^{M+n-1}}$$
$$= \frac{(2M)^n}{\left(4M(M-1)+1\right)^n}\cdot\frac{x^n}{(2M-1)^{M-2n-1}} < \frac{1}{2}$$

provided $2M-1>x$ and $M>2n+1$. Both of these conditions on M follow from E3. Here we used the fact that $n>0$ so $(2M-1)^{2n}>2\cdot(2M)^n$. Thus if $L'>0$ then $y=0$ by the first part of E2 contradicting the second part. Hence $L'=0$ and $L=\psi_M(n+1)$. Then by E2, $y=\langle\varrho\rangle$ which is x^n by the argument above.

On the other hand, suppose $y=x^n$, $x>0$, and $n>0$. Then we will show that $\mathscr{E}$ can be satisfied. Let M, A, B, C be given by E3, E5, E6, E0. Then $B\leqslant C$ (see Section 2) so we can choose k satisfying E7. Let $L=\psi_M(n+1)$ then E1 holds and $L\equiv n+1 \pmod{M-1}$ by the congruence rule. Also $n+1<M-1$ so we can choose l satisfying E4. Finally, E2 holds since $y=x^n=\langle\varrho\rangle$ by the argument above.

Next we eliminate ψ from $\mathscr{E}$. Let $\mathscr{F}$ be the system consisting of $E1, \ldots, E7$, A1, ..., A7. The parameters of $\mathscr{F}$ are x, y, n and the variables are $i, j, k, l, A, B, C, D, E, F, G, H, I, L, M$. We have put $e=0$ for this application of Theorem 4.

LEMMA. *$x>0$, $n>0$, and $y=x^n$ if and only if $\mathscr{F}$ can be satisfied.*

Proof. Suppose $\mathscr{F}$ is satisfied. Then $A>1$, $B>0$, $C>0$ by the preceding lemma. Hence by Theorem 4, E0 holds and $y=x^n$, $x>0$, and $n>0$. On the other hand, suppose $y=x^n$, $x>0$, and $n>0$. Notice that the sets of unknowns in $\mathscr{A}$ and $\mathscr{E}$ are disjoint. We can choose k, l, M, L, A, B, C so that $\mathscr{E}$ is satisfied. Then $C=\psi_A(B)$ by E0 and $A>1$, $B>0$, $C>0$ by the first lemma. Hence by Theorem 4, we can choose i, j, D, E, F, G, H, I so that $\mathscr{A}$ is satisfied. Therefore $\mathscr{F}$ can be satisfied.

Notice that the condition $B\leqslant C$ in A1 is implied by E7 and hence can be dropped from $\mathscr{F}$. Thus $\mathscr{F}$ consists of two square conditions $DFI=\square$ and $(M^2-1)L^2+1=\square$; one divisibility condition $F\mid H-C$; one inequality $xyn\left(L^2-4(C-Ly)^2\right)>0$; and 11 equations. Hence we are in position to use the Relation-combining Theorem to obtain our final result.

THEOREM 5. *There is a polynomial Z with integer coefficients such that $y=x^n$ if and only if $Z(x, y, n, i, j, k, l, m)=0$ for some natural numbers i, j, k, l, m.*

Proof. Let $Z_1(x, y, n, i, j, k, l, m)$ be the polynomial obtained from

$$M_2\left(DFI, (M^2-1)L^2+1, F, H-C, xyn\left(L^2-4(C-Ly)^2\right), m\right)$$

by putting $e=0$ and eliminating $M, L, A, B, C, D, E, F, G, H, I$ in order according to E3, ..., E7, A2, ..., A7. Here M_2 is the polynomial constructed after the proof of the Relation-combining Theorem in Section 1. So $Z_1=0$ for some i, j, k, l, m if and only if $\mathscr{F}$ can be satisfied. Therefore $Z_1=0$ can be satisfied if and only if $y=x^n$, $x>0$, and $n>0$. Finally, let

$$Z(x, y, n, i, j, k, l, m)=Z_1\cdot\left(n+(y-1)^2\right)\cdot\left(x+y+(n-1-k)^2\right).$$

Then $Z=0$ if and only if $x>0$, $n>0$, $y=x^n$; or $n=0$ and $y=1$; or $x=0$, $y=0$, and $n>0$. Hence Z satisfies the theorem.

PART II

Reduction to 13 unknowns

5. The code. The first step in our reduction of an arbitrary diophantine equation with unknowns $z_0, \ldots, z_\nu$ to one with 13 unknowns is to put a movable ceiling on the size of a solution. Thus, $P(z_0, \ldots, z_\nu)=0$ has a solution if and only if it has a solution with $z_i\leqslant b$ for some b. This permits us to code $z_0, \ldots, z_\nu$ as digits in the $(b+1)$-ary expansion of a single number. However we will need more flexibility so we let $a_0, \ldots, a_\nu$ be particular positive integers with

$$0<a_0<\ldots<a_\nu \tag{1}$$

and choose B so that $B\geqslant b+1$. A number whose B-ary expansion has the form

$$1+\sum_{i=0}^{\nu}u_iB^{a_i} \tag{2}$$

with $u_i\leqslant b$ will be called a *code with bound b*.

Every integer has a unique *symmetric* expansion in powers of an odd number $B=2u+1>1$ with integer coefficients whose absolute values are $\leqslant u$. Now it turns out that for a suitable choice for the a's there are particular numbers β and λ together with a polynomial A such that if c is the code with bound b corresponding to $u_0, \ldots, u_\nu$ then $\lambda P(u_0, \ldots, u_\nu)$ is the coefficient of B^β in the symmetric B-ary expansion of $A(B, c)$. Thus, $P(z_0, \ldots, z_\nu)=0$ has a solution if and only if there is a bound b and a code c with bound b such that the coefficient of B^β in the symmetric expansion of $A(B, c)$ is 0. This means that we can deal with just b and c no matter how many unknowns the original equation has.

