© «Вестник ИГЭУ» Вып. 3 2006 г.

УДК 511.235+511.528

ЧИСТО КУБИЧЕСКИЕ ПОЛЯ И ДИОФАНТОВЫ УРАВНЕНИЯ

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

В заметке рассматриваются некоторые аспекты теории чисто кубических полей и их применение в диофантовом анализе.

Ключевые слова: чисто кубические поля, диофантово уравнение.

PURELY CUBIC FIELDS AND DIOPHANTINE EQUATIONS

E.T. AVANESSOV, Ph.D., V.A. GUSSEV, Ph.D.

This work is devoted to some aspects of purely cubic field theory and their application in Diophantine analysis.

Key words: purely cubic fields, Diophantine equation.

К проблеме Ферма. Приведем элементарное рассуждение, опирающееся на чисто кубические поля и основную единицу в них и представляющее собою вариант доказательства неразрешимости уравнения Ферма в кубическом случае. Известно [2], что заданная в однородных координатах кривая

$$Ax^3 + By^3 + Cz^3 = Nxyz, \tag{1}$$

$(A,B,C)=1, ABC = M \neq 0, N^3 \neq 27M$, – первого рода. Пусть $\sum_{i=1}^{r_i} a_i \cdot P_i^{(1)} + \sum_{i=1}^{s_1} b_i \cdot Q_i^{(1)}$ – решения уравнения (1), где $P_i^{(1)} (i = 1,2,...r_1)$ – основные решения (1) бесконечного порядка; $Q_i^{(1)}$ – решения конечного порядка (исключительные решения); a_i, b_i – некоторые целые числа. Если

$$\eta^2 = f(\xi) = \xi^3 - h_2\xi - h_3, \quad h_2, h_3 \in R(1) - \tag{2}$$

кривая, бирационально изоморфная (1), то решения на (2) определяются представлением

$$\sum_{j=1}^{r_2} c_j \cdot P_j^{(2)} + \sum_{j=1}^{s_2} d_j \cdot Q_j^{(2)},$$

где $P_j^{(2)}$ – решения бесконечного порядка; $Q_j^{(2)}$ – решения конечного порядка.

Тогда, как известно, $r_1 = r_2$, то есть уравнения (1) и (2) имеют одинаковые ранги (без учета исключительных решений). Решение уравнения (1) в целых числах, в сущности, не отличается от решения в рациональных числах уравнения

$$A\xi^3 + B\eta^3 + C = N\xi\eta, \tag{3}$$

где $\xi = \frac{x}{z}, \quad \eta = \frac{y}{z}$,

или системы уравнений

$$\begin{cases} \alpha + \beta + \gamma = N, \\ \alpha\beta\gamma = M = ABC, \end{cases} \tag{4}$$

где $\alpha = A\frac{x^2}{yz}$, $\beta = B\frac{y^2}{xz}$, $\gamma = \frac{z^2}{xy}$.

Сведем уравнение (1) к двум различным кривым вида (2) следующим образом:

1. Полагая $\gamma = N - \alpha - \beta$, находим

$\alpha\beta(N - \alpha - \beta) = M$ или

$$\beta\alpha^2 + \beta(\beta - N)\alpha + M = 0. \tag{5}$$

Очевидно, при рациональном β уравнение (5) имеет рациональное решение относительно α тогда и только тогда, когда дискриминант (5) равен полному квадрату рационального числа, то есть

$$D_\lambda = \left(\beta(\beta - N)\right)^2 - 4M\beta = T^2. \tag{6}$$

Умножив обе части (6) на $64M^2/\beta$ и произведя бирациональные преобразования по формулам

$\frac{8M}{\beta^2} \cdot T = V', \quad \frac{N^2}{3} - \frac{4M}{\beta} = U'$,

а затем $V = \frac{V'}{27W^3}, \quad U = \frac{U'}{9W^2}$,

получим нормальную форму Вейерштрасса для кривой 1 рода

$$\begin{aligned} V^2 = U^3 - 27N(N^3 - 24M)UW^4 + \\ +54(N^6 - 36MN^2 + 216M^2)W^6. \end{aligned} \tag{7}$$

Пусть λ – действительный корень уравнения

$$\lambda^3 - MN\lambda - 2M^2 = 0, \tag{8}$$

а μ – действительный корень уравнения

$$F(\mu) = \mu^3 - A_\mu \cdot \mu - B_\mu = 0, \tag{9}$$

где $A_\mu = 27N(N^3 - 24M)$;

$B_\mu = 54(N^6 - 36MN^2 + 216M^2)$.

