$$|\frac{x}{y} - \beta| \leq \frac{4c}{3\beta^2}|\frac{1}{y^3}|$$

Нам достаточно доказать, что число пар (x, y), удовлетворяющих неравенству выше конечно. Это следует из диофантовой аппроксимации. Мы вернёмся к нему позже.

Теорема Фуета

Теорема 0.13 *Рассмотрим уравнение Морделла $y^2 = x^3 + k$, если k не имеет шестых степеней в разложении на простые, не равно 1 или -432, а уравнение имеет рациональное решение (r, s), такое что $rs \neq 0$, то имеется бесконечно много рациональных решений.*

Идея как можно действовать:
Рассмотрим пару

$$x = r + z, \quad y = s + 3r^2 z/2s$$

Предположим, что (x, y) решение, тогда $z = 9r^4/4s^2 - 3r$.

Если $x = 0$, то получаем, что $k = t^6$, чего быть не может. Рассматривая редукцию по модулю 2^n также получаем, что $y \neq 0$. И так далее, если $k \neq 1$ или -432.

Лекция 2. Кривые, род кривых, рациональные точки на кривых рода ноль: принцип Хассе.

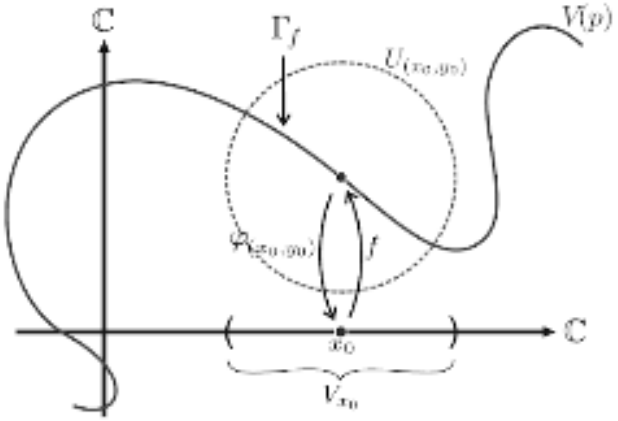
0.3 Понятие кривых

Кривые

Определение 0.14 *Для любого* $f(x,y) \in C[x,y]$ *множество* $V(f) := (x,y)|f(x,y) = 0 \subset C^2$ *называется афинной плоской кривой. Мы говорим, что кривая гладкая, если нет таких пар* (x_0, y_0), *что* $\frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial f}{\partial y}(x_0,y_0) = 0$.

Напомним, что комплексно-аналитическое многообразие размерности один называется римановой поверхностью.

Рассмотрение гладких кривых удобно в том смысле, что можно локально рассматривать кривую как график. Действительно, если хотя бы одна из частных производных не зануляется, то можно использовать теорему о неявной функции и тогда существует окрестности в образе и прообразе, такие что пересечение первой с образом второй в точности график.



Это даёт локальную карту на $V(f)$ в окрестности точки (x_0, y_0), при этом соответствующее отображение (проекция на первый фактор) в V_{x_0} голоморфно (рисунок выше). Таким аргументом можно показать, что комплексная гладкая кривая это риманова поверхность.

Классификация римановых поверхностей хорошо известна это сферы с ручками. Число ручек называется родом поверхности. На таких поверхностях есть важное, так называемое, каноническое линейное расслоение K_S, слоями которого в данной точке является пространство комплексных линейных отображений из касательного пространства в C. Сечение этого расслоения называется дифференциалом на S.

Заметим, что обычные многочлены "плохо" определены на проективной плоскости. Действительно, рассмотрим многочлен

$$p(x, y, z) = x^2 + y + z + 1$$

Легко видеть, что $p(1, 1, 1) \neq p(2, 2, 2)$ хотя это одна и та же точка в проективной плоскости. Поэтому для корректного определения нам надо рассматривать многочлены, имеющие одинаковые значения вдоль прямых, такие многочлены называются однородными.

Определение 0.15 *Многочлен P называется однородным, если все мономы имеют степень d.*

Замечание: Очевидно, что в этом случае выполнено следующее

$$P(tx, ty, tz) = t^d P(x, y, z)$$

и

$$x\frac{\partial P}{\partial x} + y\frac{\partial P}{\partial y} + z\frac{\partial P}{\partial z} = dP,$$

последнее называется тождеством Эйлера.

