1 Введение

В своих двух лекциях, которые я планирую прочитать на школе в Дубне, я собираюсь рассказать об одной из самых интересных и важных гипотез XX века. Гипотеза эта была высказана Луисом Морделлом в 1922 году и была доказана Гердом Фалтингсом в 1983 году. За доказательство гипотезы Морделла Г. Фалтингс в 1986 году получил Филдсовскую медаль.

Гипотеза Морделла на протяжении нескольких десятилетий привлекала внимание многих математиков — в основном алгебраических геометров и специалистов по теории чисел. Была выстроена стройная идейная стратегия доказательства данной гипотезы, которая и была окончательно реализована Гердом Фалтингсом в 1983 году. Цель первой лекции состоит не в том, чтобы быстро добраться до формулировки данной гипотезы, – это сделать совсем не сложно, – целью скорее является дать некоторое введение, которое позволит познакомить слушателей с различными объектами, возникающими в алгебраической и арифметической геометрии.

Арифметическая алгебраическая геометрия в основном исследует вопросы, связанные с изучением диофантовых уравнений. Я не уверен, что точно могу определить, что такое диофантовы уравнения. Но давайте сейчас это будем понимать как решение системы уравнений вида:

$$X\colon \begin{cases} f_1(x_1,\dots,x_n)=0 \\ \dots \\ f_m(x_1,\dots,x_n)=0 \end{cases}, \tag{1}$$

где все f_i — многочлены от переменных $x_1,\dots,x_n$ с целыми коэффициентами. А решения данных систем будем искать в целых или рациональных числах.

2 Примеры

Полезно начать с рассмотрения различных примеров. Какие примеры мы можем привести? Конечно, их огромное количество. Некоторые из них нам очень хорошо известны, про другие кто-то из вас что-то возможно слышал ранее. Про одни уравнения мы знаем ответы и умеем описывать решения, про другие знаем, что ответы известны или известны частично, а про некоторые не знаем практически ничего. Вот несколько таких примеров.

Пример 1 (Уравнение Пелля).

$$x^2 - 2y^2 = \pm 1.$$

Имеет бесконечно много решений; см., например, [4, 5].

Пример 2 (Теорема Ферма для $n = 3$). Уравнение

$$x^3 + y^3 = z^3$$

не имеет нетривиальных решений. Впервые данное утверждение было доказано Эйлером в 1770 году.

Пример 3 (Великая теорема Ферма). Уравнение

$$x^n + y^n = z^n.$$

не имеет нетривиальных решений для любого $n > 2$. Доказана Уайлсом в 1994 году.

Пример 4 (Taxicab number).

$$x^3 + w^3 = y^3 + z^3$$

Есть ли нетривиальные решения? Пример Рамануджана:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3;$$

Число 1729 является наименьшим числом, представимым в виде суммы двух кубов двумя различными способами. Можно доказать, что для любого n существует число, которое может быть представлено как сумма двух положительных кубов n различными способами.

Пример 5. Эйлер предположил, что уравнение:

$$x^4 + y^4 + z^4 = w^4.$$

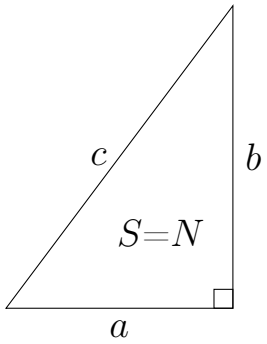
не имеет нетривиальных решений в целых числах. В 1988 г. Н. Элкис доказал [1], что решений бесконечно много, и привёл решение

$$2\,682\,440^4 + 15365639^4 + 18796760^4 = 20615673^4;$$

в том же году по предложенной им схеме R.Frye нашёл [2] и минимальное нетривиальное решение:

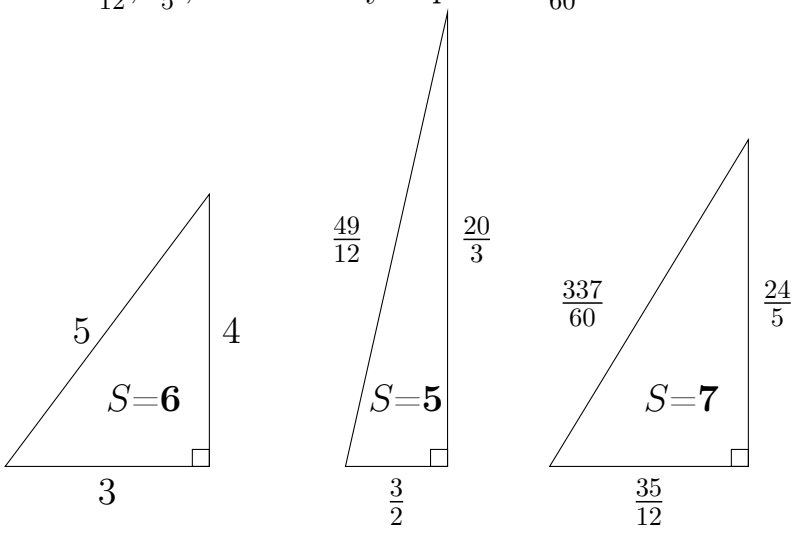
$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

Пример 6 (Задача про конгруэнтные числа). Пусть $N \in \mathbb{Z}$. Существует ли прямоугольный треугольник с рациональными сторонами и площадью равной N?



Для $N = 6$ подходит египетский треугольник со сторонами $3, 4$ и 5.

Конгруэнтными также являются числа $N = 5$, для которого имеется треугольник с катетами $\frac{3}{2}$, $\frac{20}{3}$ и гипотенузой $\frac{49}{12}$, и $N = 7$, для которого подходят катеты $\frac{35}{12}$, $\frac{24}{5}$, а гипотенуза равна $\frac{337}{60}$.



