© «Вестник ИГЭУ» Вып. 1 2011 г.

УДК 511.6

ОБ АССОЦИИРОВАННОСТИ РЕШЕНИЙ ДИОФАНТОВЫХ УРАВНЕНИЙ

Э.Т. АВАНЕСОВ, В.А. ГУСЕВ, кандидаты физ.-мат. наук

В терминах сравнений приведена теорема об ассоциативности двух произвольных решений диофантовых уравнений, доказана оценка числа попарно не ассоциированных элементов модуля М с данной нормой.

Ключевые слова: диофантово уравнение, разложимые формы, рациональные числа, признак ассоциированности.

ON DECISIONS ASSOCIATIVITY OF DIOPHANTINE EQUATIONS

E.T. AVANESOV, V.A. GUSEV, Candidates of Physics and Mathematics

The authors consider the associativity theorem of two arbitrary decisions of Diophantine Equations using the comparison terms. The authors show the number estimation of not associated elements of M module with the given standard.

Key words: Diophantine Equation, decomposable forms, rational numbers, sing of associativity.

Рассмотрим вопрос о представлении целых рациональных чисел разложимыми формами.

Наряду с представлением целого рационального числа N полной формой

$$F(x,y,z) = Norm(x + y\lambda + z\lambda^2) = N, \qquad (1)$$

исследуем и диофантово уравнение

$$f(x,y) = x^3 + p_1x^2y - p_2xy^2 + p_3y^3 = N. \qquad (2)$$

Для уравнений (1) и (2) представляет интерес разрешение вопросов расчета: 1) оценок величины решений; 2) нахождения представителей классов решений; 3) оценки числа попарно не ассоциированных элементов с данной нормой; 4) признака ассоциированности двух решений [1]; 5) критериев неразрешимости, частично распространяемых на произвольные уравнения

$$F(x_0,y_1,\dots,x_n) = Norm(x_0 + x_1\lambda + \dots + x_{n-1}\lambda^{n-1}) = N. \qquad (3)$$

Очевидно, уравнение $(3;\ N=1)$ всегда разрешимо, но не всегда можно найти целые значения для x_i $(i = 0,1,\dots,n-1)$, удовлетворяющие уравнению $(3;\ N \neq 1)$.

Пусть $w = x_0 + x_1\lambda + \dots + x_{n-1}\lambda^{n-1}$ – решение (3), тогда если $\varepsilon = \ell_0 + \ell_1\lambda + \dots + \ell_{n-1}\lambda^{n-1}$ – единица, то и $w\varepsilon$ тоже решение (3).

Исходя из некоторого определенного решения (3), можно, умножая на все решения $(3;\ N=1)$, получить бесчисленное множество решений уравнения (3).

Найденные таким путем решения принято называть *классом* решений, а сами решения из одного класса – *ассоциированными* [1].

Предварительно сформируем три леммы, справедливость которых очевидна и усматривается непосредственно.

ЛЕММА 1. Форма $F(x_0,x_1,\dots,x_{n-1})$ мультипликативна.

ЛЕММА 2. Пусть $F(w) = Norm w$, тогда

$$\bar{w} = \frac{1}{w}F(w) = \bar{x}_0 + \bar{x}_1\lambda + \dots + \bar{x}_{n-1}\lambda^{n-1} = \Phi(x_0,x_1,\dots,x_{n-1})$$

и все $x_i = \phi_i(x_0,x_1,\dots,x_{n-1})$ $(i = 0,1,\dots,n-1)$ являются формами степени $n-1$ от переменных x_i с коэффициентами, зависящими от $p_i (i = 1,2,\dots,n)$.

ЛЕММА 3. Пусть $w_z = w_x w_y$, где

$$w_x = x_0 + x_1\lambda + \dots + x_{n-1}\lambda^{n-1},$$
$$w_y = y_0 + y_1\lambda + \dots + y_{n-1}\lambda^{n-1},$$
$$w_z = z_0 + z_1\lambda + \dots + z_{n-1}\lambda^{n-1}.$$

Тогда имеют место формулы, где принято $p_0 = 1$:

$$z_0 = x_0y_0 + p_n\sum_{i=1}^{n-1}\sum_{j=0}^{n-1-i} x_{i+j}y_{n-1-j} \times$$
$$\times \sum_{\alpha_1+2\alpha_2+\dots+(i-1)\alpha_{i-1}=i-1} \frac{(\alpha_1+\alpha_2+\dots+\alpha_{i-1})!}{\alpha_1!\alpha_2!\dots\alpha_{i-1}!}\cdot\prod_{m=0}^{i-1} p_m^{\alpha_m},$$
$$z_k = \sum_{i=0}^{k} x_iy_{k-i} + \sum_{j=1}^{n-1}\sum_{\ell=0}^{n-1-j} x_{j+\ell}y_{n-1-\ell}\cdot\sum_{m=0,m\le k}^{j=1} p_{n-k+m}\times$$
$$\times \sum_{\alpha_1+\dots+(j-m-1)\alpha_{j-m-1}=i-1} \frac{(\alpha_1+\alpha_2+\dots+\alpha_{j-m-1})!}{\alpha_1!\alpha_2!\dots\alpha_{j-m-1}!}\times$$
$$\times\prod_{t=0}^{j-m-1} p_t^{\alpha_t},$$