Определение 0.16 *Для любого однородного многочлена $f(x, y, z) \in C[x, y, z]$ множество $V(f) := (x : y : z)|f(x, y, z) = 0 \subset P^2(C)$ называется проективной плоской кривой. Мы говорим, что кривая гладкая, если нет таких троек (x_0, y_0, z_0), что $\frac{\partial f}{\partial x}(x_0, y_0, z_0) = \frac{\partial f}{\partial y}(x_0, y_0, z_0) = \frac{\partial f}{\partial z}(x_0, y_0, z_0) = 0$ кроме (0,0,0).*

Геометрически, геометрическое место точек в трёхмерном комплексном пространстве, где многочлен обращается в ноль, это конус, т.е. состоит из линий, проходящих, через центр. При переходе к $P^2(X)$ мы сопоставляем каждой линии точку и получаем одномерный объект.

Предложение 0.17 *Гладкая проективная плоская кривая является компактной римановой поверхностью.*

Идея доказательства:

1. $V(F)$ компактно, достаточно доказать, что оно замкнуто в $P^2(C)$, для этого достаточно показать, что $\pi^{-1}(V(F))$ замкнуто в $C^3 \setminus (0, 0, 0)$, где $pi : C^3 \setminus (0, 0, 0) \to P^2(C)$ естественная проекция. Но также мы знаем, что $\pi^{-1}(V(F))$ совпадает с прообразом нуля при отображении $C^3 \setminus (0, 0, 0) \to P^2(C)$, которое задано многочленом f.

2. Чтобы показать, что это риманова поверхность, надо смотреть на пересечения с произвольными картами в $P^2(C)$. Рассмотрим, например, карту $z = 0$. Там есть аффинные координаты $X, Y = x/z, y/z$. Тогда пересечение с картой $V(F)$ это $V(f)$, где $f(X, Y) = F(x, y, 1)$.

Мы утверждаем, что нет таких X_0, Y_0, что в них зануляются обе производные f. В самом деле, если бы это было не так, то мы бы имели противоречии с тождеством Эйлера (оставим проверку слушателям).

Теперь мы победили, так как $V(f)$ оказывается гладкой аффинной кривой и тем самым римановой поверхностью.

Пример:

Посмотрим на многочлен $f(x, y) = y^2 - x^3 - 1$. Его гомогеннизация это многочлен $F(X, Y, Z) = Y^2Z - X^3 - Z^3$, так что мы имеем ещё одну точку на бесконечности $X = Z = 0, Y = 1$.

Род кривой.

Мы уже упомянули род римановых поверхностей, род кривой это род соответствующей римановой поверхности. Однако, его можно определить и независимо.

Родом кривой, заданной многочленом степени d будем называть число

$$\frac{(d-1)(d-2)}{2} - \sum v_p,$$

где сумма берётся по всем особым точкам.

Пример: Кривая Ферма $x^n + y^n - 1$ не имеет особых точек, так что её род $(n-1)(n-2)/2$.

Напротив, кривая $y^2 = x^2(x+1)$ имеет двойную точку в начале системы координат. Соответствующая проективная кривая $ZY^2 = X^2(X+Z)$ имеет производные $-3X^2 - XZ$, $2YZ$, $X^2 - Y^2$, которые зануляются в точке [0,0,1]. Поэтому род этой кривой 0, а не 1.

Сколько может быть точек рациональных на кривых в зависимости от степени?

Если степень 1, то это кривая $f = ax + by + c$ и решений бесконечно много.

Если степень 2, то может решений не быть вовсе, как в случае, $x^2 + y^2 + 1$ или же, если есть хотя бы одно, то их бесконечно много. Такие кривые имеют род ноль и о них речь пойдёт в следующем разделе.

Если степень 3, то такие неособые кривые оказываются эллиптическими и мы рассмотрим их также позже. В их случае рациональные точки образуют группу.

Что же происходит в случае больших степеней (и соответственно рода)? Оказывается, тогда число решений конечно, в этом и заключается гипотеза Морделла.

0.4 Рациональные точки на кривых рода ноль

Перейдём к кривым рода ноль. Первое замечание такие кривые это коники.

Пример: Рассмотрим однородный многочлен $P(X, Y, Z) = X^2 + Y^2 - Z^2$.

Простая проверка показывает, что $V(P)$ гладкая проективная кривая. Если мы дегомогенизируем относительно Z, то получим уравнение окружности, если по отношению к X или Y уравнение гиперболы. Это совершенно неслучайно ибо аффинные плоские коники получаются сечением конуса (который был до того, как мы отождествили все точки на каждой прямой, проходящей через начало координат) плоскостью.