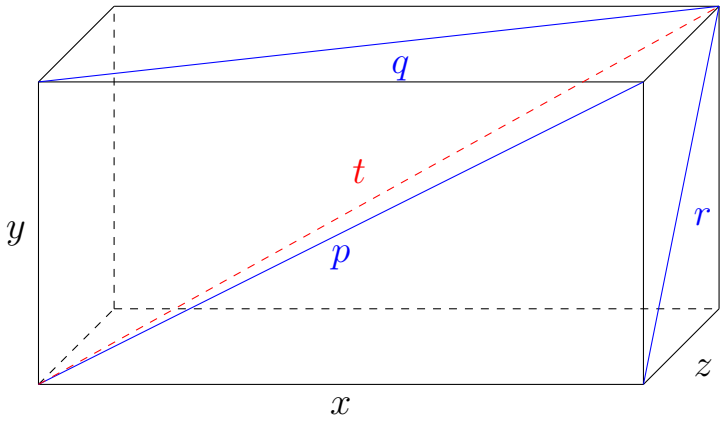
В качестве задачи можно попробовать доказать, что 1 не является конгруэнтным числом. В общем случае задача не решена. Этому вопросу, который появился в арабском манускрипте Абу Бакр аль-Караджи, более 1000 лет. В его труде это сформулировано в другой форме: для каких чисел $N \in \mathbb{Z}$ существует рациональное число v такое, что $v^2 - N$ и $v^2 + N$ оба являются квадратами рациональных чисел? Данная задача сводится к решению в рациональных числах следующей системы диофантовых уравнений:

$$\begin{cases} v^2 - N = w^2 \\ v^2 + N = u^2. \end{cases} \tag{2}$$

Задача 1. Убедитесь в равносильности формулировок.

Многое известно, но не всё[1]. Что-то следует из гипотезы Бёрча и Свинертон-Дайера для эллиптических кривых. Об этой — как и о следующей — задаче можно прочитать в [3].

Пример 7. Существует ли прямоугольный параллелепипед ("пифагоров кирпич"), у которого длины всех сторон, диагоналей граней и большой диагонали – рациональные числа?



Это открытый вопрос, ответ на него неизвестен; задача тут сводится к решению следующей системы уравнений

$$\begin{cases} x^2 + y^2 = p^2 \\ x^2 + z^2 = q^2 \\ y^2 + z^2 = r^2 \\ x^2 + y^2 + z^2 = t^2 \end{cases}. \tag{3}$$

в целых числах[2].

3 Постановка вопросов

Давайте попробуем понять, какие вопросы имеет смысл задавать, рассматривая различные диофантовы уравнения. Пусть X — это какая-то диофантова задача. Рассмотрим все решения данной задачи в целых или рациональных числах и обозначим эти множества решений через $X(\mathbb{Z})$ и $X(\mathbb{Q})$.

[1] На самом деле – это поиск рациональных точек на эллиптической кривой, которая является пересечением двух квадрик в трехмерном пространстве.

[2] Это поиск рациональных точек на поверхности, которая является пересечением 4-х квадрик в шестимерном пространстве.

Возникают следующие естественные вопросы:

Вопрос 1. Какова мощность множеств $X(\mathbb{Z})$ и $X(\mathbb{Q})$? Конечны данные множества решений или бесконечны?

Имеет смысл также поставить вопросы об оценке количества решений, если оно конечно, — или о том, как эффективно найти все решения. Кроме этого, когда решений бесконечное число, можно также пытаться задать некоторую *функцию высоты* $h\colon X(K) \to \mathbb{R}$, и искать или оценивать количество решений с заданным ограничением на значение данной функции.

Прежде чем идти дальше, давайте ещё отметим тот факт, что мы можем спрашивать не только про решение в рациональных числах, но и про решение в других числах: и это часто оказывается полезным с различных точек зрения. Вы все, наверное, хорошо понимаете, что во многих случаях, говоря про решение в целых числах, имеет смысл рассмотреть решения по модулю некоторого простого числа p, т. е. говорить о решениях $X(\mathbb{Z}/p\mathbb{Z})$ над конечным полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Я думаю, что вы неоднократно это делали при решении некоторых олимпиадных задач.

Также, вместо поля (или вместе с полем) рациональных чисел $\mathbb{Q}$, мы можем рассмотреть различные его *расширения*: например, поле рациональных Гауссовых чисел $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}, i^2 = -1\}$, или поле $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, или круговое поле $\mathbb{Q}(\xi),\ \xi^n = 1$, где ξ – первообразный корень из единицы. Такие поля — а именно, конечномерные расширения поля $\mathbb{Q}$ — называются *числовыми полями* (или *полями алгебраических чисел*).

У любого такого поля K имеется *подкольцо целых* $\mathcal{O}_K \subset K$, аналог подкольца целых $\mathbb{Z} \subset \mathbb{Q}$: это элементы поля K, являющиеся *алгебраическими целыми числами*, то есть корнями многочлена с целыми коэффициентами и со старшим коэффициентом 1. Относительно сложения $\mathcal{O}_K$ — это конечнопорожденный свободный модуль над $\mathbb{Z}$, т. е. $\mathcal{O}_K \cong \mathbb{Z}^n$.

Замечание 1. Важный частный случай числового поля — это *квадратичное расширение* $K = \mathbb{Q}[\sqrt{d}]$ поля $\mathbb{Q}$. Здесь обычно предполагают, что d целое и свободно от квадратов. Отметим, что в такой ситуации $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ далеко не всегда совпадает с «естественным» $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$; хотя такое равенство и справедливо для $\mathbb{Q}[i]$, кольцо целых в общей ситуации может оказаться чуть больше. Например, для $d = 5$ оно порождено 1 и $\varphi = \frac{1}{2}(1 + \sqrt{5})$: золотое сечение φ является корнем уравнения $\varphi^2 - \varphi - 1 = 0$.

