Доклады Академии наук СССР
1971. Том 196, № 4

УДК 511.9

МАТЕМАТИКА

Ю. В. МАТИЯСЕВИЧ

ДИОФАНТОВО ПРЕДСТАВЛЕНИЕ МНОЖЕСТВА ПРОСТЫХ ЧИСЕЛ

(Представлено академиком Ю. В. Линником 8 VII 1970)

В работе (1) доказано, что существует полином с целыми коэффициентами, множество натуральных значений которого при натуральных значениях переменных есть в точности множество всех простых чисел. Это доказательство конструктивно, т. е. позволяет выписать фактически такой полином. Однако это будет полином от сотен переменных. В настоящей заметке мы укажем полином 37-й степени от 24 переменных, представляющий множество простых чисел в указанном выше смысле. Кроме того, мы дадим простое диофантово представление одного отношения, имеющего экспоненциальный рост, а также простые диофантовы представления отношений $q = p^k$, $c = \binom{n}{k}$ и $l = k!$ Простые диофантовы представления этих отношений, с одной стороны, интересны сами по себе, с другой стороны, диофантовы представления этих отношений используются для построения полиномов, задающих произвольные перечислимые отношения, в частности, для построения полиномов Q, R, S и D из работы (1).

1. Сделаем несколько замечаний, касающихся применяемых обозначений.

Строчные латинские буквы и греческие φ и ψ используются в тех же целях, что и в (1).

Если одно из уравнений некоторой системы может быть приведено к виду $x = P$, где P — полином, не содержащий x, то мы можем исключить это уравнение из системы, а во всех остальных заменить x на P. Чтобы избежать громоздких выражений, мы не будем делать такие преобразования, а вместо этого будем отмечать знаком τ те переменные и уравнения, которые могут быть исключены указанным способом.

Указывая диофантово представление того или иного отношения, мы будем наряду с диофантовыми уравнениями использовать условия, имеющие вид $P < Q$, $P \leqslant Q$, $P \mid Q$, где P и Q — полиномы. Вводя новые переменные, мы можем заменить такие условия диофантовыми уравнениями (соответственно $P + w = Q$, $P + w - 1 = Q$, $Pw = Q$). При этом может оказаться, что получившееся уравнение может быть исключено описанным выше способом. Исключаемую в этом случае переменную мы также будем отмечать знаком τ.

Ссылки на леммы относятся к леммам из (1), если не оговорено другое.

2. Рассмотрим следующую систему условий:

$$l^2 - lv - v^2 = 1; \tag{1}$$

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

$$(\tau g) \quad l^2 \mid g; \tag{3}$$

$$(\tau h) \quad h = 2e; \tag{4}$$

$$(\tau m) \quad m = 3 + (2h + g)e; \tag{5}$$

$$x^2 - mxy + y^2 = 1; \tag{6}$$

$$(\tau y) \quad l \mid y + 1 - u; \tag{7}$$

$$(\tau x) \quad 2h + g \mid x - v. \tag{8}$$

Теорема 1. *Если числа* $u, v, l, g, h, e, m, x, y$ *удовлетворяют условиям* (1)—(8), *то* $v \leqslant \varphi_{2u}$; *если и делится на* 24, *то существуют числа* v, l, g, h, e, m, x, y, *которые удовлетворяют условиям* (1)—(8) *и условию* $v = \varphi_{2u}$.

Доказательство основано на тех же идеях, что и доказательство теоремы в [1]. Укажем лишь имеющиеся различия.

Налагаемое в [1] условие $u \leqslant v$ в данном случае является лишним, ибо если $v < u$, то тем более $v < \varphi_{2u}$. Из (1) следует, что $v < l$, поэтому излишне выписывать это условие отдельно. Нетрудно показать, что из условий (2)—(5) следует, что $l \mid m - 2$, и потому это условие также исключено. Условие $l \mid x - u$ из [1] заменено условием (7), в связи с этим заключительная часть доказательства первой половины теоремы немного отличается от конца доказательства достаточности в [1].

При доказательстве второй части теоремы следует положить $l = \varphi_{2u+1}$, $g = \varphi_{l(2u+1)}$, $h = \varphi_{l(2u+1)-1}$. Как нетрудно показать, h будет четным числом, и можно будет выбрать e так, чтобы удовлетворить условию (4). Число m выбирается согласно (5), в качестве x и y берутся соответственно числа $\psi_{m,u}$ и $\psi_{m,u-1}$. Аналогично доказательству необходимости из [1] можно показать, что при этом все условия (1)—(8) будут выполнены.