Предложение 0.18 *Кривая рода ноль с рациональной точкой изоморфна проективной прямой.*

Надо рассмотреть прямые через эту точку, пересекающие нашу конику. Это отображение задаёт изоморфизм.

Пример: Единичная окружность.

Можно заметить, что на единичной окружности лежит, например, точка (-1,0). Рассмотрим все прямые через неё проходящие, они пересекают нашу окружность в ещё одной точке (касательная пересекает только в (-1,0)). Записав уравнение прямой как $y = tx + t$, мы можем найти рациональную параметризацию окружности:

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}$$

Логично задаться вопросом, когда на конике есть рациональная точка и как доказать, что точек нет, если их нет.

Один из способов следующий. Как мы знаем кривая рода ноль изоморфна плоской конике, которая задаётся нулями многочлена

$$ax^2 + by^2 + c,$$

где a, b, c без квадратов, попарно взаимно простые. Теорема Лежандра утверждает, что рациональное решение имеется тогда и только тогда, когда у a, b, c не у всех одинаковый знак, $-ab$ квадрат по модулю c, $-bc$ квадрат по модулю a, $-ac$ квадрат по модулю b.

Группа рациональных точек окружности.

Множество рациональных точек окружности образует бесконечную абелеву группу с операцией вращения. Единица это элемент $(1, 0) = 1 + 0i$. Сложение определенно естественно $(x, y) * (t, u) = (xt - uy, xu + yt)$. Это на самом деле просто сложение углов в терминах синусов и косиносов.

На языке комплексных чисел это можно определить как умножение элементов нормы один.

Легко видеть, что эта группа изоморфна $SO(2, Q)$.

Критерий Хассе.

Как мы уже отмечали, для кривой рода ноль может быть либо ноль рациональных точек, либо бесконечно много. В частности кривая рода 0 имеет

рауиональную точку титтк у неё есть точка везде локально, что означает, что решения есть над полем вещественных чисел и Q_p для всех p. Отсутствие Q_p-точки это всегда следствие препятствий по модулю некоторой степени p

Пример: Пусть X кривая, заданная нулями многочлена $f = x^2+y^2?3$. Если есть рациональное решение, то приведя к общему знаменателю, то получаем, что есть r, s, и t, такие что $r^2 + s^2 = 3t^2$. Так как квадраты целых сравнимы с 0 или 1 по модулю 4, то после редукции получаем, что в левой части оба слагаемых делятся на 4. И все целые тут чётны, что противоречит, тому что у них нет общего делителя (могли на его квадрат сократить). Тем самым, у нас есть препятствие по модулю 4 к существованию решений над Q_2. А значит никакой рациональной точки.

Определение 0.19 *p-Адическим числом для простого p называется ряд вида*

$$a_0 + a_1 p + a_2 p^2 + ...$$

Само кольцо обозначается Z_p. Если мы обрежем ряд, то получим отображение

$$Z_p \to Z/p^k Z$$

Тогда Z_p можно определить как обратный предел колец $Z/p^k Z$. Здесь имеется в виду следующее:

рассмотрим гомоморфизмы $\pi^Z_{ji}/p^i Z \to Z/p^j Z$. Тогда обратный предел это

$$\underline{lim} Z/p^k Z = (x_i)_i \in \prod_i Z/p^i Z | \pi_{ij}(x_j) = x_i i \leq j$$

Определение 0.20 *Ряд*

$$a_{-n} 1/p^n + ...a_0 + ...$$

называется p-адическим числом.

Множество p-адических чисел обозначается Q_p. Это поле и оно содержит поле рациональных чисел.

Принцип Хассе

В листочке 1 была задача про сумму квадратов. Идея решения в том, чтобы рассмотреть два множества $A = y^2 mod p$ и $B = u - x^2 mod p$, они пересекаются и рассуждением через остатки можно показать, что если $p \equiv 3 mod 4$, то t p-адическое число раскладывается в сумму двух квадратов титтк $ord_p(t)$ чётен. А далее теорема Эйлера, что число раскладывается в сумму квадратов целых титтк все простые с остатком 3 по модулю 4 входят в чётной степени.

Можно заметить, что иметь решения для квадратичных форм в R и Z_p для всех p не влечёт наличие решений в Z. Рассмотрим пару примеров.

Лемма 0.21 *Hensel's lemma) Если $f(X) \in Z_p[X]$ и $a \in Z_p$ удовлетворяет*

$$f(a) \equiv 0 mod p$$

и $f'(a)$ не сравнимо с нулём по $mod p$, то существует единственное p-адическое α, такое что $f(\alpha) = 0$ и $\alpha \equiv a mod p$.