Естественно также рассматривать и другие расширения поля рациональных чисел $\mathbb{Q}$, такие как поле вещественных чисел $\mathbb{R}$, поле комплексных

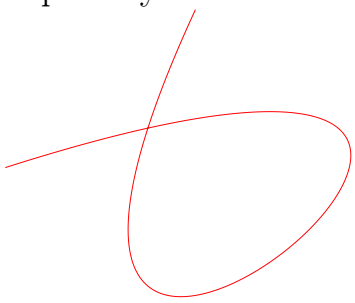
чисел $\mathbb{C}$ и поля p-адических чисел $\mathbb{Q}_p$, т. е. пополнения рациональных чисел $\mathbb{Q}$ относительно p-адической нормы.

Тем не менее, конечно, основным вопросом диофантовых задач является нахождение у уравнений и систем решений в целых и рациональных числах.

4 Кривые

Самым первым нетривиальным и естественным вопросом в нашем контексте решения диофантовых уравнений является вопрос о корнях одного уравнения с целыми коэффициентами $f(x, y) = 0$ от двух переменных. Другими словами, это вопрос о рациональных точках на плоской кривой, заданной уравнением $f(x, y) = 0$. Вопрос, что такое кривая и как её нужно представлять не является пустым и даже не является простым. Один из способов говорить про кривую — это говорить о точках, то есть о решениях уравнения $f(x, y) = 0$ со значением в различных расширениях поля $\mathbb{Q}$ (например, K, $\mathbb{R}$, $\mathbb{C}$).

Имеется такой фольклорный анекдот о Клоде Шевалле и Оскаре Зарисском. Однажды между ними зашел разговор о кривых, и ни один из них не мог понять другого. Наконец, Шевалле спросил: «Что Вы понимаете под кривой?» Так как они находились рядом с доской, то Зарисский сказал: «Конечно, вот это!» — и нарисовал картинку.

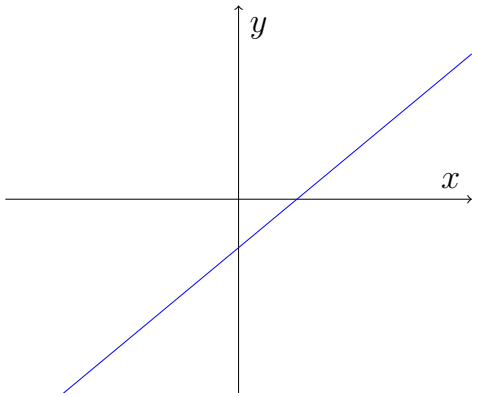


«А что Вы понимаете под кривой?» — спросил он. Шевалле ответил: «Я имел ввиду уравнение $f(x, y) = 0$».

Мы сейчас будем говорить об уравнениях $f(x, y) = 0$, а пытаться рисовать кривые $X \subset \mathbb{A}^2$ как Зарисский.

Итак, если у нас имеется уравнение $f(x, y) = 0$, то у него определена степень $d = 1, 2, \ldots$. Здесь степень многочлена — это максимальная степень монома.

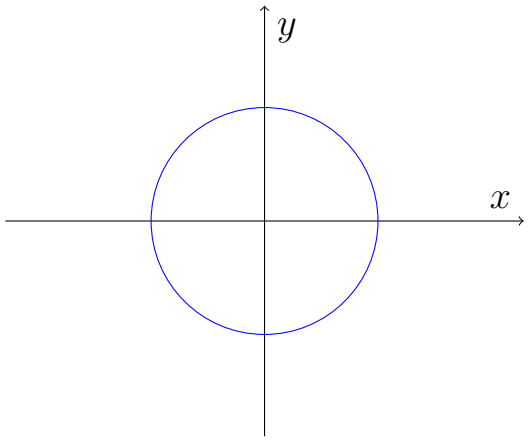
Случай $d = 1$ — это прямая $f(x, y) = ax + by + c$.



Все прямые над $\mathbb{Q}$ одинаковы, есть $\mathbb{A}^1_{\mathbb{Q}}$, и имеют бесконечно много точек.

Теперь мы можем перейти к рассмотрению кривых степени $d = 2$, то есть кривых, которые называются коники. Например,

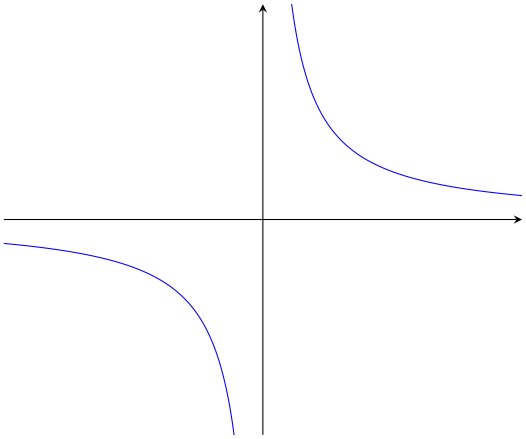
1. Уравнение $f(x, y) = x^2 + y^2 - 1 = 0$ задает нам окружность на плоскости:



Мы можем задать естественный вопрос: все ли коники на плоскости одинаковые? И быстро найдем примеры других кривых степени 2, которые очевидно отличаются от окружности. Например, гипербола и парабола.

