Ю. В. Матиясевич, Диофантовость перечислимых множеств, *Докл. АН СССР*, 1970, том 191, номер 2, 279–282

Доклады Академии наук СССР
1970. Том 191, № 2

УДК 51.01:518.5+511.5

МАТЕМАТИКА

Ю. В. МАТИЯСЕВИЧ

ДИОФАНТОВОСТЬ ПЕРЕЧИСЛИМЫХ МНОЖЕСТВ

(Представлено академиком И. М. Виноградовым 5 II 1970)

10-я проблема Гильберта сформулирована следующим образом (см. [1]):

Пусть задано диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами. Указать способ, при помощи которого за конечное число операций можно установить, разрешимо ли это уравнение в целых рациональных числах.

Когда эта проблема формулировалась, речь могла идти лишь о положительном решении проблемы, так как точное понятие алгорифма еще не было выработано. Появление этого понятия дало возможность доказывать алгорифмическую неразрешимость массовых проблем.

Такие неразрешимые проблемы были найдены сначала в математической логике, а затем в алгебре и теории чисел. В частности, М. Девис, Х. Путнам и Дж. Робинсон [2] доказали, что не существует алгорифма, позволяющего распознавать наличие целочисленных решений у так называемых показательно-диофантовых уравнений, т. е. уравнений, которые строятся из натуральных чисел и переменных с помощью сложения, умножения и возведения в степень. Используя этот результат, а также работу Дж. Робинсон [3], мы покажем, что 10-я проблема Гильберта также является алгорифмически неразрешимой.

1. Строчные латинские буквы, кроме i и j, всюду ниже используются в качестве переменных для целых положительных чисел, i и j — переменные, пробегающие целые неотрицательные числа.

Будем говорить, что предикат * $\mathcal{P}(u, v)$ имеет экспоненциальный рост, если $\mathcal{P}(u, v)$ влечет неравенство $v \leqslant u^u$ и для каждого k существуют u, v такие, что $\mathcal{P}(u, v)$ и $u^k < v$.

Предикат $\mathcal{P}(x_1, \ldots, x_n)$ называется диофантовым, если можно указать полином ** M такой, что $\mathcal{P}(x_1, \ldots, x_n)$ имеет место тогда и только тогда, когда существуют числа $y_1, \ldots, y_j$ такие, что $M(x_1, \ldots, x_n, y_1, \ldots, y_j) = 0$.

Из упомянутых выше работ М. Девиса, Х. Путнама и Дж. Робинсон следует, что если хотя бы один диофантов предикат имеет экспоненциальный рост, то любой перечислимый *** предикат является диофантовым.

Предикат «v есть $2u$-е число Фибоначчи» имеет экспоненциальный рост. Мы установим его диофантовость. Тем самым будет завершено доказательство следующего утверждения:

Любой перечислимый предикат является диофантовым.

Более того, *для каждого n можно указать такой $(n+1)$-местный диофантов предикат $\mathcal{U}_n(x_1, \ldots, x_n, s)$, что любой перечислимый n-местный предикат может быть получен из $\mathcal{U}_n$ фиксацией значения s.*

Так как существуют перечислимые, но алгорифмически неразрешимые предикаты (см. [4, 5]), то справедливо следующее утверждение:

* Под предикатами мы понимаем свойства и отношения, которые представимы формулами формального арифметического языка.

** Не ограничивая общности, можно считать, что степень полинома M не выше 4.

*** Предикат называется перечислимым, если можно указать эффективно вычислимую последовательность n-ок чисел, содержащую все те и только те n-ки, на которых он истинен.

Зак. 26

Не существует алгорифма, позволяющего узнавать по произвольному диофантову уравнению, имеет ли оно решения *.