The first problem is to express the condition that c is a code with bound b without referring to the digits of c. Let $c=c_0+c_1B+\ldots+c_\varrho B^\varrho$ be the usual B-ary expansion of c. Then

$$\operatorname{Rem}(c, B^i)=c_0+c_1B+\ldots+c_{i-1}B^{i-1}.$$

It is easy to give conditions on these partial sums for c to be a code with bound b. We give here redundant conditions in order to make the next step of the proof more direct. Namely, let

$$\begin{aligned}
&C_0 \quad 0<\operatorname{Rem}(c, B^{a_0})<2,\\
&C_i \quad 0<\operatorname{Rem}(c, B^{a_i})<(b+1)B^{a_{i-1}},\ i=1, \ldots, \nu,\\
&C_{\nu+1} \quad 0<c<(b+1)B^{a_\nu},
\end{aligned}$$

then $C_0, \ldots, C_{\nu+1}$ hold if and only if c is a code with bound b. Here C_0 implies $c_0=1$ since $a_0>0$. For $i\leqslant\nu$, C_i insures that the expansion has

the proper gap before B^{a_i} while C_{i+1} insures that the coefficient of B^{a_i} is $\leqslant b$. Conversely, if c is a code with bound b, then $C_0, \ldots, C_{\nu+1}$ hold.

From $C_0, \ldots, C_{\nu+1}$, we obtain another characterization of codes: c is a code with bound b if and only if there is an integer in each of the open intervals

$$I_0 = \left(\frac{c-2}{B^{a_0}}, \frac{c}{B^{a_0}}\right),$$

$$*(3) \qquad I_i = \left(\frac{c-(b+1)B^{a_i-1}}{B^{a_i}}, \frac{c}{B^{a_i}}\right), \quad i = 1, \ldots, \nu,$$

$$I_{\nu+1} = \left(\frac{c-(b+1)B^{a_\nu}}{(c+1)B^{a_\nu+1}}, \frac{c}{(c+1)B^{a_\nu+1}}\right).$$

The proof of the equivalence with $C_0, \ldots, C_{\nu+1}$ is immediate. In fact, C_i if and only if there is an integer in I_i, is clear for $i = 0, \ldots, \nu$. Also since $I_{\nu+1}$ is included in $(-1, +1)$, the only possible integer in $I_{\nu+1}$ is 0. Hence there is an integer in $I_{\nu+1}$ if and only if $C_{\nu+1}$.

Next we need to express the condition that the coefficient of B^β is 0 in the symmetric expansion of an integer A where $B = 2u+1 > 1$. If the coefficient of B^β is 0, then there is an integer T such that

$$|A - TB^{\beta+1}| \leqslant u(1+B+\ldots+B^{\beta-1}),$$

i.e.

$$(4) \qquad |A - TB^{\beta+1}| < \tfrac{1}{2}B^\beta.$$

On the other hand, the symmetric expansion of X for $|X| < \frac{1}{2}B^\beta$ contains only powers of B less than B^β. We can see this since there are B^β numbers with such representations and B^β values of X satisfying $|X| < \frac{1}{2}B^\beta$. Hence (4) is also a sufficient condition. Therefore the coefficient of B^β is 0 in the symmetric expansion of A if and only if there is an integer in the open interval

$$*(5) \qquad I_{\nu+2} = \left(\frac{2A - B^\beta}{2B^{\beta+1}}, \frac{2A + B^\beta}{2B^{\beta+1}}\right).$$

6. Diophantine equation with coded unknowns. We now return to the given equation $P(z_0, \ldots, z_\nu) = 0$. We will apply the results of the last section to find conditions on b and c so that c will be the code with bound b of a solution of $P = 0$. Without loss of generality we may assume that P contains some unknowns. Let

$$*(1) \qquad \delta = \text{degree of } P \text{ in } z_0, \ldots, z_\nu.$$

Thus δ is greater than 0. Let

$$*(2) \qquad a_i = (\delta+1)^i, \quad i = 0, \ldots, \nu.$$

The a's are strictly increasing positive integers as required in the last section. Put

$$(3) \qquad C = 1 + \sum_{i=0}^{\nu} z_i B^{(\delta+1)^i}.$$

Then

$$(4) \qquad C^\delta = \sum\nolimits^* c_{i_0 \ldots i_\nu} z_0^{i_0} \ldots z_\nu^{i_\nu} B^{i_0 + i_1(\delta+1) + \ldots + i_\nu(\delta+1)^\nu}$$

where the summation extends over all natural numbers $i_0, \ldots, i_\nu$ with $i_0 + \ldots + i_\nu \leqslant \delta$ and

$$*(5) \qquad c_{i_0 \ldots i_\nu} = \frac{\delta!}{i_0! i_1! \ldots i_\nu! (\delta - i_0 - i_1 - \ldots - i_\nu)!}.$$

We will continue to use $\sum^*$ to indicate a sum with this range. The exponent of B corresponding to $i_0, \ldots, i_\nu$ is $i_\nu i_{\nu-1} \ldots i_0$ written to the base $\delta+1$. Hence each power of B in the sum comes in exactly once, with the largest exponent being $\delta(\delta+1)^\nu$. Furthermore since all the multinomial coefficients divide $\delta!$, there are $P_{i_0 \ldots i_\nu}$ so that

$$*(6) \qquad \delta! P(z_0, \ldots, z_\nu) = \sum\nolimits^* P_{i_0 \ldots i_\nu} c_{i_0 \ldots i_\nu} z_0^{i_0} \ldots z_\nu^{i_\nu}.$$

Here $P_{i_0 \ldots i_\nu}$ are integer multiples of the original coefficients of P.

Now define

$$(7) \qquad A(B, C) = C^\delta D(B)$$

where

$$*(8) \qquad D(B) = B^{(\delta+1)^\nu+2} + \sum\nolimits^* P_{i_0 \ldots i_\nu} B^{(\delta+1)^\nu+1 - i_0 - \ldots - i_\nu(\delta+1)^\nu}.$$

If

$$(9) \qquad B \geqslant 1 + \sum\nolimits^* P_{i_0 \ldots i_\nu}^2,$$

then the absolute value of $\sum^*$ in (8) is less than $B^{(\delta+1)^\nu+1+1}$ so

$$D(B) > 0.$$

Using (4) to eliminate C from (7), we obtain an expansion of A in powers of B with coefficients which are polynomials in $z_0, \ldots, z_\nu$ and which may be positive or negative. Thus, let

$$(10) \qquad A(B, C) = \sum_{j=0}^{(\delta+1)^\nu+2+\delta(\delta+1)^\nu} A_j(z_0, \ldots, z_\nu) B^j.$$

We could write out A_j explicitly given P but this will not be necessary. However we will use the fact that

$$(11) \qquad A_{(\delta+1)^\nu+1}(z_0, \ldots, z_\nu) = \delta! P(z_0, \ldots, z_\nu).$$

This follows by direct calculation from (4), ..., (10).