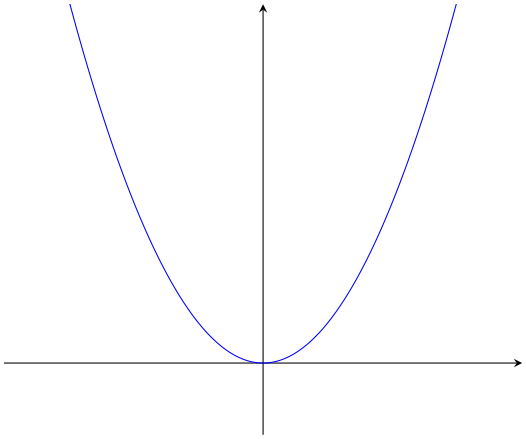
2. $f(x,y) = xy - 1 = 0$

гипербола



3. $f(x,y) = y - x^2 = 0$

парабола



Более того, мы можем рассмотреть такое уравнение степени 2, у которого вообще нет никаких решений в вещественных числах.

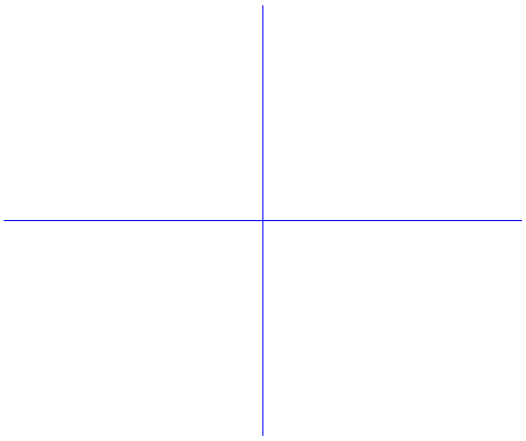
4. $f(x,y) = x^2 + y^2 + 1 = 0$.

То есть $X(\mathbb{R})$ в данном случае является пустым множеством.

Кроме таких неприводимых уравнений, мы можем рассмотреть многочлены второй степени, которые получаются произведением многочленов первой степени. При этом получатся так называемые *приводимые* коники, которые будут особыми кривыми.

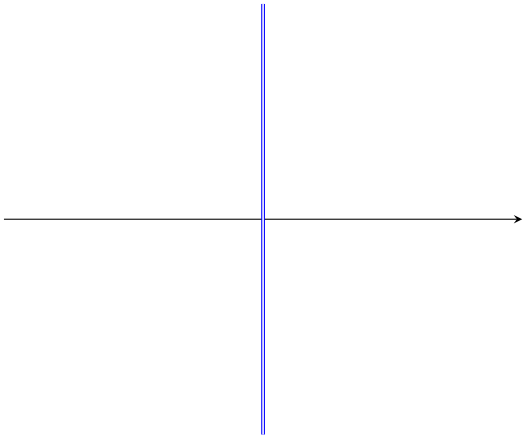
5. $f(x,y) = xy = 0$

пара прямых



6. $f(x,y) = x^2 = 0$

(двойная) прямая



Коники бывают разные, особенно над $\mathbb{Q}$, и этой теме можно посвятить

не только целую лекцию, но и отдельный курс. Мы же здесь отметим две важные общие вещи.

- Во-первых, пока еще мы работали в аффинной плоскости $\mathbb{A}^2$, и кривые у нас тоже были аффинными. Следовательно, присутствует эффект некомпактности нашей кривой и ее ухода на бесконечность.

- Во-вторых, существенное значение имеет гладкость кривой или, в противоположность этому, наличие особых точек.

5 Переход к проективной плоскости

Решение первой проблемы — это переход к проективному пространству, в нашем случае к проективной плоскости (А. Гайфуллин вам расскажет много интересного про проективные плоскости) и переход к проективным кривым. Так же, как проективная прямая $\mathbb{P}^1$ получается из аффинной прямой $\mathbb{A}^1$ добавлением точки на бесконечности, проективная плоскость $\mathbb{P}^2$ получается из аффинной плоскости $\mathbb{A}^2$ добавлением проективной прямой на бесконечности:

$$\mathbb{P}^2 = \mathbb{A}^2 \bigcup \mathbb{P}^1, \quad \text{где} \quad \mathbb{P}^1 = \mathbb{A}^1 \bigcup \infty.$$

Однако более правильное и однородное определение проективной плоскости — это задание её в виде многообразия всех прямых в трехмерном пространстве $\mathbb{A}^3$, проходящих через начало координат. На проективной плоскости таким образом возникают проективные координаты $(X : Y : Z)$, которые надо рассматривать по модулю растяжений, т.е. по модулю умножения на ненулевой элемент поля $\lambda \in K^*$

$$(X : Y : Z) \sim (\lambda X : \lambda Y : \lambda Z).$$

При естественном вложении аффинной плоскости $\mathbb{A}^2 \subset \mathbb{P}^2$ аффинная кривая $f(x, y) = 0$ будет замыкаться до проективной кривой, задаваемой уравнением

$$F(X, Y, Z) = 0, \quad F(X, Y, Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right),$$

где d – это степень $f(x, y)$. В частности, $F(X, Y, 1) = f(X, Y)$.

Так, в случае степени $d = 1$ уравнение прямой $ax+by+c = 0$ превращается в $aX+bY+cZ = 0$, а в случае степени $d = 2$ окружность (эллипс), гипербола и парабола — это одна и та же коника над $\mathbb{Q}$:

$$(X^2 + Y^2 - Z^2) \sim (XY - Z^2) \sim (YZ - X^2).$$

С другой стороны, конечно, кривая, задаваемая уравнением,

$$F(X, Y, Z) = X^2 + Y^2 + Z^2$$

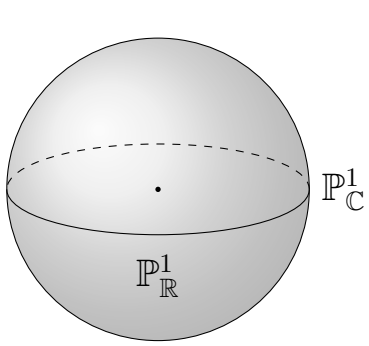
им не эквивалентна, так как не имеет точек над рациональными числами $\mathbb{Q}$ и даже над вещественными числами $\mathbb{R}$.

