To prove that conditions (6) are necessary and sufficient we consider the sequen-
ces $\psi_{m,n}$ defined for every $m \geq 2$ by

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

It can be easily proved by induction that

$$
\psi_{m,n} \equiv n \pmod{m - 2}, \\
\psi_{m,n} \equiv \varphi_{2n} \pmod{m - 3}.
$$

Hence if $d \mid m - 3$, then

$$
\text{Rem} \ (\psi_{m,n}, \ d) = \text{Rem} \ (\varphi_{2n}, \ d)
$$

(\text{Rem} \ (a, \ b) \text{ denotes the remainder obtained upon dividing } a \text{ by } b).

We study the sequence

$$
\text{Rem} \ (\varphi_0, \ d), \ \text{Rem} \ (\varphi_2, \ d), \ldots, \ \text{Rem} \ (\varphi_{2n}, \ d), \ldots
$$

(7)

where $d = \varphi_{2k} + \varphi_{2(k+1)}$ for some $k$. It can be proved that sequence (7) is periodic, the length of the period is equal to $2k + 1$, and the period consists of the following numbers:

$$
\varphi_0, \varphi_2, \ldots, \varphi_{2k} = d - \varphi_{2(k+1)}, \varphi_{2(k+1)} = d - \varphi_{2k}, \ldots, d - \varphi_4, d - \varphi_2.
$$

We also use the following properties of numbers $\varphi_n$ and $\psi_{m,n}$:

$$
\begin{align*}
x^2 - xy - y^2 = 1 &\iff \exists i [x = \varphi_{2i+1} \land y = \varphi_{2i}], \\
m \geq 2 &\implies \exists i [x = \psi_{m,i+1} \land y = \psi_{m,i}] \\
x^2 \mid \varphi_t &\implies \varphi_t \mid t, \\
\varphi_t \mid t &\implies \varphi_t \mid \varphi_n.
\end{align*}
$$

It is not very difficult to prove these properties by induction and course-of-values
induction.

Having proved the above mentioned properties of numbers $\varphi_n$ and $\psi_{m,n}$ we can
easily complete the proof of the necessity and sufficiency of the conditions (6).

Combining our Main Theorem with an earlier result of Hilary Putnam [8], we can
obtain the following theorem:

**Every recursively enumerable set $S$ of positive integers can be represented in the form**

$$
a \in S \iff \exists y_1 \ldots y_n [a = P(y_1, \ldots, y_n)]
$$

(8)

where $P$ is a polynomial.

For example, the set of all prime numbers coincides with the set of all positive values
of some polynomial with integer coefficients!

If $S$ in (8) is any recursively enumerable, but not recursive set of positive integers,
then there is no algorithm for determining for given $a$ whether the equation

$$
P(y_1, \ldots, y_n) = a
$$

has a solution. This result is stronger than the unsolvability of Hilbert's tenth problem.
Using Gödel numbering of recursively enumerable sets we can construct a polynomial \( M(y_1, \ldots, y_k, g) \) such that every recursively enumerable set \( S \) of positive integers can be represented in the form

\[
a \in S \iff \exists y_1 \ldots y_k \{a = M(y_1, \ldots, y_k, g_S)\}
\]

where \( g_S \) is any Gödel number of \( S \).

The constructions known today yield such universal polynomials with some 200 variables. For the set of all primes we can construct a polynomial with about 25 variables. Of course, these constructions are not the best ones and we can hope they will be essentially improved in the future.

REFERENCES


Steklov Mathematical Institute
of Academy of Sciences of USSR
Leningrad (U. R. S. S.)