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

Ю.В.Матиясевич

АРИФМЕТИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ СТЕПЕНЕЙ*)

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

I. Пусть p — произвольное нечетное число, k — произвольное число,

$$t_m = \sum_{0\le i\le \frac{m}{2}} \binom{m}{2i} k^{m-2i}(k^2-p)^i, \tag{I}$$

---

*) Результаты настоящей заметки были доложены на Ленинградском семинаре по конструктивной математике 23 ноября 1967 г.

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

***) Следуя работе [I], мы обозначаем через $q\,\mathfrak{Pow}\,p$ предикат „ q есть натуральная степень числа p ".

$$s_m = \sum_{1 \le i \le \frac{m+1}{2}} \binom{m}{2i-1} k^{m-2i+1} (k^2 - p)^{i-1} \qquad (m = 0, 1, \ldots). \tag{2}$$

Имеем:

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

$$t_m \equiv k^m \cdot 2^{m-1} (\mathrm{mod}\ p) \qquad (m \geqslant 1). \tag{4}$$

Из (I-4) получаем, что*)

$$\begin{aligned} & q\,\mathcal{P}ow\,(2n+1) \Rightarrow \\ & \Rightarrow \forall k\, \exists t s\, [\langle q = t^2 - (k^2 - 2n - 1) s^2 \rangle \,\& \\ & \& \,\langle k\ \mathrm{Copr}\ (2n+1) \supset t\ \mathrm{Copr}\ s \rangle]. \end{aligned} \tag{5}$$

2. Пусть ℓ – число, не являющееся полным квадратом,

---

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

$\frac{x}{y}$ и $\frac{t}{s}$ — две последовательные подходящие дроби[ж)] для числа $\sqrt{\ell}$, τ — остаток такой, что

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

Перепишем (6) следующим образом:

$$\tau=\frac{\ell s y - t x \pm \sqrt{\ell}}{t^2-\ell s^2} \tag{7}$$

Мы будем говорить, что остаток (7) с о о т в е т с т в у е т дроби $\frac{t}{s}$.

3. Пусть p — произвольное нечетное число,

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

Известно[жж)], 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:

$$\frac{\sqrt{k^2-p}}{1},\ \frac{\Delta}{p},\ \frac{\Delta}{p^2},\ldots,\frac{\Delta}{p^m},\ \frac{\Xi}{p^m},\ \frac{\Xi}{p^{m-1}},\ldots,\frac{\Xi}{1}, \tag{8}$$

$$\frac{\Xi}{2p^m},\ \frac{\Xi}{2p^{m-1}},\ldots,\frac{\Xi}{2},\ \frac{\Delta}{2p},\ \frac{\Delta}{2p^2},\ldots,\frac{\Delta}{2p^m}, \tag{9}$$

ж) Терминологию, относящуюся к цепным дробям, мы заимствуем из монографии [3].

жж) См., например, [3].

где $\Delta = k - p + \sqrt{k^2 - p}$, $\Xi = k - 1 + \sqrt{k^2 - p}$,

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

$$q\,\mathcal{P}ow\,(2n+1) \Leftrightarrow$$

$$\Leftrightarrow \exists b \forall k \exists t s x y [P(b,k,t,s,x,y,n,q)=0] \Leftrightarrow$$

$$\Leftrightarrow \exists b \forall k_{\leq b} \exists t s x y [P(b,k,t,s,x,y,n,q)=0].$$

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

$$q\,\mathcal{P}ow\,(2n+1) \Leftrightarrow$$

$$\Leftrightarrow \forall k \exists t s x y [M(k,t,s,x,y,n,q)=0] \Leftrightarrow$$

$$\Leftrightarrow \forall k_{\leq q} \exists t s x y [M(k,t,s,x,y,n,q)=0],$$

где

$$M(k,t,s,x,y,n,q) = \{ty - xs - 1\}^2 +$$

$$+ \{q - t^2 + [\langle (2n+1)(k+1)+n+1 \rangle^2 - 2n - 1] s^2\}^2.$$

Действительно, из (5) следует, что

$$q\,\mathcal{P}ow\,(2n+1) \Rightarrow$$

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

Пусть теперь числа q и n таковы, что

$$\forall k_{\leq q}\ \exists tsxy\,[M(k,t,s,x,y,n,q)=0]. \qquad (10)$$

Найдем число k такое, что

$$\langle (k+1)\ \mathcal{P}ow\ (2n+1)\rangle \,\&\, \langle \frac{q}{2n+1} \leq k+1 \leq q \rangle,$$

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

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

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

Пусть $s>0$. Из (11) получаем, что

$$t\ \mathcal{C}opr\ s, \qquad (12)$$

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

Согласно известной теореме об аппроксимации рациональными числами*) 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 $q \,\mathcal{P}ow\, (2n+1)$.

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:

а) $\forall z\,[Q(z) \supset z \,\mathcal{P}ow\, p]$;

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

Из (5), (7-8) следует, что

$$q \,\mathcal{P}ow\, p \Leftrightarrow \exists z t s\,[Q(z) \,\&\, \langle z > q\rangle \,\&$$

$$\& \langle t \,\mathrm{Copr}\, s\rangle \,\&\, \langle q = t^2 - ((pz + \frac{p+1}{2})^2 - p)\, s^2\rangle].$$

Аналогичная теорема верна и для двуместного предиката $q \,\mathcal{P}ow\, (2n+1)$. Пусть предикат $z\,Q\,n$ таков, что

а) $\forall n z\,[z\,Q\,n \supset z \,\mathcal{P}ow\, (2n+1)]$;

б) $\forall n u \exists z\,[\langle z > u\rangle \,\&\, z\,Q\,n]$.

Тогда

$$q \,\mathcal{P}ow\, (2n+1) \Leftrightarrow \exists z t s\,[z\,Q\,n \;\&$$

$$\& \langle z > q\rangle \,\&\, \langle t \,\mathrm{Copr}\, s\rangle \,\&$$

$$\& \langle q = t^2 - (((2n+1)z + n + 1)^2 - 2n - 1)\, s^2\rangle].$$

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., Экзистенциональная 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).