1. Скоробогатов А.Н. Точки на кривых Шимуры над числовыми полями

Скоробогатов Алексей, 23 декабря 2004

Я сегодня буду говорить про рациональные точки на кривых Шимуры. Начну с того, что расскажу кратко предысторию вопроса, а потом объясню, что такое кривые Шимуры.

1.1. Модулярная кривая

Надо начать с того, как Барри Мазур (B. Mazur) в 1977 г. нашел все $\mathbb{Q}$-точки на модулярных кривых $X_1(N)$. Напомню, что это такое.

Рассмотрим группу $\Gamma_1(N)$; пусть N — это целое положительное число. Рассмотрим матрицы 2×2 с целыми коэффициентами $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, которые по модулю N сравнимы с матрицей $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Потребуем также, чтобы определитель был равен 1, т.е. $ad-bc=1$, $a,b,c,d\in\mathbb{Z}$. Эти матрицы — подмножество алгебры $\mathrm{Mat}_2(\mathbb{Q})$ квадратных матриц порядка 2 над рациональными числами.

Такие матрицы действуют на верхней полуплоскости $\mathbb{H}$ (верхнюю полуплоскость можно рассматривать как множество комплексных чисел с положительной мнимой частью: $\{z\in\mathbb{C} \mid \mathrm{Im}\, z>0\}$). Тогда, как известно, есть дробно-линейное действие $z\mapsto \frac{az+b}{cz+d}$. И можно рассмотреть фактор $\Gamma_1(N)\backslash\mathbb{H}$. Фактор этот будет обозначаться $Y_1(N)$. Многие знают, что этот фактор некомпактен. Чтобы сделать его компактным, нужно добавить конечное множество точек — параболические точки или каспы. Пусть $X_1(N)$ — это такая компактификация (гладкая). Это — модулярная кривая.

Модулярная кривая, как я ее определил, это риманова поверхность. Но замечательное обстоятельство состоит в том, что на самом деле $X_1(N)$ — это алгебраическая кривая над $\mathbb{Q}$. И классики знали, как при желании написать ее уравнение. В классической науке люди делали следующее: они брали параболическую точку; в этой точке можно написать разложение в ряд. Если есть рациональная функция, инвариантная относительно действия $\Gamma_1(N)$, то можно разложить ее в ряд; если есть несколько функций, то можно написать уравнение, которое их связывает. Таким образом можно получить многочлен с постоянными коэффициентами, и это дает уравнение модулярной кривой над $\mathbb{Q}$. Но это получалось из вычислений. А глубокое объяснение этого факта состоит в том, что $Y_1(N)$ есть грубое многообразие модулей таких объектов: пара, состоящая из эллиптической кривой E и точки P на ней, где P — точка порядка ровно N. Это только грубое многообразие модулей, но всё равно, это очень важное обстоятельство. Проблема модулей над $\mathbb{Q}$ или даже над $\mathbb{Z}$ — это другой подход к тому факту, что $X_1(N)$ — многообразие над $\mathbb{Q}$.

Мазур нашел все рациональные точки этого алгебраического многообразия над $\mathbb{Q}$. Важность этого шага для теории чисел в том, что из этого он смог вывести точное описание всех возможных групп кручения эллиптических кривых. Теорема из этой работы говорит следующее: если род кривой $X_1(N)$ больше 0 (т.е. если это не проективная прямая), то все рациональные точки кривой $X_1(N)$ — это, в сущности, параболические точки (то, что нужно добавить к $Y_1(N)$, чтобы получить $X_1(N)$). Это замечательное описание.

Многообразием модулей эллиптических кривых является Y, а X получается компактификацией Y. В принципе, можно придать этому смысл, сказать, что X классифицирует как бы обобщенные эллиптические кривые, т.е. не только эллиптические кривые, но и их вырождения. А эллиптические кривые в собственном смысле отвечают только точкам Y. В этих обозначениях Мазур, собственно, доказал, что на Y рациональных точек как бы нет, т.е. $Y_1(N)(\mathbb{Q}) = \varnothing$.

Поэтому если у вас есть эллиптическая кривая E над $\mathbb{Q}$ и точка $P \in E(\mathbb{Q})$, имеющая порядок в точности N, то N должно быть не равно 11 и $N \leq 12$. То есть не может быть, скажем, рациональной точки, у которой порядок ровно 20. Это замечательное обстоятельство позволило полностью классифицировать все подгруппы кручения, состоящие из рациональных точек на эллиптических кривых.

1.2. Кватернионы

Это была мотивация. Теперь я хочу поговорить про кривые Шимуры. Они получаются таким образом. Конгруэнц-подгруппа — это подмножество алгебры $\mathrm{Mat}_2(\mathbb{Q})$ матриц порядка 2 над $\mathbb{Q}$. А теперь вместо такой алгебры рассмотрим алгебру кватернионов B. Это как бы обычная кватернионная алгебра; все знают, как она определяется: четырехмерное векторное пространство $B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ над $\mathbb{Q}$ со стандартными соотношениями $k = ij = -ji$; единственное отличие от алгебры обычных гамильтоновых кватернионов в том, что $i^2 = a$, $j^2 = b$, $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$.

Не при всяких числах a и b получается алгебра кватернионов, иногда может получиться алгебра, изоморфная матричной алгебре. B — тело тогда и только тогда, когда уравнение $ax^2 + by^2 = z^2$ не имеет ненулевых решений в $\mathbb{Q}$. Рассмотрим такие a и b; например, можно взять $-1, -1$; а можно взять что-нибудь другое.

