Кубики Решают

Алексей Кислицын Андрей Владимиров Всеволод Триль

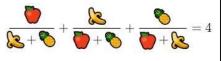
Механико-математический факультет МГУ

30 ноября 2022 г.

Постановка задачи

Всё началось с, кажущейся на первый взгляд, детской задачки:

95% of people cannot solve this!

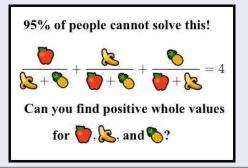


Can you find positive whole values

for **()**, **()**, and **()**?

Постановка задачи

Всё началось с, кажущейся на первый взгляд, детской задачки:



В этом докладе мы предъявим алгоритм решения данной задачи, а также постараемся её обобщить и проанализировать.

Переформулируем её в математических терминах: требуется найти все натуральные решения следующего уравнения при ${\it N}=4$:

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = N, \quad x, y, z \in \mathbb{N}.$$

Мы пока не будем придавать значения тому, что N=4, а сразу будем рассматривать постановку задачи для произвольного $N\in\mathbb{N}$.

Переформулируем её в математических терминах: требуется найти все натуральные решения следующего уравнения при ${\it N}=4$:

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = N, \qquad x, y, z \in \mathbb{N}.$$

Мы пока не будем придавать значения тому, что N=4, а сразу будем рассматривать постановку задачи для произвольного $N\in\mathbb{N}.$

Заметим, что решение исходного уравнения равносильно нахождению натуральных точек на кубике, заданной в однородных координатах (x:y:z) следующим уравнением:

$$x^3 + y^3 + z^3 + (1 - N)(x^2y + y^2x + x^2z + z^2x + y^2z + z^2y) + (3 - 2N)xyz = 0.$$

Переформулируем её в математических терминах: требуется найти все натуральные решения следующего уравнения при ${\it N}=4$:

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = N, \qquad x, y, z \in \mathbb{N}.$$

Мы пока не будем придавать значения тому, что N=4, а сразу будем рассматривать постановку задачи для произвольного $N\in\mathbb{N}$.

Заметим, что решение исходного уравнения равносильно нахождению натуральных точек на кубике, заданной в однородных координатах (x:y:z) следующим уравнением:

$$x^3 + y^3 + z^3 + (1 - N)(x^2y + y^2x + x^2z + z^2x + y^2z + z^2y) + (3 - 2N)xyz = 0.$$

Сразу отметим, что так как мы работаем в проективных координатах, то это равносильно нахождению точек с рациональными координатами, у которых знаки одинаковы.

Но перед тем, как перейти к решению исходной задачи, рассмотрим более простую задачу – поиск натуральных точек на квадрике

Но перед тем, как перейти к решению исходной задачи, рассмотрим более простую задачу – поиск натуральных точек на квадрике

Описание рациональных точек на квадрике

Рассмотрим квадрику с целыми коэффициентами на проективной плоскости в однородных координатах (x:y:z):

$$ax^2 + by^2 + cz^2 + dxy + eyz + fxz = 0$$
, $a, b, c, d, e, f \in \mathbb{Z}$.

Но перед тем, как перейти к решению исходной задачи, рассмотрим более простую задачу – поиск натуральных точек на квадрике

Описание рациональных точек на квадрике

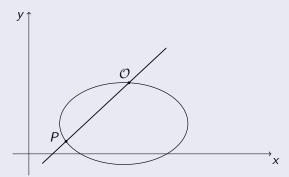
Рассмотрим квадрику с целыми коэффициентами на проективной плоскости в однородных координатах (x:y:z):

$$ax^2 + by^2 + cz^2 + dxy + eyz + fxz = 0,$$
 $a, b, c, d, e, f \in \mathbb{Z}.$

Метод секущих

Для начала заметим, что, зная одну рациональную точку на квадрике, можно получить все остальные рациональные точки методом секущих Диофанта.

А именно, если \mathcal{O} – рациональная точка, то P – тоже рациональная по теореме Виета.



Поиск рациональной точки. Шаг 1.

