Необычная задача кубического представления

Вступление

Данная статья посвящена поиску решения следующего уравнения

$$\frac{a}{b+c}+\frac{b}{a+c}+\frac{c}{a+b}=N, \qquad N,a,b,c\in\mathbb{N}$$

С первого взгляда может показаться, что найти хоть какое-то решение для малых N, скажем для $N=4$, не составит труда. Однако это не так, ведь самое короткое решение содержит порядка 80 цифр. Понятно, что прямым перебором такое решение за разумное время получить нельзя, так как компьютеры способны выполнять только порядка 10^{10} операций в секунду. Поэтому будут применены другие методы. Для начала поймём, что решение исходного уравнения равносильно нахождению натуральных точек на следующей кубике:

$$a^3+b^3+c^3+(1-N)(a^2b+b^2a+a^2c+c^2a+b^2c+c^2b)+(3-2N)abc=0.$$

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

Случай квадрики

Прежде чем переходить к описанию и нахождения рациональных точек на кубике, решим данную задачу для квадрик:

$$ax^2+by^2+cz^2+dxy+eyz+fxz=0, \qquad a,b,c,d,e,f\in\mathbb{Z}. \tag{1}$$

Понятно, что имея одну рациональную точку, методом секущих можно получить все. Отдельно можно задаться вопросом их явного описания, однако мы это рассматривать не будем. Для начала упростим задачу – приведём квадрику методом Лагранжа к одному из следующих видов:

$$\begin{aligned} Ax^2&=0\\ Ax^2-By^2&=0\\ Ax^2+By^2-Cz^2&=0 \end{aligned}$$

Итак, нас интересуют только целочисленные решения этих уравнений. Случаи 1 и 2 рассматриваются просто (упражнение). Случай 3 требует применения критерия Лежандра. Но для начала стоит понять, что числа A,B,C можно считать свободными от квадратов и более того попарно взаимно простыми. Тогда применим критерий Лежандра, согласно нему уравнение имеет целочисленное решение тогда и только тогда когда BC квадратичный вычет по модулю A, AC - по модулю B и $-AB$ по модулю C. Эти условия просто проверить. Однако, следует заметить, что просто знания того, что решение существует может быть недостаточно (как например в случае основной задачи), чтобы его можно было найти перебором за разумное время. Однако, на помощь приходит критерий Хольцера, который утверждает, что если решение существует, то оно найдётся в следующих пределах:

$$x_0^2\leqslant BC, \quad y_0^2\leqslant AC, \quad z_0^2\leqslant AB.$$

Теперь дадим краткое описание программы. Программа получает на вход кубику в форме (1), заданной матрицей 3×3. После, действует согласно алгоритму описанному выше: то есть приводит квадрику к упрощённой форме, применяет критерий Лежандра, и осуществляет поиск решения в заданных пределах. В итоге получает рациональную точку лежащую на квадрике, если она существует. Таким образом случай квадрики полностью разобран.

Приведение кубики к нормальной форме Вейерштрасса

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

$$a^3 + b^3 + c^3 + (1-N)(a^2b + b^2a + a^2c + c^2a + b^2c + c^2b) + (3-2N)abc = 0 \qquad (*)$$

к наиболее простому виду – форме Вейерштрасса, которая в однородных координатах $(x : y : z)$ может быть записана так:

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

Для кубики вида $(*)$ будет найдена явно её нормальная форма, и соответствующее преобразование, однако мы начнём с описания алгоритма приведения неособой кубики с целыми (рациональными) коэффициентами к форме Вейерштрасса. (а на самом деле любой с неособой рациональной точкой перегиба)

Для кубики

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

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

- Шаг 0. Нахождение рациональных точек перегиба.

  Для того, чтобы сделать первый шаг в алгоритме приведения неособой кубики к нормальной форме Вейерштрасса целочисленным проективным преобразованием нам сначала понадобиться найти рациональную точку перегиба. Для этого, мы рассмотрим Гессиан нашей кубики $H(F) := \det\left(\frac{\partial^2 F}{\partial x^i \partial x^j}\right)_{ij}$, где $x = x^1, y = x^2, z = x^3$. Далее, под проективными преобразованиями мы будем понимать только целочисленные проективные преобразования.