3. Теорема 2. *Для того чтобы* $q = p^k$, *необходимо и достаточно, чтобы существовали числа* $a, e, g, l, m, r, s, t, u, v, x, y, z$ *такие, что выполнены условия* (1)—(8), *а также условия:*

$$u^2 - auz + z^2 = 1; \tag{9}$$

$$(\tau u) \qquad a - 2 \mid u; \tag{10}$$

$$(\tau a) \qquad a = p + q + k + 3; \tag{11}$$

$$s^2 - ust + t^2 = 1; \tag{12}$$

$$(\tau v) \qquad t < v; \tag{13}$$

$$(\tau s) \qquad u - 2 \mid s - k; \tag{14}$$

$$(\tau t) \quad t = q + (u - p)s + (pu - p^2 - 1)(r - 1). \tag{15}$$

Достаточность. Пусть числа $q, p, k, a, \ldots, z$ удовлетворяют условиям (1)—(15). По лемме 11 из (9) следует, что существует число w такое, что $u = \psi_{a,w}$. По лемме 7 $w \equiv u \pmod{a-2}$ и, согласно (10), $a - 2 \mid w$. Следовательно, $w \geqslant a - 2$.

Аналогично лемме 19 можно доказать, что для всех n и $d \geqslant 2$

$$(d-1)^{n-1} \leqslant \psi_{d,n} < d^n. \tag{16}$$

Поэтому $u \geqslant (a-1)^{w-1} > (a-1)^{a-3}$. Из этого неравенства и условия (11) легко вывести, что

$$u > 125, \quad u > p, \quad u - 2 > k,$$
$$pu - p^2 - 1 > p^k, \quad pu - p^2 - 1 > q. \tag{17}$$

Из (15) и (17) следует, что $t > s$, а отсюда и из (12) по лемме 11 вытекает, что существует число c такое, что $s = \psi_{u,c}$, $t = \psi_{u,c+1}$. Согласно неравенствам (17), (16) и (13), теореме 1 и лемме 19 имеем

$$124^c < (u-1)^c \leqslant \psi_{u,c+1} = t < v \leqslant \varphi_{2u} < 3^u. \tag{18}$$

По лемме 7 $c \equiv s \pmod{u-2}$ и по условию (14) $c \equiv k \pmod{u-2}$. Из (18) следует, что $c < u - 2$ и, следовательно, ввиду (17), $c = k$.

С помощью индукции легко доказать, что для любых b, $d \geqslant 2$ и j

$$\psi_{d,j+1} - (d-b)\psi_{d,j} \equiv b^j \pmod{bd - b^2 - 1} \text{ *}. \tag{19}$$

Поэтому из (15) следует, что $q \equiv p^k \pmod{pu - p^2 - 1}$ и, ввиду (17), $q = p^k$. Достаточность установлена.

* Это утверждение аналогично лемме 5 из работы [2], в которой указано, как можно найти диофантово представление отношения $q = p^k$, имея диофантово отношение с экспоненциальным ростом; мы, однако, пользуемся другим способом, требующим меньшего числа дополнительных переменных.

Необходимость. Пусть $q = p^k$. Выберем a согласно (11). Легко показать, что последовательность остатков от деления чисел $\psi_{a,0}, \psi_{a,1}, \ldots$ на любое число является чисто периодической. Поэтому мы можем выбрать сколь угодно большое число w так, чтобы $24(a-2) \mid \psi_{a,w}$. Положим $u = \psi_{a,w}$, $z = \psi_{a,w+1}$, где w столь велико, что $u^{k+1} < 2^{u-1}$. Условие (10) выполнено.

Положим $s = \psi_{u,k}$, $t = \psi_{u,k+1}$. По лемме 10 выполнены условия (9) и (12). По лемме 7 выполнено условие (14). Используя (19) и (17), легко показать, что можно найти число r, удовлетворяющее условию (15).

Положим $v = \varphi_{2u}$. Согласно (16), выбору числа u и лемме 19, имеем

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

Следовательно, условие (13) выполнено. По теореме 1 можно выбрать числа e, g, h, l, m, x, y так, чтобы были выполнены условия (1)—(9). Необходимость доказана.

Замечание. Для того чтобы получить диофантово представление $3n$-местного отношения

$$q_1 = p_1^{k_1} \& \ldots \& q_n = p_n^{k_n}, \tag{20}$$

нет необходимости n раз копировать все уравнения (1)—(15). Достаточно уравнения (11)—(15) заменить на следующие:

$$(\tau a) \quad a = p_1 + \ldots + p_n + q_1 + \ldots + q_n + k_1 + \ldots + k_n + 3; \tag{11'}$$

$$s_i^2 - u s_i t_i + t_i^2 = 1 \quad (i = 1, \ldots, n); \tag{12'}$$

$$(\tau v) \quad t_1 + \ldots + t_n < v; \tag{13'}$$

$$(\tau s_i) \quad u - 2 \mid s_i - k_i \quad (i = 1, \ldots, n); \tag{14'}$$

$$(\tau t_i)\ t_i = q_i + (u - p_i)\, s_i + (p_i u - p_i^2 - 1)(r_i - 1) \quad (i = 1, \ldots, n). \tag{15'}$$

При этом если k_b совпадает с k_c, то можно проделать упрощения: исключить k_b и t_b из (11′) и (13′) соответственно, исключить условия (12′) и (14′) при $i = b$, а условие (15′) при $i = b$ заменить на

$$t_c = q_b + (u - p_b)\, s_c + (p_b u - p_b^2 - 1)(r_b - 1). \tag{15''}$$

Если мы исключим еще все переменные, отмеченные знаком τ, то для диофантова представления отношения (20) нам потребуется $n + n' + 8$ дополнительных переменных, где n' — число различных показателей степеней в (20).

