THE SOLUTION TO HILBERT'S TENTH PROBLEM

Sarah F. Cooper
The Solution to Hilbert's Tenth Problem
Department of Mathematics
Master of Science

ABSTRACT

This thesis presents a complete solution to Hilbert's tenth problem — i.e., the result that there is no algorithm to determine if an arbitrary diophantine equation has a solution in integers. This solution is contained in Chapters III, IV and V.

Chapter II is an intuitive introduction to recursion theory. Chapter III deals with some applications of results of Chapter II to exponential diophantine equations, made by M. Davis, H. Putnam and J. Robinson. In Chapters IV and V two proofs are given of the result that exponentiation is diophantine. These are due to Ju. V. Matijasevič and M. Davis. Chapter VI is an attempt by the author to analyze the results of the two preceding chapters.

THE SOLUTION TO HILBERT'S TENTH PROBLEM

by

Sarah F. Cooper

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of Master of Science.

Department of Mathematics
McGill University
Montreal

March 1972

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

My grateful thanks go to my advisor, Professor P. Olin, for all his advice and encouragement during the writing of this thesis and also to Professor E. Rosenthall for his kind help. Last but not least, I should like to thank my cousin Linette Woods for transforming an untidy manuscript into a presentable thesis.

CHAPTER I

Introduction

In 1900 Hilbert [5] gave the following problem as the tenth in his famous list of problems:

> Given a diophantine equation with any number of unknown quantities and with integral coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.

In other words, we are asked to find a general algorithm to answer questions of the form: Does the diophantine equation $P(x_1,\ldots,x_n) = 0$ have a solution in integers? Here P is a polynomial in $x_1,\ldots,x_n$ with integer coefficients.

The work of Gödel caused mathematicians to modify Hilbert's statement of the problem and to ask instead whether such a general algorithm exists. This question has recently been answered in the negative, i.e.,

> There is no general algorithm to determine if an arbitrary diophantine equation has a solution in integers.

Chapter II of this thesis gives an intuitive introduction to recursion theory which closely follows the survey article by Julia Robinson [10], together with important theorems by Gödel and Davis.

Chapter III is concerned with applications of Chapter II to exponential diophantine equations. (An exponential diophantine equation is similar to a diophantine equation except that variables may occur as exponents.) These applications were begun by Julia Robinson [9] and continued by her, M. Davis and H. Putnam [3]. The main result of Chapter III is:

> There is no general algorithm to determine if an arbitrary exponential diophantine equation has a solution in integers.

In Chapters IV and V we show that exponentiation is diophantine, which completes the negative solution to Hilbert's tenth problem. We give two proofs of this result: the original proof due to Matijasevič [7], from which the result follows by a theorem of Julia Robinson (Chapter V); and a modified form of Matijasevič's proof due to M. Davis [2] (Chapter IV).

Chapter VI contains no formal mathematics. It does contain some conjectures by the author on the ideas which led Matijasevič to his results and attempts to show how Davis modified those results to get his solution.

CHAPTER II

Computing and Listing

We first look at pairs and sequences of natural numbers. Cantor showed that there is a one-one correspondence between the set of natural numbers and the set of ordered pairs of natural numbers. A function which gives such a one-one correspondence is the function

$$J : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$J(x,y) = \tfrac{1}{2}\left((x + y)^2 + 3x + y\right) .$$

(The function values are easily seen to be integers.)

We have $J(0,0) = 0$,

$$J(x,y) + 1 = \begin{cases} J(x + 1, y - 1), & \text{if } y > 0 , \\ J(0, x + 1), & \text{if } y = 0 . \end{cases}$$

So J maps the set of ordered pairs of natural numbers onto the set of natural numbers and J is one-one. We have the following table of values of J :

$J(x,y)$	y = 0	1	2	3	4
0	0	1	3	6	10 ..
1	2	4	7	11 ..	⋮
x = 2	5	8	12 ..	⋮	
3	9	13 ..	⋮		
4	14 ..	⋮			
	⋮				

The equation $u = J\left(K(u),L(u)\right)$ uniquely determines two inverse functions K and L . (e.g., $K(8) = 2, L(8) = 1$.)

As an example of the usefulness of such functions, suppose S is the range of a function $F(x,y)$ of two variables. Then S is also the range of

$G(u) = F\Big(K(u),L(u)\Big)$ which is a function of one variable. Since $F(x,y) = G\Big(J(x,y)\Big)$ we can recover F from G.

If $R(x,y)$ is a binary relation, we may represent $R(x,y)$ by a set S of natural numbers using the equivalence $R(x,y)$ iff $J(x,y) \varepsilon S$. A sequence of sets of natural numbers, $S_0,S_1,\ldots$ may be represented by a single set S of natural numbers by the correspondence $x \varepsilon S_n$ iff $J(n,x) \varepsilon S$.

Pairing functions also provide a system of numbering diophantine equations. A diophantine equation is an equation of the form $F(x_0,x_1,\ldots) = G(x_0,x_1,\ldots)$ where F and G are terms built up from $x_0,x_1,\ldots$ and natural numbers by addition and multiplication. We may also write a diophantine equation in the form $P(x_0,x_1,\ldots) = 0$ where $P(=F-G)$ is a polynomial with integral coefficients.

We number the terms $\tau_0,\tau_1,\ldots$ built up from variables and natural numbers by addition and multiplication as follows:

$$\tau_{4n} = n ,$$

$$\tau_{4n+1} = x_n ,$$

$$\tau_{4n+2} = \tau_{K(n)} + \tau_{L(n)} ,$$

$$\tau_{4n+3} = \tau_{K(n)} \cdot \tau_{L(n)} .$$

Then we number the equations, the n^{th} equation being $\tau_{K(n)} = \tau_{L(n)}$. Thus the eighth equation is $0 + 0 = x_0$, for example.

Finally we give a method of representing finite sequences of natural numbers due to Gödel.

Definition 2.1 Rem(x,y) is the least non-negative remainder of x divided by y . i.e., Rem(x,y) = z iff there is a natural number n such that $x = ny + z$ with $0 \leqslant z < y$.

Lemma 2.2 (Gödel 1931) For every finite sequence $s_0, s_1, \ldots, s_k$ of natural numbers there are natural numbers a and d such that

$$s_t = \mathrm{Rem}\left(a, 1 + (t+1)d\right) \quad \text{for} \quad t = 0,1,\ldots,k . \tag{1}$$

Proof (1) is equivalent to $a \equiv s_t \left(\mathrm{mod}(1 + (t+1)d)\right)$ and $0 \leqslant s_t < 1 + (t+1)d$ for $t = 0,1,\ldots,k$. We choose for d a multiple of k! which is large enough to ensure that $d > s_t$ for all $t \leqslant k$. In this way the inequalities will be satisfied. We now show that the moduli are relatively prime, for suppose p prime, $p|(1 + (t+1)d)$ and $p|(1 + (t' + 1)d)$ with $t,t' \leqslant k$ and $t \neq t'$. (We suppose $t > t'$.) Then $p|(1 + (t+1)d) - (1 + (t' + 1)d)$, i.e., $p|(t - t')d$ with $0 < t - t' \leqslant k$. If $p|(t - t')$ then $p|k!$ so $p|d$ but if $p|d$ then $p \nmid (1 + (t+1)d)$. Contradiction. Since the moduli are relatively prime, we can find a common solution to the congruences $a \equiv s_t \left(\mathrm{mod}(1 + (t+1)d)\right)$, $0 \leqslant t \leqslant k$ by the Chinese remainder theorem.

We now turn to the problem of either finding a "general method" (i.e., an algorithm) to determine if an arbitrary diophantine equation has a solution in integers or of showing that there is no such general method. Intuitively, by a "general method" we mean a finite set of instructions which describe how to start from an arbitrary diophantine equation $P(x_1,\ldots,x_n) = 0$ and to finish (after a finite number of steps) with the

correct answer to the question: Does $P(x_1,\ldots,x_n) = 0$ have a solution? The instructions must be the kind that could be given to a computer to carry out, devoid of any element of ingenuity or chance. (Although we do not ask that they are necessarily practical or place any restriction on the time or space needed to carry them out.)

Before the work of Gödel, the notion of "general method" was not mathematically precise and it was therefore not possible to ask whether such a method existed. On the other hand, if a correct method had been found, Hilbert's tenth problem [5] would have been solved without having to ask precisely what was meant by a "general method". Probably this correct method would have been effective. We now try to formulate the notion of "general method".

Suppose we number all diophantine equations in a systematic way (e.g., the one that has already been described). Then given any n we can write down the n^{th} equation and given an equation we can write down its number (or one of them since some equations may occur more than once). Let S be the set of numbers of equations which have solutions. Then a method to tell whether or not an arbitrary natural number n is in S would give a method to tell whether or not an arbitrary diophantine equation has a solution.

A set S is called computable if there is a method to decide whether $n \varepsilon S$ or not for any arbitrary natural number n. A method is a finite set of instructions which for each natural number n specifies a calculation which ends with the answer "yes" or "no" to the question: Does n belong to the set being computed? This is intuitively what is meant by a computable set. Later we give a mathematical characterisation of such sets.

A set L of natural numbers is called listable if there is a method of listing the members of L. A list is a finite or infinite sequence, possibly with repetitions. A method of listing a set of numbers is a set of instructions giving a completely mechanical calculation which may or may not terminate. From time to time during the calculation a number is given as being the next on the list so we place it next on the list.

A function $F(x_1,\ldots,x_n)$ defined for all natural numbers and whose range is a subset of the natural numbers is called computable if we can mechanically calculate $F(x_1,\ldots,x_n)$ for any n-tuple of natural numbers.

We now prove some results concerning computable and listable sets and computable functions.

Lemma 2.3 A set S of natural numbers is computable iff S and $\overline{S}(=\mathbb{N}\setminus S)$ are both listable.

Proof If S is computable, the method for computing S can be modified to interchange "yes" and "no" answers so $\overline{S}$ is also computable. Since every computable set is clearly listable, S and $\overline{S}$ are listable.

If S and $\overline{S}$ are listable and both are infinite sets we can make a single list by alternating an element from the list of S and an element from the list of $\overline{S}$. To see if $n \in S$ or not we see if n occurs in an even or an odd position on the new list. (It must occur eventually and always in an even position or always in an odd one.) If either S or $\overline{S}$ is finite then clearly they are both computable. (If S is finite we can tell if $n \in S$ or not by inspection.)

Lemma 2.4 The range of a computable function is listable and conversely every non-empty listable set S is the range of a computable function.

Proof If F is a computable function of one variable then we can list $F(0),F(1),F(2)\ldots$. If F is a computable function of k variables then we can agree on an ordering of k-tuples (using the J function, iterated, for example) and list the function values in the appropriate order.

If S is a non-empty listable set then S is either finite, in which case we choose a function F which becomes constant or else S is infinite and we define $F(n)$ to be the n^{th} number on the list of S . In each case, F is computable.

Lemma 2.5 A function $F(x)$ is computable iff $\{J(x,F(x))\}$ (i.e., the graph of F) is listable.

Proof If F is a computable function then clearly $J(x,F(x))$ is a computable function also. From Lemma 2.4 the range of $J(x,F(x))$ is listable.

Conversely, suppose the graph of a function G is listable. To calculate $G(n)$ we list the members of the graph of G until some number u is listed which has $K(u) = n$. Then $G(n) = L(u)$.

Suppose that L is a mathematical language such that we can give instructions in L for listing any listable set. We may assume that L has only a finite number of symbols. We also assume that we can recognise suitable instructions in L and that the calculations given are a sequence of steps of finite length. (These assumptions can be justified but we do not do so here. See [10].)

Lemma 2.6 There is a listable set U such that $\{U_0, U_1, \ldots\}$ is the class of listable sets, and where we have $k \in U_n$ iff $J(n,k) \in U$.

Proof Let $I_0, I_1, I_2, \ldots$ be a numbering of suitable sets of instructions in L (We could order the sets of instructions by the total number of symbols occurring in each set and then use a lexicographical ordering among those of the same length, for example.) and let $U_0, U_1, U_2, \ldots$ be the corresponding listable sets. We now carry out the instructions from the sets $I_0, I_1, \ldots$ in the sequence:

1^{st} instruction from I_0,
2^{nd} " " I_0,
1^{st} " " I_1,
3^{rd} " " I_0,
2^{nd} " " I_1,
1^{st} " " I_2, etc.

When an instruction from I_m says that n is the next number on the list of U_m, we place $J(m,n)$ on the list of U. Thus U is listable and has the required property.

Lemma 2.7 There is a listable set which is not computable.

Proof Let U be as in Lemma 2.6. Let $D = \{n \mid n \in U_n\}$. To list D we list U and whenever we have $J(n,n) \in U$ we put n on the list of D. Thus D is listable. If D is computable then $\overline{D}$ is listable so $\overline{D} = U_i$ for some i, i.e., for all n, $n \in U_i$ iff $J(n,n) \notin U$ iff $n \notin U_n$. This must hold for $n = i$ which is impossible so D is not computable.

Recursive Functions

We now define mathematically a class of number-theoretic functions which we identify with computable functions.

A function is called primitive recursive if it can be obtained from initial functions by repeated (finite) substitution and recursion.

The initial functions are:

(1) the zero function 0_n of n variables with

$0_n(x_1,\ldots,x_n) = 0$ for $n \geqslant 0$,

(2) the successor function S with $S(x) = x + 1$,

(3) for every n and every k with $1 \leqslant k \leqslant n$, the identity function I_{nk} of n variables with $I_{nk}(x_1,\ldots,x_n) = x_k$.

A function F of n variables is obtained by substitution from a function A of m variables and m functions $B_1,\ldots,B_m$ of n variables if $F(x_1,\ldots,x_n) = A\Big(B_1(x_1,\ldots,x_n),\ldots,B_m(x_1,\ldots,x_n)\Big)$.

We can obtain by substitution the functions

$$SO_n(x_1,\ldots,x_n)\ ,\ SSO_n(x_1,\ldots,x_n),\ldots$$

i.e., all constant functions. If we want to introduce extra variables or change the order of variables in order that substitutions may be made, we can do so using the identity functions. For example, suppose we wish to define $F(x,y,z)$ such that $F(x,y,z) = B(z,x)$. We put

$$F(x,y,z) = B\Big(I_{33}(x,y,z)\ ,\ I_{31}(x,y,z)\Big) .$$

A function F of $n+1$ variables is obtained by recusion from a function A of n variables and a function B of $n+2$ variables if

$$F(x_1,\ldots,x_n,0) = A(x_1,\ldots,x_n) ,$$

$$F(x_1,\ldots,x_n,Sy) = B\Big(x_1,\ldots,x_n,y,F(x_1,\ldots,x_n,y)\Big) .$$

We give some examples of primitive recursive functions:

$$x + y : x + 0 = x , \; x + Sy = S(x + y) .$$

$$x \cdot y : x \cdot 0 = 0 , \; x \cdot Sy = x \cdot y + x .$$

$$x^y : \quad x^0 = 1 , \quad x^{Sy} = x^y \cdot x .$$

We define $\operatorname{sgn} x = 0^{0^x}$ $\begin{pmatrix} = 0 \text{ if } x = 0 \\ = 1 \text{ if } x \neq 0 \end{pmatrix}$ (where $0^0 = 1$ by definition) and and we see that $\operatorname{sgn} x$ can be obtained from u^v by substitution. The predecessor function P can be obtained by recursion as: $P0 = 0$, $PSx = x$. We define $x \dot{-} y$ as $x \dot{-} y = \begin{cases} x - y & \text{if } x - y \geqslant 0 \\ 0 & \text{otherwise} \end{cases}$. We can obtain $x \dot{-} y$ by recursion thus:

$$x \dot{-} 0 = x \quad \text{and} \quad x \dot{-} Sy = P(x \dot{-} y) .$$

Then $|x - y| = (x \dot{-} y) + (y \dot{-} x)$ by substitution, and we can define $\operatorname{Rem}(x,y)$ as follows:

$$\operatorname{Rem}(0,y) = 0 ,$$

$$\operatorname{Rem}(Sx,y) = \Big(S \operatorname{Rem}(x,y)\Big) \cdot \operatorname{sgn}|y - S \operatorname{Rem}(x,y)| .$$

(If $y \nmid Sx$ then $\operatorname{sgn}|y - S \operatorname{Rem}(x,y)| = 1$ and $\operatorname{Rem}(Sx,y) = S \operatorname{Rem}(x,y)$. If $y \mid Sx$ then $\operatorname{sgn}|y - S \operatorname{Rem}(x,y)| = 0$ and $\operatorname{Rem}(Sx,y) = 0$.)

If $A(x_1,\ldots,x_n,y)$ is primitive recursive then the functions B and C given by:

$$B(x_1,\ldots,x_n,z) = \sum_{y \leqslant z} A(x_1,\ldots,x_n,y) \ ;$$

$$C(x_1,\ldots,x_n,z) = \prod_{y \leqslant z} A(x_1,\ldots,x_n,y)$$

are also primitive recursive for they are obtained as follows:

$$B(x_1,\ldots,x_n,0) = A(x_1,\ldots,x_n,0) \ ,$$

$$B(x_1,\ldots,x_n,Sz) = B(x_1,\ldots,x_n,z) + A(x_1,\ldots,x_n,Sz)$$

and

$$C(x_1,\ldots,x_n,0) = A(x_1,\ldots,x_n,0) \ ,$$

$$C(x_1,\ldots,x_n,Sz) = C(x_1,\ldots,x_n,z) \cdot A(x_1,\ldots,x_n,Sz) \ .$$

All the functions which arise naturally in number theory can be shown to be primitive recursive. It is clear that every primitive recursive function is computable for if F is defined by substitution and recursion, we have a way to compute F. The converse is false for we may number all primitive recursive functions of one variable $F_0,F_1,\ldots$ in a systematic way depending on how they are generated by substitution and recursion. We define G by

$$G(t) = F_t(t) + 1 \ .$$

G is not F_n for any n so G cannot be primitive recursive, but clearly G is computable.

A function F of n variables is general recursive if there are primitive recursive functions A of one variable and B of $n + 1$ variables such that

$$F(x_1,\ldots,x_n) = A\,\mu y\{B(x_1,\ldots,x_n,y) = 0\}\ ,$$

where for every n-tuple of natural numbers $x_1,\ldots,x_n$ there is a natural number y such that $B(x_1,\ldots,x_n,y) = 0$ and $\mu y\{B(x_1,\ldots,x_n,y) = 0\}$ is the least y such that $B(x_1,\ldots,x_n,y) = 0$ (if there were no such y, $\mu y\{\ldots\}$ would be undefined).

A general recursive function is computable for in order to compute $F(x_1,\ldots,x_n)$ we compute $B(x_1,\ldots,x_n,0)$, $B(x_1,\ldots,x_n,1),\ldots$ until we reach the first y such that $B(x_1,\ldots,x_n,y) = 0$ (we are assured that such a y exists). We can compute these values since B is primitive recursive. Then $F(x_1,\ldots,x_n) = A(y)$ and since A is computable, F is computable.

We cannot apply the same argument as in the case of primitive recursive functions to show that there is a computable function which is not general recursive since there is no method of listing all general recursive functions.

From now on we accept the contention:

Church's Thesis Every computable function is general recursive.

and identify computable and general recursive functions. (Clearly we cannot prove Church's Thesis since computability is an intuitive concept and not precisely defined.)