  Теорема 1. Точки перегиба неособой кубики в $\mathbb{CP}^2$ – в точности точки пересечения кубики с её Гессианом.

  Доказательство можно посмотреть в [2].

  Итак, для нахождения рациональных точек перегиба, нам достаточно найти все общие рациональные корни F и $H(F)$. Для этого, мы рассмотрим F и $H(F)$ как многочлены от z:

$$\begin{aligned} F &= b_0(x,y)z^3 + b_1(x,y)z^2 + b_2(x,y)z + b_3(x,y) \\ H(F) &= c_0(x,y)z^3 + c_1(x,y)z^2 + c_2(x,y)z + c_3(x,y), \end{aligned}$$

  где $b_k(x, y)$ и $c_k(x, y)$ – однородные многочлены от x, y степени k.

  Рассмотрим $R(F, H(F))$ – результант F и $H(F)$ по переменной z (При фиксированных x, y – это обычный результант двух многочленов). Непосредственной проверкой проверяется, что $R(F, H(F))$ – либо однородный многочлен от x, y степени не выше, чем 9, либо тождественный ноль. Перебирая все рациональные корни этого многочлена – получаем все потенциальные рациональные точки перегиба. Подставляя их в исходное уравнение F, смотрим, есть ли точка с такими рациональными координатами по x, y с рациональной координатой и по z. Таким образом, мы находим все рациональные точки перегиба на нашей кубике.

  В программе используется немного модифицированный алгоритм. А именно, вместо того, чтобы проверять, является кубика особой, мы сначала находим все потенциальные точки перегиба – это точки пересечения с Гессианом. Это реализовано в файле InflectionPoints.py в функции find_inflection_points с помощью вспомогательных функций get_hessian (которая по кубике выдаёт её Гессиан) и intersection_points (которая выдаёт точки пересечения двух произвольных кубик). Далее в функции find_non_singular_inflection_point мы отбираем только неособые точки перегиба.

- Шаг 1. 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 $\widetilde{y}$.

  Этот шаг реализован в файле WeierstrassForm.py в функции weierstrass_form_step1.

- Шаг 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.

  Этот шаг реализован в файле WeierstrassForm.py в функции weierstrass_form_step2.

- Шаг 3. После второго преобразования, уравнение нашей кубики стало $F'(x',y',z')=0$, где

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

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

$$\left(y''\right)^2 z' = a''_{30}\left(x'\right)^3 + a''_{20}\left(x'\right)^2 z' + a''_{10}x'\left(z'\right)^2 + a''_{00}\left(z'\right)^3.$$

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

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

  Теперь делаем замену $z'' = \dfrac{1}{a'''_{30}}z'$ и получаем:

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

  Полагая теперь $a := a'''_{30}a'''_{10}, b := a'''_{00}\left(a'''_{30}\right)^2$, получаем требуемую форму:

$$\left(y''\right)^2 z'' = \left(x''\right)^3 + a\,x''\left(z''\right)^2 + b\left(z''\right)^3.$$

  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.

  Этот шаг реализован в файле WeierstrassForm.py в функции weierstrass_form_step3.

Явное вычисление для кубики из нашей задачи

Приведём явные выкладки для кривой вида:

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

В этом случае рациональная точка $P = (1 : -1 : 0)$ является также точкой перегиба (проверяется непосредственно подстановкой в Гессиан).

- Шаг 1. Переведём точку $P = (1 : -1 : 0)$ в точку $(0 : 1 : 0)$ некоторым проективным преобразованием. Например, подойдёт такое:

$$\lambda \begin{pmatrix} \widetilde{x} \\ \widetilde{y} \\ \widetilde{z} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

или

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \widetilde{x} \\ \widetilde{y} \\ \widetilde{z} \end{pmatrix}.$$

