DIOPHANTINE REPRESENTATION OF ENUMERABLE PREDICATES

Izv. Akad. Nauk SSSR
Ser. Mat. Tom 35 (1971), No. 1

Math. USSR Izvestija
Vol. 5 (1971), No. 1

DIOPHANTINE REPRESENTATION OF ENUMERABLE PREDICATES

Ju. V. MATIJASEVIČ

UDC 511

Abstract. An example is given of a diophantine relation which has exponential growth. This, together with the well-known results of Martin Davis, Hilary Putnam, and Julia Robinson, yields a proof that every enumerable predicate is diophantine. This theorem implies that Hilbert's tenth problem is algorithmically unsolvable.

Introduction

Hilbert's tenth problem was formulated in his famous lecture [1] in the following manner:

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

Today, "a process according to which it can be determined by a finite number of operations whether..." is naturally understood to mean an algorithm which solves the problem propounded. The exact concept of an algorithm was not worked out until the thirties of our century. [1)] The emergence of this concept made it theoretically possible to establish the algorithmic unsolvability of mass problems,[2)] and by now many examples of algorithmically unsolvable problems are known. In particular, Hilbert's tenth problem turns out to be unsolvable.

There cannot exist an algorithm which permits recognizing whether or not an arbitrary diophantine equation has a solution.

In the present instance it is immaterial whether we are interested in solutions in the integers (as Hilbert himself formulated the problem) or restrict ourselves to solutions in the natural numbers[3)] only. As a matter of fact, a diophantine equation is an equation of the form

---

AMS 1970 *subject classifications*. Primary 02E10, 10B99, 10N05.

1) For more detail concerning this concept see, for example, [2] or [3].

2) For more detail concerning the concept of *mass problem* see [3], Chapter V.

3) We call the positive integers natural.

$$P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n), \tag{1}$$

where P and Q are polynomials with integral coefficients. (Since all polynomials considered in this article have integral coefficients only, this property will not be specifically stipulated below.) The question of the solvability of equation (1) in the integers is equivalent, as is easily seen, to the question of the solvability of the equation

$$P(z_1 - y_1, \ldots, z_n - y_n) = Q(z_1 - y_1, \ldots, z_n - y_n)$$

in the natural numbers. Also, since every nonnegative integer is representable as a sum of four squares according to a theorem of Lagrange (see, for example, [4]), the question of the solvability of equation (1) in the natural numbers is equivalent to the question of the solvability of the equation

$$P(q_1^2 + r_1^2 + s_1^2 + t_1^2 + 1, \ldots, q_n^2 + r_n^2 + s_n^2 + t_n^2 + 1) = Q(q_1^2 + r_1^2 + s_1^2 + t_1^2 + 1, \ldots, q_n^2 + r_n^2 + s_n^2 + t_n^2 + 1)$$

in the integers.

Thus, if an algorithm which permits recognizing the solvability of an arbitrary diophantine equation in the natural numbers were possible, then an algorithm would also be possible which permits recognizing the solvability of an arbitrary diophantine equation in the integers, and conversely.

In the present article we shall restrict ourselves to considering solvability in the natural numbers. Below all lower-case Latin letters, except i and j, are used everywhere as variables for positive integers, while i and j are variables running over the nonnegative integers.

The question of what predicates[1] are *diophantine* is closely connected with Hilbert's tenth problem. By definition the predicate $\mathcal{R}(x_1, \ldots, x_n)$ is diophantine if a polynomial $R(x_1, \ldots, x_n, y_1, \ldots, y_j)$ can be found such that[2]

$$\mathcal{R}(x_1, \ldots, x_n) \Leftrightarrow \exists\, y_1 \ldots y_j [R(x_1, \ldots, x_n, y_1, \ldots, y_j) = 0]. \tag{2}$$

The relations defined by the formulas $p > q$, $p \geq q$, $p|q$, $p \equiv q \pmod m$ are examples of diophantine predicates. In fact,

$$p > q \Leftrightarrow \exists\, s[p = q + s],$$

$$p \geqslant q \Leftrightarrow \exists\, s[p = q + (s - 1)],$$

---

1) *Predicate* is the joint name for properties (which are one-place predicates) and relations (which are multiplace predicates). In the present article we consider exclusively predicates defined on the set of natural numbers.

2) The mathematical logic symbols used in this paper are read as follows: $\exists$, *there is*; $\forall$, *for all*; $\ldots \Rightarrow \ldots$, *if* $\ldots$, *then* $\ldots$; $\Leftrightarrow$, *if and only if*; &, *and*.

$$p \mid q \Leftrightarrow \exists\, s\,[ps = q],$$

$$p \equiv q \pmod{m} \Leftrightarrow \exists\, st\,[p - q = m(s - t)].$$

All diophantine predicates are *enumerable.* By definition the predicate $\mathfrak{R}(x_1, \cdots, x_n)$ is enumerable if an algorithm can be found which is applicable (i.e. which completes the task) to those and only those n-tuples of natural numbers for which the predicate $\mathfrak{R}$ is true.[1)]

The property *being a prime number* is an example of an enumerable predicate, since clearly it is possible to find an algorithm applicable to prime numbers and only to them.

Let us show that every diophantine predicate is in fact enumerable. Let $\mathfrak{R}(x_1, \cdots, x_n)$ be a diophantine predicate, and $R(x_1, \cdots, x_n, y_1, \cdots, y_j)$ its corresponding polynomial (i.e. satisfying condition (2)). Without loss of generality we shall assume $j > 0$. (Otherwise we could introduce fictitious variables.) Let us consider an algorithm which, when applied to an n-tuple of natural numbers, begins to sort out in some order all j-tuples of natural numbers until a j-tuple is found which together with the original n-tuple annihilates the polynomial R. (It is not important in the present instance just what the result of the algorithm's operation is.) According to condition (2), this algorithm is applicable to those and only those n-tuples of natural numbers for which the predicate $\mathfrak{R}$ is true.

Consequently every diophantine predicate is enumerable. The main goal of the present paper is to show that the converse assertion, formulated in the following manner, is also valid:

Basic Theorem. *Every enumerable predicate is diophantine.*

Thus the property *being an enumerable predicate,* which has an algorithmic character, coincides with the property *being a diophantine predicate,* which has an arithmetical character.

That Hilbert's tenth problem is algorithmically unsolvable follows immediately from the basic theorem. Indeed, let $\mathfrak{R}(x_1, \cdots, x_n)$ be an enumerable, but not a solvable, predicate, i.e. one for which there cannot exist an algorithm which recognizes those and only those n-tuples for which the predicate $\mathfrak{R}$ is true.[2)] According to the basic theorem, the predicate $\mathfrak{R}$ is diophantine; so let R be a polynomial satisfying condition (2). Then an algorithm is impossible which permits recognizing the solvability of an arbitrary equation of the form

$$R(a_1, \ldots, a_n, y_1, \ldots, y_j) = 0,$$

1) We are citing only one of the possible equivalent definitions. For more detail concerning enumerable predicates see, for example, [2].

2) The theorem on the existence of such predicates is one of the fundamental results in the theory of algorithms. For its proof see, for example, [2].

where $a_1, \cdots, a_n$ are parameters. All the more, therefore, it is impossible to have the algorithm required in Hilbert's tenth problem which permits recognizing the solvability of an arbitrary diophantine equation.

Our proof of the basic theorem combines the result of several mathematicians' efforts. Below (in §1) we give a short review of several results obtained earlier which are closely connected with the basic theorem.

