

## Приведение кубики к нормальной форме Вейерштрасса

Для нашей 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  $x^i y^j z^{3-i-j}$ .

- 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 понадобится найти рациональную точку перегиба. Для этого, мы рассмотрим гессиан нашей кубики  $H(F) := \det \left( \frac{\partial F}{\partial x^i \partial x^j} \right)_{ij}$ , 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 ( .. ) .

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  $k$ .

Если  $c_0(x, y) \cdot b_0(x, y) = 0$ , то есть если  $F$  или  $H(F)$  проходит через точку  $(0 : 0 : 1)$ , то мы можем сделать проективное преобразование так, что ни одна из кубик не будет через неё проходить. Сделать это можно, например, так: найти точку, которая не лежит ни на одной из наших кубик и «обменять» её с  $(0 : 0 : 1)$ . Итак, будем искать точку в виде  $(0 : i : 1)$ ,  $i = 1, 2, \dots$ . Так как кубика неособая, то она не распадается (то есть не содержит прямой) и различные кубики могут пересекаться не более, чем в 9 точках, то процесс перебора закончится не позднее, чем через 10 шагов. (Условие  $c_0 b_0 \neq 0$  нужно, чтобы ... ?)

Далее считаем, что  $c_0(x, y) \cdot b_0(x, y) \neq 0$ . Рассмотрим  $R(F, H(F))$  – результат  $F$  и  $H(F)$  по переменной  $z$  (При фиксированных  $x, y$  – это обычный результат двух многочленов). Непосредственной проверкой проверяется, что  $R(F, H(F))$  – либо однородный многочлен от  $x, y$  степени 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.

- Шаг 1. Выберем какую-то рациональную точку перегиба  $P$ . Переведём точку  $P$  в точку  $(0 : 1 : 0)$  некоторым проективным преобразованием. Например, подойдёт такое: ...

После проективного преобразования, наша кубика имеет уравнение  $\tilde{F}(\tilde{x}, \tilde{y}, \tilde{z})$ , в котором нет  $\tilde{y}$ .

- Шаг 2. Теперь мы хотим сделать преобразование, сохраняющее точку  $O = (0 : 1 : 0)$ , так, чтобы прямая  $z = 0$  была касательной к кубике  $\tilde{F}$  в точке  $O$ , то есть сделать преобразование  $(\tilde{x} : \tilde{y} : \tilde{z}) \rightarrow (x' : y' : z')$ , 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

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

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  $F'(x', y', z') = \tilde{F}(\tilde{x}(x', y', z'), \tilde{y}(x', y', z'), \tilde{z}(x', y', z'))$ , то мы имеем:

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

Аналогично получаем:

$$\begin{aligned} \frac{\partial F'}{\partial y'}(O) &= \left( \frac{\partial \tilde{F}}{\partial \tilde{x}} \frac{\partial \tilde{x}}{\partial y'} + \frac{\partial \tilde{F}}{\partial \tilde{y}} \frac{\partial \tilde{y}}{\partial y'} + \frac{\partial \tilde{F}}{\partial \tilde{z}} \frac{\partial \tilde{z}}{\partial y'} \right) \Big|_O = (2 + N) \frac{\partial \tilde{x}}{\partial y'}(O) - \frac{\partial \tilde{z}}{\partial y'}(O) = (2 + N)c_{12} - c_{32} \\ \frac{\partial F'}{\partial z'}(O) &= \left( \frac{\partial \tilde{F}}{\partial \tilde{x}} \frac{\partial \tilde{x}}{\partial z'} + \frac{\partial \tilde{F}}{\partial \tilde{y}} \frac{\partial \tilde{y}}{\partial z'} + \frac{\partial \tilde{F}}{\partial \tilde{z}} \frac{\partial \tilde{z}}{\partial z'} \right) \Big|_O = (2 + N) \frac{\partial \tilde{x}}{\partial z'}(O) - \frac{\partial \tilde{z}}{\partial z'}(O) = (2 + N)c_{13} - c_{33}. \end{aligned}$$

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:

$$F'(x', y', z') = (2N^2 + 11N + 15) (x')^3 + (5N^2 + 24N + 28) (x')^2 z' + (4N^2 + 17N + 18) x' (z')^2 + (N^2 + 4N + 4) (z')^3 + x' y' z' + (y')^2 z' + y' (z')^2.$$

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

$$-(y')^2 z' - x' y' z' - y' (z')^2 = (2N^2 + 11N + 15) (x')^3 + (5N^2 + 24N + 28) (x')^2 z' + (4N^2 + 17N + 18) x' (z')^2 + (N^2 + 4N + 4) (z')^3.$$

Выделяем полный квадрат по  $y'$ :

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

Переносим свободные члены от  $y'$  в правую часть:

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

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:

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

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

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

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

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

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

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

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

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

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

$$(y'')^2 z''' = (x''')^3 + (-432N^4 - 2592N^3 - 3240N^2 + 4536N + 7533) x''' (z''')^2 + (3456N^6 + 31104N^5 + 85536N^4 + 15552N^3 - 250776N^2 - 239112N + 68526) (z''')^3$$

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 были 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 (2) 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:

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

где  $m = (y_p - y_q)/(x_p - x_q)$ .

**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  $(0 : 1 : 0)$  является единичным элементом в группе рациональных точек. (м.б. сюда картинку).

Теперь мы можем описать алгоритм. Программа получает на вход произвольную  $(*)$  кубик 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 3.** 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 (а есть ли вообще хороший алгоритм её поиска?).

После этого программа находит точки  $P, 2P, \dots, nP$ , 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.

Последний вопрос, который мы рассмотрим - это нижняя оценка количества цифр в ответе **to be continued**