We will also need a bound on the absolute value of A_j under the restriction that all the z's are $\leqslant b$. It is easily checked that

$$|A_j(z_0, \ldots, z_\nu)| \leqslant \delta!(1+b^\delta)\left(1+\sum\nolimits^{*} P^2_{i_0 \ldots i_\nu}\right)$$

for $z_0, \ldots, z_\nu \leqslant b$, using (4) and (8).

We are now ready to go from the algebraic identity (10) to the symmetric B-ary expansion of A provided B is sufficiently large and odd. Let

$$*(12) \qquad B = 2\delta!(1+b^\delta)\left(1+\sum\nolimits^{*} P^2_{i_0 \ldots i_\nu}\right)+1$$

and c be a code with bound b. Since (9) holds, $D(B) > 0$. Suppose c is a code for $u_0, \ldots, u_\nu$. Then the digits in the symmetric B-ary expansion of $A(B, c)$ are $A_j(u_0, \ldots, u_\nu)$. Indeed, $A_j(z_0, \ldots, z_\nu)$ is the coefficient of B^j in the algebraic expansion of $A(B, C)$ when C has the algebraic form of a code for $z_0, \ldots, z_\nu$. Hence there is an expansion of $A(B, c)$ into powers of B with $A_j(u_0, \ldots, u_\nu)$ as coefficients. Also B is so large that

$$|A_j(u_0, \ldots, u_\nu)| < B/2$$

and hence the $A_j(u_0, \ldots, u_\nu)$ are the coefficients in the symmetric B-ary expansion of $A(B, c)$. Therefore by (11), we have shown that $P(z_0, \ldots, z_\nu) = 0$ has a solution if and only if there is a bound b and a code c with bound b so that the coefficient of $B^{(\delta+1)^{\nu+1}}$ in the symmetric B-ary expansion of $A(B, c)$ is 0.

Using the results of the last section, we see that $P(z_0, \ldots, z_\nu) = 0$ has a solution if and only if there is an integer (or natural number) in each of the intervals $I_0, \ldots, I_{\nu+2}$ where

$$*(13) \qquad \beta = (\delta+1)^{\nu+1},$$

$$*(14) \qquad A = A(B, c) = c^\delta D(B),$$

a_i are given by (2), B by (12), and $D(B)$ by (8). (An integer in an open interval of length $\leqslant 1$ with right end-point $\geqslant 0$ is necessarily a natural number.) Note that B and $D(B)$ are polynomials in b with coefficients which are polynomials in the coefficients of $P(z_0, \ldots, z_\nu)$. Also at this point, we are using $\nu+5$ unknowns to express the solvability of $P = 0$. Namely, b and c in the end-points of the intervals together with $t_0, \ldots, t_{\nu+2}$ which are used for the natural number in the corresponding interval, i.e. $t_i \epsilon I_i$.

Now let

$$*(15) \qquad I_i = \left(\frac{E_i(b, c)}{G_i(b, c)}, \frac{F_i(b, c)}{G_i(b, c)}\right) \quad \text{for} \quad i = 0, \ldots, \nu+2;$$

where E_i, F_i, G_i are polynomials determined by I_i according to the definition in Section 5. Thus, $P(z_0, \ldots, z_\nu) = 0$ has a solution if and only if there are $b, c, t_0, \ldots, t_{\nu+2}$ such that

$$(16) \qquad E_i(b, c) < t_i G_i(b, c) < F_i(b, c) \quad \text{for} \quad i = 0, \ldots, \nu+2.$$

Remark. Since every I_i is of length $\leqslant 1$, we can transform this system of inequalities into a system of equation in two unknowns by using the greatest integer function. Namely, $P(z_0, \ldots, z_\nu) = 0$ has a solution if and only if there are b and c such that

$$\left[\frac{E_i(b, c)}{G_i(b, c)} + 1\right] = \left[\frac{F_i(b, c)-1}{G_i(b, c)}\right] \quad \text{for} \quad i = 0, \ldots, \nu+2.$$

7. Reduction to the positiveness of a polynomial. We say a polynomial in one variable t is *positive* if it is positive for all natural numbers t. In this section, we will show that the condition that each of the intervals I_i contains a natural number is equivalent to a particular polynomial Q being positive.

Consider an open interval (σ, τ) where σ and τ are real numbers such that $0 < \tau - \sigma \leqslant 1$. There is an integer in (σ, τ) if and only if there is no integer in the closed $[\tau, \sigma+1]$, (i.e. each integer is on the same side of τ as of $\sigma+1$). Hence there is an integer in (σ, τ) if and only if

$$(T-\tau)(T-\sigma-1) > 0$$

for all integers T. In fact, there can be at most one value of T for which $(T-\tau)(T-\sigma-1) \leqslant 0$. Namely, T equal to the integer in $[\tau, \sigma+1]$ if there is one. Now suppose there is another interval (σ', τ') with $0 < \tau' - \sigma' \leqslant 1$ such that $[\tau, \sigma+1]$ and $[\tau', \sigma'+1]$ are disjoint. The two closed intervals cannot contain the same integer. Hence there are integers in both (σ, τ) and (σ', τ') if and only if

$$(T-\tau)(T-\sigma-1)(T-\tau')(T-\sigma'-1) > 0$$

for all integers T, since $(T-\tau)(T-\sigma-1)$ and $(T-\tau')(T-\sigma'-1)$ are never simultaneously $\leqslant 0$.