Пример: Рассмотрим $x^2 + 11y^2 = 3$. У него нет никаких целых решений, но есть решения вещественные и для всех Z_p. Вещественные легко. Для Z_p с $p \neq 2, 11$ надо решить сравнение $x^2 \equiv 3 - 11y^2 mod p$, используя принцип Дирихле, затем применить лемму Гензеля. В случае $p = 2$ заметим, что $3/11 \equiv 1 mod 8$ получаем, что $3/11$ квадрат в Z_2 В Z_{11} решается поскольку $3 \equiv 5^2 mod 11$, значит можем решить $x^2 + 11\Delta 0^2 = 3$ в $Z_1 1$.

По китайской теореме об остатках полиномиальное уравнение с целыми коэффициентами имеет решение в Z_p для всех p имеет решение по любому модулю m. Т.е. мы на примере выше поняли, что иметь решение по любому модулю не означает иметь решения в целых числах.

В примере выше и аналогах есть рациональные решения, к примеру $x^2 + 11y^2 = 3$ имеет решения $(1/2,\ 1/2)$ и $(4/3,\ 1/3)$, а уравнение $2x^2 + 7y^2 = 1$ из листочка имеет решения $(1/3,\ 1/3)$ и $(3/5,\ 1/5)$. Это аргумент, что наличие решений в Q и Q_p более надёжная концепция, чемZ и Z_p и это действительно так.

Теорема 0.22 *(Hasse Minkowski). Пусть $Q(x_1, ..., x_n)$ квадратичная форма с рациональными коэффициентами.*

1) Для $c \in Q^\times$ уравнение $Q(x) = c$ имеет решение в Q тогда и только тогда оно имеет решение в R и всех Q_p.

2) Уравнение $Q(x) = 0$ имеет решение в Q кроме (0,...,0) тогда и только тогда оно имеет решение в R и всех Q_p помимо (0, . . . , 0).

Более того, в обоих случаях, если $n \geq 2$, то наличие решения в Q_p следует автоматически кроме $p \neq 2$ или если какой-то коэффициент многочлена $Q(x)$ не в $Z_p^\times$. [1]

В другой формулировке

Теорема 0.23 *(Hasse principle). $C(Q) \neq \emptyset$ тогда и только тогда $C(Q_p) \neq \emptyset$ для всех p. В этом случае кривая изморфна P^1.*

Доказательство:

Отправим кривую в P^2 как конику. Образ задан квадратичным уравнением $f(x, y, z) = 0$, мы можем привести эту форму к диагональному виду $ax^2 + by^2 +$

[1] любую форму можно привести к диагональгому виду и там это уже несложно

$cz^2 = 0$ с $a, b, c \in Q^\times$. Отнормировав координаты, получим $ax^2 + by^2 = z^2$, где a, b целые числа без квадратов, и будем считать, без ограничения общности, что $|a| \leq |b|$.

Если $a = 1$, то доказывать нечего. Иначе, $y \neq 0$. Заметим, что для решения (x, y) число b оказывается нормой для $z/y + x/y\sqrt{a}$.

Напомним, что множество норм для $Q(\sqrt{a})$ образует подгруппу в $Q^\times$.

Предположим, что $C(Q_p) \neq \emptyset$ для всех p. Хотим показать, что $C(Q) \neq \emptyset$ индукцией по $m = |a| + |b|$.

Если $m = 2$, то $a = -1$, $b = 1$. Тогда ясно, что $C(Q) \neq \emptyset$.

Пусть теперь $m > 2$ или $|b| \geq 2$. Мы утверждаем, что a это квадрат по модулю b. По китайской теореме об остатках достаточно показать это по модулю любого простого делителя b. Пусть $(x, y, z) \in Q_p^3$ ненулевое решение уравнения. Можем считать, что они в Z_p и одно из них единица там. Если x не единица, то и z тоже. Но тогда и y тоже. Получаем противоречие, значит $a = (z/x)^2 mod p$. Таким образом утверждение доказано.

Из утверждения следует, что есть $t \in Z$ такое что $t^2 = a + bb'$. Можем взять t так, что $|t| \leq |b|/2$. Тогда bb' это норма $t - \sqrt{a}$. Те b норма титтк b' норма, значит

$$ax^2 + b'y^2 = z^2$$

имеет рациональное решение. Тогда $|b'| = |(t^2 - a)/2| \leq (|b|/4 + 1) < |b|$. Индукция работает. Утверждение про изоморфность проективной прямой уже было выше.