4. Доказательства следующих двух теорем основаны на идеях пятого раздела работы ([2]). Эти же идеи изложены в ([3]), на стр. 367 — 369.

Теорема 3. *Для того чтобы* $c = \binom{n}{k}$, *необходимо и достаточно, чтобы существовали числа* p, q, r, w, z *такие, что*

$$p = 2^n, \quad q = (p+1)^n, \quad r = p^k; \tag{21}$$

$$(\tau q) \quad q = (w-1)\, pr + cr + z; \tag{22}$$

$$(\tau r) \quad z < r, \quad (\tau p) \quad c < p. \tag{23}$$

Доказательство (ср. ([2], [3])). Согласно условиям (21)—(23) c является $(k+1)$-й справа цифрой в записи числа $(p+1)^n$ в p-ичной системе счисления. Остается воспользоваться известным разложением бинома Ньютона.

Теорема 4. *Для того чтобы* $l = k!$, *необходимо и достаточно, чтобы существовали числа* $c, h, m, n, p, q, r, t, w, z$ *такие, что выполнены условия* (21)—(23), *а также условия*:

$$t = (2k)^k, \quad m = n^k, \tag{24}$$

$$(\tau n) \quad n = 3kt, \quad (\tau m) \quad m = lc + h - 1, \tag{25}$$

$$(\tau c) \quad h - 1 < c. \tag{26}$$

Доказательство. Согласно теореме 1 $c = \binom{n}{k}$. Из (24)—(26) следует, что

$$l = \left[\frac{n^k}{\binom{n}{k}} \right]. \tag{27}$$

Так как $n > (2k)^{k+1}$, то, как показано в ([2], [3]), равенство (27) эквивалентно равенству $l = k!$.

Теорема 5. *Для того чтобы $k+1$ было простым числом, необходимо и достаточно, чтобы существовали числа $b, c, h, m, n, p, q, r, t, w, z$ такие, что выполнены условия* (21)—(26) *и условие*

$$(\tau l) \quad l = (k+1)b - 1. \tag{28}$$

Доказательство. По теореме 4 $l = k!$. Остается воспользоваться теоремой Вильсона.

5. Исключим из системы, состоящей из условий (21)—(26) и (28), переменные, отмеченные знаком τ, а условия (21) и (24) заменим системой диофантовых уравнений. Для этого нам потребуется, согласно замечанию к теореме 2, ввести 15 новых переменных. Перенесем все члены получившихся уравнений в левую часть и обозначим через Q сумму квадратов левых частей всех уравнений. Ясно, что уравнение $Q = 0$ имеет решения тогда и только тогда, когда $k+1$ — число простое.

Обозначим через P полином $(k+1)(1-Q)$. Следуя доказательству теоремы 1 из ([4]), легко можно показать, что множество положительных значений полинома P есть в точности множество всех простых чисел. Несложный подсчет показывает, что P — это полином 37-й степени от 24 переменных.

6. Мы ограничили область изменения переменных множеством целых положительных чисел, однако легко расширить ее до множества всех целых чисел. Традиционный способ такого расширения состоит в использовании теоремы Лагранжа о том, что любое целое неотрицательное число представимо в виде суммы квадратов четырех целых чисел (см. ([3], [4])). Однако существует более экономный (по числу переменных) способ. Любое число вида $4i+1$ представимо в виде суммы квадратов трех целых чисел (см. ([5])). Ясно, что ровно одно из этих чисел нечетно, и потому i представимо в виде $\alpha^2 + \beta^2 + \gamma^2 + \gamma$, где α, β, γ — целые числа. Поэтому натуральные числа, и только они, представимы в виде $\alpha^2 + \beta^2 + \gamma^2 + \gamma + 1$.

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

Поступило
30 VI 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Ю. В. Матиясевич, ДАН, 191, № 2, 279 (1970). [2] J. Robinson, Trans. Am. Math. Soc., 72, 3, 437 (1952); Сборн. пер. Математика, 8, 5, 3 (1964). [3] А. И. Мальцев, Алгоритмы и рекурсивные функции, М., 1965. [4] H. Putnam, J. Symb. Logic, 25, 3, 220 (1969); Сборн. пер. Математика, 8, 5, 55 (1964). [5] H. Davenport, The Higher Arithmetic, London, 1952; Дэвенпорт, Высшая арифметика, М., 1965.