Поля $K(\lambda)$ и $K(\mu)$, порождаемые кубическими числами λ и μ, тождественны, ибо (см. [3], с. 78–80):

1) их дискриминанты $D_\lambda = 4M^3(N^3 - 27M)$ и $D_\mu = (2^3 \cdot 3^6)^2 \cdot \left\{4M^3 \cdot (N^3 - 2M)\right\}$ отличаются квадратным множителем;

2) имеются переходные функции

$\mu = 3\bar{\mu}$, $\bar{\mu} = \frac{3N}{M}\lambda^2 - 6\lambda - 2N^2$,

$$\lambda = \frac{1}{2^3 \cdot 3^2 \cdot M}\left\{N\bar{\mu}^2 - (12M - N^3)\bar{\mu} + 2N^2(24M - N^3)\right\}$$

непосредственно определяемые обращением преобразования Чирнгаузена.

Представим (7) в виде

$$V^2 = (U - \mu W^2) \cdot (U - \mu' W^2) \cdot (U - \mu'' W^2) \tag{10}$$

где μ, μ', μ'' – различные корни (9).

Тогда, если

$U - \mu W^2 = Q^2$,

то этому представлению отвечает удвоенная точка в смысле группы Пуанкаре-Морделла-Вейля; а значит, для обыкновенных точек на кривой (7) должно быть

$$U - \mu W^2 = \nu_i Q^2, \qquad (11)$$

$D_\mu \equiv 0(\mathrm{mod}\, Norm\nu_i)$; $i = 1,2,...,r$; r – ранг (7).

ТЕОРЕМА 1. Пусть $(\frac{U}{W^2}, \frac{V}{W^3})$ – представитель i-го класса решений уравнения (7),

$\nu_i = (U_i + V_i\lambda + W_i\lambda^2)^2 \cdot \bar{D}_\lambda^{-1}$, $i = 1,2,...,r$; $\bar{D}_\lambda$ – индекс кубического поля λ,

$Q = (e + f\lambda + g\lambda^2)^2 \cdot \bar{D}_\lambda^{-1}$;

тогда значения U, W^2 находятся из систем уравнений:

$$\begin{cases} \bar{D}_\lambda \left\{ u_i U + 6(N^2 u_i - 3MNv_i + 6M^2 w_i) W^2 \right\} = e^2 + 4M^2 fg, \\ \bar{D}_\lambda \left\{ v_i U + 3(6u_i - N^2 v_i) W^2 \right\} = 2(M^2 g^2 + ef + MNfg), \\ \bar{D}_\lambda \left\{ w_i U + 3(-\frac{3N}{M} u_i + 6v_i - N^2 w_i) W^2 \right\} = f^2 + MNg^2 + 2eg; \end{cases} \qquad (12)$$

соответствующие значения для V определяются из (7).

2. Уравнение (1) аналогичным образом сведем к уравнению $(\alpha + \beta + \gamma)^3 = N\alpha\beta\gamma$.

Полагая $\frac{\alpha}{\gamma} = \alpha_1 + \beta_1$, $\frac{\beta}{\gamma} = \alpha_1 - \beta_1$, где α_1 и β_1 – рациональные числа, причем для решения $\gamma = 0$ имеем $\alpha_1 = \beta_1 = 0$, находим

$N^3\beta_1^2 = (2\alpha_1 + 1)^3 + N^3\alpha_1^2$.

Если теперь принять $2\alpha_1 + 1 = \frac{NX}{4Z^2}$, $8\beta_1 = \frac{Y}{Z^3}$, то получим

$Y^2 = X^3 + (NX + 4Z^2)Z^2$

Поля $K(\mu_1)$, где $\mu_1^3 + (N\mu_1 + 4)^2 = 0$, и $K(\lambda)$ (при $\mu = 1$) тождественны, так как

$D_{\mu_1} = 64\left\{4(N^3 - 27)\right\} = 8^2 D_\lambda$

и имеются переходные функции от λ к μ_1 и наоборот:

$\mu_1 = N\lambda^2 - 2\lambda - N^2$,

$\lambda = \frac{N}{8}\mu_1^2 + \frac{N^3 - 4}{8}\mu_1 + \frac{N^2}{2}$.

При $N = 0$, $M = 1$ получим чисто кубическое поле $K(\sqrt[3]{2})$, обладающее следующими арифметическими характеристиками: базис $K(\sqrt[3]{2})$ – степенной; число классов идеалов $h = 1$; основная единица $\varepsilon = -1 + \sqrt[3]{2}$; элемент $\mu_1 = -2\sqrt[3]{2}$ удовлетворяет уравнению $\mu_1^3 + 16 = 0$.

