3. A Proof of Negative Answer to Hilbert's 10th Problem

By Ken HIROSE and Shigeaki IIDA
Department of Mathematics, Waseda University

(Comm. by Kunihiko KODAIRA, M. J. A., Jan. 12, 1973)

0. Recently, the effective methods for Diophantine equations make a rapid progress.

A. Baker gave an effective procedure for the existence of integer solutions of some kinds of Diophantine equations in [1].

In his paper [2], Ju. B. Matijasevič proved the unsolvability of Hilbert's 10th problem by using the results of Julia Robinson, M. Davis and H. Putnum in [3], [4] and [5].

In the present note, we shall give a short proof of the negative solution of Hilbert's 10th problem. That is, we lead to the unsolvability of the problem directly from the following result of Davis [3]:

Every recursively enumerable set S can be expressed in the form,

$$(*) \qquad x \in S \equiv (\exists y)(\forall k)_{k<y}(\exists z_1)\cdots(\exists z_m)[P(x, y, k, z_1, \cdots, z_m)=0],$$

where P is a polynomial with integer coefficients.

We shall give a full detail in [6].

1. First, we define certain sequences and state some lemmata.

Definition 1. Let $u_n, v_n, (a)_n$ be sequences of numbers defined by

$$u_1=u_2=1, \qquad u_{n+2}=u_{n+1}+u_n,$$
$$v_1=1, \quad v_2=3, \quad v_{n+2}=v_{n+1}+v_n,$$
$$(a)_0=0, \quad (a)_1=1, \quad (a)_{n+2}=a\cdot(a)_{n+1}-(a)_n,$$

where a is a constant.

Lemma 1. (1) *If $m|n$, then $u_m|u_n$.*

(2) $2u_{m+n}=u_m v_n+u_n v_m$.

(3) $2v_{m+n}=5u_m u_n+v_m v_n$.

(4) $u_{m+n+1}=u_{m+1}u_{n+1}+u_m u_n$.

(5) $u_n v_n=u_{2n}$.

(6) $(u_n, v_n)=1$, if $3\nmid n$.

(7) $[(2x(2x)_n)_n/(2(2x)_n)_n]=x^n$.

Proof. For (1)$\sim$(6), let $\alpha=(1+\sqrt{5})/2$, $\beta=(1-\sqrt{5})/2$ and then we obtain $u_n=(\alpha^n-\beta^n)/\sqrt{5}$ and $v_n=\alpha^n+\beta^n$, from which the above formulae may be derived.

For (7), we put $p=(2x)_n$. By $(2x)_n>x^n$ we have $x^n(2p)_n\leq(2xp)_n<(x^n+1)(2p)_n$.

Definition 2. We define sequences of numbers $|a|_n, \{a\}_n$ such that:

$$|a|_1=1, \quad |a|_2=a+1, \quad |a|_{n+2}=a\cdot|a|_{n+1}-|a|_n,$$
$$\{a\}_0=1, \quad \{a\}_1=a-1, \quad \{a\}_{n+2}=a\cdot\{a\}_{n+1}-\{a\}_n.$$

Lemma 2. (1) $(a)_{(2k+1)l+m} \equiv (a)_m (\mathrm{mod}\, |a|_{k+1})$

(2) $(x^2 - axy + y^2 = 1) \equiv (\exists m)[((a)_{m+1} = x)$ *and* $((a)_m = y)]$

(3) $(\lambda i, x)[x = (a)_i]$ *is diophantine, iff* $(\lambda i, x)[x = |a|_i]$ *is diophantine.* (*Similarly* $(\lambda i, x)[x = (a)_i]$ *is diophantine, iff* $(\lambda i, x)[x = \{a\}_i]$ *is diophantine.*)

(4) *If* $(a)_n^2 \mid (a)_p$, *then* $(a)_n \mid p$.

(5) $\{a\}_s \mid (a)_{2s+1}$.

(6) $(\lambda i, y)[y = \{x\}_i]$ *is diophantine, iff* $(\lambda, y, i)[y = (x)_{2i+1}]$ *is diophantine.*

(7) $(b)_i \equiv (a)_i \ (\mathrm{mod}\, b - a)$.

Lemma 2 is proved by using induction and Lemma 1.

Lemma 3. (1) $(\lambda y, n)[y = (a)_n]$ *is diophantine, iff* $(\exists y, z, i, l)[(y = (a)_i)$ *and* $(i = la^2 + n)$ *and* $(z = (a)_{la^2})]$ *are diophantine.*

(2) $(\exists y, z, i, l)[(i = la^2 + n)$ *and* $(y = (a)_i)$ *and* $(z = (a)_{la^2})]$ *is diophantine.*

By Lemma 2, Lemma 3-(2) is proved by similar method to Matijasevič's one in [2].

Lemma 4. $(\lambda y, n)[y = (a)_n]$, $(\lambda x, n)[x = u_n]$ *and* $(\lambda z, n)[z = v_n]$ *are diophantine.*

Proof. By Lemma 3, $(\lambda y, n)[y = (a)_n]$ is diophantine, then it follows that $(\lambda x, n)[x = u_n]$ and $(\lambda z, n)[z = v_n]$ are diophantine by Lemma 1–(5).

Lemma 5. $(\lambda x, n)[x = (a)_{2n}]$ *and* $(\lambda y, n, x)[y = \binom{x}{n}]$ *are diophantine.*

Proof. By Lemma 1-(7) and Lemma 4.