У этой кватернионной алгебры есть редуцированная норма — отображение $N\colon B \to \mathbb{Q}$. Это аналог определителя; его квадрат — определитель умножения как линейного преобразования B. Есть также редуцированный след $T\colon B \to \mathbb{Q}$. Одно отображение мультипликативное, другое аддитивное. А еще у нее есть редуцированный дискриминант или просто дискриминант. Он определяется таким образом: это произведение простых чисел по всем p, для которых, если помножить B тензорно на p-адические числа, то получится по-прежнему алгебра кватернионов, т.е. нечто не изоморфное алгебре матриц над $\mathbb{Q}_p$:

$$D = \operatorname{discr} B = \prod_{p \text{ — простое: } B \otimes \mathbb{Q}_p \not\simeq \mathrm{Mat}_2(\mathbb{Q}_p)} p.$$

Для таких p после тензорного умножения на $\mathbb{Q}_p$ алгебра кватернионов остается телом. Есть только две возможности: стать алгеброй матриц или остаться телом. Таких простых чисел конечное количество. И говорят, что это числа, которые разветвлены в B. А также бесконечность разветвлена в B или нет; иными словами, умножая на $\mathbb{R}$ тензорно, мы тоже можем получить либо алгебру матриц, либо останутся кватернионы.

Кватернионные алгебры над $\mathbb{Q}$ с точностью до изоморфизма соответствуют целым положительным числам, свободным от квадратов. При этом алгебре сопоставляется ее дискриминант $B \leftrightarrow D$.

Из глобальной теории полей классов вытекает, что число нормирований поля $\mathbb{Q}$, в которых алгебра остается телом (если сюда включить и вещественные

числа), есть четное число, т.е. мощность множества

$$\{\text{нормирования } \mathbb{Q} \mid B \otimes \mathbb{Q}_\nu \not\simeq \mathrm{Mat}_2(\mathbb{Q}_\nu)\}$$

четна. Поэтому можно узнать, что если D состоит из произведения нечетного количества простых, то, значит, в бесконечности B остается телом, а если четное количество, то в бесконечности B — матричная алгебра. Например, если взять стандартную алгебру кватернионов ($a = -1, b = -1$), то она разветвлена в двойке и в бесконечности, ее дискриминант равен 2.

Для того чтобы определить аналог конгруэнц-подгрупп, мне нужен аналог кольца целых. Я напомню, что если у вас есть числовое поле k, то в нем есть кольцо целых, которое определяется как целое замыкание $\mathbb{Z}$ в k — все элементы, которые целы над $\mathbb{Z}$, все корни унитарных многочленов (т.е многочленов со старшим коэффициентом 1) с целыми коэффициентами. А соответствующий объект в кватернионной алгебре так легко нельзя определить. Надо рассматривать порядки в B — подкольца $\mathcal{O} \subset B$, содержащие единицу и порождающие над рациональными числами всё B: $\mathcal{O} \otimes \mathbb{Q} = B$. Аналогом кольца целых являются максимальные порядки; например, такие, которые действительно максимальны в смысле включения. Но проблема состоит в том, что, поскольку B не коммутативна, то максимальных порядков много; можно взять один максимальный порядок, сопрячь его, и получится другой. Здесь проявляется различие между алгебрами, которые в бесконечности расщепляются, и теми, которые не расщепляются. Оказывается, что верен такой факт: если в бесконечности B расщепляется, т.е. $B \otimes \mathbb{R} \simeq \mathrm{Mat}_2(\mathbb{R})$, то все максимальные порядки сопряжены. Это очень хорошая ситуация. (Есть стандартная книга, в которой всё это написано: это Vignéras, Lecture Notes Mathematics 800. Это стандартная ссылка для всего, что нужно знать про порядки в кватернионных алгебрах.) И мы только такие кватернионные алгебры будем рассматривать; они называются неопределенными.

1.3. Кривые Шимуры

Из-за того что B на бесконечности является алгеброй матриц, можно рассмотреть действие разных групп, которые в ней содержатся, на верхней полуплоскости. Более точно, зафиксируем максимальный порядок $\mathcal{O} \subset B$. Редуцированная норма $N\colon \mathcal{O} \to \mathbb{Z}$, отображает $\mathcal{O} \subset B$ в целые числа, так же как норма кольца целых числового поля; при этом обратимые элементы переходят в ± 1 (обратимые элементы $\mathbb{Z}$): $\mathcal{O}^* \to \{\pm 1\}$. Возьмем те из них, у которых норма равна 1: $\mathcal{O}^+ = \{x \in \mathcal{O} \mid N(x) = 1\}$. И теперь, поскольку я потребовал, чтобы норма была равна 1, то $\mathcal{O}^+$ вкладывается в $\mathrm{SL}_2(\mathbb{R})$ — из-за отождествления $B \otimes \mathbb{R} \simeq \mathrm{Mat}_2(\mathbb{R})$. Я могу подействовать соответствующими матрицами на верхней полуплоскости и рассмотреть фактор $\mathcal{O}^+\backslash\mathbb{H} = X$. Как и раньше, это риманова поверхность. Это кривая Шимуры в ее простейшем варианте.