§1. Reduction of the basic theorem and corollaries of it

The conjecture that every countable predicate is diophantine was apparently first stated by Martin Davis. In [5] he was forced to leave this supposition open; however, a close result was obtained there. That is, Davis showed in [5] that *every enumerable predicate* $\mathcal{R}(x_1, \cdots, x_n)$ *is representable in the form*

$$\mathcal{R}(x_1, \ldots, x_n) \Leftrightarrow \exists w \forall z_{\leqslant w} \exists y_1 \ldots y_j [R(x_1, \ldots, x_n, w, z, y_1, \ldots, y_j) = 0], \quad (1)$$

where R *is a polynomial.*[1)]

Using this representation, Davis, Hilary Putnam, and Julia Robinson proved in [6] that *an arbitrary enumerable predicate* $\mathcal{R}(x_1, \cdots, x_n)$ *can be represented in the form*

$$\mathcal{R}(x_1, \ldots, x_n) \Leftrightarrow \exists y_1 \ldots y_j [P(x_1, \ldots, x_n, y_1, \ldots, y_j) = Q(x_1, \ldots, x_n, y_1, \ldots, y_j)]. \quad (2)$$

Here P *and* Q *are functions constructed by superposing addition, multiplication, raising to a power, and specific natural numbers.*

The equation in the right side of (2) is called *exponential diophantine.* It is not difficult to understand that by introducing additional variables, we can transform an arbitrary exponential diophantine equation into a system of equations which is equivalent to it[2)] and each of whose equations has the form $a = b + c$, $a = bc$, or $a = b^c$, where a, b and c are variables or concrete natural numbers. Let us assume that $A(q, p, k, z_1, \cdots, z_n)$ is a polynomial such that the equivalence

$$q = p^k \Leftrightarrow \exists z_1 \ldots z_m [A(q, p, k, z_1, \ldots, z_m) = 0] \quad (3)$$

is valid, and let us replace each equation of the form $a = b^c$ with a copy of the diophantine equation in the right side of (3) (substituting appropriate variables or specific numbers for q, p and k, and each time choosing new variables as $z_1, \cdots, z_m$). We obtain as the result a system of diophantine equations which is equivalent to the ori-

1) Strictly speaking, this result was formulated in Davis' paper for the case when all variables run over the set of nonnegative integers. However, this difference is not an essential one. To obtain representation (1), it is sufficient to take the analogous Davis representation and everywhere in the polynomial replace w, z, $y_1, \cdots, y_j$ by $w - 1$, $z - 1$, $y_1 - 1, \cdots, y_j - 1$, respectively.

2) We call two systems of equations equivalent if the solvability of either one implies the solvability of the other.

ginal exponential diophantine equation. It is clear that an arbitrary system of diophantine equations

$$S_l = T_l \quad (l = 1, \ldots, a)$$

is equivalent to the single diophantine equation

$$\sum_{l=1}^{a} (S_l - T_l)^2 = 0.$$

Thus, according to the result of Davis, Putnam and Robinson to which we referred above, in order to prove that every enumerable predicate is diophantine, it is sufficient to establish that the relation defined by the formula

$$q = p^k \tag{4}$$

is diophantine.

In [7] Julia Robinson investigated the question of whether or not relation (4) is diophantine. There she found several conditions sufficient for relation (4) to be diophantine. In particular, the following result was obtained in [7]: *relation* (4) *is diophantine if there exists a diophantine relation* $\mathfrak{D}(u, v)$ *which possesses the following properties*:[1)]

$$\forall uv[\mathfrak{D}(u, v) \Rightarrow v \leqslant u^u], \tag{5}$$

$$\forall k \exists uv[\mathfrak{D}(u, v) \& v > u^k]. \tag{6}$$

A relation $\mathfrak{D}(u, v)$ possessing properties (5) and (6) is said to have *exponential growth*.

The first example of a diophantine relation having exponential growth was published in the short note [9].[2)] Thus in principle and thereby the proof of the basic theorem was completed in that paper. A detailed account of the results of [9] is given below (in §2).[3)]

We consider several corollaries of the basic theorem in the last part of this section.

As we indicated in the Introduction, the predicate $\mathfrak{R}(x_1, \ldots, x_n)$ is called diophantine if it is possible to find a polynomial $R(x_1, \ldots, x_n, y_1, \ldots, y_j)$ such that

---

1) In [7] the inequalities have the form $v < u^u$ and $v \geq u^k$; however, as is easily shown, this difference is not essential. See also [8].

2) The results set forth in [9] were first announced on January 29, 1970, at the Leningrad Seminar on Constructive Mathematics (a joint seminar of the Leningrad Branch of the Steklov Institute of Mathematics and Leningrad State University).

3) Although the proof cited in §2 is based on the same ideas as outlined in [9], it differs in many technical details and is on the whole simpler. (C. V. Čudnovskiĭ published another example of a diophantine predicate having exponential growth in Uspehi Mat. Nauk 25 (1970), no. 4 (154), 185–186.)

$$\mathscr{R}(x_1, \ldots, x_n) \Leftrightarrow \exists y_1 \ldots y_j [R(x_1, \ldots, x_n, y_1, \ldots, y_j) = 0]. \tag{7}$$

The diophantine equation in the right side of (7)

$$R(x_1, \ldots, x_n, y_1, \ldots, y_j) = 0 \tag{8}$$

actually has a general form. (An equation of the form $P = Q$ is reduced to form (8) by transferring all terms to the left side.) However, it is possible to impose additional restrictions on the form of this equation without, in spite of this, diminishing the extent of the concept *diophantine predicate.*

First of all, we can restrict ourselves to polynomials of no more than fourth degree in representation (7). Indeed, every diophantine equation is equivalent to a system of equations each of which has the form $a = b + c$ or $a = bc$. Transforming this system into a single diophantine equation by the method described above, we obtain a polynomial of not more than fourth degree. Let us note yet another property of this polynomial which is important for us: it takes only nonnegative values.

The following interesting result concerning the representation of one-place diophantine predicates was obtained by Hilary Putnam in [10]. Let $\mathscr{C}(x)$ be a one-place diophantine predicate, and let S be a polynomial such that

$$\mathscr{C}(x) \Leftrightarrow \exists y_1 \ldots y_j [S(x, y_1, \ldots, y_j) = 0].$$

As was shown above, we can assume that S takes only nonnegative values, while its degree is not higher than the fourth. Let us show that the following equivalence holds:

$$S(a, y_1, \ldots, y_j) = 0 \Leftrightarrow \exists y_0 [a = y_0(1 - S(y_0, \ldots, y_j))]. \tag{9}$$

It is clear that if the numbers $a, y_1, \cdots, y_j$ are such that

$$S(a, y_1, \ldots, y_j) = 0, \tag{10}$$

then the equality

$$a = y_0(1 - S(y_0, \ldots, y_j)) \tag{11}$$

is valid for $y_0 = a$. Now let the numbers $a, y_0, \cdots, y_j$ satisfy equality (11). Since $a > 0$ and $y_0 > 0$,

$$1 - S(y_0, \ldots, y_j) > 0. \tag{12}$$

But since the polynomial S does not take negative values, inequality (12) is possible only if $S(y_0, \cdots, y_j) = 0$. Hence (11) implies $y_0 = a$, and hence equality (10) is fulfilled.

According to (9), every one-place diophantine predicate $\mathscr{C}$ is representable in the form

$$\mathscr{C}(x) \Leftrightarrow \exists y_0 \ldots y_j [x = T(y_0, \ldots, y_j)], \tag{13}$$

where T is a polynomial of not more than the fifth degree.

Combining this result of Putnam with our basic theorem, we obtain this corollary:

every one-place enumerable predicate $\mathcal{C}$ *is representable in the form* (13).

If the property *being a prime number* is taken as $\mathcal{C}$, we obtain the fact that the set of all prime numbers coincides with the set of all positive values of some fifth degree polynomial with integral coefficients (the variables taking natural values).

Putnam's result permits various generalizations to the case of multiplace predicates. One of these is connected with the use of so-called *pairing functions*.

Let us denote by $D_2(x_1, x_2)$ the polynomial $(x_1 + x_2)^2 + x_1$. Since

$$(x_1 + x_2)^2 < (x_1 + x_2)^2 + x_1 = D_2(x_1, x_2) < (x_1 + x_2)^2 + 2x_1 + 2x_2 + 1 = (x_1 + x_2 + 1)^2,$$

we have

$$x_1 + x_2 = [\sqrt{D_2(x_1, x_2)}],$$

where the square brackets are used, as usual, to denote the integer part of the number. Hence

$$x_1 = D_2(x_1, x_2) - [\sqrt{D_2(x_1, x_2)}]^2,$$
$$x_2 = [\sqrt{D_2(x_1, x_2)}] - x_1.$$

Consequently the polynomial D_2 possesses the following property:

$$D_2(a_1, a_2) = D_2(b_1, b_2) \Rightarrow (a_1 = b_1 \,\&\, a_2 = b_2).$$

Polynomials in a large number of variables which possess this property can be defined by induction:

$$D_{k+1}(x_1, \ldots, x_{k+1}) = D_2(D_k(x_1, \ldots, x_k), x_{k+1}) \quad (k = 2, 3, \ldots).$$

Let $\mathcal{R}(x_1, \cdots, x_n)$ be an arbitrary diophantine relation, and let R be a polynomial satisfying condition (7). It is clear that

$$\mathcal{R}(x_1, \ldots, x_n) \Leftrightarrow \exists z_1 \ldots z_n\, y_1 \ldots y_j [(R(z_1, \ldots, z_n, y_1, \ldots, y_j))^2 + (D_n(x_1, \ldots, x_n) - D_n(z_1, \ldots, z_n))^2 = 0].$$

Introducing yet another variable and performing the same transformation as in the case of a one-place predicate, we obtain a representation of the relation $\mathcal{R}$ in the form

$$\mathcal{R}(x_1, \ldots, x_n) \Leftrightarrow \exists t_1 \ldots t_k [Q(t_1, \ldots, t_k) = D_n(x_1, \ldots, x_n)], \quad (14)$$

where Q is a polynomial. Combining this result with our basic theorem, we obtain this corollary: *every enumerable relation* $\mathcal{R}(x_1, \cdots, x_n)$ *is representable in the form* (14).