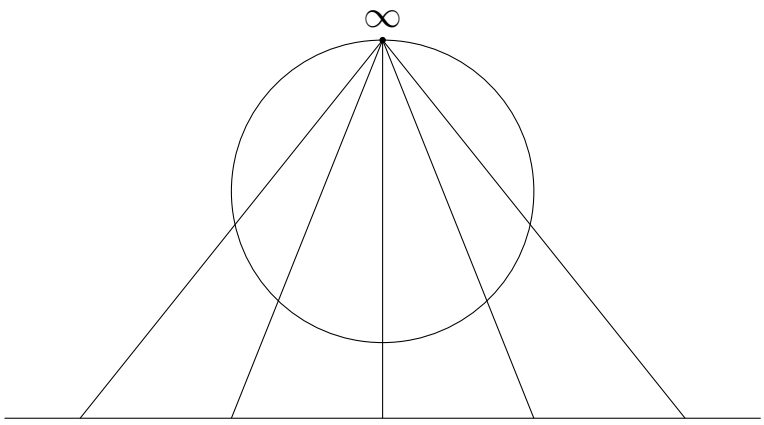
Нужно отметить, что поле вещественных чисел $\mathbb{R}$ имеет недостаток, состоящий в том, что оно не алгебраически замкнуто. Поле комплексных чисел $\mathbb{C}$ намного лучше. Давайте до конца исследуем коники. Рассмотрим их над полем комплексных чисел $\mathbb{C}$. И будем считать, что коники у нас гладкие. Общее понятие гладкости мы обсудим чуть позже, но в случае кривых степени 2 это означает что квадратичная форма $F(X, Y, Z)$ невырождена.

Теперь легко видеть, что по сути все гладкие коники одинаковые, мы говорим «изоморфные» (равные). Другими словами мы говорим это так: все невырожденные квадратичные формы над $\mathbb{C}$ приводятся к стандартному виду суммы квадратов[3]:

$$Z_1^2 + Z_2^2 + \ldots + Z_n^2.$$

Более того, все гладкие коники изоморфны проективной прямой $\mathbb{P}^1_{\mathbb{C}}$. Построить отображение можно взяв проекцию из точки. Отметим, что проективная прямая $\mathbb{P}^1_{\mathbb{C}}$ над $\mathbb{C}$ – это двумерная сфера $\mathbb{S}^2$, а проективная прямая $\mathbb{P}^1_{\mathbb{R}}$ над $\mathbb{R}$ является окружностью $\mathbb{S}^1$.





[3]Это утверждение верно для проективных гладких квадрик над $\mathbb{C}$ произвольной размерности

Над вещественными числами $\mathbb{R}$ гладкие проективные коники уже бывают двух типов — это либо проективная прямая $\mathbb{P}^1_{\mathbb{R}}$, либо коника, задаваемая уравнением

$$F(X, Y, Z) = X^2 + Y^2 + Z^2.$$

Для данной коники множество вещественных точек $X(\mathbb{R})$ пусто. Можно задать вопрос: почему это вообще кривая? Один из возможных ответов такой: это является кривой, так как она становится проективной прямой $\mathbb{P}^1_{\mathbb{C}}$ после расширения поля.

Также с точки зрения *теории схем* у данной кривой точки есть, но все они являются комплексными. А именно, в алгебраической геометрии можно перейти с «геометрического» языка на алгебраический, когда кривая описывается в терминах колец функций и идеалов. Над комплексными числами эта переформулировка равносильная — но термины и теоремы, возникающие при такой переформулировке, можно применять и к другим ситуациям. И над вещественными числами мы «находим» соответствующие «комплексные точки» (как нетривиальные *максимальные идеалы* в соответствующем кольце).

А что же происходит над полем рациональных чисел $\mathbb{Q}$? Оказывается, что вообще над любым полем, если у коники есть точка, то коника изоморфна проективной прямой $\mathbb{P}^1$, т.е. если $X(\mathbb{Q}) \neq \emptyset$, то $X \cong \mathbb{P}^1_{\mathbb{Q}}$. А если у коники нет точек над фиксированным полем? Над полем комплексных чисел $\mathbb{C}$ таких коник нет, над $\mathbb{R}$ такая коника одна, над полем рациональных чисел $\mathbb{Q}$ их очень много разных. Можно задать вопрос в каком смысле такие коники без точек являются разными? Ответом, например, может быть описание расширений $K \supset \mathbb{Q}$, над которыми у данных коник появляются точки.

Для коник над рациональными числами $\mathbb{Q}$ выполнен также *принцип Минковского–Хассе*, который говорит, что две коники (квадрики) изоморфны над $\mathbb{Q}$ тогда и только тогда, когда они изоморфны над всеми p-адическими числами $\mathbb{Q}_p$ и над $\mathbb{R}$; о нём можно прочитать в [7, гл. IV], в [8, лекция 4] или в [6]. Аналогичный принцип выполнен и над любым числовым полем K.