Тогда наше уравнение преобразуется в следующее:

$$\begin{aligned}\widetilde{F}(\widetilde{x},\widetilde{y},\widetilde{z}) = (\widetilde{z})^3 - (N+2)\,(\widetilde{x})^2\,\widetilde{y} + (1-N)\,(\widetilde{x})^2\,\widetilde{z} + (N+2)\,\widetilde{x}\,(\widetilde{y})^2 \\ + (1-N)\,\widetilde{x}\,(\widetilde{z})^2 + (\widetilde{x})^3 + \widetilde{x}\,\widetilde{y}\,\widetilde{z} - (\widetilde{y})^2\,\widetilde{z}.\end{aligned}$$

- Шаг 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:

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

Пусть имеет место соотношение

$$\begin{pmatrix} \widetilde{x} \\ \widetilde{y} \\ \widetilde{z} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

Так как точка O должна быть неподвижна, то:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

откуда $c_{12} = 0, c_{22} = 1, c_{32} = 0$.

Кроме того, поскольку $F'(x', y', z') = \widetilde{F}(\widetilde{x}(x', y', z'), \widetilde{y}(x', y', z'), \widetilde{z}(x', y', z'))$, то мы имеем:

$$\begin{aligned}\frac{\partial F'}{\partial x'}(O) &= \frac{\partial \widetilde{F}}{\partial \widetilde{x}}(\widetilde{x}(O), \widetilde{y}(O), \widetilde{z}(O))\frac{\partial \widetilde{x}}{\partial x'}(O) + \frac{\partial \widetilde{F}}{\partial \widetilde{y}}(\widetilde{x}(O), \widetilde{y}(O), \widetilde{z}(O))\frac{\partial \widetilde{y}}{\partial x'}(O) \\ &\quad + \frac{\partial \widetilde{F}}{\partial \widetilde{z}}(\widetilde{x}(O), \widetilde{y}(O), \widetilde{z}(O))\frac{\partial \widetilde{z}}{\partial x'}(O) \\ &= \frac{\partial \widetilde{F}}{\partial \widetilde{x}}(c_{12}, c_{22}, c_{32})c_{11} + \frac{\partial \widetilde{F}}{\partial \widetilde{y}}(c_{12}, c_{22}, c_{32})c_{21} + \frac{\partial \widetilde{F}}{\partial \widetilde{z}}(c_{12}, c_{22}, c_{32})c_{31} \\ &= \frac{\partial \widetilde{F}}{\partial \widetilde{x}}(0,1,0)c_{11} + \frac{\partial \widetilde{F}}{\partial \widetilde{y}}(0,1,0)c_{21} + \frac{\partial \widetilde{F}}{\partial \widetilde{z}}(0,1,0)c_{31} = (2+N)c_{11} - c_{31}.\end{aligned}$$

Аналогично получаем:

$$\frac{\partial F'}{\partial y'}(O) = \left(\frac{\partial \widetilde{F}}{\partial \widetilde{x}}\frac{\partial \widetilde{x}}{\partial y'} + \frac{\partial \widetilde{F}}{\partial \widetilde{y}}\frac{\partial \widetilde{y}}{\partial y'} + \frac{\partial \widetilde{F}}{\partial \widetilde{z}}\frac{\partial \widetilde{z}}{\partial y'}\right)\Bigg|_O = (2+N)\frac{\partial \widetilde{x}}{\partial y'}(O) - \frac{\partial \widetilde{z}}{\partial y'}(O) = (2+N)c_{12} - c_{32}$$
$$\frac{\partial F'}{\partial z'}(O) = \left(\frac{\partial \widetilde{F}}{\partial \widetilde{x}}\frac{\partial \widetilde{x}}{\partial z'} + \frac{\partial \widetilde{F}}{\partial \widetilde{y}}\frac{\partial \widetilde{y}}{\partial z'} + \frac{\partial \widetilde{F}}{\partial \widetilde{z}}\frac{\partial \widetilde{z}}{\partial z'}\right)\Bigg|_O = (2+N)\frac{\partial \widetilde{x}}{\partial z'}(O) - \frac{\partial \widetilde{z}}{\partial z'}(O) = (2+N)c_{13} - c_{33}.$$