Another interesting representation can be given for enumerable relations which are representable in the form $p = F(q_1, \cdots, q_n)$, where F is a function. Using Putnam's

method, we can pass from a representation in the form of (7) to a representation in the form

$$p = F(q_1, \ldots, q_n) \Leftrightarrow \exists\, y_1 \ldots y_j [p = R(q_1, \ldots, q_n, y_1, \ldots, y_j)],$$

where R is a polynomial.

For example, the relation p *is the kth prime number* is an enumerable relation. Consequently it is possible to find a polynomial $P(k, y_1, \ldots, y_s)$ with integral coefficients which for any fixed value k and arbitrary values of the remaining variables takes exactly one positive value, and this value is the kth prime number.

§2. Example of a diophantine relation having exponential growth

The example cited below of a diophantine relation having exponential growth was constructed on the basis of well-known properties of the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots.$$

This sequence is defined by the following relationships:

$$\varphi_0 = 0, \quad \varphi_1 = 1, \tag{1}$$

$$\varphi_{j+1} = \varphi_j + \varphi_{j-1} \quad (j = 1, 2, \ldots). \tag{2}$$

We shall show that the relation defined by the formula

$$v = \phi_{2u} \tag{3}$$

is diophantine and has exponential growth.

Let us outline the plan of the proof. The sequence of Fibonacci numbers with even indices

$$0, 1, 3, 8, 21, 55, 144, \ldots \tag{4}$$

satisfied the following relationships:

$$\varphi_0 = 0, \quad \varphi_2 = 1, \quad \varphi_{2(k+1)} = 3\varphi_{2k} - \varphi_{2(k-1)}. \tag{5}$$

Hence it is possible to deduce that

$$2^{u-1} \leqslant \varphi_{2u} < 3^u.$$

Using these inequalities, it is not difficult to show that relation (3) in fact has exponential growth.

In order to show that relation (3) is diophantine, we consider a series of sequences defined for every $m \geq 2$ by the following relationships:

$$\psi_{m,0} = 0, \quad \psi_{m,1} = 1, \quad \psi_{m,k+1} = m\psi_{m,k} - \psi_{m,k-1}. \tag{6}$$

(Comparing (5) and (6), we see that sequence (4) enters into this series; namely,

$\phi_{2j} = \psi_{3,j}$.) The numbers $\psi_{m,n}$ possess the following two properties which are important for us:

$$\psi_{m,j} \equiv j \pmod{m-2}, \tag{7}$$

$$\psi_{m,j} \equiv \varphi_{2j} \pmod{m-3}. \tag{8}$$

We show that adjacent terms of the sequence $\psi_{m,n}$, and only they, are solutions of the equation

$$x^2 - mxy + y^2 = 1.$$

Therefore, if $v = \phi_{2u}$ and the numbers d, l and m are such that

$$l \mid m-2, \tag{9}$$

$$d \mid m-3, \tag{10}$$

then it is possible to find numbers x and y such that

$$x^2 - mxy + y^2 = 1, \tag{11}$$

$$u \equiv x \pmod{l}, \tag{12}$$

$$v \equiv x \pmod{d}. \tag{13}$$

We impose additional restrictions (each of which either has the form of a diophantine equation or is easily reduced to that form) on the numbers u, v, l and d so that these additional conditions and conditions (9)–(13) imply $v = \phi_{2u}$.

First we prove a series of lemmas concerning properties of the numbers ϕ_n and $\psi_{m,n}$.

Lemma 1. $1 = \phi_1 = \phi_2 < \phi_3 < \cdots < \phi_n < \cdots$.

It is clear that this lemma follows immediately from the relationships defined in (1) and (2).

Let us extend the sequence of Fibonacci numbers by setting

$$\phi_{-1} = 1. \tag{14}$$

It is easy to verify that recursive relationship (2) is valid for also $j = 0$.

Φ_j denotes the matrix[1]

$$\begin{pmatrix} \varphi_{j-1} & \varphi_j \\ \varphi_j & \varphi_{j+1} \end{pmatrix}.$$

We denote by Ξ the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

1) Recall that, unlike the remaining lower-case Latin letters, the letters i and j are variables for nonnegative integers.

Lemma 2. *For any* j

$$\Phi_j = \Xi^j. \tag{15}$$

The proof is carried out by induction on j.

Case $j = 0$. According to (1) and (14), we have

$$\Phi_0 = \begin{pmatrix} \varphi_{-1} & \varphi_0 \\ \varphi_0 & \varphi_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \Xi^0.$$

Induction Step. Assume that equality (15) is valid for some j. Then, according to (2) and the induction hypothesis,

$$\Phi_{j+1} = \begin{pmatrix} \varphi_j & \varphi_{j+1} \\ \varphi_{j+1} & \varphi_{j+2} \end{pmatrix} = \begin{pmatrix} \varphi_j & \varphi_j + \varphi_{j-1} \\ \varphi_{j+1} & \varphi_{j+1} + \varphi_j \end{pmatrix}$$
$$= \begin{pmatrix} \varphi_{j-1} & \varphi_j \\ \varphi_j & \varphi_{j+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \Phi_j \Xi = \Xi^{j+1}.$$

The lemma is proved.

Lemma 3. *For any* i *and* j,

$$\Phi_{i+j} = \Phi_i \Phi_j, \quad \Phi_{ij} = \Phi_i^j.$$

Proof. Let i and j be arbitrary nonnegative integers. According to Lemma 2,

$$\Phi_{i+j} = \Xi^{i+j} = \Xi^i \Xi^j = \Phi_i \Phi_j,$$
$$\Phi_{ij} = \Xi^{ij} = (\Xi^i)^j = \Phi_i^j.$$

The lemma is proved.

Lemma 4. *For any* j

$$\det \Phi_j = (-1)^j.$$

Proof. Let j be a number. According to Lemma 2,

$$\det \Phi_j = \det \Xi^j = (\det \Xi)^j = (-1)^j.$$

The lemma is proved.

Lemma 5. *For any* j

$$\varphi_{j+1}^2 - \varphi_j \varphi_{j+1} - \varphi_j^2 = (-1)^j.$$

Proof. Let j be a number. According to (2),

$$\Phi_j = \begin{pmatrix} \varphi_{j-1} & \varphi_j \\ \varphi_j & \varphi_{j+1} \end{pmatrix} = \begin{pmatrix} \varphi_{j+1} - \varphi_j & \varphi_j \\ \varphi_j & \varphi_{j+1} \end{pmatrix}.$$

Consequently

$$\varphi_{j+1}^2 - \varphi_j\varphi_{j+1} - \varphi_j^2 = \det \Phi_j.$$

It remains to apply Lemma 4. The lemma is proved.

Notation of the form

$$\begin{pmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{pmatrix} \equiv \begin{pmatrix}\beta_{11} & \beta_{12}\\ \beta_{21} & \beta_{22}\end{pmatrix} \pmod s,$$

where α_{ij}, β_{ij} and s are integers, denotes that $\alpha_{ij} \equiv \beta_{ij} \pmod s$ $(i, j = 1, 2)$.

It is not difficult to verify that one can operate with matrix congruences exactly as with the usual ones, i.e. one can add them, multiply them, etc., termwise.

Lemma 6. *For any numbers i, j and s*

$$\varphi_{is+j} \equiv \varphi_j\varphi_{s+1}^i \pmod{\varphi_s}.$$

Proof. Let i, j and s be numbers. According to Lemma 3, $\Phi_{is+j} = \Phi_j\Phi_s^i$. Passing from this equality to congruence modulo ϕ_s, we obtain

$$\begin{pmatrix}\varphi_{is+j-1} & \varphi_{is+j}\\ \varphi_{is+j} & \varphi_{is+j+1}\end{pmatrix} \equiv \begin{pmatrix}\varphi_{j-1} & \varphi_j\\ \varphi_j & \varphi_{j+1}\end{pmatrix}\begin{pmatrix}\varphi_{s-1} & 0\\ 0 & \varphi_{s+1}\end{pmatrix}^i \pmod{\varphi_s}.$$

Hence $\phi_{is+j} \equiv \phi_j\phi_{s+1}^i \pmod{\phi_s}$.

The lemma is proved.