Приведём квадрику рациональным преобразованием к одному из следующих видов.

$$Ax^2 - By^2 = 0$$
$$Ax^2 + By^2 - Cz^2 = 0$$

Поиск рациональной точки. Шаг 1.

Приведём квадрику рациональным преобразованием к одному из следующих видов.

$$Ax^2 - By^2 = 0$$
$$Ax^2 + By^2 - Cz^2 = 0$$

Шаг 2.

Случай 1 разбирается тривиально. Во втором случае используем критерий Лежандра. Согласно нему, уравнение 2 имеет целочисленное решение, тогда и только тогда, когда BC есть квадратичный вычет по модулю A, AC — по модулю B и -AB — по модулю C.

Поиск рациональной точки. Шаг 1.

Приведём квадрику рациональным преобразованием к одному из следующих видов.

$$Ax^2 - By^2 = 0$$
$$Ax^2 + By^2 - Cz^2 = 0$$

Шаг 2.

Случай 1 разбирается тривиально. Во втором случае используем критерий Лежандра. Согласно нему, уравнение 2 имеет целочисленное решение, тогда и только тогда, когда BC есть квадратичный вычет по модулю A, AC — по модулю B и -AB — по модулю C.

Замечание

Таким образом поиск рациональной точки это полностью решённая проблема в случае квадрики. Более того, есть теорема Хольцера, которая даёт верхнюю оценку на границы, в которых его надо искать.

Приведение к нормальной форме Вейерштрасса

Перейдём к основной задаче, как и в случае квадрики приведём кубику

$$x^{3} + y^{3} + z^{3} + (1 - N)(x^{2}y + y^{2}x + x^{2}z + z^{2}x + y^{2}z + z^{2}y) + (3 - 2N)xyz = 0$$

к наиболее простому виду – нормальной форме Вейерштрасса, которая может записывается так:

$$y^2z = x^3 + axz^2 + bz^3$$
, $a, b \in \mathbb{C}$.

Приведение к нормальной форме Вейерштрасса

Перейдём к основной задаче, как и в случае квадрики приведём кубику

$$x^{3} + y^{3} + z^{3} + (1 - N)(x^{2}y + y^{2}x + x^{2}z + z^{2}x + y^{2}z + z^{2}y) + (3 - 2N)xyz = 0$$

к наиболее простому виду – нормальной форме Вейерштрасса, которая может записывается так:

$$y^2z = x^3 + axz^2 + bz^3$$
, $a, b \in \mathbb{C}$.

В нашем случае, так как коэффициенты кубики целые и проективные преобразования будут с целыми коэффициентами, то $a,b\in\mathbb{Z}$. Далее, под проективными преобразованиями мы будем понимать только целочисленные проективные преобразования.

Приведение к нормальной форме Вейерштрасса

Перейдём к основной задаче, как и в случае квадрики приведём кубику

$$x^{3} + y^{3} + z^{3} + (1 - N)(x^{2}y + y^{2}x + x^{2}z + z^{2}x + y^{2}z + z^{2}y) + (3 - 2N)xyz = 0$$

к наиболее простому виду – нормальной форме Вейерштрасса, которая может записывается так:

$$y^2z = x^3 + axz^2 + bz^3$$
, $a, b \in \mathbb{C}$.

В нашем случае, так как коэффициенты кубики целые и проективные преобразования будут с целыми коэффициентами, то $a,b\in\mathbb{Z}$. Далее, под проективными преобразованиями мы будем понимать только целочисленные проективные преобразования.

Мы предъявим алгоритм приведения кубики к нормальной форме Вейерштрасса для произвольной кубики с целыми (рациональными) коэффициентами.

Шаг 0. Нахождение рациональных точек перегиба

Итак, пусть у нас есть кубика, заданная уравнением ${\it F}(x,y,z)=0$, где

$$\begin{split} F(x,y,z) &= a_{30}x^3 + a_{03}y^3 + a_{00}z^3 + a_{01}yz^2 + a_{10}xz^2 + a_{11}xyz + \\ &\quad + a_{21}x^2y + a_{12}xy^2 + a_{20}x^2z + a_{02}y^2z, \end{split}$$

то есть $a_{ij} \in \mathbb{Z}$ – коэффициент при мономе $x^i y^j z^{3-i-j}$.