Итак, мы получаем следующие условия на матрицу $C = (c_{ij})$:

$$\begin{aligned}(2+N)c_{11} - c_{31} &= 0\\ (2+N)c_{12} - c_{32} &= 0\\ (2+N)c_{13} - c_{33} &\neq 0\\ c_{12} = c_{32} &= 0\\ c_{22} &= 1.\end{aligned}$$

Итого, получаем, что в качестве искомой матрицы можно взять следующую:

$$\begin{pmatrix} 1 & 0 & 1\\ 1 & 1 & 1\\ 2+N & 0 & N+1\end{pmatrix}.$$

А тогда наше преобразование будет иметь вид:

$$\lambda\begin{pmatrix} x'\\ y'\\ z'\end{pmatrix} = \begin{pmatrix} -N-1 & 0 & 1\\ -1 & 1 & 0\\ N+2 & 0 & -1\end{pmatrix}\begin{pmatrix} \widetilde{x}\\ \widetilde{y}\\ \widetilde{z}\end{pmatrix}.$$

- Шаг 3. После второго преобразования, наше уравнение приняло вид:

$$\begin{aligned}F'(x',y',z') = {} & \left(2N^2+11N+15\right)(x')^3 + \left(5N^2+24N+28\right)(x')^2 z'\\ & + \left(4N^2+17N+18\right)x'(z')^2 + \left(N^2+4N+4\right)(z')^3 + x'y'z' + (y')^2 z' + y'(z')^2.\end{aligned}$$

Поэтому условие $F'(x',y',z') = 0$ можно переписать как

$$\begin{aligned}-(y')^2 z' - x'y'z' - y'(z')^2 = {} & \left(2N^2+11N+15\right)(x')^3 + \left(5N^2+24N+28\right)(x')^2 z'\\ & + \left(4N^2+17N+18\right)x'(z')^2 + \left(N^2+4N+4\right)(z')^3.\end{aligned}$$

Выделяем полный квадрат по y':

$$\begin{aligned}-\left(y' + \frac{1}{2}(x'+z')\right)^2 z' + \frac{1}{2}(x'+z')^2 z' = {} & \left(2N^2+11N+15\right)(x')^3 + \left(5N^2+24N+28\right)(x')^2 z'\\ & + \left(4N^2+17N+18\right)x'(z')^2 + \left(N^2+4N+4\right)(z')^3.\end{aligned}$$

Переносим свободные члены от y' в правую часть:

$$\begin{aligned}-\left(y' + \frac{1}{2}(x'+z')\right)^2 z' = {} & \left(2N^2+11N+15\right)(x')^3 + \left(5N^2+24N+28-\frac{1}{4}\right)(x')^2 z'\\ & + \left(4N^2+17N+18-\frac{1}{2}\right)x'(z')^2 + \left(N^2+4N+4-\frac{1}{4}\right)(z')^3.\end{aligned}$$

Как известно, многочлен $ax^3 + bx^2 + cx + d$ линейной заменой $x \mapsto x - \frac{b}{3a}$ приводится к виду $px^3 + qx + s$. В нашем случае замена будет такой:

$$x'' = x' + \frac{5N^2 + 24N + 28 - \frac{1}{4}}{3(2N^2 + 11N + 15)} z'.$$

После подстановки получим:

$$-\left(y' + \frac{1}{2}(x' + z')\right)^2 z' = \left(2N^2 + 11N + 15\right)(x'')^3 + Ax''(z')^2 + B(z')^3,$$

где

$$A = -\frac{N^4}{3(N+3)(2N+5)} - \frac{2N^3}{(N+3)(2N+5)} - \frac{5N^2}{2(N+3)(2N+5)} + \frac{7N}{2(N+3)(2N+5)} + \frac{93}{16(N+3)(2N+5)}$$

$$B = -\frac{2N^6}{27(N+3)^2(2N+5)^2} - \frac{2N^5}{3(N+3)^2(2N+5)^2} - \frac{11N^4}{6(N+3)^2(2N+5)^2} - \frac{N^3}{3(N+3)^2(2N+5)^2} + \frac{43N^2}{8(N+3)^2(2N+5)^2} + \frac{41N}{8(N+3)^2(2N+5)^2} - \frac{47}{32(N+3)^2(2N+5)^2}.$$

