Лекция 3. Кривые рода один, закон сложения на эллиптических кривых, теорема Морделла-Вейля, гипотеза Морделла.

0.5 Эллиптические кривые

Рассмотрим для примера кривые, для которых принцип Хассе не работает

Пример:

1. Рассмотрим кривую над Q, заданную уравнением

$$x^3 + 2y^3 + 7z^3 = 0$$

Можно увидеть, что нет точек по модулю 7, а значит нет и никаких рациональных точек вовсе.

2. Пусть у нас есть кривая

$$y^2 = 8x^4 - 1$$

Можно показать, что эта кривая имеет точки по модулю всех простых. Однако нет решений по модулю 8.

Вместо изучения решений по модулю всех степений простых проще спрашивать про наличие решений над Q_p. Эти вопросы, конечно, эквивалентны, но с Q_p работать проще, так как это поле, в то время как Z/p^kZ кольцо с делителями нуля.

3. Пусть есть кривая $-y^2 = x^4 + x + 1$, многочлен в правой части не имеет вещественных корней, значит, он всегда положителен. Поэтому нет вещественных, а следовательно и рациональных решений.

Т.е. принцип Хассе не всегда применим, но мы можем иследовать наличие точек над Q_p для доказательства отсутствия рациональных точек.

Определение эллиптической кривой и форма Вейерштрассе.

Определение 0.24 *Эллиптическая кривая над полем k это неособая проективная алгебраическая кривая E рода один с заданной базовой точкой $\mathcal{O}$ на кривой.*

Пример:

1. Кривая в $P^2(Q)$, определённая однородной кубикой Y

$$Y^2Z = X^3 + XZ^2$$

это неособая кривая рода один, если взять точку $O = (0 : 1 : 0)$, то это эллиптическая кривая.

2. Кубика $3X^3 + 4Y^3 + 5Z^3$ является неособой проективной кривой рода один над Q, но это не эллиптическая кривая, так как она не содержит ни одной рациональной точки (у неё есть точки над R и над Q_p

Этот пример изучил Зелмер, доказательство наличия точек над Q_p оставим в качестве задачи (листок 3).

Очевидно, что эллиптические кривые это не эллипсы (те имеют род ноль). Но связь в названии следующая если считать циркуляцию вдоль эллипса, то получается следующие значение (при эксцентрисите e):

$$4a\int_0^1 \sqrt{\frac{1-a^2t^2}{1-t^2}}dt$$

Этот интеграл называется эллиптическим (второго типа), интегранд удовлетворяет уравнению $u^2(1?t^2) = 1?e^2t^2$, которое задаёт эллиптическую кривую. Собственно теория эллиптических кривых возниклаиз изучения решений для интегралов, схожих с приведённым выше.

Рассмотрим специальный класс эллиптических кривых, заданных конкретным уравнением. Заметим также, что любая кривая рода один вкладывается в P^2 как кубика.

Определение 0.25 *Обобщённое уравнение Вейерштрассе это уравнение вида*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

где $a_i \in C$

Во-первых, заметим, что такое уравнение задаёт кривую с одной точкой на бесконечности, $O = (0 : 1 : 0)$. Это очевидно рациональная точка, и кривая в ней неособа (она может быть особо в других точках). Обратно, любая кубика с такими условиями задаётся уравнением Вейерштрассе. Более того, заменой координат уравнение Вейерштрассе можно привести к короткому виду.

Определим для уравнения Вейерштрассе выше следующие величины: $b_2 = a_1^2 + 4a_2, b_4 = 2_4 + a_1a_3, b_6 = a_3^2 + 4a_6$

Предложение 0.26 *Уравнение Вейерштрассе задаёт неособую эллиптическую кривую титтк* $b_6 \neq 0$.

*Доказательство:*Мы уже знаем, что в точке на бесконечности наша кривая неособа. Так что можно работать с соотвествующей аффинной кривой. Замена переменой $y' = \frac{1}{2}(y - a_1x - a3)$ сводит наше исходное уравнение к виду

$$y_2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

где b_i определены выше. Эта кривая очевидно неособа, если у кубики справа нет кратных корней. □

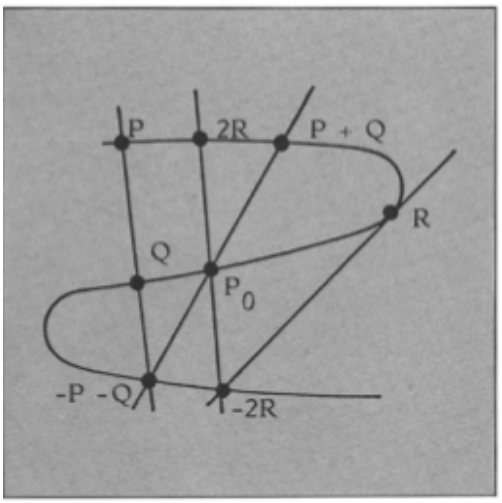
Более того, заменой $x' = x + b_2/2$ можно привести к виду $y^2 = x^3 + ax + b$.

Понятно, что рассмотрение уравнения Вейерштрассе обосновано естественными причинами, а именно следующим предложением.

Предложение 0.27 *Любая эллиптическая кривая E изоморфна кривой в P^2, заданной общем уравнением Вейерштрассе с базовой точкой $\mathcal{O}$ в (0 : 1 : 0). Обратно, любая неособое обобщённое уравнение Вейерштрассе определяет эллиптическую кривую вместе с базовой точкой.*

Также вспомним, что одну эллиптическую кривую мы уже рассматривали, а именно, кривую Морделла.