Now suppose we have ϱ intervals (σ_i, τ_i) where $0 \leqslant \tau_i$ and $0 < \tau_i - \sigma_i \leqslant 1$ for $i = 0, \ldots, \varrho-1$. We can construct new intervals (σ_i', τ_i') so that the corresponding complementary closed intervals are disjoint by translating the intervals to the right, integral distances. Choose an integer W so that $\sigma_i + 1 < W$ for $i = 0, \ldots, \varrho-2$ and let

$$(1) \qquad \sigma_i' = \sigma_i + iW, \quad \tau_i' = \tau_i + iW.$$

Then $[\tau_i', \sigma_i'+1]$ is to the left of $[\tau_{i+1}', \sigma_{i+1}'+1]$ since

$$\sigma_i' + 1 = \sigma_i + iW + 1 < (i+1)W \leqslant \tau_i + (i+1)W = \tau_{i+1}'.$$

Hence there is an integer in each of the intervals (σ_i, τ_i) if and only if

$$\prod_{i=0}^{e-1}(T-\tau_i')(T-\sigma_i'-1) > 0 \tag{2}$$

for all integers T. Since $\tau_i \geqslant 0$ and the lengths of all the (open) intervals are $\leqslant 1$, an integer in (σ_i, τ_i) is necessarily $\geqslant 0$. Also (2) holds for all negative integers T since both τ_i' and $\sigma_i'+1$ are $\geqslant 0$. Hence there is a natural number in each of the intervals (σ_i, τ_i) if and only if

$$\prod_{i=0}^{e-1}(t-\tau_i')(t-\sigma_i'-1) > 0 \tag{3}$$

for all natural numbers t.

We now return to the intervals $I_0, \ldots, I_{\nu+2}$ defined in Section 6. If we put $I_i = (\sigma_i, \tau_i)$ then $0 \leqslant \tau_i$ and $0 < \tau_i - \sigma_i \leqslant 1$. Hence for W sufficiently large, there is a natural number in each of the intervals I_i if and only if

$$\prod_{i=0}^{\nu+2}\left(t-\frac{F_i}{G_i}-iW\right)\left(t-\frac{E_i}{G_i}-iW-1\right) > 0 \quad \text{for all } t.$$

Now we may take $W = e+1$ since $\sigma_i < \tau_i \leqslant e$ for $i = 0, \ldots, \nu+1$. (No restriction is needed for $i = \nu+2$.) Let

$$*(4) \qquad Q(b, c, t) = \prod_{i=0}^{\nu+2}\left((t-ic-i)G_i-F_i\right)\left((t-ic-i-1)G_i-E_i\right).$$

We have shown that $P(z_0, \ldots, z_\nu) = 0$ for some $z_0, \ldots, z_\nu$ if and only if there are b and c such that $Q(b, c, t) > 0$ for all t. The unknowns b and c are the first two of the promised 13. They can be considered as parameters in what follows so we shall write $Q(t)$ instead of $Q(b, c, t)$. It remains to find a polynomial $\bar{Q}$ in 11 variables and the same parameters as Q (that is $a_1, \ldots, a_\mu, b, c$) such that $Q(t) > 0$ for all t if and only if $\bar{Q}(t_1, \ldots, t_{11}) = 0$ for some $t_1, \ldots, t_{11}$. In constructing $\bar{Q}$ from Q, we shall use the fact that for all b and c, the leading coefficient of $Q(t)$ is greater than 0.

8. Reduction to binomial coefficients. We wish to derive a necessary and sufficient condition that $Q(t) > 0$ for all natural numbers t. Binomial coefficients will come in quite naturally.

Let

$$**(1) \qquad Q(t) = Q_0 + Q_1 t + \ldots + Q_\nu t^\nu, \quad Q_\nu > 0,$$

$$R = 1 + \sum_{i=0}^{\nu} Q_i^2, \quad S = R^{\nu+1}, \quad T = RS^\nu. \tag{2}$$

Then the real roots of $Q(t) = 0$ are less than R (see Section 1). If $Q(t) \leqslant 0$ then $t < R$; if $t < R$ then $|Q(t)| < S$; if $t < S$ then $|Q(t)| < T$.

Suppose

$$d \equiv u \,|\, Q(d) + v \quad \text{for some } u, v < S. \tag{3}$$

Then

$$d \equiv u \,|\, Q(u) + v, \tag{4}$$

since $d - u \,|\, Q(d) - Q(u)$. Obviously for sufficiently large d, (4) can only hold if $Q(u) + v = 0$. Indeed, if $d > 2S + T$ then $Q(u) = -v$. Conversely, if $Q(u) = -v$ then (3) holds.

Thus for $d > 2S + T$, we have shown that $Q(u) \neq -v$ if and only if $d - u \nmid Q(d) + v$. Now we would like to combine the S^2 conditions

$$d - u \nmid Q(d) + v \quad \text{for} \quad u, v < S, \tag{5}$$

into one diophantine condition. We are unable to do this directly but the following theorem will be adequate for our purpose.

THEOREM 6. (A). *If $Q(t) > 0$ for all t and $S!(S+T)! \,|\, d+1$, then*

$$\binom{d}{S} \perp \binom{Q(d)+S-1}{S}. \tag{6}$$

(B). *If $d > S!^2 + S$ and*

$$\binom{d}{S} \Big/ \left(\binom{d}{S}, S!\right) \perp \binom{Q(d)+S-1}{S}, \tag{7}$$

then $Q(t) > 0$ for all t.

Remark. It will be clear in the next section why we need this unsymmetrical form of the theorem. We can combine the two parts to obtain as a corollary:

A necessary and sufficient condition for Q to be a positive polynomial is that

$$\binom{S!(S+T)!-1}{S} \perp \binom{Q(S!(S+T)!-1)+S-1}{S}$$

where S and T are defined by (1) *and* (2).

However we will need the theorem itself in order to make further reductions.

LEMMA. *If $S!(S+T)! \,|\, d+1$ and p is a prime which divides $\binom{d}{S}$, then $p > S+T$.*

Proof. Notice that

$$\binom{d}{S} = \left(\frac{d+1}{1}-1\right)\left(\frac{d+1}{2}-1\right)\ldots\left(\frac{d+1}{S}-1\right)$$

where the factors are all integers. Also

$$(S+T)!\,\Big|\,\frac{d+1}{u+1} \quad \text{for} \quad u<S.$$

Hence a prime divisor of $\binom{d}{S}$ must be greater than $S+T$.

Proof of (A). Suppose Q is a positive polynomial and $S!(S+T)!\,|\,d+1$. If a prime p divides $\binom{d}{S}$ then there is a u less than S such that $p\,|\,d-u$ so $p\,|\,Q(d)-Q(u)$. Now if $p\,|\,Q(d)+v$ for some v less than S then $p\,|\,Q(u)+v$. This is impossible by the lemma since $p>S+T$ and $0<Q(u)+v<S+T$. Hence $p\nmid\binom{Q(d)+S-1}{S}$.