Шаг О. Нахождение рациональных точек перегиба

Итак, пусть у нас есть кубика, заданная уравнением F(x,y,z)=0, где

$$F(x, y, z) = a_{30}x^3 + a_{03}y^3 + a_{00}z^3 + a_{01}yz^2 + a_{10}xz^2 + a_{11}xyz + a_{21}x^2y + a_{12}xy^2 + a_{20}x^2z + a_{02}y^2z,$$

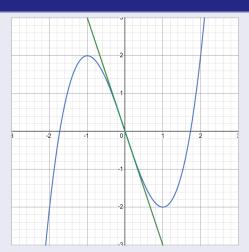
то есть $a_{ij} \in \mathbb{Z}$ – коэффициент при мономе $x^i y^j z^{3-i-j}$.

Определение

Точка P_0 кубики $F(x^1,x^2,x^3)=0$ называется точкой перегиба, если касательная к ней в точке P имеет касание третьего порядка, то есть для любой точки $Q=(x_q^1:x_q^2:x_q^3)$ на касательной выполнено

$$\sum_{i,j=1}^{3} \frac{\partial^{2} F}{\partial x^{i} \partial x^{j}} (P_{0}) x_{q}^{i} x_{q}^{j} = 0.$$

Пример



уравнение кубики $y=x^3-3x$, уравнение касательной y=-3x; точка (0,0) – точка перегиба

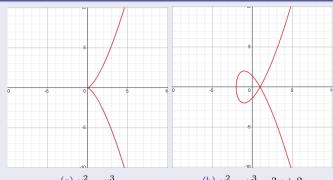
Точка P_0 кубики $F(x^1, x^2, x^3) = 0$ называется *особой*, если

$$\frac{\partial F}{\partial x^1}(P_0) = \frac{\partial F}{\partial x^2}(P_0) = \frac{\partial F}{\partial x^3}(P_0) = 0.$$

Точка P_0 кубики $F(x^1, x^2, x^3) = 0$ называется *особой*, если

$$\frac{\partial F}{\partial x^1}(P_0) = \frac{\partial F}{\partial x^2}(P_0) = \frac{\partial F}{\partial x^3}(P_0) = 0.$$

Примеры



Гессианом кубики $F(x^1,x^2,x^3)=0$ называется кубика

$$H(F) := \det \left(\frac{\partial^2 F}{\partial x^i \partial x^j} \right)_{ii}.$$

Гессианом кубики $F(x^1,x^2,x^3)=0$ называется кубика

$$H(F) := \det \left(\frac{\partial^2 F}{\partial x^i \partial x^j} \right)_{ij}.$$

Теорема

Точки перегиба неособой кубики в $\mathbb{C}\mathrm{P}^2$ – в точности точки пересечения кубики с её Гессианом.

Мы не будем проверять кубику на наличие особенностей, а просто найдём все точки пересечения с Гессианом и посмотрим, есть ли там особенности. Если среди общих точек есть неособая, то нам эта точка подходит и мы можем переходить к следующему шагу. Если все точки особые, то алгоритм продолжить нельзя.

Мы не будем проверять кубику на наличие особенностей, а просто найдём все точки пересечения с Гессианом и посмотрим, есть ли там особенности. Если среди общих точек есть неособая, то нам эта точка подходит и мы можем переходить к следующему шагу. Если все точки особые, то алгоритм продолжить нельзя.

Для поиска общих точек рассмотрим результант R(F,H(F)) по переменной z. Получим однородный многочлен 9-той степени или тождественно нулевой. Находим все его рациональный корни — пары (x,y) и подставляем в F и в H(F) для нахождения общей точки (или удостоверении, что при данных (x_0,y_0) её нет).

Мы не будем проверять кубику на наличие особенностей, а просто найдём все точки пересечения с Гессианом и посмотрим, есть ли там особенности. Если среди общих точек есть неособая, то нам эта точка подходит и мы можем переходить к следующему шагу. Если все точки особые, то алгоритм продолжить нельзя.

