Уравнения Пелля для многочленов. Решения задач и указания.

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

A. Вводная серия. Классическое уравнение Пелля.

Задача A.1. Первое утверждение проверяется прямым подсчетом. Для решения следующих задач важно заметить, что степень решения вообще всегда может быть представлена в такой форме.

По аналогии с первым утверждением можно заметить, что из пары решений нужного вида можно собрать новое решение, пользуясь тем, что $(x+y\sqrt{D})(x'+y'\sqrt{D})$ снова имеет вид $X+Y\sqrt{D}$.

Задача A.2. Рассмотрим множество неотрицательных решений и упорядочим их по возрастанию x. Легко проверить, что все решения сравнимы между собой. Более того, если $x<x'$, то и $y<y'$ (прямой подсчет). Тогда введенная ранее операция произведения монотонна на этом множестве по каждому из аргументов (в смысле только что введенного упорядочения) – это тоже проверяется прямым подсчетом. Каждое нетривиальное решение строго больше тривиального. Следовательно, степени нетривиального решения образуют бесконечную возрастающую последовательность. Далее осталось ввести аналог деления с остатком, показать, что любые два решения имеют «общий делитель», степенями которого являются одновремено. Теперь, взяв минимальное нетривиальное неотрицательное решение, получим, что оно является «общим делителем» для всех нетривиальных неотрицательных решений. Осталось разобраться со знаками, что несложно.

Задача A.3. Для $D=m^2$ имеем $1=x^2-m^2y^2=(x-my)(x+my)$. Отсюда, очевидно, $\pm1=x+my=x-my$, и следовательно, $y=0$, $x=\pm1$ при $m\neq0$. Случай $m=0=D$ легко разбирается отдельно.

Задача A.4. В силу неудачной формулировки задача оказалась тривиальной.

Задача A.5. Предположим, что это неверно. Обозначим через t_k гиперболу, заданную уравнением $x^2-Dy^2=k$. Тогда на каждой из гипербол t_k лежит лишь конечное число целочисленных точек. Следовательно, для любого M в области, заключенной между гиперболами t_M и t_{-M}, также лежит лишь конечное число точек. Обозначим эту область через T_M

Асимптоты гипербол разделяют плоскость на 4 области. В каждой из областей лежит одна из ветвей гипербол. Каждая целочисленная точка (a,b) лежит в одном из секторов. Проведем из нее два луча в направлениях, параллельных границам этого сектора (т.е. асимптотам гипербол). Обозначим область, ограниченную лучами, через $L_{a,b}$.

Лучи пересекут соответствующую ветвь гиперболы в двух точках. Назовем ту часть ветви гиперболы, которая лежит между этими точками (т.е. внутри $L_{a,b}$) «запрещенной».

Возьмем теперь произвольную точку $(\hat{x},\hat{y})$ на гиперболе $x^2-Dy^2=k$. Проведем через неё две прямые, параллельные асимптотам гиперболы, и две прямые, симметричные им относительно начала координат. Эти две пары параллельных прямых ограничивают параллелограмм, вершины которого лежат на наших двух гиперболах. Следовательно, его внутренность целиком лежит внутри T_M. Обозначим этот параллелограмм через $P_{\hat{x},\hat{y}}$. Прямым подсчетом можно убедиться, что площадь этого паралелограмма не зависит от выбора точки на гиперболе и равна $2M/\sqrt{D}$.

Легко заметить следующий факт: точка (a,b) лежит внутри $P_{\hat{x},\hat{y}}$ тогда и только тогда, когда точка $(\hat{x},\hat{y})$ лежит внутри $L_{a,b}$ (т.е. в запрещенной области).

Поскольку целочисленных точек внутри T_M конечное число, то объединение соответствующих запрещенных областей ограничено. Следовательно, на t_M найдется такая точка $(\hat{x},\hat{y})$, которая не содержится ни в одной из запрещенных областей. Значит, параллелограмм $P_{\hat{x},\hat{y}}$ не содержит целочисленных точек. Однако при достаточно большом M это противоречит лемме Минковского, поскольку площадь параллелограмма неограниченно возрастает.