Recursively Enumerable Sets and Relations

A set of natural numbers is recursively enumerable if it is empty or if it is the range of a primitive recursive function of one variable. A relation $R(x_1,\ldots,x_n)$ is recursively enumerable if it is empty or if there are n primitive recursive functions of one variable $F_1,\ldots,F_n$ such that $R(x_1,\ldots,x_n)$ iff there is a natural number m such that $x_1 = F_1(m) \wedge \ldots \wedge x_n = F_n(m)$.

Since a primitive recursive function is computable and we have shown that the range of a computable function is listable (Lemma 2.4), it follows that every recursively enumerable set is listable. Conversely we have the contention:

Every listable set is recursively enumerable.

(which is equivalent to Church's Thesis).

From now on we identify listable sets and recursively enumerable sets. It follows that the range of a general recursive function is recursively enumerable. A set is recursive if both it and its complement are recursively enumerable. So we identify recursive sets with computable sets.

Gödel's Theorem and Davis' Theorem

A formula is arithmetical if it is built up by means of logical symbols $(\forall, \exists, \sim, \wedge, \vee)$ from equations of the form $a = b$, $a + b = c$ and $ab = c$ where a, b and c are variables or symbols for particular numbers. Relations defined by arithmetical formulas are called arithmetical.

In 1931 Gödel proved that the relation given by $F(x_1,\ldots,x_n) = y$ where F is any primitive recursive function is arithmetical. It follows that every recursively enumerable set is arithmetical, for let S be any recursively enumerable set. Then there is a primitive recursive function F of one variable such that S is the range of F. Suppose $R(x,y)$ iff $F(x) = y$. Then $y \in S$ iff $(\exists x)\big(F(x) = y\big)$ iff $(\exists x)\big(R(x,y)\big)$ and since $R(x,y)$ is arithmetical, so is $(\exists x)\big(R(x,y)\big)$. Also, every recursively enumerable relation is arithmetical, for suppose $R(x,y)$ is a binary recursively enumerable relation. Then there are primitive recursive functions F and G of one variable such that $R(x,y)$ iff $(\exists n)\big(x = F(n) \wedge y = G(n)\big)$. Since each of the conjuncts is arithmetical, so is $R(x,y)$. The proof for recursively enumerable relations of higher degree is similar.

We may use bounded quantifiers in arithmetical formulas since $(\exists x \leqslant y)[\ldots]$ is equivalent to $(\exists x,t)[x + t = y \wedge \ldots]$ and $(\forall x \leqslant y)[\ldots]$ is equivalent to $(\forall x)\{(\exists t)(x = y + 1 + t) \vee \ldots\}$ (either $x > y$ or $\ldots$).

We now prove Gödel's theorem in a strengthened form due to M. Davis.

Theorem 2.8 (Gödel-Davis) Every relation given by $F(x_1,\ldots,x_n) = y$ where F is a primitive recursive function can be expressed by an arithmetical formula in which the universal quantifiers are all bounded and there are no negation signs.

Proof If F is a primitive recursive function then F is either an initial function or is obtained by substitution and/or recursion from initial functions. We show that the theorem holds if F is an initial function and that it holds if F is obtained by substitution or recursion from functions that satisfy the theorem. (i.e., the proof is by induction on the number of substitutions or recursions necessary to obtain F from the initial functions.)

I. (Induction basis) If F is an initial function then the theorem holds for F.

We have $$O_n(x_1,\ldots,x_n) = y \text{ iff } y = 0 ,$$

$$Sx = y \text{ iff } y = x + 1 ,$$

$$I_{nk}(x_1,\ldots,x_n) = y \text{ iff } y = x_k .$$

II. If $F(x_1,\ldots,x_n) = B\left(A_1(x_1,\ldots,x_n),\ldots,A_m(x_1,\ldots,x_n)\right)$ where $A_1,\ldots,A_m$ and B satisfy the theorem then F satisfies the theorem.

We have $F(x_1,\ldots,x_n) = y$ iff

$$(\exists z_1,\ldots,z_m)\left[z_1 = A_1(x_1,\ldots,x_n) \wedge \ldots \wedge z_m = A_m(x_1,\ldots,x_n) \wedge y = B(z_1,\ldots,z_m)\right] .$$

By the inductive hypothesis, each of the equations on the right side of the equivalence can be replaced by formulas of the required kind so F satisfies the theorem.

III. If $F(x_1,\ldots,x_k,0) = A(x_1,\ldots,x_k)$ and

$$F(x_1,\ldots,x_k,y+1) = B\left(x_1,\ldots,x_k,y,F(x_1,\ldots,x_k,y)\right)$$

where A and B satisfy the theorem then F satisfies the theorem.

For a fixed y, the sequence $u_0,\ldots,u_{y+1}$ is completely determined by the equations:

$$\begin{aligned} u_0 &= A(x_1,\ldots,x_k) , \\ u_1 &= B(x_1,\ldots,x_k,0,u_0) , \\ u_2 &= B(x_1,\ldots,x_k,1,u_1) , \\ &\vdots \quad\quad \vdots \quad\quad\quad \vdots \\ u_y &= B(x_1,\ldots,x_k,y-1,u_{y-1}) , \\ u_{y+1} &= B(x_1,\ldots,x_k,y,u_y) . \end{aligned} \tag{1}$$

If $u_0,\ldots,u_{y+1}$ satisfy (1) then $F(x_1,\ldots,x_k,t) = u_t$ for $t \leqslant y+1$. So by Gödel's Lemma (2.2) there are natural numbers a and d such that $u_t = \mathrm{Rem}\big(a,1+(t+1)d\big)$ for $0 \leqslant t \leqslant y+1$. (We actually have one more equation than we need.) Thus $F(x_1,\ldots,x_k,y) = z$ iff

$$\begin{aligned} &(\exists a,d)\Big[\mathrm{Rem}(a,1+d) = A(x_1,\ldots,x_k) \wedge z = \mathrm{Rem}\big(a,1+(y+1)d\big) \wedge \\ &(\forall t \leqslant y-1)\Big(\mathrm{Rem}(a,1+(t+2)d) = B\big(x_1,\ldots,x_k,t,\mathrm{Rem}(a,1+(t+1)d)\big)\Big)\Big] . \end{aligned} \tag{2}$$

Also

$$\mathrm{Rem}(u,1+v) = w \text{ iff } (\exists r,q)\big(u = (1+v)r + w \wedge w + q = v\big) .$$

So each of the equations on the right side of the equivalence in (2) can be replaced by a formula of the required kind and F satisfies the theorem.

Theorem 2.9 (Davis) Every recursively enumerable relation can be put in the form

$$(\exists y)(\forall u \leqslant y)(\exists v_1 \leqslant y)\ldots(\exists v_k \leqslant y)\big(P(x_1,\ldots,x_n,y,u,v_1,\ldots,v_k) = 0\big)$$

where P is a polynomial with integral coefficients. Conversely a relation defined by a formula of this form is recursively enumerable.
(This is called the Davis normal form of a recursively enumerable relation.)

Proof Using Theorem 2.8, we may assume that any recursively enumerable relation is given by a formula built up from diophantine equations by conjunctions, disjunctions, existential quantifiers and bounded universal quantifiers. We show how to reduce such a formula to the required form.

1. If all the quantified variables are distinct, the Gödel-Davis formula is equivalent to the formula obtained by writing all the quantifiers at the beginning of the formula in the same relative order and leaving the rest of the formula unchanged.

2. A formula which is built from equations by conjunctions and disjunctions is equivalent to a polynomial equal to zero, since

$$A = 0 \wedge B = 0 \quad \text{iff} \quad A^2 + B^2 = 0$$

and

$$A = 0 \vee B = 0 \quad \text{iff} \quad AB = 0 .$$

3. We have the following equivalences:

$$x > y \quad \text{iff} \quad (\exists z)(x = y + 1 + z)$$

and

$$x \geqslant y \quad \text{iff} \quad (\exists z)(x = y + z)$$

and we could use the bounded quantifier $(\exists z \leqslant x)$ in both cases.

4. A formula of the form

$$(\forall t \leqslant x)(\exists u_1,\ldots,u_k)(\forall z \leqslant x')(\exists v_1,\ldots,v_\ell)(P = 0)$$

is equivalent to

$$(\exists a_1,\ldots,a_k,d_1,\ldots,d_k)(\forall t \leqslant x)(\forall z \leqslant x')(\exists u_1,\ldots,u_k,v_1,\ldots,v_\ell)$$

$$[u_1 = \mathrm{Rem}\left(a_1, 1 + (t+1)d_1\right) \wedge \ldots \wedge u_k = \mathrm{Rem}\left(a_k, 1 + (t+1)d_k\right) \wedge P = 0] ,$$

where the two universal quantifiers are adjacent. We see that $a_1,\ldots,a_k,d_1,\ldots,d_k$ can be chosen so that $u_1,\ldots,u_k$ are arbitrary numbers depending on t for each t with $t \leqslant x$. We can use the equivalence

$$\mathrm{Rem}(u,1+v) = w \text{ iff } (\exists r,q)\left(u = (1+v)r + w \wedge w + q = v\right)$$

together with reductions 1 and 2 to reduce the formula to the form

$$(\exists\ldots)(\forall t \leqslant x)(\forall z \leqslant x')(\exists\ldots)(P' = 0) ,$$

where P' is some polynomial with integral coefficients.

5. A formula of the form $(\forall u \leqslant x)(\forall v \leqslant x')(\exists w)(P = 0)$ is equivalent to a formula with one universal quantifier, viz.,

$$(\exists z)(\forall r \leqslant z)(\exists u,v,w)\left[z = J(x,x') \wedge r = J(u,v) \wedge (u > x \vee v > x' \vee P = 0)\right] ,$$

where we use the fact that if $u \leqslant x$ and $v \leqslant x'$ then $J(u,v) \leqslant J(x,x')$ (from the definition of J). Also $z = J(x,x')$ is equivalent to $2z = 2J(x,x')$ which has integral coefficients. We use reductions 2 and 3 to obtain an equivalent formula of the form $(\exists z)(\forall r \leqslant z)(\exists u,v,w,s,t)(P'' = 0)$, where P'' is some polynomial with integral coefficients.

6. Thus given any recursively enumerable relation in the Gödel-Davis form, we first apply reductions 1, 2 and 3 wherever possible and then use reductions 4 and 5 repeatedly to obtain a formula in the form

$$(\exists x_1,\ldots,x_k)(\forall u \leqslant z)(\exists v_1,\ldots,v_\ell)(P = 0) ,$$

where P is some polynomial with integer coefficients.

7. A formula of the form

$$(\exists x,y)(\forall u \leqslant z)(\exists v_1,\ldots,v_k)(P = 0)$$

is equivalent to

$$(\exists t)(\forall u \leqslant t)(\exists v_1,\ldots,v_k,x,y,)\Big(t = J(J(x,y),z) \wedge (u > z \vee P = 0)\Big) .$$

8. Using reduction 7 repeatedly we obtain a formula of the form

$$(\exists w)(\forall u \leqslant w)(\exists v_1,\ldots,v_r)(P' = 0)$$

which is equivalent to

$$(\exists y)(\forall u \leqslant y)(\exists v_1 \leqslant y)\ldots(\exists v_r \leqslant y)(\exists w \leqslant y)(\exists z \leqslant y)(\exists t \leqslant y)$$

$$[y = J(w,z) \wedge (u = w + 1 + t \vee P' = 0)] .$$

Applying reduction 2 we at last obtain the Davis normal form.

Conversely, if $x \varepsilon S$ is defined by:

$$x \varepsilon S \text{ iff } (\exists y)(\forall u \leqslant y)(\exists v_1 \leqslant y)\ldots(\exists v_k \leqslant y)(P = 0) ,$$

then S is recursively enumerable, for let $G(x,y)$ be defined by

$$G(x,y) = \sum_{u \leqslant y} \prod_{v_1 \leqslant y} \cdots \prod_{v_k \leqslant y} P^2(x,y,u,v_1,\ldots,v_k) ;$$

then G is primitive recursive and $x \varepsilon S$ iff $(\exists y)\Big(G(x,y) = 0\Big)$.

[This is similar to the reasoning in statement 2 of Davis' theorem for:

$$(\exists x \leqslant x')\Big(P(x) = 0\Big) \text{ iff } \prod_{x \leqslant x'} P(x) = 0 ;$$

$$(\forall x \leqslant x')\Big(P(x) = 0\Big) \text{ iff } \sum_{x \leqslant x'} P^2(x) = 0 .]$$

Hence if $S \neq \emptyset$, let a be a particular element of S . (If $S = \emptyset$, S is recursively enumerable by definition.) Then

$$H(x,y) = 0^{G(x,y)} \cdot x + \Big(\operatorname{sgn} G(x,y)\Big) \cdot a$$

is primitive recursive. Now $x \varepsilon S$ iff $(\exists y)\left(G(x,y) = 0\right)$. Let this y be y_x. So if $x \varepsilon S$, $H(x,y_x) = 0^0 \cdot x + 0 \cdot a = x$ and if $G(x,y) \neq 0$, $H(x,y) = 0 \cdot x + 1 \cdot a = a$. If $x \notin S$, $H(x,y) = 0 \cdot x + 1 \cdot a = a$ for all y. So S is the range of H and therefore S is recursively enumerable.

CHAPTER III

Diophantine and Exponential Diophantine Relations

A diophantine equation is an equation of the form $A(x_1,\ldots,x_n) = B(x_1,\ldots,x_n)$ where A and B are terms built from particular natural numbers and the variables $x_1,\ldots,x_n$ by addition and multiplication. We may also write such an equation in the form $P(x_1,\ldots,x_n) = 0$ where P is a polynomial in $x_1,\ldots,x_n$ with integer coefficients. Hilbert's statement [5] of the tenth problem was for integer solutions to diophantine equations but it can be shown that the corresponding problem for solutions in the natural numbers is equivalent to the original problem. For suppose we could solve the problem for solutions in the natural numbers. Then the diophantine equation $P(x_1,\ldots,x_n) = 0$ has a solution in integers iff one of the 2^k equations $P(\pm x_1,\ldots,\pm x_n) = 0$ has a solution in natural numbers. Let $Q(x_1,\ldots,x_n)$ be formed by multiplying together the 2^k polynomials $P(\pm x_1,\ldots,\pm x_n)$. Then $P(x_1,\ldots,x_n) = 0$ has a solution in integers iff $Q(x_1,\ldots,x_n) = 0$ has a solution in natural numbers. Conversely, since Lagrange's theorem (c.f. [4], p. 300) states that every non-negative integer can be written as the sum of four squares, $P(x_1,\ldots,x_n) = 0$ has a solution in natural numbers iff $P(u_1^2 + v_1^2 + w_1^2 + z_1^2,\ldots,u_n^2 + v_n^2 + w_n^2 + z_n^2) = 0$ has a solution in integers.

We note that if we have equations $A_i = B_i$, $i = 1,\ldots,n$ then $A_1 = B_1$ and $A_2 = B_2$ and ... and $A_n = B_n$ is equivalent to the single equation $\sum_{i=1}^{n} (A_i - B_i)^2 = 0$. Also $A_1 = B_1$ or $A_2 = B_2$ or ... or $A_n = B_n$ is equivalent to the single equation $\prod_{i=1}^{n} (A_i - B_i) = 0$. In this way we can combine

systems of diophantine or exponential diophantine equations into a single equation.

A set S of natural numbers is diophantine iff there is a polynomial $P(n,x_1,\ldots,x_k)$ with integer coefficients such that $n \in S$ iff there are natural numbers $x_1,\ldots,x_k$ such that $P(n,x_1,\ldots,x_k) = 0$. A relation $R(y_1,\ldots,y_n)$ is diophantine iff there is a polynomial $P(y_1,\ldots,y_n,x_1,\ldots,x_k)$ with integer coefficients such that $R(y_1,\ldots,y_n)$ iff there are natural numbers $x_1,\ldots,x_k$ such that $P(y_1,\ldots,y_n,x_1,\ldots,x_k) = 0$.

We give some simple diophantine relations:

$a \leqslant b$ iff there is a natural number n such that $a + n = b$.

$a < b$ iff there is a natural number n such that $a + 1 + n = b$.

$a|b$ iff there is a natural number n such that $na = b$.

$a \nmid b$ iff there are natural numbers x and y such that
$b = ax + y$ and $0 < y < a$ or $a = 0$ and $b > 0$;
iff there are natural numbers x,y,z,u,v such that
$b = ax + y$ and $y = 1 + z$ and $a = y + 1 + u$
or $a = 0$ and $b = 1 + v$;
iff there are natural numbers x,y,z,u,v such that
$$\left((b - ax - y)^2 + (y - 1 - z)^2 + (a - y - 1 - u)^2\right)\left(a^2 + (b - 1 - v)^2\right) = 0 .$$

$\gcd(a,b) = 1$ iff there are natural numbers u and v such that $ua = 1 + vb$.

An exponential diophantine equation is an equation that can be put in the form $E(x_1,\ldots,x_k) = F(x_1,\ldots,x_k)$ where E and F are terms built from particular natural numbers and the variables $x_1,\ldots,x_k$ by addition, multiplication and exponentiation.

A set S of natural numbers is exponential diophantine iff there is an

exponential diophantine equation $E(n,x_1,\ldots,x_k) = F(n,x_1,\ldots,x_k)$ which has a solution for $x_1,\ldots,x_k$ in natural numbers iff $n \in S$. Exponential diophantine relations are defined analogously.

Lemma 3.1 (Robinson) [9,10 p. 98] The relation $m = \binom{n}{r}$ is exponential diophantine (where m,n,r are natural numbers).

Proof We establish the following result:

$$\binom{n}{r} = [2^{nr}(1+2^{-n})^n] - 2^n[2^{n(r-1)}(1+2^{-n})^n] + 0^{n+r} . \qquad (1)$$

($[x]$ is the greatest integer in x.) Suppose $n > 0$ and $r > 0$. Then expanding by the binomial theorem,

$$2^{nr}(1+2^{-n})^n = 2^{nr} \sum_{t=0}^{n} \binom{n}{t} 2^{-nt}$$

$$2^{nr}(1+2^{-n})^n = \sum_{t=0}^{r} \binom{n}{t} 2^{n(r-t)} + \sum_{t=r+1}^{n} \binom{n}{t} 2^{n(r-t)} . \qquad (2)$$

We show that $\sum_{t=r+1}^{n} \binom{n}{t} 2^{n(r-t)} < 1$.

$$\sum_{t=r+1}^{n} \binom{n}{t} 2^{n(r-t)} = \binom{n}{r+1} 2^{-n} + \binom{n}{r+2} 2^{-2n} + \ldots + \binom{n}{n} 2^{n(r-n)}$$

$$= 2^{-n}\left(\binom{n}{r+1} + \binom{n}{r+2} 2^{-n} + \ldots + \binom{n}{n} 2^{n(r-n+1)}\right)$$

$$\leqslant 2^{-n}\left(\binom{n}{r+1} + \binom{n}{r+2} + \ldots + \binom{n}{n}\right) .$$

Since $r \geqslant 1$, the terms on the R.H.S. of (2) with factors of $\binom{n}{0}$ and $\binom{n}{1}$

must occur in $\sum_{t=0}^{r} \binom{n}{t} 2^{n(r-t)}$. It is well known that

$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$ (i.e., a set of n elements has 2^n subsets)

and as $\binom{n}{0} = 1$, $\binom{n}{1} = n > 0$, $\sum_{t=r+1}^{n} \binom{n}{t} 2^{n(r-t)} < 2^{-n}(2^n - 1) = \frac{2^n - 1}{2^n} < 1$.