6 Гладкость и особые точки

Все гладкие точки похожи друг на друга, каждая особая точка особа по-своему. Геометрически гладкость очень понятное свойство, состоящее в том, что локально наш геометрический объект некоторой размерности выглядит как маленький шарик той же размерности. В нашем конкретном случае, когда дана кривая $f(x, y) = 0$ на аффинной плоскости, точка $p = (x, y)$ на

этой кривой (т.е. $f(p) = 0$) является особой, если имеется обращение в нуль обеих частных производных:

$$\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = 0.$$

Для однородного уравнения на проективной плоскости это означает, что

$$\frac{\partial F}{\partial X}(p) = \frac{\partial F}{\partial Y}(p) = \frac{\partial F}{\partial Z}(p) = 0.$$

Обычно почти все точки кривой являются гладкими. Однако, в случае кривой, заданной уравнением $f(x, y) = x^2$, мы видим, что

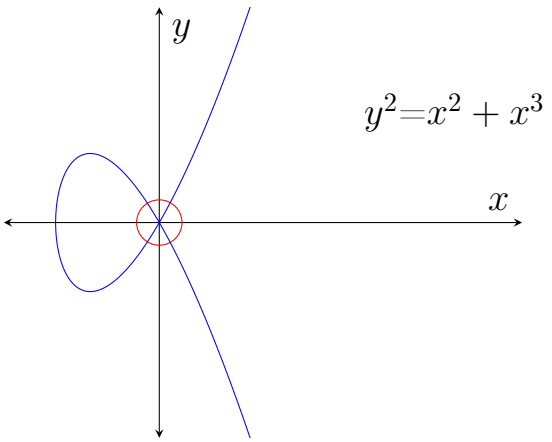
$$\frac{\partial f}{\partial x} = 2x, \quad \frac{\partial f}{\partial y} = 0,$$

и поэтому особые точки задаются уравнением $x = 0$. В этом случае вся кривая состоит из особых точек!

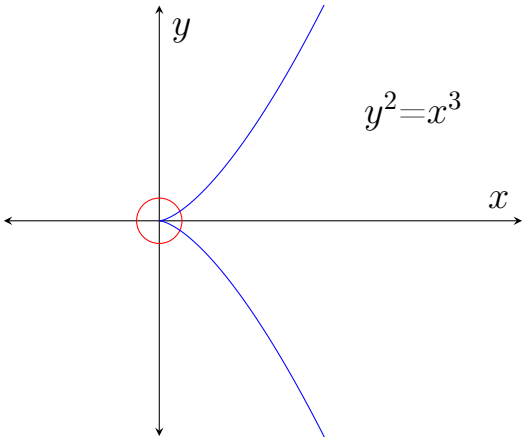
Кривая будет называться гладкой, если все её точки гладкие, в противном случае мы будем говорить, что кривая является особой.

Самые простые примеры особенностей для плоской кривой – это обыкновенная двойная точка и каспидальная точка:

1) Пример обыкновенной двойной точки у кубической кривой ($y^2 = x^2 + x^3$):



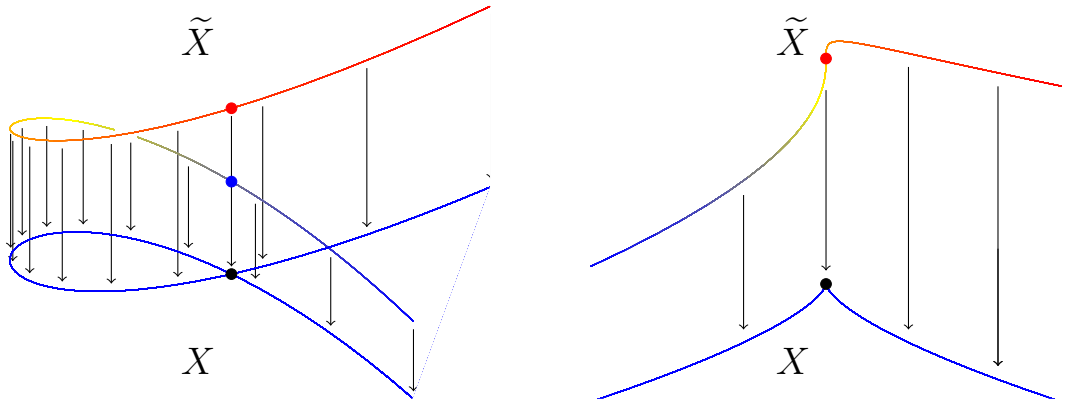
2) Пример каспидальной точки у кубической кривой ($y^2 = x^3$):



Конечно, бывают и более сложные особенности. Но про них мы говорить здесь не будем.

Важным инвариантом особенности является кольцо $K[x,y]/\langle\frac{\partial f}{\partial x},\frac{\partial f}{\partial y}\rangle$, которое является фактором кольца многочленов $K[x,y]$ по идеалу, порожденному частными производными, и называется *кольцом Милнора*. Размерность данного кольца как векторного пространства над полем K называется *числом Милнора* и обозначается μ. Легко видеть, что число Милнора обыкновенной двойной точки равно 1, а число Милнора для каспидальной точки есть 2.

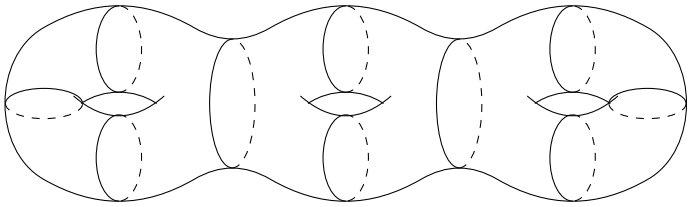
Если кривая X особая, то мы всегда можем взять её *гладкую модель* $\widetilde{X}\to X$, то есть *разрешить её особенности*. В случае кривой гладкая модель, которая называется *нормализацией*, однозначно определена.