Указанное рассуждение позволяет также получить конкретную оценку для M. Достаточно потребовать $2M/\sqrt{D}>4$, т.е. $M>2\sqrt{D}$.

Задача A.6. В силу предыдущей задачи существует такое M, что решений для $m\leq M$ бесконечно много. Достаточно взять в качестве k наименьшее из таких чисел M.

Задача A.7. Рассмотрим снова «обобщенное» уравнение $x^2-Dy^2=k$, где k – некоторый выбираемый параметр. Решения таких уравнений для различных k и l можно «перемножить» по тем же формулам, что и обычные решения, получив новое решение для kl. Исходя из этого можно определить понятие «деления» решений (заметим, что его результат уже не всегда будет целой точкой, но всегда будет рациональной).

Умножая решение для 1 на решение для k, получаем снова решение для k. Поэтому нетривиальное решение для 1 можно попытаться сконструировать из двух различных решений для произвольного k. Мы уже знаем, что найдется такое k, для которого различных решений бесконечно много. Осталось выяснить, при каких обстоятельствах результат деления будет целочисленной парой. Это делается прямым подсчетом.

Задача А.8. Пусть (x, y) – нетривиальное рациональное решение. Проведем прямую через точки (x, y) и $(1, 0)$. Тангенс угла наклона будет рациональным числом $\lambda = (x-1)/y$. Обратно, пусть через точку $(1, 0)$ проходит прямая с рациональным наклоном. Тогда она пересекает гиперболу $x^2 - Dy^2 = 1$ в двух точках, одна из которых $(1, 0)$. Следовательно, вторая также имеет рациональные координаты (и однозначно определена).

Таким образом, имеется взаимно однозначное соответствие между прямыми указанного вида и нетривиальными рациональными решениями уравнения Пелля. Осталось лишь выписать это соответствие явно.

В. Уравнения Пелля для многочленов.

Задача В.1. Легко заметить, что для любого нетривиального решения (P, Q) выполняется равенство $\deg P = \deg Q + 1$. Пара $(x, 1)$ является решением. Поэтому по каждому решению (P, Q) можно построить новые решения, а именно $(Px + Q(x^2-1), P + Qx)$ и $(Px - Q(x^2-1), P - Qx)$ (результат умножения (P, Q) на $(x, 1)$ и $(x, -1)$). Отметим, что эти новые решения являются степенями $(x, 1)$ тогда и только тогда, когда его степенью является (P, Q).

Упорядочим решения по степени $\deg Q$ и покажем, что для любого решения (P, Q) одно из решений $(Px + Q(x^2-1), P + Qx)$, $(Px - Q(x^2-1), P - Qx)$ будет меньше исходного.

Перепишем исходное уравнение в виде

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

В правой части равенства степень в точности равна $2\deg Q$. Разложим левую часть на множители:

$$(P - xQ)(P + xQ) = 1 - Q^2.$$

Следовательно, $\deg(P-xQ)+\deg(P+xQ) = 2\deg Q$. Значит, хотя бы в одном из сомножителей старшие члены в слагаемых взаимно сокращаются. При этом $\deg P = \deg((P - xQ) + (P + xQ)) \le \max(\deg(P - xQ), \deg(P + xQ))$, поэтому сократиться одновременно в обоих сомножителях старшие члены не могут. Следовательно, одна из степеней в точности равна $\deg P$, а вторая равна $2\deg Q - \deg P = \deg Q - 1 < \deg Q$. Вот эта пара и будет нужным нам решением, которое меньше исходного.

Пусть теперь (P, Q) – наименьшее из решений, не являющихся степенью $(x, 1)$. Если $\deg Q > 0$, то, пользуясь описанной выше процедурой, построим меньшее решение, которое также не является степенью $(x, 1)$. Это противоречит минимальности (P, Q). Если же $\deg Q = 0$, то прямым подсчетом устанавливается, что единственно возможные варианты: $P = \pm x, Q = \pm 1$.

Задача В.2. Аналогично А.8.