Proof of (B). We shall suppose that $d>S!^2+S$ and $Q(u)=-v$ for some natural numbers u and v, and show that (7) cannot hold. Then

$$d-u\,|\,Q(d)+v$$

and $u, v<S$ by the choice of S. Hence

$$\frac{d-u}{(d-u,\,S!)}\,\Big|\,\binom{Q(d)+S-1}{S}. \tag{8}$$

Also

$$\frac{d-u}{(d-u,\,S!^2)}\,\Big|\,\frac{\binom{d}{S}}{\left(\binom{d}{S},\,S!\right)} \tag{9}$$

and the left side is greater than 1 by hypothesis. Hence the right sides of (8) and (9) have a common factor greater than 1 which contradicts (7).

In the following section, we will let $Z=Q(d)+S-1$. Note that Z is a polynomial in $a_1, \ldots, a_\mu, b, c,$ and d.

9. Reduction to a partial binomial expansion. For $n>0$, $s>0$, and $x>n^s$,

$$\left[\frac{(x+1)^n}{x^s}\right]=\sum_{i=0}^{n-s}\binom{n}{s+i}x^i \tag{1}$$

and

$$\operatorname{Rem}\left(\left[\frac{(x+1)^n}{x^s}\right],\,x\right)=\binom{n}{s}. \tag{2}$$

To check this, write out the binomial expansion of $(x+1)^n$,

$$1+\ldots+\binom{n}{s-1}x^{s-1}+\binom{n}{s}x^s+\binom{n}{s+1}x^{s+1}+\ldots+x^n.$$

Since $x>n^s$, the first s terms have coefficients $\leqslant x-1$. Hence their sum is less than x^s and (1) holds. Then (2) is an immediate consequence since $x>\binom{n}{s}$. (We call the left side of (1) a *partial binomial expansion.*)

Using (1) and (2), we will see that the conditions given in Theorem 6 can be replaced by a combination of divisibility and square conditions together with one relation of the form

$$Y=\left[\frac{(X+1)^N}{X^S}\right] \tag{3}$$

where S is defined in Section 8.

One tool which we use is the simple observation: If $a\equiv b\pmod d$ then

$$\binom{a}{c}\equiv\binom{b}{c}\bmod\left(\frac{d}{(d,\,c!)}\right). \tag{4}$$

This follows since

$$a(a-1)\ldots(a-c+1)\equiv b(b-1)\ldots(b-c+1)\pmod d$$

and we can divide both sides of the congruence by $c!$, provided we divide the modulus by $(d, c!)$.

In Theorem 6, both $\binom{d}{S}$ and $\binom{Z}{S}$ come in. We can avoid defining both binomial coefficients (or the corresponding partial binomial expansions) from scratch, by using (3) where N is sufficiently large and X is divisible by both $N-d$ and $N-Z$. Then by (2) and (4), we have

$$Y\equiv\binom{N}{S}\pmod X,$$

$$Y\equiv\binom{N}{S}\equiv\binom{d}{S}\bmod\left(\frac{N-d}{(N-d,\,S!)}\right),$$

$$Y\equiv\binom{N}{S}\equiv\binom{Z}{S}\bmod\left(\frac{N-Z}{(N-Z,\,S!)}\right).$$

By imposing other conditions on X, Y, and N, we will obtain a definition of $\binom{d}{S}$ and show that

$$Y\equiv\binom{Z}{S}\bmod\left(\frac{\binom{d}{S}}{\left(\binom{d}{S},\,S!\right)}\right)$$

and

$$\binom{d}{S}\perp Y$$

which is sufficient to apply Theorem 6.

Let $\mathscr{S}$ be the following system:

S0 $Y = \left[\dfrac{(X+1)^N}{X^S}\right]$,

S1 $U(2S, d) = \square$,

S2 $V\big(d(e+1)S, f, d\big) = \square$,

S3 $V(N+S, g, e) = \square$,

S4 $e+1 \mid gY+1$,

**S5 $S = (1+\sum_{i=0}^{\gamma} Q_i^2)^{\gamma+1}$,

**S6 $Z = \sum_{i=0}^{\gamma} Q_i d^i + S - 1$,

**S7 $N = Z + (e+1)f$,

**S8 $X = g(N-d)(N-Z)$,

**S9 $Y = e+1+h(N-d)$.

The parameters of $\mathscr{S}$ are $Q_0, \ldots, Q_\gamma$ and the unknowns are $d, e, f, g, h, S, Z, N, X, Y$. Here U and V are the polynomial functions given in the lemmas on exponential size (see Section 2).

THEOREM 7. *Suppose* $Q(t) = Q_0 + Q_1 t + \ldots + Q_\gamma t^\gamma$, $\gamma > 0$, *and* $Q_\gamma > 0$. *Then* $Q(t) > 0$ *for all* t *if and only if* $\mathscr{S}$ *is satisfied for some* $d, e, f, g, h, S, Z, N, X, Y$. [*Also* S1, ..., S9 *imply that* $Y > 0$, $X > 4N^S$, $N \geqslant S > 0$.]

Remark. We could eliminate the unknowns S, Z, N, X, Y by means of S5, ..., S9. For the purpose of this section, it would be sufficient for $X > N^S$ but later we will need $X > 4N^S$.

Proof. Suppose $\mathscr{S}$ is satisfied. Then we will show that

$$d > S!^2 + S \tag{5}$$

and

$$\frac{\binom{d}{S}}{\left(\binom{d}{S}, S!\right)} \perp \binom{Z}{S}. \tag{6}$$