Далее воспользуемся оценкой ранга, установленной в [2].

ТЕОРЕМА 2. Если одновременно 1) M не содержит квадратов, 2) $M + N \equiv 1$ (mod 2), 3) $h = 1$, 4) хотя бы одно сравнение системы $\begin{cases} M \equiv 1 \ (\mathrm{mod}\ 9), \\ N \equiv M + 2 \ (\mathrm{mod}\ 27) \end{cases}$ не имеет места, 5) канонические разложения индексов D_λ и D_μ содержат одни и те же простые делители p, 6) MN содержит все простые делители индексов $\bar{D}_\lambda$ и D_μ в степени выше первой, то имеет место оценка $r \le k_0$, где k_0 – количество основных единиц поля $K(\lambda)$.

В нашем случае $\bar{D}_\lambda < 0$, $k_0 = 1$, $\bar{D}_\lambda = \bar{D}_\mu = 1$, а значит, согласно теореме 2, следует составить лишь одну систему вида (12), полученную из представления

$(\sqrt[3]{2} - 1) \cdot (X + 2\sqrt[3]{2}Z^2) = (e + f\sqrt[3]{2} + g\sqrt[3]{4})^2$.

Приравнивая коэффициенты при $\sqrt[3]{2}$ и $\sqrt[3]{4}$, находим

$$\begin{cases} -f^2 + 2g^2 + 2ef - 2eg = 0, \\ e^2 - 2g^2 - 2ef + 4fg = 2Z^2. \end{cases} \qquad (13)$$

Очевидно, если система (13) имеет ненулевые целые решения, то, e, f и g должны быть четными. Сократив на 4, получим подобную же систему, значит, возможно применение метода бесконечного спуска, а следовательно, диофантово уравнение

$X^3 + Y^3 + Z^3 = 0$

не имеет нетривиальных решений, отличных от $XYZ = 0$.

К проблеме Мниха. Исследуем теперь частный случай уравнения (1), получающийся для $M = ABC = 1$, то есть уравнение

$$X^3 + Y^3 + Z^3 = NXYZ. \qquad (14)$$

При $N = 1$ мы имеем дело с так называемой проблемой Мниха существования рациональных решений системы уравнений

$$X_1 X_2 X_3 = X_1 + X_2 + X_3 = 1, \qquad (15)$$

разрешенной в отрицательном смысле в [1].

Исходя из того, что проблема Мниха эквивалентна проблеме существования рационального числа r, такого, что уравнение

$$U^3 - U^2 + rU - 1 = 0 \qquad (16)$$

имеет рациональные корни, докажем следующее предложение.

ТЕОРЕМА 3. Не существует чисто кубических полей, в которых при рациональном r уравнение (16) разрешимо.

Для доказательства заменой $U = \frac{1}{3}(Z + 1)$ приведем (16) к виду

$$Z^3 = 3(1 - 3r)Z + 29 - 9r. \qquad (17)$$

Последующее представление

$D_z = -27^2 \cdot (4r^3 - r^2 - 18r + 31)$, откуда

$3(4r^3 - r^2 - 18r + 31) = t^2$, где $t \in R(1)$, и подстановки $r = \frac{1}{12}(x + 1)$, $12t = y$ приведут к уравнению

$$y^2 = x^3 - 651x + 12742. \qquad (18)$$

Следуя (12), составим систему уравнений

$$\begin{cases} -x+20z^2 = f^2+g^2+2eg, \\ x-5z^2 = 2(g^2+ef+fg), \\ x-32z^2 = e+4fg. \end{cases} \tag{19}$$

Система (19) при условии (x,z)=1 неразрешима в целых числах, откуда вытекает, что кривая (18) не содержит обыкновенных базисных точек, а значит, ее ранг, без учета исключительных точек, равен нулю, и если на этой кривой есть рациональные точки, то они должны быть исключительными.

Единственная исключительная пара точек (3;±104) приводит через $r=\frac{1}{3}$, $z=\sqrt[3]{26}$ к решению $U_1=\frac{1}{3}(1+\sqrt[3]{26})$, $U_{2,3}=\frac{1}{3}(1+\frac{-1\pm i\sqrt{3}}{2}\sqrt[3]{26})$, которое принадлежит композиту чисто кубического поля $K(\sqrt[3]{26})$ и классического поля Эйзенштейна, образованного кубическим корнем из единицы.

Диофантовы уравнения. Здесь мы покажем, как задачу решения диофантова уравнения:

$$f(x,y)=x^3+\sum_{i=1}^{3}(-1)^i a_i\cdot x^{3-i}y^i = A \tag{20}$$

можно свести к исследованию во вспомогательном чисто кубическом поле.