Lemma 7. *For any numbers s and q, if $\phi_s > 1$ and $\phi_s | \phi_q$, then $s | q$.*

Proof. Let s and q be numbers satisfying the lemma's conditions. Let us represent q in the form $is + j$, where $j < s$. According to Lemma 6,

$$\varphi_q \equiv \varphi_{is+j} \equiv \varphi_j\varphi_{s+1}^i \pmod{\varphi_s}$$

and therefore $\phi_s | \phi_j\phi_{s+1}^i$. Lemma 5 implies that ϕ_s and ϕ_{s+1} are relatively prime; consequently $\phi_s | \phi_j$. According to Lemma 1, this implies $j = 0$. The lemma is proved.

Lemma 8. *For any s and t,*

$$\varphi_{st} \equiv t\varphi_s\varphi_{s+1}^{t-1} \pmod{\varphi_s^2}.$$

Proof. Let s and t be natural numbers. According to Lemma 3,

$$\begin{pmatrix}\varphi_{st-1} & \varphi_{st}\\ \varphi_{st} & \varphi_{st+1}\end{pmatrix} = \begin{pmatrix}\varphi_{s-1} & \varphi_s\\ \varphi_s & \varphi_{s+1}\end{pmatrix}^t = \left\{\varphi_s\begin{pmatrix}-1 & 1\\ 1 & 0\end{pmatrix} + \begin{pmatrix}\varphi_{s+1} & 0\\ 0 & \varphi_{s+1}\end{pmatrix}\right\}^t$$

$$= \sum_{j=0}^{t} C_t^j\varphi_s^j\begin{pmatrix}-1 & 1\\ 1 & 0\end{pmatrix}^j\begin{pmatrix}\varphi_{s+1} & 0\\ 0 & \varphi_{s+1}\end{pmatrix}^{t-j}, \tag{16}$$

where, as usual,

$$C_t^j = \frac{t(t-1)\dots(t-j+1)}{1\cdot 2\cdots j}.$$

Passing from equality (16) to congruence modulo ϕ_s^2, we can drop all terms except the first two in the sum in the right side. Thus

$$\begin{pmatrix} \varphi_{st-1} & \varphi_{st} \\ \varphi_{st} & \varphi_{st+1} \end{pmatrix} \equiv \begin{pmatrix} \varphi_{s+1}^t & 0 \\ 0 & \varphi_{s+1}^t \end{pmatrix} + t\varphi_s \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \varphi_{s+1}^{t-1} & 0 \\ 0 & \varphi_{s+1}^{t-1} \end{pmatrix} \pmod{\varphi_s^2}.$$

Hence

$$\varphi_{st} \equiv t\varphi_s\varphi_{s+1}^{t-1} \pmod{\varphi_s^2}.$$

The lemma is proved.

Lemma 9. *For any numbers s and t, if $\phi_s | t$, then $\phi_s^2 | \phi_{st}$.*

Proof. Let s and t be numbers satisfying the lemma's condition. By Lemma 8

$$\varphi_{st} \equiv t\varphi_s\varphi_{s+1}^{t-1} \pmod{\varphi_s^2};$$

consequently $\phi_s^2 | \phi_{st}$. The lemma is proved.

Lemma 10. *For any numbers s and q, if $\phi_s^2 | \phi_q$, then $\phi_s | q$.*

Proof. Let s and q be numbers satisfying the lemma's condition. If $\phi_s = 1$, the conclusion is true. Therefore in what follows we shall assume $\phi_s > 1$.

According to Lemma 7, $s | q$. Let us represent q in the form st. According to Lemma 8,

$$\varphi_q \equiv \varphi_{st} \equiv t\varphi_s\varphi_{s+1}^{t-1} \pmod{\varphi_s^2};$$

consequently $\phi_s | t\phi_{s+1}^{t-1}$. But according to Lemma 5 the numbers ϕ_s and ϕ_{s+1} are relatively prime. Consequently $\phi_s | t$, and therefore $\phi_s | q$. The lemma is proved.

Lemma 11. *For any k,*

$$\Phi_{2(2k+1)} \equiv \mathrm{E} \pmod{\varphi_{2k} + \varphi_{2k+2}},$$

where E *is the unit matrix.*

Proof. Let k be a number. According to Lemma 4,

$$\Phi_{2k}^{-1} = \begin{pmatrix} \varphi_{2k+1} & -\varphi_{2k} \\ -\varphi_{2k} & \varphi_{2k-1} \end{pmatrix}. \tag{17}$$

According to (2),

$$\varphi_{2k-1} = \varphi_{2k+1} - \varphi_{2k} = \varphi_{2k+2} - 2\varphi_{2k};$$

consequently

$$\begin{pmatrix} \varphi_{2k+1} & -\varphi_{2k} \\ -\varphi_{2k} & \varphi_{2k-1} \end{pmatrix} = \begin{pmatrix} \varphi_{2k+1} & -\varphi_{2k} \\ -\varphi_{2k} & \varphi_{2k+2} - 2\varphi_{2k} \end{pmatrix}. \tag{18}$$

Since

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

we have

$$\begin{pmatrix} \varphi_{2k+1} & -\varphi_{2k} \\ -\varphi_{2k} & \varphi_{2k+2} - 2\varphi_{2k} \end{pmatrix} \equiv \begin{pmatrix} \varphi_{2k+1} & \varphi_{2k+2} \\ \varphi_{2k+2} & 2\varphi_{2k+2} - \varphi_{2k} \end{pmatrix} \pmod{\varphi_{2k} + \varphi_{2k+2}}. \tag{19}$$

According to (2),

$$2\varphi_{2k+2} - \varphi_{2k} = \varphi_{2k+2} + \varphi_{2k+1} = \varphi_{2k+3};$$

consequently

$$\begin{pmatrix} \varphi_{2k+1} & \varphi_{2k+2} \\ \varphi_{2k+2} & 2\varphi_{2k+2} - \varphi_{2k} \end{pmatrix} = \begin{pmatrix} \varphi_{2k+1} & \varphi_{2k+2} \\ \varphi_{2k+2} & \varphi_{2k+3} \end{pmatrix}. \tag{20}$$

From (17)–(20) it follows that

$$\Phi_{2k}^{-1} \equiv \Phi_{2k+2} \pmod{\varphi_{2k} + \varphi_{2k+2}}. \tag{21}$$

According to Lemma 3,

$$\Phi_{2(2k+1)} = \Phi_{2k+2k+2} = \Phi_{2k}\Phi_{2k+2};$$

so, according to (21),

$$\Phi_{2(2k+1)} \equiv \mathrm{E} \pmod{\varphi_{2k} + \varphi_{2k+2}}.$$

The lemma is proved.

Lemma 12. *For any numbers i, j and k,*

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

Proof. Let i, j and k be numbers. According to Lemmas 3 and 11,

$$\Phi_{2((2k+1)i+j)} \equiv \Phi_{2(2k+1)}^{i}\Phi_{2j} \equiv \Phi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}.$$

Hence

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

The lemma is proved.

Lemma 13. *For any numbers j and k, if $j \leq 2k + 1$, then*

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

Proof. Let j and k be numbers satisfying the lemma's conditions. According to Lemma 2,

$$\Phi_{2(2k+1-j)} = \Xi^{2(2k+1-j)} = \Xi^{2(2k+1)}\Xi^{-2j} = \Phi_{2(2k+1)}\Phi_{2j}^{-1}.$$

Hence, according to Lemma 11,

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

According to Lemma 4,

$$\Phi_{2j}^{-1} = \begin{pmatrix} \varphi_{2j+1} & -\varphi_{2j} \\ -\varphi_{2j} & \varphi_{2j-1} \end{pmatrix};$$

consequently

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

The lemma is proved.

Lemma 14. *For any j and $m \geq 2$,*

$$\psi_{m,j+1} > \psi_{m,j} \geqslant 0. \tag{22}$$

The proof is carried out by induction on j.

Case $j = 0$. According to (6), for any $m \geq 2$ we have

$$\psi_{m,1} = 1 > 0 = \psi_{m,0}.$$

Induction Step. Assume that inequality (22) is valid for some numbers j and $m \geq 2$. According to (6) and the induction hypothesis, we have

$$\psi_{m,j+2} = m\psi_{m,j+1} - \psi_{m,j} \geqslant \psi_{m,j+1} + (\psi_{m,j+1} - \psi_{m,j}) > \psi_{m,j+1} > 0.$$

The lemma is proved.

Lemma 15. *For any n and $m \geq 2$,*

$$(m-1)^{n-1} \leqslant \psi_{m,n} < m^n. \tag{23}$$

The proof is carried out by induction on n.