Объединяя наш результат с результатами работы ([6]), получаем такие следствия:

1) *Можно указать полином пятой степени* $Q(y_1, \ldots, y_k, z)$ *с целыми коэффициентами такой, что любое перечислимое множество* $\mathcal{M}$ *натуральных чисел* (например, множество простых чисел) *совпадает с множеством натуральных значений полинома* $Q(y_1, \ldots, y_k, a_{\mathcal{M}})$, *где* $a_{\mathcal{M}}$ *— некоторое число, которое эффективно строится по множеству* $\mathcal{M}$.

2) *Можно указать полиномы* $R(y_1, \ldots, y_k, z)$ *и* $S(y_1, \ldots, y_k, z)$ *с целыми коэффициентами такие, что любое перечислимое множество целых чисел совпадает с множеством целочисленных значений дроби*

$$\frac{S(y_1, \ldots, y_k, a_{\mathcal{M}})}{R(y_1, \ldots, y_k, a_{\mathcal{M}})},$$

где $a_{\mathcal{M}}$ *— некоторое число, которое эффективно строится по множеству* $\mathcal{M}$.

3) *Можно указать полином пятой степени* $D(y_1, \ldots, y_k)$ *с целыми коэффициентами такой, что не существует алгорифма, позволяющего узнавать по числу* n, *имеет ли решения уравнение* $D(y_1, \ldots, y_k) = n$.

2. Определение 1. $\varphi_0 = 0$, $\varphi_1 = 1$, $\varphi_{n+1} = \varphi_n + \varphi_{n-1}$. φ_j называется j-м числом Фибоначчи.

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

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

Лемма 2. $\varphi_{2(k+j)} \equiv -\varphi_{2(k+1-j)} (\mathrm{mod}\ \varphi_{2k} + \varphi_{2k+2})$, $0 \leqslant j \leqslant k+1$ (индукция по j; индукционный переход по лемме 1 и ее следствию).

Лемма 3. $\varphi_{2(2k+1+j)} \equiv \varphi_{2j} (\mathrm{mod}\ \varphi_{2k} + \varphi_{2k+2})$ (индукция по j; база по леммам 2 и 1, индукционный переход по лемме 1).

Лемма 4. $\varphi_{2((2k+1)i+j)} \equiv \varphi_{2j} (\mathrm{mod}\ \varphi_{2k} + \varphi_{2k+2})$ (индукция по i; индукционный переход по лемме 3).

Следствие лемм 4 и 2. *По* mod $(\varphi_{2k} + \varphi_{2k+2})$

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

Определение 2. Для каждого $m \geqslant 2$ $\psi_{m,0} = 0$, $\psi_{m,1} = 1$, $\psi_{m,n+1} = m\psi_{m,n} - \psi_{m,n-1}$.

Лемма 5. *Если* $m \geqslant 2$, $d \mid (m-3)$, *то* $\psi_{m,j} \equiv \varphi_{2j} (\mathrm{mod}\ d)$ (индукция по j; индукционный переход по лемме 1).

Лемма 6. *Если числа* k, m, n, v *таковы, что* $m \geqslant 2$, $v < \varphi_{2k+1}$, $(\varphi_{2k} + \varphi_{2k+2}) \mid (m-3)$, $\psi_{m,n} \equiv v (\mathrm{mod}\ \varphi_{2k} + \varphi_{2k+2})$, *то существуют числа* i, j *такие, что* $v = \varphi_{2j}$, $n = (2k+1)i + j$ (по лемме 5 и следствию лемм 4 и 2).

Лемма 7. *Если* $m \geqslant 2$, $l \mid (m-2)$, *то* $\psi_{m,j} \equiv j (\mathrm{mod}\ l)$ (индукция по j).

Лемма 8. $\varphi^2_{i+1} - \varphi_i\varphi_{i+1} - \varphi_i{}^2 = (-1)^i$ (индукция по i).

Лемма 9. *Если числа* j, k *таковы, что* $(k^2 - jk - j^2)^2 = 1$, *то существует число* i *такое, что* $j = \varphi_i$, $k = \varphi_{i+1}$ (возвратная индукция по $j+k$: если $j > 0$, *то* $j \leqslant k$, положим $j_1 = k - j$, $k_1 = j$, тогда $(k_1{}^2 - j_1k_1 - j_1{}^2)^2 = 1$, $j_1 + k_1 < j + k$).

