

Уравнения Пелля для многочленов

Илья Иванов-Погодаев, Алексей Канель-Белов, Роман Крутовский, Игорь Мельников, Борис Френкин, Алексей Чиликов

А. ВВОДНАЯ СЕРИЯ. КЛАССИЧЕСКОЕ УРАВНЕНИЕ ПЕЛЛЯ.

Вводная серия А относится к классическим фактам об уравнении Пелля $x^2 - Dy^2 = 1$ для целых чисел. Решение $(\pm 1, 0)$ называется *тривиальным*, а остальные – *нетривиальными*.

Задача А.1. Пусть (x_1, y_1) – решение уравнения Пелля, т.е. $x_1^2 - Dy_1^2 = 1$. Пусть $(x_1 + \sqrt{D}y_1)^n = x_n + \sqrt{D}y_n$. Докажите, что тогда (x_n, y_n) – тоже решение уравнения Пелля (отметим, что $x_{-n} = x_n, y_{-n} = -y_n$). Решение (x_n, y_n) называется *степенью решения* (x_1, y_1) . Введите понятие *произведения решений*.

Задача А.2. Докажите, что все нетривиальные решения (если существуют) являются степенью одного решения (x_1, y_1) (с точностью до знака при x).

Задача А.3. Докажите, что если D есть квадрат целого, то нетривиальных решений у уравнения Пелля нет.

В следующих пунктах серии считаем, что $D \neq t^2 \forall t \in \mathbb{Z}, D \in \mathbb{Z}$.

Задача А.4. Покажите, что существуют $M > 0$ и точка (x, y) с ненулевыми целыми координатами, что $|x^2 - Dy^2| \leq M$.

Задача А.5. С помощью леммы Минковского докажите, что существует $M > 0$, для которого таких точек бесконечно много.

Задача А.6. Докажите, что существует такое целое положительное число $k < M$, что уравнение $|x^2 - Dy^2| = k$ имеет бесконечно много решений.

Задача А.7. С помощью предыдущих пунктов докажите, что нетривиальное решение уравнения Пелля существует.

Задача А.8. Опишите все рациональные решения уравнения Пелля в общем виде.

В. УРАВНЕНИЯ ПЕЛЛЯ ДЛЯ МНОГОЧЛЕНОВ.

Задача В.1. Найдите все пары $(P(x), Q(x))$ многочленов над \mathbb{R} такие, что

$$P^2(x) - (x^2 - 1)Q^2(x) = 1.$$

Задача В.2. Решите уравнение Пелля для рациональных функций.

Задача В.3. Решите уравнения а) $P^2 + Q^2 = R^2$, б) $P^2 + Q^2 = 1$ для многочленов с комплексными коэффициентами.

Задача В.4. Докажите, что для $n > 2$ и для многочленов P, Q существуют комплексные числа ψ_1, ψ_2, ψ_3 , такие, что $\psi_i^n = -1$ и $P^n + Q^n$ делится на $(P - \psi_1 Q)(P - \psi_2 Q)(P - \psi_3 Q)$.

Задача В.5. Пусть $P^n + Q^n = R^n$. В условиях п. В4 докажите, что существуют такие многочлены R_1, R_2, R_3 , что $P - \psi_i Q = R_i^n$.

Задача В.6. Докажите, что для $n > 2$ уравнение Ферма $x^n + y^n = z^n$ для многочленов и для рациональных функций не имеет нетривиальных решений.

С. ПРИМЕНЕНИЯ ТЕОРЕМЫ КОЛЛАРА.

Под *нетривиальным решением* здесь понимается неконстантное решение.

Задача С.1. Решите уравнение Пелля, когда D есть квадрат многочлена.

Задача С.2. Рассмотрим уравнение над множеством многочленов из $\mathbb{Z}[x]$:

$$(1) \quad P^2(x) - (R^2(x) - 1)Q^2(x) = 1.$$

Здесь R – уже произвольный неконстантный многочлен, а не просто переменная.

Докажите, что множество решений состоит из степеней одного нетривиального: $(R, 1)$.

Задача С.3. Теорема Коллара *** Аналогичное утверждение верно для многочленов из $\mathbb{C}[x]$

Задача С.4. Решите уравнение (1) для случая, когда R – константа. Отдельно рассмотрите случай, когда $R^2 = 1$ и когда $R^2 \neq 1$.

Далее в серии С предполагается, что $R \neq \text{const}$. Кроме того, можно пользоваться теоремой Коллара.

Задача С.5. Докажите, что Q имеет вид $Q_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} (R^2 - 1)^k R^{n-1-2k}$ для некоторого целого n . Выпишите аналогичную формулу для P .