Особенность состоит в следующем: для кватернионной алгебры этот фактор компактен, если алгебра не матричная (а если алгебра матричная, то фактор некомпактен). Это чрезвычайно важное обстоятельство: никаких параболических точек добавлять не надо. И это в каком-то смысле хорошо, а в некотором смысле плохо. Кроме этого вся остальная теория переносится в общем-то довольно хорошо.

Я упомянул раньше, что классический вариант кривой можно задать уравнением (это часть классической теории модулярных форм), которое получается

из-за того, что можно написать разложение в каспе. Можно выбрать параболическую точку, в ней написать разложение в ряды функций, потом получить соотношение на эти функции — уравнение кривой. Здесь ничего такого сделать нельзя. Отсутствие параболических точек означает, что описывать уравнением кривые Шимуры — очень сложное занятие. Не то чтобы это было совсем невозможно, есть много разных примеров, но нет такого единого метода, который бы с этим справлялся.

Есть очень важный факт (это как раз работа Шимуры 60-х годов), что эти кривые определены над $\mathbb{Q}$, то есть кривая Шимуры — гладкая проективная алгебраическая кривая над $\mathbb{Q}$. Это не очень простой факт. И Шимура его доказывал, используя теорию комплексного умножения, то, как действует группа Галуа на всём — таким классическим способом. А современный подход к этому состоит в том, что надо написать проблему модулей; т.е. надо сказать, что эта кривая решает некую задачу модулей, написать объекты, которые надо параметризовать. Это маленькая статья Дринфельда в «Функциональном анализе», которая потом превратилась в большую книгу Катца и Мазура “Arithmetic moduli of elliptic curves«.

Кривая Шимуры X решает следующую проблему модулей (это грубое многообразие модулей, но всё равно): она параметризует пары (A, i), где A — абелева поверхность (значит, абелево многообразие размерности 2), а $i\colon \mathcal{O} \subset \operatorname{End} A$ — вложение максимального порядка, который мы зафиксировали, в эндоморфизмы. То есть это абелевы поверхности с кватернионным умножением, как говорят. Такое описание достаточно для задания проблемы модулей над $\mathbb{Q}$; в принципе, можно поднапрячься и задать проблему модулей над $\mathbb{Z}$. Труды Дринфельда как раз позволяют это всё сделать. Это нужно уточнить, я не буду про это говорить; там появляются дополнительные трудности, довольно тонкие.

Про эти кривые Шимуры много всего известно. В частности, из трудов Дринфельда можно вывести, как выглядит ее модель над спектром $\mathbb{Z}$, где редукция хорошая, где плохая. Модель над $\mathbb{Z}$ устроена так: если p не делит дискриминант, то редукция хорошая, т.е. эту кривую можно продолжить до гладкой кривой над спектром $\mathbb{Z}_p$; а если p делит дискриминант, то тут есть абсолютно явное описание того, как устроен плохой слой: все компоненты являются проективными прямыми, известно, как они пересекаются, известно, как действует группа Галуа на компонентах. Это описание получается из p-адической униформизации Чередника–Дринфельда. Это абсолютно фундаментальная вещь, но сейчас у меня нет возможности про это детально говорить.

1.4. Точки кривых Шимуры над числовыми полями

Вопрос, который я хотел бы обсудить, такой: что можно сказать про точки кривых Шимуры над числовыми полями. Почему над числовыми полями, а не над $\mathbb{Q}$? Потому что над $\mathbb{Q}$ их нет. А над $\mathbb{Q}$ их нет, потому что их нет над $\mathbb{R}$. Шимура в своих работах выяснил, что над $\mathbb{R}$ эти кривые точек не имеют: $X(\mathbb{R}) = \varnothing$.

Поэтому первое, что осмыслено рассматривать, это мнимо-квадратичные поля. Пусть k — мнимо-квадратичное поле, т.е. такое расширение $\mathbb{Q}$ степени 2, которое получается присоединением корня из какого-нибудь отрицательного целого числа, свободного от квадратов.

Почему надо говорить именно про числовые поля, а не про локальные вначале? Дело в том, что над локальными полями получен окончательный ответ

лет 15 назад. Джордан (B. Jordan) и Ливне (R. Livné) нашли необходимое и достаточное условие над локальными полями. То есть над $\mathbb{R}$ всё ясно, над $\mathbb{C}$ всё ясно, остаются еще p-адические поля. Они полностью разобрались с ситуацией с p-адическими полями, т.е. с конечными расширениями $\mathbb{Q}_p$ (когда p делит D и когда не делит — для всех). Простейшая кривая Шимуры, как я ее определил, задается исключительно дискриминантом; я сказал, что надо зафиксировать максимальный порядок, но от этого, в общем, ничего не зависит. Значит, если есть дискриминант и есть конечное расширение поля p-адических чисел, то просто есть некая процедура (не очень короткая).

Интересно, каким методом они действовали. Когда p не делит D, в ситуации с хорошей редукцией, надо просто посчитать число точек над конечным полем. И потом, если у вас есть гладкая точка в замкнутом слое, то по лемме Гензеля она поднимается до точки над p-адическим полем. А как посчитать число точек над конечным полем? Для этого есть большая наука: формула следа Эйхлера–Сельберга для вычислению следа операторов Гекке - очень громоздкая аналитическая формула; это чистый анализ. Поэтому можно написать точную формулу. А когда p делит дискриминант, нужно пользоваться явным описанием p-адической униформизации Дринфельда и явным описанием компонент вырожденного слоя, которое из нее получается. Но это всё на самом деле вполне вычислимые вещи, с которыми можно работать. Получаются результаты, которые легко использовать на практике.