Задача В.3. Для пункта б) перейти к уравнению $(P - iQ)(P + iQ) = 1$. Оба сомножителя – многочлены, но такое уравнение имеет только константные решения вида $(\lambda, 1/\lambda)$. Далее прямой подсчет показывает, что $P = \frac{\lambda^2+1}{2\lambda}$, $Q = \frac{\lambda^2-1}{2i\lambda}$, т.е. все решения тривиальны. Пункт а) эквивалентен пункту б) для рациональных функций. В этом случае λ уже не обязана быть константой, а может быть произвольной рациональной функцией. Форма решений при этом остается той же самой.

Задача В.4. Используем «школьную» формулу

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

для $x = P$, $y = \psi Q$ при любом $\psi^n = -1$. Далее замечаем, что таких ψ ровно n штук, т.е. 3 различных выбрать можно.

Задача В.5. Из предыдущей задачи следует, что $P - \psi_i Q$ – делители $P^n + Q^n$, а следовательно и R^n. Поскольку все $P - \psi_i Q$ попарно взаимно просты, то каждый линейный сомножитель может входить лишь в одно из них. Но в R^n он входит в степени, кратной n. Следовательно, любой из $P - \psi_i Q$ является произведением n-х степеней своих линейных сомножителей, т.е. равен R_i^n для некоторого R_i.

Для полноты картины нужно все же исключить в условии тривиальные решения, т.е. те, при которых P и Q отличаются на константный комплексный множитель.

Задача В.6. Пусть P, Q, R – нетривиальное решение, минимальное по степени. Тогда из предыдущей задачи имеем $R_i^n = P - \psi_i Q$. Подберем такие $\lambda_i \neq 0$, для которых выполнено $\lambda_1 R_1^n + \lambda_2 R_2^n = \lambda_3 R_3^n$. Для этого достаточно решить систему уравнений

$$\begin{cases} \lambda_1 + \lambda_2 = \lambda_3 \\ \lambda_1\psi_1 + \lambda_2\psi_2 = \lambda_3\psi_3, \end{cases}$$

которая, очевидно, совместна. Теперь осталось заметить, что тройка

$$(\lambda_1^{1/n} R_1, \lambda_2^{1/n} R_2, \lambda_3^{1/n} R_3)$$

даст новое решение, меньшее по степени, чем (P, Q, R).

Случай рациональных функций сводится к случаю многочленов.

C. Применения теоремы Коллара.

Под *нетривиальным решением* здесь понимается неконстантное решение.

Задача C.1. Аналогично A.3.

Задача C.2. Решение очень похоже на решение B.1. Пара $(R, 1)$ – решение, и для любого нетривиального решения (P, Q) выполнено равенство $\deg P = \deg Q + \deg P$.

Умножением на $(R, \pm 1)$ получаем решения $(PR + Q(R^2 - 1), P + QR)$ и $(PR - Q(R^2 - 1), P - QR)$, они будут степенями $(R, 1)$ одновременно с (P, Q).

Упорядочим решения по степени $\deg Q$ и покажем, что для любого решения (P, Q) одно из решений $(PR + Q(R^2 - 1), P + QR)$, $(PR - Q(R^2 - 1), P - QR)$ будет меньше исходного.

Перепишем исходное уравнение в виде

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

В правой части равенства степень в точности равна $2 \deg Q$. Разложим левую часть на множители:

$$(P - RQ)(P + RQ) = 1 - Q^2.$$

Следовательно, $\deg(P - RQ) + \deg(P + RQ) = 2 \deg Q$. Значит, хотя бы в одном из сомножителей старшие члены в слагаемых взаимно сокращаются. $\deg P = \deg((P-RQ)+(P+RQ)) \leq \max(\deg(P-RQ), \deg(P+RQ))$, поэтому сократиться одновременно в обоих сомножителях старшие члены не могут. Следовательно, одна из степеней в точности равна $\deg P$, а вторая равна $2 \deg Q - \deg P = \deg Q - \deg R < \deg Q$. Вот эта пара и будет нужным нам решением, которое меньше исходного.

Пусть теперь (P, Q) – наименьшее из решений, не являющихся степенью $(R, 1)$. Если $\deg Q > 0$, то, пользуясь описанной выше процедурой, построим меньшее решение, которое также не является степенью $(R, 1)$. Это противоречит минимальности (P, Q). Если же $\deg Q = 0$, то прямым подсчетом устанавливается, что единственно возможные варианты: $P = \pm R, Q = \pm 1$.