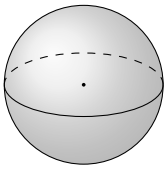
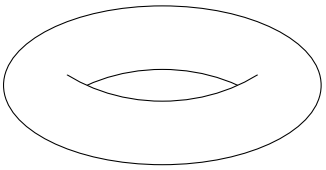
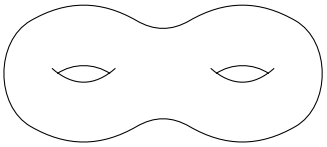
7 Топология и геометрия кривых

Ранее мы уже видели, что кривые разной степени могут оказаться изоморфными. Например, прямая и коника могут оказаться одинаковыми кривыми. Таким образом, степень многочлена $f(x,y)$ не является абсолютным инвариантом кривой. Однако, степень кривой, особенно если кривая гладкая, это

очень близко к инварианту. Чтобы увидеть правильный инвариант, давайте всё-таки рассмотрим кривую $X(\mathbb{C})$, задаваемую уравнением $F(X, Y, Z) = 0$, над комплексными числами $\mathbb{C}$. Если кривая гладкая, она является римановой поверхностью и имеет следующий вид:



Её топологический инвариант это число "ручек"(=число дырок) $g(X)$; оно называется *родом* кривой. Мы предполагаем, что кривая *неприводимая*, то есть состоит из одной компоненты.

 $g = 0$	 $g = 1$	 $g \geq 2$
Рациональная кривая $\mathbb{P}^1$	Эллиптическая кривая	Кривые общего типа
Единственная	Один параметр	$3g - 3$ параметра

Как выразить род плоской кривой через ее степень d?

1) Если кривая гладкая, то имеется формула для рода:

$$g = \frac{(d-1)(d-2)}{2}.$$

Замечание 2. Из нее сразу видно, что при $d = 1$ и $d = 2$ мы получаем кривую рода $g = 0$.

2) Гладкая кривая степени $d = 3$ имеет род $g = 1$. Например, кривая

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

является гладкой и имеет род $g = 1$. Над $\mathbb{Q}$ она имеет только три точки:

$$(1, -1, 0), (0, 1, 1), (1, 0, 1).$$

Кривые рода $g = 1$ с точкой называются *эллиптическими кривыми*.

3) Гладкая кривая степени $d = 4$ имеет род $g = 3$. Например, кривая Клейна

$$X^3Y + Y^3Z + Z^3X = 0$$

является гладкой кривой степени $d = 4$ и рода $g = 3$.

А где же кривые рода 2? Так как 2 нельзя представить в виде $\frac{(d-1)(d-2)}{2}$, мы получаем, что кривая рода $g = 2$ не может быть гладко вложена в проективную плоскость $\mathbb{P}^2$. Однако она может получаться при разрешении особенностей, как

$$\widetilde{X} \to X \subset \mathbb{P}^2,$$

где X уже особая плоская кривая. Для особых кривых род кривой может определяться по разному, в частности, выделяют арифметический род и геометрический род. Нас будет интересовать именно геометрический род $p_g(X)$, который по определению есть род гладкой кривой $\widetilde{X}$, т.е. $p_g(X) = g(\widetilde{X})$. Имеется замечательная формула для геометрического рода плоской кривой

$$p_g(X) = \frac{(d-1)(d-2)}{2} - \sum_{p \in \text{Sing } X} \delta_p,$$

где дефект δ_p ("насколько падает геометрический род из-за особенности в этой точке") зависит исключительно от локальных свойств особенности в точке p. В простейших случаях обыкновенной двойной точки и каспа $\delta_p = 1$. Отсюда следует, например, что кривая степени $d = 4$ с одной двойной точкой будет как раз иметь геометрический род 2.

Существует формула, которая связывает число Милнора μ_p и дефект δ_p :

$$\mu_p = 2\delta_p - r_p + 1,$$

где r_p – это количество ветвей кривой X в маленькой окрестности точки p.

Я думаю, что про эллиптические кривые вы узнаете много из разных курсов здесь в Ратмино (например, курсы Г.Б. Шабата, К.А. Шрамова), а про кривые больших родов из курса И.А. Панина.

8 Точки на кривой

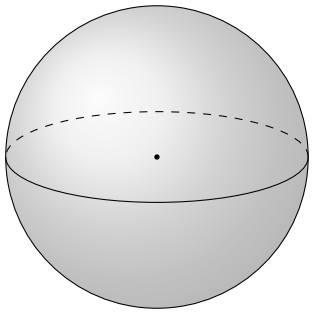
В заключение своей первой лекции отмечу следующую трихотомию.

В качестве инварианта гладкой кривой X вместо рода g удобнее иметь дело с ее эйлеровой характеристикой $\chi(X)$, которая выражается через род g следующим образом: $\chi(X) = 2 - 2g$. Рассматривая эйлерову характеристику, естественно выделять три случая:

$$\chi(X) > 0, \quad \chi(X) = 0, \quad \chi(X) < 0.$$

Данные три случая существенно различаются как над полем комплексных чисел $\mathbb{C}$, так и над числовым полем K.

8.1 Кривые рода $g = 0$ ($\chi > 0$)



Эйлерова характеристика $\chi(X)$ равна 2, и, следовательно, больше 0.

Над полем комплексных чисел $\mathbb{C}$ имеется только одна кривая – это проективная прямая $\mathbb{P}^1_{\mathbb{C}}$, которая является двумерной сферой $\mathbb{S}^2$.

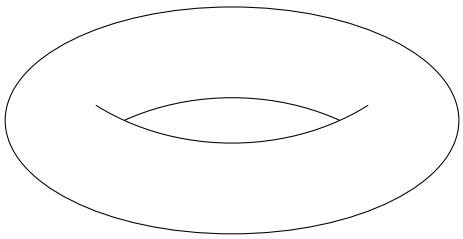
Имеется метрика постоянной положительной кривизны.