k = 1, 2,... , n–2;

$$z_{n-1} = \sum_{i=0}^{n-1} x_iy_{n-1-i} + \sum_{j=1}^{n-1}\sum_{\ell=0}^{n-1-j} x_{j+\ell}y_{n-1-\ell}\times$$
$$\times \sum_{\alpha_1+2\alpha_2+\dots+j\alpha_j=j} \frac{(\alpha_1+\alpha_2+\dots+\alpha_j)!}{\alpha_1!\alpha_2!\dots\alpha_j!}\cdot\prod_{m=1}^{j} p_m^{\alpha_m}.$$

Следующая теорема устанавливает арифметический признак ассоциированности двух решений.

ТЕОРЕМА 1. Для того, чтобы два решения

$$w_x = x_0 + x_1\lambda + \dots + x_{n-1}\lambda^{n-1}$$

и $w_y = y_0 + y_1\lambda + \dots + y_{n-1}\lambda^{n-1}$

уравнения (3) при $N \neq 1$ были ассоциированы, необходимо и достаточно, чтобы выполнились следующие сравнения:

© ГОУВПО «Ивановский государственный энергетический университет имени В.И. Ленина»

$$y_0\bar{x}_0 + p_n\sum_{i=1}^{n-1}\sum_{j=0}^{n-1-i} y_{n-1-j}\bar{x}_{i+j}\times$$
$$\times\sum_{\alpha_1+2\alpha_2+\ldots+(i-1)\alpha_{i-1}=i-1}\frac{(\alpha_1+\alpha_2+\ldots+\alpha_j)!}{\alpha_1!\alpha_2!\ldots\alpha_{i-1}!}\cdot\prod_{m=0}^{j-1}p_m^{\alpha_m}\equiv 0(\mathrm{mod}\,N);$$

$$\sum_{i=0}^{k} y_{k-i}\bar{x}_i + \sum_{j=1}^{n-1}\sum_{\ell=0}^{n-1-j} y_{n-1-\ell}\cdot\bar{x}_{j+\ell}\sum_{m=0,m\le k}^{j-1}p_{n-k+m}\times$$
$$\times\sum_{\alpha_1+\ldots+(j-m-1)\alpha_{j-m-1}=j-m-1}\frac{(\alpha_1+\alpha_2+\ldots+\alpha_{j-m-1})!}{\alpha_1!\alpha_2!\ldots\alpha_{j-m-1}!}\times$$
$$\times\prod_{t=0}^{j-m-1}p_t^{\alpha_t}\equiv 0(\mathrm{mod}\,N),$$
$k = 1, 2,\ldots, n-2$;
$$\sum_{i=1}^{n-1} y_{n-1-i}\bar{x}_i + \sum_{j=1}^{n-1}\sum_{\ell=0}^{n-1-j} y_{n-1-\ell}\cdot\bar{x}_{j+\ell}\times$$
$$\times\sum_{\alpha_1+2\alpha_2+\ldots+j\alpha_j=j}\frac{(\alpha_1+\alpha_2+\ldots+\alpha_j)!}{\alpha_1!\alpha_2!\ldots\alpha_j!}\times$$
$$\times\prod_{m=1}^{j}p_m^{\alpha_m}\equiv 0(\mathrm{mod}\,N),$$
где $\bar{x}_s (s = 0,1,\ldots,n-1)$ определены из лемм 1 и 2.

Доказательство.

Если два решения w_x и w_y ассоциированы, то справедливо равенство $w_y = \varepsilon w_x$, или $\varepsilon = \frac{w_e}{w_x} = \frac{1}{N}\bar{w}_y\bar{w}_x$, из чего и вытекает необходимость условия.

Наоборот, если вышеуказанные сравнения выполняются, то получим
$$\bar{w}_x\cdot w_y = N(\ell_0 + \ell_1\lambda + \ldots + \ell_{n-1}\lambda^{n-1})$$
с целыми коэффициентами ℓ_i.

Тогда имеем
$$N\cdot N^{n-1} = N^n\cdot F(\ell_0 + \ell_1\lambda + \ldots + \ell_{n-1}\lambda^{n-1}),$$
$F(\ell_0 + \ell_1\lambda + \ldots + \ell_{n-1}\lambda^{n-1}) = 1$, а значит, w_x и w_y ассоциированы.