Поэтому следующий этап — это как раз работа над числовыми полями. И тут нет большой ясности. Сейчас я скажу, что известно над числовыми полями. Я не буду подробно рассказывать, зачем нужны кривые Шимуры. Они сами по себе очень интересны; они используются в теореме Ферма, в гипотезах Ленглендса, они используются везде. Можно, например, спросить, можно ли параметризовать эллиптические кривые кривыми Шимуры. Это осмысленная деятельность, потому что тогда можно строить рациональные точки на эллиптических кривых.

Есть следующая относительно малоизвестная теорема Джордана. Пусть p — простое число, $p \geq 11$, $p \equiv 3 \pmod 4$, p делит дискриминант. Пусть k — мнимоквадратичное поле, такое что над k кватернионная алгебра расщепляется, т.е. $B \otimes k \simeq \mathrm{Mat}_2(k)$. И пусть вдобавок p инертно, т.е. p остается простым в k. Это такие условия, которые легко понять; а еще есть условие, которое понять несколько более трудно. Пусть не существует сюръективного гомоморфизма конечных абелевых групп следующего вида:

$$Cl_k^{(p)} \twoheadrightarrow Cl_k \times \mathbb{Z}/\frac{p^2-1}{12}.$$

Тогда над k у X нет точек: $X(k) = \varnothing$.

Группа Cl_k — это группа классов поля k. Это фактор группы дробных идеалов по главным идеалам. Напомню, что дробные идеалы — это подмножества $I \subset k$, для которых существует ненулевой элемент $a \in k$, такой что если помножить a на I, то получится обычный идеал в кольце целых $\mathcal{O}_k$. Идеал I называется главным, если $I = b\mathcal{O}_k$ для некоторого $b \in k^*$. Это аналог группы Пикара. А $Cl_k^{(p)}$ — это дробные идеалы, взаимно простые с p; факторизовать их нужно по главным идеалам, которые порождаются b, сравнимым с 1 по модулю p:

$$Cl_k^{(p)} = \frac{\text{дробные идеалы, взаимно простые с } p}{(b) : b \equiv 1 \pmod p}.$$

Эта группа иногда называется лучевой группой классов с кондуктором p. Как ясно из этого описания, есть точная последовательность:

$$1 \to (\mathcal{O}_k/p)^*/\mathcal{O}_k^* \to Cl_k^{(p)} \to Cl_k \to 1.$$

Группа классов с кондуктором p отображается в просто группу классов сюръективно, потому что любой идеал можно сдвинуть с p. Такая конструкция известна из геометрии - это конструкция обобщенных якобианов. Cl_k — это группа Галуа максимального абелева расширения k, которое нигде не разветвлено, а $Cl_k^{(p)}$ — такого, которое разветвлено только в p.

Что простое p инертно, это означает, что p остается простым в k. Тогда фактор кольца целых по p будет конечным полем, которое квадратично над полем из p элементов. Значит, здесь будет содержаться циклическая группа порядка p^2-1, которой изоморфна $(\mathcal{O}_k/p)^* = \mathbb{F}_{p^2}^*$. А $\mathcal{O}_k^* = \{\pm 1\}$ — единственные единицы кольца целых, за исключением того случая, когда $k = \mathbb{Q}(\sqrt{-1})$ или $k = \mathbb{Q}(\sqrt{-3})$. Хорошо известный простой результат, что кольцо целых в квадратичном поле содержит нетривиальные корни из 1 только когда оно содержит корень 4-й степени из 1 или корень 6-й степени из 1. То есть в большей части случаев это есть циклическая группа порядка $\frac{p^2-1}{2}$. Поэтому на самом деле вполне реально, что такой сюръективный гомоморфизм существует. И действительно, при нынешнем развитии техники, с помощью программы типа Matematika вы просто пишете ваше мнимо-квадратичное поле и p, и она вам говорит, чему эта группа будет равна. То есть это такие вещи, которые сейчас считаются компьютером мгновенно.

Я приведу вкратце доказательство этой теоремы и объясню происхождение условия инертности. Я также хочу привести пример.

Пусть дискриминант есть произведение двух простых чисел $D = 23 \times 107$, а $k = \mathbb{Q}(\sqrt{-23})$. Число 23 здесь разветвлено, а 107, наоборот, инертно. Можно посчитать символ Лежандра и увидеть, что это достаточно, чтобы убить B переходом к k. А с другой стороны, все условия выполнены. В качестве p я предлагаю взять 107. Тогда лучевая группа классов есть произведение трех циклических групп $Cl_k^{(107)} = \mathbb{Z}/4 \times \mathbb{Z}/81 \times \mathbb{Z}/53$. А просто группа классов — группа из трех элементов: $Cl_k = \mathbb{Z}/3$. И если разложить в произведение циклических групп, там получится 4 циклических фактора. И соответственно, заключение такое, что у этой кривой нет точек над таким полем.

Я не буду выписывать теорему Джордана–Ливне, которую я процитировал. Но ее можно применить, и окажется, что у этой кривой есть точки всюду локально. То есть такая кривая является контрпримером к принципу Хассе: это многообразие, которое имеет точки над всеми пополнениями основного поля. Принцип Хассе — это такой принцип (иногда он бывает верен, а иногда нет), который говорит, что в некоторых случаях, для некоторых классов многообразий из наличия точек над всеми пополнениями следует наличие точек над глобальным полем. В нашем примере принцип Хассе не выполнен.