Задача C.3. Аналогично C.2. В самом деле, при решении C.2 мы никак не использовали структуру основного кольца.

Задача C.4. Аналогично A.3.

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

Задача C.5. Решается прямым подсчетом.

Задача C.6. Решается прямым подсчетом.

Задача C.7. Задача на «понимание». Последнее уравнение гарантирует, что U и V – константы (многочлены степени 0). Для первого уравнения возможные решения описаны в предыдущих задачах как серии вида (P_n, Q_n). При этом

$$Q_n = n \bmod (R - 1).$$

В силу второго уравнения $V = n$. Остальные переменные определяются прямым подсчетом.

Задача C.8. Основная задача. Идея заключается в том, чтобы продублировать систему из предыдущей задачи в n экземплярах и далее воспользоваться тем, что нетривиальные серии будут возникать лишь в том случае, когда V_i – целые константы. Добавив к системе уравнение $W(V_1, \ldots, V_n) = 0$, почти получаем нужную эквивалентность.

Для полноты картины нужно исключить случай константного R. При $R \neq 1$ все решения системы будут тривиальными (т.е. константами). Особый случай $R = 1$ для вещественного случая исключается, например, путем добавления уравнения $R = S^2 + 2$.

D. Аффинные многобразия.

Задача D.1. Все пункты задачи решаются прямым подсчетом. Указание: для начала понять, как можно из заданных систем уравнений для множеств сконструировать уравнения для их пересечения и объединения.

Задача D.2. Пусть f и g – две различные функции из одного класса эквивалентности. Тогда $f - g = R_1P_1 + \ldots + R_kP_k$. В частности, $f(x) - g(x) = R_1(x)P_1(x) + \ldots + R_k(x)P_k(x)$. Поскольку все $P_i(x) = 0$ при $x \in X$, получаем $f(x) - g(x) = 0$.

Задача D.3. Положим $t = \frac{y}{x}$. Дальнейшее проверяется прямым подсчетом.

Задача D.4. Формулы для вложения двумерного тора уже получены в п. 6 задачи D.1. Осталось связать параметрические представления таким образом, чтобы обход одной из них осуществлялся вдвое быстрее, чем другой. Можно, например, воспользоваться тригонометрической параметризацией окружности и формулами двойного угла (легко заметить, что они полиномиальны).

Задача D.5. (1) Пусть Петя может бесконечно долго продолжать игру. Это значит, что существует бесконечное множество прожекторов, не освещающих друг друга. Очевидно, что при $n = 1$ это невозможно. Далее нужно воспользоваться индукцией по n. Рассмотрим произвольный прожектор $(\hat{x}_1, \ldots, \hat{x}_n)$. Для любого другого имеется хотя бы одна координата с условием $x_m < \hat{x}_m$. Значит, хотя бы для одного m найдется бесконечное число прожекторов с координатой $x_m < \hat{x}_m$. Среди них можно выбрать бесконечное подмножество прожекторов с одинаковым значением x_m. Далее, исключая эту координату, оказываемся в условиях той же задачи для размерности $n - 1$.

(2) Векторы степеней старших мономов можно рассматривать как координаты прожекторов из предыдущего пункта.

(3) Указание: разделить полиномы друг на друга с остатком. Остаток будет уменьшаться, если старший моном делимого больше или равен старшему моному делителя.

E. Отображения аффинных многообразий.

Не забывайте подходить с вопросами и за подсказками!

Задача E.1. Все пункты проверяются прямым подсчетом.

Задача E.2. 1) Возьмем в идеале многочлен минимальной степени и покажем, используя алгоритм Евклида, что все остальные элементы идеала на него делятся.

2) Например, $\mathbb{C}[x, y]$.

Задача E.3. Проверяется прямым подсчетом.