Case $n = 1$. According to (6), for any $m \geq 2$

$$(m-1)^0 = 1 = \psi_{m,1} < 2 \leqslant m^1.$$

Induction Step. Assume that inequality (23) is valid for some numbers n and $m \geq 2$. Then, according to (6), Lemma 14 and the induction hypothesis,

$$\begin{gathered} \psi_{m,n+1} = m\psi_{m,n} - \psi_{m,n-1} = (m-1)\,\psi_{m,n} + (\psi_{m,n} - \psi_{m,n-1}) \\ > (m-1)\,\psi_{m,n} \geqslant (m-1)^n, \\ \psi_{m,n+1} = m\psi_{m,n} - \psi_{m,n-1} \leqslant m\psi_{m,n} < m^{n+1}. \end{gathered} \tag{24}$$

The lemma is proved.

Lemma 16. *For any* j,

$$\psi_{3,j} = \varphi_{2j}. \tag{24}$$

The proof is carried out by induction on j.

Cases $j = 0$ and $j = 1$. According to (1) and (6),

$$\psi_{3,0} = 0 = \varphi_0, \quad \psi_{3,1} = 1 = \varphi_2.$$

Induction Step. Assume that equality (24) holds for all j not greater than some number n. According to (2), (6) and the induction hypothesis,

$$\psi_{3,n+1} = 3\psi_{3,n} - \psi_{3,n-1} = 3\varphi_{2n} - \varphi_{2n-2} = 2\varphi_{2n} + \varphi_{2n-1} = \varphi_{2n} + \varphi_{2n+1} = \varphi_{2n+2}.$$

The lemma is proved.

Lemma 17. *For any* j *and* $m \geq 2$,

$$\psi_{m,j}^2 - m\psi_{m,j}\psi_{m,j+1} + \psi_{m,j+1}^2 = 1. \tag{25}$$

The proof is carried out by induction on j.[1)]

Case $j = 0$. According to (6), for any $m \geq 2$

$$\psi_{m,0}^2 - m\psi_{m,0}\psi_{m,1} + \psi_{m,1}^2 = 0^2 - m \cdot 0 \cdot 1 + 1^2 = 1.$$

Induction Step. Assume that equality (25) is valid for some numbers j and $m \geq 2$. According to (6) and the induction hypothesis,

$$\begin{aligned}\psi_{m,j+1}^2 - m\psi_{m,j+1}\psi_{m,j+2} + \psi_{m,j+2}^2 &= \psi_{m,j+1}^2 - m\psi_{m,j+1}(m\psi_{m,j+1} - \psi_{m,j}) \\ &+ (m\psi_{m,j+1} - \psi_{m,j})^2 = \psi_{m,j+1}^2 - m^2\psi_{m,j+1}^2 + m\psi_{m,j}\psi_{m,j+1} + m^2\psi_{m,j+1}^2 \\ &- 2m\psi_{m,j}\psi_{m,j+1} + \psi_{m,j}^2 = \psi_{m,j}^2 - m\psi_{m,j}\psi_{m,j+1} + \psi_{m,j+1}^2 = 1.\end{aligned}$$

The lemma is proved.

Lemma 18. *For any numbers* j, k *and* $m \geq 2$, *if*

$$j^2 - mjk + k^2 = 1 \tag{26}$$

and

$$j \leqslant k, \tag{27}$$

then it is possible to find a number i *such that* $j = \psi_{m,i}$ *and* $k = \psi_{m,i+1}$.

The proof is carried out by recursive induction on j.

Let j, k and m be numbers satisfying the lemma's conditions.

If $j = 0$, then $k = 1$ according to (26), i.e. $j = \psi_{m,0}$ and $k = \psi_{m,1}$.

Therefore in what follows we assume that

1) This lemma can also be proved by a method analogous to the one applied to Lemma 5 if congruent matrices are taken into consideration. However, we shall not introduce these matrices since we do not need them for any other purpose.

$$j > 0 \tag{28}$$

According to (26) and (27),

$$k(k - mj + j) = k^2 - mjk + jk = 1 - j^2 + jk = 1 + j(k - j) > 0;$$

consequently

$$j > mj - k. \tag{29}$$

From (26) and (28) it follows that

$$k(mj - k) = mjk - k^2 = j^2 - 1 \geqslant 0; \tag{29}$$

consequently

$$mj - k \geqslant 0. \tag{30}$$

Let us set $j_1 = mj - k$ and $k_1 = j$. According to (29) and (30),

$$0 \leqslant j_1 < k_1. \tag{31}$$

By virtue of (26),

$$\begin{aligned} j_1^2 - mj_1k_1 + k_1^2 &= (mj - k)^2 - m(mj - k)j + j^2 \\ &= m^2j^2 - 2mjk + k^2 - m^2j^2 + mjk + j^2 = j^2 - mjk + k^2 = 1. \end{aligned} \tag{32}$$

Since $j_1 < j$ according to (29), by the induction hypothesis (31) and (32) imply that it is possible to find a number i for which

$$j_1 = \psi_{m,i}, \quad k_1 = \psi_{m,i+1}.$$

Then, according to (6),

$$\begin{aligned} j &= \psi_{m,i+1}, \\ k &= mj - j_1 = m\psi_{m,i+1} - \psi_{m,i} = \psi_{m,(i+1)+1}. \end{aligned}$$

The lemma is proved.

Lemma 19. *For any j and k, if $k^2 - jk - j^2 = 1$, then it is possible to find a number i such that $j = \phi_{2i}$ and $k = \phi_{2i+1}$.*

Proof. Let j and k be numbers satisfying the lemma's condition. Then

$$j^2 - 3j(j + k) + (j + k)^2 = j^2 - 3j^2 - 3jk + j^2 + 2jk + k^2 = k^2 - jk - j^2 = 1.$$

According to Lemma 18, this implies that it is possible to find a number i such that

$$j = \psi_{3,i}, \quad j + k = \psi_{3,i+1}.$$

But then, according to Lemma 16,

$$j = \varphi_{2i}, \quad k = \varphi_{2i+2} - \varphi_{2i} = \varphi_{2i+1}.$$

The lemma is proved.

Lemma 20. *For any* j

$$\psi_{2,j} = j. \tag{33}$$

The proof is carried out by induction on j. For $j = 0$ and $j = 1$ equality (33) follows from (6).

Induction Step. Assume that equality (33) is valid for all j not greater than some number n. Then according to (6) and the induction hypothesis,

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

The lemma is proved.

Lemma 21. *For any numbers* $a \geq 2$, $m \geq 2$ *and* j,

$$\psi_{m,j} \equiv \psi_{a,j} \pmod{m-a}. \tag{34}$$

The proof is carried out by induction on j.

Cases $j = 0$ **and** $j = 1$. According to (6), in these cases $\psi_{m,j} = \psi_{a,j}$ for any $a \geq 2$ and $m \geq 2$; therefore condition (34) is fulfilled.

Induction Step. Assume that congruence (34) holds for some $a \geq 2$ and $m \geq 2$, and all j not greater than some n. Then, according to (6) and the induction hypothesis,

$$\psi_{m,n+1} \equiv m\psi_{m,n} - \psi_{m,n-1} \equiv a\psi_{a,n} - \psi_{a,n-1} \equiv \psi_{a,n+1} \pmod{m-a}.$$

The lemma is proved.

Lemma 22. *For any numbers* l, j *and* $m \geq 2$, *if* $l \mid m-2$, *then* $\psi_{m,j} \equiv j \pmod{l}$; *for any numbers* d, j *and* $m \geq 2$, *if* $d \mid m-3$, *then* $\psi_{m,j} \equiv \phi_{2j} \pmod{d}$.

It is clear that this lemma is an immediate consequence of Lemmas 21, 20 and 16.

Theorem 1. *For any natural numbers* u *and* v, *in order that the equation* $v = \phi_{2u}$ *hold, it is necessary and sufficient that there exist natural numbers* l, g, h, m, x, y *and* z *such that*

$$u < l, \tag{35}$$

$$v < l, \tag{36}$$

$$l^2 - lz - z^2 = 1, \tag{37}$$

$$g^2 - gh - h^2 = 1, \tag{38}$$

$$l^2 \mid g, \tag{39}$$

$$l \mid m-2, \tag{40}$$

$$2h + g \mid m-3, \tag{41}$$

$$x^2 - mxy + y^2 = 1, \tag{42}$$

$$l \mid x-u, \tag{43}$$

$$2h + g \mid x-v. \tag{44}$$

Sufficiency. Let the numbers u, v, l, g, h, m, x, y and z satisfy conditions (35)–(44). According to Lemma 19, (37) and (38) imply

$$l = \varphi_s, \tag{45}$$

$$g = \varphi_{2k+1}, \quad h = \varphi_{2k} \tag{46}$$

for some numbers k and s. Hence according to (2) we have

$$2h + g = 2\varphi_{2k} + \varphi_{2k+1} = \varphi_{2k} + \varphi_{2k+2}. \tag{47}$$

According to Lemma 10, the fact that

$$l \mid 2k + 1 \tag{48}$$

follows from (39), (45) and (46).