1.5. Препятствие Манина

Манин 35 лет назад предложил подход, который дает общий способ построить препятствие к принципу Хассе. Я отвлекусь от темы о кривых Шимуры, поговорю просто о препятствии Манина. Если X — многообразие над числовым полем k, такое что над всеми пополнениями оно имеет рациональные точки

($X(k_v) \neq \varnothing$ для всех v), то можно рассмотреть произведение множеств локальных точек по всем нормированиям $\prod X(k_v)$ и в нем определить некоторое подмножество $\prod X(k_v)^{\mathrm{Br}}$: это множества локальных точек (по одной локальной точке для каждого нормирования), такие что сумма локальных инвариантов элементов группы Брауэра X равна 0:

$$\prod X(k_v)^{\mathrm{Br}} = \{(P_v), P_v \in X(k_v), \sum \mathrm{inv}_v\ A(P_v) = 0\}.$$

Здесь A принадлежит группе Брауэра $\mathrm{Br}\, X = H^2(X, \mathbb{G}_m)$. Группу Брауэра многообразия X можно определить разными способами, например, как вторую группу этальных когомологий с коэффициентами в $\mathbb{G}_m$. По ее функториальности можно рассмотреть специализацию ее элемента в любой точке, например, в P_v. Тогда получится элемент группы Брауэра локального поля $A(P_v) \in \mathrm{Br}\, k_v$. Локальная теория полей классов доставляет отображение inv_v, которое задает изоморфизм Brk_v с $\mathbb{Q}/\mathbb{Z}$ (для $\mathbb{R}$ —с циклической группой из двух элементов). Если набор локальных точек происходит на самом деле из одной точки с координатами в k, то тогда значение A в этой точке будет элементом группы Брауэра поля k, и закон взаимности глобальной теории полей классов говорит, что сумма всех локальных инвариантов равна 0. Таким образом, если вложить k-точки X диагонально в произведение $\prod X(k_v)$, то они будут лежать в $\prod X(k_v)^{\mathrm{Br}}$. Получается такой промежуточный объект, как бы верхняя граница, вместилище k-точек в этом произведении:

$$X(k) \subset \prod X(k_v)^{\mathrm{Br}} \subset \prod X(k_v).$$

Смысл того, что Манин ввел группу Брауэра, состоит в том, что в ряде случаев она вычисляется. Для кубических поверхностей она по модулю группы Брауэра k — просто конечная группа. Была большая деятельность, которая продолжается, по исследованию всех мыслимых контрпримеров к принципу Хассе и объяснению того, что на самом деле происходит в ситуации, когда локальные точки есть всюду, а глобальных нет. Иногда это происходит за счет препятствия Манина, т.е. за счет того что уже $\prod X(k_v)^{\mathrm{Br}}$ пусто. Если можно доказать, что $\prod X(k_v)^{\mathrm{Br}}$ пусто, то автоматически $X(k)$ тоже пусто. Это универсальный подход, который, когда он работает, позволяет сводить трудную задачу решения диофантова уравнения над k (над числовым полем) к более простой задаче. Если группа Брауэра конечна, то в принципе условия, которыми $\prod X(k_v)^{\mathrm{Br}}$ задается в $\prod X(k_v)$, вычислимы.

Но группа Брауэра не всегда конечна. В частности, если X — гладкая проективная кривая (именно это мы сегодня обсуждаем), то интересная часть группы Брауэра (фактор по группе Брауэра поля, которая никакой роли здесь не играет) — это когомологии Галуа с коэффициентами в группе Пикара кривой над замыканием: $\mathrm{Br}\, X/\mathrm{Br}\, k = H^1(k, \mathrm{Pic}\, \bar{X})$, где $\bar{X} = X \times_k \bar{k}$. И это является фактором первой группы когомологий с коэффициентами в якобиане $J = \mathrm{Jac}(X)$.

Вопрос о том, является ли препятствие Манина на кривых единственным препятствием к принципу Хассе (иначе говоря, верно ли, что всегда, когда на данной кривой есть локальные точки, а глобальных точек нет, то это происходит из-за того, что $\prod X(k_v)^{\mathrm{Br}}$ пусто) в очень сильной степени является открытым. В частности, известно только, что это так для кривых рода 1, что получается немедленно из стандартных глобальных теорем двойственности.

Известны также отдельные очень частные случаи с разными дополнительными условиями. Вопрос этот имеет смысл не только как чисто теоретическое удовлетворение любопытства, но он еще занимает людей, которые занимаются вычислениями. Есть очень много специалистов по вычислительной теории чисел, которые любят решать такие задачи: дана явно кривая (большого рода), найти все рациональные точки. И они находят эту идеологию полезной.

Кривая X над k может быть двух типов: такая кривая, у которой есть класс дивизоров степени 1, определенный над k, и такая, у которой его нет. Если считать, что X его не имеет, то второй случай трудности не представляет, потому что в этом случае X можно представить себе как вложенную в главное однородное пространство якобиана, которое не имеет рациональных точек. Тогда вопрос просто решается опять же из глобальных теорем двойственности, при условии что мы примем гипотезу, что группа Тэйта–Шафаревича якобиана конечна: $|Ш(J)| < \infty$.