Therefore $[2^{nr}(1 + 2^{-n})^n] = \sum_{t=0}^{r} \binom{n}{t} 2^{n(r-t)}$.

Similarly, $2^{n(r-1)}(1 + 2^{-n})^n = \sum_{t=0}^{r-1} \binom{n}{t} 2^{n(r-1-t)} + \sum_{t=r}^{n} \binom{n}{t} 2^{n(r-1-t)}$

$$< \sum_{t=0}^{r-1} \binom{n}{t} 2^{n(r-1-t)} + \frac{2^n - 1}{2^n}$$

$$< \sum_{t=0}^{r-1} \binom{n}{t} 2^{n(r-1-t)} + 1$$

so $[2^{n(r-1)}(1 + 2^{-n})^n] = \sum_{t=0}^{r} \binom{n}{t} 2^{n(r-1-t)}$.

Thus $2^n[2^{n(r-1)}(1 + 2^{-n})^n] = \sum_{t=0}^{r} \binom{n}{t} 2^{n(r-t)}$, and therefore

$[2^{nr}(1 + 2^{-n})^n] - 2^n[2^{n(r-1)}(1 + 2^{-n})^n] = \binom{n}{r} 2^{n(r-r)} = \binom{n}{r}$ (if $n + r > 0$ then $0^{n+r} = 0$). So we have established (1) if $n > 0$ and $r > 0$.

If $r = 0$ then $[2^{nr}(1+2^{-n})^n] - 2^n[2^{n(r-1)}(1+2^{-n})^n] + 0^{n+r}$

$$= [(1+2^{-n})^n] - 2^n[2^{-n}(1+2^{-n})^n] + 0^n .$$

If $n = 0$ also then the above becomes $[1] - [1] + 1 = 1 = \binom{0}{0}$.

(By convention $0^0 = 1$.)

If $n > 0$ the above becomes

$$\left[\binom{n}{0} + \binom{n}{1} 2^{-n} + \dots + \binom{n}{n} 2^{-n^2}\right] - 2^n\left[\binom{n}{0} 2^{-n} + \binom{n}{1} 2^{-2n} + \dots + \binom{n}{n} 2^{-n(n+1)}\right] + 0$$

$$= 1 - 2^n 0 + 0 = 1 = \binom{n}{0} .$$

If $n = 0$ and $r > 0$ we define $\binom{n}{r} = 0$. (1) is easily verified in this case also.

To show that the relation $m = \binom{n}{r}$ is exponential diophantine we use the fact that if $b > 0$,

$$\left[\frac{a}{b}\right] = c \quad \text{iff} \quad bc \leqslant a < b(c+1) . \tag{3}$$

Let $$x = [2^{nr}(1+2^{-n})^n] \; ; \; y = [2^{n(r-1)}(1+2^{-n})^n] . \tag{4}$$

Then $$\binom{n}{r} = m = x - 2^n y + 0^{n+r} \text{ , from (1)}$$

but $2^{nr}(1+2^{-n})^n = \dfrac{2^{nr}}{2^{n^2}}(2^n+1)^n$ and $2^{n(r-1)}(1+2^{-n})^n = \dfrac{2^{n(r-1)}}{2^{n^2}}(2^n+1)^n$

$$= \frac{2^{nr}}{2^{n^2}\,2^n}(2^n+1)^n .$$

So using (3), (4) is equivalent to

$$m = x - 2^n y + 0^{n+r}$$

$$2^{n^2}x \leqslant 2^{nr}(2^n+1)^n < 2^{n^2}(x+1)$$

$$2^n \cdot 2^{n^2}y \leqslant 2^{nr}(2^n+1)^n < 2^n 2^{n^2}(y+1) .$$

Thus, $m = \binom{n}{r}$ iff there are natural numbers x and y which satisfy the above conditions. Equivalently, $m = \binom{n}{r}$ iff there are natural numbers x,y,u,v,w,z such that:

$$m + 2^n y = x + 0^{n+r}$$

and $$2^{n^2} x + u = 2^{nr}(2^n + 1)^n$$

and $$2^{nr}(2^n + 1)^n + 1 + v = 2^{n^2}(x + 1)$$

and $$2^n \cdot 2^{n^2} y + w = 2^{nr}(2^n + 1)^n$$

and $$2^{nr}(2^n + 1)^n + 1 + z = 2^n \cdot 2^{n^2}(y + 1) .$$

As previously remarked, we may combine these five equations into a single exponential diophantine equation with three parameters m, n and r which has a solution in natural numbers iff $m = \binom{n}{r}$.

Lemma 3.2 (Robinson) [9,10 p. 99] The relation $m = n!$ is exponential diophantine.

Proof We need the inequalities: a) $\frac{1}{1-\theta} < 1 + 2\theta$ for $0 < \theta < \frac{1}{2}$, and b) $(1+\theta)^k < 1 + 2^k\theta$ for $0 < \theta < 1$ (where $k \in N$).

Proofs a) If $0 < \theta < \frac{1}{2}$ then $0 < \theta^2 < \frac{1}{2}\theta$, so $2\theta^2 < \theta$.

Therefore $1 < 1 + \theta - 2\theta^2$; i.e., $1 < (1 - \theta)(1 + 2\theta)$.

Since $1 - \theta > 0$, $\frac{1}{1-\theta} < 1 + 2\theta$.

b) Now $$(1+\theta)^k = \binom{k}{0} + \binom{k}{1}\theta + \ldots + \binom{k}{k}\theta^k$$

$$= 1 + \theta\left(\binom{k}{1} + \binom{k}{2}\theta + \ldots + \binom{k}{k}\theta^{k-1}\right) ,$$

and since $0 < \theta < 1$, $\binom{k}{1} + \binom{k}{2}\theta + \ldots + \binom{k}{k}\theta^{k-1} < 2^k$, so $(1+\theta)^k < 1 + 2^k\theta$.

We now show that for any $s > (2n)^{n+1}$, $n! = \left[\frac{s^n}{\binom{s}{n}}\right]$.

For $n > 0$, $\frac{s^n}{\binom{s}{n}} = \frac{s^n \cdot n!(s-n)!}{s!} = \frac{s^{n-1}\, n!(s-n)!}{(s-1)!}$

$$= \frac{s^{n-1}\, n!}{(s-1)(s-2)\cdots(s-(n-1))}$$

$$= n!\left(\frac{s}{s-1}\right)\left(\frac{s}{s-2}\right)\cdots\left(\frac{s}{s-(n-1)}\right) .$$

But $n! \leqslant n!\left(\frac{s}{s-1}\right)\left(\frac{s}{s-2}\right)\cdots\left(\frac{s}{s-(n-1)}\right)$

and $1 < \frac{s}{s-r} = \frac{1}{1-\frac{r}{s}} < \frac{1}{1-\frac{n}{s}}$ for $1 \leqslant r \leqslant n-1$,

so $n!\left(\frac{s}{s-1}\right)\left(\frac{s}{s-2}\right)\cdots\left(\frac{s}{s-(n-1)}\right) < n!\left(\frac{1}{1-\frac{n}{s}}\right)^n$.

Now if $s > (2n)^{n+1}$, clearly $0 < \frac{n}{s} < \frac{1}{2}$,

so $n! \leqslant \frac{s^n}{\binom{s}{n}} < n!\left(\frac{1}{1-\frac{n}{s}}\right)^n < n!\left(1 + 2\left(\frac{n}{s}\right)\right)^n$ from a)

$$< n!\left(1 + 2^n\left(\frac{2n}{s}\right)\right) \text{ from b) .}$$

Thus, $\frac{s^n}{\binom{s}{n}} < n! + \frac{2^n \cdot 2n \cdot n!}{s}$, but $n!2^n \leqslant 2^n \cdot n^n$ so $n!2^n(2n) \leqslant (2n)^{n+1} < s$

and $\frac{s^n}{\binom{s}{n}} < n! + 1$, i.e., $n! = \left[\frac{s^n}{\binom{s}{n}}\right]$. We may write $m = \left[\frac{s^n}{\binom{s}{n}}\right]$ as

$\binom{s}{n}m \leqslant s^n < \binom{s}{n}(m+1)$, i.e., $s^n = \binom{s}{n}m + r$ and $r < \binom{s}{n}$.

Thus $m = n!$ iff there are natural numbers r, s and t such that

$$s > (2n)^{n+1}$$

and

$$t = \binom{s}{n}$$

and

$$s^n = mt + r$$

and

$$r < t \ ;$$

i.e., $m = n!$ iff there are natural numbers r,s,t,u,v such that

$$s = (2n)^{n+1} + 1 + u$$

and

$$t = \binom{s}{n}$$

and

$$s^n = mt + r$$

and

$$r + 1 + v = t \ .$$

We have shown in Lemma 3.1 that the relation $t = \binom{s}{n}$ is exponential diophantine and it follows that the relation $m = n!$ is exponential diophantine.

Corollary 3.3 (Matijasevič) [8] The set of primes is exponential diophantine.

Proof To show this we use Wilson's theorem and its converse, viz.: If p is prime then $(p-1)! \equiv -1 \pmod{p}$. If $p > 1$ and $(p-1)! \equiv -1 \pmod{p}$ then p is prime. (See [6], pp. 44-45.) So we may write: p is prime iff there are positive integers b,u,ℓ such that

$$p = 1 + u$$

and

$$\ell = (p-1)!$$

and

$$\ell = pb - 1 \ .$$

with $\alpha > r$. Let x be a real number with $0 < x < 1$. Then expanding $(1+x)^{\alpha}$ around $x = 0$ by Taylor's theorem with Lagrange's form for the remainder, we have $(1+x)^{\alpha} = \sum_{j=0}^{r} \binom{\alpha}{j} x^j + \binom{\alpha}{r+1} x^{r+1}\left(1+\theta x\right)^{\alpha-(r+1)}$ for some θ with $0 < \theta < 1$. Let $\alpha = \frac{p}{q} > r$ and let $x = a^{-2}$ where a is an integer, $a > 1$. Then $(1+a^{-2})^{\alpha} = \sum_{j=0}^{r} \binom{\alpha}{j} a^{-2j} + \binom{\alpha}{r+1} a^{-2(r+1)}\left(1+\theta a^{-2}\right)^{\alpha-r-1}$, so

$$a^{2r+1}(1+a^{-2})^{\alpha} = \sum_{j=0}^{r} \binom{\alpha}{j} a^{2r-2j+1} + \binom{\alpha}{r+1} a^{-1}(1+\theta a^{-2})^{\alpha-r-1} . \qquad (1)$$

Let $S_r^{\alpha}(a) = \sum_{j=0}^{r} \binom{\alpha}{j} a^{2r-2j+1}$. So $S_{r-1}^{\alpha}(a) = \sum_{j=0}^{r-1} \binom{\alpha}{j} a^{2r-2j-1}$, and

$$a^{-1}S_r^{\alpha}(a) - aS_{r-1}^{\alpha}(a) = \sum_{j=0}^{r} \binom{\alpha}{j} a^{2r-2j} - \sum_{j=0}^{r-1} \binom{\alpha}{j} a^{2r-2j}$$

$$= \binom{\alpha}{r} a^{2r-2r} = \binom{\alpha}{r} . \qquad (2)$$

As $\alpha > r$, $\binom{\alpha}{r+1} = \frac{\alpha(\alpha-1)\ \ldots\ (\alpha-r)}{(r+1)!} > 0$ and the remainder term in (1), namely $\binom{\alpha}{r+1} a^{-1}\left(1+\theta a^{-2}\right)^{\alpha-r-1}$, is positive. Furthermore,

$$\binom{\alpha}{r+1} = \frac{\alpha^{r+1}\left(\frac{\alpha-1}{\alpha}\right)\ \ldots\ \left(\frac{\alpha-r}{\alpha}\right)}{(r+1)!} < \alpha^{r+1} , \quad \text{and} \quad 1 < (1+\theta a^{-2}) < 2 \quad \text{so}$$

$(1 + \theta a^{-2})^{\alpha-r-1} = (2\beta)^{\alpha-r-1} = 2^{\alpha} \cdot \frac{1}{2^{r+1}} \cdot \frac{1}{\beta} \cdot \beta^{\alpha-r}$ for some β with $\frac{1}{2} < \beta < 1$. Since $1 < \frac{1}{\beta} < 2$, $\frac{1}{2} < \frac{1}{2\beta} < 1$, so $0 < \beta^{\alpha-r} \cdot \frac{1}{2^r} \cdot \frac{1}{2\beta} < 1$, i.e., $(1 + \theta a^{-2})^{\alpha-r-1} < 2^{\alpha}$. Therefore,

$$0 < \binom{\alpha}{r+1} a^{-1} \left(1 + \theta a^{-2}\right)^{\alpha-r-1} < \alpha^{r+1} a^{-1} 2^{\alpha},$$

so we may write (1) as

$$a^{2r+1}\left(1 + a^{-2}\right)^{\alpha} = S_r^{\alpha}(a) + \theta' \alpha^{r+1} a^{-1} 2^{\alpha} \tag{3}$$

for some θ' with $0 < \theta' < 1$. In a similar fashion,

$$a^{2r-1}\left(1 + a^{-2}\right)^{\alpha} = \sum_{j=0}^{r-1} \binom{\alpha}{j} a^{2r-2j-1} + \binom{\alpha}{r} a^{-1}\left(1 + \varphi a^{-2}\right)^{\alpha-r}$$

for some φ with $0 < \varphi < 1$. Therefore

$$a^{2r-1}\left(1 + a^{-2}\right)^{\alpha} = S_{r-1}^{\alpha}(a) + \varphi' \alpha^{r} a^{-1} 2^{\alpha} \tag{4}$$

for some φ' with $0 < \varphi' < 1$. We show that for a suitable choice of a, $S_r^{\alpha}(a)$ and $S_{r-1}^{\alpha}(a)$ are integers. Consider

$$\binom{\frac{p}{q}}{j} = \frac{\left(\frac{p}{q}\right)\left(\frac{p}{q} - 1\right) \cdots \left(\frac{p}{q} - (j-1)\right)}{j!} = \frac{p(p-q)(p-2q) \cdots \left(p - q(j-1)\right)}{q^j\, j!}$$

If $q^r r! \mid a$, (and thus $q^j j! \mid a$ for $j = 0,1,\ldots,r$) then each term in $S_r^{\frac{p}{q}}(a)$ and in $S_{r-1}^{\frac{p}{q}}(a)$ is an integer (the smallest power of a appearing in each sum is a^2). We also show that for a suitable choice of a, the

remainder terms in (3) and (4) are less than 1. The remainder term in (3) is $\theta'\left(\frac{p}{q}\right)^{r+1} \frac{2^{\frac{p}{q}}}{a} < 1$ if $a > p^{r+1}\, 2^p$, and the remainder term in (4) is $\varphi'\left(\frac{p}{q}\right)^{r} \cdot \frac{2^{\frac{p}{q}}}{a} < 1$ if $a > p^{r+1}\, 2^p$. Thus, if $q^r r! \mid a$ and $a > p^{r+1}\, 2^p$, then $\left[a^{2r+1}\left(1 + a^{-2}\right)^{\frac{p}{q}}\right] = S^{\frac{p}{q}}_{r}(a)$, and $\left[a^{2r-1}\left(1 + a^{-2}\right)^{\frac{p}{q}}\right] = S^{\frac{p}{q}}_{r-1}(a)$.

So we have shown that the relation $R(s,t,p,q,r)$ which holds among natural numbers s,t,p,q,r iff

$$\frac{s}{t} = \binom{\frac{p}{q}}{r}, \quad \text{g.c.d.}(s,t) = 1, \quad \frac{p}{q} > r,$$

is equivalent to the relation $R(s,t,p,q,r)$ which holds iff there is a natural number a such that

$$\frac{p}{q} > r$$

and

$$\text{g.c.d.}(s,t) = 1$$

and

$$a > p^{r+1}\, 2^p$$

and

$$q^r \cdot r! \mid a$$

and $a\frac{s}{t} = \left[a^{2r+1}\left(1 + a^{-2}\right)^{\frac{p}{q}}\right] - a^2\left[a^{2r-1}\left(1 + a^{-2}\right)^{\frac{p}{q}}\right]$ (from (2)).

The condition $u = \left[vw^{\frac{p}{q}}\right]$ is equivalent to $u^q \leqslant v^q w^p < (u+1)^q$ which is exponential diophantine and the other conditions given above have

already been shown to be exponential diophantine. Thus we have proved that

the relation $m = \prod_{k=1}^{n} (c + dk)$ is exponential diophantine.

Corollary 3.5 The relation $m = \prod_{k=0}^{n} (c - k)$ is exponential diophantine.

Proof Either $c = k$ for some k with $0 \leqslant k \leqslant n$, in which case a factor in the product is zero, or $c > n$ and there is a natural number x such that $c = n + x + 1$, i.e., $x = c - (n + 1)$. In this case,

$$\begin{aligned}\prod_{k=0}^{n} (c-k) &= (c-0)(c-1) \ldots (c-n) \\ &= \Big(c-(n+1) + (n+1)\Big)\Big(c-(n+1) + n\Big) \ldots \Big(c-(n+1)+1\Big) \\ &= \Big(x+(n+1)\Big)\Big(x+n\Big) \ldots \Big(x+1\Big) \\ &= \prod_{k=1}^{n+1} (x+k) .\end{aligned}$$

Thus, $m = \prod_{k=0}^{n} (c-k)$ iff there is a natural number x such that

either $$c + x = n \quad \text{and} \quad m = 0 ,$$

or $$c = n + x + 1 \quad \text{and} \quad m = \prod_{k=1}^{n+1} (x+k) .$$

All these conditions have been shown to be exponential diophantine and thus

$m = \prod_{k=0}^{n} (c-k)$ is exponential diophantine.

Lemma 3.6 (Davis, Putnam, Robinson) [3,10 p. 103] (Let χ stand for $x_1,\ldots,x_n$.) Let $P(\chi,y,u,v_1,\ldots,v_k)$ be a polynomial with integral coefficients. Let $Q(\chi,y)$ be any polynomial with integral coefficients such that

$$Q(\chi,y) \geqslant y \tag{1}$$

and

$$(\forall u \leqslant y)(\forall v_1 \leqslant y) \ldots (\forall v_k \leqslant y)\Big(|P(\chi,y,u,v_1,\ldots,v_k)| \leqslant Q(\chi,y)\Big) . \tag{2}$$

Then

$$(\forall u \leqslant y)(\exists v_1 \leqslant y) \ldots (\exists v_k \leqslant y)\Big(P(\chi,y,u,v_1,\ldots,v_k) = 0\Big) \tag{3}$$

is equivalent to

$$\begin{aligned}(\exists c,t,a_1,\ldots,a_k)\Big[& t = Q(\chi,y)! \wedge 1+(c+1)t = \prod_{m\leqslant y}\Big(1+(m+1)t\Big) \\ & \wedge\ 1+(c+1)t \,\Big|\, P(\chi,y,c,a_1,\ldots,a_k) \\ & \wedge\ 1+(c+1)t \,\Big|\, \prod_{j\leqslant y}(a_1-j) \wedge \ldots \\ & \wedge\ 1+(c+1)t \,\Big|\, \prod_{j\leqslant y}(a_k-j)\Big] .\end{aligned} \tag{4}$$

(Note: k is a natural number which depends only on the number of variables in P , so for any given polynomial P , k is a constant.)