Hence by part (B) of Theorem 6, $Q(t) > 0$ for all t. Notice that S and Z are defined by S5 and S6 just as in Theorem 6. By S1, S2, S3, and the lemmas on exponential size, we obtain

$$d > (2S)^{2S} \geqslant S^{2S} + S \geqslant S!^2 + S, \tag{7}$$

$$f > \big(d(e+1)S\big)^{d(e+1)S} \geqslant \big(d(e+1)S\big)^{dS}, \tag{8}$$

$$g > (N+S)^{N+S}. \tag{9}$$

Now by (8), $f > 0$ and by (7), d is so large that $Q(d) > 0$ (see the last section). Hence

$$N > Z \geqslant S > 0 \tag{10}$$

by S7, S6, S5 respectively. Also by S7,

$$N > d \geqslant 2 \tag{11}$$

since $f > d$ by (8) and (10). Hence

$$X \geqslant g > N^{N+S} \geqslant 4N^S \tag{12}$$

by S8, (10), and (11). Thus the second part of the theorem holds. Now using the argument at the beginning of this section,

$$Y \equiv \binom{N}{S} \equiv \binom{d}{S} \bmod \left(\frac{N-d}{((N-d), S!)}\right) \tag{13}$$

by S0 and the fact that $N-d \mid X$ by S8. Also $Y \equiv e+1 \bmod (N-d)$ by S9, so

$$e+1 \equiv \binom{d}{S} \bmod \left(\frac{N-d}{(N-d, S!)}\right). \tag{14}$$

Now $N > d^S + d$ and $N > (e+1)S^S + d$ by (8) since $N > f$, $d \geqslant 2$, and $d^2 > 2d$. Hence

$$\frac{N-d}{S!} > \binom{d}{S}, \quad \frac{N-d}{S!} > e+1. \tag{15}$$

Therefore $e+1 = \binom{d}{S}$ by (14) and (15). Also $e+1 \mid N-Z$ by S7, so

$$Y \equiv \binom{N}{S} \equiv \binom{Z}{S} \bmod \left(\frac{e+1}{(e+1, S!)}\right).$$

Hence by S4,

$$\frac{e+1}{(e+1, S!)} \mid g\binom{Z}{S} + 1$$

so (6) holds as required. Hence if $\mathscr{S}$ is satisfied then Q is a positive polynomial.

On the other hand, suppose Q is a positive polynomial. Let S be given by S5 and put

$$T = \left(1 + \sum_{i=0}^{\gamma} Q_i^2\right)^{\gamma(\gamma+1)+1}$$

as in the preceding section. By the first lemma on exponential size, we choose d satisfying both

$$S!(S+T)! \mid d+1 \tag{16}$$

and S1. Let Z be given by S6 and put $e = \binom{d}{S} - 1$ so $e+1 \perp S!$ by the lemma of Section 8 since all primes dividing $\binom{d}{S}$ are greater than $S+T$. Also $e+1 \perp \binom{Z}{S}$ by part (A) of Theorem 6. Choose f satisfying both

$$Z + (e+1)f - d \equiv 1 \pmod{S!} \tag{17}$$

and S2. This is possible by the second lemma on exponential size and the facts that $S! \mid d+1$ and $e+1 \perp S!$. Let N be given by S7 then $N-d > 0$ and $N-Z > 0$, since $f > 0$ by S2 and $e+1 = \binom{d}{S} \geqslant d$. Also

$$N - d \perp S! \tag{18}$$

by (17). Choose g satisfying both

$$e+1 \mid g\binom{Z}{S} + 1 \tag{19}$$

and S3. This is possible by the second lemma on exponential size since $e+1 \perp \binom{Z}{S}$. Let X be given by S8. Then

$$X \geqslant g > (N+S)^{N+S} > 4N^S \tag{20}$$

by S3 since $N-d > 0$ and $N-Z > 0$. Let Y be given by S0. Then

$$Y \equiv \binom{N}{S} \equiv \binom{d}{S} = e+1 \bmod (N-d). \tag{21}$$

The first congruence holds by the argument at the beginning of this section since $X > N^S$ and $N-d \mid X$. The second congruence holds by (18). Also $Y \geqslant \binom{N}{S} > \binom{d}{S} = e+1$ since $N > d$. Hence we can determine h satisfying S9. Furthermore

$$Y \equiv \binom{N}{S} \equiv \binom{Z}{S} \bmod (e+1) \tag{22}$$

since $e+1 \perp S!$ and $e+1 \mid N-Z$ so $e+1 \mid X$. Hence by (19) and (22), S4 holds and the proof is completed.

Going back to the original equation, $P(z_0, \ldots, z_n) = 0$, we have shown that $P = 0$ has a solution if and only if there are b, c, d, e, f, g, h satisfying $\mathscr{S}$ where $Q(t)$ is $Q(b, c, t)$ defined in Section 7. (Here the unknowns S, Z, N, X, Y have been eliminated from $\mathscr{S}$ by means of S5, ..., S9.) S0 is the only condition not obviously diophantine. In the next section, we will give a diophantine definition of that relation.

10. Definition of a partial binomial expansion. The diophantine definition of $Y = [(X+1)^N / X^S]$ will be valid whenever $Y > 0$, $X > 4N^S$, and $N \geqslant S > 0$. The definition is parallel to that of $y = x^n$ in Section 4. Let

$$\sigma = \frac{\psi_{M(X+1)}(N+1)}{\psi_M(N-S+1)\,\psi_{MX}(S+1)}, \tag{1}$$

then by the bounds on ψ from Section 2,

$$\sigma \to \frac{(X+1)^N}{X^S} \quad \text{as} \quad M \to \infty. \tag{2}$$

We wish to find a lower bound M_0 for M so that for $M > M_0$,

$$\langle \sigma \rangle = \left[\frac{(X+1)^N}{X^S}\right] \quad \text{for} \quad X > 4N^S.$$

First we estimate the size of σ for $M \geqslant N$ using the inequalities (i) and (ii) of Section 4.

$$\sigma \leqslant \frac{(2M(X+1))^N}{(2M-1)^{N-S}(2MX-1)^S} \leqslant \frac{(X+1)^N}{X^S}\left(1 - \frac{1}{2M}\right)^{-N}$$
$$\leqslant \frac{(X+1)^N}{X^S}\left(1 - \frac{N}{2M}\right)^{-1} \leqslant \frac{(X+1)^N}{X^S}\left(1 + \frac{N}{M}\right)$$

and

$$\sigma \geqslant \frac{(2M(X+1)-1)^N}{(2M)^{N-S}(2MX)^S} = \frac{(X+1)^N}{X^S}\left(1 - \frac{1}{2M(X+1)}\right)^N$$
$$\geqslant \frac{(X+1)^N}{X^S}\left(1 - \frac{N}{2M(X+1)}\right).$$

Now if

$$|\varrho - \sigma| < \tfrac{1}{4} \quad \text{and} \quad \varrho - [\varrho] < \tfrac{1}{4}$$

then $\langle \sigma \rangle = [\varrho]$. For $M \geqslant N$,

$$\sigma \geqslant \frac{1}{2}\frac{(X+1)^N}{X^S}.$$

Let $Y = \langle \sigma \rangle$ so $Y+1 > \frac{1}{2}\frac{(X+1)^N}{X^S}$. Therefore, if $M > 8N(Y+1)$ then

$$\frac{(X+1)^N}{X^S} - \frac{1}{4} < \sigma < \frac{(X+1)^N}{X^S} + \frac{1}{4}.$$

Also

$$\frac{(X+1)^N}{X^S}-\left[\frac{(X+1)^N}{X^S}\right]=\sum_{i=0}^{S-1}\binom{N}{i}X^{i-S}\leqslant\frac{SN^{S-1}}{X}\leqslant\frac{N^S}{X}<\frac{1}{4}$$

provided $X>4N^S$. Hence $Y=[(X+1)^N/X^S]$.