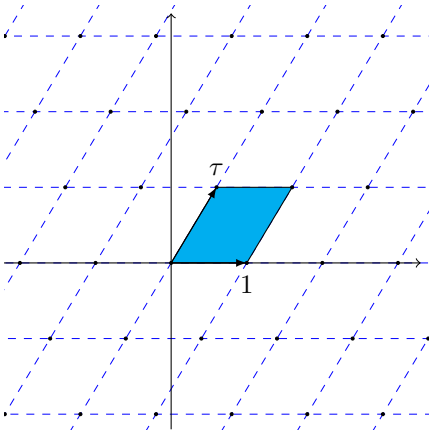
Над числовым полем K, если $X(K) \neq \emptyset$, то X является[4] проективной прямой $\mathbb{P}^1_K$, и, следовательно, число точек $X(K)$ бесконечно.

Выполнен локально-глобальный *принцип Минковского–Хассе*: коника над числовым полем K имеет точку тогда и только тогда, когда она имеет точку над каждым пополнением K (вещественным, комплексным или p-адическим). Более того, две коники над K изоморфны тогда и только тогда, когда они изоморфны над всеми пополнением K (вещественными, комплексными или p-адическими).

[4]Этот факт верен над любым полем

8.2 Кривые рода $g = 1$ ($\chi = 0$)





Эйлерова характеристика $\chi(X)$ равна 0.

При наличии хотя бы одной точки такие кривые называются эллиптическими кривыми.

Над полем комплексных чисел $\mathbb{C}$ эллиптическая кривая – это тор, и представляется в виде фактора $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ комплексной плоскости $\mathbb{C}$ по двумерной решетке, порожденной 1 и $\tau \in \mathbb{C}$.

Имеется один параметр: это точка τ верхней полуплоскости, рассматриваемая с точностью до разрешённых переходов $\tau \mapsto \tau + 1$ и $\tau \mapsto \frac{-1}{\tau}$.

Имеется плоская метрика, т.е. метрика с кривизной 0: это метрика, пришедшая из комплексной плоскости $\mathbb{C}$ при факторизации.

Над числовым полем K, если множество $X(K)$ не пусто, то $X(K)$ имеет структуру абелевой (коммутативной) группы.

Оказывается, группа $X(K)$ всегда конечнопорождена, т.е. она устроена следующим образом:

Теорема 1 (Л. Морделл, 1922, см. [9]).

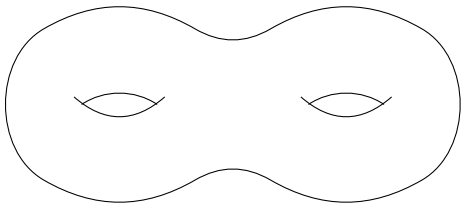
$$X(K) \cong \mathbb{Z}^r \oplus \mathrm{Tors},$$

где Tors — *конечная* абелева группа (состоящая из всех элементов конечного порядка в $X(K)$), а (конечная) величина r — называется *рангом* кривой.

Ранг кривой — штука довольно загадочная. Над полем рациональных чисел $\mathbb{Q}$ имеются примеры эллиптических кривых с рангом $r = 0, ..., 28$, но неизвестно, может ли ранг быть сколь угодно большим у эллиптических кривых над фиксированным полем K. Статистически у большинства эллиптических кривых ранг равен либо 0, либо 1.

Андрэ Вейль в 1929 году (см. [10]) обобщил эту теорему Морделла на абелевы многообразия, т.е. на алгебраические торы любой размерности.

8.3 Кривые рода $g \geqslant 2$ ($\chi < 0$)



Эйлерова характеристика $\chi(X) = 2 - 2g$ меньше 0.

Над полем комплексных чисел $\mathbb{C}$ риманова поверхность рода $g \geq 2$ является фактором диска по дискретной группе.

Имеется $3g - 3$ параметров.

Имеется метрика постоянной отрицательной кривизны.

Теперь мы готовы сформулировать гипотезу Морделла:

Теорема 2 (Гипотеза Л. Морделла = Теорема Г. Фалтингса). Пусть X – это гладкая проективная кривая рода $g \geqslant 2$, определенная над числовым полем K. Тогда множество $X(K)$ конечно.

9 Завершающие замечания

Про группу кручения Tors для эллиптических кривых над полем рациональных чисел $\mathbb{Q}$ известно практически все. Существует всего 15 случаев и все они реализуются.

Теорема 3 (Б. Мазур). Существует всего 15 возможностей для подгрупп кручения Tors у эллиптические кривых, определенных над $\mathbb{Q}$:

$$\begin{array}{lll} (1) & \mathbb{Z}/m\mathbb{Z}, & 1 \leq m \leq 10, \quad \text{или} \quad m = 12, \\ (2) & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & m = 1, 2, 3, 4. \end{array}$$

Список литературы

[1] Noam D. Elkies, On $A^4 + B^4 + C^4 = D^4$, *Mathematics of Computation*, **51**:184 (1988), pp. 825-835.

[2] R.E. Frye, Finding $95800^4 + 217519^4 + 414560^4 = 422481^4$ on the Connection Machine, *Supercomputing '88:Proceedings of the 1988 ACM/IEEE Conference on Supercomputing, Vol. II Science and Applications*, DOI:10.1109/SUPERC.1988.74138

[3] В. В. Острик, М. А. Цфасман, Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые, 3-е издание, М.:МЦНМО, 2011.

[4] В. О. Бугаенко, Уравнения Пелля, М.:МЦНМО, 2001.

[5] В. Сендеров, А. Спивак, Уравнения Пелля // Квант. — 2002. — No. 3. — с. 2–9.

[6] В. Доценко, Арифметика квадратичных форм. — М.: МЦНМО, 2015.

[7] Ж.-П. Серр, Курс арифметики, М.:Мир, 1972.

[8] Дж. Конвей, Квадратичные формы, данные нам в ощущениях, М.: МЦНМО, 2008.

[9] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.* **21** (1922), pp. 179–192.

[10] André Weil, L'arithmétique sur les courbes algébriques, *Acta Mathematica.* **52**:1 (1929), pp. 281–315.