Proof

We note first that the conditions $t = Q(\chi,y)!$ and

$$1+(c+1)t = \prod_{m\leqslant y}\Big(1+(m+1)t\Big) \text{ uniquely determine } t \text{ and } c . \tag{5}$$

If $m \leqslant y$ and $m' \leqslant y$ and $m \neq m'$ then we show that g.c.d. $\left(1 + (m+1)t, 1 + (m'+1)t\right) = 1$. For suppose p prime, $p \mid \left(1 + (m+1)t\right)$ and $p \mid \left(1 + (m'+1)t\right)$, (we suppose $m > m'$), then $p \mid \left(1 + (m+1)t\right) - \left(1 + (m'+1)t\right)$, i.e., $p \mid (m - m')t$ with $0 < m - m' \leqslant y$. If $p \mid m - m'$ then $p \mid t$ because $t = Q(\chi,y)!$ and $Q(\chi,y) \geqslant y$ from (1) and (5). But clearly, if $p \mid t$ then $p \nmid 1 + (m+1)t$, so

$$\left(1 + (m+1)t, 1 + (m'+1)t\right) = 1. \tag{6}$$

Also, since $1 + (c+1)t = \prod_{m \leqslant y} \left(1 + (m+1)t\right)$,

$$1 + (c+1)t \equiv 0 \left(\mathrm{mod}\left(1 + (m+1)t\right)\right),$$

$$(c+1)t \equiv -1 + \left(1 + (m+1)t\right) \left(\mathrm{mod}\left(1 + (m+1)t\right)\right)$$

$$\equiv (m+1)t \bmod \left(1 + (m+1)t\right),$$

and since g.c.d. $\left(t, 1 + (m+1)t\right) = 1$,

$$c + 1 \equiv m + 1 \bmod \left(1 + (m+1)t\right),$$

$$\text{i.e.,} \quad c \equiv m \bmod \left(1 + (m+1)t\right). \tag{7}$$

Furthermore, if p prime, $p \mid \left(1 + (m+1)t\right)$ then g.c.d.$(p,t) = 1$, and $t = Q(\chi,y)!$, so $p \nmid Q(\chi,y)!$, which implies that $p > Q(\chi,y) \geqslant y$. Hence, by (2),

$$p > |P(\chi,y,u,v_1,\ldots,v_k)| \quad \text{for all } u,v_1,\ldots,v_k \text{ less than or equal to } y. \tag{8}$$

Now we prove the equivalence of (3) and (4).

<u>(4) implies (3)</u> Suppose (4) holds. Let $u < y$ and let p be prime,

$p \mid 1+(u+1)t$. (Since $1+(c+1)t = \prod_{m \leq y} \left(1+(m+1)t\right)$, clearly $p \left| \left(1+(c+1)t\right) \right.$.) As previously remarked, $p > y$. Put $v_i = \text{Rem}(a_i,p)$ for $i = 1 \ldots k$. (i.e., $a_i \equiv v_i \bmod p$ and $0 \leq v_i < p$.) Since $\left(1+(c+1)t\right) \left| \prod_{j \leq y} (a_i - j) \right.$ for $i = 1 \ldots k$, $p \left| \prod_{j \leq y} (a_i - j) \right.$ for $i = 1 \ldots k$. Thus for each $i = 1 \ldots k$, there is some $j_i \leq y$ such that $p \mid a_i - j_i$, so $a_i \equiv v_i \equiv j_i \bmod p$, and since $v_i < p$ and $j_i \leq y < p$, we must have $v_i = j_i$ so $v_i \leq y$. From (7), $c \equiv u \bmod \left(1+(u+1)t\right)$ and hence $c \equiv u \bmod p$. Thus, since $a_i \equiv v_i \bmod p$,

$$P(\chi,y,u,v_1,\ldots,v_k) \equiv P(\chi,y,c,a_1,\ldots,a_k) \equiv 0 \pmod p$$

(since $p \left| \left(1+(c+1)t\right) \right.$ and $\left(1+(c+1)t\right) \left| P(\chi,y,c,a_1,\ldots,a_k) \right.$ by assumption). We have shown in (8) that $p > |P(\chi,y,u,v_1,\ldots,v_k)|$ so $P(\chi,y,u,v_1,\ldots,v_k) = 0$.

<u>(3) implies (4)</u> Suppose (3) holds. Let t and c be determined by (5). By hypothesis, for every $u \leq y$ there are $v_1,\ldots,v_k \leq y$ such that $P(\chi,y,u,v_1,\ldots,v_k) = 0$. We denote the $v_1,\ldots,v_k$ corresponding to a particular u by $v_{u1},\ldots,v_{uk}$. We have shown that if $u_1 \neq u_2$, $\left(1+(u_1+1)t \, , \, 1+(u_2+1)t\right) = 1$. Thus by the Chinese remainder theorem, the system of congruences $z_1 \equiv v_{u1} \bmod \left(1+(u+1)t\right)$, $u \leq y$, have a common solution which is unique $\bmod \prod_{u \leq y} \left(1+(u+1)t\right)$. Let this common solution be a_1 . We proceed similarly to find $a_2,\ldots,a_k$,

$$\text{i.e., } a_1,\ldots,a_k \text{ satisfy } a_i \equiv v_{ui} \left(\bmod (1+(u+1)t)\right) , \; u \leq y . \qquad (9)$$

Hence $P(\chi,y,c,a_1,\ldots,a_k) \equiv P(\chi,y,v_{u1},\ldots,v_{uk}) \equiv 0 \bmod\left(1+(u+1)t\right)$ for each $u \leqslant y$. But since the moduli are relatively prime, this implies that

$$\prod_{u\leqslant y}\left(1+(u+1)t\right)\Big|P(\chi,y,c,a_1,\ldots,a_k)\ ,$$

$$\text{i.e.,}\quad 1+(c+1)t\,|\,P(\chi,y,c,a_1,\ldots,a_k)\ .$$

Also, from (9), for each $u \leqslant y$ and for each i with $1 \leqslant i \leqslant k$, $1+(u+1)t\,|\,a_i - v_{ui}$, and $v_{ui} \leqslant y$ by hypothesis. So using (6),

$$\prod_{u\leqslant y}\left(1+(u+1)t\right)\Big|\prod_{j\leqslant y}(a_i-j)\quad \text{for}\quad i=1\ldots k\ ,$$

$$\text{i.e.,}\quad 1+(c+1)t\Big|\prod_{j\leqslant y}(a_i-j)\quad \text{for}\quad i=1\ldots k\ ,$$

and we have established (4).

Theorem 3.7 (Davis, Putnam, Robinson) [3,10 p. 105] Every recursively enumerable relation is exponential diophantine.

Proof Let $R(x_1,\ldots,x_n)$ be a recursively enumerable relation. So by Theorem 2.9 there is a polynomial $P(\chi,y,u,v_1,\ldots,v_k)$ such that $R(x_1,\ldots,x_n)$ iff $(\exists y)(\forall u \leqslant y)(\exists v_1 \leqslant y)\ldots(\exists v_k \leqslant y)\left(P(\chi,y,u,v_1,\ldots,v_k) = 0\right)$. We make the following changes in P :

1) replace the coefficients by their absolute value,

2) substitute y for each of the variables $u,v_1,\ldots,v_k$,

3) add y to the resulting polynomial.

Let the new polynomial obtained be $Q(\chi,y)$. Clearly $Q(\chi,y)$ satisfies conditions (1) and (2) of Lemma 3.6. Therefore, by Lemma 3.6, $R(x_1,\ldots,x_n)$ iff there is a natural number y satisfying the relation given by (4) of Lemma 3.6. We have shown that each of the relations occurring in (4) is

exponential diophantine so $R(x_1,\ldots,x_n)$ is exponential diophantine.

In the next chapter we show that the relation $\alpha = \beta^u$ is diophantine. It follows that all the relations which have been shown to be exponential diophantine are diophantine. We also have the following corollary.

Corollary 3.8 There is a particular diophantine equation $P(n,x_1,\ldots,x_k) = 0$ for which there is no general method to tell, for an arbitrary natural number n, whether $P(n,x_1,\ldots,x_k) = 0$ has a solution for $x_1,\ldots,x_k$ in natural numbers.

Proof Let S be a recursively enumerable set which is not recursive. By Theorem 3.7, S is exponential diophantine and hence diophantine. So there is a diophantine equation $P(n,x_1,\ldots,x_k) = 0$ such that $n \in S$ iff $P(n,x_1,\ldots,x_k) = 0$ has a solution for $x_1,\ldots,x_k \in N$. If there were a general method to tell, for an arbitrary $n \in N$, whether $P(n,x_1,\ldots,x_k) = 0$ has a solution or not then there would be a general method to tell whether $n \in S$ or not. This implies that S is recursive. Contradiction.

Remark This is actually a stronger result than the fact that there is no general method to tell whether an arbitrary diophantine equation has a solution.

CHAPTER IV

The Relation $\alpha = \beta^{u}$ is Diophantine (Davis)

Unless the context indicates otherwise, all arguments are positive integers.

We need some preliminary results concerning solutions to Pell's equation in the form:

$$x^2 - (a^2 - 1)y^2 = 1 \qquad 4.(i)$$

with $a > 1$, $a \varepsilon Z$.

For $n \geqslant 0$, $n \varepsilon Z$, define $x_n(a)$ and $y_n(a)$ by:

$$x_n(a) + y_n(a)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n . \qquad 4.(ii)$$

We write x_n for $x_n(a)$ and y_n for $y_n(a)$ if the meaning is clear. By equating rational and irrational parts in 4.(ii) ($\sqrt{a^2 - 1}$ is irrational) we have:

$$x_0 = 1 \; ; \; y_0 = 0 \; ,$$

$$x_1 = a \; ; \; y_1 = 1 \; ,$$

and also

$$x_{n+1} = 2ax_n - x_{n-1} \; ; \; y_{n+1} = 2ay_n - y_{n-1} . \qquad 4.(iii)$$

Proof for 4.(iii) By induction on n .

For $n = 1$: $x_2 + y_2\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^2 = 2a^2 - 1 + 2a\sqrt{a^2 - 1}$,

so $x_2 = 2a^2 - 1$; $y_2 = 2a$. But $2a^2 - 1 = 2a \cdot a - 1$; $2a = 2a \cdot 1 - 0$.

Therefore $x_2 = 2ax_1 - x_0$; $y_2 = 2ay_1 - y_0$. Assume the result for $n = m - 1$. We wish to show that this implies that

$$x_{m+1} = 2ax_m - x_{m-1} \; ; \; y_{m+1} = 2ay_m - y_{m-1} .$$

Now, $x_{m+1} + y_{m+1}\sqrt{a^2-1} = (a + \sqrt{a^2-1})^{m+1}$

$= (a + \sqrt{a^2-1})^{m}(a + \sqrt{a^2-1})$

$= (x_m + y_m\sqrt{a^2-1})(a + \sqrt{a^2-1})$,

but by hypothesis, $x_m = 2ax_{m-1} - x_{m-2}$; $y_m = 2ay_{m-1} - y_{m-2}$,

so $x_{m+1} + y_{m+1}\sqrt{a^2-1} = \left[(2ax_{m-1} - x_{m-2}) + (2ay_{m-1} - y_{m-2})\sqrt{a^2-1}\right](a + \sqrt{a^2-1})$

$= \left[2a(x_{m-1} + y_{m-1}\sqrt{a^2-1}) - (x_{m-2} + y_{m-2}\sqrt{a^2-1})\right](a + \sqrt{a^2-1})$

$= \left[2a(a + \sqrt{a^2-1})^{m-1} - (a + \sqrt{a^2-1})^{m-2}\right](a + \sqrt{a^2-1})$

$= 2a(a + \sqrt{a^2-1})^{m} - (a + \sqrt{a^2-1})^{m-1}$

$= 2a(x_m + y_m\sqrt{a^2-1}) - (x_{m-1} + y_{m-1}\sqrt{a^2-1})$

$= (2ax_m - x_{m-1}) + (2ay_m - y_{m-1})\sqrt{a^2-1}$.

Thus, $x_{m+1} = 2ax_m - x_{m-1}$; $y_{m+1} = 2ay_m - y_{m-1}$.

(Consequently $x_{m-1} = 2ax_m - x_{m+1}$; $y_{m-1} = 2ay_m - y_{m+1}$.)

Thus the sequences $\{x_n\}$ and $\{y_n\}$ are determined completely.

It is well known (cf. [6], pp. 137-143) that natural numbers x and y satisfy 4.(i) iff there is a natural number n such that $x = x_n$; $y = y_n$. It also follows from 4.(i) that g.c.d. $(x_n, y_n) = 1$, for any common divisor of x_n and y_n must divide the L.H.S. of 4.(i) and hence must divide 1 .

On occasion we write $d = a^2 - 1$. The "de Moivre" formula states that $(x_n + y_n\sqrt{d})(x_m + y_m\sqrt{d}) = (x_{n+m} + y_{n+m}\sqrt{d})$.

[Proof $(x_n + y_n\sqrt{d})(x_m + y_m\sqrt{d}) = (a + \sqrt{a^2-1})^n (a + \sqrt{a^2-1})^m$

$= (a + \sqrt{a^2-1})^{n+m}$

$= x_{n+m} + y_{n+m}\sqrt{d}$.]

Multiplying out the L.H.S. gives $x_n x_m + dy_n y_m + (x_m y_n + y_m x_n)\sqrt{d} = x_{n+m} + y_{n+m}\sqrt{d}$.

Hence,

$$\begin{aligned} x_n x_m + dy_n y_m &= x_{n+m} \ ; \\ x_m y_n + y_m x_n &= y_{n+m} \ . \end{aligned} \qquad 4.(iv)$$

For $m = 1$, this gives

$$\begin{aligned} x_{n+1} &= x_n x_1 + dy_n y_1 = x_n a + (a^2-1)y_n \ ; \\ y_{n+1} &= x_1 y_n + y_1 x_n = a y_n + x_n \ . \end{aligned} \qquad 4.(v)$$

Lemma 4A $\quad y_n | y_t$ iff $n | t$.

Proof a) For each n , $y_n | y_{nk}$ for all k .

By induction on k . For $k = 1$ the result is clear. Assume the result for $k = s$. We wish to show that this implies that $y_n | y_{n(s+1)}$. Now $y_{n(s+1)} = y_{ns+n} = y_{ns}x_n + y_n x_{ns}$ from 4.(iv). By hypothesis, $y_n | y_{ns}$ and since $y_n | y_n$, $y_n | (y_{ns}x_n + y_n x_{ns})$, so $y_n | y_{n(s+1)}$.

b) If $y_n | y_t$ then $n | t$.

Suppose $y_n | y_t$ but $n \nmid t$. Then we may write $t = nq + r$ with $0 < r < n$. Now $y_t = y_{nq+r} = x_r y_{nq} + y_r x_{nq}$ from 4.(iv). But $y_n | y_t$ and $y_n | y_{nq}$ so $y_n | y_r x_{nq}$, and since g.c.d. $(y_{nq}, x_{nq}) = 1$, $y_n | y_r$. This is a contradiction since $r < n$ implies $y_r < y_n$ by definition of the y_n .

Lemma 4B a) $y_{nk} \equiv k\, x_n^{k-1} y_n \bmod (y_n)^3$,

b) $y_{nk} \equiv k\, x_n^{k-1} y_n \bmod (a^2-1)$,

c) $y_k \equiv k \bmod (a-1)$.

Proof We have $x_{nk} + y_{nk}\sqrt{d} = (a + \sqrt{a^2-1})^{nk}$

$= [(a + \sqrt{a^2-1})^n]^k$

$= (x_n + y_n\sqrt{d})^k$.

Expanding by the Binomial Theorem,

$$x_{nk} + y_{nk}\sqrt{d} = x_n^k + \binom{k}{1} x_n^{k-1}(y_n\sqrt{d}) + \binom{k}{2} x_n^{k-2}(y_n\sqrt{d})^2 + \ldots + \binom{k}{k-1} x_n (y_n\sqrt{d})^{k-1} + (y_n\sqrt{d})^k$$

$$= \sum_{\substack{j=0 \\ j \text{ even}}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j}{2}} + \sum_{\substack{j=1 \\ j \text{ odd}}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j-1}{2}} \sqrt{d} .$$

Therefore $y_{nk} = \sum_{\substack{j=1 \\ j \text{ odd}}}^{k} \binom{k}{j} x_n^{k-1} y_n^j d^{\frac{j-1}{2}}$. *

Thus, $y_{nk} \equiv k\, x_n^{k-1} y_n \bmod (y_n)^3$, and $y_{nk} \equiv k\, x_n^{k-1} y_n \bmod d$, since every term in * after the first is congruent to zero in both cases. Setting $n = 1$ in the last congruence gives $y_k \equiv k\, x_1^{k-1} y_1 \bmod (a^2-1)$, i.e., $y_k \equiv k\, a^{k-1} \bmod (a^2-1)$, and since $a^2 - 1 = (a-1)(a+1)$, $y_k \equiv k\, a^{k-1} \bmod (a-1)$. But $a^{k-1} - 1 = (a-1)(a^{k-2} + a^{k-3} + \ldots + a + 1)$

so $a-1 | a^{k-1} - 1$. Therefore $a^{k-1} \equiv 1 \bmod (a-1)$ and $y_k \equiv k \bmod (a-1)$.

Lemma 4.1 a) $y_n^2 | y_{n \cdot y_n}$.

b) For all t , if $y_n^2 | y_t$ then $y_n | t$.

Proof a) Setting $k = y_n$ in Lemma 4B a), we have $y_{n \cdot y_n} \equiv y_n x_n^{y_n - 1} y_n \bmod (y_n)^3$, so $(y_n)^3 | y_{n \cdot y_n} - y_n^2 x_n^{y_n - 1}$.

Therefore $y_n^2 | y_{n \cdot y_n} - y_n^2 x_n^{y_n - 1}$, and since $y_n^2 | y_n^2$, $y_n^2 | y_{n \cdot y_n}$.

b) If $y_n^2 | y_t$ then $y_n | y_t$ so $n | t$ by Lemma 4A.

Therefore $t = nk$ for some $k \in Z$. So $y_t = y_{nk} \equiv k x_n^{k-1} y_n \bmod (y_n)^3$ by Lemma 4B a). As above, $y_n^2 | y_{nk} - k x_n^{k-1} y_n$, and by assumption, $y_n^2 | y_{nk}$ so $y_n^2 | k x_n^{k-1} y_n$. Therefore $y_n | k x_n^{k-1}$ and since $(x_n, y_n) = 1$, $y_n | k$ and thus $y_n | t$.

Lemma 4.2 For each k , $y_{k+u} \equiv -y_{k+1-u} \bmod (y_k + y_{k+1})$ for all $u \leq k + 1$.