Задача E.4. Естественный способ индуцировать φ по заданному $f : X \to Y$ следующий: положить $\varphi(g) = h$, где $h(x) = g(f(x))$ для любого $x \in X$. Легко проверить, что $\varphi : R[Y] \to R[X]$ – гомоморфизм колец. Теперь посмотрим, как по заданному φ построить f. Должно выполняться условие $g \circ f = \varphi(g)$ для любого g. Пусть $\pi_i \in R[Y]$ – функция, сопоставляющая точке y ее i-ю координату. Тогда $h_i = \pi \circ f = \varphi(\pi)$, и отображение $h : x \to (h_1(x), \ldots, h_n(x))$ удовлетворяет нужным условиям. Осталось проверить, что h отображает точки X в точки Y. Это делается прямым подсчетом (с учетом того, что φ – гомоморфизм).

Задача E.5. Имеем $\varphi^*(g) = g \circ \varphi$, поэтому $\varphi^*(g) = g$ тогда и только тогда, когда $g(x, y) = g(-x, -y)$ для любых $(x, y) \in \mathbb{C}^2$. Прямым подсчетом проверяется, что это верно в точности для всех многочленов, которые являются суммами мономов, общая степень которых четна. Наименьшими такими неконстантными мономами являются x^2, xy и y^2. Все остальные выражаются как многочлены от них. Иными словами, искомое инвариантное кольцо порождено (как кольцо) этими мономами (и 1). Осталось построить явно искомый изоморфизм. Положим $u \to x^2$, $v \to y^2$, $w \to xy$ и продолжим его до гомоморфизма колец. Прямым подсчетом убедимся, что это изоморфизм. При наличии явного изоморфизма вторая часть задачи сводится к E.4.

Задача E.6. Для решения явно построим соответствующие кольца функций и вложения. Далее остается показать, что вложение кольца функций над $\mathbb{C}^n$ в кольцо функций над $(\mathbb{C} \setminus 0)^n$ не является факторизацией. Для этого, можно, например, воспользоваться тем фактом, что над $\mathbb{C}^n$ обратимы только константы, а над $(\mathbb{C} \setminus 0)^n$ обратимых функций гораздо больше (например, над $\mathbb{C} \setminus 0$ обратимы все полиномы $f(x) = x^n$).

Задача E.7. Идея решения аналогична предыдущей задаче. Нужно показать, что $\mathbb{C}[t^2, t^3]$ не изоморфно никакому фактор-кольцу кольца $\mathbb{C}[t]$. Легко видеть, что $\mathbb{C}[t^2, t^3]$ не изоморфно самому $\mathbb{C}[t]$. Поэтому осталось рассмотреть случай факторизации по некоторому собственному идеалу. Все идеалы главные, поэтому задача сводится к случаю факторизации по идеалу $\langle f \rangle$, где $f \in \mathbb{C}[t]$ – неконстантый многочлен. Далее можно описать такие фактор-кольца и показать, что ни одно из них не изоморфно $\mathbb{C}[t^2, t^3]$. Идея описания состоит в рассмотрении корней многочлена f.

Задача E.8. Первое утверждение задачи становится очевидным после построения графика. Для решения второй части задачи нужно явно вычислить точки самопересечения плоского графика и подобрать многочлен h таким образом, чтобы эти точки в пространстве образовывали нужную конфигурацию (т.е. значения $h(t)$ при соответствующих t появлялись в правильном порядке). Это можно сделать прямым подсчетом.

Задача E.9 (Слабая теорема Гильберта о нулях)**.** (1) Выберем в качестве a один из корней многочлена p. Т.к. $p(a) = 0$, получаем $p(x_1) = (x_1 - a)q(x_1)$ для некоторого $q \in \mathbb{C}[x_1]$, $\deg q = \deg p - 1$.

Пусть пункт 1 не выполняется. Тогда $ev_a(I) = \mathbb{C}[x_2, \ldots, x_n]$ и, следовательно, $1 \in ev_a(I)$. Для любого $f \in \mathbb{C}[x_1, \ldots, x_n]$ выполнено равенство $f = (x_1 - a)g + ev_a(f)$, где $g \in \mathbb{C}[x_1, \ldots, x_n]$ (это просто деление с остатком на $x_1 - a$). Поэтому найдется такое $\hat{f} \in I$, что $\hat{f} = (x_1 - a)\hat{g} + 1$. Умножая это равенство на $q(x_1)$, получаем $q\hat{f} = (x_1 - a)q\hat{g} + q$ или же $q = q\hat{f} - p\hat{g}$. Оба слагаемых в правой части лежат в I, поскольку $\hat{f} \in I$ и $p \in I$. Следовательно, $q \in I \cap \mathbb{C}[x_1] = \langle p(x_1) \rangle$. А это невозможно, т.к. $q = p/(x_1 - a)$. Полученное противоречие доказывает, что пункт 1 должен выполняться.