Известно, что произвольная кубическая форма $f(x,y)$ имеет два ковариантa:

$$H=H(x,y)=-\frac{1}{4}\left\{\frac{\partial^2 f}{\partial x}\cdot\frac{\partial^2 f}{\partial y^2}-\left(\frac{\partial^2 f}{\partial x\partial y}\right)^2\right\};$$

$$Q=Q(x,y)=\frac{\partial f}{\partial x}\cdot\frac{\partial H}{\partial y}-\frac{\partial f}{\partial y}\cdot\frac{\partial H}{\partial x},$$

удовлетворяющие тождеству

$$Q^2=4H^3-27D_f^2, \tag{21}$$

где D_f – дискриминанта формы f.

Соотношение (21) есть частный случай диофантова уравнения

$$\eta^2=4\xi^3-g_2\xi-g_3 \tag{22}$$

которое, как показал Морделл [4], имеет конечное число рациональных решений (ξ,η) при определенном ограничении на правую часть (22), причем каждому такому решению соответствует представление единицы бинарной биквадратичной формой, и наоборот.

Для решения уравнения (21) можно использовать разложение в поле $K(\alpha)$, где $\alpha=\sqrt[3]{2D_f\cdot A^2}$, и это приведет к уравнениям

$$H'-\alpha=\mu\beta^2, \tag{23}$$

где $H'=4H$; β – целое алгебраическое число чисто кубического поля $K(\alpha)$; μ – некоторое целое алгебраическое число из конечного множества элементов $Q(\alpha)$.

Это множество зависит от числа $2D_f A^2$, от основной единицы и числа классов идеалов $Q(\alpha)$. Тогда уравнение (23) эквивалентно совокупности уравнений вида

$$g(U,V)=1, \tag{24}$$

где g – биквадратичная форма.

Если в (23) $\mu=1$, то (24) приводимо и легко решается, в противном случае (24) неприводимо.

Некоторые из биквадратичных уравнений могут быть исключены рассмотрением по соответствующим модулям. Для оставшихся уравнений известно некоторое решение $(U_o,V_o)=(1;0)$, а значит, и решение (21), которое обозначим через (H_o,Q'_o), $Q'_o=4Q_o$.

Это означает, что (23) может быть записано как $\frac{H'-\alpha}{H'_o-\alpha}$, равное квадрату элемента $K(\alpha)$, а уравнение (24) обратится в уравнение

$$g(U,V)=U^4-6H'_oU^2V^2-8Q'_oUV^3-3H_o^2V^4=1. \tag{25}$$

Очевидно, различные решения (24) приведут к различным уравнениям этого типа.

Итак, проблема заключается в том, чтобы показать, что каждое получаемое таким путем уравнение вида (25) имеет только тривиальное решение $(U,V)=(1;0)$.

ПРИМЕР 1. Для уравнения

$f(x,y)=x^3+\alpha x^2y+y^3=1$,

где α – целый параметр,

$D_f=-(4\alpha^3+27)$ и свободно от квадратов.

Непосредственно находим:

$H(x,y)=\alpha^2x^2-9xy-3\alpha y^2$,

$Q(x,y)=-(2\alpha^3+27)x^3-27\alpha x^2y-18\alpha^2xy^2+27y^3$

и далее $V^2=U^3+432(4\alpha^3+27)$,

откуда

$$U+6\sqrt[3]{2(4\alpha^3+27)}=\pm\mu\left\{x_o+y_o\sqrt[3]{-2D_f}++z_o\sqrt[3]{4D_f^2}\right\},$$

где $x_o,y_o,z_o\in Z$; μ – определяется:

1) основной единицей чисто кубического поля $K(\sqrt[3]{2(4\alpha^3+27)})$;

2) числом h классов идеалов этого поля;

3) элементами с нормой, равной делителям числа $12(4\alpha^3+27)$.