Лемма 10. *Для каждого* $m \geqslant 2$ $\psi^2_{m,i+1} - m\psi_{m,i}\psi_{m,i+1} + \psi^2_{m,i} = 1$ (индукция по i).

Лемма 11. *Если числа* j, k, m *таковы, что* $m \geqslant 2$, $j \leqslant k$, $k^2 - mjk + j^2 = 1$, *то существует число* i *такое, что* $j = \psi_{m,i}$, $k = \psi_{m,i+1}$ (аналогично лемме 9).

---

* Здесь не существенно, интересуемся ли мы целыми, целыми положительными или целыми неотрицательными решениями, ибо, как известно, эти три массовые проблемы эквивалентны друг другу (см. ([4, 5])).

Лемма 12. Н.о.д. $(\varphi_i, \varphi_j) = \varphi_{\text{н.о.д.}(i,\,j)}$ (доказано в [7]).

Следствие. $\varphi_n | \varphi_{jn}$.

Лемма 13. *Если p и q — простые числа, $p | \varphi_n$, $q \neq p$, то $p\varphi_n \nmid \varphi_{qn}$.*
Если p — простое число, $p \neq 2$, $p | \varphi_n$, то $p\varphi_n | \varphi_{pn}$, но $p^2\varphi_n \nmid \varphi_{pn}$.
Если $2 | \varphi_n$, $4 \nmid \varphi_n$, то $4\varphi_n | \varphi_{2n}$, но $8\varphi_n \nmid \varphi_{2n}$.
Если $4 | \varphi_n$, то $2\varphi_n | \varphi_{2n}$, но $4\varphi_n \nmid \varphi_{2n}$.

Лемма доказана в [7].

Лемма 14. *Если p — простое число, $p | \varphi_n$, $p \nmid r$, то $p\varphi_n \nmid \varphi_{rn}$* (индукция по числу простых сомножителей числа r; индукционный переход по следствию леммы 12 и лемме 13).

Лемма 15. *Если p — простое число, $p \neq 2$, $p | \varphi_n$, то $p^i\varphi_n | \varphi_{p^i n}$, но $p^{i+1}\varphi_n \nmid \varphi_{p^i n}$* (индукция по i; индукционный переход по следствию леммы 12 и лемме 13).

Лемма 16. *Если $4 | \varphi_n$, то $2^i\varphi_n | \varphi_{2^i n}$, но $2^{i+1}\varphi_n \nmid \varphi_{2^i n}$* (аналогично лемме 15).

Лемма 17. *$\varphi_s^2 | \varphi_{rs}$ тогда и только тогда, когда $\varphi_s | r$* (следует из лемм 13—16).

Следствие лемм 12 и 17. *Если $\varphi_s^2 | \varphi_t$, то $\varphi_s | t$.*

Лемма 18. $2\varphi_{2n} < \varphi_{2(n+1)} \leqslant 3\varphi_{2n}$ (следует из леммы 1).

Лемма 19. $n \leqslant 2^{n-1} \leqslant \varphi_{2n} < 3^n$ (индукция по n; индукционный переход по лемме 18).

3. Теорема. *Для того чтобы v было $2u$-м числом Фибоначчи, необходимо и достаточно, чтобы существовали числа g, h, l, m, x, y, z такие, что:*

$$u \leqslant v < l, \tag{1}$$

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

$$g^2 - gh - h^2 = 1, \tag{3}$$

$$l^2 | g, \tag{4}$$

$$l | m - 2, \tag{5}$$

$$(2h + g) | (m - 3), \tag{6}$$

$$x^2 - mxy + y^2 = 1, \tag{7}$$

$$l | (x - u), \tag{8}$$

$$(2h + g) | (x - v). \tag{9}$$

Достаточность. Пусть числа u, v, g, h, l, m, x, y, z удовлетворяют условиям (1)—(9). Согласно лемме 9 из (2) следует, что существует число s такое, что