Для поиска общих точек рассмотрим результант R(F,H(F)) по переменной z. Получим однородный многочлен 9-той степени или тождественно нулевой. Находим все его рациональный корни — пары (x,y) и подставляем в F и в H(F) для нахождения общей точки (или удостоверении, что при данных (x_0,y_0) её нет).

Этот шаг реализован в файле InflectionPoints.py в функции find_non_singular_inflection_point.

Шаг 1. Избавление от монома y^3

Выберем какую-то рациональную точку перегиба P и переведём её в точку (0:1:0) некоторым проективным преобразованием. После проективного преобразования, наша кубика имеет уравнение $\widetilde{F}(\widetilde{x},\widetilde{y},\widetilde{z})$, в котором нет \widetilde{y} . Таким образом, у нас уйдёт моном y^3 .

Шаг 1. Избавление от монома y^3

Выберем какую-то рациональную точку перегиба P и переведём её в точку (0:1:0) некоторым проективным преобразованием. После проективного преобразования, наша кубика имеет уравнение $\widetilde{F}(\widetilde{x},\widetilde{y},\widetilde{z})$, в котором нет \widetilde{y} . Таким образом, у нас уйдёт моном y^3 .

Этот шаг реализован в файле WeierstrassForm.py в функции weierstrass form step1.

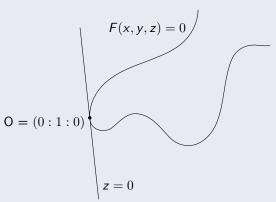
Шаг 2. Избавление от мономов y^2x и yx^2

Теперь мы хотим сделать преобразование, сохраняющее точку O=(0:1:0), так, чтобы прямая z=0 была касательной к кубике \widetilde{F} в точке O, то есть сделать преобразование $(\widetilde{x}:\widetilde{y}:\widetilde{z}) \to (x':y':z')$, такое что для F'(x',y',z') будет выполнено:

$$\frac{\partial F'}{\partial x'}(O) = \frac{\partial F'}{\partial y'}(O) = 0, \quad \frac{\partial F'}{\partial z'}(O) \neq 0.$$

То есть нет монома xy^2 , однако, коэффициент при y^2z отличен от нуля, и поэтому, разделив на него, можем считать, что он равен 1. Кроме того, так как O – точка перегиба, то касание прямой z=0 с нашей кубикой имеет порядок 3, таким образом нет монома x^2y .

Схематично это себе можно представлять так:



Шаг 3. Выделение y^2z и избавление от x^2z

После второго преобразования, уравнение нашей кубики стало F'(x',y',z')=0, где

$$F'(x', y', z') = a'_{30}(x')^{3} + a'_{20}(x')^{2}z' + a'_{11}x'y'z' + (y')^{2}z' + a'_{10}x'(z')^{2} + a'_{01}y'(z')^{2} + a'_{00}(z')^{3}.$$

Шаг 3. Выделение y^2z и избавление от x^2z

После второго преобразования, уравнение нашей кубики стало F'(x',y',z')=0, где

$$F'(x', y', z') = a'_{30} (x')^{3} + a'_{20} (x')^{2} z' + a'_{11} x' y' z' + (y')^{2} z' + + a'_{10} x' (z')^{2} + a'_{01} y' (z')^{2} + a'_{00} (z')^{3}.$$

Делая замену $y''=y'+(a'_{01}z'+a'_{11}x')/2$, выделяем полный квадрат по y' и уравнение кубики становится:

$$(y'')^2 z' = a_{30}''(x')^3 + a_{20}''(x')^2 z' + a_{10}''x'(z')^2 + a_{00}''(z')^3$$
.

Шаг 3. Выделение y^2z и избавление от x^2z

После второго преобразования, уравнение нашей кубики стало F'(x',y',z')=0, где

$$F'(x', y', z') = a'_{30} (x')^{3} + a'_{20} (x')^{2} z' + a'_{11} x' y' z' + (y')^{2} z' + + a'_{10} x' (z')^{2} + a'_{01} y' (z')^{2} + a'_{00} (z')^{3}.$$

Делая замену $y''=y'+(a_{01}'z'+a_{11}'x')/2$, выделяем полный квадрат по y' и уравнение кубики становится:

$$(y'')^2 z' = a_{30}''(x')^3 + a_{20}''(x')^2 z' + a_{10}''x'(z')^2 + a_{00}''(z')^3$$
.