Задача С.6. Докажите, что $Q_n \equiv n \pmod{R-1}$, то есть $Q_n - n = (R-1)S$, для некоторого многочлена S .

Задача С.7. Решите систему уравнений для многочленов из $\mathbb{C}[x]$

$$(2) \quad \begin{cases} X^2 - (R^2 - 1)Y^2 = 1 \\ Y - (R - 1)Z = V \\ V \cdot U = 1 \end{cases}$$

Задача С.8. Основная задача. Докажите, что для произвольного уравнения W в целых числах можно построить систему уравнений для многочленов из $\mathbb{C}[x]$, имеющую нетривиальное решение тогда и только тогда, когда имеет решение уравнение W .

D. АФФИННЫЕ МНОГОВБРАЗИЯ.

Задача D.1. Задайте следующие множества уравнениями или наборами уравнений:

- (1) эллипс;
- (2) пару прямых на плоскости;
- (3) окружность и эллипс;
- (4) окружность и параболу, проходящие через начало координат и касающиеся в этой точке, причем ось ординат – ось параболы;
- (5) экваториальную окружность на единичной сфере в трехмерном пространстве;
- (6) n -мерный тор (то есть декартово произведение n окружностей).

Определение 1. Идеалом в кольце R называется такое множество I , что

- (1) $I \cdot R \subset I$;
- (2) $I + I \subset I$.

Идеал называется главным, если он порождается одним элементом.

Определение 2. Пусть R некоторое кольцо. Будем называть аффинным многообразием над R множество X решений конечного числа алгебраических уравнений от нескольких переменных, то есть тех, которые можно записать в виде $P(x_1, \dots, x_n) = 0$, где P – многочлен.

Определение 3. Пусть X задано несколькими уравнениями в $R[x_1, \dots, x_n]$. Левые части этих уравнений порождают идеал в кольце $R[x_1, \dots, x_n]$, который мы будем обозначать $I(X)$. Кольцом функций $R[X]$ на X будем называть кольцо $R[x_1, \dots, x_n]/I(X)$.

Задача D.2. Убедитесь в том, что для каждого элемента из $R[X]$ в каждой точке многообразия X можно однозначно определить значение.

Задача D.3. Покажите, что кольцо функций полукубической параболы, заданной уравнением $y^2 = x^3$ в \mathbb{C}^2 , изоморфно кольцу $\mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$.

Задача D.4. Пусть X и Y аффинные многообразия и задано отображение $\varphi: R[Y] \rightarrow R[X]$. Постройте по φ отображение $f: X \rightarrow Y$, которое бы индуцировало φ .

Замечание 4. Нас будут интересовать только отображения между многообразиями, которые происходят из отображения соответствующих колец. Такие отображения будем называть алгебраическими.

Задача D.5. Рассмотрим на \mathbb{C}^2 действие группы $\mathbb{Z}/2\mathbb{Z}$ такое, что нетривиальный элемент группы переводит (x, y) в $(-x, -y)$. Это действие индуцирует автоморфизм кольца $\mathbb{C}[x, y]$. Покажите, что подкольцо, инвариантное относительно этого действия, изоморфно $\mathbb{C}[u, v, w]/(uv - w^2)$.

Постройте изоморфизм между аффинным многообразием, заданным этим кольцом, и фактором \mathbb{C}^2 по действию $\mathbb{Z}/2$ (как топологическими пространствами).

Пусть I некоторый идеал в кольце $R[x_1, \dots, x_n]$. Многообразие, соответствующее кольцу $R[x_1, \dots, x_n]/I$ будем обозначать $V(I)$. Радикалом идеала I будем называть множество $\text{rad}(I)$ всех таких элементов кольца $R[x_1, \dots, x_n]$, что некоторая их степень содержится в I .

Теорема 5 (Теорема Гильберта о нулях). Пусть k некоторое алгебраически замкнутое поле. Тогда для любого идеала $I \subset k[x_1, \dots, x_n]$ выполнено

$$I(V(I)) = \text{rad}(I).$$

Задача D.6. Используя теорему, покажите, что точки аффинного многообразия X над \mathbb{C} взаимнооднозначно соответствуют максимальным идеалам кольца $\mathbb{C}[X]$.

Задача D.7. Пусть X и Y — аффинные многообразия над \mathbb{C} . Пусть задано отображение $\varphi: \mathbb{C}[Y] \rightarrow \mathbb{C}[X]$. Постройте по нему отображение из множества максимальных идеалов кольца $\mathbb{C}[X]$ в множество максимальных идеалов кольца $\mathbb{C}[Y]$, не используя теорему Гильберта о нулях. Убедитесь, что это отображение совпадает с отображением, построенным в задаче 4.