А в первом случае ситуация такая. Если такой класс дивизоров существует, то можно использовать его для того, чтобы вложить X в его собственный якобиан: $X \subset J$. И всё сводится, используя опять же стандартные теоремы, которые я всё время упоминаю, к такой задаче. k-рациональные точки X можно вложить в произведение точек X над локальными полями, внутри такого же произведения для якобианов:

$$X(k) \hookrightarrow \prod X(k_v) \cap \text{замыкание } J(k).$$

Возьмем замыкание рациональных точек якобиана в топологии произведения его локальных точек. Есть теорема Серра, опубликованная в двух статьях в «Известиях Академии Наук СССР», о том, что это замыкание — то же самое, что проконечное пополнение $J(k)$; если эта группа конечна, слово “замыкание” можно забыть. Ясно, что k-точки X лежат в вышеуказанном множестве. Задача состоит в том, верно ли, что здесь имеется равенство, что включение можно заменить на равенство? И это ровно есть то, как формулируется проблема о единственности препятствия Манина для кривых, в этом трудном случае. Равенство есть тогда и только тогда, когда препятствие Манина объясняет такие контрпримеры к принципу Хассе.

Я не буду это использовать, просто хочу привлечь внимание к этой проблеме. Очень трудно доказать, что это неверно. Есть люди, которые считают, что все контрпримеры для кривых к принципу Хассе должны объясняться препятствием Манина.

Я недавно присутствовал на докладе, где Пунен (B. Poonen) проделал такие чисто вероятностные рассуждения. Например, можно сделать некоторое приближение к этой задаче: можно рассмотреть произведение точек над конечными полями. Пусть у нас есть X — кривая над $\mathbb{Q}$ и на ней есть рациональный класс степени 1. Можно вложить X в якобиан и рассмотреть

$$\prod X(\mathbb{F}_q) \cap \text{замыкание образа } J(\mathbb{Q}) \subset \prod J(\mathbb{F}_p).$$

(Здесь произведение по всем p; а можно брать некоторые p, тогда будет множество конечно, тогда замыкания нет.) И он сделал такое замечание: если считать, что на кривой находится в среднем $p+1$ точка, на якобиане сколько-то точек, то размеры этих множеств таковы, что они не должны пересекаться случайным образом; т.е. если эти подмножества являются случайными, то пересечение должно быть пусто. Это навело на мысль о том, что гипотеза должна

быть верна. Но присутствовавший при этом Серр сказал, что он не убежден. Конечно, проблема в том, когда простых бесконечное количество. По тем же соображениям Пунен считал, что это должно быть верно для абелевых многообразий.

Этот метод любят специалисты по вычислительной теории чисел, потому что он позволяет строить алгоритмы, которые для разных кривых находят точки, определенные над $\mathbb{Q}$, которые, в принципе, довольно сложно искать.

1.6. Метод спуска

Теперь я хочу рассказать про метод спуска, который в практических случаях часто удобнее для тех же целей. Метод спуска имеет дело с конечным неразветвленным накрытием. Пусть $Y \xrightarrow{f} X$ — отображение, которое получается факторизацией по свободному действию конечной группы G (или конечной групповой схемы), $X = Y/G$. Тогда Y — это X-торсор относительно G (или G-торсор на X). Типичный пример этой ситуации — это изогении эллиптических кривых.

Пусть у нас есть 1-коцикл, т.е. элемент группы когомологий Галуа $\xi \in H^1(k, G)$, где G коммутативна. Тогда есть операция скручивания Y на ξ. (Как известно, если группа действует на каком-нибудь объекте, например, на многообразии, то имея класс из первой группы когомологий, можно скрутить то, на чем она действует, на этот класс.) Скрученный объект Y^ξ, так же как и Y, отображается на X. На нем действует G, и $f^\xi \colon Y^\xi \to X$ является торсором над X относительно G. И первое следствие (это верно для любого поля): множество рациональных точек $X(k)$ является непересекающимся объединением образов рациональных точек на всех скрученных формах:

$$X(k) = \bigsqcup_{\xi \in H^1(k,G)} f^\xi(Y^\xi(k)).$$

А объясняется это таким образом: мы берем точку P на X, смотрим на ее слой; P — точка определенная над k, поэтому группа Галуа поля k будет действовать, переставляя точки слоя. Иными словами, она будет действовать на слое при помощи некоторого характера. В ситуации, когда на G нет действия группы Галуа, можно думать, что это просто гомоморфизмы группы Галуа в G. И таким образом точке P, лежащей на X и определенной над k, отвечает такой гомоморфизм. И если я скручу ровно на этот самый гомоморфизм, то окажется, что в прообразе P у меня есть рациональные точки (все точки в прообразе будут рациональными). Каждая точка на X поднимается до рациональной точки ровно на одной из скрученных форм.

Это пока общая картина. Применение к арифметике состоит в следующем. Опять пусть k — числовое поле; если есть k-рациональная точка на X, то существует единственный коцикл $\xi \in H^1(k, G)$, такой что скрученная форма Y^ξ тоже имеет k-точку: $Y^\xi(k) \neq \varnothing$. Это следует из того, что я сказал. И можно утверждение ослабить: из непустоты $X(k)$ следует, что существует $\xi \in H^1(k, G)$ такое, что $Y^\xi(k_v) \neq \varnothing$ для всех v. Это абсолютно тривиальное, банальное наблюдение. Его можно перевернуть и сказать следующее: если для любого ξ существует v такое, что $Y^\xi(k_v)$ пусто, то $X(k)$ тоже пусто — упражнение в логике. Но несмотря на абсолютно банальный характер этих замечаний, они полезны на практике, потому что позволяют получить нетривиальную информацию о наличии точек на X над числовым полем, исходя из чисто локальных

вычислений на Y. Можно сделать еще замечание, что если X проективно, то достаточно рассматривать только конечное количество классов ξ и конечное количество нормирований v; т.е. на самом деле это конечная процедура. Этот принцип используется традиционно для вычисления группы Сельмера.