(2) Очевидно, отображение ev_a является гомоморфизмом колец. На его основе можно определить его аналоги над векторами и матрицами, коэффициентами которых являются многочлены. Эти отображения также будут гомоморфизмами. Также легко доказать следующий факт: для любого набора попарно различных чисел $a_0, \ldots, a_d$ и любого целого i, $0 \le i \le d$, существует единственный многочлен $\chi_i(t)$ степени d, такой что $\chi_i(a_i) = 1$ и $\chi_i(a_j) = 0$ при любом $j \ne i$.

Отсюда будет следовать, что для любого коммутативного кольца R, содержащего $\mathbb{C}$ в качестве подкольца, любого набора попарно различных чисел $a_0, \ldots, a_d$ и любого набора элементов $r_0, \ldots, r_d$ существует единственный многочлен $r \in R[t]$ степени не выше d, для которого при всех i выполнено $r(a_i) = r_i$. В самом деле, достаточно положить $r(t) = \sum_{i=0}^{d} r_i \chi_i(t)$.

В последнем пункте задачи D.5 было показано, что любой идеал может быть задан конечным базисом. Обозначим элементы конечного базиса для I через $g_1, \ldots, g_m$. Ясно, что $ev_a(g_1), \ldots, ev_a(g_m)$ образуют базис в $ev_a(I)$. Обозначим через d максимальную из степеней g_i относительно переменной x_1.

Каждый из g_i может быть представлен в виде $g_i = \sum_{i=0}^{d} x_1^j g_{ij}$, где $g_{ij} \in \mathbb{C}[x_2]$. Обозначим через G матрицу $m \times (d+1)$, состоящую из элементов вида $g_{ij} \in \mathbb{C}[x_2]$, где $1 \le i \le m$, $0 \le j \le d$. Поскольку все элементы G суть многочлены из $\mathbb{C}[x_2]$, то $ev_a(G) = G$.

Если v - вектор-строка, то через v^T обозначим соответствующий ему вектор-столбец (результат транспонирования).

Обозначим через $V(z)$ вектор-строку $(1, z, \ldots, z^d)$ длины $d+1$. В данном случае z может быть любым многочленом, но нам потребуется его использовать лишь для случая $z = x_1$ или же $z \in \mathbb{C}$. Легко проверить, что $ev_a(V(x_1)) = V(a)$, $ev_a(V^T(x_1)) = V^T(a)$.

Прямой подсчет показывает, что $GV^T(x_1) = (g_1, \ldots, g_m)^T$ - вектор-столбец, состоящий из базисных полиномов для I. Применяя операцию ev_a, мы можем явно представить базисы для идеалов $ev_a(I)$ в матрично-векторном виде. А именно,

$$ev_a(GV^T(x_1)) = G \cdot ev_a(V^T(x_1)) = GV(a)$$

будет матрицей, строки которой образуют базис в $ev_a(I)$.

Допустим теперь, что утверждение пункта 2 не выполняется. Тогда рассмотрим произвольный набор попарно различных чисел $a_0, \ldots, a_d$. Для каждого из них $ev_{a_i}(I) = \mathbb{C}[x_2]$. Это означает, что $1 \in ev_{a_i}(I)$, т.е. существуют такие $h_{ij} \in \mathbb{C}[x_2]$, что $1 = \sum_{j=1}^{m} h_{ij} \cdot ev_{a_i}(g_j)$. Для каждого j, $1 \le j \le m$, обозначим через H_j такой многочлен из $\mathbb{C}[x_1, x_2]$ степени не выше d (по x_1), для которого $ev_{a_i}(H_j) = h_{ij}$. Как указано выше, он существует и единственен.