Definition 3. For a polynomial P satisfying $(*)$, we define polynomials P_1, P_2, and numbers n, t, z such that:

$$(\forall \eta)_{\eta < y}(\exists z_1) \cdots (\exists z_m)[(P(x, y, \eta, z_2, \cdots, z_m) = 0) \text{ and } (v_{2\eta} = z_1)]$$
$$\equiv (\forall \eta)_{\eta < y}(\exists z_1) \cdots (\exists z_k)[P_1(x, y, \eta, z_1, \cdots, z_k) = 0]$$

And

$$\begin{aligned}(\exists a)(\exists z_1) \cdots (\exists z_l)&[P_2(a, t, n, x, y, z_1, \cdots, z_l) = 0] \\ \equiv (\exists a)(\exists z_1) \cdots (\exists z_{k+4})&[[(u_{2v\cdot n})^t \mid (u_n)^t \cdot P_1(x, y, a, z_1, \cdots, z_k)] \text{ and} \\ &[(u_{2v\cdot n})^z \mid z_{k+1} \cdot z_1] \text{ and } [z_{k+2} \cdot z_{k+3} + z_{k+4} \cdot u_{2v\cdot n} = 1] \text{ and} \\ &[z_{k+1} = z_{k+3} \cdot (u_{2v\cdot n})^{z-1}] \text{ and } [(u_{2v\cdot n})^t \mid \tbinom{a}{y}] \\ &\text{and } (\forall_i)_{i \le k}[(u_{2v\cdot n})^t \mid \tbinom{z_i}{B}]\end{aligned}$$

where B is a maximal value of solutions $z_1, \cdots, z_k$ of the equation $P_1(x, y, \eta, z_1, \cdots, z_k) = 0$ for $0 < \eta < y$. Let $\varphi(x, y)$ be such a polynomial that

$$(\forall \eta)_{\eta < y}(\forall z_1)_{z_1 < B} \cdots (\forall z_k)_{z_k < B}[|P_1(x, y, \eta, z_1, \cdots, z_k)| < \varphi(x, y)],$$

and let n be a number such that $(v_n)^t > \varphi(x, y)$ and $3 \nmid n$ and $z = t - B^2$. (Note that the existence of P_1 and P_2 is derived from Lemma 5.)

2. Next, we prove the following

Theorem 1.

$$(\exists y)(\forall k)_{k < y}(\exists z_1) \cdots (\exists z_m)[P(x, y, k, z_1, \cdots, z_m) = 0]$$
$$\equiv (\exists a)(\exists t)(\exists z)(\exists y)(\exists n)(\exists a_1) \cdots (\exists a_l)[P_2(a, t, n, x, y, a_1, \cdots, a_l) = 0$$

Proof. First, we assume the left side of the equivalence and show that it implies the right side. From Lemma 1-(5), we have $u_n \cdot v_n \cdot \cdots \cdot v_{2^y-1 \cdot n} = u_{2^y \cdot n}$ and from Lemma 1-(6), $v_n, v_{2 \cdot n}, \cdots, v_{2^y-1 \cdot n}$ are relatively prime. The remaining can be obtained from Chinese Remainder Theorem and $u_{2^y n} \equiv v_{2^i n} \pmod{v_{2^i n}}$ for $0 < i < y$.

Next, assume the right side and prove the left side.

Let z_{ik} be $\mathrm{Rem}(a_i, (v_{2^k \cdot n})^z) = z_{ik}$ $(k < y)$. From $(v_n)^z > \varphi(x, y)$ and $v_{2^i n} \mid u_{2^y n}$, we have

$$(v_{2^i n})^z \mid P_1(x, y, a, a_1, \cdots, a_k),$$

thus

$$(v_{2^i n})^z \mid P_1(x, y, a', z_{1i}, \cdots, z_{ki}) \qquad \text{for some } a' < y.$$

Hence,

$$P(x, y, i, z_{1i}, \cdots, z_{mi}) = 0.$$

3. Now we have:

Theorem 2. *Recursively enumerable predicates are diophantine.*

Proof. By (*), Lemma 4, Lemma 5 and Theorem 1.

Thus, we have obtained the negative solution of Hilbert's 10th problem.

It is very interesting to consider the relation between the positive results and the negative ones.

In Baker [1], the homogeneity of polynomials is used essentially. But it is impossible to extend the number of variables of the polynomials, even if the homogeneity of the polynomials is used. We should remark the following result:

There exists a positive integer m and an irreducible μ-ary form f of degree $n \geqq 3$ with integer coefficients such that the existence of solutions of the equation

$$f(x_1, x_2, \cdots, x_\mu) = m$$

can not be determined effectively.

References

[1] A. Baker: Contributions to the theory of diophantine equations. Phil. Trans. Roy. Soc. London, Ser. A, **263**, 173–191 (1968).

[2] Yu. B. Matijasevič: Recursively enumerable sets are diophantine. Dokl. Akad. Nauk, **191**(2), 279–282 (1970).

[3] M. Davis: Arithmetical problems and recursively enumerable predicates. J. S. L., **18**, 33–41 (1953).

[4] J. Robinson: Existential definability in arithmetic. T. A. M. S., **72**, 437–449 (1952).

[5] M. Davis, H. Putnum, and J. Robinson: The decision problem for exponential diophantine equations. Ann. of Math., **74**, 425–436 (1961).

[6] K. Hirose and S. Iida: A diophantine representation of complete predicate for $\sum_1^0$-form (to appear).