Пусть теперь у нас имеется торсор $f\colon Y \to X$ такой, что для любого ξ существует v, для которого $Y^{\xi}(k_v)$ пусто. Если X имеет точки над всеми локальными полями, то, как мы видели, X - контрпример к принципу Хассе. Нетривиальная, хотя и не очень сложная теорема (Colliot-Thélène, Sansuc) утверждает, что любой такой контрпример объясняется препятствием Манина. То есть, если у вас есть набор локальных точек на X, лежащий в $\prod X(k_v)^{\mathrm{Br}}$, то какое бы ни было неразветвленное накрытие $Y \to X$, можно подобрать скрученную форму, на которую они все разом подымутся. Соответственно, это дает некоторый рецепт на практике, как доказать тот факт, что контрпример к принципу Хассе объясняется при помощи препятствия Манина, таким достаточно простым способом, работая с одним накрытием. Понятно, что это очень маленькая грань, потому что препятствие Манина, как я говорил, связано с бесконечной группой (H^1 с коэффициентами в якобиане), а тут это как бы его маленькая тень. Тем не менее, это эффективный метод.

1.7. Накрытие Шимуры

Теперь моя цель состоит в том, чтобы подойти к результату Джордана, который я выше сформулировал, при помощи этого подхода. Если X — кривая Шимуры, то какова может быть кривая Y? Понятно, что нелепо ожидать, что будет только одно накрытие, которое годится для всех мыслимых контрпримеров к принципу Хассе на кривых Шимуры. Но есть одно такое совершенно замечательное накрытие, которое объясняет теорему Джордана. Оно называется накрытием Шимуры.

Давайте построим Y следующим образом. Я сказал (возвращаясь к предыдущей проблематике), что редуцированная норма отображает $\mathcal{O}$ в $\mathbb{Z}$. Рассмотрим простые числа p, которые делят дискриминант, и рассмотрим целые числа кратные p. Их прообраз назовем I_p. Тогда I_p — это двусторонний идеал в $\mathcal{O}$, и у него есть разные приятные свойства. Например, его квадрат — это просто главный идеал, порожденный p; фактор по нему — конечное поле $\mathcal{O}/I_p \cong \mathbb{F}_{p^2}$. Я хочу использовать аналог конгруэнц-подгруппы. Пусть $\Gamma_p = \{x \in \mathcal{O}^+ \mid x \equiv 1 \bmod I_p\}$. Это такие элементы $\mathcal{O}^+$ (я напомню, что это кватернионы из максимального порядка $\mathcal{O} \subset B$, которые имеют норму 1), что x сравним с 1 по модулю p. Это выделяет некоторую подгруппу в $\mathcal{O}^+$; и я могу ей действовать на верхней полуплоскости и рассмотреть фактор $\Gamma_p\backslash\mathbb{H}$. Это тоже компактная риманова поверхность, чуть более общего класса, чем раньше.

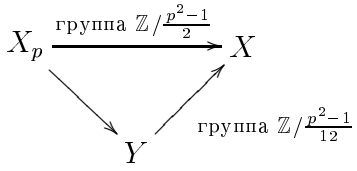
Но она имеет следующий дефект. Шимура вычислил поле, над которым будет определена эта алгебраическая кривая. Можно представить, что это алгебраическая кривая над числовым полем; но это поле оказывается не $\mathbb{Q}$. Она просто не определена над $\mathbb{Q}$. Определена она над круговым полем $\mathbb{Q}(\mu_p) = \mathbb{Q}(\sqrt[p]{1})$, получающимся добавлением корня p-ой степени из 1.

Иными словами, то, что мне нужно, будет приводимой кривой, уже определенной над $\mathbb{Q}$: X_p будет кривая над $\mathbb{Q}$, состоящая из $p-1$ неприводимых компонент, изоморфных $\Gamma_p\backslash\mathbb{H}$. И есть забывающее отображение $X_p \to X$.

Кривую X_p можно также рассматривать как многообразие модулей с дополнительной структурой. Напомню, что X было многообразием модулей пар

(A, i), где A — абелева поверхность, i — это вложение $\mathcal{O} \subset \operatorname{End} A$. У нас есть действие $\mathcal{O}$ на A (кватернионное умножение), и надо рассмотреть подгруппу $A[I_p] \subset A$, которая аннулируется умножением на I_p. Это аналог кривой с комплексным умножением, где можно рассматривать ядро умножения на разные элементы кольца целых соответствующего мнимо-квадратичного поля. Имеем $A[I_p] = \mathcal{O}/I_p \simeq \mathbb{F}_{p^2}^*$. Тогда X_p — грубое многообразие модулей троек (A, i, P), где P - образующая $A[I_p] \subset A$ как $\mathcal{O}$-модуля.