Определение 6. Отображение $\iota: X \rightarrow Y$ между аффинными многообразиями будем называть замкнутым вложением, если $R[X] = R[Y]/I$ и отображение колец функций, соответствующее ι является отображением факторизации $R[Y] \rightarrow R[Y]/I$.

Замечание 7. Легко заметить, что любое аффинное многообразие над \mathbb{C} канонически замкнуто вложено в некоторое \mathbb{C}^n .

Задача D.8. Задайте двукратную обмотку как замкнутое вложение окружности в тор.

Задача D.9. Рассмотрим естественное вложение $(\mathbb{C} \setminus 0)^n$ в \mathbb{C}^n . Покажите, что это вложение является алгебраическим отображением. Докажите, что оно не является замкнутым вложением.

Задача D.10. Покажите, что стандартное вложение $\varphi: \mathbb{C}[t^2, t^3] \hookrightarrow \mathbb{C}[t]$ не задает замкнутое вложение прямой в полукубическую параболу.

Е. ОТОБРАЖЕНИЯ АФФИННЫХ МНОГООБРАЗИЙ.

Не забывайте подходить с вопросами и за подсказками!

Определение 8. Множество R с двумя ассоциативными коммутативными бинарными операциями \cdot и $+$ (умножением и сложением) называется кольцом, если выполнены следующие свойства:

(1) $\exists 0 \in R: 0 + a = a + 0 = a \quad \forall a \in R;$

- (2) $\forall a \in R \exists b \in R: a + b = b + a = 0;$
 (3) $\exists 1 \in R: 1 \cdot a = a \cdot 1 = a \quad \forall a \in R;$
 (4) $a \cdot (b + c) = a \cdot b + a \cdot c;$
 (5) $(a + b) \cdot c = a \cdot c + b \cdot c.$

Замечание 9. Основными кольцами (кроме множеств целых, рациональных, вещественных и комплексных чисел), которые нас интересуют, являются кольца многочленов, а так же кольца функций на аффинных многообразиях.

Замечание 10. Многочлены $P_1(x_1, \dots, x_n), \dots, P_k(x_1, \dots, x_n)$, которые задают аффинное многообразие X , порождают также некоторое подмножество $I = P_1 \cdot R[x_1, \dots, x_n] + \dots + P_k \cdot R[x_1, \dots, x_n] \subset R[x_1, \dots, x_n]$. Все элементы этого множества зануляются на точках многообразия.

Такое множество является идеалом в кольце функций на X .

Задача Е.1. Пусть I некоторый идеал в кольце многочленов $\mathbb{C}[x_1, \dots, x_n]$. Через X_I обозначим многообразие, соответствующее данному идеалу. Докажите следующие свойства:

- (1) $I \subseteq J \Rightarrow X_J \subseteq X_I;$
 (2) $X_I \cup X_J = X_{I \cdot J} = X_{I \cap J};$
 (3) если $I + J = R$, то $I \cdot J = I \cap J;$
 (4) идеалы $I_1 = \langle x \rangle$ и $I_2 = \langle x^2 \rangle$ в кольце $\mathcal{R}[x]$ задают одинаковые множества нулей.

Задача Е.2. (1) Докажите, что все идеалы кольца многочленов от одной переменной $\mathcal{R}[x]$ являются главными. Такие кольца называются кольцами главных идеалов (КГИ).

(2) Приведите пример кольца, не являющегося КГИ.

Определение 11. Дан идеал $I \subseteq R$. Факторкольцом R/I называется множество классов эквивалентности элементов кольца R по модулю I : $a \sim b \Leftrightarrow a - b \in I$. Умножение и сложение на факторкольце задаются следующим образом:

- (1) $(a + I) + (b + I) = (a + b) + I;$
 (2) $(a + I) \cdot (b + I) = (a \cdot b) + I.$

Задача Е.3. Проверьте корректность данного определения. Докажите, что факторкольцо является кольцом.

Замечание 12. В задаче 2 из листочка "Многообразия и уравнения" мы уже неявно работали с факторкольцом. А именно, мы показали, что для многообразия X_I над \mathbb{C} , заданного идеалом I (X_I — это множество общих нулей всех элементов из I), все значения полиномиальных функций на X_I определяются факторкольцом $\mathbb{C}[x_1, \dots, x_n]/I$.