Proof By induction on u .

If $u = 0$ we have $y_k + y_{k+1} | y_k + y_{k+1}$ so $y_k \equiv -y_{k+1} \bmod (y_k + y_{k+1})$.

If $u = 1$, as above $-y_k \equiv y_{k+1} \bmod (y_k + y_{k+1})$. Assume the result for $u = j - 2$ and for $u = j - 1$ $(j \geq 2)$. Thus,

$y_{k+(j-1)} \equiv -y_{k+1-(j-1)} \bmod (y_k + y_{k+1})$, i.e., $y_k + y_{k+1} | y_{k+j-1} + y_{k+1-(j-1)}$, so $y_k + y_{k+1} | 2a(y_{k+j-1} + y_{k+1-(j-1)})$.

Also $y_k + y_{k+1} | y_{k+j-2} + y_{k+1-(j-2)}$ (hypothesis for $u = j - 2$) .

Therefore $y_k + y_{k+1} \mid 2a(y_{k+j-1} + y_{k+1-(j-1)}) - (y_{k+j-2} + y_{k+1-(j-2)})$,

i.e., $y_k + y_{k+1} \mid (2ay_{k+j-1} - y_{k+j-2}) + (2ay_{k+2-j} - y_{k+3-j})$.

Thus $y_k + y_{k+1} \mid y_{k+j} + y_{k+1-j}$ (using 4.(iii)),

and $y_{k+j} \equiv -y_{k+1-j} \bmod (y_k + y_{k+1})$.

Lemma 4.3 a) $y_{2k+1} \equiv 0 \bmod (y_k + y_{k+1})$,

b) $y_{2k} \equiv -1 \bmod (y_k + y_{k+1})$,

c) $y_{2k+2} \equiv 1 \bmod (y_k + y_{k+1})$.

Proof a) From Lemma 4.2 with $u = k+1$, $0 = -y_0 \equiv y_{2k+1} \bmod (y_k + y_{k+1})$.

b) From Lemma 4.2 with $u = k$, $-1 = -y_1 \equiv y_{2k} \bmod (y_k + y_{k+1})$.

c) $y_{2k+2} = 2ay_{2k+1} - y_{2k} \equiv 0 - (-1) \equiv 1 \bmod (y_k + y_{k+1})$.

Lemma 4.4 The numbers y_i , with $0 \leqslant i < 2k+1$, are incongruent mod $(y_k + y_{k+1})$.

Proof For $i \leqslant k$ the y_i are increasing and less than half the modulus. For $k+1 \leqslant i < 2k+1$, each y_i is congruent to a unique $-y_j$ with $1 \leqslant j \leqslant k$ by Lemma 4.2 and these are all incongruent as above. We cannot have $y_i \equiv -y_j \bmod (y_k + y_{k+1})$, $i \leqslant k$, $1 \leqslant j \leqslant k$, for this implies that $y_k + y_{k+1} \mid y_i + y_j$ and $0 < y_i + y_j < y_k + y_{k+1}$ (y_i and y_j are each less than half the modulus).

Lemma 4.5 For every n, $y_{n+2k+1} \equiv y_n \bmod (y_k + y_{k+1})$ for each k.

Proof By induction on n.

If $n = 0$, $y_0 = 0 \equiv y_{2k+1} \bmod (y_k + y_{k+1})$ (Lemma 4.3(a)).

If $n = 1$, $y_1 = 1 \equiv y_{2k+2} \bmod (y_k + y_{k+1})$ (Lemma 4.3(c)).

Assume the result for $n = m-2$ and for $n = m-1$ $(m \geqslant 2)$.

So $y_k + y_{k+1} \mid y_{(m-1)+2k+1} - y_{m-1}$,

and therefore $y_k + y_{k+1} \mid 2a(y_{(m-1)+2k+1} - y_{m-1})$.

Also $y_k + y_{k+1} \mid y_{(m-2)+2k+1} - y_{m-2}$ (hypothesis for $n = m-2$).

Therefore $y_k + y_{k+1} \mid 2a(y_{(m-1)+2k+1} - y_{m-1}) - (y_{(m-2)+2k+1} - y_{m-2})$

i.e., $y_k + y_{k+1} \mid (2ay_{m+2k} - y_{m+2k-1}) - (2ay_{m-1} - y_{m-2})$.

Thus $y_k + y_{k+1} \mid y_{m+2k+1} - y_m$ (using 4.(iii)),

and $y_{m+2k+1} \equiv y_m \bmod (y_k + y_{k+1})$.

Lemma 4.6 If $a \equiv b \bmod c$ then $y_n(a) \equiv y_n(b) \bmod c$.

Proof By induction on n.

If $n = 0$, $y_0(a) = 0 = y_0(b)$.

If $n = 1$, $y_1(a) = 1 = y_1(b)$.

Assume the result for $n = j-1$ and for $n = j-2$ $(j \geqslant 2)$.

So $y_{j-1}(a) \equiv y_{j-1}(b) \bmod c$, i.e., $c \mid y_{j-1}(a) - y_{j-1}(b)$,

so $c \mid 2a\left(y_{j-1}(a) - y_{j-1}(b)\right)$.

Also $c \mid y_{j-2}(a) - y_{j-2}(b)$ (hypothesis for $n = j-2$).

Therefore $c \mid 2a\left(y_{j-1}(a) - y_{j-1}(b)\right) - \left(y_{j-2}(a) - y_{j-2}(b)\right)$

i.e., $c \mid \left(2ay_{j-1}(a) - y_{j-2}(a)\right) - \left(2ay_{j-1}(b) - y_{j-2}(b)\right)$.

Thus $c \mid y_j(a) - y_j(b)$ (using 4.(iii)) and $y_j(a) \equiv y_j(b) \bmod c$.

Lemma 4.7 Let $v \leq y_k(a)$, $y_k(a) + y_{k+1}(a) \mid m - a$ and let $y_n(m) \equiv v \bmod \left(y_k(a) + y_{k+1}(a)\right)$. Then there is a j such that $v = y_j(a)$ and $n \equiv j \bmod (2k+1)$.

Proof Clearly, $m \equiv a \bmod (m-a)$. Thus by Lemma 4.6 , $y_n(m) \equiv y_n(a) \bmod (m-a)$. Since $y_k(a) + y_{k+1}(a) \mid m - a$, $y_n(m) \equiv y_n(a) \bmod \left(y_k(a) + y_{k+1}(a)\right)$. From Lemma 4.5 we can find a j with $0 \leq j \leq 2k$ such that $y_j(a) \equiv y_n(a) \equiv v \bmod \left(y_k(a) + y_{k+1}(a)\right)$. This j is unique by Lemma 4.4 . We show that we must have $j \leq k$. For suppose $j = k + r$ with $1 \leq r \leq k$. Then $v \equiv y_{k+r}(a) \equiv -y_{k+1-r}(a) \bmod \left(y_k(a) + y_{k+1}(a)\right)$, with $y_1 \leq y_{k+1-r} \leq y_k$, by Lemma 4.2 . Thus $y_k(a) + y_{k+1}(a) \mid v + y_{k+1-r}(a)$. But the $y_i(a)$ are increasing so $0 < y_{k+1-r}(a) < y_{k+1}(a)$. Also, $v \leq y_k(a)$ so $0 < v + y_{k+1-r}(a) < y_k(a) + y_{k+1}(a)$. Contradiction. Thus we must have $v \equiv y_j(a) \bmod \left(y_k(a) + y_{k+1}(a)\right)$ where $j \leq k$. And since both sides of the congruence are less than the modulus, $v = y_j(a)$. Clearly $n \equiv j \bmod (2k+1)$.

Note If n is odd then $y_n(a)$ is odd because $y_1(a) = 1$ and $y_n(a) = 2ay_{n-1}(a) - y_{n-2}(a)$. Thus $y_{n+1}(a) \equiv y_{n-1}(a) \bmod 2$.

Lemma 4.8 $y_{2k+1} = (y_{k+1} + y_k)(y_{k+1} - y_k)$.

Proof We have $y_{m+n} = x_n y_m + x_m y_n$ from 4.(iv), so $y_{2k+1} = y_k x_{k+1} + y_{k+1} x_k$. Now $x_{k+1} = ax_k + dy_k$ from 4.(v),

and therefore $y_{2k+1} = y_k(ax_k + dy_k) + y_{k+1}x_k$

$= ay_kx_k + (a^2 - 1)y_k^2 + x_ky_{k+1}$

$= ay_k(x_k + ay_k) + x_ky_{k+1} - y_k^2$.

Also, $y_{k+1} = ay_k + x_k$ from 4.(v),

so $y_{2k+1} = ay_ky_{k+1} + x_ky_{k+1} - y_k^2$

$= y_{k+1}(ay_k + x_k) - y_k^2$

$= y_{k+1}^2 - y_k^2$

$= (y_{k+1} + y_k)(y_{k+1} - y_k)$.

Lemma 4.9 g.c.d. $(y_{k+1} + y_k, y_{k+1} - y_k) = 1$.

Proof Suppose p is prime and $p|(y_{k+1} + y_k)$, $p|(y_{k+1} - y_k)$.

Then $p|(y_{k+1} + y_k) \pm (y_{k+1} - y_k)$, i.e., $p|2y_{k+1}$ and $p|2y_k$.

Now y_{2k+1} is odd so Lemma 4.8 implies that p is odd.

Therefore $p|y_{k+1}$ and $p|y_k$. But since $y_{k+1} = ay_k + x_k$ (from 4.(v)),

we must have $p|x_k$. This is a contradiction since g.c.d. $(x_k, y_k) = 1$.

Lemma 4.10 Let $2s + 1|2n + 1$. Then

$(y_{s+1} + y_s)|(y_{n+1} + y_n)$ and $(y_{s+1} - y_s)|(y_{n+1} - y_n)$.

Proof Let $2n + 1 = q(2s + 1)$. Since $2n + 1$ is odd, q must be odd.

The proof is by induction on q . If $q = 1$ the result is clear.

Assume the result for q_1 odd. We show that this implies the result for

$q = q_1 + 2$. Set $2n_1 + 1 = q_1(2s + 1)$, $2n + 1 = q(2s + 1) = q_1(2s + 1) + 2(2s + 1)$

$= 2n_1 + 1 + 2(2s + 1)$. Then $n = n_1 + 2s + 1$.

Therefore $y_{n+1} \pm y_n = y_{(n_1+1)+(2s+1)} \pm y_{n_1+(2s+1)}$.

But $y_{m+n} = x_n y_m + x_m y_n$; $y_{2k+1} = (y_{k+1} + y_k)(y_{k+1} - y_k)$ by 4.(iv) and Lemma 4.8.

So $y_{n+1} \pm y_n = (y_{n_1+1}x_{2s+1} + y_{2s+1}x_{n_1+1}) \pm (y_{n_1}x_{2s+1} + x_{n_1}y_{2s+1})$

$= x_{2s+1}(y_{n_1+1} \pm y_{n_1}) + y_{2s+1}(x_{n_1+1} \pm x_{n_1})$

$= x_{2s+1}(y_{n_1+1} \pm y_{n_1}) + (y_{s+1} + y_s)(y_{s+1} - y_s)(x_{n_1+1} \pm x_{n_1})$.

By hypothesis, $(y_{s+1} + y_s) \mid (y_{n_1+1} + y_{n_1})$ so $(y_{s+1} + y_s)$ divides the R.H.S. with + .

Also, $(y_{s+1} - y_s) \mid (y_{n_1+1} - y_{n_1})$ so $(y_{s+1} - y_s)$ divides the R.H.S. with - .

Therefore $(y_{s+1} + y_s) \mid (y_{n+1} + y_n)$ and $(y_{s+1} - y_s) \mid (y_{n+1} - y_n)$.

<u>Lemma 4.11</u> Let $2n + 1 = (2s+1)y_{2s+1}$.

Then $(y_{s+1} - y_s)^2 \mid (y_{n+1} - y_n)$ and $(y_{s+1} + y_s)^2 \mid (y_{n+1} + y_n)$.

Also g.c.d. $(y_{s+1} - y_s , y_{n+1} + y_n) =$ g.c.d. $(y_{s+1} + y_s , y_{n+1} - y_n) = 1$.

<u>Proof</u> Let $\ell = y_{s+1} - y_s$; $\ell' = y_{s+1} + y_s$;

$N = y_{n+1} - y_n$; $N' = y_{n+1} + y_n$.

Now $y_{2k+1} = (y_{k+1} + y_k)(y_{k+1} - y_k)$ (Lemma 4.8),

so $(\ell\ell')^2 = (y_{2s+1})^2$; $NN' = y_{2n+1} = y_{(2s+1)} \cdot y_{2s+1}$,

and since $y_n^2 \mid y_n \cdot y_n$ (Lemma 4.1), $(\ell\ell')^2 \mid (NN')$.

Since $2n+1 = (2s+1)\, y_{2s+1}$, $2s+1 \mid 2n+1$ so by Lemma 4.10, $\ell \mid N$ and $\ell' \mid N'$.

To show that g.c.d. $(\ell, N') =$ g.c.d. $(\ell', N) = 1$, suppose p is prime and $p \mid \ell$, $p \mid N'$. This implies that $p \mid N$ since $\ell \mid N$. This is a

contradiction since g.c.d. $(N,N') = 1$ by Lemma 4.9. So g.c.d. $(\ell,N') = 1$ and similarly g.c.d. $(\ell',N) = 1$. To show that $\ell^2|N$ and $(\ell')^2|N'$, suppose p is prime and $p|\ell$, so $p^2|\ell^2$. Then $p^2|(\ell\ell')^2$ so $p^2|(NN')$. Since $\ell|N$, $p|N$ and by Lemma 4.9, g.c.d. $(N,N') = 1$. Therefore $p^2|N$, and thus $\ell^2|N$. Similarly $(\ell')^2|N'$.

We next show that the relation $v = y_u(a)$ is diophantine.

Consider the Diophantine equations:

$$u + j - 1 = v \qquad \text{I}$$

$$p + (a - 1)q = v + r \qquad \text{II a.}$$

$$g = v + t \qquad \text{II b.}$$

$$p^2 - (a^2 - 1)q^2 = 1 \qquad \text{III}$$

$$h + (a + 1)g = b\left(p + (a + 1)q\right)^2 \qquad \text{IV a.}$$

$$h + (a - 1)g = c\left(p + (a - 1)q\right)^2 \qquad \text{IV b.}$$

$$h^2 - (a^2 - 1)g^2 = 1 \qquad \text{V}$$

$$m = \left(h + (a + 1)g\right)z + a \qquad \text{VI}$$

$$m = f\left(p + (a - 1)q\right) + 1 \qquad \text{VII}$$

$$x^2 - (m^2 - 1)y^2 = 1 \qquad \text{VIII}$$

$$y = (d - 1)\left(p + (a - 1)q\right) + u \qquad \text{IX}$$

$$y = (e - 1)\left(h + (a + 1)g\right) + v \qquad \text{X}$$

We show that $v = y_u(a)$ iff I to X have a solution in the remaining arguments.

I to X implies $v = y_u(a)$.

III and V imply that there are s and k such that

$p = x_s(a)$, $q = y_s(a)$,

$h = x_k(a)$, $g = y_k(a)$.

We know that $y_{m+1}(a) = x_m(a) + ay_m(a)$ from 4.(v),

so that $y_{s+1}(a) - y_s(a) = x_s(a) + (a-1)y_s(a) = p + (a-1)q$.

Similarly $y_{k+1}(a) - y_k(a) = h + (a-1)g$.

Also $y_{s+1}(a) + y_s(a) = x_s(a) + (a+1)y_s(a) = p + (a+1)q$,

and $y_{k+1}(a) + y_k(a) = h + (a+1)g$.

Let $y_{s+1}(a) - y_s(a) = p + (a-1)q = \ell$

$y_{s+1}(a) + y_s(a) = p + (a+1)q = \ell'$

$y_{k+1}(a) - y_k(a) = h + (a-1)g = N$ 4.(vi)

$y_{k+1}(a) + y_k(a) = h + (a+1)g = N'$

From I we get $u \leqslant v$.

From II a. we get $\ell = p + (a-1)q = v + r$, so $v < \ell$. } 4.(vii)

From II b. we get $v < g$.

From IV a., $N' = h + (a+1)g = b\left(p + (a+1)q\right)^2 = b(\ell')^2$, so $(\ell')^2 | N'$.

From IV b., similarly, $N = c\ell^2$, so $\ell^2 | N$.

Using Lemma 4.8, $(y_{2s+1})^2 = (\ell\ell')^2$ and $y_{2k+1} = NN'$, so $(\ell\ell')^2 | NN'$,

i.e., $(y_{2s+1})^2 | y_{2k+1}$.

By Lemma 4.1 b) , $y_{2s+1} | 2k+1$,

and therefore $\ell | 2k+1$. 4.(viii)

From VI, $m = N'z + a$ so $m \equiv a \bmod N'$.

From VII, $m = f\ell + 1$ so $m \equiv 1 \bmod \ell$. 4.(ix)

From VIII $y = y_n(m)$ for some n.

Also, IX gives $y = (d-1)\ell + u$ so $y \equiv u \bmod \ell$,

and X gives $y = (e-1)N' + v$ so $y \equiv v \bmod N'$. 4.(x)

Now $v < g = y_k(a)$ by 4.(vii).

Since $y_{k+1}(a) + y_k(a) = N'$ and $m \equiv a \bmod N'$ from 4.(ix),

we have $y_{k+1}(a) + y_k(a) \mid m - a$.

Also, $y = y_n(m) \equiv v \bmod N'$ from 4.(x), i.e., $y_n(m) \equiv v \bmod \left(y_{k+1}(a) + y_k(a)\right)$.

Thus we have the hypotheses of Lemma 4.7 and so $v = y_j(a)$ with

$n \equiv j \bmod (2k+1)$.

Since $\ell \mid 2k+1$ by 4.(viii), $n \equiv j \bmod \ell$. 4.(xi)

From Lemma 4B c), $y_n(m) \equiv n \bmod (m-1)$,

and since $m \equiv 1 \bmod \ell$ from 4.(ix), $\ell \mid m-1$

and $y = y_n(m) \equiv n \bmod \ell$. 4.(xii)

From 4.(x), $y \equiv u \bmod \ell$, so $u \equiv y \equiv n \equiv j \bmod \ell$.

From 4.(vii), $u < \ell$ and $j \leqslant y_j(a) = v < \ell$,

so we must have $u = j$ and $v = y_u(a)$.

$v = y_u(a)$ implies I to X.

Let $v = y_u(a)$. We show how to satisfy I to X. Since $v \geqslant u$ we can satisfy I. Choose s such that $y_s(a) > v$ and put $p = x_s(a)$; $q = y_s(a)$.

This satisfies II a). (Since $a > 1$, $p + (a-1)q > q > v$.) Choose k such that $2k+1 = y_{2s+1}(2s+1)$ (so $k \geqslant s$) and put $h = x_k(a)$; $g = y_k(a)$. Then $g \geqslant q > v$ and we can satisfy II b). Equations III and V are also satisfied. We write equations 4.(vi) as before. From Lemma 4.11 we get $\ell^2 | N$, $(\ell')^2 | N'$, which gives IV a) and IV b). Also from Lemma 4.11, $(N', \ell) = 1$, so by the Chinese remainder theorem we can find an m such that $m \equiv a \bmod N'$ and $m \equiv 1 \bmod \ell$ where m is unique mod $(N'\ell)$. We choose such an $m > a$. Thus VI and VII can be satisfied (with $z \geqslant 1$, $f \geqslant 1$ since $m > a$). To satisfy VIII set $x = x_u(m)$; $y = y_u(m)$.

