



# Math-Net.Ru

Общероссийский математический портал

Ю. В. Матиясевич, Арифметические представления степеней, *Зап. научн. сем. ЛОМИ*, 1968, том 8, 159–165

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.97.14.83

3 декабря 2024 г., 07:33:08



АРИФМЕТИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ СТЕПЕНЕЙ<sup>\*</sup>)

М. Дэвис, Х. Путнам и Дж. Робинсон [1 - 2] доказали, что любое перечислимое множество натуральных<sup>\*\*</sup>) чисел диофантово, если диофантов предикат<sup>\*\*\*</sup>)  $q \text{ Pow } p$ . Несколько изменив их рассуждения, можно доказать, что диофантовость предиката  $q \text{ Pow}(2n+1)$  также влечет диофантовость любого перечислимого множества. В настоящей работе рассматриваются некоторые вопросы, связанные с арифметическими представлениями предиката  $q \text{ Pow}(2n+1)$ .

1. Пусть  $p$  - произвольное нечетное число,  $k$  - произвольное число,

$$t_m = \sum_{0 \leq i \leq \frac{m}{2}} \binom{m}{2i} k^{m-2i} (k^2 - p)^i, \quad (1)$$

<sup>\*</sup>) Результаты настоящей заметки были доложены на Ленинградском семинаре по конструктивной математике 23 ноября 1967 г.

<sup>\*\*</sup>) Натуральными мы называем целые неотрицательные числа. Строчные латинские буквы, быть может с нижними индексами, везде ниже являются переменными для натуральных чисел.

<sup>\*\*\*</sup>) Следуя работе [1], мы обозначаем через  $q \text{ Pow } p$  предикат „ $q$  есть натуральная степень числа  $p$ “.

$$S_m = \sum_{1 \leq i \leq \frac{m+1}{2}} \binom{m}{2i-1} k^{m-2i+1} (k^2 - p)^{i-1} \quad (2)$$

( $m = 0, 1, \dots$ ).

Имеем:

$$\begin{aligned} p^m &= (k + \sqrt{k^2 - p})^m (k - \sqrt{k^2 - p})^m = \\ &= (t_m + s_m \sqrt{k^2 - p}) (t_m - s_m \sqrt{k^2 - p}) = \\ &= t_m^2 - (k^2 - p) s_m^2, \end{aligned} \quad (3)$$

$$t_m \equiv k^m \cdot 2^{m-1} \pmod{p} \quad (m \geq 1). \quad (4)$$

Из (1-4) получаем, что\*

$$\begin{aligned} & q \text{ Pow } (2n+1) \Rightarrow \\ & \Rightarrow \forall k \exists t s [\langle q = t^2 - (k^2 - 2n - 1) s^2 \rangle \& \\ & \& \langle k \text{ Copr } (2n+1) \supset t \text{ Copr } s \rangle]. \end{aligned} \quad (5)$$

2. Пусть  $l$  - число, не являющееся полным квадратом,

\* По аналогии с записью предиката  $q \text{ Pow } p$  мы обозначаем через  $b \text{ Copr } d$  предикат "числа  $b$  и  $d$  взаимно просты". При этом мы считаем, что  $0 \text{ Copr } 1, \neg(0 \text{ Copr } j)$  ( $j \neq 1$ ).

$\frac{x}{y}$  и  $\frac{t}{s}$  — две последовательные подходящие дроби<sup>\*)</sup> для числа  $\sqrt{\ell}$ ,  $\tau$  — остаток такой, что

$$\frac{x + \tau t}{y + \tau s} = \sqrt{\ell}. \quad (6)$$

Перепишем (6) следующим образом:

$$\tau = \frac{lsy - tx \pm \sqrt{\ell}}{t^2 - ls^2} \quad (7)$$

Мы будем говорить, что остаток (7) соответствует дроби  $\frac{t}{s}$ .

3. Пусть  $p$  — произвольное нечетное число,

$$k = p^m + \frac{p+1}{2} \quad (m \geq 1).$$

Известно<sup>\*\*)</sup>, что квадратичная иррациональность при разложении в цепную дробь имеет лишь конечное число различных остатков. Нетрудно проверить, что остатками для числа  $\sqrt{k^2 - p}$  являются следующие и только следующие числа:

$$\frac{\sqrt{k^2 - p}}{1}, \frac{\Delta}{p}, \frac{\Delta}{p^2}, \dots, \frac{\Delta}{p^m}, \frac{\Sigma}{p^m}, \frac{\Sigma}{p^{m-1}}, \dots, \frac{\Sigma}{1}, \quad (8)$$

$$\frac{\Sigma}{2p^m}, \frac{\Sigma}{2p^{m-1}}, \dots, \frac{\Sigma}{2}, \frac{\Delta}{2p}, \frac{\Delta}{2p^2}, \dots, \frac{\Delta}{2p^m}, \quad (9)$$

<sup>\*)</sup> Терминологию, относящуюся к цепным дробям, мы заимствуем из монографии [3].

<sup>\*\*)</sup> См., например, [3].

где  $\Delta = k - p + \sqrt{k^2 - p}$ ,  $\Sigma = k - 1 + \sqrt{k^2 - p}$ ,  
 причем остатки (8) соответствуют подходящим дробям нечетного  
 порядка, а остатки (9) — дробям четного порядка.