$l \geq 2$ follows from (35). This and (40) imply

$$m \geqslant 2. \tag{49}$$

According to Lemma 18, the equality

$$x = \psi_{m,n} \tag{50}$$

for some number n follows from (49) and (42).

According to Lemma 22, the congruence

$$x \equiv \varphi_{2n} \pmod{\varphi_{2k} + \varphi_{2k+2}} \tag{51}$$

follows from (49), (41), (50) and (47). This and (44) imply

$$v \equiv \varphi_{2n} \pmod{\varphi_{2k} + \varphi_{2k+2}}. \tag{52}$$

Let us represent the number n in the form $(2k + 1)i + j$, where

$$0 \leqslant j < 2k + 1. \tag{53}$$

According to Lemma 12,

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

This and (52) imply

$$v \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}. \tag{54}$$

According to (39), $l \leq g$; this, (36), and (46) imply

$$v < g = \varphi_{2k+1}; \tag{55}$$

consequently

$$v < \varphi_{2k} + \varphi_{2k+2}. \tag{56}$$

According to Lemma 13,

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

so, according to (54),

$$v + \varphi_{2(2k+1-j)} \equiv 0 \pmod{\varphi_{2k} + \varphi_{2k+2}}.$$

Hence

$$v + \varphi_{2(2k+1-j)} \geqslant \varphi_{2k} + \varphi_{2k+2};$$

so, according to (55),

$$\varphi_{2(2k+1-j)} \geqslant \varphi_{2k} + \varphi_{2k+2} - v > \varphi_{2k} + \varphi_{2k+2} - \varphi_{2k+1} > \varphi_{2k}. \tag{57}$$

By Lemma 1, (57) implies that $2k + 1 - j > k$, whence

$$j < k + 1. \tag{58}$$

Again according to Lemma 1, this implies that $\phi_{2j} < \phi_{2k+2}$, and especially that

$$\varphi_{2j} < \varphi_{2k} + \varphi_{2k+2}. \tag{59}$$

The equation

$$v = \varphi_{2j} \tag{60}$$

follows from (54), (56) and (59).

According to Lemmas 16 and 15, by (1) we have $j \leq \phi_{2j}$; therefore, according to (60) and (36),

$$j \leqslant v < l. \tag{61}$$

According to Lemma 22, $x \equiv n \pmod{l}$ follows from (50) and (40). Therefore, according to (43),

$$u \equiv n \pmod{l}. \tag{62}$$

Since $n = (2k + 1)i + j$, according to (48) and (62) we have $u \equiv j \pmod{l}$. This, (35) and (61) imply $u = j$; so, according to (60), $v = \phi_{2u}$. Sufficiency has been established.

Necessity. Let u be an arbitrary natural number and let

$$v = \varphi_{2u}. \tag{63}$$

We set

$$l = \varphi_{24u+1}, \quad z = \varphi_{24u}. \tag{64}$$

According to Lemmas 16 and 15,

$$u < 2^{12u-1} \leqslant \varphi_{24u+1} = l;$$

consequently inequality (35) is fulfilled.

According to Lemma 1 and (64),

$$v = \varphi_{2u} < \varphi_{24u+1} = l;$$

consequently inequality (36) is also fulfilled.

According to Lemma 5, equality (37) is fulfilled.

We set

$$g = \varphi_{l(24u+1)}, \quad h = \varphi_{l(24u+1)-1}. \tag{65}$$

According to Lemma 6,

$$\varphi_{24u+1} \equiv \varphi_1 \varphi_{3+1}^{8u} \pmod{\varphi_3}.$$

Since $\phi_1 = 1$, $\phi_3 = 2$ and $\phi_4 = 3$, it follows from (64) that $l \equiv 1 \pmod 2$; consequently

$$l(24u + 1) - 1 \equiv 0 \pmod 2.$$

Therefore, according to (65) and Lemma 5, equality (38) is fulfilled.

According to Lemma 9, condition (39) is fulfilled.

According to Lemma 6,

$$\varphi_{24u+1} \equiv \varphi_1 \varphi_4^{6u} \pmod{\varphi_4}.$$

Since $\phi_1 = 1$, $\phi_4 = 3$ and $\phi_5 = 5$, it follows from (64) that $l \equiv 5^{6u} \equiv 25^{3u} \equiv 1 \pmod 3$; consequently

$$l(24u + 1) - 1 \equiv 0 \pmod 3.$$

Let us represent the number $l(24u + 1) + 1$ in the form $3t$. According to (65) and Lemma 6,

$$h \equiv \varphi_{l(24u+1)-1} \equiv \varphi_0 \varphi_3^t \pmod{\varphi_3};$$

so, since $\phi_0 = 0$ and $\phi_3 = 2$, h is an even number.

Let us set

$$m = 3 + (2h + g)\frac{h}{2}. \tag{66}$$

According to (39), $m \equiv 3 + h^2 \pmod l$. But according to (38) and (39), $h^2 \equiv -1 \pmod l$; consequently condition (40) is fulfilled. It is clear that condition (41) also is fulfilled.

Let us set

$$x = \psi_{m,u}, \quad y = \psi_{m,u+1}. \tag{67}$$

According to Lemma 17, condition (42) is fulfilled.

According to Lemma 22, the congruence $x \equiv u \pmod l$ follows from (40) and (67), i.e. condition (43) is fulfilled.

Also according to Lemma 22, the congruence $x \equiv v \pmod{2h + g}$, i.e. condition (44), follows from (41), (63) and (67). Necessity is proved.

Let us show that the relation defined by the formula

$$v = \phi_{2u} \tag{68}$$

is diophantine. To this end let us consider the following system of diophantine equations:

$$u + a = l, \tag{69}$$
$$v + b = l, \tag{70}$$
$$l^2 - lz - z^2 = 1, \tag{71}$$
$$g^2 - gh - h^2 = 1, \tag{72}$$
$$l^2 c = g, \tag{73}$$
$$ld = m - 2, \tag{74}$$
$$(2h + g)e = m - 3, \tag{75}$$
$$x^2 - mxy + y^2 = 1, \tag{76}$$
$$l(p - q) = x - u, \tag{77}$$
$$(2h + g)(r - s) = x - v, \tag{78}$$

It is clear that if the numbers a, b, c, d, e, g, h, l, m, p, q, r, s, u, v, x, y and z satisfy conditions (69)–(78), then conditions (35)–(44) are fulfilled. The converse is also true: if the numbers u, v, l, g, h, m, x, y and z satisfy conditions (35)–(44), then it is possible to choose the remaining numbers so that conditions (69)–(78) are fulfilled. Therefore, by Theorem 1, $v = \phi_{2u}$ if and only if the system of diophantine equations (69)–(78) is solvable with respect to the remaining variables. To prove that relation (68) is diophantine, it remains to remark that, as indicated in §1, an arbitrary system of diophantine equations can easily be transformed into a single diophantine equation equivalent to it.

Let us show that relation (68) has exponential growth, i.e. that for all u

$$\varphi_{2u} \leqslant u^u \tag{79}$$

and for any k it is possible to find u such that

$$u^k < \varphi_{2u}. \tag{80}$$

According to Lemmas 16 and 15, the inequalities

$$2^{u-1} \leqslant \varphi_{2u} < 3^u \tag{81}$$

hold for any u. Hence inequality (79) is fulfilled for $u \geq 3$. We verify inequality (79) for the cases $u = 1$ and $u = 2$ immediately by calculating

$$\varphi_{2\cdot 1} = 1 = 1^1,$$
$$\varphi_{2\cdot 2} = 3 < 2^2.$$

Let k be an arbitrary natural number. Since a power function grows more slowly than an exponential one, the inequality

$$u^k < 2^{u-1}$$

is valid for sufficiently large u; so, according to (81), inequality (80) is fulfilled for those same u.

Thus relation (68) in fact has exponential growth.

§3. Diophantine representations of resursive sequences

In proving that the relation $v = \phi_{2u}$ is diophantine, we used the Fibonacci numbers in very special ways, and the proof cannot be immediately generalized to the case of an arbitrary recursive sequence. Nevertheless, Theorem 1 implies indirectly (via the basic theorem) that for any recursive sequence χ_n the relation

$$v = \chi_u \tag{1}$$

is diophantine. However, if we follow the proof of the basic theorem, there will be a polynomial of hundreds of variables in the diophantine representation of relation (1),

even in the case of an uncomplicated recursive sequence. Below we present a direct proof that relations of the kind in (1) for sequences defined by linear recursive relationships are diophantine.