Теперь линейной заменой $x''=x'-\frac{a_{20}''}{3a_{30}''}z'$ избавляемся от монома $\left(x'\right)^2z'$ и получаем:

$$(y'')^2 z' = a_{30}''' (x'')^3 + a_{10}''' x'' (z')^2 + a_{00}''' (z')^3.$$

Далее, делаем замену $z'' = \frac{1}{a_{222}'''}z'$ и получаем:

$$(y'')^2 z'' = (x'')^3 + a_{30}''' a_{10}''' x'' (z'')^2 + a_{00}''' (a_{30}''')^2 (z'')^3.$$

Обозначая $a:=a_{30}^{\prime\prime\prime}a_{10}^{\prime\prime\prime}, b:=a_{00}^{\prime\prime\prime}\left(a_{30}^{\prime\prime\prime}\right)^2$, получаем требуемую форму:

$$(y'')^2 z'' = (x'')^3 + ax'' (z'')^2 + b (z'')^3.$$

Далее, делаем замену $z'' = \frac{1}{a_{30}'''}z'$ и получаем:

$$\left(y''\right)^{2}z''=\left(x''\right)^{3}+a_{30}'''a_{10}'''x''\left(z''\right)^{2}+a_{00}'''\left(a_{30}'''\right)^{2}\left(z''\right)^{3}.$$

Обозначая $a:=a_{30}^{\prime\prime\prime}a_{10}^{\prime\prime\prime}, b:=a_{00}^{\prime\prime\prime}\left(a_{30}^{\prime\prime\prime}\right)^2$, получаем требуемую форму:

$$(y'')^2 z'' = (x'')^3 + ax'' (z'')^2 + b (z'')^3.$$

Замечание

Отметим, что все коэффициенты в ходе алгоритма получались целочисленными или рациональными (так как совершались только целочисленные проективные преобразования). Соответственно, если коэффициенты a,b оказались рациональными, мы их можем сделать целыми с помощью замены $x'''=\frac{1}{d}x'',z'''=\frac{1}{d^3}z''$, где d – наименьшее общее кратное знаменателей a,b.



Опишем рациональные точки на кубике в форме Вейерштрасса. Пусть нам известно несколько точек, можно ли по ним как в случае квадрики получить ещё?

Опишем рациональные точки на кубике в форме Вейерштрасса. Пусть нам известно несколько точек, можно ли по ним как в случае квадрики получить ещё?

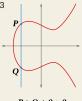
Сложение точек



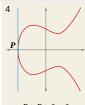




P+Q+Q=0



P+Q+0=0



P+P+0=0

Опишем рациональные точки на кубике в форме Вейерштрасса. Пусть нам известно несколько точек, можно ли по ним как в случае квадрики получить ещё?

Определение

Суммой точек P и Q назовём точку пересечения прямой PQ с кубикой, отражённую относительно оси x и будем обозначать P+Q.

Теорема

Множество рациональных точек кубики $E(\mathbb{Q})$ в нормальной форме Вейерштрасса образуют абелеву группу.

Теорема

Множество рациональных точек кубики $E(\mathbb{Q})$ в нормальной форме Вейерштрасса образуют абелеву группу.

Теорема (Морде)

Группа $E(\mathbb{Q})$ конечно порождена.

Теорема

Множество рациональных точек кубики $E(\mathbb{Q})$ в нормальной форме Вейерштрасса образуют абелеву группу.

Теорема (Морде)

Группа $E(\mathbb{Q})$ конечно порождена.

Это даёт надежду на полное описание рациональных точек на кубике. Ведь есть явные формулы для сложения точек в нормальной форме.

Явные формулы для P+Q

Пусть $P=(x_p,y_p),\,Q=(x_q,y_q),\,R=(x_r,y_r),\,$ где R=P+Q и $P\neq Q.$ Тогда мы имеем:

$$x_r = m^2 - x_p - x_q$$

$$y_r = y_p + m(x_r - x_p)$$

где $m = (y_p - y_q)/(x_p - x_q)$.