Деля на $2N^2 + 11N + 15$, получаем

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

где

$$\begin{aligned} y'' &= y' + \frac{1}{2}(x' + z') \\ z'' &= \frac{z'}{2N^2 + 11N + 15} \\ a &= A\left(2N^2 + 11N + 15\right) \\ b &= B\left(2N^2 + 11N + 15\right)^2. \end{aligned}$$

Заметим, что все N-ки в знаменателях сократятся и в итоге у нас получится:

$$\begin{aligned} -(y'')^2 z' = (x'')^3 &+ \frac{1}{48}\left(-16N^4 - 96N^3 - 120N^2 + 168N + 279\right)x''(z'')^2 \\ &+ \frac{1}{864}\left(-64N^6 - 576N^5 - 1584N^4 - 288N^3 + 4644N^2 + 4428N - 1269\right)(z'')^3. \end{aligned}$$

Окончательно, делая замены $x''' = \frac{1}{6}x''$, $z''' = -\frac{1}{6^3}z''$, получаем:

$$\begin{aligned} (y'')^2 z''' = (x''')^3 &+ \left(-432N^4 - 2592N^3 - 3240N^2 + 4536N + 7533\right)x'''(z''')^2 \\ &+ \left(3456N^6 + 31104N^5 + 85536N^4 + 15552N^3 - 250776N^2 - 239112N + 68526\right)(z''')^3. \end{aligned}$$

Преобразования в шаге 3:

$$\lambda \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & \frac{20N^2+96N+111}{180+132N+24N^2} \\ \frac{1}{2} & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2N^2+11N+15} \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

И

$$\lambda \begin{pmatrix} x''' \\ y''' \\ z''' \end{pmatrix} = \begin{pmatrix} \frac{1}{6} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{216} \end{pmatrix} \begin{pmatrix} x'' \\ y'' \\ z'' \end{pmatrix}.$$

Итого, собирая все преобразования вместе, получаем искомое проективное преобразование:

$$\lambda \begin{pmatrix} x''' \\ y''' \\ z''' \end{pmatrix} = \begin{pmatrix} \frac{1}{6} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{216} \end{pmatrix} \begin{pmatrix} 1 & 0 & \frac{20N^2+96N+111}{180+132N+24N^2} \\ \frac{1}{2} & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2N^2+11N+15} \end{pmatrix} \begin{pmatrix} -N-1 & 0 & 1 \\ -1 & 1 & 0 \\ N+2 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

То есть искомая матрица есть

$$\begin{pmatrix} \frac{-4N^3-20N^2-9N+42}{72(N+3)(2N+5)} & \frac{-4N^3-20N^2-9N+42}{72(N+3)(2N+5)} & \frac{4N^2+36N+69}{72(N+3)(2N+5)} \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{-N-2}{216(N+3)(2N+5)} & \frac{-N-2}{216(N+3)(2N+5)} & \frac{1}{216(N+3)(2N+5)} \end{pmatrix}.$$

Так как матрица проективного преобразования определена с точностью до умножения на скаляр, то умножая всю матрицу на $216(3+N)(5+2N)$, имеем:

$$\begin{pmatrix} -12N^3-60N^2-27N+126 & -12N^3-60N^2-27N+126 & 12N^2+108N+207 \\ 216N^2+1188N+1620 & -216N^2-1188N-1620 & 0 \\ -N-2 & -N-2 & 1 \end{pmatrix}.$$

Подытожим: исходная кубика, заданная уравнением

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

приводится к кубике, заданной уравнением

$$\begin{aligned} (y'')^2 z''' = (x''')^3 &+ \left(-432N^4-2592N^3-3240N^2+4536N+7533\right) x''' (z''')^2 \\ &+ \left(3456N^6+31104N^5+85536N^4+15552N^3-250776N^2-239112N+68526\right) (z''')^3 = 0 \end{aligned}$$

проективным преобразованием с матрицей:

$$\begin{pmatrix} -12N^3-60N^2-27N+126 & -12N^3-60N^2-27N+126 & 12N^2+108N+207 \\ 216N^2+1188N+1620 & -216N^2-1188N-1620 & 0 \\ -N-2 & -N-2 & 1 \end{pmatrix}.$$