We begin by establishing that the relation defined by the formula

$$q = p^k \tag{2}$$

(i.e. a relation of the kind in (1) for a sequence defined by the relationships $\chi_0 = 1$ and $\chi_{i+1} = p\chi_i$) is diophantine. Julia Robinson showed in [7] how a diophantine representation of relation (2) can be found if we have a diophantine relation with exponential growth. We shall utilize a somewhat different method, based, however, on ideas similar to those set forth in [7]. (Compare Lemmas 23 and 24 with Lemmas 5 and 8 in [7].)

In §2 we utilized the following two properties of the numbers $\psi_{m,j}$:

$$\psi_{m,j} \equiv j \pmod{m-2}, \tag{3}$$

$$\psi_{m,j} \equiv \varphi_{2j} \pmod{m-3}. \tag{4}$$

Here we use the analog of property (4); that is, we choose numbers α, β and d such that

$$\alpha\psi_{m,j+1} + \beta\psi_{m,j} \equiv p^j \pmod{d}. \tag{5}$$

The numbers α, β and d are chosen on the basis of the following considerations. If congruence (5) holds for all j, then according to the recursive relationship for $\psi_{m,j}$ we have

$$\begin{aligned} p^{n+1} &\equiv \alpha\psi_{m,n+2} + \beta\psi_{m,n+1} \\ &\equiv \alpha(m\psi_{m,n+1} - \psi_{m,n}) + \beta(m\psi_{m,n} - \psi_{m,n-1}) \\ &\equiv m(\alpha\psi_{m,n+1} + \beta\psi_{m,n}) - (\alpha\psi_{m,n} + \beta\psi_{m,n-1}) \equiv mp^n - p^{n-1} \pmod{d}. \end{aligned}$$

Thus it is necessary that

$$d \mid mp^n - p^{n-1} - p^{n+1};$$

so we shall set $d = pm - p^2 - 1$.

The numbers α and β are chosen so that congruence (5) turns into an equality for $j = 0$ and $j = 1$, i.e. so that

$$\begin{cases} \alpha = 1, \\ \alpha m + \beta = p; \end{cases}$$

hence we have $\alpha = 1$ and $\beta = p - m$.

The following assertion is valid.

Lemma 23. *For any j, p and $m \geq 2$,*

$$\psi_{m,j+1} + (p-m)\psi_{m,j} \equiv p^j \pmod{pm - p^2 - 1}.$$

The proof is easily carried out by induction on j. The basic condition for the induc-

tion is satisfied, thanks to the choice of the numbers α and β; and the induction step is easily justified, thanks to the choice of the number d.

According to Lemma 23, if

$$\begin{gathered} q \equiv \psi_{m,i+1} + (p-m)\psi_{m,i} \pmod{pm - p^2 - 1}, \\ q < pm - p^2 - 1, \\ p^i < pm - p^2 - 1, \end{gathered} \tag{6}$$

then $q = p^i$. We can replace condition (6) with a stronger diophantine condition by utilizing the following lemma.

Lemma 24. *For any u, w and a, if*

$$u^2 - a(a+2)uw + a^2w^2 = 1, \tag{7}$$

then $u \geq (a+1)^{a-2}$; for any a it is possible to find numbers u and w as large as desired which satisfy equality (7).

Proof. Let u, w and a be natural numbers satisfying (7). According to Lemma 18, $aw = \psi_{a+2,s}$ for some number s; moreover, if $u \leq aw$, then

$$u = \psi_{a+2,s-1}, \tag{8}$$

while in the opposite case

$$u = \psi_{a+2,s+1}. \tag{9}$$

According to Lemma 22, $s \equiv aw \pmod{a}$; consequently $s \geq a$. This and (8) and (9) imply that $u \geq \psi_{a+2,a-1}$; so that, according to Lemma 15,

$$u \geqslant (a+1)^{a-2}.$$

The first part of the lemma is proved.

Let a be an arbitrary natural number. According to Lemma 22,

$$\psi_{a+2,ak} \equiv ak \pmod{a}$$

for any k, whence $a \mid \psi_{a+2,ak}$. Set

$$u = \psi_{a+2,ak+1}, \quad w = \frac{\psi_{a+2,ak}}{a}.$$

According to Lemma 17, equality (7) is fulfilled. According to Lemma 15, having chosen the number k sufficiently large, we can make the numbers u and w as large as we wish. The lemma is proved.

Theorem 2. *For any natural numbers q, p and k, in order that the equation $q = p^k$ hold, it is necessary and sufficient that there exist natural numbers a, s, t, u, v and w such that*

$$a = q + p + k + p^2 + 2, \tag{10}$$

$$u^2 - a(a+2)uw + a^2w^2 = 1, \tag{11}$$

$$v = \varphi_{2u}, \tag{12}$$

$$s^2 - ust + t^2 = 1, \tag{13}$$

$$s \leqslant t, \tag{14}$$

$$9t < v, \tag{15}$$

$$u - 2 \mid s - k, \tag{16}$$

$$pu^2 - p^2 - 1 \mid t + (p - u)s - q. \tag{17}$$

Sufficiency. According to Lemma 24, (11) implies that $u \geq (a+1)^{a-2}$, i.e., according to (10),

$$u \geqslant (q + p + k + p^2 + 3)^{q+p+k+p^2}.$$

This implies

$$u \geqslant 4, \tag{18}$$

$$u - 2 > k, \tag{19}$$

$$pu - p^2 - 1 > q, \tag{20}$$

$$pu - p^2 - 1 > p^k. \tag{21}$$

According to Lemma 18, the fact that

$$s = \psi_{u,n}, \quad t = \psi_{u,n+1} \tag{22}$$

for some number n follows from (13) and (14).

According to Lemmas 15 and 16 and conditions (12), (15) and (18), we have

$$9 \cdot 3^n \leqslant 9\psi_{u,n+1} = 9t < v = \varphi_{2u} = \psi_{3,u} < 3^u.$$

Hence

$$u - 2 > n. \tag{23}$$

According to Lemma 22, $n \equiv s \pmod{u-2}$; hence by (16) we have

$$n \equiv k \pmod{u-2}. \tag{24}$$

This, (19) and (23) imply that $n = k$; thus by (17) and (22) we have

$$q \equiv \psi_{u,k+1} + (p - u)\psi_{u,k} \pmod{pu - p^2 - 1}.$$

According to Lemma 23, this implies

$$q \equiv p^k \pmod{pu - p^2 - 1};$$

so according to (20) and (21), $q = p^k$. Sufficiency is proved.

Necessity. Let p and k be natural numbers, and let $q = p^k$.

Choose a number a in accordance with (10). Since a power function grows more slowly than an exponential one, for sufficiently large u the inequality

$$9u^{k+1} < 2^{u-1} \tag{25}$$

is valid. We choose numbers u and w in accordance with Lemma 24 so that (11) and (25) are fulfilled. Let us choose a number v in accordance with (12).

Let us set $s = \psi_{u,k}$ and $t = \psi_{u,k+1}$. According to Lemma 17, condition (13) is fulfilled; according to Lemma (14), condition (14) is fulfilled.

According to Lemmas 15 and 16 and (25), we have

$$9t = 9\psi_{u,k+1} < 9u^{k+1} < 2^{u-1} \leqslant \psi_{3,u} = \varphi_{2u} = v.$$

Consequently condition (15) is also fulfilled.

By Lemma 22, $s \equiv k \pmod{u-2}$, i.e. condition (16) is fulfilled.

According to Lemma 23, the congruence

$$t \mid (p-u)\, s \equiv q \pmod{pu - p^2 - 1},$$

i.e. condition (17), follows from (24). Necessity is proved.

Let us complete the proof that the relation $q = p^k$ is diophantine. Utilizing Theorem 1, we can change condition (12) to a system of diophantine equations. It is clear that we can also change conditions (14)–(17) to diophantine equations. It remains to transform the resulting system of equations into a single diophantine equation.

Having established that the relation $q = p^k$ is diophantine, as was shown in §1, we can transform every exponential diophantine equation into a diophantine equation equivalent to it. Therefore, when establishing diophantineness, we shall henceforth utilize, along with diophantine equations, also exponential diophantine equations.

We turn now to an exposition of the general method which permits finding diophantine representations for a broad class of recursive sequences. We begin by considering one of the simplest cases, the case when a sequence of natural numbers χ_n is defined by relationships of the form

$$\chi_i = \alpha_i \quad (i = 0, 1, \ldots, j), \tag{26}$$

$$\chi_i = \sum_{k=1}^{j+1} \gamma_k \chi_{i-k} \quad (i = j+1, j+2, \ldots \tag{27}$$

where j, α_i and γ_k are fixed integers.