Явные формулы для P+Q

Пусть $P=(x_p,y_p),\,Q=(x_q,y_q),\,R=(x_r,y_r)$, где R=P+Q и $P\neq Q$. Тогда мы имеем:

$$x_r = m^2 - x_p - x_q$$

$$y_r = y_p + m(x_r - x_p)$$

где $m = (y_p - y_q)/(x_p - x_q)$.

Таким образом зная хотя бы одну точку $P \notin \mathrm{Tor}\,(E(\mathbb{Q}))$, можно явно найти бесконечно точек вида $P, 2P, \ldots, nP$.

Наглядное умножение на скаляр в исходной задаче Sum of points Sum of points 40000 30000 30000 20000 20000 10000 10000 -10000 -10000 -20000 -20000 -30000 -1000 -250 -1000 -250 750

Наглядное умножение на скаляр в исходной задаче Sum of points Sum of points 40000 40000 30000 30000 20000 20000 10000 10000 -10000 -10000 -20000 -20000 -30000 -250 -250

24 / 28

Теперь у нас все готово для решения первоначальной задачи. Дадим краткое описания алгоритма, который был реализован.

Теперь у нас все готово для решения первоначальной задачи. Дадим краткое описания алгоритма, который был реализован.

Алгоритм. Шаг 1.

Программа приводит кубику

$$x^3 + y^3 + z^3 + (1 - N)(x^2y + y^2x + x^2z + z^2x + y^2z + z^2y) + (3 - 2N)xyz = 0 \qquad (*).$$

к нормальной форме Вейерштрасса. То есть находит коэффициенты а, b и прямое и обратное преобразование.

Теперь у нас все готово для решения первоначальной задачи. Дадим краткое описания алгоритма, который был реализован.

Алгоритм. Шаг 1.

Программа приводит кубику

$$x^3 + y^3 + z^3 + (1 - N)(x^2y + y^2x + x^2z + z^2x + y^2z + z^2y) + (3 - 2N)xyz = 0 \qquad (*).$$

к нормальной форме Вейерштрасса. То есть находит коэффициенты a, b и прямое и обратное преобразование.

Замечание

Хоть для кубик вида (*) известны явные формулы для коэффициентов a, b, а так же для преобразования в терминах N, программа проделывает это вычисления отдельно. Это позволяет применить этот алгоритм почти для произвольной кубики.

Алгоритм. Шаг 2.

На кубике находится произвольная рациональная точка $P \notin \mathrm{Tor}\,(E(\mathbb{Q})).$ Это выполняется простым перебором числа $x = \frac{p}{q}$ где p,q ищутся в определённых пределах.

Алгоритм. Шаг 2.

На кубике находится произвольная рациональная точка $P \notin \mathrm{Tor}\,(E(\mathbb{Q}))$. Это выполняется простым перебором числа $x = \frac{p}{q}$ где p,q ищутся в определённых пределах.

Алгоритм. Шаг 3.

Далее найденная точка умножается на себя n раз. Именно поэтому важно, чтобы исходная точка не являлась точкой кручения.

Алгоритм. Шаг 2.

На кубике находится произвольная рациональная точка $P \notin \mathrm{Tor}\,(E(\mathbb{Q}))$. Это выполняется простым перебором числа $x = \frac{p}{q}$ где p,q ищутся в определённых пределах.

Алгоритм. Шаг 3.

Далее найденная точка умножается на себя n раз. Именно поэтому важно, чтобы исходная точка не являлась точкой кручения.

Алгоритм. Шаг 4.

Находятся координаты точек в изначальной системе. Отбираются точки у которых все координаты одного знака.

Алгоритм. Итог

В случае исходной задачи

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4, \quad x, y, z \in \mathbb{N}.$$

При удачном выборе P, точка 9P будет соответствовать решению уравнения.

В котором будет порядка 80 цифр.

Спасибо за внимание

Спасибо за внимание

Исходный код можно посмотреть тут:

https://github.com/andreykaere/MathPrac