Определение 13. Пусть многообразие X над R задано идеалом $I(X)$ (здесь мы подразумеваем, что набор уравнений порождает некоторый идеал). Тогда кольцом функций $R[X]$ многообразия X называется факторкольцо $R[x_1, \dots, x_n]/I(X)$.

Замечание 14. В задаче 5 из предыдущей серии было показано, что любой идеал $I \subset \mathbb{C}[x_1, \dots, x_n]$ имеет конечный набор порождающих $\Gamma = \{g_1, \dots, g_k\}$.

Рассмотрим идеал G , порожденный наибольшими мономами всех элементов из I . В задаче 5 мы доказали, что старшие мономы элементов Γ также порождают идеал G . Такой набор образующих идеала I принято называть базисом Грёбнера.

Рассмотрим на \mathbb{C}^2 действие инволюции $\varphi: (x, y) \rightarrow (-x, -y)$ (т.е. $\varphi^2 = Id$). Эта инволюция задает отображение φ^* из кольца $\mathbb{C}[x, y]$ в себя. Покажите, что множество инвариантных элементов относительно φ^* образует подкольцо изоморфное $\mathbb{C}[u, v, w]/(uv - w^2)$.

Определение 15. Отображение $\iota: X \rightarrow Y$ между аффинными многообразиями будем называть замкнутым вложением, если $R[X] = R[Y]/I$ и отображение, соответствующее ι является отображением факторизации $R[Y] \rightarrow R[Y]/I$.

Замечание 16. Легко заметить, что любое аффинное многообразие над \mathbb{C} канонически замкнуто вложено в некоторое \mathbb{C}^n .

Задача Е.4. Рассмотрим естественное вложение $(\mathbb{C} \setminus 0)^n$ в \mathbb{C}^n . Покажите, что это вложение является алгебраическим отображением. Докажите, что оно не является замкнутым вложением.

Задача Е.5. Покажите, что стандартное вложение $\varphi: \mathbb{C}[t^2, t^3] \hookrightarrow \mathbb{C}[t]$ не задает замкнутое вложение прямой в полукубическую параболу.

Задача Е.6. В этой задаче мы построим нетривиальное алгебраическое вложение прямой \mathcal{R} в \mathcal{R}^3 . Для начала рассмотрим отображение

$$\varphi: \mathcal{R} \rightarrow \mathcal{R}^2: t \mapsto (t^3 - 3t, t^4 - 4t^2)$$

Убедитесь, что образ этого отображения в \mathcal{R}^2 является проекцией на плоскость узла трилистника, из которого выкинули одну точку (она лежит на бесконечности).

Придумайте такой многочлен $h(t)$, что отображение

$$t \mapsto (\varphi(t), h(t))$$

переводит прямую в трилистник в \mathcal{R}^3 , из которого выкинули одну точку (она так же будет лежать на бесконечности).

Замечание 17. Очевидно, что не у любой системы полиномиальных уравнений есть решение. Например, у системы $\{x-y=0, x-y+1=0\}$ нет решений. Заметим, что идеал, который порождают эти два многочлена совпадает со всем кольцом $R[x, y]$ так как $1 \in I$.

Таким образом, если идеал I порождается элементами g_1, \dots, g_k и существуют элементы $h_1, \dots, h_k \in R[x_1, \dots, x_n]$, такие, что

$$g_1 h_1 + \dots + g_k h_k = 1,$$

то I совпадает со всем $R[x_1, \dots, x_n]$. В следующей задаче мы доказываем, что если $1 \notin I$, то найдется общее решение для всех элементов I .

Задача Е.7 (Слабая теорема Гильберта о нулях). Любой собственный идеал $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ задает непустое множество решений.

Докажем эту теорему в несколько шагов. Введем отображение подстановки числа $a \in \mathbb{C}$ на место первой координаты:

$$ev_a: \mathbb{C}[x_1, \dots, x_n] \rightarrow \mathbb{C}[x_2, \dots, x_n]: f(x_1, \dots, x_n) \mapsto f(a, x_2, \dots, x_n).$$

- (1) Пусть $I \cap \mathbb{C}[x_1] = \langle p(x_1) \rangle$, $\deg p > 0$. Тогда существует $a \in \mathbb{C}$ такое, что $ev_a(I) \subsetneq \mathbb{C}[x_2, \dots, x_n]$.
- (2) Предположим, что $I \cap \mathbb{C}[x_1] = \emptyset$. Докажите, что найдется такое $a \in \mathbb{C}$ что, выполнено $ev_a(I) \subsetneq \mathbb{C}[x_2]$.
- (3) Предположим, что $I \cap \mathbb{C}[x_1] = \emptyset$. Докажите, что найдется такое $a \in \mathbb{C}$, что выполнено $ev_a(I) \subsetneq \mathbb{C}[x_2, \dots, x_n]$.
- (4) Докажите теорему.