ПРИМЕР 2. Пусть

$f(x,y)=x^3+\alpha x^2y-(\alpha+1)xy^2+y^3=1$,

a – целый параметр, D_f – свободно от квадратов, тогда

$D_f=(\alpha^2+\alpha-3)^2-32=\alpha^4+2\alpha^3-5\alpha^2-6\alpha-23$,

$H(x,y)=(\alpha^2+3\alpha+3)x^2-(\alpha^2+\alpha+9)xy+(\alpha^2-\alpha+1)y^2$

$Q(x,y)=-(2\alpha^3+9\alpha^2+9\alpha+27)x^3+3(\alpha^3+7\alpha^2+3\alpha+6)x^2y+$
$+3(\alpha^3-4\alpha^2-11\alpha-3)xy^2-(2\alpha^3-3\alpha^2-3\alpha-25)y^3$

и все сводится к чисто кубическому полю

$K(\sqrt[3]{2(a^4+2a^3-5a^2-6a-23)})$

ПРИМЕР 3. Если

$f(x,y)=x^3-ax^2y+b(a-3b)xy^2+b^3y^3=1$,

где $a,b\in Z$; $b>0$; $a\ge\frac{3}{2}b$; $D_f=b^2(a^2-3ab+9b^2)^2>0$,

то есть группа Галуа уравнения $f(x,1)=0$ циклическая,

$H(x,y)=(\alpha^2-3\alpha b+9b^2)\cdot(x^2-bxy+b^2y^2)$,

$Q(x,y)=(\alpha^2-3\alpha b+9b^2)\cdot\{(2\alpha-3b)x^3-3b(\alpha-6b)x^2y-$
$-3b^2\cdot(\alpha+3b)xy^2+b^3\cdot(2\alpha-3b)y^3\}$,

то находим $V^2 = U^3 - 432b^2(a^2 - 3ab + 9b^2)^2$, и чисто кубическое поле $K(\sqrt[3]{2b^2 \cdot (a^2 - 3ab + 9b^2)^2})$ сведет задачу в соответствии с основной единицей, числом h и элементами этого поля с нормой, равной делителям числа $6b(a^2 - 3ab + 9b^2)$, к представлениям приводимыми либо неприводимыми биквадратичными формами отрицательного дискриминанта.

ПРИМЕР 4. В качестве иллюстрации исследуем представление единицы бинарной кубической формой наименьшего неквадратного положительного дискриминанта $D_f = 148$:

$$f(x,y) = x^3 + x^2y - 3xy^2 - y^3 = 1 \tag{26}$$

Вычисления дают:

$$H = 2(5x^2 + 3xy + 6y^2),$$

$$Q = 2(-x^3 + 99x^2y + 63xy^2 - 27y^3) = 2(x+y)\cdot$$

$$\cdot(-x^2 + 100xy - 27y^2)$$

И при $V = \frac{1}{2}Q,\ \ \mathrm{U} = \mathrm{H}$,

$$V^2 = U^3 - 999\,. \tag{27}$$

Известно, что уравнение (27) имеет лишь следующие шесть решений в целых числах:

$(U,V) = (10,\pm 1),\ (12,\pm 27),\ (40,\pm 251),\ (147,\pm 1782),$
$(174,\pm 2295),\ (22480,\pm 3370501).$

Так как $\mathrm{U} = \mathrm{H}$ – четно, то отбросим четвертое решение, а для оставшихся значений (U,V) составим и решим в целых числах следующие 5 систем уравнений вида

$$\begin{cases} 5x^2 + 3xy + 6y^2 = \frac{1}{2}U, \\ -x - y = d, \\ x^2 - 100xy + 27y^2 = \frac{V}{d}, \end{cases}$$

где d – один из возможных делителей числа V. В последнем случае для простого V =3370501 соответствующая система неразрешима, а другие системы дают

$x = 1;\ 0;\ -2;\ 3$

и, соответственно,

$y = 0;\ -1;\ 1;\ 2$.

Итак, диофантово уравнение (26) имеет лишь следующие четыре решения в целых числах:

$(x;y) = (1;0),(0;-1),(-2;1)$ и $(3;2)$.

Список литературы

1. Аванесов Э.Т. Замечания к проблеме В. Мниха // Matem, Casopis. – 1967. – Т. 17. – № 2. – С. 85–91.

2. Аванесов Э.Т. Об уравнении $Ax^3 + By^3 + Cz^3 = Nxyz$ // ДАН БССР. – 1978. – Т. 22. – № 5. – С. 405–408.

3. Делоне Б.Н., Фадеев Д.К. Теория иррациональностей 3-ей степени: Тр. МИАН СССР. – 1940. – Т. 11.

4. Mordell L.J. Diophantine equations. – London: Academic Press,1969.

Аванесов Эдуард Тигранович,
Пятигорский государственный технологический университет,
кандидат физико-математических наук, профессор кафедры высшей математики,
e-mail: dekan@ivtf.ispu.ru

Гусев Владимир Алексеевич,
ГОУВПО «Ивановский государственный энергетический университет имени В.И. Ленина»,
кандидат физико-математических наук, профессор, зам. декана факультета информатики и вычислительной техники,
телефон (4932) 26-98-78,
E-mail: dekan@ivtf.ispu.ru