In defining σ, we used three terms of Lucas sequences $\psi_{M(X+1)}(N+1)$, $\psi_M(N-S+1)$, and $\psi_{MX}(S+1)$. Just as in Section 4, we can define the last two in terms of the first.

Let $\mathscr{T}$ be the following system:

T0 $C=\psi_A(B)$,
T1 $(M^2-1)K^2+1=\square$,
T2 $(M^2X^2-1)L^2+1=\square$,
T3 $\left(\frac{C}{KL}-Y\right)^2<\frac{1}{4}$ (or $K^2L^2-4(C-KLY)^2>0$),
**T4 $M=8N(X+Y)+2$,
**T5 $K=N-S+1+k(M-1)$,
**T6 $L=S+1+l(MX-1)$,
**T7 $A=M(X+1)$,
**T8 $B=N+1$,
**T9 $C=m+B$.

The parameters of $\mathscr{T}$ are X, Y, N, S and the unknowns are $k, l, m, A, B, C, K, L, M$.

THEOREM 8. *Suppose $X>4N^S$, $Y>0$, and $N\geqslant S>0$. Then $Y=[(X+1)^N/X^S]$ if and only if $\mathscr{T}$ is satisfied for some $k, l, m, A, B, C, K, L, M$. [Also the hypothesis on X, Y, N, S together with* T4, T7, T8, T9 *implies that $A>1$, $B>0$, $C>0$.]*

Remark. We can eliminate the integer unknowns M, K, L, A, B, C in turn from $\mathscr{T}$ by T4, T5, T6, T7, T8, T9 so that $\mathscr{T}$ becomes a system with unknowns k, l, m. The equivalence of the two forms of T3 is clear since $K>0$, $L>0$ by T4, T5, T6, and the hypothesis.

Proof. The second part of the theorem is trivial. Suppose that T0, ..., T9 hold. We will show first that

$$K=\psi_M(N-S+1), \tag{3}$$

$$L=\psi_{MX}(S+1). \tag{4}$$

Notice that by T4,

$$M>8NX+2 \tag{5}$$

since $Y>0$. Also K and L are positive, $K\equiv N-S+1 \bmod (M-1)$, and $L\equiv S+1 \bmod (MX-1)$ by T5 and T6. Hence by T1, T2, and the congruence rule,

$$K=\psi_M\big(N-S+1+K'(M-1)\big),\qquad L=\psi_{MX}\big(S+1+L'(MX-1)\big)$$

for some integers K' and L'. Since $N-S+1<M-1$ and $S+1<MX-1$ by (5) both K' and L' are non-negative. We need to show that $K'=L'=0$. Now

$$\frac{\big(2M(X+1)\big)^N}{(2M-1)^{M-1}}=\frac{(2M)^N}{\big(4M(M-1)+1\big)^N}\cdot\frac{(X+1)^N}{(2M-1)^{M-2N-1}}<\frac{1}{2}$$

since $2M-1\geqslant X+1$ and $M-2N-1\geqslant N$. Hence both

$$\frac{\psi_{M(X+1)}(N+1)}{\psi_M(N-S+1+M-1)}<\frac{1}{2},\qquad\frac{\psi_{M(X+1)}(N+1)}{\psi_{MX}(S+1+MX-1)}<\frac{1}{2}$$

by the bounds on ψ in Section 2. Therefore, if either K' or L' were $\geqslant 1$ then T3, T0, T7, T8 would imply $Y=0$ contrary to hypothesis. Hence (3) and (4) have been proved so T3 implies $Y=\langle\sigma\rangle$. Then by T4, $M>8N(Y+1)$ so

$$Y=\left[\frac{(X+1)^N}{X^S}\right]$$

by the argument at the beginning of this section.

On the other hand, suppose $Y=[(X+1)^N/X^S]$, $X>4N^S$, $N\geqslant S>0$. We must show that there are natural numbers k, l, m and integers M, K, L, A, B, C so that T0, ..., T9 hold. Let M, A, B, C be given by T4, T7, T8, T0. Put $K=\psi_M(N-S+1)$ and $L=\psi_{MX}(S+1)$. Then T1 and T2 hold. Also there are k and l satisfying T5 and T6 by the congruence rule and the facts that $M-1>N-S+1$ and $MX-1>S+1$ which follow from the hypothesis and T4. Next choose m so that T9 holds which is possible since $\psi_A(B)\geqslant B$ for $A>0$. Finally, T3 holds since

$$0<\frac{(X+1)^N}{X^S}-Y<\frac{1}{4},\qquad\left|\frac{(X+1)^N}{X^S}-\frac{C}{KL}\right|<\frac{1}{4}.$$

11. Completion of the proof. Let $\mathscr{U}$ be the system consisting of A1, ..., A7, S1, ..., S9, T1, ..., T9. The parameters of $\mathscr{U}$ are $Q_0, \ldots, Q_\nu$ and the unknowns are $d, e, f, g, h, i, j, k, l, m, A, B, C, D, E, F, G, H, I, K, L, M, N, S, X, Y, Z$.

THEOREM 9. *Let $Q(t)=Q_0+Q_1t+\ldots+Q_\nu t^\nu$ and $Q_\nu>0$. Then $Q(t)>0$ for all t if and only if $\mathscr{U}$ can be satisfied.*

Proof. Suppose $\mathscr{U}$ is satisfied. Then $Y>0$, $X>4N^S$, $N\geqslant S>0$ by Theorem 7. Hence $A>1$, $B>0$, $C>0$ by Theorem 8. Hence by Theorem 4, T0 holds so by Theorem 8, S0 holds. Therefore Q is a positive polynomial by Theorem 7.