Since $m \equiv a \bmod N'$, $y_u(m) \equiv y_u(a) \bmod N'$ by Lemma 4.6.

Thus $y = y_u(m) \equiv y_u(a) = v \pmod{N'}$, i.e., $y \equiv v \bmod N'$, which satisfies X.

Also, $y = y_u(m) \equiv u \bmod (m-1)$ by Lemma 4B c),

and since $m \equiv 1 \bmod \ell$, i.e., $\ell | m-1$, $y \equiv u \bmod \ell$, and IX can be satisfied.

We now give the Diophantine definition of $\alpha = \beta^u$. We use the following results:

<u>Lemma 4.12</u> $\quad x_n(a) - y_n(a)(a-y) \equiv y^n \bmod (2ay - y^2 - 1)$

<u>Proof</u> By induction on n .

If $n = 0$, $x_0(a) - y_0(a)(a-y) = 1$ and $y^0 = 1$ so the result is clear.

If $n = 1$, $x_1(a) - y_1(a)(a-y) = a - (a-y) = y = y^1$ and the result is clear.

Assume the result for $n = m-1$ and for $n = m-2$ $(m \geqslant 2)$.

Using the difference equation 4.(iii),

$$x_m(a) - y_m(a)(a-y) = \left(2ax_{m-1}(a) - x_{m-2}(a)\right) - \left(2ay_{m-1}(a) - y_{m-2}(a)\right)\left(a-y\right)$$

$$= 2a\left(x_{m-1}(a) - y_{m-1}(a)(a-y)\right) - \left(x_{m-2}(a) - y_{m-2}(a)(a-y)\right)$$

$$\equiv 2ay^{m-1} - y^{m-2} \bmod (2ay - y^2 - 1) \quad \text{by the inductive hypothesis.}$$

But $2ay^{m-1} - y^m - y^{m-2} = y^{m-2}(2ay - y^2 - 1)$,

so $2ay^{m-1} - y^m - y^{m-2} \equiv 0 \bmod (2ay - y^2 - 1)$,

i.e., $2ay^{m-1} - y^{m-2} \equiv y^m \bmod (2ay - y^2 - 1)$.

So $x_m(a) - y_m(a)(a-y) \equiv y^m \bmod (2ay - y^2 - 1)$.

We have $x_{m+1}(a) = 2ax_m(a) - x_{m-1}(a)$. Now $a > 1$, $x_m(a) \geqslant 1$ and the x_n are increasing so $x_{m+1}(a) \geqslant ax_m(a)$.

Thus $x_n(a) \geqslant ax_{n-1}(a) \geqslant a^2x_{n-2}(a) \geqslant \ldots \geqslant a^nx_0(a) = a^n$ since $x_0(a) = 1$.

4.(xiii)

We also need the following inequality for $y > 1$:

$a > y^n$ implies $2ay - y^2 - 1 > y^n$ (where $n \geqslant 1$). 4.(xiv)

For $2ay - (y^2 + 1) > 2y^{n+1} - y^2 - 1$ (since $a > y^n$)

$$> 2y^{n+1} - y^{n+1} - y^n \quad \text{(since } y > 1 \text{)}$$

$$> y^{n+1} - y^n = y^n(y - 1) .$$

So $2ay - y^2 - 1 > y^n$ (since $y > 1$).

We now adjoin six more equations to equations I to X:

$$w^2 - (a^2 - 1)v^2 = 1 \qquad \text{XI}$$

$$w - v(a - \beta) = \alpha + (\gamma - 1)(2a\beta - \beta^2 - 1) \qquad \text{XII}$$

$$\alpha + \delta = 2a\beta - \beta^2 - 1 \qquad \text{XIII}$$

$$\beta + \zeta = \eta \qquad \text{XIV a)}$$

$$u + \xi = \eta \qquad \text{XIV b)}$$

$$a^2 - (\eta^2 - 1)(\eta - 1)^2\delta^2 = 1 \qquad \text{XV .}$$

We show that $\alpha = \beta^u$ iff I to XV have a solution in the remaining arguments.

I to XV imply $\alpha = \beta^u$

We have show that I to X imply $v = y_u(a)$. From XI, $w = x_u(a)$.

From Lemma 4.12, $w - v(a - \beta) \equiv \beta^u \bmod (2a\beta - \beta^2 - 1)$,

but from XII, $w - v(a - \beta) \equiv \alpha \bmod (2a\beta - \beta^2 - 1)$,

so $\alpha \equiv \beta^u \bmod (2a\beta - \beta^2 - 1)$.

From XIII, $\alpha < 2a\beta - \beta^2 - 1$. From XIV a), $\beta < \eta$ and

from XIV b), $u < \eta$. From XV, we can find an n such that

$a = x_n(\eta)$; $(\eta - 1)\delta = y_n(\eta)$, and since $a > 1$, $n > 0$.

From Lemma 4B c), $y_n(\eta) \equiv n \bmod (\eta - 1)$,

but since $y_n(\eta) = (\eta - 1)\delta \equiv 0 \bmod (\eta - 1)$, $n \equiv 0 \bmod (\eta - 1)$.

As $n \geqslant 1$ we must have $n \geqslant \eta - 1$.

From 4.(xiii), $a = x_n(\eta) \geqslant \eta^n \geqslant \eta^{\eta-1}$, since $n \geqslant \eta - 1$ and $\eta \geqslant 1$.

But from above, $\beta < \eta$ and $u < \eta$ so $a \geqslant \eta^{\eta-1} > \beta^{\eta-1} \geqslant \beta^u$.

We have $a > \beta^u$ and if $\beta > 1$, $2a\beta - \beta^2 - 1 > \beta^u$ from 4.(xiv).

Since we already have $\alpha \equiv \beta^u \bmod (2a\beta - \beta^2 - 1)$ and $\alpha < 2a\beta - \beta^2 - 1$, this implies that $\alpha = \beta^u$. If $\beta = 1$ then $\alpha \equiv 1 \bmod (2a - 2)$ and since $\alpha < 2a - 2$ from XIII, $\alpha = 1$.

$\alpha = \beta^u$ implies I to XV

Given $\alpha = \beta^u$, set $\eta > \beta$, $\eta > u$, $a = x_{\eta-1}(\eta)$.

Then $y_{\eta-1}(\eta) \equiv (\eta - 1) \bmod (\eta - 1)$ from Lemma 4B c)

$\equiv 0 \bmod (\eta - 1)$

and we can satisfy XV. By this choice of η we can also satisfy XIV a) and XIV b). To satisfy XIII, if $\beta > 1$ we use 4.(xiv). Since $\alpha = \beta^u$ and $a = x_{\eta-1}(\eta) \geqslant \eta^{\eta-1} > \beta^{\eta-1} \geqslant \beta^u$, $a > \beta^u$ and the result follows as before. If $\beta = 1$, $\alpha = 1$ and since $a > 1$, $\alpha < 2a - 2$ so XIII follows directly. Using Lemma 4.12 we can satisfy XI and XII with $w = x_u(a)$, $v = y_u(a)$. We have already shown that with this choice of u, a, v, I to X can be satisfied.

CHAPTER V

The Relation $\alpha = \beta^u$ is Diophantine (Matijasevič and Robinson)

Lower case Latin letters are used as variables ranging over the positive integers with the exception of i and j which range over the non-negative integers.

We first prove some results concerning Fibonacci numbers, which are defined as follows:

$$\varphi_0 = 0 \; ; \; \varphi_1 = 1 \; ; \; \varphi_{n+1} = \varphi_n + \varphi_{n-1} \cdot$$

φ_j is called the j^{th} Fibonacci number. From the definition it is clear that $\varphi_{n+1} \geqslant \varphi_n$ (in fact $\varphi_{n+1} = \varphi_n$ only when $n = 1$).

We may also write $\varphi_{n-1} = \varphi_{n+1} - \varphi_n$

$$\varphi_n = \varphi_{n+1} - \varphi_{n-1}$$

Lemma 5.1 $\quad \varphi_{2(n+1)} = 3\varphi_{2n} - \varphi_{2(n-1)}$

Proof $\quad \varphi_{2n+2} = \varphi_{2n+1} + \varphi_{2n}$

$$= 2\varphi_{2n} + \varphi_{2n-1}$$

$$= 2\varphi_{2n} + (\varphi_{2n} - \varphi_{2n-2}) \quad \text{from above}$$

$$= 3\varphi_{2n} - \varphi_{2(n-1)}$$

Corollary $\quad \varphi_{2(n-1)} = 3\varphi_{2n} - \varphi_{2(n+1)}$

Lemma 5.2 $\varphi_{2(k+j)} \equiv -\varphi_{2(k+1-j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$, $0 \leq j \leq k+1$.

Proof By induction on j .

For $j = 0$ and $j = 1$ the result is clear, since $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2k} + \varphi_{2k+2}$.

Suppose the result holds for $j = \ell$ and for $j = \ell + 1$.

We show that this implies that $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(k+\ell+2)} + \varphi_{2(k+1-(\ell+2))}$.

By hypothesis, $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(k+\ell+1)} + \varphi_{2(k+1-(\ell+1))}$

and $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(k+\ell)} + \varphi_{2(k+1-\ell)}$

so $\varphi_{2k} + \varphi_{2k+2} | 3(\varphi_{2(k+\ell+1)} + \varphi_{2(k+1-(\ell+1))}) - (\varphi_{2(k+\ell)} + \varphi_{2(k+1-\ell)})$

$\varphi_{2k} + \varphi_{2k+2} | (3\varphi_{2(k+\ell+1)} - \varphi_{2(k+\ell)}) + (3\varphi_{2(k+1-(\ell+1))} - \varphi_{2(k+1-\ell)})$

$\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(k+\ell+2)} + \varphi_{2(k+1-(\ell+2))}$ from Lemma 5.1 and its Corollary.

Lemma 5.3 $\varphi_{2(2k+1+j)} \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$.

Proof By induction on j .

If $j = 0$, $\varphi_{2(2k+1+j)} = \varphi_{2(2k+1)} = \varphi_{2(k+k+1)}$

$\equiv -\varphi_{2(k+1-(k+1))} \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by Lemma 5.2.

$\equiv -\varphi_0 \pmod{\varphi_{2k} + \varphi_{2k+2}}$

and $\varphi_0 = 0$.

If $j = 1$, $\varphi_{2(2k+1+j)} = \varphi_{2(2k+2)} = 3\varphi_{2(2k+1)} - \varphi_{2(2k)}$ by Lemma 5.1 .

From above, $\varphi_{2(2k+1)} \equiv 0 \pmod{\varphi_{2k} + \varphi_{2k+2}}$,

so $\varphi_{2(2k+2)} \equiv -\varphi_{2(2k)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$

$\equiv -\varphi_{2(k+k)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$

$\equiv -(-\varphi_{2(k+1-k)}) \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by Lemma 5.2

$\equiv \varphi_2 \pmod{\varphi_{2k} + \varphi_{2k+2}}$.

Suppose that the result holds for $j = \ell$ and for $j = \ell + 1$.

We show that this implies that $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(2k+1+(\ell+2))} - \varphi_{2(\ell+2)}$.

By hypothesis, $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(2k+1+(\ell+1))} - \varphi_{2(\ell+1)}$

and $\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(2k+1+\ell)} - \varphi_{2\ell}$,

so $\varphi_{2k} + \varphi_{2k+2} | 3(\varphi_{2(2k+1+(\ell+1))} - \varphi_{2(\ell+1)}) - (\varphi_{2(2k+1+\ell)} - \varphi_{2\ell})$,

$\varphi_{2k} + \varphi_{2k+2} | (3\varphi_{2(2k+1+(\ell+1))} - \varphi_{2(2k+1+\ell)}) - (3\varphi_{2(\ell+1)} - \varphi_{2\ell})$,

$\varphi_{2k} + \varphi_{2k+2} | \varphi_{2(2k+1+(\ell+2))} - \varphi_{2(\ell+2)}$ by Lemma 5.1 .

Lemma 5.4 $\varphi_{2((2k+1)i+j)} \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$

Proof By induction on i .

If $i = 0$ the result is trivial.

If $i = 1$, $\varphi_{2(2k+1+j)} \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by Lemma 5.3 .

Suppose that the result holds for $i = \ell$.

Then $\varphi_{2((2k+1)(\ell+1)+j)} = \varphi_{2((2k+1)\ell+(2k+1+j))}$

$\equiv \varphi_{2(2k+1+j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by the inductive hypothesis

$\equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by Lemma 5.3 .

Corollary to Lemmas 5.4 and 5.2

$$\varphi_2\Big((2k+1)i+j\Big) \equiv \begin{cases} \varphi_{2j} & \text{for } 0 \leqslant j \leqslant k \\ \varphi_{2k} + \varphi_{2k+2} - \varphi_{2(2k+1-j)} & \text{for } k+1 \leqslant j \leqslant 2k \,. \end{cases}$$

Proof The first congruence follows from Lemma 5.4 .

For the second: $\varphi_2\Big((2k+1)i+j\Big) \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by Lemma 5.4 ;

and for $k+1 \leqslant j \leqslant 2k$, $\varphi_{2j} = \varphi_2\Big(k+(j-k)\Big)$.

So $\varphi_2\Big((2k+1)i+j\Big) \equiv \varphi_2\Big(k+(j-k)\Big) \pmod{\varphi_{2k} + \varphi_{2k+2}}$

$\equiv -\varphi_2\Big(k+1-(j-k)\Big) \pmod{\varphi_{2k} + \varphi_{2k+2}}$ by Lemma 5.2

$\equiv -\varphi_{2(2k+1-j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$

$\equiv \varphi_{2k} + \varphi_{2k+2} - \varphi_{2(2k+1-j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$.

Definition For each $m \geqslant 2$, $\Psi_{m,0} = 0$; $\Psi_{m,1} = 1$; $\Psi_{m,n+1} = m\Psi_{m,n} - \Psi_{m,n-1}$.

Lemma 5.5 If $m \geqslant 2$, $d \mid m-3$ then $\Psi_{m,j} \equiv \varphi_{2j} \pmod{d}$.

Proof By induction on j .

Since $\Psi_{m,0} = 0 = \varphi_0$ and $\Psi_{m,1} = 1 = \varphi_2$, the result is clear for $j = 0$

and $j = 1$.

Suppose the result holds for $j = k$ and for $j = k+1$.

We show that this implies that it holds for $j = k+2$.

By hypothesis, $\Psi_{m,k} \equiv \varphi_{2k} \pmod{d}$

and $\Psi_{m,k+1} \equiv \varphi_{2(k+1)} \pmod{d}$.

So $\Psi_{m,k+2} = m\Psi_{m,k+1} - \Psi_{m,k}$

$\equiv m\varphi_{2(k+1)} - \varphi_{2k} \pmod{d}$

$\equiv 3\varphi_{2(k+1)} - \varphi_{2k} + (m-3)\varphi_{2(k+1)} \pmod{d}$

$\equiv 3\varphi_{2(k+1)} - \varphi_{2k} \pmod{d}$ since $d \mid m-3$

$\equiv \varphi_{2(k+2)} \pmod{d}$ by Lemma 5.1 .

Lemma 5.6 If the numbers k,m,n,v are such that

$m \geqslant 2$, $v < \varphi_{2k+1}$, $(\varphi_{2k} + \varphi_{2k+2}) \mid (m-3)$, $\Psi_{m,n} \equiv v \pmod{\varphi_{2k} + \varphi_{2k+2}}$

then there exist numbers i,j such that $v = \varphi_{2j}$, $n = (2k+1)i + j$.

Proof Setting $d = \varphi_{2k} + \varphi_{2k+2}$, we have the hypotheses of Lemma 5.5 , so $\Psi_{m,n} \equiv \varphi_{2n} \pmod{\varphi_{2k} + \varphi_{2k+2}}$. Using the division algorithm we may write $n = (2k+1)i + j$ with $0 \leqslant j \leqslant 2k$.

Therefore $v \equiv \Psi_{m,n} \equiv \varphi_{2((2k+1)i+j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$.

If $0 \leqslant j \leqslant k$ then by the corollary to Lemmas 5.4 and 5.2 ,

$v \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$. *

Since $v < \varphi_{2k+1} \leqslant \varphi_{2k+2}$ and $\varphi_{2j} \leqslant \varphi_{2k}$, both sides of * are less than the modulus. Thus $v = \varphi_{2j}$.

If $k+1 \leqslant j \leqslant 2k$ then by the corollary to Lemmas 5.4 and 5.2 ,

$v \equiv -\varphi_{2(2k+1-j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$

with $1 \leqslant 2k+1-j \leqslant k$ (i.e., $1 \leqslant \varphi_{2(2k+1-j)} \leqslant \varphi_{2k}$) .

Thus $\varphi_{2k} + \varphi_{2k+2} \mid v + \varphi_{2(2k+1-j)}$ with $1 < v + \varphi_{2(2k+1-j)} < \varphi_{2k} + \varphi_{2k+2}$ which is impossible.

Lemma 5.7 If $m \geq 2$, $\ell | m-2$ then $\Psi_{m,j} \equiv j \pmod{\ell}$.

Proof By induction on j .

For $j = 0$ and $j = 1$ the result is trivial.

Suppose that the result holds for $j = k$ and for $j = k+1$.

So, by hypothesis, $\Psi_{m,k} \equiv k \pmod{\ell}$

and $\Psi_{m,k+1} \equiv k+1 \pmod{\ell}$.

Then $\Psi_{m,k+2} = m\Psi_{m,k+1} - \Psi_{m,k}$

$\equiv m(k+1) - k \pmod{\ell}$

$\equiv (m-2)k + k + (m-2) + 2 \pmod{\ell}$

$\equiv k + 2 \pmod{\ell}$ since $\ell | m-2$.

Lemma 5.8 $\varphi_{i+1}^2 - \varphi_i\varphi_{i+1} - \varphi_i^2 = (-1)^i$

Proof By induction on i .

For $i = 0$, $\varphi_1^2 - \varphi_0\varphi_1 - \varphi_0^2 = 1 = (-1)^0$

and for $i = 1$, $\varphi_2^2 - \varphi_1\varphi_2 - \varphi_1^2 = 1 - 1 - 1 = (-1)^1$.

Suppose that the result holds for $i = k$.

Then $\varphi_{k+2}^2 - \varphi_{k+1}\varphi_{k+2} - \varphi_{k+1}^2 = (\varphi_{k+2} - \varphi_{k+1})^2 + \varphi_{k+1}\varphi_{k+2} - 2\varphi_{k+1}^2$

$= (\varphi_{k+1} + \varphi_k - \varphi_{k+1})^2 + \varphi_{k+1}(\varphi_{k+1} + \varphi_k) - 2\varphi_{k+1}^2$

$= \varphi_k^2 + \varphi_{k+1}\varphi_k - \varphi_{k+1}^2$

$= (-1)(\varphi_{k+1}^2 - \varphi_{k+1}\varphi_k - \varphi_k^2)$

$= (-1)(-1)^k$ by the inductive hypothesis

$= (-1)^{k+1}$.