Проекция на X просто забывает про P: $(A, i, P) \mapsto (A, i)$. Это отображение, к сожалению, разветвлено. То, что называется накрытием Шимуры, является его максимальным этальным фактором. Я хочу рассмотреть промежуточное пространство Y. В дальнейшем p будет не равно 2 и 3. Тогда отображение $X_p \to X$ является накрытием Галуа с группой $\mathbb{F}_{p^2}^* / \pm 1$, т.к. точку P можно выбрать $p^2 - 1$ способами.



Пусть Y есть то единственное промежуточное накрытие Галуа, для которого группа Галуа Y/X — это $\mathbb{Z}/\frac{p^2-1}{12}$. Утверждается, что отображение $Y \xrightarrow{f} X$ неразветвлено. Этот факт, как вы понимаете, чисто топологический, потому что речь идет о действии некоторых фуксовых групп на верхней полуплоскости, и там у них есть эллиптические точки, за счет которых это отображение не является неразветвленным, и надо просто посчитать стабилизаторы и по ним отфакторизовать. Это факт на уровне классификации матриц, у которых есть неподвижные точки в верхней полуплоскости.

Теперь я могу абстрактный аппарат теории спуска, о котором я говорил выше, применить в нашей конкретной ситуации. Моя цель состоит в том, чтобы доказать, что для любого характера группы Галуа $\varphi \in \operatorname{Hom}(\operatorname{Gal}(\bar{k}/k), \mathbb{Z}/\frac{p^2-1}{12})$ существует v, для которого соответствующая скрученная форма не имеет локальных точек: $Y^{\xi}(k_v) = \varnothing$. Но я не хочу ничего вычислять про Y, я хочу действовать иначе. Эквивалентная формулировка состоит в следующем. Мы рассматриваем любые наборы локальных точек P_v на X. Как я уже говорил, если Y неразветвленно накрывает X и имеется рациональная точка на X, то на слое группа Галуа действует некоторым характером, переставляя точки слоя. Соответственно, любая локальная точка определяет локальный характер: для любой точки $P_v \in X(k_v)$ определен характер

$$\varphi \in \operatorname{Hom}(\operatorname{Gal}(\bar{k}/k), \mathbb{Z}/\frac{p^2-1}{12}).$$

Эквивалентная формулировка требуемого утверждения состоит в том, что никакой набор таких характеров, задаваемых локальными точками, не происходит из глобального характера. Значит, надо доказать, что для любого семейства точек (P_v) характеры φ_v не происходят из глобального характера φ. Это всё, что нужно сделать.

Если я это сделаю, то по теореме теории спуска, которую я процитировал, я смогу заключить, что контрпримеры к принципу Хассе, которые получаются на основании теоремы Джордана, объясняются препятствием Манина. Сейчас я опишу кратко план доказательства, не вдаваясь в детали. Всё сводится к

такой арифметической проблеме: как здесь найти противоречие, какие нужно использовать свойства этих локальных характеров, которые делают их несовместимыми друг с другом?

Есть два утверждения. Первый факт такой. Если рассмотреть нормирование $v \neq p$, то φ_v неразветвлен; иными словами, его ограничение на группу инерции тривиально. Объяснение этому можно дать совершенно геометрическое: надо рассмотреть X и Y как схемы над $\mathbb{Z}$ и доказать, что отображение $Y \to X$ будет этальным накрытием вне p. Это следует из того, что Y получается из X наложением условия в p (дополнительное условие касается только p). И из неразветвленности этого морфизма схем следует, что характер, который таким образом получается, будет тоже неразветвлен.

А второй факт состоит в том, что если $v = p$, то характер φ_v, наоборот, полностью разветвлен. Что я имею в виду, когда говорю «полностью разветвлен»? Ограничение на подгруппу инерции сюръективно отображает ее туда, куда характер бьет; т.е. характер сюръективен на подгруппе инерции группы Галуа максимального абелева расширения k_v.

Эти факты я не буду доказывать. То геометрическое объяснение, которое я дал, использует интерпретацию кривых Шимуры как грубых схем модулей. Можно этого не использовать, можно действовать по-другому. Но в любом случае используется теория полей классов и другие результаты: теоремы Нерона–Огга–Шафаревича и Серра–Тейта. А второй факт основан на теореме Мишеля Райно (Michel Raynaud) про конечные плоские группы.

Мы знаем следующее обстоятельство: эллиптическая кривая определена над тем полем, над которым определен ее модулярный инвариант. Но пара (A, i) (абелева поверхность с кватернионным умножением) уже не обязательно определена над полем вычетов $k(P)$ точки P, которая в пространстве модулей ее задает, потому что это только грубое пространство модулей. Джордан доказал, что это поисходит ровно тогда, когда $k(P)$ расщепляет B, т.е. B становится изоморфной матричной алгебре при подъеме поля с k на $k(P)$.

И теперь, соединяя все эти факты, мы получаем противоречие с условием теоремы. А именно, таким образом: если глобальный характер φ неразветвлен всюду вне p, то он пропускается через лучевую группу классов $Cl_k^{(p)}$. Поскольку φ полностью разветвлен в p, то его ограничение на подгруппу инерции дает сюръективное отображение. И отсюда получается противоречие с условием теоремы. Примерно такова схема доказательства. Всё это доказательство, должен сказать, на самом деле является более или менее пересказом того, что сделал Джордан. Надо просто чуть-чуть подправить его местами, и тогда оно переводится на геометрический язык.