On the other hand, suppose Q is a positive polynomial. Notice that the sets of unknowns in the three systems $\mathscr{A}$, $\mathscr{S}$, and $\mathscr{T}$ are disjoint.

We can choose $d, e, f, g, h, S, Z, N, X, Y$ so that $\mathscr{S}$ is satisfied by Theorem 7. Hence $Y = [(X+1)^N/X^S]$ and $Y > 0$, $X > 4N^S$, $N \geqslant S > 0$. Then by Theorem 8, we can choose $k, l, m, A, B, C, K, L, M$ so that $\mathscr{T}$ is satisfied and $A > 1$, $B > 0$, $C > 0$. Therefore $C = \psi_A(B)$ so by Theorem 4 we can find i, j, D, E, F, G, H, I satisfying $\mathscr{A}$.

We are now ready to construct $\bar{Q}$ the polynomial described at the end of Section 7.

THEOREM 10. *There is a polynomial $\bar{Q}$ with 11 variables $d, e, f, g, h, i, j, k, l, m, n$ and the same parameters as Q such that $Q(t) > 0$ for all t if and only if $\bar{Q} = 0$ for some $d, e, f, g, h, i, j, k, l, m, n$.*

Proof. First we modify $\mathscr{U}$ by replacing S4 by

S4′ $\quad (e+1)F \mid (e+1)(H-C)+F(gY+1),$

and omitting the second and third conditions in A1. This system has exactly the same solutions as $\mathscr{U}$. Indeed, S4′ implies both S4 and $F \mid H-C$ since $e+1 \perp F$ by A3 and A4. Conversely, S4 and $F \mid H-C$ imply S4′. Also $B \leqslant C$ by T9. Now we have a system consisting of six square conditions A1, S1, S2, S3, T1, and T2; one divisibility condition S4′; one inequality; and 17 equations. Let M_6 be the polynomial constructed after the proof of the Relation-combining Theorem in Section 1 corresponding to 6 square conditions. Let

$$** \quad \bar{Q}(d, e, f, g, h, i, j, k, l, m, n)$$
$$= M_6\big(DFI,\ U(2S, d),\ V\big(d(e+1)S, f, d\big),\ V(N+S, g, e),$$
$$(M^2-1)K^2+1,\ (M^2X^2-1)L^2+1,\ (e+1)F,$$
$$(e+1)(H-C)+F(gY+1),\ K^2L^2-4(C-KLY)^2,\ n\big),$$

that is, $\bar{Q}$ is the polynomial obtained from the right side by substituting the coefficients of Q for $Q_0, \ldots, Q_\gamma$ and eliminating all the integer unknowns by means of the 17 equations. To see that this is possible, we carry out the elimination in the following order $S, Z, N, X, Y, M, K, L, A, B, C, D, E, F, G, H, I$ using S5, ..., S9, T4, ..., T9, A2, ..., A7. Here each unknown is expressed in terms of earlier ones and $Q_0, \ldots, Q_\gamma$. By the Relation-combining Theorem, $\bar{Q} = 0$ has a solution if and only if $\mathscr{U}$ can be satisfied. Hence Q is a positive polynomial if and only if $\bar{Q} = 0$ has a solution by Theorem 9.

In Section 7, we showed that the given diophantine equation $P(z_0, \ldots, z_\nu) = 0$ has a solution if and only if there are b and c such that $Q(b, c, t) > 0$ for all t. Here Q is the particular polynomial defined by the *-formulas in Sections 5, 6, and 7. Finally, let

$$** \quad \bar{P}(a_1, \ldots, a_\mu, b, c, d, e, f, g, h, i, j, k, l, m, n) = \bar{Q}$$

where $\bar{Q}$ corresponds to $Q(b, c, t)$. We thus obtain our final result:

THEOREM 11. *Given a polynomial P there is a polynomial $\bar{P}$ such that $P(a_1, \ldots, a_\mu, z_0, \ldots, z_\nu) = 0$ for some $z_0, \ldots, z_\nu$ if and only if*

$$\bar{P}(a_1, \ldots, a_\mu, b, c, d, e, f, g, h, i, j, k, l, m, n) = 0$$

for some $b, c, d, e, f, g, h, i, j, k, l, m, n$.

References

[1] Г. Чудновский, *Диофантовы предикаты*, Успехи мат. наук 25: 4 (1970), pp. 185–186.

[2] Martin Davis, *An explicit diophantine definitions of the exponential function*, Comm. Pure Appl. Math. 24 (1971), pp. 137–145.

[3] — *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly 80 (1973), pp. 233–269.

[4] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. 74 (1961), pp. 425–436 = Математика 8:5 (1964), pp. 69–79.

[5] Н. Косовский, *О диофантовых представлениях последовательности решений уравнения Пелля*, Зап. научн. семинаров Ленингр. отд. Матем. ин-та им. В. А. Стеклова 20 (1971), pp. 49–59. J. of Soviet Math. 1:1 (1973), pp. 28–35.

[6] Ю. Манин, *Десятая проблема Гильберта*, Современные проблемы математики 1 (1973), pp. 5–37.

[7] Ю. Матиясевич, *Диофантовость перечислимых множеств*, Докл. АН СССР 191 (1970), pp. 279–282 = Soviet Math. Doklady 11 (1970), pp. 354–357.

[8] — *Диофантовы множества*, Успехи мат. наук 27:5 (1972), pp. 185–222 = Russian Math. Surveys 27:5 (1972), pp. 124–164.

[9] Hilary Putnam, *An unsolvable problem in number theory*, J. Symb. Logic 25 (1960), pp. 220–232 = Математика 8:5 (1964), pp. 55–67.

[10] Julia Robinson, *Existential definability in arithmetic*, Trans. Amer. Math. Soc. 72 (1952), pp. 437–449 = Математика 8:5 (1964), pp. 3–14.

[11] Thoralf Skolem, *Diophantische Gleichungen*, Berlin 1938.

[12] Martin Davis, Yuri Matijasevič, and Julia Robinson, *Hilberts tenth problem. Diophantine equations: Positive aspects of a negative solution*, Proceedings of the Symposium on Hilbert's problems, Amer. Math. Soc. 1975.

STEKLOV MATHEMATICAL INSTITUTE
OF ACADEMY OF SCIENCES OF USSR
Leningrad

UNIVERSITY OF CALIFORNIA
Berkeley, California

Received on 28. 2. 1974 (538)