4. Из результатов, полученных Р.Робинсоном в [4], следует,  
 что можно построить полином с целыми коэффициентами  
 $P(b, k, t, s, x, y, n, q)$  такой, что

$$\begin{aligned} & q \text{Pow}(2n+1) \Leftrightarrow \\ & \Leftrightarrow \exists b \forall k \exists t s x y [P(b, k, t, s, x, y, n, q) = 0] \Leftrightarrow \\ & \Leftrightarrow \exists b \forall k_{\leq b} \exists t s x y [P(b, k, t, s, x, y, n, q) = 0]. \end{aligned}$$

Получающийся по конструкции Р.Робинсона полином весьма  
 громоздок и трудно выписать его явным образом. Мы докажем, что

$$\begin{aligned} & q \text{Pow}(2n+1) \Leftrightarrow \\ & \Leftrightarrow \forall k \exists t s x y [M(k, t, s, x, y, n, q) = 0] \Leftrightarrow \\ & \Leftrightarrow \forall k_{\leq q} \exists t s x y [M(k, t, s, x, y, n, q) = 0], \end{aligned}$$

где

$$\begin{aligned} M(k, t, s, x, y, n, q) = & \{t y - x s - 1\}^2 + \\ & + \{q - t^2 + [\langle (2n+1)(k+1) + n+1 \rangle^2 - 2n - 1] s^2\}^2. \end{aligned}$$

Действительно, из (5) следует, что

$$\begin{aligned} & q \text{Pow}(2n+1) \Rightarrow \\ & \Rightarrow \forall k \exists t s x y [M(k, t, s, x, y, n, q) = 0]. \end{aligned}$$

Пусть теперь числа  $q$  и  $n$  таковы, что

$$\forall k \leq q \exists t s x y [M(k, t, s, x, y, n, q) = 0]. \quad (10)$$

Найдем число  $k$  такое, что

$$\langle (k+1) \text{Pow}(2n+1) \rangle \& \langle \frac{q}{2n+1} \leq k+1 \leq q \rangle,$$

и построим согласно (10) числа  $t, s, x, y$  такие, что

$$M(k, t, s, x, y, n, q) = 0. \quad (11)$$

Если  $s = 0$ , то из (11) получаем, что  $q = 1$  и, следовательно,  $q \text{Pow}(2n+1)$ .

Пусть  $s > 0$ . Из (11) получаем, что

$$t \text{ Copr } s, \quad (12)$$

$$0 < \frac{t}{s} - \sqrt{\langle (2n+1)(k+1) + n+1 \rangle^2 - 2n-1} < \frac{1}{2s^2}. \quad (13)$$

Согласно известной теореме об аппроксимации рациональными числами<sup>\*</sup> из (12-13) следует, что дробь  $\frac{t}{s}$  является подходящей дробью для числа

$$\sqrt{\langle (2n+1)(k+1) + n+1 \rangle^2 - 2n-1},$$

---

\* См., например [3].

причем, очевидно, дробью нечетного порядка. Отсюда ввиду (7-8) следует, что  $q \text{ Pow } (2n+1)$ .

5. Пусть  $p$  — некоторое нечетное число. Допустим, что некоторое бесконечное подмножество множества степеней числа  $p$  диофантово. Докажем, что в этом случае диофантовым является также множество всех степеней числа  $p$ .

Пусть предикат  $Q(z)$  обладает следующими свойствами:

$$a) \forall z [Q(z) \supset z \text{ Pow } p];$$

$$b) \forall u \exists z [\langle z > u \rangle \& Q(z)].$$

Из (5), (7-8) следует, что

$$q \text{ Pow } p \Leftrightarrow \exists z t s [Q(z) \& \langle z > q \rangle \& \langle t \text{ Copr } s \rangle \& \langle q = t^2 - ((pz + \frac{p+1}{2})^2 - p) s^2 \rangle].$$

Аналогичная теорема верна и для двуместного предиката  $q \text{ Pow } (2n+1)$ . Пусть предикат  $z Q_n$  таков, что

$$a) \forall n z [z Q_n \supset z \text{ Pow } (2n+1)];$$

$$b) \forall n u \exists z [\langle z > u \rangle \& z Q_n].$$

Тогда

$$q \text{ Pow } (2n+1) \Leftrightarrow \exists z t s [z Q_n \& \langle z > q \rangle \& \langle t \text{ Copr } s \rangle \& \langle q = t^2 - (((2n+1)z + n + 1)^2 - 2n - 1) s^2 \rangle].$$

6. Автор выражает признательность С.Ю.Маслову, который сделал ряд ценных замечаний по изложению работы.

### Литература

1. Robinson J. Existential definability in arithmetic. "Trans. Amer. Math. Soc.", 1952, 72, № 3, 437-449. (Имеется русский перевод: Робинсон Дж., Экзистенциальная выразимость в арифметике, сб. "Математика", 1964, 8 : 5, 3-14).
2. Davis M., Putnam H., Robinson J. The decision problem for exponential diophantine equations. "Annals of Math.", 1961, 74, № 3, 425-436. (Имеется русский перевод: Дэвис М., Путнам Х., Робинсон Дж., Проблема разрешимости для показательно-диофантовых уравнений, сб. "Математика", 1964, 8 : 5, 69-79).
3. Хинчин А.Я. Цепные дроби. М., 1961.
4. Robinson R.M. Arithmetical representation of recursively enumerable sets. "J. Symbolic Logic", 1956, 21, № 2, 162-186. (Имеется русский перевод: Робинсон Р.М., Арифметическое представление степеней, сб. "Математика", 1964, 8 : 5, 23-47).