Поиск рациональных точек

Итак, нам дана кубика в форме Вейерштрасса, наша задача понять, как устроены рациональные точки на ней. Для этого удобно ввести дополнительную структуру на множестве рациональных точек. Определим сложение точек. Суммой P и Q назовём третью точку пересечения прямой проходящей через P и Q с кубикой. Понятно, что если исходные точки был рациональны, то $P + Q$, тоже будет рациональной. Оказывается, что множество рациональных точек, на кубике в форме Вейерштрасса образуют абелеву группу, для данной операции сложения. Более того, даже для произвольной кубики что-то можно сказать про устройство этой группы. Имеет место следующая теорема:

Теорема 2. На эллиптической кривой E, заданной уравнением с рациональными коэффициентами, группа $E(\mathbb{Q})$ рациональных точек является конечно порождённой абелевой группой.

В нашем случае известно (см. например [1]) устройство этой группы: $\mathbb{Z}\oplus\mathbb{Z}_6$. Это позволяет нам конструктивно описать много рациональных точек, ибо есть явные формулы для сложения точек на кубике в форме Вейерштрасса, приведём их. Пусть $P = (x_p, y_p), Q = (x_q, y_q), R = (x_r, y_r)$, где $R = P + Q$. Тогда мы имеем:

$$\begin{aligned} x_r &= m^2 - x_p - x_q \\ y_r &= y_p + m(x_r - x_p) \end{aligned} \qquad (*),$$

где $m = (y_p - y_q)/(xp - xq)$.

Замечание 1. Эти формулы справедливы для различных P и Q, однако несложно получить и для случая $P = Q$.

Замечание 2. Эти формулы работают только в аффинной карте $z = 1$, однако это не ограничивает общность, т.к. единственная точка кубики вне этой карты это $(0 : 1 : 0)$, которая является единичным элементом в группе рациональных точек.

Теперь мы можем описать алгоритм. Программа получает на вход произвольную $(*)$ кубику и приводит её к форме Вейерштрасса, и заодно находит прямое и обратное преобразование. После этого на кривой ищется произвольная рациональная точка, которая не является точкой кручения, то есть рациональная P, такая что, среди $P, 2P, 3P, 4P, 5P, 6P$ нет единичного элемента. Функция FindRational получает коэффициенты a, b и радиус в котором следует искать рациональную точку, а выдаёт её координаты. Точки вида nP находятся в функции ScMult, которая складывает точку P с собой n раз с помощью PoinSum - функции складывающей произвольные две точки на кубике с помощью формул $(*)$ (в аффинной карте $z = 1$).

Замечание. Поиск рациональной точкой перебором является самой вычислительное сложной частью алгоритма, например, для некоторых коэффициентов a, b кубики в форме $y^2 = x^3 + ax + b$ рациональная точка не находится за разумное время, хоть и известно, что она существует

После этого программа находит точки $P, 2P, ..., nP$, с помощью функции GenerateNpoints. Затем находит координаты каждой из них в начальной системе координат посредством Reverse. Чтобы точка соответствовала натуральному решению исходного уравнения, все координаты должны быть одного знака. После чего домножая их на общий знаменатель получаем решение исходной задачи. Это выполняется в функции RevNFind. Таким образом, вызывая данную функцию от коэффициентов кубики, найденной рациональной точки и количества точек, которое мы хотим перебрать – n, получаем натуральные решения исходного уравнения. Например, в случае $N = 4$, достаточно взять $n = 9$, т.е. точка $9P$ будет соответствовать натуральному решению.

Заметим только, что размер полученного решения зависит от выбора точки P, неудачный выбор может привести к тому, что количество цифр в ответе станет 400, вместо 80.

Список литературы

[1] Macleod A. Bremner A. «An unusual cubic representation problem». В: *Annales Mathematicae et Informaticae* (2014).

[2] Ю.П. Соловьёв В.В. Прасолов. *Эллиптические функции и алгебраические уравнения.* Факториал, 1997.