Рассмотрим теперь вектор-строку $H = (H_1, \ldots, H_m)$ и матричное произведение $HGV^T(x_1)$. С одной стороны, это некоторый многочлен из $\mathbb{C}[x_1, x_2]$. Легко проверить, что это есть линейная комбинация строк $GV^T(x_1)$ с полиномиальными коэффициентами (H_j). Поскольку строки $GV^T(x_1)$ суть элементы базиса I, то и $HGV^T(x_1) \in I$. С другой стороны, если зафиксировать i и рассмотреть $ev_{a_i}(HGV^T(x_1))$, то мы получим

$$ev_{a_i}(HGV^T(x_1)) = \sum_{j=1}^{m} h_{ij} \cdot ev_{a_i}(g_j) = 1.$$

Таким образом, $HGV^T(x_1)$ равен 1 в $d+1$ различных точках (как многочлен от x_1). При этом он имеет степень $\le d$ по x_1. Отсюда следует, что $HGV^T(x_1) = 1$. А значит, $1 \in I$. Это противоречит исходному требованию $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$. Полученное противоречие доказывает, что пункт 2 должен выполняться.

(3) Аналогично пункту 2. В самом деле, мы нигде не пользовались тем, что переменных в точности две. Поэтому достаточно везде, где использовалось кольцо $\mathbb{C}[x_2]$, заменить его на $\mathbb{C}[x_2, \ldots, x_n]$ (и, соответственно, $\mathbb{C}[x_1, x_2]$ на $\mathbb{C}[x_1, x_2, \ldots, x_n]$).

(4) Пункт 4 доказывается при помощи предыдущих пунктов индукцией по n. В случае $n = 1$ утверждение теоремы в точности эквивалентно пункту 1. При $n > 1$ есть два варианта – либо $I \cap \mathbb{C}[x_1] = \emptyset$ и задача сводится к пункту 3 и утверждению самой теоремы для $n-1$ переменных (т.е. предположению индукции), либо $I \cap \mathbb{C}[x_1] = \emptyset$ и задача сводится к пункту 1 и опять-таки предположению индукции.

Заметим, что фактически мы доказали более сильное утверждение, чем исходная задача. А именно: если в идеале I присутствуют уравнения от одной конкретной переменной x_i, то среди них существует минимальное (в смысле степени) уравнение вида $P_i(x_i) = 0$. При этом, с одной стороны, все решения системы должны совпадать в координате x_i с корнем многочлена P_i, а с другой стороны, любой корень многочлена P_i содержится хотя бы в одном решении исходной системы; в противном случае почти все значения переменной x_i содержатся в решениях, за исключением конечного их числа, не превосходящего максимальную степень уравнений в системе по переменной x_i.

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 $H(x_1, \ldots, x_m)$ установить, имеет ли он целочисленное решение или нет.* [1]

Серия F1. Разложение многочленов и подстановки.

Задача F.1. Решается прямым подсчетом.

Задача F.2. Будет опубликовано позже.

Замечание. Доказательство аналогичного факта даже для кубического многочлена нам неизвестно. Мы можем доказать его для двучленов $ax^n + b$.

Задача F.3. Решается прямым подсчетом.

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

Построим такие семейства полиномов $H_m(x_1, \ldots, x_m)$, $P_m(x_1, \ldots, x_m)$, для которых одновременно выполняются условия делимости $H_k(x_1, \ldots, x_k) \mid (P_m(x_1, \ldots, x_m) - k)$ при всех $k \in \{1, \ldots, m\}$.

Для $m = 1$ можно положить $H_1(x_1) = x_1$, $P_1(x_1) = x_1 + 1$.