$$l = \varphi_s. \tag{10}$$

Согласно леммам 9 и 8 из (3) следует, что существует число k такое, что

$$h = \varphi_{2k}, \quad g = \varphi_{2k+1}. \tag{11}$$

Отсюда

$$2h + g = \varphi_{2k} + \varphi_{2k+2}. \tag{12}$$

Согласно следствию лемм 12 и 17 из (10)—(11), (4) следует, что

$$l | (2k + 1). \tag{13}$$

Из (1), (4), (11), (5) следует, что

$$2 \leqslant l < \varphi_{2k+1}, \quad m \geqslant 2. \tag{14}$$

Согласно лемме 11 из (14), (7) следует, что существует число n такое, что

$$x = \psi_{m,\,n}. \tag{15}$$

Согласно лемме 6 из (14), (1), (12), (6), (9) следует, что существуют числа i, j такие, что

$$v = \varphi_{2j}, \quad n = (2k + 1)i + j. \tag{16}$$

Согласно лемме 7 из (14), (5), (15), следует, что $x \equiv n \pmod{l}$. Отсюда и из (8), (16), (13) следует, что

$$u \equiv j \pmod{l}. \tag{17}$$

Согласно лемме 19 из (16) следует, что $j \leqslant v$. Отсюда и из (1), (17) следует, что $u = j$ и, согласно (16), $v = \varphi_{2u}$. Достаточность установлена.

Необходимость. Пусть $v = \varphi_{2u}$. Согласно лемме 19 первое неравенство в (1) выполнено. Положим $l = \varphi_{6s+1}$, $z = \varphi_{6s}$, где s столь велико, что выполнено и второе неравенство в (1). Согласно лемме 8, условие (2) выполнено. Положим $g = \varphi_{l(6s+1)}$, $h = \varphi_{l(6s+1)-1}$. Согласно лемме 17, условие (4) выполнено. Согласно лемме 12, l нечетно, ибо $2 = \varphi_3$. Поэтому, согласно лемме 8, условие (3) также выполнено. Согласно лемме 12, н.о.д.$(h, g) = 1$ и, так как l нечетно и делит g, то н.о.д.$(2h + g, l) = 1$. Поэтому, согласно китайской теореме об остатках, мы можем выбрать число m так, что условия (5)—(6) будут выполнены. Положим $x = \psi_{m, u}$, $y = \psi_{m, u+1}$. Согласно лемме 10, выполнено условие (7); согласно лемме 7, выполнено условие (8); согласно лемме 5, выполнено условие (9). Необходимость доказана.

Условия (1)—(9) легко могут быть заменены одним диофантовым предикатом (см. ([4], [5])). Таким образом, предикат «v есть $2u$-е число Фибоначчи» является диофантовым. Из леммы 19 следует, что он имеет экспоненциальный рост.

4. Некоторые конструкции настоящей работы навеяны методами Дж. Робинсон из статьи ([8]).

Ленинградское отделение
Математического института им. В. А. Стеклова
Академии наук СССР

Поступило
5 II 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] D. Hilbert, Gesammelte Abhandlungen, 3, Berlin, 1935. [2] M. Davis, H. Putnam, J. Robinson, Ann. Math., 74, 3, 425 (1961); Сборн. пер. Математика, 8, 5, 69 (1964). [3] J. Robinson, Trans. Am. Math. Soc., 72, 3, 437 (1952); Сборн. пер. Математика, 8, 5, 3 (1964). [4] А. И. Мальцев, Алгоритмы и рекурсивные функции, М., 1965. [5] M. Davis, Computability and Unsolvability, N. Y., 1958. [6] H. Putnam, J. Symb. Logic, 25, 3, 220 (1960); Сборн. пер. Математика, 8, 5, 55 (1964). [7] Н. Н. Воробьев, Числа Фибоначчи, М., 1969. [8] J. Robinson, Proc. Am. Math. Soc., 22, 2, 534 (1969).