Важный частный случай для уравнения (3) формулируется следующим образом:

ТЕОРЕМА 2. Для того, чтобы два решения
$$w_i = x_i + y_i\lambda + z_i\lambda^2 \quad (i = 1, 2)$$
уравнения (1) были ассоциированы, необходимо и достаточно, чтобы выполнялись следующие сравнения:
$$x_2\bar{x}_1 + p_3(y_2\bar{z}_1 + z_2\bar{y}_1) + p_1p_2z_2\bar{z}_1 \equiv 0(\mathrm{mod}\,N);$$
$$x_2\bar{y}_1 + y_2\bar{y}_1 + p_2(y_2\bar{z}_1 + z_2\bar{y}_1) +$$
$$+(p_1p_2 + p_3)z_2\bar{z}_1 \equiv 0(\mathrm{mod}\,N);$$
$$x_2\bar{z}_1 + y_2\bar{x}_1 + z_2\bar{x}_1 + p_1(y_2\bar{z}_1 + z_2\bar{y}_1) +$$
$$+(p_1^2 + p_2)z_2\bar{z}_1 \equiv 0(\mathrm{mod}\,N),$$
где
$$\bar{x}_1 = x_1^2 - p_2y_1^2 + (p_2^2 - p_1p_3)z_1^2 + p_1x_1y_1 +$$
$$+(p_1^2 + 2p_2)x_1z_1 - (p_1p_2 + p_3)y_1z_1;$$
$$\bar{y}_1 = -p_1y_1^2 + (p_1p_2 + p_3)z_1^2 - x_1y_1 - p_1^2y_1z_1;$$
$$\bar{z}_1 = y_1^2 - p_2z_1^2 - x_1z_1 + p_1y_1z_1.$$

Пусть $\tau_n(N)$ число попарно не ассоциированных элементов модуля $M_n(\lambda)$ с данной нормой N или, другими словами, количество классов ассоциированных решений уравнения (3).

ТЕОРЕМА 3. Имеет место неравенство
$$\tau_n(N) \le [c(n)N],$$
где $c(n) = \prod_{p<n}\max_k\frac{C_{n+k-1}^k}{p^k}$.

Здесь p – простое число; max рассматривается на всех дробях $\frac{C_{n+k-1}^k}{p^k}$, превышающих единицу.

Доказательство.

Известно, что $\tau_n(N) \le \psi(N)$, где $\psi(N)$ – количество целых неотрицательных решений диофантова уравнения
$$y_1y_2\ldots y_k = N. \qquad (4)$$

Учитывая каноническое разложение N:
$N = p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_\ell^{\gamma_\ell}$, где $2 \le p_1 < p_2 < \ldots < p_\ell$,
устанавливаем мультипликативность $\tau_n(N)$, из чего следует
$$\tau_n(N) \le \prod_{i=1}^{\ell}q_n(\gamma_i),$$
где $q_n(\gamma)$ – число целых неотрицательных решений диофантова уравнения
$$z_1 + z_2 + \ldots + z_n = \gamma.$$

Но $q_n(\gamma) = C_{\gamma+n-1}^{\gamma}$, поэтому
$$\tau_n(N) \le \prod_{i=1}^{\ell}C_{\gamma+n-1}^{\gamma}.$$

Оценим $\tau_n(p^\gamma)$. Так как значение элемента $u = p^k$ растет быстрее, нежели парабола k-й степени $u = C_{n+k-1}^k$, то существует лишь конечное число целых положительных k, заполняющих начальный отрезок натурального ряда и таких, что выполняется неравенство
$$C_{n+k-1}^k > p^k. \qquad (5)$$

Отметим, что для всех остальных значений k, начиная с некоторого, неравенство (5) будет противоположного смысла.

Из указанного конечного набора чисел K можно выбрать такое k_0 (может быть не одно), что дробь $\frac{1}{p^k}C_{n+k-1}^k$ будет наибольшей, т. е.
$$\frac{C_{n+k-1}^k}{p^k} \le \frac{C_{n+k0-1}^{k0}}{p^{k0}}.$$

Тогда получим
$\tau_n(p^\gamma) \le C_p(n)\cdot p^\gamma$, где
$$C_p(n)\max_k\frac{C_{n+k-1}^k}{p^k} = \frac{C_{n+k0-1}^{k0}}{p^{k0}},$$
и остается использовать мультипликативность $\tau_n(N)$.

Теорема 3 доказана.

© ГОУВПО «Ивановский государственный энергетический университет имени В.И. Ленина»

В качестве иллюстрации приведем некоторые вычисленные согласно теореме 3 оценки $\tau_n(N)$ для частных значений n, а именно:

$\tau_3(N) \le \left[\frac{3}{2}N\right]$, $\tau_4(N) \le \left[\frac{10}{3}N\right]$, $\tau_5(N) \le \left[\frac{175}{24}N\right]$ и т.д.

Список литературы

1. **Аванесов Э.Т., Гусев В.А.** Ассоциированные решения диофантовых уравнений: мат-лы Междунар. науч.-техн. конф. (XV Бенардосовские чтения). Т. 1. – Иваново, 2009. – С. 107.

Аванесов Эдуард Тигранович,
Пятигорский государственный технологический университет,
кандидат физико-математических наук, профессор кафедры высшей математики,
телефон 8-928-360-37-49.

Гусев Владимир Алексеевич,
ГОУВПО «Ивановский государственный энергетический университет имени В.И. Ленина»
кандидат физико-математических наук, профессор,
зам. декана факультета информатики и вычислительной техники,
e-mail: dekan@ivtf.ispu.ru

© ГОУВПО «Ивановский государственный энергетический университет имени В.И. Ленина»