Lemma 5.9 If the numbers j,k are such that $(k^2 - jk - j^2)^2 = 1$ then there is a number i such that $j = \varphi_i$; $k = \varphi_{i+1}$.

Proof (We recall that $j \geqslant 0$, $k \geqslant 1$ by a previous remark.)

We see that $(k^2 - jk - j^2)^2 = 1$ implies that $j \leqslant k$.

For if $k^2 - jk - j^2 = 1$ then $k^2 - j^2 = 1 + jk \geqslant 1$ so $k > j$.

If $j = 0$ it is impossible to find a k with $k^2 - jk - j^2 = -1$ so in this case we must have $j > 0$.

We have $k^2 = j^2 + jk - 1$, so $k^2 \geqslant j^2$ since $jk \geqslant 1$, i.e., $k \geqslant j$.

The proof of the lemma is by induction on $j+k$.

If $j + k = 1$ then $j = 0$, $k = 1$, so $j = \varphi_0$, $k = \varphi_1$.

Suppose that j and k are such that $(k^2 - jk - j^2)^2 = 1$ and suppose also that the result holds for all j' and k' for which

$\left((k')^2 - j'k' - (j')^2\right)^2 = 1$ with $j' + k' < j + k$.

(We may assume $j > 0$ since $j = 0$ implies $k = 1$ and this is our inductive basis.)

Set $j_1 = k - j$, $k_1 = j$. Then $j_1 \geqslant 0$, $k_1 > 0$ and

$$(k_1^2 - j_1k_1 - j_1^2)^2 = \left(j^2 - j(k-j) - (k-j)^2\right)^2$$

$$= (j^2 + jk - k^2)^2$$

$$= (k^2 - jk - j^2)^2 = 1 .$$

Furthermore, $j_1 + k_1 = k < j + k$.

Therefore, by the inductive hypothesis there is a number i such that

$j_1 = \varphi_i$, $k_1 = \varphi_{i+1}$ so $j = \varphi_{i+1}$ and $k = \varphi_i + \varphi_{i+1} = \varphi_{i+2}$.

Lemma 5.10 For each $m \geqslant 2$, $\Psi^2_{m,i+1} - m\Psi_{m,i}\Psi_{m,i+1} + \Psi^2_{m,i} = 1$.

Proof By induction on i .

For $i = 0$, $\Psi^2_{m,1} - m\Psi_{m,1}\Psi_{m,0} + \Psi^2_{m,0} = 1$.

For $i = 1$, $\Psi^2_{m,2} - m\Psi_{m,2}\Psi_{m,1} + \Psi^2_{m,1} = m^2 - m^2 + 1 = 1$.

Suppose the result holds for $i = k$.

Then $\Psi^2_{m,k+2} - m\Psi_{m,k+1}\Psi_{m,k+2} + \Psi^2_{m,k+1}$

$= (m\Psi_{m,k+1} - \Psi_{m,k})^2 - m\Psi_{m,k+1}(m\Psi_{m,k+1} - \Psi_{m,k}) + \Psi^2_{m,k+1}$

$= \Psi^2_{m,k+1} - m\Psi_{m,k}\Psi_{m,k+1} + \Psi^2_{m,k} = 1$ by the inductive hypothesis.

Lemma 5.11 If the numbers j,k,m are such that

$m \geqslant 2$, $j \leqslant k$, $k^2 - mjk + j^2 = 1$ then there is a number i such that

$j = \Psi_{m,i}$, $k = \Psi_{m,i+1}$.

Proof Suppose $m \geqslant 2$.

The proof of the lemma is by induction on $j+k$.

If $j+k = 1$ then $j = 0$, $k = 1$ so $j = \Psi_{m,0}$, $k = \Psi_{m,1}$.

Suppose that j and k are such that $j \leqslant k$, $k^2 - mjk + j^2 = 1$ and

suppose also that the result holds for all j' and k' for which $j' \leqslant k'$,

$(k')^2 - mj'k' + (j')^2 = 1$ with $j' + k' < j + k$.

Let $j_1 = mj - k$, $k_1 = j$.

Then $k_1^2 - mj_1k_1 + j_1^2 = j^2 - m(mj-k)j + (mj-k)^2 = j^2 + k^2 - mjk = 1$.

Since $j \leqslant k$, $j(j-k) \leqslant 0$ so $1 = k^2 - mjk + j^2 > j(j-k)$, $k^2 - mjk > -jk$,

and therefore $mj - k < j$ since $k > 0$, i.e., $j_1 < k_1$.

Furthermore, $j_1 + k_1 < 2k_1 = 2j \leq j + k$. Therefore, by the inductive hypothesis there is a number i such that $j_1 = \Psi_{m,i}$, $k_1 = \Psi_{m,i+1}$ so $j = \Psi_{m,i+1}$ and $k = m\Psi_{m,i+1} - \Psi_{m,i} = \Psi_{m,i+2}$.

Lemma 5.12 : g.c.d. $(\varphi_i, \varphi_{i+1}) = 1$.

Proof By induction on i .

The result is clear if $i = 0$ and if $i = 1$.

Suppose that the result holds for $i = k$.

Now $\varphi_{k+2} = \varphi_{k+1} + \varphi_k$ by definition.

Suppose that φ_{k+2} and φ_{k+1} have a common divisor $d > 1$.

Since $d|\varphi_{k+2}$ and $d|\varphi_{k+1}$, $d|\varphi_{k+2} - \varphi_{k+1}$, i.e., $d|\varphi_k$, which implies that g.c.d. $(\varphi_k, \varphi_{k+1}) > 1$.

So we have shown that g.c.d. $(\varphi_{k+1}, \varphi_{k+2}) > 1$ implies g.c.d. $(\varphi_k, \varphi_{k+1}) > 1$. The contrapositive of this statement gives the required result.

Lemma 5.13 $\varphi_{i+j} = \varphi_{i-1}\varphi_j + \varphi_i\varphi_{j+1}$.

Proof By induction on j .

For $j = 1$ the formula becomes $\varphi_{i+1} = \varphi_{i-1}\varphi_1 + \varphi_i\varphi_2 = \varphi_{i-1} + \varphi_i = \varphi_{i+1}$ by definition.

For $j = 2$ the formula becomes $\varphi_{i+2} = \varphi_{i-1}\varphi_2 + \varphi_i\varphi_3 = \varphi_{i-1} + 2\varphi_i$

$= \varphi_i + \varphi_{i+1} = \varphi_{i+2}$

by definition.

Suppose the result holds for $j = k$ and for $j = k+1$

so $\varphi_{i+k} = \varphi_{i-1}\varphi_k + \varphi_i\varphi_{k+1}$

$\varphi_{i+k+1} = \varphi_{i-1}\varphi_{k+1} + \varphi_i\varphi_{k+2}$.

Adding the two equations we have

$$\varphi_{i+k+2} = \varphi_{i+k} + \varphi_{i+k+1} = \varphi_{i-1}(\varphi_k + \varphi_{k+1}) + \varphi_i(\varphi_{k+1} + \varphi_{k+2})$$

$$= \varphi_{i-1}\varphi_{k+2} + \varphi_i\varphi_{k+3} .$$

Lemma 5.14 If $m|n$ then $\varphi_m|\varphi_n$.

Proof Let $n = mk$.

The proof is by induction on k .

For $k = 1$ the result is clear.

Suppose the result holds for $k = \ell$, i.e., $\varphi_m|\varphi_{m\ell}$.

We show that this implies that $\varphi_m|\varphi_{m(\ell+1)}$.

$\varphi_{m(\ell+1)} = \varphi_{m\ell+m} = \varphi_{m\ell-1}\varphi_m + \varphi_{m\ell}\varphi_{m+1}$ by Lemma 5.13 .

Since $\varphi_m|\varphi_m$ and $\varphi_m|\varphi_{m\ell}$ by hypothesis, $\varphi_m|\varphi_{m\ell-1}\varphi_m + \varphi_{m\ell}\varphi_{m+1}$,

i.e., $\varphi_m|\varphi_{m(\ell+1)}$.

Lemma 5.15 g.c.d. $(\varphi_n,\varphi_m) = \varphi_{\text{g.c.d.}(n,m)}$.

Proof Suppose $m > n$.

We apply the Euclidean algorithm to find g.c.d. (m,n) (cf. [6], pp.14-15) .

We have:

$$m = q_0 n + r_1 \quad \text{where} \quad 0 < r_1 < n$$

$$n = r_1 q_1 + r_2 \quad \text{where} \quad 0 < r_2 < r_1$$

$$r_1 = r_2 q_1 + r_3 \quad \text{where} \quad 0 < r_3 < r_2$$

$$\vdots \qquad\qquad \vdots$$

$$r_{t-2} = r_{t-1} q_{t-1} + r_t \quad \text{where} \quad 0 < r_t < r_{t-1}$$

$$r_{t-1} = r_t q_t$$

and g.c.d. $(m,n) = r_t$.

So g.c.d. (φ_m, φ_n) = g.c.d. $(\varphi_{q_0 n + r_1}, \varphi_n)$

= g.c.d. $(\varphi_{q_0 n - 1}\varphi_{r_1} + \varphi_{q_0 n}\varphi_{r_1 + 1}, \varphi_n)$ using Lemma 5.13 ,

= g.c.d. $(\varphi_{q_0 n - 1}\varphi_{r_1}, \varphi_n)$ since $\varphi_n | \varphi_{q_0 n}$ by Lemma 5.14 .

But by Lemma 5.12, g.c.d. $(\varphi_{q_0 n}, \varphi_{q_0 n - 1}) = 1$, so g.c.d. $(\varphi_n, \varphi_{q_0 n - 1}) = 1$.

Therefore g.c.d. (φ_m, φ_n) = g.c.d. $(\varphi_{r_1}, \varphi_n)$.

Writing $n = r_1 q_1 + r_2$ we repeat the process to obtain:

g.c.d. $(\varphi_{r_1}, \varphi_n)$ = g.c.d. $(\varphi_{r_2}, \varphi_{r_1})$.

Similarly, g.c.d. $(\varphi_{r_2}, \varphi_{r_1})$ = g.c.d. $(\varphi_{r_3}, \varphi_{r_2})$

$\vdots$ $\qquad\qquad$ $\vdots$

g.c.d. $(\varphi_{r_{t-1}}, \varphi_{r_{t-2}})$ = g.c.d. $(\varphi_{r_t}, \varphi_{r_{t-1}})$

so g.c.d. (φ_m, φ_n) = g.c.d. $(\varphi_{r_t}, \varphi_{r_{t-1}})$.

But $r_t | r_{t-1}$ so using Lemma 5.14 ,

g.c.d. (φ_m, φ_n) = g.c.d. $(\varphi_{r_t}, \varphi_{r_{t-1}}) = \varphi_{r_t}$

$= \varphi_{\text{g.c.d.}(m,n)}$.

Lemma 5.16 $\varphi_{in+1} \equiv \varphi_{n+1}^{i} \pmod{\varphi_n}$.

Proof By induction on i .

For $i = 0$. we have $\varphi_1 = 1 = (\varphi_{n+1})^0$.

For $i = 1$, the result is clear.

Suppose that the result holds for $i = k$.

$\varphi_{(k+1)n+1} = \varphi_{(kn+1)+n} = \varphi_{kn}\varphi_n + \varphi_{kn+1}\varphi_{n+1}$ by Lemma 5.13

$\equiv \varphi_{kn+1}\varphi_{n+1} \pmod{\varphi_n}$

$\equiv (\varphi_{n+1})^k \varphi_{n+1} \pmod{\varphi_n}$ by the inductive hypothesis

$\equiv (\varphi_{n+1})^{k+1} \pmod{\varphi_n}$.

Lemma 5.17 $\varphi_{mn} \equiv m\,\varphi_n \varphi_{n+1}^{m-1} \pmod{\varphi_n^2}$.

Proof By induction on m .

If $m = 1$, $m\varphi_n\varphi_{n+1}^{m-1} = \varphi_n(\varphi_{n+1})^0 = \varphi_n$.

Suppose the result holds for $m = k$.

Then $\varphi_{(k+1)n} = \varphi_{(kn+1)+(n-1)}$

$= \varphi_{kn}\varphi_{n-1} + \varphi_{kn+1}\varphi_n$ by Lemma 5.13

$= \varphi_{kn}(\varphi_{n+1} - \varphi_n) + \varphi_{kn+1}\varphi_n$.

Using Lemma 5.14 , $\varphi_n^2 \mid \varphi_{kn}\varphi_n$, and from Lemma 5.16 , $\varphi_{kn+1} \equiv \varphi_{n+1}^{k} \pmod{\varphi_n}$, so there is an integer c such that $\varphi_{kn+1} = c\,\varphi_n + \varphi_{n+1}^{k}$.

Therefore $\varphi_{(k+1)n} \equiv \varphi_{kn}\varphi_{n+1} + \varphi_{kn+1}\varphi_n \pmod{\varphi_n^2}$

$\equiv \varphi_{kn}\varphi_{n+1} + (c\,\varphi_n + \varphi_{n+1}^k)\varphi_n \pmod{\varphi_n^2}$

$\equiv \varphi_{kn}\varphi_{n+1} + \varphi_{n+1}^k\varphi_n \pmod{\varphi_n^2}$

$\equiv k\varphi_n\varphi_{n+1}^k + \varphi_{n+1}^k\varphi_n \pmod{\varphi_n^2}$ by the inductive hypothesis

$\equiv (k+1)\varphi_n\varphi_{n+1}^k \pmod{\varphi_n^2}$.

Lemma 5.18 $\varphi_s^2 | \varphi_{rs}$ iff $\varphi_s | r$.

Proof Suppose $\varphi_s^2 | \varphi_{rs}$.

Then $\varphi_{rs} \equiv r\varphi_s\varphi_{s+1}^{r-1} \pmod{\varphi_s^2}$ by Lemma 5.17 ,

so $\varphi_s^2 | r\varphi_s\varphi_{s+1}^{r-1}$,

$\varphi_s | r\varphi_{s+1}^{r-1}$.

But by Lemma 5.12 , g.c.d. $(\varphi_s, \varphi_{s+1}) = 1$, so $\varphi_s | r$.

Suppose $\varphi_s | r$.

Then $\varphi_s^2 | r\varphi_s$ and since $\varphi_{rs} \equiv r\varphi_s\varphi_{s+1}^{r-1} \pmod{\varphi_s^2}$, $\varphi_{rs} \equiv 0 \pmod{\varphi_s^2}$,

i.e., $\varphi_s^2 | \varphi_{rs}$.

Corollary If $\varphi_s^2 | \varphi_t$ then $\varphi_s | t$.

Proof Since $\varphi_s | \varphi_t$, g.c.d. $(\varphi_s, \varphi_t) = \varphi_s$.

But from Lemma 5.15 , g.c.d. $(\varphi_s, \varphi_t) = \varphi_{\text{g.c.d.}(s,t)}$, so $s = $ g.c.d. (s,t) ,

which implies that $s | t$.

Therefore there is an integer r such that $t = rs$.

By Lemma 5.18 , $\varphi_s | r$ so $\varphi_s | t$.

Lemma 5.19 $2\varphi_{2n} < \varphi_{2(n+1)} \leqslant 3\varphi_{2n}$ (for $n > 0$) .

Proof From Lemma 5.1 , $\varphi_{2(n+1)} = 3\varphi_{2n} - \varphi_{2(n-1)}$, and since the φ_i are all non-negative, $\varphi_{2(n+1)} \leqslant 3\varphi_{2n}$.

Again from Lemma 5.1 , $2\varphi_{2n} = \varphi_{2(n+1)} + \varphi_{2(n-1)} - \varphi_{2n}$

$$= \varphi_{2(n+1)} + \varphi_{2(n-1)} - (\varphi_{2n-1} + \varphi_{2n-2})$$

$$= \varphi_{2(n+1)} - \varphi_{2n-1} .$$

But $2n-1$ is odd and the smallest Fibonacci number of odd subscript is $\varphi_1 = 1$, so $2\varphi_{2n} < \varphi_{2(n+1)}$.

Lemma 5.20 $n \leqslant 2^{n-1} \leqslant \varphi_{2n} < 3^n$ (for $n > 0$) .

Proof By induction on n .

If $n = 1$ the result is clear.

Suppose the result holds for $n = m$.

If $m \leqslant 2^{m-1}$, clearly $m+1 \leqslant 2^m$.

If $2^{m-1} \leqslant \varphi_{2m}$, then $2^m \leqslant 2\varphi_{2m} < \varphi_{2(m+1)}$ by Lemma 5.19 .

If $\varphi_{2m} < 3^m$ then $\varphi_{2(m+1)} \leqslant 3\varphi_{2m} < 3^{m+1}$ by Lemma 5.19 .

Theorem 5.21 $v = \varphi_{2u}$ iff there exist positive integers g,h,ℓ,m,x,y,z such that:

$$u \leqslant v < \ell \qquad \text{I}$$

$$\ell^2 - \ell z - z^2 = 1 \qquad \text{II}$$

$$g^2 - gh - h^2 = 1 \qquad \text{III}$$

$$\ell^2 | g \qquad \text{IV}$$

$$\ell | (m-2) \qquad \text{V}$$

$$(2h+g) | (m-3) \qquad \text{VI}$$

$$x^2 - mxy + y^2 = 1 \qquad \text{VII}$$

$$\ell | (x-u) \qquad \text{VIII}$$

$$(2h+g) | (x-v) \qquad \text{IX}$$

I to IX imply $v = \varphi_{2u}$

Suppose that the numbers u,v,g,h,ℓ,m,x,y,z satisfy conditions I to IX. By Lemma 5.9 it follows from II that there is a number s such that

$$i = \varphi_s \ , \ z = \varphi_{s-1} \ . \qquad 5.(i)$$

Also by Lemma 5.9 , it follows from III that there is a number k' such that $h = \varphi_{k'}$, $g = \varphi_{k'+1}$.

Lemma 5.8 implies that k' is even so there is a number k with $2k = k'$ such that

$$h = \varphi_{2k} \ , \ g = \varphi_{2k+1} \ . \qquad 5.(ii)$$

So $2h + g = 2\varphi_{2k} + \varphi_{2k+1} = \varphi_{2k} + \varphi_{2k+2}$.

From IV, $\ell^2 | g$, i.e., $\varphi_s^2 | \varphi_{2k+1}$,

so by the corollary to Lemma 5.18 , $\varphi_s | 2k+1$,

$$\text{i.e.,} \quad \ell | 2k+1 \ . \qquad 5.(iii)$$

From I, $v < \ell$ and since v is a positive integer,

$$\ell \geqslant 2 . \qquad 5.(iv)$$

From V, $\ell | m-2$ so

$$m \geqslant 2 . \qquad 5.(v)$$

Since $\ell \geqslant 2$, $\ell^2 > \ell$ and since $\ell^2 | g$ from IV, $g \geqslant \ell^2$, so $\ell < \ell^2 \leqslant g$,

$$\text{i.e.,} \quad \ell < \varphi_{2k+1} . \qquad 5.(vi)$$

By Lemma 5.11, it follows from 5.(v) and VII that there is a number n such that

$$x = \Psi_{m,n} \qquad 5.(vii)$$

(Note: We do not in fact have the hypothesis of Lemma 5.11 corresponding to "$j \leqslant k$". However, either $x \leqslant y$ or $y \leqslant x$ and since the L.H.S. of the equation $x^2 - mxy + y^2 = 1$ is symmetric in x and y then either $x = \Psi_{m,n}, y = \Psi_{m,n+1}$ or $x = \Psi_{m,n}, y = \Psi_{m,n-1}$. It is not necessary in this proof to specify which of the alternatives holds.)