F. КОМПЛЕКСНЫЙ СЛУЧАЙ.

Нам потребуется следующая теорема, которой был посвящен проект <https://www.turgor.ru/lktg/2007/2/index.php>.

Теорема Матиясевича. Не существует алгоритма, позволяющего по набору коэффициентов многочлена от нескольких переменных $H(x_1, \dots, x_m)$ установить, имеет ли он целочисленное решение или нет.¹

Мы рассмотрим комплексный случай, из которого вытекает и случай произвольного поля.

Серия F1. Разложение многочленов и подстановки.

¹На самом деле можно положить $m = 11$

Задача F.1. Докажите, что $P(x + P(x))$ делится на $P(x)$.

Задача F.2. Дан квадратный трехчлен $P(x) \neq \text{const}$ с целыми коэффициентами. Докажите, что существует целое n такое, что все простые делители числа $P(n)$ меньше $n/2019$.

Замечание. Аналогичный факт даже для кубического многочлена нам неизвестно. Мы можем доказать это для двучленов $ax^n + b$.

Задача F.3. Пусть $P(x_1, \dots, x_n), Q(x_1, \dots, x_n)$ – произвольные полиномы от n переменных. Пусть

$$\hat{P}(x_1, \dots, x_n, u) = P(x_1 + uQ(x_1, \dots, x_n), \dots, x_n + uQ(x_1, \dots, x_n))$$

Тогда существует $R(x_1, \dots, x_n, u)$, такой, что

$$\hat{P}(x_1, \dots, x_n, u) = P(x_1, \dots, x_n) + Q(x_1, \dots, x_n)R(x_1, \dots, x_n, u).$$

Задача F.4. Существует многочлен $H(x_1, \dots, x_n)$ такой, что при всех целых k таких, что $1 \leq k \leq 2019$ все многочлены $H(x_1, \dots, x_n) - k$ имеют нетривиальное разложение на множители.

Задача F.5. В предыдущей задаче можно выбрать $H(x_1, \dots, x_n)$ в виде $P_k Q_k + k$, где Q_i алгебраически независимы (т.е. нет ненулевого многочлена R такого, что $R(Q_1, \dots, Q_{2019}) \equiv 0$).

Задача F.6. Существуют такие семейства полиномов $H_m(x_1, \dots, x_m), P_m(x_1, \dots, x_m)$ для которых одновременно выполняются условия делимости

$$H_k(x_1, \dots, x_k) \mid (P_m(x_1, \dots, x_m) - k)$$

при всех $k \in \{1, \dots, t\}$, причем H_m и P_m существенно зависят от x_m и при этом H_s при $s < t$ от x_m не зависят.

Серия F2. Конструкция систем.

Задача F.7. Зададим многообразие $\mathcal{B}_{(d,e)}$ при помощи системы образующих и соотношений.

$$(3) \quad \begin{cases} X_{ij}^2 - (T_j^2 - 1)Y_{ij}^2 = 1 \\ Y_{ij} - (T_j - 1)Z_{ij} = V_{ij} \\ V_{ij}U_{ij} = 1 \\ T_{j+1} = \prod_{k=1}^j ((T_k^2 - 1)W_k) W_{j+1}^{m_{j+1}} \\ T_1 = \hat{P}(W_1, \dots, W_n) \end{cases}$$

где $1 \leq i \leq d, 1 \leq j \leq e, \{m_j\}_{j=1}^e$ достаточно быстро растущая последовательность целых чисел. При этом полином \hat{P} выберем таким образом, чтобы W_i был делителем $\hat{P}(W_1, \dots, W_n) - 3i$. (Этот полином можно построить явно (см. п.6 предыдущей серии).

Последовательность $\{m_j\}_{j=1}^e$ выбирается так, что в случае, когда все переменные, входящие в T_1 , принимают различные значения, многочлены T_j алгебраически независимы.

Задача F.8. Пусть для некоторого N выполнено $T_N = C_N \neq 0$ (т.е. T_N – ненулевая константа). Тогда все W_k при $k \leq N$ и все T_k при $k \leq N - 1$ являются константами.

Задача F.9. Задача о вложимости произвольного алгебраического многообразия \mathcal{A} над \mathbb{C} в произвольное алгебраические многообразие \mathcal{B} алгоритмически неразрешима.