0.6 Сложение точек на эллиптической кривой



Рассматривая проективную плоскость как объединие аффиной плоскости и P^1, наша проективная кривая состоит из аффиной кривой и точек на бесконечности. Рассмотрим в уравнении Вейерштрассе случай $Z = 0$, чтобы понять, какие могут быть бесконечно удалённые точки. Получаем $X^3 = 0$, т.е. (0,1,0) единственная точка на бесконечности. При изоморфизме $P^2 \simeq A^2 \cup P^1$ эта точка соответствует точке, где все вертикальные прямые (в плоскости xy) пересекаются. С этого момента мы рассматриваю аффинную кривую плюс точку пересечения вертикальных прямых.

Во-первых, заметим, что любая прямая пересекает нашу кубику трижды, если считать $\mathcal{O}$ и кратности точек касания (2 и 3). Это частный случай теоремы Безу, которая утверждает, что число точек пересечения кривых степени m и n равно mn (с кратностями).

Если мы проведём линию через две рациональные точки P и Q, тогда, во-первых, третья точка $P * Q$ пересечения будет рациональной, а во-вторых в качестве суммы возьмём пересечение прямой, проходящей через $P * Q$ и через $\mathcal{O}$ и нашей кубики. Заметим, что так как мы договорились рассматривать кривую в форме уравнения Вейерштрассе, то чтобы построить $P + Q$ по $P * Q$ (которую мы в дальнейшем будем обозначать $-P - Q$) надо провести вертикальную прямую и взять точку её пересечения с кубикой. Легко видеть, что

если (x, y) лежит на кубике, заданной уравнений Вейерштрассе, то и $(x, -y)$ тоже. Значит, $P + Q$ просто симметрична $P * Q$ относительно оси x. Возможен случай, что $P = Q$, тогда можно взять касательную к кривой в точке P (тк кривая неособая, то это корректно). Тогда третья точка пересечения касательной с кривой это $P * P = -2P$, как и раньше за сумму возьмём отражение $-2P$ относительно оси x.

Мы утверждаем, что это коммутативная бинарная операция и множество $E(Q)$ с этой операцией является группой. Оставим проверку ассоциативности слушателю.

При этом ключевым в доказательстве ассоциативности является следующий факт.

Теорема 0.28 *Пусть есть две кубические кривые C_1, C_2. Пусть есть кривая C, проходящая через восемь из девяти точек пересечения. Тогда она проходит и через девятую.*

Для того чтобы завершить доказательство того, что $(E(Q), +)$ группа нам нужно показать существование единицы и обратного. Единицей является базовая точка $\mathcal{O}$, действительно, линия через P и $\mathcal{O}$ это вертикальная прямая через P, значит по определению $P + \mathcal{O} = P$ для всех P. А обратный это $P * \mathcal{O}$.

Сложение точек можно задать явно, если $P = (x_1, y_1), Q = (x_2, y_2)$. Уравнение кривой будем использовать в короткой форме Вейерштрассе $y^2 = x^3 + ax + b$ Найдём $P + Q = (x_3, y_3)$. Пусть $y = \lambda x + \nu = \lambda(x - x_1) + y_1$ прямая через P, Q. Можно записать условие, что все три точки лежат в виде

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3)$$

Раскрыв и приравняв коэффициенты при x^2, получим, что

$$x_3 = \lambda^2 - x_1 - x_2$$

и

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

где $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

Если точки совпадают, то $\lambda = \frac{3x_1^2 + b}{2y_1}$.

Пример:

$$E : y^2 + y = x^3 ? x$$

$P = (0, 0), Q = (-1, -1)$, ищем $P + Q$. Линия через $P, Q \quad y = x$. Она пересекает кривую ещё в точке $R = (2, 2)$. Нам нужна точка, которая лежит в пересечении прямой $x = 2$ и нашей кубики. Эта точку легко найти $y^2 + y = 6$, следовательно, эта точка имеет координаты (2,-3).

Точки кручения

Точки кручения — это точки конечного порядка, т.е. такие P, что $mP = \mathcal{O}$

Рассмотрим точки 2-кручения, те $P = -P$, т.е. $(x, y) = (x, -y)$. Значит $y = 0$. Если x_1, x_2, x_3 — корни $f(x) = x^3 + ax^2 + bx + c$, то $E[2] = \mathcal{O}, (0, x_1), (0, x_2), (0, x_3)$. Так как у всех этих точек порядок два, то легко видеть, что $E[2] = Z/2Z \times Z/2Z$.

В общем случае, имеем $E[m] = Z/mZ \times Z/mZ$. Это факт не так очевиден и следует из того, что комплексные точки $E(C) = C/\Lambda$, где Λ решётка.

Оказывается, что группа $E(Q)$ конечно порождена, для доказательства этого факта нам достаточно строения $E[2]$.

Мы с особым интересом смотрим на ту часть $E(Q)$, которая состоит из точек кручения — $E(Q)_{tors}$. Про эту подгруппу есть следующий забавный факт, который мы оставим без доказательства.

Теорема 0.29 *(Nagell-Lutz) Пусть $E : y^2 = x^3 + ax^2 + bx + c$, где $a, b, c \in Z$. Если $(x, y) \in E(Q)_{tors}$, то $x, y \in Z$.*

0.7 Рациональные точки на кривых рода один, строение $E(Q)$

Теорема Морделла-Вейля

Теорема 0.30 *(The Mordell-Weil Theorem). $E(Q)$ конечно-порождённая абелева группа.*