We have:

$$m \geqslant 2 ,$$

$$v < \ell < \varphi_{2k+1} , \text{ (from I and 5.(vi))}$$

$$2h + g = \varphi_{2k} + \varphi_{2k+2} ,$$

$$\text{so} \quad \varphi_{2k} + \varphi_{2k+2} | m - 3 , \text{ (from VI)}$$

$$\text{and} \quad \varphi_{2k} + \varphi_{2k+2} | x - v , \text{ (from IX)}$$

$$\text{i.e.,} \quad \varphi_{2k} + \varphi_{2k+2} | \Psi_{m,n} - v ,$$

$$\text{i.e.,} \quad \Psi_{m,n} \equiv v \pmod{\varphi_{2k} + \varphi_{2k+2}} .$$

Thus by Lemma 5.6 there are numbers i and j such that

$$v = \varphi_{2j} \ , \ n = (2k+1)i + j \ . \qquad 5.(viii)$$

Also, $m \geqslant 2$, $\ell | m-2$, (from V) so by Lemma 5.7 ,

$$x = \Psi_{m,n} \equiv n \pmod{\ell} \ . \qquad 5.(ix)$$

By VIII, $\ell | x-u$, i.e., $x = \Psi_{m,n} \equiv u \pmod{\ell}$,

so $n \equiv u \pmod{\ell}$ (from 5.(ix)).

From 5.(iii), $\ell | 2k+1$ and from 5.(viii), $n = (2k+1)i + j$

so $n \equiv j \pmod{\ell}$, and therefore $u \equiv j \pmod{\ell}$.

From 5.(viii), $v = \varphi_{2j}$ and from Lemma 5.20 , $j \leqslant \varphi_{2j}$ so $j \leqslant v$.

Since $u \leqslant v < \ell$ (from I), $j < \ell$ and $u < \ell$, so $u = j$ and $v = \varphi_{2u}$.

$v = \varphi_{2u}$ implies I to IX

Suppose $v = \varphi_{2u}$. By Lemma 5.20 , $u \leqslant \varphi_{2u}$ so $u \leqslant v$.

Set $\ell = \varphi_{6s+1}$, $z = \varphi_{6s}$ where s is chosen large enough to make $v < \ell$.

Thus we have satisfied I. By Lemma 5.8 , II holds.

Put $g = \varphi_{\ell(6s+1)}$, $h = \varphi_{\ell(6s+1)-1}$.

By Lemma 18, since $\ell | \ell$, i.e., $\varphi_{6s+1} | \ell$,

$\varphi^2_{6s+1} | \varphi_{\ell(6s+1)}$, i.e., $\ell^2 | g$ and IV is satisfied.

Since $\varphi_3 = 2$ and by Lemma 5.15 ,

g.c.d. $(\varphi_{6s+1}, \varphi_3) = \varphi_{\text{g.c.d.}(6s+1,3)} = \varphi_1 = 1$, ℓ is odd.

Therefore $\ell(6s+1) - 1$ is even and by Lemma 5.8 ,

$g^2 - hg - h^2 = (-1)^{\ell(6s+1)-1} = 1$, so III is satisfied.

By Lemma 5.12 , g.c.d. $(h,g) = 1$ and since ℓ is odd and $\ell | g$,

g.c.d. $(2h+g,\ell) = 1$.

Thus by the Chinese remainder theorem, the congruences $m \equiv 2 \pmod{\ell}$ and $m \equiv 3 \pmod{2h+g}$ have a common solution. (Clearly we can choose this m such that $m \geqslant 2$.) This satisfies V and VI.

Set $x = \Psi_{m,u}$, $y = \Psi_{m,u+1}$.

By Lemma 5.10 , VII is satisfied.

By Lemma 5.7 , $x = \Psi_{m,u} \equiv u \pmod{\ell}$ so $\ell | (x-u)$ and VIII is satisfied.

Since $2h+g | m-3$, $\Psi_{m,u} \equiv \varphi_{2u} \pmod{2h+g}$ by Lemma 5.5 ,

i.e., $x \equiv v \pmod{2h+g}$, so $2h+g | x-v$ and IX is satisfied.

The fact that exponentiation is diophantine follows from this theorem using Lemma 5.20 and the following theorem by J. Robinson [9,10 pp. 108-110].

Lemma 5.22 (Robinson) There is a diophantine relation $R(a,u)$ such that

(i) if $R(a,u)$ then $u \geqslant a^a$

(ii) if $a > 1$ and $u \geqslant a^{2a}$ then $R(a,u)$.

In fact we may take for $R(a,u)$ the relation between a and u which holds iff there exist x and y such that

$$x^2 - (a^2-1)(a-1)^2y^2 = 1 \qquad (1)$$

$$x > 1 \qquad (2)$$

$$u \geqslant ax . \qquad (3)$$

Proof Suppose $R(a,u)$ holds. Since $x > 1$ it follows from (1) that $a > 1$. So there is an $n > 0$ such that $x = x_n(a)$ and

$(a-1)y = y_n(a)$. By Lemma 4B (c) , $y_n(a) \equiv n \pmod{a-1}$.

But $y_n(a) \equiv 0 \pmod{a-1}$ so $n \equiv 0 \pmod{a-1}$ and since $n > 0$, $n \geqslant a-1$.

By ③, $u \geqslant ax$, so $u \geqslant ax_{a-1}(a)$ since the x_n are increasing.

But $x_n(a) \geqslant a^n$ (by 4.(xiii)) so $u \geqslant a \cdot a^{a-1}$, i.e., $u \geqslant a^a$.

Now suppose that we have $a > 1$.

To satisfy ① and ② we set $x = x_{a-1}(a)$, $y = \dfrac{y_{a-1}(a)}{(a-1)}$ (which is a positive integer from Lemma 4B (c)).

To satisfy ③ we want $u \geqslant a \cdot x_{a-1}(a)$.

Now $x_n(a)$ is the rational part of $(a + \sqrt{a^2-1})^n$ and since $\sqrt{a^2-1} < a$, $x_n(a) \leqslant (2a)^n \leqslant a^{2n}$ (since $a \geqslant 2$).

Hence $a \cdot x_{a-1}(a) \leqslant a \cdot a^{2(a-1)} < a^{2a}$.

To satisfy ③ we want $u \geqslant a \cdot x_{a-1}(a)$ so if we take $u \geqslant a^{2a}$ and $a > 1$ then $R(a,u)$.

Theorem 5.23 (Robinson) If there is a diophantine relation $S(p,q)$ such that

(iii) if $S(p,q)$ then $p > 1$ and $q \leqslant p^p$,

(iv) for every k there are p and q with $S(p,q)$ and $q > p^k$,

then the relation $r = s^t$ is diophantine.

Proof We show that $r = s^t$ with $s > 0$, $t > 0$ iff there are natural numbers a,x,y and z such that

$$s > 0 \ , \ t > 0 \qquad ④$$

$$R(s+t+1 \ , \ 2as - s^2 - 1) \qquad ⑤$$

$$S(a,z) \qquad ⑥$$

$$x < z \ , \ y > 0 \ , \ x^2 - (a^2 - 1)y^2 = 1 \qquad ⑦$$

$$\mathrm{Rem}(y, a-1) = t \qquad ⑧$$

$$\mathrm{Rem}\big(x - (a-s)y \ , \ 2as - s^2 - 1\big) = r \qquad ⑨$$

Suppose ④-⑨ are satisfied.

Since $R(s+t+1 \ , \ 2as - s^2 - 1)$ and $s > 0 \ , \ t > 0$, it follows from Lemma 5.22 that $2as - s^2 - 1 \geqslant (s+t+1)^{s+t+1} > s^t$.

Since $S(a,z)$ then $a > 1$ and $z \leqslant a^a$ so $x < a^a$ and $y > 0$.

Hence $x = x_n(a)$ and $y = y_n(a)$ for some $n > 0$ (from ⑦).

Since $x_n(a) \geqslant a^n$ and $x = x_n(a) < a^a$ we must have $n < a$.

Since $\mathrm{Rem}(y, a-1) = t$, $y_n(a) \equiv t \pmod{a-1}$ with $0 \leqslant t < a-1$ and since $t > 0$, $0 < t < a-1$.

But $y_n(a) \equiv n \pmod{a-1}$ (Lemma 4B (c)) and $0 < n \leqslant a-1$.

Therefore $n \equiv t \pmod{a-1}$ and we must have $n = t$.

So $x = x_t(a)$, $y = y_t(a)$.

Since $\mathrm{Rem}\big(x - (a-s)y \ , \ 2as - s^2 - 1\big) = r$,

$x - (a-s)y \equiv r \pmod{2as - s^2 - 1}$ with $0 \leqslant r < 2as - s^2 - 1$.

But by Lemma 4.12 , $x_t(a) - y_t(a)(a-s) \equiv s^t \pmod{2as - s^2 - 1}$

so $r \equiv s^t \pmod{2as - s^2 - 1}$ and $r < 2as - s^2 - 1 \ , \ s^t < 2as - s^2 - 1$.

Therefore $r = s^t$.

Now suppose $r = s^t$ with $s > 0$, $t > 0$.

Conditions (iii) and (iv) ensure that for every k there are infinitely many p and q with $S(p,q)$ and $q > p^k$.

Hence we can choose a sufficiently large such that

$R(s+t+1, 2as - s^2 - 1)$, $t < a-1$ and such that for some z,

$S(a,z)$ and $z > a^{2t}$.

For this choice of a, $z > x_t(a)$. Hence if we take $x = x_t(a)$, $y = y_t(a)$, conditions ④ to ⑨ will be satisfied.

To show that $S(u,v)$ (which holds iff $v = \varphi_{2u}$) satisfies the hypotheses of Theorem 5.23, we must show that:

(a) If $S(u,v)$ then $v \leqslant u^u$.

(b) For every k there are u and v with $S(u,v)$ and $v > u^k$.

From Lemma 5.20 we have $\varphi_{2u} < 3^u$ so if $v = \varphi_{2u}$, (a) is satisfied.

To satisfy (b) we show that for every k there is a u such that $u^k < 2^{u-1}$. We want $u^k < 2^{u-1}$, i.e., $k \log u < (u-1)\log 2$, i.e., $\frac{k}{\log 2} < \frac{(u-1)}{\log u}$ (both logarithms are positive).

Since $\lim_{u \to \infty} \frac{u-1}{\log u} = \infty$, for any given k we can make $\frac{u-1}{\log u}$ as large as required. By Lemma 5.20, $2^{u-1} \leqslant \varphi_{2u}$ and the result follows.

Note: Matijasevič [8] has since given a proof that the relation $r = s^t$ is diophantine which is based on his previous work with Fibonacci numbers and does not use Theorem 5.23.

CHAPTER VI

This chapter will contain no formal mathematics. It is a series of conjectures by the author. We try to suggest how Matijasevič was led to Theorem 5.21 and what led Davis to produce his modification of Matijasevič's argument.

Julia Robinson [9,10] gave several sets of conditions which would lead to a diophantine definition of exponentiation but nowhere in her paper and article or in the paper by Davis, et al. [3], is there any mention of Fibonacci numbers.

It is hard to suggest the order of the events which led Matijasevič to his results. Firstly, it is fairly easy to see that the relation $S(u,v)$, which holds iff $v = \varphi_{2u}$, satisfies Julia Robinson's inequalities (see Theorem 5.23 and the remarks at the end of Chapter V).

We refer to the section of the theorems of Matijasevič and Davis which show that

$$\begin{bmatrix}\text{Diophantine} \\ \text{equations}\end{bmatrix} \Longrightarrow \begin{bmatrix} v = \varphi_{2u} \\ v = y_u(a)\end{bmatrix}$$

as the first part of the proof and to the converse as the second part. The basic steps of the first part of each of these theorems follow the pattern:

1) show $\ell \mid 2k+1$,

2) show $v = \varphi_{2j}$ or $v = y_j(a)$,

3) show $j = u$ using $\ell \mid 2k+1$.

Consider the first part of the theorem by Matijasevič. An important requirement to prove this was a result similar to Lemma 5.6 — certain

diophantine conditions under which $v = \varphi_{2j}$. Matijasevič noticed that for the φ_{2n} there are $2k+1$ equivalence classes mod $(\varphi_{2k} + \varphi_{2k+2})$ and that the φ_{2n} fall into these classes in a regular manner, i.e., their behaviour is similar to the integers mod n . (See Lemma 5.4 and the corollary to Lemmas 5.4 and 5.2 . It is easy to prove that the numbers φ_{2i} with $0 \leqslant i < 2k+1$ are incongruent mod $(\varphi_{2k} + \varphi_{2k+2})$. The proof is analogous to the proof of Lemma 4.4 .) This result suggested that by taking $v < \varphi_{2k+1}$, the condition $v \equiv \varphi_{2n} \bmod (\varphi_{2k} + \varphi_{2k+2})$ would force the result $v = \varphi_{2j}$ (cf. latter part of proof of Lemma 5.6). In order to obtain the condition $v \equiv \varphi_{2n} \bmod (\varphi_{2k} + \varphi_{2k+2})$, Matijasevič needed sequences (the $\Psi_{m,n}$) giving Lemmas 5.5 and 5.7 (Lemma 5.7 is needed later to show that $u = j$). We suggest how Matijasevič found such $\Psi_{m,n}$.

The φ_{2n} are the solutions for y of the Pell equation: $x^2 - 5y^2 = 4$. Consider the Pell equations: $x^2 - (m^2-4)y^2 = 4$ for $m \geqslant 3$. For each $m \geqslant 3$, the $\Psi_{m,n}$ are precisely the solutions for y of the corresponding Pell equation: $x^2 - (m^2-4)y^2 = 4$ (see [6], p. 145). (From Lemma 5.1 it is easy to see that $\Psi_{3,n} = \varphi_{2n}$.) Furthermore, for the Pell equation: $x^2 - (a^2-1)y^2 = 1$, a result analogous to Lemma 5.7 was proved by Julia Robinson [9] (here given as Lemma 4B (c)). For $m = 2$, $\Psi_{m,n} = n$ and Lemmas 5.5 and 5.7 are trivial.

The other major result necessary to prove the first part of the theorem is the result "$\ell \mid 2k+1$" and to obtain this result, Matijasevič searched for and found the corollary to Lemma 5.18 .

Finally (and essentially) by the very nature of the problem, Matijasevič had to obtain the φ_i and the $\Psi_{m,n}$ as solutions to diophantine equations to

prove the first part of the theorem. Conversely, for the second part, the φ_i and the $\Psi_{m,n}$ had to satisfy diophantine equations. This is the importance of Lemmas 5.8, 5.9, 5.10 and 5.11 . Lemma 5.8 is a well-known result (see [11], p. 11, equation (12)) and perhaps it suggested its converse (Lemma 5.9). Lemma 5.10 could be found by generalizing the result for $m = 3$ (found from Lemma 5.8) and Lemma 5.11 is the converse of Lemma 5.10 . The relationship given in Lemma 5.8 also has the property that we are able to distinguish between Fibonacci numbers of even and odd subscript, a fact which is essential in the proof of the first part of the theorem.

The second part of the theorem is relatively easy to obtain once the first part has been proved. It uses some known properties of Fibonacci numbers and relies on a clever choice of ℓ and g .

The analogies between the proofs of Matijasevič and M. Davis immediately become apparent. Julia Robinson used the Pell equation: $x^2 - (a^2 - 1)y^2 = 1$ in the proof of Theorem 5.23 . In fact she showed [9] that if the relation $v = x_u(a)$ is diophantine then exponentiation is diophantine. This, together with the previous remarks concerning Pell's equation must have suggested the modification of Matijasevič's proof to M. Davis. He found that just as Matijasevič had considered congruences mod $(\varphi_{2k} + \varphi_{2k+2})$ (i.e., mod the $k^{th} + k + 1^{th}$ solutions in y of $x^2 - 5y^2 = 4$), he could obtain similar results by considering congruences mod $\left(y_k(a) + y_{k+1}(a)\right)$ (i.e., mod the $k^{th} + k + 1^{th}$ solutions in y of $x^2 - (a^2 - 1)y^2 = 1$). Lemmas 4A, 4B, 4.1-4.7 are almost exact parallels of Lemmas 5.1-5.7, 5.14, 5.18 and the corollary to Lemma 5.18 . (The $y_n(m)$ are analogous to the $\Psi_{m,n}$ [when m is variable] and the $y_n(a)$ are

analogous to the $\varphi_{2n} = \Psi_{3,n}$ [when we consider a and m as constant]. However, in the latter case, the constant a can be any integer greater than 1 whereas the constant m has the value 3 .) However, to obtain the result "$\ell \mid 2k+1$" in the first part of his theorem and to satisfy IV a. and IV b. and get $(N',\ell) = 1$ in the second part, Davis needed to consider properties of the $y_i(a)$ for odd i .

BIBLIOGRAPHY

[1] Davis, Martin, Computability and Unsolvability. McGraw-Hill, New York, 1958.

[2] Davis, Martin, "An Explicit Diophantine Definition of the Exponential Function", Comm. Pure Appl. Math., XXIV (1971), 137-145.

[3] Davis, Martin, Putnam, Hilary, and Robinson, Julia, "The decision problem for exponential diophantine equations", Ann. of Math., 74 (1961), 425-436.

[4] Hardy, G.H., and E.M. Wright, An Introduction to the Theory of Numbers, 3rd edition. New York: Oxford University Press, 1954.

[5] Hilbert, Davis, "Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker — Kongress zu Paris 1900", Nachr. K. Ges. Wiss. Göttingen, Math. Phys. Kl. 1900, 253-297. Reprinted, Arch. Math. Phys., 3s, 1 (1901), 44-63, 213-237. English translation, Bull. Amer. Math. Soc., 8 (1901-1902), 437-479.

[6] LeVeque, William J., Topics in Number Theory, Volume 1. Addison-Wesley, Reading, Mass., 1956.

[7] Matijasevič, Ju. V., "Enumerable sets are diophantine", Dokl. Acad. Nauk SSSR, 191 (1970), 279-282. (In Russian.) (Improved) English translation, Soviet Math. Dokl., 11 (1970), 354-357.

[8] Matijasevič, Ju. V., "Diophantine representation of the set of prime numbers", Dokl. Acad. Nauk SSSR, 196 (1971), 770-773. (In Russian.) English translation, Soviet Math. Dokl., 12 (1971), 249-254.

[9] Robinson, Julia, "Existential definability in arithmetic", Trans. Amer. Math. Soc., 72 (1952), 437-449.

[10] Robinson, Julia, "Diophantine decision problems", M.A.A. Studies in Mathematics, Vol. 6 (Studies in Number Theory, edited by W.J. Leveque), (1969), 76-116.

[11] Vorob'ev, N.N., Fibonacci Numbers. Blaisdell, New York, 1961.

∞∞∞∞∞∞∞∞∞