Пусть для некоторого m соответствующие семейства уже построены. Положим $P'_{mk} = P_m - k$ и

$$Q_m(x_1, \ldots, x_m) = \prod_{k=1}^{m} P'_{mk}(x_1, \ldots, x_m) = \prod_{k=1}^{m} (P_m(x_1, \ldots, x_m) - k).$$

Рассмотрим полином

$$P''_m(x_1, \ldots, x_m, u) = P(x_1 + uQ_m(x_1, \ldots, x_m), \ldots, x_m + uQ_m(x_1, \ldots, x_m)).$$

Из решения задачи F.1 следует, что $P''_m(x_1, \ldots, x_m, u)$ представляется в виде

$$P_m(x_1, \ldots, x_m) + Q_m(x_1, \ldots, x_m)R_m(x_1, \ldots, x_m, u)$$

Обозначая $P'''_{mk} = P''_m - k$, получаем аналогичное представление

$$P'''_{mk}(x_1, \ldots, x_m, u) = P'_{mk}(x_1, \ldots, x_m) + Q_m(x_1, \ldots, x_m)R_m(x_1, \ldots, x_m, u)$$

По предположению индукции для P_m выполнены условия делимости: $H_k \mid P'_{mk}$. Поскольку Q_m также делится на P'_{mk}, имеем

$$P'''_{mk}(x_1, \ldots, x_m, u) = P'_{mk}(x_1, \ldots, x_m)R'_{mk}(x_1, \ldots, x_m, u), \tag{1}$$

где

$$R'_{mk}(x_1, \ldots, x_m, u) = 1 + R_m(x_1, \ldots, x_m, u) \cdot \frac{Q_m(x_1, \ldots, x_m)}{P'_{mk}(x_1, \ldots, x_m)} \tag{2}$$

Это означает, что полином $P''_m(x_1, \ldots, x_m, u)$ делится на P'_{mk}, а следовательно и на H_k (при всех $k \in \{1, \ldots, m\}$).

Таким образом, сконструированный нами полином P''_m (от $m + 1$ переменной) выглядит подходящим кандидатом на роль нового P_{m+1}. Осталось лишь выбрать подходящий H_{m+1} и добиться выполнения условия делимости для $k = m + 1$.

Запишем искомое условие делимости: $H_{m+1} \mid P'''_{m,m+1}$. В силу формул (1) и (2) получаем

$$P'''_{m,m+1}(x_1, \ldots, x_m, u) = P'_{m,m+1}(x_1, \ldots, x_m)R'_{m,m+1}(x_1, \ldots, x_m, u)$$

где

$$R'_{m,m+1}(x_1, \ldots, x_m, u) = 1 + R_m(x_1, \ldots, x_m, u) \cdot \frac{Q_m(x_1, \ldots, x_m)}{P'_{m,m+1}(x_1, \ldots, x_m)}$$

Для выполнения условий делимости достаточно положить

$$H_{m+1}(x_1, \ldots, x_m, x_{m+1}) = R'_{m,m+1}(x_1, \ldots, x_m, x_{m+1})$$

и

$$P_{m+1}(x_1, \ldots, x_m, x_{m+1}) = P''_m(x_1, \ldots, x_m, x_{m+1}).$$

Дополненные семейства полиномов будут удовлетворять условиям делимости при всех $k \in \{1, \ldots, m+1\}$, что и приводит к решению задачи.

Задача F.5. Из построения многочленов в предыдущей задаче ясно, что H_{m+1} и P_{m+1} существенно зависят от переменной x_{m+1}.

---

[1] На самом деле можно положить $m = 11$.

Задача F.6. Примером является конструкция из предыдущих задач.

Серия F2. Конструкция систем уравнений.

Задача F.7. Возможность построения нужного полинома $\hat{P}$ следует из решения задач предыдущей серии. Ясно, что полученная система уравнений задает некоторое многообразие.

Задача F.8. Проверяется прямым подсчетом.

Задача F.9. Строим многообразие по схеме, описанной в задаче F.7. Нетривиальные решения кодируются целочисленными параметрами (по одному на каждую из подсистем). Идеи, аналогичные использованным в решении задачи C.8, приводят к возможности построения системы, имеющей нетривиальные решения лишь в случае, когда некоторый полином от многих переменных имеет целочисленное решение. Решение задачи F.8 позволяет проконтролировать случай «лишних» компонент, порождаемых «частично константными» решениями (когда константы присутствуют лишь в некоторых из подсистем). Это делается через контроль размерности. Таким образом, задача о существовании вложения сводится к задаче о разрешимости диофантовых уравнений. А она неразрешима в силу теоремы Матиясевича.