Theorem 3. *Let χ_n be a sequence of natural numbers defined by* (26) *and* (27), *and let u and v be any natural numbers. In order that $v = \chi_u$, it is necessary and sufficient that there exist natural numbers p, x and z such that*

$$p = (|\alpha_0| + \ldots + |\alpha_j| + 1)\,(|\gamma_1| + \ldots + |\gamma_{j+1}| + 2)^u, \tag{28}$$

$$\left(\sum_{k=1}^{j+1} \gamma_k p^k - 1\right) x \equiv \sum_{i=1}^{j} \sum_{k=1}^{i} \gamma_k \alpha_{i-k} p^i - \sum_{i=0}^{j} \alpha_i p^i \pmod{p^{u+1}}, \tag{29}$$

$$x \equiv vp^u + z \pmod{p^{u+1}}, \tag{30}$$

$$v < p, \tag{31}$$

$$z < p^u. \tag{32}$$

Proof. According to (26) and (27), for any p and u we have[1]

$$\left(\sum_{k=1}^{j+1} \gamma_k p^k - 1\right) \sum_{i=0}^{u} \chi_i p^i \equiv \sum_{i=j+1}^{u} \left(\sum_{k=1}^{j+1} \gamma_k \chi_{i-k} - \chi_i\right) p^i$$

$$+ \sum_{i=1}^{j} \sum_{k=1}^{i} \gamma_k \chi_{i-k} p^i - \sum_{i=0}^{j} \chi_i p^i \equiv \sum_{i=1}^{j} \sum_{k=1}^{i} \gamma_k \alpha_{i-k} p^i - \sum_{i=0}^{j} \alpha_i p^i \pmod{p^{u+1}}.$$

Thus the number

$$\sum_{i=0}^{u} \chi_i p^i \tag{33}$$

is a solution of congruence (29). Since the number

$$\sum_{k=1}^{j+1} \gamma_k p^k - 1$$

and p are relatively prime, all solutions of (29) have the form

$$\lambda p^{u+1} + \sum_{i=0}^{u} \chi_i p^i,$$

where λ is an integer. In other words, (29) is equivalent to

$$x \equiv \sum_{i=0}^{u} \chi_i p^i \pmod{p^{u+1}}. \tag{34}$$

Condition (34) can be reformulated in the following manner: the first[2] $(u+1)$ digits in the p-adic representation of the numbers (33) and x respectively coincide. But using (28), it can easily be shown that $\chi_i < p$ $(0 \le i \le u)$. Consequently the numbers $\chi_0, \cdots, \chi_u$ are the first $(u+1)$ digits of the number (33) in p-adic notation. But conditions (30)–(32) mean that v is the $(u+1)$th digit of the number x in p-adic notation, and consequently also of the number (33) in p-adic notation, i.e. $v = \chi_u$. The theorem is proved.

Let us note that the sequences x_n and y_n defined as the nth solution of Pell's equation $x^2 - (a^2 - 1)y^2 = 1$ fall into the recursive scheme (26)–(27).

Theorem 3 admits various generalizations. We shall indicate in turn a few possible directions of such generalizations; however, it is actually possible to develop generalizations in several directions simultaneously.

In Theorem 3 we assumed that α_i and γ_k are specific numbers. However, it is obvious from the proof that these numbers can depend on parameters. Sequences $\psi_{m,n}$

1) This transformation has a very simple "geometric" meaning if we write the factors in a p-adic number system (admitting negative digits and digits larger than $p-1$) and carry out formal multiplication "by column."

2) The counting begins with the least signigicant digits.

such that the three-place relation defined by the formula

$$m \geqslant 2 \,\&\, x = \psi_{m,n}$$

is diophantine,[1] fall into this generalized scheme.

It is easy to obtain a generalization of Theorem 3 to the case of a recursive relationship which has the following somewhat more general form:

$$\rho_i = \sum_{k=1}^{t} \delta_k \rho_{i-k} + \chi_i,$$

where δ_k is a fixed number and χ_i is a recursive sequence of the form (26)–(27). It is possible to iterate the process which consists of defining a new sequence by means of another sequence which has already been proved to be diophantine by the method described.

It is not difficult to obtain a generalization of Theorem 3 to the case of sequences defined not as sequences but as simultaneous recursions, i.e. when the recursive relation has the form

$$\chi_{l,i} = \alpha_{l,i} \quad (l = 1, \ldots, t;\ i = 0, \ldots, j),$$

$$\chi_{l,i} = \sum_{s=1}^{t} \sum_{k=1}^{j+1} \gamma_{l,s,k} \chi_{s,i-k} \quad (l = 1, \ldots, t;\ i = j+1, \ldots).$$

Having obtained this generalization, we have thereby proved that the relation defined by the formula $X = A^k$ is diophantine. Here X is a square matrix of variables, while A, of the same order, is a square matrix of specific natural numbers.

It is somewhat more complicated to obtain a generalization to the case of a multidimensional (i.e. depending on two or more indices) sequence defined by relationships of the form[2]

$$\chi_{0,i} = \rho_i \quad (i = 0, 1, \ldots), \tag{35}$$

$$\chi_{l,i} = \sum_{j=0}^{n} \gamma_j \chi_{l-1,i+j} \quad (l = 1, 2, \ldots;\ i = 0, 1, \ldots), \tag{36}$$

where ρ_i is a one-dimensional recursive sequence whose diophantineness has been previously established by the method described. Here it is necessary to consider numbers in whose p-adic representation the number $\chi_{j,i}$ occupies the p^{jd+i}th place (where d is a sufficiently large number and $i \leq d - nj$).

Let us observe that the binomial coefficients forming the Pascal triangle fall into recursive scheme (35)–(36).

We have been considering recursive sequences of natural numbers. In the case of recursive sequences of integers it is sufficient to use, instead of a p-adic number system, a $(2p+1)$-adic system with digits $-p, -p+1, \cdots, p-1, p$.

Received 17 SEPT 1970

1) The diophantineness of this relation can be established in the same way that it was for the relation $q = p^k$ if Lemma 21 is used instead of Lemma 23. This results in a simpler representation.

2) The relationship is given here for the two-dimensional case.

BIBLIOGRAPHY

[1] D. Hilbert, *Mathematische Probleme*, Lecture presented at the Second Internat. Congress Math. (Paris, 1900), Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. 1900, 253–297; reprinted in *Gesammelte Abhandlungen*, Vol. III, Springer-Verlag, Berlin, 1935 (reprint, Chelsea, New York, 1965), pp 290–329; Russian transl. in *Hilbert's problems*, "Nauka", Moscow, 1969; English transl., Bull. Amer. Math. Soc. 8 (1902), 437–479. MR 40 #4036.

[2] A. I. Mal'cev, *Algorithms and recursive functions*, "Nauka", Moscow, 1965; English transl., Wolters-Noordhoff, Groningen, 1970. MR 34 #2453.

[3] A. A. Markov, *Theory of algorithms*, Trudy Mat. Inst. Steklov. 42 (1954); English transl., Israel Program for Scientific Translations, Jerusalem, 1961. MR 17, 1038; 24 #A2527.

[4] H. Davenport, *The higher arithmetic. An introduction to the theory of numbers*, Hutchinson's University Library, London; Longmans, Green, New York, 1952; Russian transl., "Nauka", Moscow, 1965.

[5] M. Davis, *Arithmetical problems and recursively enumerable predicates*, J. Symbolic Logic 18 (1953), 33–41; Russian transl., Matematika 8 (1964), no. 5, 15–22. MR 14, 1052.

[6] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) 74 (1961), 425–436; Russian transl., Matematika 8 (1964), no. 5, 69–79. MR 24 #A3061.

[7] J. Robinson, *Existential definability in arithmetic*, Trans. Amer. Math. Soc. 72 (1952), 437–449; Russian transl., Matematika 8 (1964), no. 5, 3–14. MR 14, 4.

[8] M. Davis, *Extensions and corollaries of recent work on Hilbert's tenth problem*, Illinois J. Math. 7 (1963), 246–250; Russian transl., Matematika 8 (1964), no. 5, 80–84. MR 26 #6046.

[9] Ju. V. Matijasevič, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR 191 (1970), 279–282 = Soviet Math. Dokl. 11 (1970), 354–358. MR 41 #3390.

[10] H. Putnam, *An unsolvable problem in number theory*, J. Symbolic Logic 25 (1960), 220–232; Russian transl., Matematika 8 (1964), no. 5, 55–67.. MR 28 #2048.

Translated by:
F. M. Goldware